Liljana Babinkostova

CONTACT INFORMATION

Department of Mathematics
Boise State University

E-mail: liljanababinkostova@boisestate.edu
Website: math.boisestate.edu/~liljanab

EDUCATION

Ss. Cyril and Methodius University, Skopje, Macedonia

Ph.D. in Mathematics, 2001

Ss. Cyril and Methodius University, Skopje, Macedonia

M.S. in Mathematics, 1997

Ss. Cyril and Methodius University, Skopje, Macedonia

B.S. in Mathematics and Computer Science, 1989

APPOINTMENTS

Boise State University, Boise ID USA

Associate Professor	**2011 - present**
Assistant Professor	**2007 - 2011**
Visiting Assistant Professor	**2003 - 2007**

Ss. Cyril and Methodius University, Skopje, MACEDONIA

Assistant Professor	**2002 - 2004**
Assistant (tenured)	**1997 - 2002**
Teaching Assistant (tenure track)	**1990 - 1997**

PUBLICATIONS

L. Babinkostova, C. Guido and Lj.D.R. Kocinac, *On relative gamma sets*, **East-West Journal of Mathematics** 2 (2000), 195–199.

L. Babinkostova, Lj. D. R. Kocinac, *Function Spaces and some relative covering properties*, **Far East Journal of Mathematics and Science** (Special Volume), Part II (2000), 247–255.

L. Babinkostova, *Relative Hurewicz property and games*, **Mathematica Macedonica** 1 (2003), 31–33.

L. Babinkostova, *Selective versions of screenability*, **Filomat** 17:2 (2003), 127–134.

L. Babinkostova and M. Scheepers, *Game on groups and information security*, **Proceedings of the III International Conference on Informatics and Information Technology** (2003).

L. Babinkostova, *Relative Hurewicz property and games*, **Mathematica Macedonica** 1 (2003), 31–33.

L. Babinkostova and M. Scheepers, *Combinatorics of open covers (IX): Basis properties*, **Note di Matematica** 22(2) (2003), 167–178.

L. Babinkostova, Lj. D. R. Kocinac and M. Scheepers, *Combinatorics of open covers (VIII)*, **Topology and its Applications** 140:1 (2004), 15–32.

L. Babinkostova and M. Scheepers, *An Infinite Game on Groups*, **Real Analysis Exchange** 29 (2) (2004), 1–15.

L. Babinkostova, Lj. D. R. Kočinac and M. Scheepers, *Notes on selection principles in topology (I): Paracompactness*, **Journal of the Korean Mathematical Society** 42:4 (2005), 709–721.

L. Babinkostova, *Selective screenability game and covering dimension*, **Topology Proceedings** 29:1 (2005), 1–5.

L. Babinkostova, *Metrizable groups and strict o-boundness*, **Mathematički Vesnik** 58:3-4 (2006), 131–138.

L. Babinkostova, Lj. D. R. Kočinac and M. Scheepers, *Combinatorics of open covers (XI): Menger- and Rothberger-bounded groups*, **Topology and its Applications** 154:7 (2007), 1269–1280.

L. Babinkostova, *When does the Haver property imply selective screenability?*, **Topology and its Applications** 154:9 (2007), 1971–1979.

L. Babinkostova and M. Scheepers, *Selection principles and countable dimension*, **Note di Matematica** 27:1 (2007), 5–15.

L. Babinkostova and M. Scheepers, *Products and selection principles*, **Topology Proceedings** 31 (2007), 431-443.

L. Babinkostova, *Selective screenability in topological groups*, **Topology and its Applications** 156:1 (2008), 2–9.

L. Babinkostova, *Selective screenability and the Hurewicz property*, **Topology Proceedings** 32 (2008), 245–252.

L. Babinkostova, *On some questions about selective separability*, **Mathematical Logic Quarterly** 55:5 (2009), 539–541.

L. Babinkostova and M. Scheepers, *Weakly infinite dimensional subsets of R^N*, **Topology and its Applications** 157:8 (2010), 1302–1313.

L. Babinkostova, *Topological games and covering dimension*, **Topology Proceedings**, 38 (2011), 99-120.

L. Babinkostova, *Topological groups and covering dimension*, **Topology and its Applications**, Vol. 158: 12 (2011), 1460-1470.

L. Babinkostova, B.A. Pansera and M. Scheepers, *Weak covering properties and infinite games*, **Topology and its Applications** Vol.159 (2012), 3644–3657.

L. Babinkostova, B. A. Pansera and M. Scheepers, *Weak covering properties and selection principles*, **Topology and its Applications** (2013), Vol.160, Issue 18, (2013), 2251–2271.

L. Babinkostova, K.W. Bombardier*, M.C. Cole*, T.A. Morrell* and C.B. Scott*, *Algebraic Properties of Generalized Rijndael-like Ciphers*[1], **Groups Complexity Cryptology**, Vol. 6, Issue 1, 37–54 (2014).

L. Babinkostova, A.M. Bowden*, A.M. Kimball*, K. Williams*, *A simplified and generalized treat-*

[1] The symbol * indicates an undergraduate student.

ment of DES related ciphers, **Cryptologia** 39:1 (2015), 3–24.

L. Babinkostova and M. Scheepers, *Selective strong screenability and a Game*, **Topology Proceedings** Vol. 47, (2016) 297–311.

Other Peer-Reviewed Publications

C. Humphreys* and L. Babinkostova (faculty advisor), *Prime Numbers and the Convergents of a Continued Fraction*, Proceedings of The National Conference On Undergraduate Research (NCUR), 309–316 (2013).

S. Craig* and L. Babinkostova (faculty advisor), *A Simplified Advanced Encryption Standard over a Field of Characteristic 3* , Proceedings of The National Conference On Undergraduate Research (NCUR), 307–317 (2014).

B. Barker*, M. Smith*, L. Babinkostova (faculty advisor) and M. Scheepers (faculty advisor), *Techniques to Enhance Security of an Authentication Protocol*, Proceedings of The National Conference On Undergraduate Research (NCUR), 811–820, (2015).

Papers in preparation

L. Babinkostova, K.W. Bombardier*, M.C. Cole*, T.A. Morrell* and C.B. Scott*, *Elliptic Reciprocity* (2015), (submitted).

L. Babinkostova, B. Pansera and M. Scheepers, *Selective versions of θ- and δ-separability.*

L. Babinkostova, J. Keller*, B. Schreiner*, J. Schreiner-McGraw* and K. Stubbs*, *Almost Translation Based Ciphers.*

L. Babinkostova, R. R. Dias and M. Scheepers, *On a covering property of Corson*

L. Babinkostova, Dmitriy Khripkov*, Nicholas Lacasse*, Bai Lin*, and Michelle Mastrianni*, *Permutation Sums and Generalized Hash Functions.*

Grants

College of Arts and Sciences

Principal Investigator **2010 - 2011**
Mini-Development grant to Aid Instruction, $980.00.

College of Arts and Sciences

Conference Travel Grant, $2,400.00 **2010, 2013, 2015, and 2016**

National Science Foundation

Principal Investigator **2011 –2014**
Research Experience for Undergraduates: Complexity in Algebra, Geometry and Applications, $329,300.00 (DMS-1062857).

Boise State University and National Science Foundation

Participating Faculty Mentor **2010, and 2012 – 2015**
STEM Talent Expansion Program (STEP), $5,000.00 (DUE-0856815).

National Science Foundation

Principal Investigator **2012 – 2013**
Boise Extravaganza in Set Theory Conference, $17,600.00 (DMS-1330103).

National Science Foundation

Principal Investigator **2014 – 2016**
Boise Extravaganza in Set Theory Conference, $38,366.00 (DMS-1440263).

National Science Foundation
Principal Investigator **2014 – 2017**
Boise Extravaganza in Set Theory Conference, $287,976.00 (DMS-1359425).

National Science Foundation
Principal Investigator **2016 – 2017**
Boise Extravaganza in Set Theory Conference, $5,000.00 (DMS-1440263).

Mathematical Association of America
Principal Investigator **2016 –2017**
TENSOR SUMMA: Research Experience in Mathematics for Young Scientists, $6,000.00.

State Board of Education/Higher Education Research Council
Principal Investigator **2016 – 2017**
Idaho Conference on Undergraduate Research, $15,000.00.

Honors and Awards

University Foundation Scholar Award for Service, 2016.

Presentations

Concerning γ-spaces, International Conference on Topology and its Applications, September 2–9, 2000, Ohrid, Macedonia.

Function Spaces and relative Star Covering Properties, International Conference on Topology and its Applications, September 2–9, 2000, Ohrid, Macedonia.

On some relative covering properties, Second Congress of Mathematics and Informatics, September 28–October 1, 2000, Ohrid, Macedonia,.

Selective Versions of Screenability, International Conference FILOMAT, August 26-30, 2001 in Niš, Serbia.

The property of Screenability, Mathematics Seminar, September 10, 2001, Institute of Mathematics, Ss. Cyril and Methodius University.

Relative Selection Principles on Metric Spaces. Invited Talk (November 9, 2001). University of Kragujevac, Serbia.

The Selection Principle $\mathsf{S}_c(\mathcal{A},\mathcal{B})$, Workshop on Coverings, Selections and Games, June 27–29, 2002, Lecce, Italy.

Relative Selection Principles in Metrizable Spaces. BEST conference [2], March 28–30, 2003, Boise State University. (Invited Talk)

Topology and its Applications to Pattern Recognition, Colloquium Talk (April 25, 2003), Boise State University.

Selective Screenability and Games, BEST conference, March 20–22, 2004, Boise State University.

Selective Screenability and Classical Selection Principles, Third Japan-Mexico Joint Meeting on Topology and its Applications (JAMEX III), December 6–10, 2004, Oaxaca, Mexico.

[2] Boise Extravaganza in Set Theory Conference

Selection principles and Basis Properties, BEST conference, March 25–27, 2005, Boise State University.

From $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ *to* $\mathsf{S}_c(\mathcal{A},\mathcal{B})$, Second Workshop on Coverings, Selections and Games, December 19–22, 2005, Lecce, Italy.

Measure and Boundedness Conditions in Topological Groups, BEST conference, March 31–April 2, 2006, Boise State University.

$\mathsf{S}_c(\mathcal{A},\mathcal{B})$*, Games, Powers and Groups*, Annual Meeting of the Association of Symbolic Logic, May 17–21, 2006, Montreal, Canada. (Invited Talk)

Selection Principles and Infinite Games, Colloquium talk (May 1, 2006), Boise State University.

Selective Screenability and the Haver Property, BEST conference, March 25–26, 2007, Idaho City, Idaho.

Selective Screenability, Products and Topological Groups, Third Workshop on Coverings, Selections and Games, April 25–29, 2007, Vrnjacka Banja, Serbia. (Invited Talk)

Selective Separability, BEST conference, March 28–30, 2008, Boise State University.

Selective Version of Some Topological Properties, Advances in Set-Theoretic topology, June 9–19, 2008, Erice, Italy.

The Length of Dimension Related Games, BEST conference, March 27–29, 2009, Boise State University.

Game Dimension for Separable Metric Spaces, Spring Topology and Dynamics Conference: Ulam Centennial Conference, March 7–11, 2009, Gainesville, FL.

Selective Screenability in Topological Groups, BEST conference, March 27-29, 2010, Boise State University.

Techniques for Actively Engaging Students in Learning Cryptology, Annual Meeting of the Pacific Northwest Section of the Mathematical Association of America, April 9–10, 2010, Seattle, Washington.

Game Dimension and Topological Groups, International conference on Analysis, Topology and Applications, June 20–25, 2010, Niš, Serbia.

Games and Dimension, Colloquium Talk (September 2, 2010), Boise State University.

Groups and Dimension, AMS Spring Western Section Meeting, April 30–May 1, 2011, University of Nevada, Las Vegas, NV. (Invited Talk)

Publishing Undergraduate Research, PNW MAA Meeting, April 20–21, 2012, University of Portland, OR. (Invited Talk)

REU in Mathematics at Boise State University, CUR (Council on Undergraduate Research) REU Symposium, October 26–27, 2013, Arlington, VA.

REU Site: Complexity in Algebra, Geometry and Applications, Great Ideas in STEM Education Symposium, January 13, 2014, Boise State University. (with J. Harlander and M. Scheepers)

Effectiveness of using Cryptography to improve Math Understanding and to Engage Undergrads in Research, 57^{th} Annual meeting of the Idaho Academy of Science and Engineering, March 19–20, 2015, Boise State University. (Invited Talk)

Broadening Participation in Undergraduate Research: Maximizing Student Experiences in Undergraduate Research and Bridging the Gap between Students and Educators from K-12 and Higher Education, NCUR: National Conference on Undergraduate Research, April 16–18, 2015, Eastern Washington University, WA. (joint with P. Pyke)

The Selective Strong Screenability Game, AMS Spring Western Section Meeting, April 18–19, 2015, University of Nevada, Las Vegas, NV. (Invited Talk)

REU Programs at Boise State University and Their Initiatives to Generate Interest in STEM Fields, STEM Innovations Conference, May 28–29, 2014, Boise, ID.

The Selective Strong Screenability Game, Set Theory Seminar, September 30, 2015, Boise State University.

Selective Strong Screenability and a Game, BEST Symposium, 96th Annual Meeting of the AAAS Pacific Division, June 14-17, 2015, San Francisco State University.

Gröstl, Permutations and Transversals, Algebra, Geometry and Cryptology (AGC) Seminar, December 4, 2015, Boise State University.

Selective Strong Screenability, Joint Mathematics Meetings, January 6–9, 2016, Seattle, WA.

Other Scholarly Presentations

Elliptic Curves over Finite Fields, Algebra, Geometry and Cryptology (AGC) Seminar, Spring 2011. (Series of Three Talks)

Continued Fractions and a Result of Erdoš, Algebra, Geometry and Cryptology (AGC) Seminar, Fall 2011. (Series of Two Talks)

Ideas and Methods in Game Theory and Cryptography, Graduate Seminar, November 13, 2015, Boise State University.

Workshops

NSF GRFP (Graduate Research Fellowship Program) Workshop, October 2, 2015, Boise State University.

Selected Student Presentations

K. Williams, *Luby - Rackoff over Finite Groups*, CUR Conference for Undergraduates Student Scholarship, October 16–17, 2011, Arlington, VA.

A. Kimball, *On the Design of Simplified DES Based on Elliptic Curves*, AMS Southeastern Section Meeting, March 9–10, 2012, Clayton State University, Georgia.

K. Williams, *Symmetric key Cryptography Over Non-binary Algebraic Structures*, American Association for Advancement of Science - Pacific Division (2012), Abstracts with Programs, Vol. 31(45).

T. Morell, *Computability and Complexity in Elliptic Curves and Cryptography: An Algorithm for Finding Elliptic Curves of Prime Order*, American Association for Advancement of Science - Pacific Division (2012), Abstracts with Programs, Vol. 31(45).

K. Bombardier, *Algebraic Properties of Generalized Rijndael-like Ciphers*, AMS Spring Western Sectional Meeting, April 13–14, 2013, University of Colorado, Boulder, CO.

T. Morrell, *Elliptic Reciprocity*, AMS Spring Eastern Sectional Meeting, April 5–6, 2013, Boston College, Chestnut Hill, MA.

M. Cole, *AES-like Ciphers over Arbitrary Finite Fields*, AMS Spring Eastern Sectional Meeting, April 5–6, 2013, Boston College, Chestnut Hill, MA.

H. de Kergorlay, *Generalizations of the Whirlpool Hash Function*, CUR Conference of Research Experiences for Undergraduates Student Scholarship October 27–28, 2013, Arlington, VA.

K. Stubbs, *Generalized AES-based Hash Functions*, Joint Mathematics Meetings, January 10–13, 2015, San Antonio, TX.

M. Mastrianni, N. Lacasse, and D. Khripkov, *Sums of Permutations in Cryptographic Hash Functions*, Joint Mathematics Meetings, January 6–9, 2016, Seattle, WA.

G. Currier*, C. Okasaki*, *Minimality of Uniform Splitting Families*, Joint Mathematics Meetings, January 6–9, 2016, Seattle, WA.

Teaching

Courses Taught at Boise State University

- Business Calculus
- Calculus I
- Calculus II
- Discrete and Foundational Mathematics
- Introduction to Number Theory
- Introduction to Number Theory and Group Theory
- Foundations of Cryptology
- Introduction to Algebraic Cryptology
- Topology
- Symmetric Key Cryptology
- Advanced Public Key Cryptology

Curriculum Development

- Initiated collaboration among Mathematics (College of Arts and Sciences), Computer Science (College of Engineering) and Information Technology Management (College of Business and Economics) to develop the *Minor in Cybersecurity program.* This program was officially launched under the auspices of the Department of Computer Science in Fall, 2015.
- Redesigned introductory upper division courses in Cryptology (MATH 307 and MATH 308) to accommodate a student base from a wider diversity of academic backgrounds
- Designed and introduced a graduate level course in Public Key Cryptology and a graduate course in Symmetric Key Cryptology
- Initiated a collaboration among colleagues from several STEM and non-STEM disciplines to develop an upper division course in Transdisciplinary Research Methods. This course will be offered for the first time in Fall 2016, team-taught by a diverse team of six faculty.

Mentoring

- *Undergraduate Level.* Mentored more than 20 undergraduate students during the regular academic year on independent research projects. Three of these mentorships resulted in professionally reviewed student publications in national student research journals.
- *Graduate Level.* Current advisor for a Master's level thesis (Nathan Schmidt, *Latin Squares and Their Applications*). Committee member of seven graduate student thesis in mathematics and computer science at Boise State University. Supervised numerous graduate course projects.

Student Scholarship and Professional Development

- An organizer of the Student Research Graduate Symposium, Boise State University, 2013–2014.

- Coordinator of the Student Research Program (SRP) Cohort Meetings, 2012–2014.
- Organizer of the Student Conference in Cryptology and Related Areas, 2009–present.[3]

Professional Service

Editorial Work

- Set Theory and Its Applications - L. Babinkostova and A. E. Caicedo, Boise State University, S. Geschke, University of Bonn, and M. Scheepers, Boise State University, Editors - AMS, 2011, 307 pp., Softcover, ISBN-10: 0-8218-4812-7, ISBN-13: 978-0-8218-4812-8.

Referee and Review Work

- Refereed papers for Cryptologia, East-West Journal of Mathematics, Mathematica Sinica, Matematički Vesnik, Topology Proceedings, Topology and its Applications, Mathematical Logic Quarterly, Journal of Combinatorics, Houston Journal of Mathematics, Central European Journal of Mathematics, and American Mathematical Monthly.
- Reviewer for NSF, Rustaveli NSF (Republic of Georgia), Mathematical Reviews, and Zentralblatt MATH.
- Reviewer of applications to the National Council on Undergraduate Research (CUR) "Posters on the Hill", CUR REU Symposium, National Conference on Undergraduate Research (NCUR)
- Reviewer of proposals for the 2016 Scientific Program of the Banff International Research Station (BIRS) for Mathematical Innovations and Discovery.
- Reviewer of proposals for the Mini-Development Grants to Aid Instruction Program, College of Arts and Sciences, Boise State University, 2007–2008.
- Judge for the MAA Undergraduate Student Poster Session, Joint Mathematics Meetings, 2015–2016.

Grant Review Panel Member

- NSF Research Experience For Undergraduates (REU) proposals reviewer and panelist (2014).

Professional Societies

- Elected Councilor of the Mathematics Division of the American Association for the Advancement of Science (AAAS) - Pacific Division [4].
- Elected Councilor of the Mathematics and Computer Science Division of the national Council on Undergraduate Research [5] (CUR).
- Member of the American Mathematical Society.
- Member of the Mathematical Association of America.

Conference Invited Organizer

- Workshop on Coverings, Selections and Games in Topology, December 19 –22, 2005, Lecce, Italy.
- Workshop on Coverings, Selections and Games in Topology, April 21–25, 2007, Vrnjacka Banja, Serbia.
- CUR Research Experience for Undergraduates (REU) Symposium, October 25–27, 2015, Arlington, VA.
- Annual Meeting of the Association of Symbolic Logic (ASL), 2017.

Seminar Organizer

- Set Theory Seminar, Boise State University, 2007 – 2012.
- Algebra, Geometry and Cryptology (AGC) Seminar, Boise State University, 2009–2012.

Outreach Activities

Presentations

- *The Mathematics in Cryptography.* Invited Talk (April, 2011). College of Western Idaho.
- *Women in Technical Careers*, March 20, 2014, Boise High School.

[3] http://math.boisestate.edu/ liljanab/BoiseCrypt.htm
[4] http://associations.sou.edu/aaaspd/
[5] http://www.cur.org/

- *Cryptography: the Bridge to Security*, Osher Lifelong Learning Institute, March 19, 2014, Boise State University. (Invited Talk)
- *Workshop: The Mathematics in Cryptology Workshop*, 2013 Summer Academy - Idaho Science and Aerospace Scholar Program, Boise State University. (joint workshop with M. Scheepers, July 14 and July 26)
- *Workshop: The Mathematics in Cryptology Workshop*, 2014 Summer Academy - Idaho Science and Aerospace Scholar Program, Boise State University. (joint workshop with M. Scheepers, July 18 and August 01)
- *Workshop: The Mathematics in Cryptology*, 2015 Summer Academy - Idaho Science and Aerospace Scholar Program, Boise State University. (joint workshop with M. Scheepers, July 17 and July 31)
- *Latin Squares: What do Mathematicians Do?*, Boise Math Circles, February 20, 2016, Boise State University.

Recruitment and Organizing

- Special lecture by Bruce Schneier [6], an internationally renowned security technologist and author, Chief Technology Officer at IBM Company and fellow at the Berkman Center for Internet and Society at Harvard Law School, 2010.
- Special lecture by Dr. Michael Dorff[7], Professor of Mathematics at Brigham Young University and the founder of the Center for Undergraduate Research in Mathematics (CURM), 2013.

Competitions

- Virtual Judge for eCYBERMISSION - Science, Technology, Engineering and Mathematics competition for K-12 students.

Academic Service

Committee Member

- Mathematics Course Evaluation Form Committee, 2010–2011.
- Summer Research Community (SRC) Committee, Boise State University, 201–present.
- Set Theory hiring committee, 2009.
- Interdisciplinary hiring committee, 2009.
- Evaluation committee for Math T.A. applicants, 2010.
- Advisory committee of the Idaho Science and Aerospace Scholar (ISAS), State Department of Education (2013–present).
- Program Chair, Idaho Conference on Undergraduate Research (2014–present). [8]
- Education Committee for the Pacific Division of the American Association for the Advancement of Science (2015–present).

Faculty Leadership

- REU Program in Mathematics: Complexity Across Disciplines (CAD).[9]
- Research Experience in Mathematics for Young Scientists Program (REMYS). [10]
- Student Research Program, Boise State University. [11]

[6] http://www.schneier.com/
[7] http://curm.byu.edu/
[8] http://academics.boisestate.edu/icur/
[9] http://math.boisestate.edu/reu/
[10] https://math.boisestate.edu/remys/
[11] http://academics.boisestate.edu/undergraduate/45811-2/

TOPOLOGY PROCEEDINGS
Volume 38, 2011
Pages 99–120

http://topology.auburn.edu/tp/

Topological Games and Covering Dimension

by

Liljana Babinkostova

Electronically published on August 16, 2010

Topology Proceedings

Web:	http://topology.auburn.edu/tp/
Mail:	Topology Proceedings Department of Mathematics & Statistics Auburn University, Alabama 36849, USA
E-mail:	topolog@auburn.edu
ISSN:	0146-4124

http://topology.auburn.edu/tp/
TOPOLOGY PROCEEDINGS
Volume 38 (2011)
Pages 99-120
E-Published on August 16, 2010

TOPOLOGICAL GAMES AND COVERING DIMENSION

LILJANA BABINKOSTOVA

Abstract. We consider a natural way of extending the Lebesgue covering dimension to various classes of infinite dimensional separable metric spaces.

All spaces in this paper are assumed to be separable metric spaces. Infinite games can be used in a natural way to define ordinal valued functions on the class of separable metric spaces. One of our examples of such an ordinal function coincides in any finite dimensional metric spaces with the covering dimension of the space, and may thus be thought of as an extension of Lebesgue covering dimension to all separable metric spaces. We will call this particular extension of Lebesgue covering dimension the *game dimension* of a space.

Game dimension is defined using a game motivated by a selection principle. Several natural classical selection principles are related to the one motivating game dimension, and their associated games can be used to compute upper bounds on game dimension. These games, and the upper bounds they provide, are interesting in their own right. We develop two such games and use them then to obtain upper bounds on our game dimension.

2010 *Mathematics Subject Classification.* Primary 54D20, 54D45, 55M10; Secondary 03E20.

Key words and phrases. countable dimensional, game dimension, infinite game, selection principle.

Topology and its Applications 158 (2011) 1460–1470

Contents lists available at ScienceDirect

Topology and its Applications

www.elsevier.com/locate/topol

Topological groups and covering dimension

Liljana Babinkostova

Department of Mathematics, Boise State University, Boise, ID 83725, United States

ARTICLE INFO

MSC:
primary 54D20, 54F45, 91A44
secondary 03E10

Keywords:
Countable dimensional
Game dimension
Selection principle
Infinite game

ABSTRACT

We consider a natural way of extending the Lebesgue covering dimension to various classes of infinite dimensional topological groups. The dimension function that we introduce extends Lebesgue covering dimension, has the hereditary property, and has a product theory that is more similar to the product theory for the finite dimensional case.

Published by Elsevier B.V.

All spaces in this paper are assumed to be separable and metrizable. In a previous paper [5] we introduced a dimension function called *game dimension* and denoted $\dim_{\mathsf{G}}(\cdot)$. Game dimension is an extension of Lebesgue covering dimension, denoted dim. For a separable metrizable space X, $\dim_{\mathsf{G}}(X) \leqslant \omega_1$ (Theorem 21 of [5]), and when $\dim_{\mathsf{G}}(X) < \omega_1$, then in fact X is a selectively screenable space[1] (Theorem 22 of [5]). Also, an infinite dimensional separable metric space X is countable dimensional if, and only if, $\dim_{\mathsf{G}}(X) = \omega$ (Theorem 2.2 of [2]). Though the theory of game dimension has some nice properties it has two drawbacks: Unlike in the finite or countable case, game dimension does not have nice hereditary properties for spaces with game dimension larger than ω, and its product theory also contains properties not present for the finite dimensional case it generalizes.

The purpose of this paper is to introduce a dimension function which extends Lebesgue covering dimension, has the hereditary property, and has a product theory that is more similar to the product theory for the finite dimensional case. The classical embedding theorem of Menger and Nöbeling provides one inspiration for this new dimension function, to be denoted $\dim_{\mathsf{nbd}}(\cdot)$: Every separable metric space X of covering dimension n is homeomorphic to a subspace of $\mathbb{R}^{2n+1}$. Now $\mathbb{R}^{2n+1}$ is a topological group under addition. A game theoretic characterization of finite dimension n in topological groups [4, Theorem 15] is the second source of inspiration for our new dimension function. Relative to the group $\mathbb{R}^{2n+1}$ we obtain $\dim(X) = \dim_{\mathsf{nbd}}(X)$. Indeed, for any topological group $(H, *)$ such that finite dimensional metric space X is homeomorphic to a subspace of H we have $\dim(X) = \dim_{\mathsf{nbd}}(X)$.

Given a topological group $(H, *)$ we define an infinite game on $(H, *)$ and use the length required so that TWO would have a winning strategy to define a dimension for H. Corresponding dimension values can be defined for topological subspaces X of H. When the group $(H, *)$ is clear from context, the dimension of X as derived from the game is denoted $\dim_{\mathsf{nbd}}(X)$.

For the class of separable metric spaces there are several choices of a separable metric group $(H, *)$ such that each separable metric space is homeomorphic to a subspace of the group. The group $(\mathbb{R}^{\mathbb{N}}, +)$ is such an example. By the classical theorem of Banach and Mazur that every separable metric space embeds isometrically into the topological group $(\mathrm{C}[0,1], +)$ of continuous real-valued functions on the unit interval endowed with the supremum norm, is another example. Any such group is a candidate relative to which a corresponding dimension function $\dim_{\mathsf{nbd}}$ may be defined. For the results presented

E-mail address: liljanababinkostova@boisestate.edu.

[1] We define the notion in the next section.

0166-8641/$ – see front matter Published by Elsevier B.V.
doi:10.1016/j.topol.2011.05.018

in this paper the reader may use either of these groups as the group relative to which the new dimension function is computed.

1. Selection principles, open covers and games

Let $(H,*)$ be a topological group with identity element e. We will assume that H is not compact. The collection of all open covers of H is denoted by $\mathcal{O}$. When X is a subset of H, the collection of all covers of X by sets open in H is denoted $\mathcal{O}_X$.

For a neighborhood U of the identity element of H the set $\mathcal{O}(U)=\{x*U\colon\ x\in H\}$ is an open cover of H. The symbol

$$\mathcal{O}_{nbd}=\big\{\mathcal{O}(U)\colon\ U \text{ a neighborhood of } e\big\}$$

denotes the collection of all such open covers of H.

Now we describe the relevant selection principles for this paper. Let S be an infinite set, and let $\mathcal{A}$ and $\mathcal{B}$ be collections of families of subsets of S.

The selection principle $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ is defined as follows:

For each sequence $(A_n\colon\ n\in\mathbb{N})$ of elements of $\mathcal{A}$ there is a sequence $(B_n\colon\ n\in\mathbb{N})$ such that for each n we have $B_n\in A_n$, and $\{B_n\colon\ n\in\mathbb{N}\}\in\mathcal{B}$.

The selection principle $\mathsf{S}_c(\mathcal{A},\mathcal{B})$, introduced in [2], is defined as follows:

For each sequence $(A_n\colon\ n<\infty)$ of elements of the family $\mathcal{A}$ there exists a sequence $(B_n\colon\ n<\infty)$ such that for each n B_n is a pairwise disjoint family refining A_n, and $\bigcup_{n<\infty}B_n$ is a member of the family $\mathcal{B}$.

We say that a space is *selectively screenable* if it has the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$. The class of spaces satisfying $\mathsf{S}_c(\mathcal{O},\mathcal{O})$ was introduced in [1]. We should point out that the selection principles $\mathsf{S}_c(\mathcal{O},\mathcal{O})$ and $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})$ in topological groups do not coincide. In Theorem 1.2 of [17] E. and R. Pol use Martin's Axiom to construct a vector subspace M of the separable Hilbert space ℓ_2 such that the topological group $(M,+)$ has the property $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})$ and the Menger property, but does not have the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$. It can be shown that the topological groups $(\mathbb{R}^{\mathbb{N}},+)$ and $(\mathsf{C}([0,1],+)$ do not have the property $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})$.

The metrizable space X is said to be *Haver* [10] with respect to a metric d if there is for each sequence $(\epsilon_n\colon\ n<\infty)$ of positive reals a sequence $(\mathcal{V}_n\colon\ n<\infty)$ where each $\mathcal{V}_n$ is a pairwise disjoint family of open sets, each of d-diameter less than ϵ_n, such that $\bigcup_{n<\infty}\mathcal{V}_n$ is a cover of X.

A topological space X has the *Hurewicz property* if for each sequence $\mathcal{U}_n$, $n<\infty$ of open covers of X there is a sequence $\mathcal{F}_n$, $n<\infty$ of finite sets such that each $\mathcal{F}_n\subset\mathcal{U}_n$, and for each $x\in X$, the set $\{n\colon\ x\notin\bigcup\mathcal{F}_n\}$ is finite. Every σ-compact space has the Hurewicz property, but not conversely.

Let α be an ordinal number.

The game $\mathsf{G}_1^{\alpha}(\mathcal{A},\mathcal{B})$ associated with the selection principle $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ is as follows:

The players play an inning per $\gamma<\alpha$. In the γ-th inning ONE first chooses an $A_\gamma\in\mathcal{A}$: TWO then responds with a $B_\gamma\in A_\gamma$. A play $A_0,B_0,\ldots,A_\gamma,B_\gamma,\ldots$ of length α is won by TWO if $\{B_\gamma\colon\ \gamma<\alpha\}\in\mathcal{B}$. Else, ONE wins.

The game $\mathsf{G}_c^{\alpha}(\mathcal{A},\mathcal{B})$ associated with the selection principle $\mathsf{S}_c(\mathcal{A},\mathcal{B})$ is as follows:

The players play an inning per $\gamma<\alpha$. In the γ-th inning ONE first chooses an $A_\gamma\in\mathcal{A}$: TWO then responds with a pairwise disjoint family of sets B_γ that refines A_γ. A play $A_0,B_0,\ldots,A_\gamma,B_\gamma,\ldots$ of length α is won by TWO if $\bigcup_{n\in\mathbb{N}}B_n\in\mathcal{B}$. Else, ONE wins.

When for a set S and families $\mathcal{A}$ and $\mathcal{B}$ there is an ordinal number α such that TWO has a winning strategy in the game $\mathsf{G}_c^{\alpha}(\mathcal{A},\mathcal{B})$ played on S, then we define $\mathsf{tp}_{\mathsf{S}_c(\mathcal{A},\mathcal{B})}(S)$ to be $\min\{\alpha\colon$ TWO has a winning strategy in $\mathsf{G}_c^{\alpha}(\mathcal{A},\mathcal{B})$ on $S\}$. We now define for topological group H the *neighborhood game dimension* of H, denoted $\mathsf{dim}_{\mathsf{nbd}}(H)$, by

$$1+\mathsf{dim}_{\mathsf{nbd}}(H)=\mathsf{tp}_{\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})}(H).$$

The neighborhood game dimension of a subset X of the group H, $\mathsf{dim}_{\mathsf{nbd}}(X)$ is defined similarly, using the ordinal $\mathsf{tp}_{\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_X)}(H)$.

In the proof of Theorem 2 we make a use of the following classical result of Hurewicz and Tumarkin [13, p. 288].

Theorem 1. *Let n be a non-negative integer. If X is a separable metric space and if for each m, $\mathsf{dim}(A_m)\leqslant n$ and $A_m\subseteq X$ is closed, then $\mathsf{dim}(\bigcup_{m=1}^{\infty}A_m)\leqslant n$.*

The following theorem is a starting point for exploring the neighborhood game dimension of a topological group and its subspaces.

Theorem 2. *Let $(H,*)$ be a metrizable group and let X be a subset of H. Then the following are equivalent*:

(1) $\dim(X) = n$.
(2) $\dim_{\mathsf{nbd}}(X) = n$.

Proof. The proof of (1) $\Rightarrow$ (2) is similar to the proof of the corresponding statement in Theorem 22. We give an inductive proof of (2) $\Rightarrow$ (1). Throughout the proof, when we work with a metrizable group $(H,*)$, we shall assume we have fixed a metric d and a neighborhood basis $(U_n\colon\ n<\infty)$ of the identity element e of H so that $diam_d(U_n) < \frac{1}{n}$ for all n.

Let $n=0$ and $(H,*)$ be a metrizable group and let X be a subset of H for which TWO has a winning strategy, say σ, in $G_c^1(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_X)$. Put $C_\emptyset = \bigcap\{\bigcup\sigma(\mathcal{O}(U_n))\colon\ n<\omega\}$.

Claim 1: $C_\emptyset$ is zero-dimensional.

For consider an $x\in C_\emptyset = \bigcap\{\bigcup\sigma(\mathcal{O}(U_n))\colon\ n<\infty\}$. For each n choose a neighborhood $V_n(x)\in\sigma(\mathcal{O}(U_n))$. Since for each n we have $diam_d(V_n(x)) < \frac{1}{n}$, the set $\{V_n(x)\cap C_\emptyset\colon\ n<\infty\}$ is a neighborhood basis for x in $C_\emptyset$. Observe also that each $V_n(x)$ is closed in $C_\emptyset$ because the set $V = \bigcup\sigma(\mathcal{O}(U_n))\setminus V_n(x)$ is open in H, and so $C_\emptyset\setminus V_n(x) = C_\emptyset\cap V$ is open in $C_\emptyset$. Thus each element of $C_\emptyset$ has a basis consisting of clopen sets.

Claim 2: $X\subseteq C_\emptyset$.

Suppose not: Choose $x\in X\setminus C_\emptyset$ and then choose n with $x\notin\bigcup\sigma(\mathcal{O}(U_n))$. Then $(\mathcal{O}(U_n), \sigma(\mathcal{O}(U_n)))$ is a play of $G_c^1(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_X)$ lost by TWO, contradicting that σ is a winning strategy for TWO.

Let $n<\omega$ be given and assume that the following two statements hold at n:

(a) If $(H,*)$ is a metrizable group such that TWO has a winning strategy in $G_c^{n+1}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O})$ on H, then $\dim(H)\leqslant n$.
(b) If $(H,*)$ is a metrizable group and X is a subset of H such that TWO has a winning strategy in $G_c^{n+1}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_X)$, then $\dim(X)\leqslant n$.

We show that (a) and (b) also hold at $n+1$.

Towards proving (a) at $n+1$, let $(H,*)$ be a metrizable group such that TWO has a winning strategy in $G_c^{n+2}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O})$ on H and let σ be such a winning strategy for TWO. Define $C_\emptyset = \bigcap\{\bigcup\sigma(\mathcal{O}(U_n))\colon\ n<\omega\}$. As before $\dim(C_\emptyset)=0$. Then for each m, $X_m = H\setminus(\bigcup\sigma\mathcal{O}(U_m))$ is closed in H and has covering dimension $\leqslant n$. To see that $\dim(X_m)\leqslant n$, we argue as follows: Define from the winning strategy σ for TWO in $G_c^{n+2}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O})$ on H the following strategy, σ_m, in the game $G_c^{n+1}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_{X_m})$ played on the subset X_m of H:

$$\sigma_m\big(\mathcal{O}(U_{k_1}),\dots,\mathcal{O}(U_{k_j})\big) = \sigma\big(\mathcal{O}(U_m),\mathcal{O}(U_{k_1}),\dots,\mathcal{O}(U_{k_j})\big),\quad j\leqslant n+1.$$

We claim that σ_m is a winning strategy for TWO in the game $\mathsf{G}_c^{n+1}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_{X_m})$. For suppose that σ_m is not a winning strategy for TWO. Look at a play $\mathcal{O}(U_{m_1}), \mathcal{O}(U_{m_2}),\dots,\mathcal{O}(U_{m_{n+1}})$ by ONE for which TWO, using strategy σ_m, looses. Then the union of the $(n+1)$ sets

$$\bigcup\sigma_m\big(\mathcal{O}(U_{m_1})\big),\qquad \bigcup\sigma_m\big(\mathcal{O}(U_{m_1}),\mathcal{O}(U_{m_2})\big),\quad\dots,\quad \bigcup\sigma_m\big(\mathcal{O}(U_{m_1}),\mathcal{O}(U_{m_2}),\dots,\mathcal{O}(U_{m_{n+1}})\big)$$

doesn't cover X_m. But then the union of the $(n+2)$ sets $\bigcup\sigma(\mathcal{O}(U_m)), \bigcup\sigma(\mathcal{O}(U_m),\mathcal{O}(U_{m_1})), \bigcup\sigma(\mathcal{O}(U_m),\mathcal{O}(U_{m_1}),\mathcal{O}(U_{m_2})),\dots,\bigcup\sigma(\mathcal{O}(U_m)),\mathcal{O}(U_{m_1}),\mathcal{O}(U_{m_2}),\dots,\mathcal{O}(U_{m_{n+1}})$ doesn't cover $H = X_m\cup(\bigcup\sigma(\mathcal{O}(U_m)))$, contradicting the fact that σ is a winning strategy for TWO in the game on H.

By part (b) of the induction hypothesis, $\dim(X_m)\leqslant n$. But, each $X_m\subset H$ is closed, so by Theorem 1 $\dim(\bigcup_{m=1}^\infty X_m)\leqslant n$. But $\bigcup_{m=1}^\infty X_m = \bigcup_{m=1}^\infty(H\setminus(\bigcup\sigma(U_m))) = H\setminus\bigcap_{m=1}^\infty(\bigcup\sigma(\mathcal{O}(U_m))) = H\setminus C_\emptyset$. So, $H = C_\emptyset\cup(\bigcup_{m=1}^\infty X_m)$. Since $C_\emptyset$ is zero-dimensional and $\dim(\bigcup_{m=1}^\infty X_m)\leqslant n$ we have $\dim(H)\leqslant n+1$.

In a very similar way we prove (b) at $n+1$, namely: If $(H,*)$ is a metrizable group and X is a subset of H for which TWO has a winning strategy in $G_c^{n+2}(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_X)$, then $\dim(X)\leqslant n+1$.

This completes the inductive proof. □

We also have the following satisfying property of the neighborhood game dimension in the case of countable dimensional spaces:

Lemma 3. *([4]) Let H be a metrizable group. The following are equivalent*:

(1) *H is countable dimensional.*
(2) $\dim_{\mathsf{nbd}}(H) = \omega$.

We find that for every finite dimensional space $X \subseteq H$, $\dim_{\mathsf{nbd}}(X) = \dim(X)$, and for each countable (and not finite) dimensional space $X \subseteq H$, $\dim_{\mathsf{nbd}}(X) = \omega$. Note that the concept $\dim_{\mathsf{nbd}}$ is defined relative to the group H. Except when we indicate otherwise, we assume H is $\mathbb{R}^{\mathbb{N}}$ or $C[0,1]$.

2. Selected examples and basic theorems

A few examples from classical and recent literature are useful in illustrating some of the properties of the dimension function $\dim_{\mathsf{nbd}}$. For the reader's convenience we collect some of these here for reference further in the paper.

Example 1. (L. Rubin et al. [21]) There exists a strongly infinite dimensional complete metric space $\mathbb{M}$ which is totally disconnected.

Example 2. (R. Pol [19]) There is a compact metric space $\mathbb{K}$ of the form $\mathbb{L} \cup \mathbb{M}$ where $\mathbb{L}$ provided by Theorem 4 is a union of countably many compact finite dimensional spaces.

Example 3. (J. van Mill and R. Pol) There exists a complete metric space $\mathbb{V}$ with the properties that $\mathbb{V} = X \cup Y$ where X is countable dimensional and every $C \subseteq \mathbb{V} \setminus X$ which is closed in $\mathbb{V}$ is countable dimensional, but $\mathbb{V} \times \mathbb{V}$ is strongly infinite dimensional [14, Example 1.1].

Example 4. (E. Pol and R. Pol) There exists a complete metric space $(\mathbb{E}, d)$ such that $\mathbb{E} = X \cup Y$ where X is countable dimensional and every $C \subseteq \mathbb{E} \setminus X$ which is closed in $\mathbb{E}$ is countable dimensional, but $\mathbb{E} \times \mathbb{E}$ does not have the Haver property in the equivalent metric $\rho((x_1, x_2), (y_1, y_2)) = \max\{d(x_1, y_1), d(x_2, y_2)\}$ [18].

Example 5. (E. Pol) There exists a separable metric space $\mathbb{F}$ of the form $X \cup Y$ such that X is countable dimensional and for any closed subset C of $\mathbb{F}$ such that $C \subseteq Y$, C is zero-dimensional, and there is a zero-dimensional subset B of the real line such that $\mathbb{F} \times B$ is strongly infinite dimensional [16, Example 1].

Example 6. (E. Pol and R. Pol) Assume Martin's Axiom. There is a vector subspace $\mathbb{G}$ of the separable Hilbert space ℓ_2 which has the property $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O})$ and the Menger property, but does not have the property $\mathsf{S}_c(\mathcal{O}, \mathcal{O})$ [17, Theorem 1.2].

Example 7. $(\mathbb{R}^{\mathbb{N}}, +)$ is the group of sequences of real numbers with the operation of coordinatewise addition. Every separable metric space is homeomorphic to a subspace of this group.

Example 8. $(C[0,1], +)$ is the group of continuous real-valued functions on the closed unit interval with the operation of pointwise addition. Every separable metric space embeds isometrically into this group.

The following theorems are among the fundamental tools we use to compute upper bounds for $\dim_{\mathsf{nbd}}$:

Theorem 4 *(Lelek). If (X, d) is a complete metric space which is not compact, then it has a compactification $\mathsf{L}(X)$ of the form $X \cup C$ where C is a union of countably many compact finite dimensional spaces.*

Theorem 5 *(Hurewicz–Tumarkin). ([13]) Let n be a non-negative integer. A separable metric space X is n-dimensional if, and only if, it is the union of $n+1$ but not fewer zero-dimensional subsets.*

Another basic tool is the following theorem (Theorem 2 of [4]) slightly adapted:

Theorem 6. *Let $(H, *)$ be a metrizable topological group and let X be a subspace of H. The following are equivalent*:

(1) $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}}, \mathcal{O}_X)$ *holds.*
(2) *X has the Haver property in all left invariant metrics of $(H, *)$.*

The following fact is Theorem 5 of [3]:

Theorem 7. *For a subspace X of a metrizable Hurewicz space Y the following are equivalent*:

(1) $\mathsf{S}_c(\mathcal{O}, \mathcal{O}_X)$ *holds.*
(2) *X has the Haver property in some equivalent metric of Y.*
(3) *X has the Haver property in all equivalent metrics of Y.*

And the following fact is Theorem 5 of [4]:

Corollary 8. *For a subspace X of a metrizable group $(H,*)$ with the Hurewicz property the following are equivalent*:

(1) $\mathsf{S}_c(\mathcal{O},\mathcal{O}_X)$ *holds.*
(2) $\mathsf{S}_c(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_X)$ *holds.*

3. The relationship between the dimension functions $\dim_{\mathsf{G}}$ and $\dim_{\mathsf{nbd}}$

It is convenient that game dimension provides an upper bound for $\dim_{\mathsf{nbd}}$, since there are already some techniques (see [5]) for computing game dimension:

Theorem 9. *Let $(H,*)$ be a topological group and let $X\subseteq H$ be a subspace of H. Then*

$$\dim_{\mathsf{nbd}}(X)\leqslant\dim_{\mathsf{G}}(X)\leqslant\dim_{\mathsf{G}}(H).$$

Proof. Let σ be a winning strategy for TWO in the game $\mathsf{G}_c^{1+\alpha}(\mathcal{O},\mathcal{O})$ played on X. Define a strategy τ for TWO in the game $\mathsf{G}_c^{1+\alpha}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_X)$ as follows: For any open neighborhood U of the identity of H, consider the open cover $\mathcal{O}_X(U)=\{X\cap x*U\colon\ x\in G\}$ of X, and the corresponding open cover $\mathcal{O}(U)=\{x*U\colon\ x\in G\}$ of H.

To define $\tau(\mathcal{O}(U_1),\dots,\mathcal{O}(U_n))$, compute in X the disjoint refinement

$$\sigma\big(\mathcal{O}_X(U_1),\dots,\mathcal{O}_X(U_n)\big)$$

of $\mathcal{O}_X(U_n)$. By Theorem II.21.1 on p. 226 of [13] there is a canonical disjoint family $\mathcal{F}$ of open sets in H such that $\{X\cap U\colon\ U\in\mathcal{F}\}=\sigma(\mathcal{O}_X(U_1),\dots,\mathcal{O}_X(U_n))$. Define $\tau(\mathcal{O}(U_1),\dots,\mathcal{O}(U_n))=\mathcal{F}$.

Then τ is a winning strategy for TWO in the game $\mathsf{G}_c^{1+\alpha}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_X)$. This establishes that $\dim_{\mathsf{nbd}}(X)\leqslant\dim_{\mathsf{G}}(X)$. The fact that $\dim_{\mathsf{G}}(X)\leqslant\dim_{\mathsf{G}}(H)$ follows from Theorem 12 below. □

We shall see that the inequality between $\dim_{\mathsf{nbd}}$ and $\dim_{\mathsf{G}}$ can in fact be strict, even for completely metrizable spaces.

Corollary 10. *For any topological group $(H,*)$ which contains a homeomorphic copy of the space $\mathbb{K}$, we have* $\dim_{\mathsf{nbd}}(\mathbb{K})=\omega+1$.

Proof. $\mathbb{K}$ is not countable dimensional, so by Theorem 15 of [4], $\dim_{\mathsf{nbd}}(\mathbb{K})>\omega$. Now apply Theorem 9 and the fact from [5] that $\dim_{\mathsf{G}}(\mathbb{K})=\omega+1$. □

4. Monotonicity of $\dim_{\mathsf{nbd}}$

A well-known classical theorem states

Theorem 11 *(Monotonicity). If Y is a finite dimensional metric space and $X\subseteq Y$, then* $\dim(X)\leqslant\dim(Y)$.

This monotonicity theorem does not hold for the dimension function $\dim_{\mathsf{G}}$: The compact metric space $\mathbb{K}$ of Example 2 contains the strongly infinite dimensional subspace $\mathbb{M}$ of Example 1, and by the results of [5], $\dim_{\mathsf{G}}(\mathbb{K})=\omega+1$ while $\dim_{\mathsf{G}}(\mathbb{M})=\omega_1$.

The monotonicity theorem holds for our new dimension function $\dim_{\mathsf{nbd}}$.

Theorem 12. *Let $(H,*)$ be a topological group and let $X\subseteq Y\subseteq H$ be subspaces of H. Then*

$$\dim_{\mathsf{nbd}}(X)\leqslant\dim_{\mathsf{nbd}}(Y)\leqslant\dim_{\mathsf{nbd}}(H).$$

Proof. Let α be the minimal ordinal such that TWO has a winning strategy in the game $\mathsf{G}_c^{1+\alpha}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})$ on H. Let σ be such a winning strategy for TWO. Then σ is also a winning strategy for TWO in the game $\mathsf{G}_c^{1+\alpha}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_Y)$. It follows that the least β such that TWO has a winning strategy in $\mathsf{G}_c^{1+\beta}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O}_Y)$ is no larger than α, and thus $\dim_{\mathsf{nbd}}(Y)\leqslant\dim_{\mathsf{nbd}}(H)$. A similar argument shows that $\dim_{\mathsf{nbd}}(X)\leqslant\dim_{\mathsf{nbd}}(Y)$. □

The space $\mathbb{M}$ of Example 1 is a subspace of $\mathbb{K}$, is complete and is strongly infinite dimensional. By Theorem 22 of [5] we have $\dim_{\mathsf{G}}(\mathbb{M})=\omega_1$. But by Theorem 12 and Corollary 10, $\dim_{\mathsf{nbd}}(\mathbb{M})=\omega+1$.

5. Products

Menger's product theorem [13, Theorem II.VIII on p. 301] states:

Theorem 13. *For X and Y finite dimensional separable metric spaces,*

$$\dim(X \times Y) \leqslant \dim(X) + \dim(Y).$$

Thus, when $\dim(Y) = 0$, we have $\dim(X \times Y) = \dim(X)$. This particular consequence of Menger's product theorem also holds for our new dimension function $\dim_{\mathrm{nbd}}$ as is shown below in Theorem 14. The analogue of Theorem 14 does not hold for game dimension $\dim_{\mathrm{G}}$. To see this consider Example 1 in [16]: Examining the details of this example we see that a separable metric space X and a set B of real numbers are constructed so that $\dim_{\mathrm{G}}(X) = \omega + 1$ and $\dim_{\mathrm{G}}(B) = 0$, but $\dim_{\mathrm{G}}(X \times B) = \omega_1$.

Theorem 14. *For $(H, *)$ and $(K, *)$ topological groups and $(K, *)$ zero-dimensional,*

$$\dim_{\mathrm{nbd}}(H \times K) = \dim_{\mathrm{nbd}}(H).$$

Proof. Fix an ordinal α with $\dim_{\mathrm{nbd}}(H) = \alpha$ and let σ be a winning strategy for TWO in the game $\mathrm{G}_c^{1+\alpha}(\mathcal{O}_{\mathrm{nbd}}, \mathcal{O})$ on $(H, *)$.

Define a strategy τ of TWO as follows: When in inning γ ONE chooses a neighborhood $U_\gamma \times V_\gamma$, TWO applies strategy σ to find

$$\sigma\big(\mathcal{O}(U_\delta)\colon\ \delta \leqslant \gamma\big),$$

a disjoint refinement of $\mathcal{O}(U_\gamma)$. Since H is zero-dimensional, choose a disjoint refinement $\mathcal{H}_\gamma$ of $\mathcal{O}(V_\gamma)$ such that $\mathcal{H}_\gamma$ covers H. Define

$$\tau\big(\mathcal{O}(U_\delta \times V_\delta)\colon\ \delta \leqslant \gamma\big) := \big\{A \times B\colon\ A \in \sigma\big(\mathcal{O}(U_\delta)\colon\ \delta \leqslant \gamma\big) \text{ and } B \in \mathcal{H}_\gamma\big\}.$$

It is clear that $\tau(\mathcal{O}(U_\delta \times V_\delta)\colon\ \delta \leqslant \gamma)$ is a disjoint family of open sets. We must see that it refines $\mathcal{O}(U_\gamma \times V_\gamma)$, and that TWO wins each play of length $1 + \alpha$ played using τ.

Let $A \times B \in \tau(\mathcal{O}(U_\delta \times V_\delta)\colon\ \delta \leqslant \gamma)$ be given. Choose an $x \in H$ with $A \subseteq x * U_\gamma$, and choose a $y \in K$ with $B \subseteq y * V_\gamma$. Then $A \times B \subseteq (x, y) * U_\gamma \times V_\gamma$ and the latter is an element of $\mathcal{O}(U_\gamma \times V_\gamma)$.

To see that TWO wins a play of length $1 + \alpha$, consider an $(x, y) \in H \times K$. Since σ is a winning strategy for TWO in $\mathrm{G}_c^{1+\alpha}(\mathcal{O}_{\mathrm{nbd}}, \mathcal{O})$ on H, find a $\gamma < 1 + \alpha$ with $x \in \bigcup \sigma(\mathcal{O}(U_\delta)\colon\ \delta \leqslant \gamma)$, and choose $A \in \sigma(\mathcal{O}(U_\delta)\colon\ \delta \leqslant \gamma)$ with $x \in A$. Since $\mathcal{H}_\gamma$ covers K, find a $B \in \mathcal{H}_\gamma$ with $y \in B$. Then we have

$$(x, y) \in A \times B \in \tau\big(\mathcal{O}(U_\delta \times V_\delta)\colon\ \delta \leqslant \gamma\big). \qquad \square$$

More generally, the following analogues of Menger's Product Theorem hold for the dimension function $\dim_{\mathrm{nbd}}$:

Theorem 15. *For $(H, *)$ and $(K, *)$ topological groups and $(K, *)$ finite dimensional, and $\dim_{\mathrm{nbd}}(H) = \alpha + n$ where α is a limit ordinal and $0 \leqslant n < \omega$,*

$$\dim_{\mathrm{nbd}}(H \times K) \leqslant \dim_{\mathrm{nbd}}(H) + \dim_{\mathrm{nbd}}(K) \cdot n.$$

Proof. Consider the case when $n > 0$. Let the dimension of K be k. Then write $K = \bigcup_{j=1}^{k+1} K_j$ where each K_j is zero-dimensional. Also, write $\alpha = \bigcup_{j=1}^{k+1} S_j$ where each S_j has order type α. For each j let σ_j be a winning strategy for TWO in the game $\mathrm{G}_c^{\alpha+n}(\mathcal{O}_{\mathrm{nbd}}, \mathcal{O})$ played on $H \times K_j$ as in Theorem 14. Now play the first α innings as follows: In inning $\gamma < \alpha$ first identify j with $\gamma \in S_j$. Then put

$$\tau(\mathcal{U}_\nu\colon\ \nu \leqslant \gamma) = \sigma_j(\mathcal{U}_\mu\colon\ \mu \leqslant \gamma \text{ and } \mu \in S_j).$$

After α innings, TWO has completed α innings in each of the games associated with the different $H \times K_j$, using a winning strategy for each of the corresponding games. Thus, for each j, the uncovered part of $H \times K_j$ requires $\leqslant n$ additional innings to cover. This has dimension less than or equal to n. By Theorem 5 the union of these k sets has dimension at most $k \cdot n - 1 = \dim(H) \cdot n - 1$. By Theorem 2 covering this requires no more than $k \cdot n$ additional innings. $\square$

Analogous arguments can be used to prove the following two theorems.

Theorem 16. *For $(H,*)$ and $(K,*)$ topological groups and $(K,*)$ countable dimensional, and $\dim_{\mathrm{nbd}}(H)$ a successor ordinal,*

$$\dim_{\mathrm{nbd}}(H\times K)\leqslant \dim_{\mathrm{nbd}}(H)+\dim_{\mathrm{nbd}}(K).$$

Theorem 17. *For $(H,*)$ and $(K,*)$ topological groups and $(K,*)$ countable dimensional, and $\dim_{\mathrm{nbd}}(H)$ a limit ordinal,*

$$\dim_{\mathrm{nbd}}(H\times K)=\dim_{\mathrm{nbd}}(H).$$

6. The union theorem

For finite dimensional metric spaces we have the following classical theorem:

Theorem 18 *(Union Theorem). If X and Y are finite dimensional subspaces of a metric space Z then*

$$\dim(X\cup Y)\leqslant \dim(X)+\dim(Y)+1.$$

A corresponding theorem holds for $\dim_{\mathrm{nbd}}$. First we define, as in [6], for ordinals α and β the "sum" $\alpha\oplus\beta$ as follows: Write $\alpha=\alpha'+m$ and $\beta=\beta'+n$ where α' and β' are limit ordinals or zero and $m,n<\omega$,

$$\alpha\oplus\beta=\begin{cases}\alpha & \text{if } \alpha'>\beta',\\ \alpha+n & \text{if } \alpha'=\beta',\\ \beta & \text{otherwise.}\end{cases}$$

Theorem 19 *(Union Theorem). If X and Y are subspaces of a separable metric space Z then*

$$\dim_{\mathrm{nbd}}(X\cup Y)\leqslant \dim_{\mathrm{nbd}}(X)\oplus\dim_{\mathrm{nbd}}(Y).$$

Proof. Choose winning strategies σ_X and σ_Y for TWO in the corresponding games of the corresponding lengths. If $\alpha'>\beta'$, then write $\beta'=S_1\cup S_2$ where S_1 and S_2 are disjoint sets, each of order type β'. During the first β' innings, if the inning number is in S_1, TWO plays the strategy σ_X, and if the inning number is in S_2, TWO plays σ_Y. After these innings TWO plays σ_Y for the next finite number of innings until Y is covered, and then plays σ_X the rest of the innings until X is also covered. This takes α innings in total. A similar argument shows that if $\alpha'<\beta'$, then TWO wins the game on $X\cup Y$ in β innings. Thus assume that $\alpha'=\beta'$. Then using the above schedule based on S_1 and S_2 we see that after α' innings the uncovered part of X is $(m-1)$-dimensional, and the uncovered part of Y is $(n-1)$-dimensional. By Theorem 18 the dimension of the uncovered part of $X\cup Y$ is at most $m+n-1$. Thus, covering this part requires at most $m+n$ additional innings. □

7. Discussion of examples

We now discuss neighborhood dimension for a number of examples from the literature. Towards this discussion we now collect some facts that are needed.

Theorem 20. *Let X be a completely metrizable separable metric space with compactification $\mathsf{L}(X)$ as in Theorem 4. Assume that for each natural number n we have $\dim_{\mathsf{G}}(\mathsf{L}(X)^n)\leqslant\alpha_n$. Then for the subgroup $\langle\mathsf{L}(X)\rangle$ of $\mathsf{C}[0,1]$ generated by an isometric copy of $\mathsf{L}(X)$, $\dim_{\mathsf{G}}(\langle\mathsf{L}(X)\rangle)\leqslant\alpha$, where $\alpha=\sup\{\alpha_n\colon n<\omega\}$.*

Fact A. If the subset X of a topological group $(G,*)$ is such that $\dim_{\mathrm{nbd}}(X)<\omega_1$, then $\mathsf{S}_c(\mathcal{O}_{\mathrm{nbd}},\mathcal{O}_X)$ holds.

Regarding uniformities and uniformizable spaces we refer the reader to [11,12] or [22]. For metrizable space X, and a metric d of X, define for each $\epsilon>0$ the set $D_{d,\epsilon}:=\{(x,y)\in X\times Y\colon\ d(x,y)<\epsilon\}$. Then $\mathcal{D}_d$ is the uniformity on X generated by the metric d. For $U\in\mathcal{D}_d$ and for $x\in X$ we define $U[x]=\{y\in X\colon\ (x,y)\in U\}$. Then $\mathcal{O}(U)=\{U[x]\colon\ x\in X\}$ is an open cover of X. We declare

$$\mathcal{O}(d)=\big\{\mathcal{O}(U)\colon\ U\in\mathcal{D}_d\big\}.$$

Then $\mathcal{O}(d)$ is the family of "d-uniform" open covers of X. In this context one can show:

Fact B. A metrizable space X has the Haver property with respect to the metric d if, and only if, X has the property $\mathsf{S}_c(\mathcal{O}(d),\mathcal{O})$.

Fact C. (E. Pol and R. Pol [18, Comment D]) A metrizable space X has the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$ if, and only if, for each metric d generating the topology, (X,d) has the Haver property.

Fact D. Let $(G,*)$ be a metrizable group and let μ be a left invariant metric on G. If the metric space (X,d) embeds isometrically into (G,μ), then the relativization to this isometric copy of X of the open covers of G in the family $\mathcal{O}_{\mathsf{nbd}}$ is isomorphic to the metric uniformity $\mathcal{O}(d)$ on X.

Example 1: $\mathbb{M}$. Since $\mathbb{M}$ is strongly infinite dimensional it does not have the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$, and $\dim_{\mathsf{G}}(\mathbb{M})=\omega_1$. By Fact B and Fact C there is a compatible metric, say d, on $\mathbb{M}$ such that $\mathsf{S}_c(\mathcal{O}(d),\mathcal{O})$ fails. Embedding $(\mathbb{M},d)$ isometrically into the group $(\mathsf{C}[0,1],+)$. Now using Facts A and D we see that for this isometric copy of $\mathbb{M}$, say $\mathbb{M}'$, we have $\dim_{\mathsf{nbd}}(\mathbb{M}')=\omega_1$.

On the other hand, $\mathbb{M}$ is a subspace of $\mathbb{K}$ and for any compatible metric d of $\mathbb{K}$, $(\mathbb{M},d)$ embeds isometrically into $\langle\mathbb{K}\rangle$, the topological group generated by $\mathbb{K}$ considered as a subspace of, for example, the topological group $(\mathsf{C}[0,1],+)$. By the discussion following Theorem 12 and by Theorem 9 we have $\dim_{\mathsf{nbd}}(\mathbb{M})=\omega+1$, and $\dim_{\mathsf{nbd}}(\langle\mathbb{M}\rangle)\leqslant\omega^2$ (see the discussion of Example 2).

Example 2: $\mathbb{K}$. As noted earlier, $\dim_{\mathsf{G}}(\mathbb{K})=\omega+1=\dim_{\mathsf{nbd}}(\mathbb{K})$. It was shown in [5] that for each n $\dim(\mathbb{K}^n)\leqslant\omega\cdot n+1$, and thus by Theorem 9, $\dim_{\mathsf{nbd}}(\mathbb{K}^n)\leqslant\omega\cdot n+1$. Then Theorem 20 implies that $\dim_{\mathsf{nbd}}(\langle\mathbb{K}\rangle)\leqslant\omega^2$.

Example 3: $\mathbb{V}$. Examination of Example 1.1 in [14] illustrates complex behavior of the dimension function $\dim_{\mathsf{nbd}}(\cdot)$ with respect to products. J. van Mill and R. Pol constructed a complete separable metric space $\mathbb{V}$ such that $\dim_{\mathsf{G}}(\mathbb{V})\leqslant\omega\cdot 2$, and yet $\mathbb{V}\times\mathbb{V}$ does not have the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$, implying $\dim_{\mathsf{G}}(\mathbb{V}\times\mathbb{V})=\omega_1$. The space $\mathbb{V}$ has the following structure:

$$\mathbb{V}=X\cup Y$$

where X is countable dimensional, and for any closed subset C of $\mathbb{V}$ disjoint from X, C is countable dimensional.

Since $\dim_{\mathsf{G}}(\mathbb{V})\leqslant\omega\cdot 2$, Theorem 9 implies that all isometric copies of $\mathbb{V}$ in $\mathsf{C}[0,1]$ (or any metrizable group that isometrically embeds $\mathbb{V}$, endowed with a metric generating the topology) we have $\dim_{\mathsf{nbd}}(\mathbb{V})\leqslant\omega\cdot 2$.

Let $\mathsf{L}(\mathbb{V})$ be a compactification of $\mathbb{V}$ as in Theorem 4. Then a standard argument shows that we still have $\dim_{\mathsf{G}}(\mathsf{L}(\mathbb{V}))\leqslant\omega\cdot 2$.

Lemma 21. *For each positive integer n, $\dim_{\mathsf{nbd}}(\mathsf{L}(\mathbb{V})^n)\leqslant\omega\cdot(n+1)$.*

Proof. The proof is by induction on n. First recall that

(i) $\mathbb{V}$ is a complete metric space of the form $X\cup Y$ where X is countable dimensional, and each closed subset of Y (disjoint from X) is countable dimensional.
(ii) $\mathbb{V}\times\mathbb{V}$ is strongly infinite dimensional.
(iii) $\mathsf{L}(\mathbb{V})$ is a compactification of $\mathbb{V}$ of the form $\mathbb{V}\cup C$ where C is a union of countably many compact finite dimensional spaces.

For $n=1$: $\dim_{\mathsf{G}}(\mathsf{L}(\mathbb{V}))\leqslant\omega\cdot 2$ is clear, so by Theorem 12, $\dim_{\mathsf{nbd}}(\mathsf{L}(\mathbb{V}))\leqslant\omega\cdot 2$.

For $n=k+1$: Assume that for all $j\leqslant k$, $\dim_{\mathsf{nbd}}(\mathsf{L}(\mathbb{V})^j)\leqslant\omega\cdot(j+1)$. Consider the space $\mathsf{L}(\mathbb{V})^n=\mathsf{L}(\mathbb{V})^{k+1}$. The subspace $\mathsf{L}(\mathbb{V})^{k+1}\setminus Y^{k+1}$ is the union of $k+1$ subspaces $\mathsf{L}(\mathbb{V})^i\times(\mathsf{L}(\mathbb{V})\setminus Y)\times\mathsf{L}(\mathbb{V})^{k+1-i-1}=S_i$, $1\leqslant i\leqslant k+1$. Each S_i is homeomorphic to $\mathsf{L}(\mathbb{V})^k\times(\mathsf{L}(\mathbb{V})\setminus Y)$. By the induction hypothesis, $\dim_{\mathsf{nbd}}(\mathsf{L}(\mathbb{V})^k)\leqslant\omega\cdot(k+1)$. Since $\mathsf{L}(\mathbb{V})\setminus Y$ is countable dimensional an argument in the proof of Theorem 15, and by extension Theorem 17, shows that $\dim_{\mathsf{nbd}}(\mathsf{L}(\mathbb{V})^k)\times(\mathsf{L}(\mathbb{V})\setminus Y)\leqslant\omega\cdot(k+1)$. Then Theorem 19 implies that

$$\dim_{\mathsf{nbd}}\big(\mathsf{L}(\mathbb{V})^{k+1}\setminus Y^{k+1}\big)\leqslant\omega\cdot(k+1).$$

Let σ be a strategy in $\mathsf{G}_c^{\omega\cdot(k+1)}(\mathcal{O}_{nbd},\mathcal{O})$ for TWO such that after $\omega\cdot(k+1)$ innings have been played, the subspace $\mathsf{L}(\mathbb{V})^{k+1}\setminus Y^{k+1}$ of $\mathsf{L}(\mathbb{V})^{k+1}$ has been covered by an open set. The uncovered part of $\mathsf{L}(\mathbb{V})^{k+1}$ is compact and a subset of Y^{k+1}. Since the projection on each of the $k+1$ coordinates of this compact subset of Y^{k+1} is a compact subset of Y, each projection is countable dimensional compact. But then the uncovered part of $\mathsf{L}(\mathbb{V})^{k+1}$ is compact, countable dimensional. By Theorem 3 TWO can cover the remaining part of $\mathsf{L}(\mathbb{V})^{k+1}$ in another ω innings. It follows that

$$\dim_{\mathsf{nbd}}\big(\mathsf{L}(\mathbb{V})^{k+1}\big)\leqslant\omega\cdot(k+1)+\omega=\omega\cdot(k+2).$$

This completes the proof. □

Thus, considering $\mathbb{V}$ as a subspace of $\mathsf{C}[0,1]$, the subgroup $\langle\mathsf{L}(\mathbb{V})\rangle$ of $\mathsf{C}[0,1]$ has $\dim_{\mathsf{nbd}}(\langle\mathsf{L}(\mathbb{V})\rangle)\leqslant\omega^2$. Thus, in any metric d of $\mathsf{L}(\mathbb{V})$, the corresponding isometric copy of $\mathbb{V}$ in $\mathsf{C}[0,1]$ has the property that $\dim_{\mathsf{nbd}}(\mathbb{V}^n)\leqslant\omega\cdot(n+1)$.

On the other hand, by Facts B and C, there is a metric d generating the topology of $\mathbb{V}\times\mathbb{V}$ for which $\mathsf{S}_c(\mathcal{O}(d),\mathcal{O})$ is false. The corresponding isometric copy in $\mathsf{C}[0,1]$ of the metric space $(\mathbb{V}\times\mathbb{V},d)$, denoted as $(\mathbb{V}\times\mathbb{V})'$, satisfies $\dim_{\mathsf{nbd}}((\mathbb{V}\times\mathbb{V})')=\omega_1$.

Example 4: $\mathbb{E}$. Similar arguments can be applied to $\mathbb{E}$: Since $\dim_{\mathsf{G}}(\mathbb{E})\leqslant\omega\cdot 2$ we find that $\dim_{\mathsf{nbd}}(\mathbb{E}')\leqslant\omega\cdot 2$ for any isometric copy $\mathbb{E}'$ of $\mathbb{E}$ in a group with left invariant metric. Since $\mathbb{E}$ is a complete metric space, it has a metrizable compactification $\mathsf{L}(\mathbb{E})$ as in Theorem 4. For the corresponding topological group $\langle\mathsf{L}(\mathbb{E})\rangle$ generated in $\mathsf{C}[0,1]$ we find as in Example 3 that $\dim_{\mathsf{nbd}}(\langle\mathsf{L}(\mathbb{E})\rangle)\leqslant\omega^2$. Note that for positive integers n, for metrics d inherited from $\mathsf{L}(\mathbb{E})^n$ by $\mathbb{E}^n$, isometric copies of $\mathbb{E}^n$ in $\mathsf{C}[0,1]$ have $\dim_{\mathsf{nbd}}(\mathbb{E}^n)\leqslant\omega\cdot(n+1)$.

But for some metric that generates the topology of $\mathbb{E}^2$ the isometric copy, $(\mathbb{E}\times\mathbb{E})'$, in $\mathsf{C}[0,1]$ has $\dim_{\mathsf{nbd}}((\mathbb{E}\times\mathbb{E})')=\omega_1$.

Example 5: $\mathbb{F}$. Examination of this example shows that $\dim_{\mathsf{G}}(\mathbb{F})=\omega+1$. By Theorem 9 $\dim_{\mathsf{nbd}}(\mathbb{F})\leqslant\omega+1$. But since $\mathbb{F}$ is not countable dimensional, we have $\dim_{\mathsf{nbd}}(\mathbb{F})=\omega+1$.

Let $\mathbb{C}$ denote the Cantor ternary set, endowed with the topology inherited from the real line. In [16] it was shown that $\mathbb{F}$ can be taken as a subspace of $\mathbb{C}\times\mathbb{K}$, and that for some subspace $\mathbb{B}$ of $\mathbb{C}$, the subspace $\mathbb{F}\times\mathbb{B}$ of the space $\mathbb{C}\times\mathbb{K}\times\mathbb{C}$ is strongly infinite dimensional. Thus, $\dim_{\mathsf{G}}(\mathbb{F}\times\mathbb{B})=\omega_1$.

Since for each positive integer n, $\mathbb{C}^n$ is homeomorphic to $\mathbb{C}$, results of [5] imply that $\dim_{\mathsf{G}}((\mathbb{C}\times\mathbb{K}\times\mathbb{C})^n)=\dim_{\mathsf{G}}(\mathbb{K}^n)\leqslant\omega\cdot n+1$. But then we have by Theorem 20 that $\dim_{\mathsf{G}}(\langle\mathbb{C}\times\mathbb{K}\times\mathbb{C}\rangle)\leqslant\omega^2$. Then for any isometric copy of $\mathbb{F}$ in $\mathbb{C}\times\mathbb{K}\times\mathbb{C}$ we have for the subgroup $\langle\mathbb{F}\rangle$ of $\langle\mathbb{C}\times\mathbb{K}\times\mathbb{C}\rangle$ that $\dim_{\mathsf{nbd}}(\langle\mathbb{F}\rangle)\leqslant\omega^2$. We also have for each n, that $\dim_{\mathsf{nbd}}(\mathbb{F}^n)\leqslant\omega\cdot n+1$. Similar remarks apply to isometric copies of $\mathbb{F}\times\mathbb{B}$ in $\mathbb{C}\times\mathbb{K}\times\mathbb{C}$.

On the other hand, by Facts B, C and D, there is a metric d on $\mathbb{F}\times\mathbb{B}$ for which an isometric copy of $(\mathbb{F}\times\mathbb{B},d)$ in $\mathsf{C}[0,1]$, say $(\mathbb{F}\times\mathbb{B})'$, has $\dim_{\mathsf{nbd}}((\mathbb{F}\times\mathbb{B})')=\omega_1$.

Example 6: $\mathbb{G}$. In the construction of the topological group $\mathbb{G}$ in [17] the authors construct two special separable metrizable spaces $S\subset T$ with special properties (see Proposition 5.1 in [17]). The spaces S and T are embedded in a special way into ℓ^2 by an embedding σ. See the beginning of the proof of Theorem 1.2 on p. 1502 of [17].

The proof of (17) of [17] shows that for each space A of cardinality less than $2^{\aleph_0}$, the space $A\times T$ has $\dim_{\mathsf{G}}(A\times T)=\omega+1$. An analysis of the space T constructed for Proposition 5.1 of [17] reveals that for each positive integer n we have $\dim_{\mathsf{G}}(T^n)\leqslant\omega^\omega$ (the least countable ordinal that exceeds ω^n for each n).

Thus the vector subspace $\langle\sigma(T)\rangle$ of ℓ_2 satisfies $\dim_{\mathsf{G}}(\langle\sigma(T)\rangle)\leqslant\omega^\omega$, and $\sigma(T)$ is homeomorphic to a closed subspace of $\langle\sigma(T)\rangle$. It follows that for the Menger subspace S of T constructed for Proposition 5.1 of [17], $\sigma(S)$ generates the vector subspace $\mathbb{G}=\langle\sigma(S)\rangle$ of $\langle\sigma(T)\rangle$ which still has the Menger property, and which contains a homeomorphic copy of $\sigma(S)$ as a closed subspace. From the properties of the subspace $\sigma(S)$ it follows that $\dim_{\mathsf{G}}(\mathbb{G})=\omega_1$. From Theorem 9 we find that $\dim_{\mathsf{nbd}}(\mathbb{G})\leqslant\omega^\omega$. For any translation invariant metric d on the vector space $\mathbb{G}$, $(\mathbb{G},d)$ has the Haver property.

By Facts B, C and D the topological space $\mathbb{G}$ has a metrization d (which cannot be translation invariant) in which it does not have the Haver property, and a corresponding isometric copy, $\mathbb{G}'$ in $\mathsf{C}[0,1]$ has $\dim_{\mathsf{nbd}}(\mathbb{G}')=\omega_1$: However, this embedding does not embed $\mathbb{G}$ as a subgroup of $\mathsf{C}[0,1]$. Starting from the space S: An isometric copy which does not have the Haver property is present in $\mathsf{C}[0,1]$, and this isometric copy generates a subgroup $[S]$ of $\mathsf{C}[0,1]$ for which the uniform norm on $\mathsf{C}[0,1]$ provides a translation invariant metric with respect to which the subgroup $[S]$ fails the Haver property. Since the Haver property is hereditary, the linear subspace of $\mathsf{C}[0,1]$ generated by this isometric copy of S also does not have the Haver property with respect to this translation invariant metric.

Example 7: $\mathbb{R}^{\mathbb{N}}$. The neighborhood dimension $\dim_{\mathsf{nbd}}(\mathbb{R}^{\mathbb{N}})=\omega_1$. The space $\mathbb{R}^{\mathbb{N}}$ is hereditarily Lindelöf. By a theorem of P. Daniels and G. Gruenhage [9] TWO wins the game $\mathsf{G}_1^{\omega_1}(\mathcal{O},\mathcal{O})$ and so TWO wins the game $\mathsf{G}_1^{\omega_1}(\mathcal{O}_{nbd},\mathcal{O})$ which is a special case of $\mathsf{G}_c^{\omega_1}(\mathcal{O}_{\mathsf{nbd}},\mathcal{O})$. But, TWO can not win the game $\mathsf{G}_c^{\alpha}(\mathcal{O}_{nbd},\mathcal{O})$ in fewer than ω_1 innings since $(\mathbb{R}^{\mathbb{N}},+)$ is not $\mathsf{S}_c(\mathcal{O}_{nbd},\mathcal{O})$. To see this, recall that the group generated by the Hilbert cube, $[0,1]^{\mathbb{N}}$, is σ-compact and consequently has the Hurewicz property. It is easy to see that any subgroup of a group with $\mathsf{S}_c(\mathcal{O}_{nbd},\mathcal{O})$ has the $\mathsf{S}_c(\mathcal{O}_{nbd},\mathcal{O})$ property. Now, suppose $(\mathbb{R}^{\mathbb{N}},+)$ has $\mathsf{S}_c(\mathcal{O}_{nbd},\mathcal{O})$. Then the group generated by $[0,1]^{\mathbb{N}}$ as a subgroup of subgroup of $(\mathbb{R}^{\mathbb{N}},+)$ also has $\mathsf{S}_c(\mathcal{O}_{nbd},\mathcal{O})$ and by Theorem 5 of [5] we have that it must be selectively screenable. But by a theorem of J. Nagata, the Hilbert cube is strongly infinite dimensional and so it cannot be selectively screenable.

Considered as vector space the algebraic dimension of $\mathbb{R}^{\mathbb{N}}$, written $\dim_{\mathsf{alg}}(\mathbb{R}^{\mathbb{N}})$, is $2^{\aleph_0}$. We have for each finite n that

$$\dim_{\mathsf{nbd}}\big(\mathbb{R}^n\big)=n=\dim_{\mathsf{alg}}\big(\mathbb{R}^n\big).$$

The equation

$$\dim_{\mathsf{nbd}}\big(\mathbb{R}^{\mathbb{N}}\big)=\dim_{\mathsf{alg}}\big(\mathbb{R}^{\mathbb{N}}\big)$$

is equivalent to the Continuum Hypothesis.

Example 8: $\mathsf{C}[0,1]$. Also $\dim_{\mathsf{nbd}}(\mathsf{C}[0,1])=\omega_1$ and $\dim_{\mathsf{alg}}(\mathsf{C}[0,1])=2^{\aleph_0}$, and so the Continuum Hypothesis is equivalent to the statement that $\dim_{\mathsf{nbd}}(\mathsf{C}[0,1])=\dim_{\mathsf{alg}}(\mathsf{C}[0,1])$.

8. Remarks

As illustrated in some of the examples, the computation of $\dim_{\mathrm{nbd}}$ can depend on the ambient group, and on how a space is embedded as a subspace of a group. It seems important to know for which spaces X the dimension $\dim_{\mathrm{nbd}}(X)$ depends on the group into which X is embedded as subspace. A compact metrizable space has a unique uniformity – see 36.19 of [22] – and thus $\dim_{\mathrm{nbd}}(X)$ for a compact separable metric space X does not depend on the ambient group.

In examples of a separable metric space X where $\dim_{\mathsf{G}}(X) = \omega_1$ we were able to find an appropriate metric generating the topology of X such that an isometric embedding X' of this metric space in $\mathsf{C}[0,1]$ has $\dim_{\mathrm{nbd}}(X') = \omega_1$. The main tool for this was the fact that the example X failed to have property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$. We do not know of an example of a separable metric space X which has the property $\mathsf{S}_c(\mathcal{O},\mathcal{O})$, but $\dim_{\mathsf{G}}(X) = \omega_1$. We conjecture that there are such separable metric spaces.

Question 1. Let X be a separable metrizable space for which $\dim_{\mathsf{G}}(X) = \omega_1$. Is there an isometric copy X' of X in $\mathsf{C}[0,1]$ such that $\dim_{\mathrm{nbd}}(X') = \omega_1$?

As the reader may have noticed, for spaces that are not countable or finite dimensional and for which we have information about $\dim_{\mathrm{nbd}}$, this information is mostly in terms of upper bounds, with the obvious lower bound being $\omega + 1$. We suspect that our upper bounds are in fact sharp. Here is a specific question:

Question 2. Is $\dim_{\mathrm{nbd}}(\mathbb{G}) = \omega^\omega$?

Our results do not seem to indicate that $\dim_{\mathrm{nbd}}$ must be a limit ordinal for an infinite dimensional topological group.

Question 3. Is there an infinite dimensional separable metrizable topological group G for which $\dim_{\mathrm{nbd}}(G)$ is a successor ordinal?

There are other well-known dimension functions that were introduced for compact metrizable spaces by R. Pol [20] and by P. Borst [6] and [7]. These dimension functions assign ordinals larger than ω to some countable dimensional spaces: As an example, consider the Smirnov compacta S_α, $\alpha < \omega_1$. The reader could for example consult [8], which contains a description of these right after Definition 3 of [8]. Each Y_α is countable dimensional. Let $\dim_B$ denote the dimension function introduced by Borst, and let $\dim_P$ denote the dimension function introduced by Pol.

As a consequence of Theorem 2 of [8] we have for each ordinal α that $\dim_B(\mathsf{S}_\alpha) = \alpha$. By Theorem 3.3.8 of [6], $\dim_P(X) = \omega^{\dim_B(X)}$ whenever $\dim_B(X)$ is defined for an infinite dimensional compact metric space X. Thus for each infinite ordinal α

$$\dim_{\mathrm{nbd}}(\mathsf{S}_\alpha) = \omega \leqslant \alpha = \dim_B(\mathsf{S}_\alpha) < \omega^\alpha = \dim_P(\mathsf{S}_\alpha).$$

Thus, for each ordinal $\alpha > \omega \cdot 2$ we have, by Corollary 3.14 of [5], that

$$\dim_{\mathrm{nbd}}(\mathbb{K} \times \mathsf{S}_\alpha) \leqslant \omega \cdot 2 < \alpha \leqslant \dim_B(\mathbb{K} \times \mathsf{S}_\alpha).$$

It appears that in general, for separable metric spaces for which $\dim_B(X)$ is defined and infinite we have $\dim_{\mathrm{nbd}}(X) \leqslant \dim_B(X)$. However, a general comparison of these dimension functions at this time seems difficult, especially since very little is known about the values of $\dim_B$ on even classical examples such as $\mathbb{K}$.

Question 4. What is the minimal value of $\dim_B(\mathbb{K})$?

Acknowledgement

I thank the referee for a careful reading of the paper, and for remarks that improved the quality of the paper.

Appendix A

Following the referee's suggestion we include the proof of the following theorem from [2].

Theorem 22. *Let X be a metrizable space. Then the following are equivalent*:

(1) $\dim(X) = n$.
(2) *TWO has a winning strategy in* $\mathsf{G}_c^{n+1}(\mathcal{O},\mathcal{O})$.

Proof. (1) $\Rightarrow$ (2): Suppose that X is n-dimensional. We define the following strategy for TWO: Write $X = \bigcup_{1\leqslant i\leqslant n+1} X_i$ where each X_i is zero-dimensional. Let $\mathcal{U}$ be an element of $\mathcal{O}$. For $i \leqslant n+1$, consider $\mathcal{U}$ as a cover of X_i. Since X_i is zero-dimensional, find a pairwise disjoint family $\mathcal{V}_k$ of subsets of X_i open in X_i such that $\mathcal{V}_k$ covers X_i and refines $\mathcal{U}$. Choose a pairwise disjoint family $\sigma(\mathcal{U}, i)$ of sets open in X and refining $\mathcal{U}$ such that each element V of $\mathcal{V}_k$ is of the form $U \cap X_i$ for some $U \in \sigma(\mathcal{U}, i)$. Now TWO plays as follows: In inning 1 ONE plays $\mathcal{U}_1$, and TWO responds with $\sigma(\mathcal{U}_1, 1)$, thus covering X_1. When ONE has played $\mathcal{U}_2$ in the second inning TWO responds with $\sigma(\mathcal{U}_2, 2)$, thus covering X_2, and so on. And in the $(n+1)$-th inning, when ONE has chosen the cover $\mathcal{U}_{n+1}$ of X TWO responds with $\sigma(\mathcal{U}_{n+1}, n+1)$, covering X_{n+1}. This strategy evidently is a winning strategy for TWO in $(n+1)$-innings.

(2) $\Rightarrow$ (1): Let TWO have a winning strategy σ in $\mathsf{G}_c^{n+1}(\mathcal{O}, \mathcal{O})$. Let $\mathcal{U}$ be an open cover of X. Consider the plays of the game in which in each inning ONE chooses the cover $\mathcal{U}$ i.e. $\mathcal{V}_1 = \sigma(\mathcal{U}), \mathcal{V}_2 = \sigma(\mathcal{U}, \mathcal{U}), \ldots, \mathcal{V}_{n+1} = \sigma(\mathcal{U}, \mathcal{U}, \ldots, \mathcal{U})$. Each $\mathcal{V}_i$ is pairwise disjoint and $\mathcal{V} = \bigcup_{i=1}^{n+1} \mathcal{V}_i$ refines $\mathcal{U}$, covers X and has order at most $n+1$. Since the open cover $\mathcal{U}$ of X was arbitrary, Theorem 1 from [15] implies that $\dim(X) \leqslant n$. $\square$

References

[1] D.F. Addis, J.H. Gresham, A class of infinite dimensional spaces. Part I: Dimension theory and Alexandroff's problem, Fund. Math. 101 (1978) 195–205.
[2] L. Babinkostova, Selective screenability game and covering dimension, Topology Proc. 29 (2005) 13–17.
[3] L. Babinkostova, When does the Haver property imply selective screenability?, Topology Appl. 154 (2007) 1971–1979.
[4] L. Babinkostova, Selective screenability in topological groups, Topology Appl. 156 (2008) 2–9.
[5] L. Babinkostova, Topological games and covering dimension, Topology Proc. 38 (2011) 99–120.
[6] P. Borst, Classification of weakly infinite dimensional spaces Part I: Transfinite extension of the covering dimension, Fund. Math. 130 (1988) 1–25.
[7] P. Borst, Some remarks concerning C-spaces, Topology Appl. 154 (2007) 665–674.
[8] V.A. Chatyrko, On the dimension of products of infinite dimensional compacta, Sib. Math. J. 38 (1997) 807–816.
[9] P. Daniels, G. Gruenhage, The point-open types of subsets of the reals, Topology Appl. 37 (1990) 53–64.
[10] W.E. Haver, A covering property for metric spaces, Springer Lecture Notes in Math. 375 (1974) 108–113.
[11] J.R. Isbell, Uniform Spaces, Math. Surveys, vol. 12, The American Mathematical Society, 1964.
[12] J.L. Kelley, General Topology, Grad. Texts in Math., vol. 27, Springer-Verlag, 1975.
[13] K. Kuratowski, Topology, vol. 1, Academic Press, 1966.
[14] J. van Mill, R. Pol, A complete C-space whose square is strongly infinite-dimensional, Israel J. Math. 154 (2006) 209–220.
[15] P. Ostrand, Covering dimension in general spaces, Gen. Topol. Appl. 1 (1970) 209–221.
[16] E. Pol, A weakly infinite-dimensional space whose product with the irrationals is strongly infinite dimensional, Proc. Amer. Math. Soc. 98 (1986) 349–352.
[17] E. Pol, R. Pol, On metric spaces with the Haver property which are Menger spaces, Topology Appl. 157 (2010) 1495–1505.
[18] E. Pol, R. Pol, A metric space with the Haver property whose square fails this property, Proc. Amer. Math. Soc. 137 (2009) 745–750.
[19] R. Pol, A weakly infinite-dimensional compactum which is not countable-dimensional, Proc. Amer. Math. Soc. 82 (1981) 634–636.
[20] R. Pol, On classification of weakly infinite dimensional compacta, Fund. Math. 116 (1983) 169–188.
[21] L.R. Rubin, R.M. Schori, J.J. Walsh, New dimension-theory techniques for constructing infinite-dimensional examples, Gen. Topol. Appl. 10 (1979) 93–102.
[22] S. Willard, General Topology, Addison–Wesley Publishing Company, 1970.

Topology and its Applications 159 (2012) 3644–3657

Contents lists available at SciVerse ScienceDirect

Topology and its Applications

www.elsevier.com/locate/topol

Weak covering properties and infinite games

L. Babinkostova [a], B.A. Pansera [b], M. Scheepers [a,*]

[a] Department of Mathematics, Boise State University, Boise, ID 83725, United States
[b] Dipartimento di Matematica, Universita di Messina, Via F. Stagno d'Alcontres N. 31, 8166 Messina, Italy

ARTICLE INFO

Article history:
Received 14 February 2012
Received in revised form 13 September 2012
Accepted 16 September 2012

MSC:
03E35
54A35
54D20

Keywords:
Lindelöf
Menger
Rothberger
Weakly
Almost
Infinite game

ABSTRACT

We investigate game-theoretic properties of selection principles related to weaker forms of the Menger and Rothberger properties. For appropriate spaces some of these selection principles are characterized in terms of a corresponding game. We use generic extensions by Cohen reals to illustrate the necessity of some of the hypotheses in our theorems.

1. Introduction

A *Lindelöf space* is a topological space for which each open cover contains a countable subset covers the space. Some unresolved or undecidable problems about Lindelöf spaces have definite answers for spaces having a stronger version of the Lindelöf property. For example: Cardinality questions that are undecidable for classes of Lindelöf spaces have been resolved for the corresponding classes of *compact* spaces. While it is not known if regular T_3 Lindelöf spaces are D-spaces[1] it is known that each T_1 *Menger* space (a selective version of the Lindelöf property and defined later in our paper) is a D-space [1]. Whereas the Lindelöf property is not preserved by the product construction, compactness is.

In some cases where the Lindelöf property (or one of its strengthenings) is not preserved by a topological construction, it has been found that a weaker version of the Lindelöf property is preserved. Also, it has been found that some theorems true for Lindelöf spaces are in fact true for a wider class of spaces that have a weak version of the Lindelöf property. We consider two such weakenings of the Lindelöf property that have emerged in the literature.

To define these, let $\mathcal{O}$ denote the collection of all open covers of a space, let $\mathcal{D}$ denote the collection of families of open sets with union dense in the space, and let $\overline{\mathcal{O}}$ denote the collection of families $\mathcal{U}$ of open subsets of the space for which $\{\overline{U}\colon\ U \in \mathcal{U}\}$ covers the space.[2] A space is said to be *weakly Lindelöf* if each open cover contains a countable subset with

* Corresponding author.
E-mail addresses: liljanababinkostova@boisestate.edu (L. Babinkostova), bpansera@unime.it (B.A. Pansera), mscheepe@boisestate.edu (M. Scheepers).

[1] As we do not need the concept of a D-space elsewhere in our paper, it is left undefined.

[2] The symbol $\overline{V}$ denotes the closure of the set V. The notation $\overline{\mathcal{O}}$ is due to Boaz Tsaban.

0166-8641/$ – see front matter
http://dx.doi.org/10.1016/j.topol.2012.09.009

union dense in the space. Thus, weakly Lindelöf means that each element of $\mathcal{O}$ has a countable subset which is a member of $\mathcal{D}$. The notion of weakly Lindelöf appears to have been introduced in the 1959 paper [10] of Frolik. The name "weakly Lindelöf" however seems to have been coined by Hager and Mrowka (see the introductory paragraph of [6]). A thorough introduction to weakly Lindelöf spaces can be found in [6]. A topological space X is said to be *almost Lindelöf* if there is for each open cover $\mathcal{U}$ of X a countable subset $\mathcal{V}$ such that $\{\overline{V}\colon\ V \in \mathcal{V}\}$ is a cover of X. The notion of an almost Lindelöf space was introduced in the 1984 paper [36] by Willard and Dissanayake. The following implications hold among these three properties:

$$\text{Lindelöf} \Rightarrow \text{almost Lindelöf} \Rightarrow \text{weakly Lindelöf}.$$

Moreover, almost Lindelöf T_3-spaces are Lindelöf.

Various selective versions of the Lindelöf property, for example the Menger property or the Rothberger property (defined below), have characterizations in terms of infinite games. These game characterizations are powerful tools to derive other mathematical properties of these classes of spaces. We investigate the possibility of characterizing certain selective versions of the almost Lindelöf and the weakly Lindelöf properties by infinite games. To indicate to what extent some of the hypotheses of some of our results are necessary we also explore the preservation of selective versions of these properties under generic extensions of the universe. Behavior of these properties under topological constructions will be addressed in the paper [3].

2. Definitions

Recall the general framework for describing selection hypotheses (as in [15] and [23]): Let **N** denote the set of positive integers. Let $\mathcal{A}$ and $\mathcal{B}$ be collections of subsets of an infinite set. Then $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ denotes the following hypothesis:

For each sequence $(A_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{A}$ there is a sequence $(B_n\colon\ n \in \mathbb{N})$ such that, for each n, $B_n \in A_n$ and $\{B_n\colon\ n \in \mathbb{N}\}$ is an element of $\mathcal{B}$.

Then $\mathsf{S}_1(\mathcal{O},\mathcal{O})$ denotes the *Rothberger* property.

The symbol $\mathsf{S}_{fin}(\mathcal{A},\mathcal{B})$ similarly denotes the hypothesis:

For each sequence $(A_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{A}$ there is a sequence $(B_n\colon\ n \in \mathbb{N})$ such that, for each n, $B_n \subseteq A_n$ is finite, and $\bigcup\{B_n\colon\ n \in \mathbb{N}\}$ is an element of $\mathcal{B}$.

$\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$ denotes the *Menger* property.

Our conventions for the rest of the paper are: By "space" we mean a topological space. Unless stronger separation axioms are indicated specifically, we assume all spaces to be infinite and T_1. Undefined notation and terminology will be as in [9].

3. Preserving Lindelöf like properties in Cohen real generic extensions

It is well known that

Theorem 1. *Let $\mathbb{P}$ be a proper partial order and let X be a space.*

(1) *If X is non-Lindelöf, then $\mathbf{1}_{\mathbb{P}} \models$ "$\check{X}$ is not Lindelöf".*
(2) *If X is not almost Lindelöf, then $\mathbf{1}_{\mathbb{P}} \models$ "$\check{X}$ is not almost Lindelöf".*
(3) *If X is not weakly Lindelöf, then $\mathbf{1}_{\mathbb{P}} \models$ "$\check{X}$ is not weakly Lindelöf".*

Proof. These statements follow directly from Proposition 4.1 of [14]: Consider a ground model that satisfies ZFC. If $\mathbb{P}$ is a proper partially ordered set in this ground model and S is a ground model set, then for a countable set Y that is a subset of S but a member of the generic extension, there is a countable set Z that is a subset of S and is a member of the ground model, and contains Y. □

The Lindelöf property is preserved by adding Cohen reals or random reals (see for example [30]), but need not be preserved by countably closed forcing [33] or even certain ccc forcing extensions [12]. More information about these issues can be found in [16,30,33]. We now establish some corresponding results for the almost Lindelöf and the weakly Lindelöf properties.

For κ a fixed uncountable cardinal, $\mathbb{C}(\kappa)$ denotes the partially ordered set for adding κ Cohen reals generically: The underlying set, $\mathsf{Fn}(\kappa \times \omega, \omega)$, of elements of $\mathbb{C}(\kappa)$ is

$$\big\{p \subset (\kappa \times \omega) \times \omega\colon\ p \text{ a finite function with domain a subset of } \kappa \times \omega\big\}.$$

For p and q in $\mathsf{Fn}(\kappa \times \omega, \omega)$ we write $p < q$ if $q \subset p$. It is well known that forcing with $\mathbb{C}(\kappa)$ preserves cardinals and cofinalities, and that in the resulting model $2^{\aleph_0} \geqslant \kappa$. Since $\mathbb{C}(\kappa)$ is a proper partially ordered set, Theorem 1 applies to it.

Definition 2. For a positive integer n, an n-dowment is a family $\mathcal{L}_n$ of finite antichains of $\mathbb{C}(\kappa)$ such that:

(1) For each maximal antichain $\mathbb{A} \subset \mathbb{C}(\kappa)$ there is an $L \in \mathcal{L}_n$ such that $L \subseteq \mathbb{A}$.
(2) For each $p \in \mathbb{C}(\kappa)$ such that $|dom(p)| < n$ and for every collection $L_1, L_2, \ldots, L_n \in \mathcal{L}_n$ there are $q_1 \in L_1, \ldots, q_n \in L_n$, and there is $r \in \mathbb{C}(\kappa)$, such that $r \leqslant p$ and $r \leqslant q_i$ for each $i \leqslant n$.

The notion of an n-dowment as well as a proof of the existence of n-dowments is treated in Section 1 of [8].

3.1. Preserving weakly Lindelöf

Theorem 3. *Let $\kappa > \aleph_0$ be a cardinal. Let X be a topological space. If X is weakly Lindelöf, then in $\mathbf{V}^{\mathbb{C}(\kappa)}$ X is weakly Lindelöf.*

Proof. For each n let $\mathcal{L}_n$ be an n-dowment for $\mathbb{C}(\kappa)$. Let τ denote the (ground model) topology of X. Let $\dot{\mathcal{U}}$ be a $\mathbb{C}(\kappa)$-name such that

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{“}\dot{\mathcal{U}} \subseteq \check{\tau} \text{ is an open cover of } \check{X}\text{”}.$$

For each x choose a maximal antichain $\mathbb{A}_x \subseteq \mathbb{C}(\kappa)$ and ground model open sets $V_{p,x}$, $p \in \mathbb{A}_x$, such that $x \in V_{p,x}$ and $p \models \text{“}\check{V}_{p,x} \in \dot{U}\text{”}$. For each n choose $\mathbb{A}_{n,x} \in \mathcal{L}_n$ with $A_{n,x} \subseteq A_x$ and define $V_{n,x} = \bigcap\{V_{p,x}\colon\ p \in \mathbb{A}_{n,x}\}$. Then $V_{n,x}$ is open, and $\mathcal{U}_n = \{V_{n,x}\colon\ x \in X\}$ is an open cover of X in the ground model.

Since X is weakly Lindelöf, choose a countable set $\mathcal{V}_n \subseteq \mathcal{U}_n$ such that $\bigcup \mathcal{V}_n$ is dense in X.

Claim. $\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{“}(\forall V \in \check{\tau})(\exists n)(\exists U \in \check{\mathcal{V}}_n)(\exists \check{W} \in \dot{\mathcal{U}})(V \cap U \neq \emptyset \text{ and } U \subseteq \check{W})\text{”}$.

Fix $V \in \tau$ nonempty and fix an element $q \in \mathbb{C}(\kappa)$. Choose n so that $|dom(q)| \leqslant n$. Since $\bigcup \mathcal{V}_n$ is dense in X, choose $V_{n,x} \in \mathcal{V}_n$ such that $\emptyset \neq V \cap V_{n,x}$. Choose $p \in \mathbb{A}_{n,x}$ such that for an $r \in \mathbb{C}(\kappa)$ we have $r \leqslant q, p$. Then

$$r \models \text{“}\check{V} \cap \check{V}_{n,x} \neq \emptyset \text{ and } \check{V}_{n,x} \subseteq \check{V}_{p,x} \in \dot{\mathcal{U}}\text{”}.$$

Thus the set of $r \in \mathbb{C}(\kappa)$ forcing the statement in the claim is dense in $\mathbb{C}(\kappa)$. The claim follows.

Now let G be a $\mathbb{C}(\kappa)$-generic filter and let V be a ground model open set. In the generic extension we find an n and a $U \in \mathcal{V}_n$ and a $W \in \dot{\mathcal{U}}_G$ with $V \cap U \neq \emptyset$ and $U \subseteq W$. Thus, choose for each n and each $U \in \mathcal{V}_n$ for which this is possible, a $W_U \in \dot{\mathcal{U}}_G$ with $U \subseteq W_U$. Then $\{W_U\colon\ (\exists n)(U \in \mathcal{V}_n)\}$ is a countable subset of $\dot{\mathcal{U}}_G$ and has dense union in X. □

3.2. Preserving almost Lindelöf

Since T_3 almost Lindelöf spaces are Lindelöf, and since the Lindelöf property of the T_3 product space ${}^{\omega_1}2$ is not preserved by forcing with countably closed partially ordered sets, the almost Lindelöf property is not preserved by countably closed forcing. This phenomenon can also occur in generic extensions obtained by forcing with certain countable chain condition partially ordered sets. However, generic extensions by Cohen reals preserve the property of being almost Lindelöf.

Lemma 4. *Let $\kappa > \aleph_0$ be a cardinal number and let X be a topological space and let $U \subseteq X$ be an open subset of X. Then*

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{“}\overline{\check{U}} = \check{\overline{U}}\text{”}.$$

Proof. Note that the ground model open subsets of X is a basis for the topology of X in the generic extension. This implies that the ground model closure of a ground model set is equal to the closure of that ground model set in the generic extension. This argument applies to all generic extensions, not only the Cohen real extension. □

Using Lemma 4 and minor modifications in the proof of Theorem 3, one also obtains the following preservation theorem:

Theorem 5. *Let $\kappa > \aleph_0$ be a cardinal. If a topological space X is almost Lindelöf, then in $\mathbf{V}^{\mathbb{C}(\kappa)}$ X is almost Lindelöf.*

4. The Rothberger property and weakenings

For the properties considered in this section the following table contains the property name, its symbolic definition and, where available, a reference for where the property was introduced:

Property name	Definition	Source
Rothberger	$\mathsf{S}_1(\mathcal{O},\mathcal{O})$	[22]
Almost Rothberger	$\mathsf{S}_1(\mathcal{O},\overline{\mathcal{O}})$	[26, p. 251]
Weakly Rothberger	$\mathsf{S}_1(\mathcal{O},\mathcal{D})$	[7, p. 98]

The implications

$$\text{Rothberger} \Rightarrow \text{almost Rothberger} \Rightarrow \text{weakly Rothberger}$$

are irreversible, but almost Rothberger T_3-spaces are Rothberger spaces. It is clear that the Rothberger property implies the Lindelöf property, the almost Rothberger property implies the almost Lindelöf property, and the weakly Rothberger property implies the weakly Lindelöf property. The weakly Rothberger property and the almost Rothberger property have not been as extensively studied as the Rothberger property. The related properties $\mathsf{S}_1(\mathcal{D},\mathcal{D})$, $\mathsf{S}_1(\overline{\mathcal{O}},\mathcal{D})$ and $\mathsf{S}_1(\overline{\mathcal{O}},\overline{\mathcal{O}})$ have received some attention, but we will not report on these properties here.

The symbol $\mathsf{G}_1^{\omega}(\mathcal{A},\mathcal{B})$ denotes the following game: Players ONE and TWO play ω innings: In inning $n<\omega$ ONE first selects an O_n from $\mathcal{A}$, and then TWO responds with a $T_n \in O_n$. A play

$$O_0, T_0, \ldots, O_n, T_n, \ldots$$

is won by TWO if $\{T_n\colon\ n<\omega\}\in\mathcal{B}$. Otherwise, ONE wins.

For a specific instance of these games either TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{A},\mathcal{B})$, or ONE has a winning strategy in the game, or else neither player has a winning strategy in the game. In the last case the game is said to be *undetermined*.

The game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{O})$ was introduced by Galvin [11]. In [11] Galvin considers winning strategies for TWO in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{O})$ and he proves:

Theorem 6 *(Galvin). Let X be a Lindelöf space such that each one-element subset of X is a G_δ subset of X. Then the following are equivalent*:

(1) *TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{O})$ on X.*
(2) *X is a countable set.*

In [20] Pawlikowski proved the following fundamental theorem, characterizing the Rothberger property in terms of games:

Theorem 7 *(Pawlikowski). For a space X the following are equivalent*:

(1) *X has property $\mathsf{S}_1(\mathcal{O},\mathcal{O})$.*
(2) *ONE has no winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{O})$.*

Thus, in the class of Rothberger spaces whose singleton subsets are G_δ sets, the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{O})$ is undetermined if and only if, the space is uncountable.

Tkachuk considered the game of length ω for the weakly Rothberger property in [35], denoted there as the game Θ_*. Games seem to be unexamined for the almost Rothberger property. We now explore to what extent analogues of Theorem 6 and Theorem 7 hold for the weakly Rothberger spaces and the almost Rothberger spaces.

4.1. Games and the weakly Rothberger property

The following observation is essentially Proposition 2.6(iii) of [35]:

Lemma 8. *If X has a dense subspace Y and TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$ on Y, then TWO has a winning strategy in $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$ on X.*

It follows that on each separable space TWO has a winning strategy in $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$. We do not currently have a general characterization of spaces for which TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$. Theorem 9 below is the most general result we know that is for weakly Rothberger spaces an analogue of Theorem 6 for Rothberger spaces. Theorem 9 has been obtained earlier by Tkachuk and can be deduced from [35] Theorem 2.11(i) plus Theorem 3.3(2). Since Tkachuk derives this for a game dual of $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$ (Theorem 2.11(i)) and then introduces and proves the duality (Theorem 3.3(2)), we decided to include a new proof customized to our context here. Also note that although the blanket assumption in [35] is that spaces are at least Tychonoff, the arguments in [35] also work for the wider class of T_3 spaces.

Theorem 9 *(Tkachuk). If X is a first-countable T_3 space the following are equivalent*:

(1) *X is separable.*
(2) *TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$.*

Proof. The implication (1) $\Rightarrow$ (2) follows from the preceding remarks. We must prove that (2) $\Rightarrow$ (1). Thus, let X be a first countable topological space in which TWO has a winning strategy, σ, in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$. Let $\prec$ be a well-order of X. Let θ be an infinite regular cardinal which is so large that X, its topology, $\mathcal{O}$, ${}^{<\omega}\mathcal{O}$, $\mathcal{D}$, $\prec$, σ, and for each $x\in X$ a neighborhood base $(U_n(x)\colon\ n\in\mathbb{N})$ of $\{x\}$, are elements of H_θ. We may assume that $\mathcal{N}=\{(U_n(x)\colon\ n\in\mathbb{N})\colon\ x\in X\}$ is a member of H_θ. Let $(\mathcal{M},\in_{\mathcal{M}})$ be a countable elementary submodel of $(\mathsf{H}_\theta,\in_\theta)$ such that each of the objects above is an element of $\mathcal{M}$.

Claim 1. *For each finite sequence $(\mathcal{U}_1,\dots,\mathcal{U}_k)$ of open covers of X there is a point $x\in X$ such that for each neighborhood U of x there is an open cover $\mathcal{U}$ such that $U=\sigma(\mathcal{U}_1,\dots,\mathcal{U}_k,\mathcal{U})$.*

The argument for the proof of this claim is originally due to Galvin [11], and goes as follows: For suppose the contrary. Then choose for each $x\in X$ a neighborhood U_x such that for each open cover $\mathcal{U}$ of X, $U_x\neq\sigma(\mathcal{U}_1,\dots,\mathcal{U}_k,\mathcal{U})$. But then as $\mathcal{V}=\{U_x\colon\ x\in X\}$ is an open cover of X, we have that for some $y\in X$, $\sigma(\mathcal{U}_1,\dots,\mathcal{U}_k,\mathcal{V})=U_y$. This contradicts the selection of U_y, completing the proof of Claim 1.

The sentence in Claim 1 holds in $(\mathsf{H}_\theta,\in_\theta)$ and all its parameters are in $\mathcal{M}$, so the statement holds in $(\mathcal{M},\in_{\mathcal{M}})$. Thus, choose for each finite sequence ν of open covers of X an x_ν the $\prec$-least element of X satisfying Claim 1. Note that x_ν also satisfies Claim 1 in $(\mathsf{H}_\theta,\in_\theta)$, and is in H_θ also the $\prec$-first such element. The set $D=\{x_\nu\colon\ \nu\in{}^{<\omega}\mathcal{O}\}$ is definable from $\prec$, σ, X and ${}^{<\omega}\mathcal{O}$, all parameters in $\mathcal{M}$, and thus is a member of $\mathcal{M}$.

Enumerate $\mathcal{O}\cap\mathcal{M}$ bijectively as $(O_n\colon\ n\in\mathbb{N})$. Now $D\cap\mathcal{M}$ is the countable set $\{x_\nu\colon\ \nu\in{}^{<\omega}\{O_0,O_1,\dots,O_n,\dots\}\}$.

Claim 2. *$D\cap\mathcal{M}$ is dense in X.*

For suppose the contrary, and choose a nonempty open set U for which $\overline{U}\cap\mathcal{M}\cap D$ is the empty set. The latter is possible since X is T_3.

Since $x_\emptyset$ is a member of $\mathcal{M}$, and $\mathcal{N}=\{(U_n(x)\colon\ n\in\mathbb{N})\colon\ x\in X\}$ is a member of $\mathcal{M}$, also $(U_n(x_\emptyset)\colon\ n\in\mathbb{N})$ (which is definable from $\mathcal{N}$ and $x_\emptyset$, both parameters in $\mathcal{M}$) is in $\mathcal{M}$. But then $\{U_n(x_\emptyset)\colon\ n\in\mathbb{N}\}$ is an element, and subset of, $\mathcal{M}$. Since $x_\emptyset$ is not in $\overline{U}$, fix an m_1 with $U_{m_1}(x_\emptyset)\cap\overline{U}=\emptyset$. Then by Claim 1 $\mathcal{M}$ witnesses that there is an open cover $\mathcal{U}(\in\mathcal{M})$ of X such that $U_{m_1}(x_\emptyset)=\sigma(\mathcal{U})$. Thus, choose n_1 so that $U_{m_1}(x_\emptyset)=\sigma(O_{n_1})$.

Next, consider x_{n_1}. By the same considerations as above there is a neighborhood $U_{m_2}(x_{n_1})$ disjoint from $\overline{U}$, and an n_2 such that for the open cover O_{n_2} of X, $U_{m_2}(x_{n_1})=\sigma(O_{n_1},O_{n_2})$. Then apply these considerations to x_{n_1,n_2} to choose a neighborhood $U_{m_3}(x_{n_1,n_2})$ disjoint from $\overline{U}$, and an open cover O_{n_3} of X so that $U_{m_3}(x_{n_1,n_2})=\sigma(O_{n_1},O_{n_2},O_{n_3})$, and so on. Proceeding like this we obtain a σ-play

$$O_{n_1},\sigma(O_{n_1}),O_{n_2},\sigma(O_{n_1},O_{n_2}),\dots,O_{n_k},\sigma(O_{n_1},\dots,O_{n_k}),\dots$$

for which $\overline{U}\cap\bigcup_{k\in\mathbb{N}}\sigma(O_{n_1},\dots,O_{n_k})$ is the empty set. Since $\overline{U}$ has nonempty interior this contradicts the fact that σ is a winning strategy of TWO in $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$.

This completes the proof of (2) $\Rightarrow$ (1). $\square$

A. Bella informed us in a personal communication that he has further generalized Theorem 9 as follows:

Theorem 10 *(Bella). Let X be a first countable space. The following assertions are equivalent*:

(1) *There exists a countable set $D\subseteq X$ such that for any neighborhood assignment $\phi: D\to\tau(X)$, where $x\in\phi(x)$ for each $x\in D$, we have $X=\overline{\bigcup\phi(D)}$.*
(2) *TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$.*

Note that in Bella's Theorem, the hypothesis used in Theorem 9 that X is T_3 has been eliminated, a significant strengthening. Also note that condition imposed on the countable set D in (1) of Bella's Theorem is equivalent to the condition that the set D is dense. Thus, (1) of Bella's Theorem is a nice reformulation of separability, revealing the analogy with Theorem 14.

Next we explore the possibility of an analogue of Theorem 7 for the weakly Rothberger property. In a number of specific examples it has been proven that the property $\mathsf{S}_1(\mathcal{O},\mathcal{D})$ is equivalent to ONE not having a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$. This raises the question of when the property $\mathsf{S}_1(\mathcal{O},\mathcal{D})$ is equivalent to player ONE not having a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$. Here is a partial result in this direction. The Menger property, studied later in this paper, is needed in Theorem 11 below. The fact we need in the proof of Theorem 11, due to Hurewicz, is that a space has the Menger

property if and only if, ONE does not have a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$. This game is played as follows: ONE and TWO play an inning per $n<\omega$. In the n-th inning ONE first chooses an open cover O_n of the space, and then TWO responds by choosing a finite subset T_n of O_n. A play $O_0, T_0, \dots, O_m, T_n, \dots$ is won by TWO if $\bigcup_{n<\omega} T_n$ is an open cover of the space. Else, ONE wins.

Theorem 11. *Let X be a Menger space. The following are equivalent*:

(1) *X is weakly Rothberger.*
(2) *ONE has no winning strategy in $G^{\omega}_1(\mathcal{O},\mathcal{D})$.*

Proof. We must show that if a space has property $S_1(\mathcal{O},\mathcal{D})$, then ONE has no winning strategy in the game $G^{\omega}_1(\mathcal{O},\mathcal{D})$. The argument used here is due to Pawlikowski [20] for Rothberger spaces. We give some of the details for the convenience of the reader.

Since X is assumed to be a Menger space, it is a Lindelöf space. Let F be a strategy for ONE in the game $G^{\omega}_1(\mathcal{O},\mathcal{D})$. We may assume that in each inning F calls on ONE to play a countable element of $\mathcal{O}$. Define the array U_σ, $\sigma\in {}^{<\omega}\mathbb{N}$, as follows: $(U_n\colon n\in\mathbb{N})$ enumerates ONE's first move, $F(\emptyset)$. For n_1, $(U_{(n_1,n)}\colon n\in\mathbb{N})$ enumerates $F(U_{n_1})$. For n_1,n_2, $(U_{(n_1,n_2,n)}\colon n\in\mathbb{N})$ enumerates $F(U_{n_1},U_{(n_1,n_2)})$, and so on. This array has the property that for each σ the set $\{U_{\sigma^\frown n}\colon n\in\mathbb{N}\}$ is in $\mathcal{O}$.

For fixed m and $j\in\mathbb{N}$ and ρ a function from $\{1,\dots,j^m\}$ to $\mathbb{N}$, define the set

$$U_\rho(m,j)=\bigcap_{\sigma\in{}^m\{1,\dots,j\}}\left(\bigcup\{U_{\sigma^\frown\rho\restriction i}\colon i\leqslant j^m\}\right)$$

and then for fixed m and j define

$$\mathcal{U}(m,j)=\left\{U_\rho(m,j)\colon \rho \text{ a function from } \left\{1,\dots,j^m\right\} \text{ to } \mathbb{N}\right\}.$$

Then each $\mathcal{U}(m,j)\in\mathcal{O}$.

Claim. *There exist increasing sequences $\{j_n\colon n\in\mathbb{N}\}$ and $\{m_n\colon n\in\mathbb{N}\}$ such that for each $x\in X$ and for each n there is a function σ from $\{1,\dots,m_{n+1}-m_n\}$ to j_{n+1} for which $x\in U_\sigma(m_n,j_n)$.*

Proof. We observe that X is Menger and this implies that ONE does not have a winning strategy in the corresponding game $G^{\omega}_{fin}(\mathcal{O},\mathcal{O})$ using the following strategy, G.

For a first move ONE puts $j_1=m_1=1$, and plays $G(\emptyset)=\mathcal{U}(m_1,j_1)$. For a response $T_1\subseteq\mathcal{U}(m_1,j_1)$ by TWO, ONE first does the following computations: $m_2=m_1+j_1^{m_1}$, and $j_2>j_1$ is at least the maximum of all values of σ's for which $U_\sigma(m_1,j_1)$ is in T_1. Then ONE plays $G(T_1)=\mathcal{U}(m_2,j_2)$.

For a response $T_2\subseteq G(T_1)$ by TWO, ONE again first computes the numbers m_3 and j_3 according to the rules that $m_3=m_2+j_2^{m_2}$, and $j_3>j_2$ is at least the maximum of all values of σ's for which $U_\sigma(m_2,j_2)$ is in T_2, and so on.

Look at a G-play $G(\emptyset),T_1,G(T_1),T_2,G(T_1,T_2),\dots$ which is lost by ONE. Then $\bigcup_{n\in\mathbb{N}}T_n\in\mathcal{O}$, and we find increasing sequences $(j_n\colon n\in\mathbb{N})$ and $(m_n\colon n\in\mathbb{N})$ such that for each n:

(1) $m_{n+1}=m_n+j_n^{m_n}$;
(2) $G(T_1,\dots T_n)=\mathcal{U}(m_{n+1},j_{n+1})$;
(3) j_{n+1} is at least as large as the value of a σ for which $U_\sigma(m_n,j_n)$ is in T_n.

It follows that the m_n's and j_n's have the required properties, completing the proof of the claim.

With the sequences $(j_n\colon n\in\mathbb{N})$ and $(m_n\colon n\in\mathbb{N})$ fixed, define next for each n the family $\mathcal{W}_n$ as follows: For every sequence $k_1<\dots<k_n$ from $\mathbb{N}$, and for any $\sigma_1,\dots,\sigma_n$ where each σ_i is a $\{1,\dots,j_{k_i+1}\}$-valued function with domain $m_{k_i+1}-m_{k_i}$, define

$$\mathcal{W}(k_1,\dots,k_n,\sigma_1,\dots,\sigma_n)=\bigcap_{i\leqslant n}U_{\sigma_i}(m_{k_i},j_{k_i}).$$

$\mathcal{W}_n$ consists of all sets of the form $W(k_1,\dots,k_n,\sigma_1,\dots,\sigma_n)$.

Since each $\mathcal{W}_n$ is in $\mathcal{O}$, the selection hypothesis $S_1(\mathcal{O},\mathcal{D})$ applied to $(\mathcal{W}_n\colon n\in\mathbb{N})$ gives for each n a set $S_n=W(k_1^n,\dots,k_n^n,\sigma_1^n,\dots,\sigma_n^n)$ such that $\{S_n\colon n\in\mathbb{N}\}$ is in $\mathcal{D}$.

Recursively choose for each n an $\ell_n\in\{k_1^n,\dots,k_n^n\}\setminus\{\ell_i\colon i<n\}$. For each n define $\rho_n=\sigma^n_{i_n}$ where i_n is such that $\ell_n=k^n_{i_n}$.

From the definitions we see that for each n, $S_n\subseteq U_{\rho_n}(m_{\ell_n},j_{\ell_n})$.

If we now define $f:\mathbb{N}\to\mathbb{N}$ so that, for each n, $f(m_{\ell_n}+i)=\rho_n(i)$, whenever $i\leqslant m_{\ell_n+1}-m_{\ell_n}$, we find that the play

$$F(\emptyset),U_{f(1)},F(U_{f(1)}),U_{f(1),f(2)},F(U_{f(1)},U_{f(1),f(2)}),\dots$$

is won by TWO. □

To what extent is the hypothesis that a space is a Menger space needed in Theorem 11? Towards an answer to this question we show that in some models of set theory there are many non-Lindelöf (and thus non-Menger) spaces where ONE does not have a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$. Our proof for one of the main ingredients of the argument is modeled on the arguments in [28].

Theorem 12. *Let $\kappa > \aleph_0$ be a cardinal. If a topological space X is weakly Lindelöf, then in $\mathsf{V}^{\mathbb{C}(\kappa)}$ ONE has no winning strategy in $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$ on X.*

Proof. Let $\dot\sigma$ be a $\mathbb{C}(\kappa)$ name such that $\mathbf{1}_{\mathbb{C}(\kappa)} \models$ "$\dot\sigma$ is a strategy for ONE in $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$". By Theorem 3,

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot\sigma(\emptyset) \text{ has a countable subset with union dense in } \check X\text{"}.$$

Choose a $\mathbb{C}(\kappa)$ name $\dot{\mathcal{U}}_\emptyset$ such that

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_\emptyset \subseteq \dot\sigma(\emptyset) \text{ is a countable subset with union dense in } \check X\text{"}.$$

Thus choose $\mathbb{C}(\kappa)$ names $\dot U_n$, $n<\omega$ such that

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_\emptyset = \{\dot U_n\colon n<\omega\}\text{"}.$$

Then we have

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}(\forall n)\big(\dot\sigma(\dot U_n) \text{ has a countable subset with union dense in } \check X\big)\text{"}.$$

For each n we choose $\mathbb{C}(\kappa)$ names $\dot{\mathcal{U}}_n$ and $\dot U_{n,k}$, $k<\omega$ such that

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_n \subseteq \dot\sigma(\dot U_n) \text{ is a countable subset with union dense in } \check X\text{"}$$

and

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_n = \{\dot U_{n,k}\colon k<\omega\}\text{"}$$

and so on. In this way we find for each finite sequence in ω $\mathbb{C}(\kappa)$ names $\dot{\mathcal{U}}_{n_1,\dots,n_k}$ and $\dot U_{n_1,\dots,n_k}$ such that

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\{\dot U_{n_1,\dots,n_k,m}\colon m<\omega\} = \dot{\mathcal{U}}_{n_1,\dots,n_k}\text{"}$$

and

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_{n_1,\dots,n_k} \subseteq \dot\sigma(\dot U_{n_1},\dots,\dot U_{n_1,\dots,n_k})\text{"}$$

and

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{"}\dot{\mathcal{U}}_{n_1,\dots,n_k} \text{ is a countable subset with union dense in } \check X\text{"}.$$

Since $\mathbb{C}(\kappa)$ has countable chain condition and each of the names $\dot{\mathcal{U}}_\tau$ and $\dot U_\tau$ is a name for an open single set or a countable set of open sets, there is an $\alpha<\kappa$ such that each of these is a $\mathbb{C}(\alpha)$ name. Thus, factoring the forcing as $\mathbb{C}(\alpha)*\mathbb{C}([\alpha,\kappa))$ we may assume that all the named objects are in the ground model. Then, in the generic extension by $\mathbb{C}([\alpha,\kappa))$ over this ground model there is a function $f\in{}^\omega\omega$ such that f is not in any first category set definable from parameters in the ground model.

Now for each nonempty open subset V of X in the ground model the set

$$F_V = \big\{f\in{}^\omega\omega\colon (\forall k)(V\cap U_{f\restriction k}=\emptyset)\big\}$$

is first category and is definable from parameters in the ground model only. Thus, in the generic extension by $\mathbb{C}([\alpha,\kappa))$ $\bigcup_{V\in\check{\mathbf{t}}} F_V \neq {}^\omega\omega$. Choose in this generic extension an f with

$$f\in{}^\omega\omega\setminus\bigcup\{F_V\colon V \text{ a ground model open set}\}.$$

Then in the generic extension the σ-play during which TWO selected the sets $U_{f\restriction n}$, $0<n<\omega$ is won by TWO. This completes the proof that in the generic extension ONE has no winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$ on X. □

A weakly Lindelöf space need not be Lindelöf: Consider a separable space which is not Lindelöf. Since every proper forcing preserves being not Lindelöf, Theorem 12 shows that it is consistent that there are non-Menger spaces in which ONE has no winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$. It is not clear how much of the Rothberger property must be indirectly present when a space has the weak Rothberger property. Is the converse of the following true?

Theorem 13. *If X has a dense Rothberger subspace then ONE has no winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$ on X.*

Proof. Let D be a dense Rothberger subspace of X. Let F be a strategy for ONE in $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$ on X. From F define a strategy G for ONE on the space D as follows: $G(\emptyset)=\{U\cap D\colon\ U\in F(\emptyset)\}$. For $T\in G(\emptyset)$ choose $U_T\in F(\emptyset)$ with $T=D\cap U_T$. Define $G(T)=\{U\cap D\colon\ U\in F(U_T)\}$, and so on.

Now by Theorem 7 G is not a winning strategy for ONE in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{O})$. Thus let $O_1,T_1,\dots,O_n,T_n,\dots$ be a G-play of $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{O})$ which is won by TWO on D. From the definition of G we find a corresponding sequence $B_1,W_1,\dots,B_n,W_n,\dots$ where $B_1=F(\emptyset)$ and $O_1=\{D\cap U\colon\ U\in B_1\}$, $W_1\in B_1$ is such that $T_1=D\cap W_1$, and for each n we have $B_{n+1}=F(W_1,\dots,W_n)$ with $O_{n+1}=\{D\cap U\colon\ U\in B_{n+1}\}$ and $T_n=D\cap W_n$. But then we have that

$$D=\bigcup_{n\in\mathbb{N}}T_n\subseteq\bigcup_{n\in\mathbb{N}}W_n.$$

Since D is dense in X, so is $\bigcup_{n\in\mathbb{N}}W_n$. Thus TWO wins this F-play of X. □

4.2. Games and the almost Rothberger property

Theorem 14. *Let (X,τ) be a first countable topological space (but not necessarily T_3). Then the following are equivalent*:

(1) *X has countable subset D such that for each neighborhood assignment $f:D\to\tau$ with $x\in f(x)$ for each x in D, the family $\{\overline{f(x)}\colon\ x\in D\}$ covers X.*
(2) *TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$.*

Proof. (1) ⇒ (2): Let a countable set D as in (1) be given, and enumerate it as $(d_n\colon\ n<\omega)$. TWO's strategy which chooses in inning n an element T_n of ONE's move O_n so that $d_n\in T_n$ is a winning strategy.

Proof of (2) ⇒ (1): Let X be a first countable topological space in which TWO has a winning strategy σ in the game $\mathsf{G}_1(\mathcal{O},\overline{\mathcal{O}})$. Let $\prec$ be a well-order of X. Let θ be an infinite regular cardinal which is so large that X, its topology, $\mathcal{O}$, ${}^{<\omega}\mathcal{O}$, $\mathcal{D}$, $\prec$, σ, and for each $x\in X$ a neighborhood base $(U_n(x)\colon\ n\in\mathbb{N})$ of $\{x\}$, are elements of H_θ. We may assume that $\mathcal{N}=\{(U_n(x)\colon\ n\in\mathbb{N})\colon\ x\in X\}$ is a member of H_θ. Let $(\mathcal{M},\in_{\mathcal{M}})$ be a countable elementary submodel of $(\mathsf{H}_\theta,\in_\theta)$ such that each of the objects above is an element of $\mathcal{M}$.

Claim 1. *For each finite sequence $(\mathcal{U}_1,\dots,\mathcal{U}_k)$ of open covers of X there is a point $x\in X$ such that for each neighborhood U of x there is an open cover $\mathcal{U}$ such that $U=\sigma(\mathcal{U}_1,\dots,\mathcal{U}_k,\mathcal{U})$.*

This claim holds because a strategy for TWO in game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$ is also a strategy for TWO in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$. Now use the argument of Claim 1 of Theorem 9.

The sentence in Claim 1 holds in $(\mathsf{H}_\theta,\in_\theta)$ and all its parameters are in $\mathcal{M}$, so the statement holds in $(\mathcal{M},\in_{\mathcal{M}})$. Thus, choose for each finite sequence ν of open covers of X an x_ν the $\prec$-least element of X satisfying Claim 1. Note that x_ν also satisfies Claim 1 in $(\mathsf{H}_\theta,\in_\theta)$, and is in H_θ also the $\prec$-first such element. The set $E=\{x_\nu\colon\ \nu\in{}^{<\omega}\mathcal{O}\}$ is definable from $\prec$, σ, X and ${}^{<\omega}\mathcal{O}$, all parameters in $\mathcal{M}$, and thus is a member of $\mathcal{M}$.

Enumerate $\mathcal{O}\cap\mathcal{M}$ bijectively as $(O_n\colon\ n\in\mathbb{N})$. Now $D=E\cap\mathcal{M}$ is the countable set $\{x_\nu\colon\ \nu\in{}^{<\omega}\{O_0,O_1,\dots,O_n,\dots\}\}$.

Claim 2. *D has the property defined in* (1).

For suppose the contrary. Choose a neighborhood assignment $f:D\to\tau$ for which $\{\overline{f(x)}\colon\ x\in D\}$ does not cover X. Pick a point $y\in X\setminus\bigcup\{\overline{f(x)}\colon\ x\in D\}$.

Since $x_\emptyset$ is a member of $\mathcal{M}$, and $\mathcal{N}=\{(U_n(x)\colon\ n\in\mathbb{N})\colon\ x\in X\}$ is a member of $\mathcal{M}$, also $(U_n(x_\emptyset)\colon\ n\in\mathbb{N})$ (which is definable from $\mathcal{N}$ and $x_\emptyset$, both parameters in $\mathcal{M}$) is in $\mathcal{M}$. But then $\{U_n(x_\emptyset)\colon\ n\in\mathbb{N}\}$ is an element, and subset of, $\mathcal{M}$. Fix an m_1 with $U_{m_1}(x_\emptyset)\subset f(x_\emptyset)$. Since y is not in $\overline{f(x_\emptyset)}$, y is also not a member of $\overline{U}_{m_1}(x_\emptyset)$.

Then by Claim 1 $\mathcal{M}$ witnesses that there is an open cover $\mathcal{U}$ of X such that $U_{m_1}(x_\emptyset)=\sigma(\mathcal{U})$. Thus, choose n_1 so that $U_{m_1}(x_\emptyset)=\sigma(O_{n_1})$.

Next, consider $x_{\langle O_{n_1}\rangle}$. By the same considerations as above there is a neighborhood $U_{m_2}(x_{\langle O_{n_1}\rangle})$ with $y\notin\overline{U}_{m_2}(x_{\langle O_{n_1}\rangle})$, and an n_2 such that for the open cover O_{n_2} of X, $U_{m_2}(x_{\langle O_{n_1}\rangle})=\sigma(O_{n_1},O_{n_2})$.

Apply these considerations to $x_{\langle O_{n_1},O_{n_2}\rangle}$ to choose a neighborhood $U_{m_3}(x_{\langle O_{n_1},O_{n_2}\rangle})$ with y not a member of $\overline{U}_{m_3}(x_{\langle O_{n_1},O_{n_2}\rangle})$ and an open cover O_{n_3} of X so that $U_{m_3}(x_{\langle O_{n_1},O_{n_2}\rangle})=\sigma(O_{n_1},O_{n_2},O_{n_3})$, and so on. Proceeding like this we obtain a σ-play

$$O_{n_1},\sigma(O_{n_1}),O_{n_2},\sigma(O_{n_1},O_{n_2}),\dots,O_{n_k},\sigma(O_{n_1},\dots,O_{n_k}),\dots$$

for which y is not a member of $\bigcup_{k\in\mathbb{N}}\overline{\sigma(O_{n_1},\dots,O_{n_k})}$. This contradicts the fact that σ is a winning strategy of TWO in $\mathsf{G}_1(\mathcal{O},\overline{\mathcal{O}})$.

This completes the proof of (2) ⇒ (1). □

Corollary 15.[3] *If X is a first countable T_2-space such that TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$, then X is countable.*

Proof. Let $D \subseteq X$ be the countable subset as in (1) of Theorem 14. We claim that $D = X$. For suppose the contrary and choose $y \in X \setminus D$. Then as X is T_2, choose for each $d \in D$ a neighborhood $f(d)$ with y not in $\overline{f(d)}$. It follows that f is a neighborhood assignment violating the property (1) of D, a contradiction. □

In Theorem 14 some hypothesis like first countability is needed to derive that (2) implies (1): In Example F in the examples section of the paper we present an uncountable T_2 space which is not Lindelöf, not first countable, and TWO has a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$, and the space does not satisfy property (1) of Theorem 14.

In Theorem 8 of [29] it is shown that there is for each infinite cardinal number κ a T_4 Lindelöf P-space X of cardinality κ for which TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{O})$, and thus also in the games $\mathsf{G}_1^\omega(\mathcal{O},\mathcal{D})$ and $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$. By Galvin's Theorem, Theorem 6, X has some one-element subset which is not a G_δ set. Since X is in fact a topological group it follows that no one-element subset of X is a G_δ set.

Question 16. Can there be an uncountable T_2-space X such that each one-element subset of X is a G_δ set, and TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$?

Question 17. Can there be an uncountable T_1-space X which is first countable such that TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$?

Theorem 18. *Let X be a Menger space. The following are equivalent*:

(1) *X is almost Rothberger.*
(2) *ONE has no winning strategy in $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$.*

Proof. The proof of (1) implies (2) proceeds like the proof of the corresponding implication in the proof of Theorem 11. But at the stage of that proof where $\mathsf{S}_1(\mathcal{O},\mathcal{D})$ is applied to the sequence of $\mathcal{W}_n$'s, apply instead $\mathsf{S}_1(\mathcal{O},\overline{\mathcal{O}})$. □

Using the same technique as in the proof of Theorem 12 we find:

Theorem 19. *For X an almost Lindelöf space and κ an uncountable cardinal,*

$$\mathbf{1}_{\mathbb{C}(\kappa)} \models \text{“ONE has no winning strategy in the game } \mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}}) \text{ on } \check{X}\text{”}.$$

There are non-Lindelöf, almost Lindelöf spaces. Since Cohen real forcing preserves non-Lindelöf, Theorem 19 implies it is consistent that there are non-Menger spaces for which ONE has no winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O},\overline{\mathcal{O}})$.

5. The Menger property and weakenings

The following table contains names for properties considered in this section, symbolic definitions, and where available a reference for where the property was introduced:

Property name	Definition	Source
Menger	$\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$	[13]
Almost Menger	$\mathsf{S}_{fin}(\mathcal{O},\overline{\mathcal{O}})$	[18]
Weakly Menger	$\mathsf{S}_{fin}(\mathcal{O},\mathcal{D})$	[7, p. 94]

The weakly Menger property was investigated in [19]. Fig. 1 below depicts the implications among the properties have been introduced thus far:

If a space is T_3, then it is almost Menger if, and only if, it is Menger. However, $\mathsf{S}_{fin}(\mathcal{O},\overline{\mathcal{O}})$ is not equivalent to $\mathsf{S}_{fin}(\overline{\mathcal{O}},\overline{\mathcal{O}})$, even in the context of metrizable spaces:

Theorem 20. *([26, Theorem 2]) An uncountable set of real numbers has the property $\mathsf{S}_{fin}(\overline{\mathcal{O}},\overline{\mathcal{O}})$ if, and only if, it is a Lusin set.*

[3] A. Bella (personal communication) proved that first countability can be replaced by the weaker hypothesis that each point is the intersection of countably many closed sets.

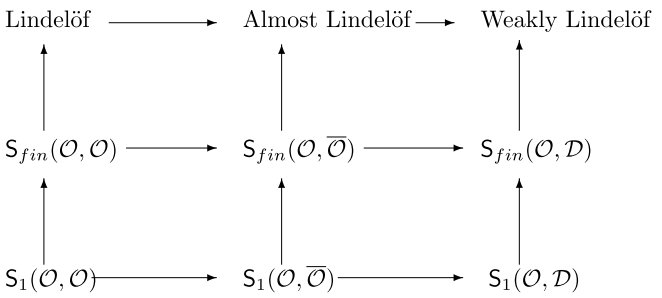

Fig. 1. Basic relationships.

5.1. Games and the Menger property

In Corollary 4 of [34] Telgársky characterized the metrizable spaces for which TWO has a winning strategy as the ones that are σ-compact. A more direct proof of Telgársky's result was given in [27]. There appears to be no satisfactory more general characterizations of topological spaces for which player TWO has a winning strategy in the games $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$, $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\overline{\mathcal{O}})$ or $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$.

It is not clear how this characterization would generalize to say T_4 spaces. It is false that for T_4-spaces TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$ if, and only if, the space is σ-compact. This can be seen by considering the examples in Section 4 of [29]: By Theorem 8 of [29] there is for each infinite cardinal number κ a T_4 Lindelöf P-group of cardinality κ such that TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{O})$ (and thus in $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$). An uncountable T_4 Lindelöf P-space cannot be a closed subset of a σ-compact space.

It is clear that if a space is σ-compact, then TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$. A weaker condition than this permits TWO a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$:

Definition 21. ([21]) X is H-*closed* if every open cover $\mathcal{U}$ of X has a finite subfamily $\mathcal{V}$ whose union is dense in X (i.e. $X\subseteq cl_X(\bigcup_{V\in\mathcal{V}} V)$).

It is well known that a T_2-space is H-closed if, and only if it is a closed subspace of each T_2-space it embeds in. Equally well-known, a T_3-space is H-closed if, and only if, it is compact.

Definition 22. X is σ-H-*closed* if it is a union of countably many subspaces, each of which is H-closed.

Proposition 23. *If X contains a dense σ-H-closed subspace then TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$.*

Proof. Let $Y\subseteq X$ be a dense σ-H-closed subspace of X. Since Y is a σ-H-closed space, write $Y=\bigcup_{n\in\mathbb{N}} Y_n$ where each Y_n is an H-closed subspace of Y. Define a strategy σ for player TWO as follows: When in inning n ONE plays an open cover O_n of X, let $\sigma(O_1,\ldots,O_n)\subseteq O_n$ be a finite set with $\bigcup\sigma(O_1,\ldots,O_n)\supseteq Y_n$. Then σ is a winning strategy for TWO. □

Question 24. (T_2) Is it true that X contains a dense σ-H-closed subspace if, and only if, TWO has a winning strategy in $G^{\omega}_{fin}(\mathcal{O},\mathcal{D})$?[4]

Question 25. (T_3) Is it true that X has a dense σ-compact subset if, and only if, TWO has a winning strategy in $G^{\omega}_{fin}(\mathcal{O},\mathcal{D})$?

Question 26. Characterize the topological spaces for which TWO has winning strategy in:

(1) The game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$.
(2) The game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\overline{\mathcal{O}})$.
(3) The game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$.

Conditions under which ONE has no winning strategy in these games are somewhat better understood. Hurewicz, who introduced and studied the Menger property in [13], proved there

[4] A. Bella (personal communication) has shown that the answer to this question is "NO".

Theorem 27 *(Hurewicz). For a space X the following are equivalent*:

(1) *X has the Menger property.*
(2) *ONE has no winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{O})$.*

For Lindelöf spaces Hurewicz's proof of Theorem 27 generalizes to also give the corresponding characterizations for weakly Menger and almost Menger spaces. For the convenience of the reader we now give the proof of the characterization of weakly Menger Lindelöf spaces, and then indicate what modification is needed to also obtain the characterization for Lindelöf almost Menger spaces.

Theorem 28. *Let X be a Lindelöf space. Then the following are equivalent*:

(1) *X is weakly Menger.*
(2) *ONE does not have a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$.*

Proof. The implication that if a Lindelöf space satisfies $S_{fin}(\mathcal{O},\mathcal{D})$ then ONE has no winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$ requires proof. The argument used here is due to Hurewicz [13] for Menger spaces, and has been used in [25] for a different context. We give some of the details of Hurewicz's argument for the convenience of the reader.

Let X be Lindelöf and let F be a strategy for ONE. Without loss of generality, we may assume that each move of ONE according to the strategy F, is an ascending ω-chain of open sets covering X.

Write $F(\emptyset) = (U(n)\colon\ n\in\mathbb{N})$, listed in $\subset$-increasing order. Then, for each n, list $F(U_{(n)})$ in $\subset$-increasing order as $(U_{(n,m)}\colon\ m\in\mathbb{N})$, and so on.

Supposing that U_τ, has been defined for each finite sequences τ of length at most k of positive integers, we now define for each $(n_1,\dots,n_k)$:

$$F(U_{(n_1)},\dots,U_{(n_1,\dots,n_k)}) = (U_{(n_1,\dots,n_k,m)}\colon\ m\in\mathbb{N}).$$

Then the family $(U_\tau\colon\ \tau$ a finite sequence of positive integers$)$ has the following properties for each τ:

(1) If m is less than n, then $U_{\tau^\frown(m)}$ is a subset of $U_{\tau^\frown(n)}$.
(2) For each n, $U_\tau\subseteq U_{\tau^\frown(n)}$.
(3) $\{U_{\tau^\frown(n)}\colon\ n$ a positive integer$\}$ is an open cover of X.

Define for each n and κ:

$$U^n_k = \begin{cases} U_{(k)}, & \text{if } n=1;\\ (\bigcap\{U_{\tau^\frown(k)}\colon\ \tau\in {}^{n-1}\mathbb{N}\})\cap U^{n-1}_k, & \text{otherwise.}\end{cases}$$

Note that for each n the set $\{U^n_k\colon\ k\in\mathbb{N}\}$, denoted $\mathcal{U}_n$, is an open cover of X. To see this, first show (by induction) that for each $(i_1,\dots,i_n)$ such that $\max\{i_l,\dots,i_n\}\geqslant k$ one has $U^n_k\subseteq U_{(i_1,\dots,i_n)}$. It then follows that each U^n_k is an intersection of finitely many open sets, and thus is itself open. Now observe that by its definition each $\mathcal{U}_n$ is an increasing chain of open sets such that each $\mathcal{U}_n$ is an open cover of X.

Apply the fact that X is weakly Menger to the sequence $(\mathcal{U}_n\colon\ n\in\mathbb{N})$. Since each $\mathcal{U}_n$ is an ascending chain this gives for each n a $U^n_{k_n}\in\mathcal{U}_n$ such that $\{U^n_{k_n}\colon\ n\in\mathbb{N}\}$ is in $\mathcal{D}$. Since, for each n, $U^n_{k_n}\subseteq U_{(k_1,\dots,k_n)}$, the sequence of moves $U_{k_1}, U_{k_1,k_2},\dots$ by TWO defeats ONE's strategy F. □

The corresponding theorem for almost Menger is:

Theorem 29. *Let X be a Lindelöf space. Then the following are equivalent*:

(1) *X is almost Menger.*
(2) *ONE does not have a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\overline{\mathcal{O}})$.*

Proof. The proof proceeds like for Theorem 28. In that proof at one point we apply the selection property $\mathsf{S}_{fin}(\mathcal{O},\mathcal{D})$ to a sequence $(\mathcal{U}_n\colon\ n<\omega)$ of special open covers of X. Applying the selection property $\mathsf{S}_{fin}(\mathcal{O},\overline{\mathcal{O}})$ instead at the same point of the proof produces a proof of Theorem 29. □

The hypothesis that X is Lindelöf in Theorem 28 or 29 is not necessary: By Theorem 12 it is consistent that there is a non-Lindelöf space X for which TWO has a winning strategy in $\mathsf{G}^{\omega}_1(\mathcal{O},\mathcal{D})$, and thus in $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$. Similar remarks apply to the almost Menger case. We do not know the answers to the following questions:

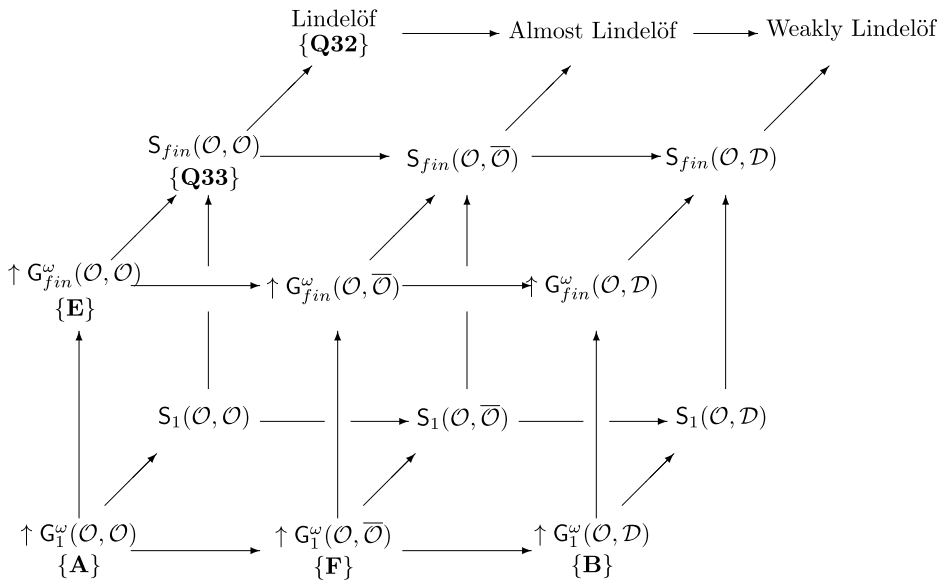

Fig. 2. Classes considered in this paper.

Question 30. Is there an almost Menger space for which ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\overline{\mathcal{O}})$?

Question 31. Is there a weakly Menger space for which ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$?

6. Examples

The relationships among the covering properties we consider in this paper are indicated in Fig. 1. Also considering the game theoretic versions, the strongest property considered in this paper is the property that TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{O})$. The following diagram, Fig. 2, is Fig. 1 updated to include the classes where TWO has a winning strategy in the corresponding game. We use the symbol $\uparrow \mathsf{G}^{\omega}_{fin}(\mathcal{A},\mathcal{B})$ to denote that TWO has a winning strategy in the corresponding game.

We now consider examples that distinguish these classes from each other. We are missing two examples, as indicated in the following two questions:

Question 32. Is there a Lindelöf space which is not weakly Menger?

Question 33. Is there a Menger space for which TWO does not have a winning strategy in $\mathsf{G}^{\omega}_{fin}(\mathcal{O},\mathcal{D})$?

These questions are associated with the corresponding vertices in Fig. 2. The rest of our examples are as follows:

A: Large compact T_2 spaces where TWO has a winning strategy in $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{O})$.
For an infinite cardinal number κ let D_κ be the one-point compactification of a discrete space of cardinality κ. Then TWO has a winning strategy in $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{O})$ on D_κ.

B: Non-almost Lindelöf spaces where TWO has a winning strategy in $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{D})$.
Note that such an example indicates that none of the implications from the middle panel to the right panel of Fig. 2 is reversible.

(a) The space $\mathbb{P}$ of irrational numbers with the topology inherited from the real line is not Menger. As $\mathbb{P}$ is T_3, it follows that this space is also not almost Menger. For any refinement of this topology on $\mathbb{P}$, these statements remain true. As $\mathbb{P}$ is separable, TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{D})$. Define the topology

$$\tau_0 := \{U \setminus C\colon\ U \text{ open in the usual topology on } \mathbb{P} \text{ and } C \subseteq \mathbb{P} \text{ is countable}\}.$$

Then $(\mathbb{P},\tau_0)$ is a T_2-space but no longer a T_3-space. It is still Lindelöf and not almost Menger, but it is no longer separable. Yet, TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{D})$ on $(\mathbb{P},\tau_0)$. This indicates that in Theorem 9 the hypothesis that the space is T_3 cannot be weakened to T_2.

(b) Examination of Examples 6 in [19] shows that also that example is non-separable, T_2 but not T_3, and the space is not almost Lindelöf, but TWO has a winning strategy in the game $\mathsf{G}^{\omega}_{1}(\mathcal{O},\mathcal{D})$.

(c) Example 11 of [19] is, on the other hand, a separable $\mathsf{T}_{3\frac{1}{2}}$-space which is not almost Lindelöf.

(d) Let $\mathbb{S}$ denote the *Sorgenfrey line*, the topological space obtained from refining the standard topology on the real line by also declaring each interval of the form $[a, b)$ open. Since the set of rational numbers still is a dense subset of $\mathbb{S}$, TWO has a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$ on $\mathbb{S}$ and all its finite powers. In Lemma 17 of [2] it was shown that $\mathbb{S}$ does not have the property $\mathsf{S}_{fin}(\mathcal{O}, \mathcal{O})$, and since $\mathbb{S}$ is T_3, this means that $\mathbb{S}$ is not almost Menger. Note that finite powers of $\mathbb{S}$ are still separable, but are not Lindelöf and as these powers remain T_3, they also are not almost Lindelöf. Thus, for finite powers of $\mathbb{S}$ TWO has a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$ while the space is not almost Lindelöf.

(e) The space $\mathbb{Z}^{\omega_1}$ is T_3 and not T_4, it is not Lindelöf and thus also not almost Lindelöf. But it is separable, and so TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$ for this space.

C: Non-Lindelöf (but almost Menger) spaces where TWO has a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$.

Such an example shows that none of the implications from the top left edge of Fig. 2 to the top middle is reversible.

Example 77 of [31], the deleted radius topology in the plane, is a non-Lindelöf space. In [17, Example 1], Kočev points out that the space in this example is almost Menger (and thus not T_3). Indeed, TWO has a winning strategy in the game $\mathsf{G}_{fin}^\omega(\mathcal{O}, \overline{\mathcal{O}})$: When ONE presents TWO with an open cover, TWO may first replace it with basic open sets consisting of the appropriate deleted radius open disks. Ignoring the deleted radii, this would be a move of ONE in the usual topology of $\mathbb{R}^2$, and TWO may, in the n-th inning, choose finitely many of these open disks (including radii) that cover the Euclidean compact set $[-n, n] \times [-n, n]$. Then remove the radii so as to recover sets from the replacement family of basic open sets of the deleted radius topology, and then select finitely many elements of ONE's presented cover that contain the corresponding finitely many basis elements. This example illustrates that in the proof of Theorem 29 the hypothesis that a space be Lindelöf is not required for the conclusion that TWO has a winning strategy in the almost Menger game.

This space is not almost Rothberger, as can be shown by for each positive integer n letting $\mathcal{U}_n$ be the open cover consisting of all open discs of area less than $\frac{1}{2^n}$ with horizontal radius (excluding the center) removed. If for each n we choose a $U_n \in \mathcal{U}_n$, then the total area covered by the sets $\overline{U}_n$, $n \in \mathbb{N}$, is finite, and so these sets do not cover the plane. But the set D of points in the plane with rational coordinates only is still dense in the deleted radius topology, so that this space is separable. It follows that TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$. Should we refine the deleted radius topology further by declaring all countable sets closed, the resulting space would no longer be separable, but TWO would still have a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$, and in the game $\mathsf{G}_{fin}^\omega(\mathcal{O}, \overline{\mathcal{O}})$.

D: Non-Lindelöf almost Rothberger spaces.

Such an example eliminates one more implication from the middle panel to the left panel of Fig. 2.

Consider subspaces of the space in Example 77 of [31], the Euclidean plane with the deleted radius topology. It is a non-Lindelöf space. Now assume X is an uncountable subset of $\mathbb{R}$ such that $X \times X$ has the Rothberger property. Let $\mathsf{R}(X)$ denote the set $X \times X$ with the deleted radius topology inherited. Then one can show that $\mathsf{R}(X)$ still is not Lindelöf, but it is almost Rothberger.

E: Compact T_2 spaces which are not weakly Rothberger.

This example shows that there are no implications from the top level to the bottom level of Fig. 2.

Let $\mathbf{I}$ be the closed unit interval. Let X be a dense subset of $\mathbf{I}$. Consider the following subspace $T(X)$ of the *Alexandroff double of* $\mathbf{I}$. $T(X) = \mathbf{I} \times \{0\} \cup X \times \{l\}$. For $A \subset \mathbf{I}$ and for $x \in \mathbf{I}$ we write A_i for $A \times \{i\}$ and x_i for (x, i), $i \in \{0, 1\}$. The family $\mathcal{B} = \{U_0 \cup ((U \cap X)_1 \backslash \{x_1\})\colon\ U \text{ open in } \mathbf{I} \text{ and } x \in U \cap X\} \cup \{\{x_1\}\colon\ x \in X\}$ is a basis for a topology on $T(X)$. In this topology $T(X)$ is compact and T_2. In particular, TWO has a winning strategy in the game $\mathsf{G}_{fin}^\omega(\mathcal{O}, \mathcal{O})$.

The weakly Rothberger property for $T(X)$ is connected with the classical strong measure zero sets of real numbers. A subset X of the real line $\mathbb{R}$ has *strong measure zero* if there is for every sequence $(\varepsilon_n\colon\ n \in \mathbb{N})$ of positive real numbers a sequence $(J_n\colon\ n \in \mathbb{N})$ of nonempty open intervals such that each J_n has length at most ε_n, and $X \subseteq \bigcup_{n\in\mathbb{N}} J_n$. This concept was introduced in [5] where Borel observed that every countable set of real numbers has this property. Borel conjectured that every strong measure zero set is countable. The truth of tis conjecture is independent of ZFC. In [24] it is shown that for X a dense subset of $\mathbf{I}$, the following are equivalent:

(1) X has strong measure zero.
(2) $T(X)$ satisfies the selection hypothesis $S_1(\mathcal{O}, \mathcal{D})$.
(3) ONE has no winning strategy $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$ played on the space $T(X)$.

One can also show that TWO has a winning strategy in $\mathsf{G}_1^\omega(\mathcal{O}, \mathcal{D})$ if, and only if, X is countable. Thus, by choosing $X \subseteq \mathbb{R}$ appropriately we obtain a compact T_2 space which is not weakly Rothberger.

F: Non-Lindelöf T_2 space for which TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{O}, \overline{\mathcal{O}})$.

This example demonstrates that none of the implications from the left panel of Fig. 2 to its middle panel is reversible.

The following is Example 3.3 of [32]. The space X is a subset of $\mathbb{R} \times \mathbb{R}$ with a special topology: First, choose a subset $\{x_\alpha\colon\ \alpha < \omega_1\}$ of $\aleph_1$ distinct elements of the set of nonnegative real numbers.

$$X = \big\{(x_\alpha, m)\colon\ m \text{ an integer larger than } -2 \text{ and } \alpha < \omega_1\big\} \cup \big\{(-1, -1)\big\}.$$

For convenience we also define:

$$A = \big\{(x_\alpha, -1)\colon\ \alpha < \omega_1\big\}$$

and

$$Y = \big\{(x_\alpha, n)\colon\ 0 \leqslant n \in \mathbb{N} \text{ and } \alpha < \omega_1\big\}.$$

Topologize X as follows: Declare each element of Y to be an isolated point; for each $\alpha < \omega_1$ and $n < \omega$ the neighborhood $U_{n,\alpha}$ of $(x_\alpha, -1)$ is the set $\{(x_\alpha, -1)\} \cup \{(x_\alpha, m)\colon\ m \geqslant n\}$. Finally, for each α the neighborhood V_α of $(-1, 1)$ is the set $\{(-1, -1)\} \cup \{(x_\beta, n)\colon\ \beta > \alpha,\ -1 < n < \omega\}$.

Since the uncountable subset A of X is a closed and discrete subset of X, X is not Lindelöf. Also, for a fixed α, for neighborhood V_α of $(-1, -1)$ we see that $\overline{V}_\alpha$ contains all but countably many elements of X. Thus, TWO wins $\mathsf{G}_1^\omega(\mathcal{O}, \overline{\mathcal{O}})$ as follows: In the first inning TWO chooses the set T_1 from the open cover O_1 provided by ONE so that T_1 contains a neighborhood of $(-1, -1)$ of the form V_α. Then in the remaining innings TWO makes sure to cover the at most countably many points in the set $X \setminus \overline{T}_1$.

Moreover, the point $(-1, 1)$ does not have a countable neighborhood base, and so this space is not first countable. We now show that this example does not meet condition (1) of Theorem 14: Let D be a countable subset of X. We may assume that $(-1, -1)$ is an element of D. Fix a $\beta < \omega_1$ such that $D \cap \{(x_\alpha, n)\colon\ -1 \leqslant n < \omega,\ \beta < \alpha < \omega_1\} = \emptyset$. Then any neighborhood assignment which uses only neighborhoods from the family

$$\{V_{\beta+\omega}\} \cup \big\{\big\{(x_\alpha, n)\big\}\colon\ -1 < n \text{ and } \alpha < \beta + \omega\big\} \cup \{U_{0,\alpha}\colon\ \alpha < \beta + \omega\}$$

witnesses the failure of condition (1) of Theorem 14.

Acknowledgements

The research for the results reported in this paper occurred while Dr. Pansera was visiting the Department of Mathematics at Boise State University. The Department's hospitality and support during this visit is gratefully acknowledged.

After we submitted this paper A. Bella communicated several very interesting improvements to some results in this paper. Some of these have been noted in appropriate places in the paper. Additionally, Bella has also found direct arguments for some of our proofs that use the elementary submodel technique. Bella's results are available in [4]. We thank Professor Bella for very stimulating correspondence about the topic of this paper.

References

[1] L. Aurichi, D-spaces, topological games and selection principles, Topology Proc. 36 (2010) 107–122.
[2] L. Babinkostova, M. Scheepers, Combinatorics of open covers (IX): Basis properties, Note Mat. 22 (2) (2003/2004) 167–178.
[3] L. Babinkostova, B.A. Pansera, M. Scheepers, Weak covering properties and selection principles, in preparation.
[4] A. Bella, Infinite games and cardinality, preprint.
[5] E. Borel, Sur la classification des ensembles de mesure nulle, Bull. Soc. Math. France 47 (1919) 97–125.
[6] W.W. Comfort, N. Hindman, S. Negrepontis, F-spaces and their products with P-spaces, Pacific J. Math. 28 (1969) 489–502.
[7] P. Daniels, Pixley-Roy spaces over subsets of the reals, Topology Appl. 29 (1988) 93–106.
[8] A. Dow, F.D. Tall, W.A.R. Weiss, New proofs of the consistency of the normal Moore space conjecture I, Topology Appl. 37 (1990) 33–51.
[9] R. Engelking, General Topology, 2nd edition, Sigma Ser. Pure Math., vol. 6, Heldermann, Berlin, 1989.
[10] Z. Frolik, Generalizations of compact and Lindelöf spaces, Czechoslovak Math. J. 9 (84) (1959) 172–217 (in Russian).
[11] F. Galvin, Indeterminacy of the point-open game, Bull. Pol. Acad. Sci. Math. 26 (1978) 445–449.
[12] I. Gorelic, The Baire category theorem, and forcing large Lindelöf spaces with points G_δ, Proc. Amer. Math. Soc. 118 (1993) 603–607.
[13] W. Hurewicz, Über eine Verallgemeinerung des Borelschen Theorems, Math. Z. 24 (1925) 401–421.
[14] T.J. Jech, Multiple Forcing, Cambridge Tracts in Math., vol. 88, 1987.
[15] W. Just, A.W. Miller, M. Scheepers, P.J. Szeptycki, The combinatorics of open covers (II), Topology Appl. 73 (1996) 241–266.
[16] M. Kada, Preserving the Lindelöf property under forcing extensions, Topology Proc. 38 (2011) 237–251.
[17] D. Kocev, Almost Menger and related spaces, Mat. Vesn. 61 (2009) 173–180.
[18] Lj.D.R. Kočinac, Star-Menger and related spaces II, Filomat 13 (1999) 129–140.
[19] B.A. Pansera, Weaker forms of the Menger property, Quaest. Math. 35 (2) (2012) 161–169.
[20] J. Pawlikowski, Undetermined sets of point-open games, Fund. Math. 144 (1994) 279–285.
[21] J.R. Porter, R.G. Woods, Extensions and Absolutes of Hausdorff Spaces, Springer-Verlag, 1988.
[22] F. Rothberger, Eine Verschärfung der Eigenschalft C, Fund. Math. 3 (1938) 50–55.
[23] M. Scheepers, Combinatorics of open covers I: Ramsey theory, Topology Appl. 69 (1996) 31–62.
[24] M. Scheepers, Combinatorics of open covers (IV): Subspaces of the Alexandroff double unit interval, Topology Appl. 83 (1998) 63–75.
[25] M. Scheepers, Combinatorics of open covers (V): Pixley-Roy spaces of sets of reals, and ω-covers, Topology Appl. 102 (2000) 13–31.
[26] M. Scheepers, Lusin sets, Proc. Amer. Math. Soc. 197 (1999) 251–257.
[27] M. Scheepers, A direct proof of a theorem of Telgársky, Proc. Amer. Math. Soc. 123 (11) (1995) 3483–3485.
[28] M. Scheepers, Remarks about countable tightness, arXiv:1201.4909.
[29] M. Scheepers, Rothberger bounded groups and Ramsey theory, Topology Appl. 158 (2011) 1575–1583.
[30] M. Scheepers, F.D. Tall, Lindelöf indestructibility, topological games and selection principles, Fund. Math. 210 (2010) 1–46.
[31] L.A. Steen, J.A. Seebach, Counterexamples in Topology, Dover Publications, New York, 1995.
[32] P. Stoyanova, A comparison of Lindelöf type covering properties of topological spaces, Rose-Hulman Und. Math. J. 12 (2) (2011) 163–204.
[33] F.D. Tall, On the cardinality of Lindelöf spaces with points G_δ, Topology Appl. 63 (1995) 21–38.
[34] R. Telgársky, On games of Topsoe, Math. Scand. 54 (1984) 170–176.
[35] V.V. Tkachuk, Some new versions of an old game, Comment. Math. Univ. Carolin. 36 (1) (1995) 177–196.
[36] S. Willard, U.N.B. Dissanayake, The almost Lindelöf degree, Canad. Math. Bull. 27 (4) (1984) 452–455.

Topology and its Applications 160 (2013) 2251–2271

Contents lists available at ScienceDirect

Topology and its Applications

www.elsevier.com/locate/topol

Weak covering properties and selection principles

L. Babinkostova [a], B.A. Pansera [b], M. Scheepers [a,*]

[a] *Department of Mathematics, Boise State University, Boise, ID 83725, USA*
[b] *Dipartimento di Matematica, Universita di Messina, via F. Stagno d'Alcontres N. 31, 8166, Messina, Italy*

ARTICLE INFO

MSC:
54B10
54D20
54G10
54G12
54G20

Keywords:
Productively Menger
Weakly Menger
Productively Hurewicz
Weakly Hurewicz
Productively Rothberger
Weakly Rothberger

ABSTRACT

No convenient internal characterization of spaces that are productively Lindelöf is known. Perhaps the best general result known is Alster's internal characterization, under the Continuum Hypothesis, of productively Lindelöf spaces which have a basis of cardinality at most $\aleph_1$. It turns out that topological spaces having Alster's property are also productively weakly Lindelöf. The weakly Lindelöf spaces form a much larger class of spaces than the Lindelöf spaces. In many instances spaces having Alster's property satisfy a seemingly stronger version of Alster's property and consequently are productively X, where X is a covering property stronger than the Lindelöf property. This paper examines the question: When is it the case that a space that is productively X is also productively Y, where X and Y are covering properties related to the Lindelöf property.

1. Introduction

A topological space is said to be Lindelöf if each of its open covers contains a countable subset that covers the space. Though this class of spaces has been extensively studied there are still several easy to state problems that have not been resolved. Call a space X *productively Lindelöf* if $X \times Y$ is a Lindelöf space whenever Y is a Lindelöf space.

In the quest to find an internal characterization of the productively Lindelöf spaces K. Alster identified the following conditions: Call a family $\mathcal{F}$ of G_δ subsets of a space X a G_δ *compact* cover if there is for each compact subset K of X a set $F \in \mathcal{F}$ such that $K \subseteq F$. A space is said to be an *Alster space* if each G_δ-compact cover of the space has a countable subset covering the space.[1] Alster (and independently Barr et al. [6]) proved that if X is an Alster space then it is productively Lindelöf, and $X^{\aleph_0}$ is Lindelöf.

* Corresponding author.
E-mail address: mscheepe@boisestate.edu (M. Scheepers).

[1] This definition is not identical to the definition in [6], but is equivalent to it, and is in fact the property (*) defined by Alster on p. 133 of [1].

0166-8641/$ – see front matter
http://dx.doi.org/10.1016/j.topol.2013.07.022

Problem 1 *(K. Alster).* Is every productively Lindelöf space an Alster space?

A significant body of partial results has developed around this problem, yet no definitive answer is known to it.

There are several weakenings of the Lindelöf property that have been investigated because of their natural occurrence in some mathematical contexts. The corresponding product theory for these is not as extensively developed as for Lindelöf spaces. Product theoretic questions may be more manageable for the corresponding weakened analogues of the selective versions of the Lindelöf property.

In another direction, a number of selective versions of the Lindelöf property and weakenings of it have been investigated because of their relevance to several other mathematical problems. It has been found that some questions about Lindelöf spaces are "easier" for these more restricted classes. It is natural to inquire whether the corresponding product theoretic problem for these narrower classes of spaces is more manageable. Some such questions have been raised: For example: In [30] and [31] the notion of a *productively Menger* space is considered and in [2] the notion of a *productively FC-Lindelöf space* is introduced.

And thirdly, solving versions of a problem still unresolved for Lindelöf spaces by strengthening the hypotheses to selective versions while weakening the conclusions to weak covering properties, may yield some insights on the original problem. Progress on the internal characterization problem may also yield insights on an older problem of E. Michael [19]:

Problem 2 *(E.A. Michael).* If X is a productively Lindelöf space, then is $X^{\aleph_0}$ a Lindelöf space?

These are the motivations for our paper. The paper is organized as follows. In Section 2 we introduce some basic notation and terminology. In Section 3 we give a number of examples of when products fail to have some of the properties we are investigating. Section 4 focuses on the question of characterizing the productively Lindelöf spaces. We raise the question of when P and Q are covering properties of topological spaces, is a space that is productively P also productively Q? In Section 5 we incorporate the weak covering properties into the investigation.

2. Some notations and terminology

A space is said to be *weakly Lindelöf* if each of its open covers contains a countable subset for which the union is dense in the space. A space is said to be *almost Lindelöf* if each of its open covers contains a countable subset for which the set of closures of elements of the countable set is a cover of the space. Both of these properties are weaker than the Lindelöf property, and we have the following implications: Lindelöf $\Rightarrow$ almost Lindelöf $\Rightarrow$ weakly Lindelöf. For spaces with the T_3 separation property almost Lindelöf also implies Lindelöf. Aside from this there are no other implications among these three properties. We will focus on the "weakly" properties in this paper, leaving the "almost" properties for another time.

Next we describe selective versions of these covering properties. We use the following notation for three of several upcoming relevant classes of families of open sets of a given topological space:

$\mathcal{O}$ The collection of open covers
$\mathcal{D}$ $\{\mathcal{U}\colon (\forall U \in \mathcal{U})\ (U \text{ open}) \text{ and } (\bigcup \mathcal{U} \text{ dense in } X)\}$

Let $\mathcal{A}$ and $\mathcal{B}$ be collections of subsets of an infinite set. Then $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ denotes the following hypothesis:

For each sequence $(A_n\colon n \in \mathbb{N})$ of elements of $\mathcal{A}$ there is a sequence $(B_n\colon n \in \mathbb{N})$ such that, for each n, $B_n \in A_n$ and $\{B_n\colon n \in \mathbb{N}\}$ is an element of $\mathcal{B}$.

Thus, $\mathsf{S}_1(\mathcal{O},\mathcal{O})$ denotes the classical *Rothberger* property [22]. We shall call spaces with the property $\mathsf{S}_1(\mathcal{O},\mathcal{D})$ *weakly Rothberger*.

The symbol $\mathsf{S}_{fin}(\mathcal{A},\mathcal{B})$ denotes the hypothesis:

For each sequence $(A_n\colon\ n\in\mathbb{N})$ of elements of $\mathcal{A}$ there is a sequence $(B_n\colon\ n\in\mathbb{N})$ such that, for each n, $B_n\subseteq A_n$ is finite, and $\bigcup\{B_n\colon\ n\in\mathbb{N}\}$ is an element of $\mathcal{B}$.

$\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$ denotes the classical *Menger* property, while $\mathsf{S}_{fin}(\mathcal{O},\mathcal{D})$ denotes the *weakly Menger* property.

Several additional families $\mathcal{A}$ and $\mathcal{B}$ of topologically significant objects will be introduced as needed during the rest of the paper. Our conventions for the rest of the paper are: By "space" we mean a topological space. Unless other separation axioms are indicated specifically, we assume all spaces to be infinite and T_1. Undefined notation and terminology will be as in [10].

3. Possibilities of failure for products

Towards investigating the product theory as outlined above, we consider if it is possible for certain products to fail having a covering property. We asked above, for example, if there could be a Rothberger space whose product with the space of irrational numbers is not weakly Lindelöf. First, we settle that it is at least possible that the product of two Rothberger spaces can fail to be a weakly Lindelöf space. We give two examples of how this could be. Both are consistency results.

Theorem 1. *It is consistent, relative to the consistency of* ZFC*, that there are Rothberger spaces X and Y for which $X\times Y$ is not weakly Lindelöf.*

Proof. In [13] Hajnal and Juhasz give examples X and Y of Lindelöf spaces for which $X\times Y$ is not weakly Lindelöf.[2] These examples are constructed in ZFC. Now consider these two ground model examples in the generic extension obtained by adding $\kappa>\aleph_0$ Cohen reals. Since X and Y are Lindelöf in the ground model, Theorem 11 of [27] implies that X and Y are Rothberger in the generic extension. Since $X\times Y$ is not weakly Lindelöf in the ground model, Theorem 1 of [3] implies that $X\times Y$ is not weakly Lindelöf in the generic extension. □

Our second example is a little stronger than the one just given. A *Souslin line* is a complete dense linearly ordered space X which is not separable but every family of disjoint intervals is countable. SH, the *Souslin Hypothesis*, states that there are no Souslin lines. SH is independent of ZFC. Theorem 1 is proven using forcing. One may ask to what degree axiomatic circumstances determine whether a product fails to have the covering property of its factor spaces. Shelah [28] proved that in the generic extension obtained by adding a Cohen real there is a Souslin line. Thus, the following Theorem 2 improves Theorem 1. In the proof of this theorem we use the following notation. If $(L,<)$ is a linearly ordered set there are three topologies considered on it: We denote the topological space by L if the topology is generated by sets of the form (a,b) where $a<b$ are elements of L. When the topology is generated instead by sets of the form $[a,b)$, the topological space is denoted by the symbol L^+. When the topology is generated by sets of the form $(a,b]$, then the topological space is denoted by the symbol L^-.

Theorem 2 *(¬SH). There are Rothberger spaces X and Y such that $X\times Y$ is not weakly Lindelöf.*

[2] A nice exposition of this example can be found in [29], Example 3.25.

Proof. Let L be a Souslin line. We may assume that L has no nonempty open intervals that are separable. Then L^+ as well as L^- are Lindelöf spaces ([29], Lemma 3.31). But L^+ is a refinement of the standard topology on L, and so L is Lindelöf.

Claim 1. *L^+ (and similarly L^-) is a Rothberger space.*[3]

Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of L^+. By Lemma 3.31 in [29] we may assume that each $\mathcal{U}_n$ consists of countably many open intervals of form $[a_k^n, b_k^n)$, $k \in \mathbb{N}$.

Consider $(\mathcal{U}_{2\cdot n}\colon\ n \in \mathbb{N})$. The set $A := \overline{\{a_k^{2\cdot n}\colon\ k \in \mathbb{N}\} \bigcup \{b_k^{2\cdot n}\colon\ k \in \mathbb{N}\}}$ is countable (lest L has a separable uncountable interval) nowhere dense in L. Choose for each $x \in L \setminus A$ an open interval $I_x \subseteq L \setminus A$ with $x \in I_x$. Note that for each n there is a k with $I_x \subseteq (a_k^{2\cdot n}, b_k^{2\cdot n})$ (since $I_x \cap A = \emptyset$).

Choose from each $\mathcal{U}_{2\cdot n+1}$ an element $J_{2\cdot n+1}$ such that $A \subseteq \bigcup_{n\in\mathbb{N}} J_{2\cdot n+1}$. Now $K := L \setminus (\bigcup_{n\in\mathbb{N}} J_{2\cdot n+1})$ is a closed subset of L and so Lindelöf. Moreover $\{I_x\colon\ x \in K\}$ is an open cover of K, and so has a countable subcover, say $\{I_{x_n}\colon\ n \in \mathbb{N}\}$. Now choose for each n a k_n such that $I_{x_n} \subseteq J_{2\cdot n} = [a_{k_n}^{2\cdot n}, b_{k_n}^{2\cdot n}) \in \mathcal{U}_{2\cdot n}$. Then the sequence $(J_n\colon\ n \in \mathbb{N})$ is a cover of L^+, and for each n, $J_n \in \mathcal{U}_n$. This completes the proof of the claim. As L is not separable, [29], Lemma 3.33 shows that $L^+ \times L^-$ is not weakly Lindelöf. □

Our third example is in a different direction: Spaces that are weakly Rothberger in finite powers need not have a weakly Menger product. Since the topological sum of two Rothberger spaces is Rothberger, and their product is a closed subspace of the square of their topological sum, the negation of Souslin's Hypothesis implies that there is a Rothberger space whose square is not weakly Lindelöf. But if two Rothberger spaces are weakly Rothberger in their finite powers, must their product be weakly Rothberger?

Theorem 3 *(CH). There are weakly Rothberger spaces X and Y such that*

(1) *Each (finite or infinite) power of X and of Y is weakly Rothberger, and*
(2) *$X \times Y$ is not weakly Menger.*

Proof. The proof of Theorem 3 is developed through a few propositions. Recall that for topological space $(X, \mathcal{T})$, $\mathsf{PR}(X)$ denotes the collection of nonempty finite subsets of X. For $S \in \mathsf{PR}(X)$ and an open set $V \subseteq X$, $[S, V]$ denotes $\{T \in \mathsf{PR}(X)\colon\ S \subseteq T \subseteq V\}$. The collection of subsets of the form $[S, V]$ of $\mathsf{PR}(X)$ is a basis for a topology, denoted $\mathsf{PR}(\mathcal{T})$, on $\mathsf{PR}(X)$. Then $(\mathsf{PR}(X), \mathsf{PR}(\mathcal{T}))$ is the Pixley–Roy space of X. If X has a countable base, then $\mathsf{PR}(X)$ is a union of countably many sets, each with the finite intersection property; this implies that $\mathsf{PR}(X)$ has countable cellularity. But countable cellularity is equivalent to: each element of $\mathcal{D}$ has a countable subset which is in $\mathcal{D}$.

For topological spaces X and Y, the space $X \oplus Y$ denotes the topological sum of X and Y.

Proposition 4. *Let X and Y be spaces. Then $\mathsf{PR}(X) \times \mathsf{PR}(Y)$ is homeomorphic to $\mathsf{PR}(X \oplus Y)$.*

Proof. The function $\Phi\colon \mathsf{PR}(X) \times \mathsf{PR}(Y) \to \mathsf{PR}(X \oplus Y)$ defined by $\Phi((F, G)) = F \cup G$ is one-to-one and onto, continuous and open, and thus a homeomorphism. □

At this point it is convenient to introduce another family of open covers: A family $\mathcal{F}$ of subsets of an infinite set S is said to be an *ω-cover*[4] of S if S is not a member of $\mathcal{F}$, yet for each finite subset F of S there is a member U of $\mathcal{F}$ such that $F \subseteq U$. Let X be a topological space.

[3] Towards proving this we refine the argument from p. 19 of [24].
[4] Note that we are deviating from standard usage of the term ω-cover: We do not require that the cover be an open cover of a space.

$$\Omega := \{\mathcal{U} \in \mathcal{O}\colon \mathcal{U} \text{ is an } \omega\text{-cover of } X\}.$$

Proposition 5. *([25])* (CH) *There are separable metric spaces X and Y each with the property $\mathsf{S}_1(\Omega,\Omega)$, but their topological sum $Z = X \oplus Y$ does not have $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$.*

Proof. In [25] CH is used to construct subsets X and Y of ${}^{\omega}\mathbb{Z}$ such that each has the property $\mathsf{S}_1(\Omega,\Omega)$, but $(X \cup Y) \oplus (X \cup Y) = {}^{\omega}\mathbb{Z}$.

As was noted in Theorem 3.9 of [16], a topological space has the Menger property in all finite powers if, and only if, it has the property $\mathsf{S}_{fin}(\Omega,\Omega)$. Since $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$ is preserved by continuous images, closed subsets, and countable unions, since $\mathsf{S}_{fin}(\Omega,\Omega)$ is equivalent to $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$ in all finite powers, and since $\mathsf{S}_{fin}(\Omega,\Omega)$ is preserved by closed subsets, finite powers, and continuous images, and since ${}^{\omega}\mathbb{Z}$ (which is homeomorphic to the set of irrational numbers) does not have $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$, it follows that $(X \cup Y)^2$ does not have $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$. Thus neither $X \cup Y$ nor $X \times Y$ has $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$. It follows that $X \oplus Y$ does not have the Menger property. □

Theorem 6. *(Daniels, [9], Theorem 5B) If Z is a metrizable space with the property $\mathsf{S}_1(\Omega,\Omega)$, then $\mathsf{PR}(Z)$ is weakly Rothberger in each (finite or infinite) power.*

Thus Theorem 6 implies that each of $\mathsf{PR}(X)$ and $\mathsf{PR}(Y)$ is weakly Rothberger in all powers. Next apply the following theorem to $X \oplus Y$:

Theorem 7. *(Daniels, [9], Theorem 2A) If for a space Z, $\mathsf{PR}(Z)$ is weakly Menger, then each finite power of Z is Menger.*

Thus Theorem 7 states that if $\mathsf{PR}(X)$ has property $\mathsf{S}_{fin}(\mathcal{O},\mathcal{D})$, then X has property $\mathsf{S}_{fin}(\Omega,\Omega)$: For metrizable spaces the converse is implied by Theorem 6.

It follows that $\mathsf{PR}(X \oplus Y)$ is not weakly Menger. But then Proposition 4 implies that $\mathsf{PR}(X) \times \mathsf{PR}(Y)$ is not weakly Menger. This completes the proof of Theorem 3. □

As far as ZFC results are concerned, there is also the following result by Todorčević. First we introduce another family of open covers: A family $\mathcal{F}$ of subsets of an infinite set S is said to be a *γ-cover* of S if for each $x \in S$ the set $\{F \in \mathcal{F}\colon x \notin F\}$ is finite and $\mathcal{F}$ is infinite. Then for a topological space X we define

$$\Gamma := \{\mathcal{U} \in \mathcal{O}\colon \mathcal{U} \text{ is an } \gamma\text{-cover of } X\}.$$

Following Gerlits and Nagy, call a space which satisfies $\mathsf{S}_1(\Omega,\Gamma)$ is a *γ-space* [11].

Theorem 8. *(Todorčević, [32], Theorem 8) There are T_3 γ-spaces X and Y such that $X \times Y$ is not Lindelöf.*

And finally for this section:

Theorem 9. *It is consistent, relative to the consistency of* ZFC*, that there is a T_3-Rothberger space whose square is not Lindelöf.*

Proof. Let $\mathbb{S}$ denote the *Sorgenfrey line*, the topological space obtained from refining the standard topology on the real line by also declaring each interval of the form $[a,b)$ open. It is well known that $\mathbb{S}$ is a T_3 Lindelöf space while $\mathbb{S} \times \mathbb{S}$ is not Lindelöf, but still T_3. By Theorem 11 of [27], if κ is an uncountable cardinal and if $\mathbb{C}(\kappa)$ denotes the Cohen forcing notion for adding κ Cohen reals, then in the generic extension the ground model Sorgenfrey line is a Rothberger space. But proper forcing preserves not being Lindelöf, and $\mathbb{S}$ in the

generic extension by $\mathbb{C}(\kappa)$, the square of the ground model copy of $\mathbb{S}$ is not Lindelöf. Since T_3 is preserved, it follows that the square of a (almost) Rothberger space need not be (almost) Lindelöf. □

As an aside to the proof of Theorem 9: In Lemma 17 of [4] it was shown that $\mathbb{S}$ does not have the property $\mathsf{S}_{fin}(\mathcal{O},\mathcal{O})$, and since $\mathbb{S}$ is T_3, this means that $\mathbb{S}$ is not almost Menger. As noted in the proof of Theorem 9, in the generic extension by uncountably many Cohen reals, the ground model version of $\mathbb{S}$ is Rothberger and thus Menger. Thus, proper forcing does not preserve being not Menger.

Also note that the ground model Sorgenfrey line remains a separable space in the generic extension, and thus a weakly Rothberger space in a strong sense: TWO has a winning strategy in the game $\mathsf{G}_1^{\omega}(\mathcal{O},\mathcal{D})$.

4. Productively Lindelöf spaces

For a topological property Q that is inherited by closed sets we shall say that a space X is *productively* Q if for any space Y which has property Q, also $X\times Y$ has property Q. Note that if a space X is productively Q, then each finite power of X is also productively Q.

Much work has been done on characterizing the members of the class of productively Lindelöf spaces. We expand the basic problem of characterizing the class of productively Lindelöf spaces to also characterizing the classes of spaces that are productive for covering properties that are relatives of the Lindelöf property. Some basic problems emerge: Assume that we have topological properties Q and R where Q implies R. When is it the case that:

(1) If a space is productively R, then it is productively Q?
(2) If a space is productively Q, then it is productively R?
(3) If the product of X with every space of property Q has property R, then is X productively R?

Compact spaces are productively Lindelöf but need not be Rothberger spaces, and thus need not be productively Rothberger. Thus, spaces that are productive for one class of Lindelöf spaces need not be productive for another.

Alster's theorems and a property of Alster

In [1] Alster proves the following interesting theorem:

Theorem 10 *(Alster). Consider the following statements about a space X:*

(1) *X is an Alster space.*
(2) *X is productively Lindelöf.*

Then (1) *implies* (2). *If X is a space of weight at most $\aleph_1$, and if* CH *holds, then also* (2) *implies* (1).

Alster [1], Lemma 1, also proved that the Alster spaces give an affirmative answer to Problem 2.

Theorem 11 *(Alster). If X is an Alster space, then $X^{\aleph_0}$ is a Lindelöf space.*

The following classes of covers are central to Alster's analysis of the productively Lindelöf spaces:

$\mathcal{G}_K$: The family consisting of sets $\mathcal{U}$ where X is not in $\mathcal{U}$, each element of $\mathcal{U}$ is a G_δ-set, and for each compact set $C\subset X$ there is a $U\in\mathcal{U}$ such that $C\subseteq U$.
$\mathcal{G}$: The family of all covers $\mathcal{U}$ of the space X for which each element of $\mathcal{U}$ is a G_δ-set.

In [6], Theorem 4.5 it is proved that the product of finitely many Alster spaces is again an Alster space. On account of this fact it is useful to also consider the following class of covers of spaces:

$\mathcal{G}_\Omega$: This is the set of covers $\mathcal{U} \in \mathcal{G}$ for which X is not in $\mathcal{U}$, but for each finite set $F \subset X$ there is a $U \in \mathcal{U}$ such that $F \subseteq U$.

Observe that $\mathcal{G}_K$ is a subset of $\mathcal{G}_\Omega$.

The connection of Alster's condition to selection principles will now be determined through a sequence of lemmas, culminating in Theorem 15:

Lemma 12. *For a topological space X the following are equivalent*:

(1) *X is an Alster space.*
(2) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$.*
(3) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Omega)$.*

Proof. (1) $\Rightarrow$ (2): Suppose that X is an Alster space and let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of elements of $\mathcal{G}_K$. Define

$$\mathcal{U} = \left\{ \bigcap_{n\in\mathbb{N}} U_n\colon\ (\forall n)(U_n \in \mathcal{U}_n) \right\}.$$

Then $\mathcal{U}$ is a member of $\mathcal{G}_K$. Since X is Alster, choose a countable subset $(V_n\colon\ n \in \mathbb{N})$ of $\mathcal{U}$ which is a cover of X. For each n write

$$V_n = \bigcap_{k\in\mathbb{N}} U_k^n$$

where for each k, U_k^n is an element of $\mathcal{U}_k$. Finally for each n set $W_n = U_n^n$, an element of $\mathcal{U}_n$. Then $\{W_n\colon\ n \in \mathbb{N}\}$ is a cover of X and thus a member of $\mathcal{G}$.

(2) $\Rightarrow$ (1): Let a member $\mathcal{U}$ of $\mathcal{G}_K$ be given. For each n, set $\mathcal{U}_n = \mathcal{U}$. Then apply $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ to this sequence and select for each n a $U_n \in \mathcal{U}_n$ such that $\{U_n\colon\ n \in \mathbb{N}\}$ is a cover of X.

(2) $\Rightarrow$ (3):

Claim 1. *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ if and only if X^2 satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ (hence every finite power of X satisfies $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$).*

The proof follows since the finite power of Alster space is an Alster space.

Claim 2. *Each finite power of X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ if and only if X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Omega)$.*

Proof. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of elements of $\mathcal{G}_K$. Then $(\mathcal{W}_n\colon\ n \in \mathbb{N})$, where $\mathcal{W}_n = \{(U_n)^\kappa\colon\ U \in \mathcal{U}_n\}$, is a sequence of elements of $\mathcal{G}_K$ of X^κ. Then we can select by hypothesis $(U_n)^k \in \mathcal{W}_n$ such that $\{(U_n)^k\colon\ n \in \mathbb{N}\}$ is a cover of X^k. Consider now a finite subset $F = \{x_1, \ldots, x_k\}$ of X. We consider F like a point of X^k, say $z = (x_1, \ldots, x_k)$. So there is an element $(U_n)^k$ such that $z \in (U_n)^k$. Then there is an

element $U_n \in \mathcal{U}_n$ such that $F \subset U_n$. It follows that $\{U_n\colon\ n \in \mathbb{N}\}$ witnesses that X satisfies $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Omega)$. The converse is obvious. This completes the proof. □

(3) ⇒ (2): Obvious. □

A space X is has the *Hurewicz property* [14] if for each sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of open covers of X there is a sequence $(\mathcal{V}_n\colon\ n \in \mathbb{N})$ such that for each n, $\mathcal{V}_n$ is a finite subset of $\mathcal{U}_n$ and for each $x \in X$, for all but finitely many n, x belongs to $\bigcup \mathcal{V}_n$. The Alster property implies the following strengthening of the Hurewicz property:

Lemma 13. *If X is a space that has property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$, then there is for each sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{G}_K$ a sequence $(\mathcal{V}_n\colon\ n \in \mathbb{N})$ such that for each n we have $\mathcal{V}_n \subseteq \mathcal{U}_n$, $|\mathcal{V}_n| \leqslant n$, and for each $x \in X$, for all but finitely many n, $x \in \bigcup \mathcal{V}_n$.*

Proof. Let a sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{G}_K$ be given. For each n define $\mathcal{W}_n$ to be the set $\mathcal{W} = \{\bigcap_{k\in\mathbb{N}} U_k\colon\ (\forall k)(U_k \in \mathcal{U}_k)\}$. Applying $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ to the sequence $(\mathcal{W}_n\colon\ n \in \mathbb{N})$ we find for each n a $W_n \in \mathcal{W}_n$ such that for each $x \in X$ there is an n with $x \in W_n$.

For each n write $W_n = \bigcap\{U_k^n\colon\ k \in \mathbb{N}\}$ where for each n and k we have $U_k^n \in \mathcal{U}_k$. Then, for each k, set

$$\mathcal{V}_k = \{U_k^1, \ldots, U_k^k\},$$

a finite subset of $\mathcal{U}_k$. Note that if $x \in X$ is an element of W_n, then for each $k \geqslant n$ we have $x \in \bigcup \mathcal{V}_k$. □

For each n, let T_n be the n-th triangular number.[5] Using the technique in the proof of the previous lemma, we find

Lemma 14. *If X is a space that has property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$, then there is for each sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{G}_K$ a sequence $(U_n\colon\ n \in \mathbb{N})$ such that for each n we have $U_n \in \mathcal{U}_n$, and for each $x \in X$, for all but finitely many n,*

$$x \in \bigcup_{T_n < j \leqslant T_{n+1}} U_j.$$

Proof. Let a sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{G}_K$ be given. For each n define

$$\mathcal{V}_n = \left\{ \bigcap_{T_n < i \leqslant T_{n+1}} U_i\colon\ (\forall i)(T_n < i \leqslant T_{n+1})(U_i \in \mathcal{U}_i) \right\}.$$

Now apply the conclusion of the previous lemma to the sequence $(\mathcal{V}_n\colon\ n \in \mathbb{N})$ to find for each n a set $\mathcal{W}_n \subseteq \mathcal{V}_n$ of cardinality n such that for each x, for all but finitely many n, $x \in \bigcup \mathcal{W}_n$. Each element of $\mathcal{W}_n$ is of the form $U^j_{T_n+1} \cap \cdots \cap U^j_{T_{n+1}}$ where $1 \leqslant j \leqslant n$ and each U_i^j is an element of $\mathcal{U}_i$.

Now for each m choose $V_m \in \mathcal{U}_m$ as follows: Find the largest n with $T_n < m$ and then identify j with $1 \leqslant j \leqslant n+1$ with $m = T_n + j$, and put $V_m = U^j_{T_n+j}$. □

$\mathcal{G}^{gp}$: This is the set of covers $\mathcal{U} \in \mathcal{G}$ for which there is a (disjoint) partition $\mathcal{U} = \bigcup_{n\in\mathbb{N}} \mathcal{U}_n$ such that each $\mathcal{U}_n$ is finite, and for each $x \in X$ for all but finitely many n, x is in $\bigcup \mathcal{U}_n$.

[5] $T_n = 1 + 2 + \cdots + n$.

Theorem 15. *For a topological space X the following are equivalent*:

(1) *X is an Alster space.*
(2) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$.*
(3) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Omega)$.*
(4) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}^{gp})$.*
(5) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}^{gp}_\Omega)$.*
(6) *X satisfies the selection principle $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G})$.*
(7) *X satisfies the selection principle $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G}^{gp})$.*
(8) *X satisfies the selection principle $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G}^{gp}_\Omega)$.*

Corollary 16. *If X is an Alster space then X has a Hurewicz space in all finite powers.*

Strengthening Alster's property: $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$

Of several standard ways in which to strengthen the Alster property, consider the following one. Define

$\mathcal{G}_\Gamma$: This is the set of covers $\mathcal{U} \in \mathcal{G}$ which are infinite, and each infinite subset of $\mathcal{U}$ is a cover of X.

Then $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$ is a formal strengthening of the Alster property. It is not clear if this formal strengthening is in fact a real strengthening. Several known examples of productively Lindelöf spaces are so because they have this stronger version of Alster's property. We review some of these:

A: An easy consequence of one of Alster's results gives:

Theorem 17 *(CH). Assume that X is a space of weight at most $\aleph_1$, and that each compact subset of X is a G_δ-set. If X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$, then X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$.*

Proof. It follows immediately from Alster's theorem, Theorem 10, that if X is a space of weight at most $\aleph_1$ in which each compact set is G_δ and if X is productively Lindelöf, then CH implies that X is σ-compact (as the set of compact subsets of X is a cover of X by G_δ-sets of the required kind). Thus, under CH, every productively Lindelöf space of weight at most $\aleph_1$ for which each compact subspace is a G_δ-set has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$. □

B: A topological space is said to be a P-*space* if each intersection of countably many open sets is open.

Galvin (see [11]) pointed out that any Lindelöf P-space is a γ-space. Thus, as the topology of a P-space is the G_δ topology, we find:

Lemma 18 *(Galvin). Each Lindelöf P-space has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$.*

In [17], Proposition 2.1, the authors show that the product of a Lindelöf P-space with any Lindelöf space is a Lindelöf space. This result now follows from (1) ⇒ (2) of Theorem 10, and Lemma 18. A classical theorem of Noble [21] states that the product of countably many Lindelöf P-spaces is still Lindelöf. This result now follows from Theorem 11 and Lemma 18. Additionally it is also known that:

Theorem 19. *(Misra, [20]) A Lindelöf P-space is a productively P space.*

C: A space is *scattered* if each nonempty subspace has an isolated point.

Theorem 20. *(Gewand [12], Theorem 2.2) If X is a scattered Lindelöf space, then in the G_δ topology X is a Lindelöf P-space.*

Corollary 21. *A scattered Lindelöf space satisfies $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$.*

It follows that Lindelöf scattered spaces are productively Lindelöf, and that the countable power of such a space is Lindelöf.

D: A space is σ-compact if it is the union of countably many compact subsets.

Theorem 22. *Each σ-compact space has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$.*

Proof. Let X be σ-compact and write $X = \bigcup_{n\in\mathbb{N}} K_n$ where for each n we have $K_n \subseteq K_{n+1}$ and K_n is compact. Let a sequence $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ of elements of $\mathcal{G}_K$ be given. For each n, choose $U_n \in \mathcal{U}_n$ with $K_n \subseteq U_n$. Then each U_n is a G_δ subset of X, and for each $x \in X$, for all but finitely many n, $x \in U_n$. □

This implies the well-known fact that σ-compact spaces are productively Lindelöf. Via Theorem 11 we also find that the countable power of a σ-compact space is Lindelöf.

We now explore the productive properties of spaces with this stronger version of the Alster property.

Theorem 23. *If X is a topological space with property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$, then X is*:

(1) *productively Lindelöf.*
(2) *productively Menger.*
(3) *productively Hurewicz.*

Proof. We show that X is productively Hurewicz. The proof that X is productively Menger is similar.

Let Y be a Hurewicz space, and let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. We may assume that each $\mathcal{U}_n$ is closed under finite unions. For each compact subset K of X, and for each n, find a G_δ-set $\phi_n(K) \supset K$ such that for each $y \in Y$ there is an open set $U \in \mathcal{U}_n$ with $\phi_n(K) \times \{y\} \subseteq U$.

This defines, for each n, a set $\mathcal{G}_n = \{\phi_n(K)\colon\ K \subset X \text{ compact}\} \in \mathcal{G}_K$. Applying $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$ to $(\mathcal{G}_n\colon\ n \in \mathbb{N})$, we find for each n a compact set $K_n \subset X$ such that $\{\phi_n(K_n)\colon\ n \in \mathbb{N}\}$ is a member of $\mathcal{G}_\Gamma$.

Now for each n define

$$\mathcal{H}_n = \big\{V \subset Y\colon\ V \text{ open and there is a } U \in \mathcal{U}_n \text{ with } \phi_n(K_n) \times V \subseteq U\big\}.$$

Apply the fact that Y is a Hurewicz space to the sequence $(\mathcal{H}_n\colon\ n \in \mathbb{N})$: For each n choose a finite set $\mathcal{J}_n \subseteq \mathcal{H}_n$ such that for each $y \in Y$, for all but finitely many n, $y \in \bigcup \mathcal{J}_n$.

Finally, for each n choose for each $H \in \mathcal{J}_n$ a $U_H \in \mathcal{U}_n$ with $\phi_n(K_n) \times H \subseteq U_H$, and put $\mathcal{V}_n = \{U_H\colon\ H \in \mathcal{J}_n\}$. Then we have for each n that $\mathcal{V}_n$ is a finite subset of $\mathcal{U}_n$, and for each $(x, y) \in X \times Y$, for all but finitely many n, (x, y) is a member of $\bigcup \mathcal{V}_n$. □

There are many ZFC examples of Lindelöf P-spaces. For example in [26] it is shown that for each uncountable cardinal number κ there is a $\mathsf{T}_{3\frac{1}{2}}$ Lindelöf P-group of cardinality κ on which TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\Omega, \Gamma)$. Since the topology is the G_δ topology, this means that in these examples TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\mathcal{G}_K, \mathcal{G}_\Gamma)$.

Now we need two more classes of open covers: A family $\mathcal{F}$ of subsets of an infinite set S is said to be a *large cover* of S if for each $x \in S$ the set $\{F \in \mathcal{F}\colon\ x \in F\}$ is infinite.

A family $\mathcal{F}$ is a *groupable* cover if, and only if, there is a partition $\mathcal{F} = \bigcup_{n<\infty} \mathcal{F}_n$ where the $\mathcal{F}_n$'s are finite and disjoint from each other, such that each point in the space belongs to all but finitely many of the sets $\bigcup \mathcal{F}_n$.

We associate the following symbols with classes of open covers that are large or groupable:

$$\Lambda := \{\mathcal{U} \in \mathcal{O}\colon\ \mathcal{U} \text{ is an } \textit{large}\text{-cover of } X\}.$$
$$\mathcal{O}^{gp} := \{\mathcal{U} \in \mathcal{O}\colon\ \mathcal{U} \text{ is groupable in } X\}.$$

A space X is called a *Gerlits–Nagy space* if it satisfies the selection principle $\mathsf{S}_1(\Omega, \mathcal{O}^{gp})$ [18]. Each γ-space is a Gerlits–Nagy space, and each Gerlits–Nagy space is a Rothberger space.

Theorem 24. *If X is a Rothberger space with property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$, then X is*:

(1) *productively Rothberger.*
(2) *productively Gerlits–Nagy.*

Proof. (1) Let a Rothberger space Y be given, and let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. As X is Rothberger, each of its compact subsets is Rothberger. Write $\mathbb{N} = \bigcup_{n\in\mathbb{N}} S_n$ where the S_n's are infinite and pairwise disjoint.

Fix n, and for each compact subset C of X, and for each $y \in Y$, choose a finite sequence $U_{i_1}, \ldots, U_{i_k}$ where

(1) $i_1 < \cdots < i_k$ are elements of S_n and
(2) U_{i_j} is an element of $\mathcal{U}_{i_j}$, $1 \leqslant j \leqslant k$, and
(3) $C \times \{y\} \subseteq U_{i_1} \cup \cdots \cup U_{i_k}$.

This is possible as compact subsets of X are Rothberger spaces.

Thus, for fixed n, for each compact subset C of X we find that $C \times Y$ is Rothberger, thus Lindelöf, and we can find a G_δ subset $\phi_n(C)$ of X such that $C \subseteq \phi_n(C)$, and for each $y \in Y$ there is a sequence $i_1 < \cdots < i_k$ of elements of S_n such that $\phi_n(C) \times \{y\}$ is a subset of $U_{i_1} \cup \cdots \cup U_{i_k}$ as above. But then $\mathcal{G}_n = \{\phi_n(C)\colon\ C \subset X \text{ compact}\}$ is a member of $\mathcal{G}_K$ for X.

Apply $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$ to the sequence $(\mathcal{G}_n\colon\ n \in \mathbb{N})$ and select for each n a $G_n \in \mathcal{G}_n$ such that for each $x \in X$, for all but finitely many n, $x \in G_n$.

For fixed n, choose for each $y \in Y$ an open set $U^n_y \subset Y$ such that $y \in U^n_y$ and there is a sequence $i_1 < \cdots < i_k$ of elements of S_n such that $G_n \times U^n_y$ is a subset of $U_{i_1} \cup \cdots \cup U_{i_k}$ as above. Then $\mathcal{H}_n = \{U^n_y\colon\ y \in Y\}$ is an open cover of Y.

Next apply the fact that Y is Rothberger to the sequence $(\mathcal{H}_n\colon\ n \in \mathbb{N})$, and choose for each n an $H_n \in \mathcal{H}_n$ such that for each $y \in Y$ there are infinitely many n with $y \in H_n$.

Then for each n choose $i^n_1 < \cdots < i^n_{k_n} \in S_n$ such that $G_n \times H_n \subseteq U_{i^n_1} \cup \cdots \cup U_{i^n_{k_n}}$.

It follows that there is a sequence of $U_n \in \mathcal{U}_n$ such that $\{U_n\colon\ n \in \mathbb{N}\}$ is an open cover of $X \times Y$.

The proof of (2) is similar, and left to the reader. □

It follows that Lindelöf P-spaces, Lindelöf scattered spaces, as well as σ-compact Rothberger spaces are not only productively Lindelöf, but also productively Menger, productively Hurewicz, productively Rothberger and productively Gerlits–Nagy.

Regarding the hypothesis of Theorem 24 that X should be Rothberger: Note that the hypothesis $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$ implies $\mathsf{S}_1(\mathcal{O}_K, \mathcal{O})$, which implies $\mathsf{S}_{fin}(\mathcal{O}, \mathcal{O})$. In Example 2 of [5] it was shown that CH implies the existence of a subspace X of $\mathbb{R}^{\mathbb{N}}$ which is not countable-dimensional and yet satisfies $\mathsf{S}_1(\mathcal{O}_K, \Gamma)$. Such an X cannot be

a Rothberger space, since metrizable Rothberger spaces are zero-dimensional. One may consider weakening the hypothesis that X is Rothberger to the hypothesis that each compact subset of X is Rothberger. However, this is not a weakening of the hypotheses, since:

Lemma 25. *If X is a space such that each compact subspace is Rothberger, and $\mathsf{S}_1(\mathcal{O}_K, \mathcal{O})$ holds of X then X is a Rothberger space.*

Similarly, one can show:

Lemma 26. *If X is a space such that each compact subspace is Rothberger, and $\mathsf{S}_1(\mathcal{O}_K, \mathcal{O}^{gp})$ holds of X then X is a Gerlits–Nagy space.*

We leave the proof of these lemmas to the reader. We do not know if a similar statement is true about γ-spaces:

Problem 3. Is it true that if each compact subset of X is a Rothberger space and X has the property $\mathsf{S}_1(\mathcal{O}_K, \Gamma)$, then X has the property $\mathsf{S}_1(\Omega, \Gamma)$?

What we can prove is:

Lemma 27. *If X is a space such that each compact subspace is finite, and $\mathsf{S}_1(\mathcal{O}_K, \Gamma)$ holds of X then X is an $\mathsf{S}_1(\Omega, \Gamma)$-space.*

We now record the few results we have on productively γ-spaces.

Lemma 28. *([16]) Every open ω-cover of $X \times Y$ is refined by one whose elements are of the form $U \times V$ where $U \subseteq X$ and $V \subseteq Y$ are open.*

Theorem 29. *If X is a space satisfying $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$ and if each compact subset of X is finite, then X is $\mathsf{S}_1(\Omega, \Gamma)$-productive.*

Proof. We know that X is productively Lindelöf. Let a γ-space Y be given, and let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open ω-covers of $X \times Y$.

Claim. *$X \times Y$ is Lindelöf in each finite power.*

For γ-spaces it is well known that each finite power of a γ-space is a γ-space. Similarly for P-spaces, each finite power of a P-space is a P-space. Moreover, $(X \times Y)^n$ is homeomorphic to $X^n \times Y^n$. Note that since $X \times Y$ is a Lindelöf space in each finite power, we may assume, by the proposition on p. 156 of [11], that each $\mathcal{U}_n$ is a countable set. For each n we may also assume by Lemma 28 that the elements of $\mathcal{U}_n$ are of the form $U \times V$ where U is open in X and V is open in Y. Thus, each $\mathcal{U}_n$ is of the form $\{U_k^n \times V_k^n\colon\ k \in \mathbb{N}\}$.

Fix n and fix a finite subset F of X. For each finite set $G \subset Y$ choose a $U^n_{k(F,G)} \times V^n_{k(F,G)} \in \mathcal{U}_n$ containing $F \times G$. The intersection $W^n(F) = \bigcap\{U^n_{k(F,G)}\colon\ G \subset Y \text{ finite}\}$ is a countable intersection as $\mathcal{U}_n$ is countable, and thus is an element of $\mathcal{G}_K$ for X. Likewise, $W(F) = \bigcap_{n\in\mathbb{N}} W^n(F)$ is and element of $\mathcal{G}_K$ for X, and for each finite $G \subset Y$ and each n, $W(F) \times V^n_{k(F,G)}$ contains $F \times G$.

Note that $\{W(F)\colon\ F \subset X \text{ finite}\}$ is an ω-cover of X. Since X is a Lindelöf space satisfying $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$, choose a countable set $\{F_n\colon\ n \in \mathbb{N}\}$ of finite subsets of X with $\{W(F_n)\colon\ n \in \mathbb{N}\}$ an element of $\mathcal{G}_\Gamma$.

Fix n: Then $\{W(F_n) \times V_k^n\colon\ k \in \mathbb{N} \text{ and } W(F_n) \subseteq U_k^n\}$ is an ω-cover of $W(F_n) \times Y$, and also $\mathcal{Z}_n = \{V_k^n\colon\ k \in \mathbb{N} \text{ and } W(F_n) \subseteq U_k^n\}$ is an ω-cover for Y.

Since Y is a γ-set, choose for each n a k_n such that $\{V^n_{k_n}: n \in \mathbb{N}\}$ is a γ-cover of Y. Then $\{W(F_n)\times V^n_{k_n}: n \in \mathbb{N}\}$ is a γ-cover for $X \times Y$, and so $\{U^n_{k_n} \times V^n_{k_n}: n \in \mathbb{N}\}$ is a γ-cover of $X \times Y$. □

Since in a T_2 Lindelöf P-space compact subsets are finite, it follows that T_2 Lindelöf P-spaces as well as T_2 Lindelöf scattered spaces are productively γ-spaces. As T_2-compact Rothberger spaces are scattered Lindelöf spaces, these are productively γ-spaces.

Corollary 30. *σ-compact Rothberger spaces are productively γ.*

Proof. Since X is σ-compact we write $X = \bigcup_{n\in\mathbb{N}} X_n$ where each X_n is a compact Rothberger space. Since the union of finitely many compact Rothberger spaces is a compact Rothberger space, we may assume that for each n we have $X_n \subseteq X_{n+1}$. A compact Rothberger space is a scattered Lindelöf space. Then for Y a γ-space, for each n $X_n \times Y$ is a γ-space. This gives a union of an increasing sequence of γ-spaces, and so by Jordan's theorem ([15], Corollary 14) is again a γ-space. □

By Corollary 15 of [26] there is for each infinite cardinal κ a σ -compact T_0 topological group of cardinality κ such that TWO has a winning strategy in the game $\mathsf{G}^{\omega}_1(\Omega, \Gamma)$. By Corollary 17 of [26] there is for each infinite cardinal number κ a T_0 topological group $(G, *)$ of cardinality κ which is a σ-compact Rothberger space in all finite powers.

Alster also showed:

Theorem 31. *(Alster, [1], Theorem 4) Assume* CH*. If X is of weight at most $\aleph_1$ and has property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G})$, and if each compact subset of X is at most countable, then in the G_δ topology X is Lindelöf.*

It follows that in addition to be productively Lindelöf such spaces are also productively Menger-, Hurewicz-, Rothberger-, Gerlits–Nagy- and γ.

5. Productivity of weak covering properties

Spaces that are productively weakly Lindelöf do not currently have as well developed a theory. A number of ways of generalizing the notion of an Alster space or its strengthenings as considered in the previous section suggest themselves, but we have had limited success in exploiting these to identify classes of spaces that are for example productively weakly Lindelöf spaces. In this section we report some of these results, and pose a number of questions whose answers may help identify criteria under which a space with a weak covering property is productively so.

The following two elementary properties of the notion of dense set will be used several times.

Lemma 32. *Let X be a topological space. If $Y \subset X$ is dense in X, and $D \subset Y$ is dense in Y, then D is dense in X.*

Lemma 33. *If $D \subset X$ is dense in X and $E \subset Y$ is dense in Y, then $D \times E$ is dense in $X \times Y$.*

The power of these two lemmas lie in the following:

Theorem 34. *Let X be a topological with dense subset D.*

(1) *If D is productively weakly Lindelöf, so is X.*
(2) *If D is productively weakly Menger, so is X.*
(3) *If D is productively weakly Hurewicz, so is X.*

(4) *If D is productively weakly Rothberger, so is X.*
(5) *If D is productively weakly Gerlits–Nagy, so is X.*

Proof. We show the argument for productively weakly Rothberger, leaving the rest to the reader. Thus, let Y be a weakly Rothberger space and let D be productively weakly Rothberger. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. Then the relativizations to $D \times Y$ is a sequence of open covers of $D \times Y$, since D is dense in X. Applying the fact that $D \times Y$ is weakly Rothberger we find in each $\mathcal{U}_n$ an element U_n such that $\bigcup_{n\in\mathbb{N}} U_n$ is dense in $D \times Y$, and so by Lemma 32 is dense in $X \times Y$. □

Also the following fact is useful:

Theorem 35. *Let (X, τ) be a topological and let τ' be a finer topology on X (i.e., $\tau \subset \tau'$).*

(1) *If (X, τ') is productively weakly Lindelöf, so is (X, τ).*
(2) *If (X, τ') is productively weakly Menger, so is (X, τ).*
(3) *If (X, τ') is productively weakly Hurewicz, so is (X, τ).*
(4) *If (X, τ') is productively weakly Rothberger, so is (X, τ).*
(5) *If (X, τ') is productively weakly Gerlits–Nagy, so is (X, τ).*

In what follows we find conditions under which a space is productively weakly T, where T is one of the weak covering properties we are considering.

Weakly compact spaces

The space (X, τ) is *weakly* compact if there is for each open cover of the space a finite subset with union dense in the space. Since the closure of a finite union of sets is the union of the finitely many sets individual closures, the weakly compact spaces coincide with the almost compact spaces, and in the context of T_2-spaces, coincide with the H-closed spaces.

Analogous to Tychonoff's theorem for compact spaces, one has:

Theorem 36. *(Scarborough and Stone [23], Theorem 2.4) The product of weakly compact spaces is weakly compact.*

The argument in Proposition 1.9 of [7] shows:

Theorem 37. *If X is a weakly compact space then X is productively weakly Lindelöf.*

This can be extended to the following:

Theorem 38. *Let X be a weakly compact space.*

(1) *X is productively weakly Menger.*
(2) *X is productively weakly Hurewicz.*

Since compact spaces are weakly compact, these results also imply that compact spaces are productively weakly Lindelöf, productively weakly Menger, and productively weakly Hurewicz.

Weak versions of the Alster property

Towards exploration of productiveness for the weaker versions of the covering properties we considered, we introduce the following family of subsets of a topological space:

$\mathcal{G}_D$ denotes the collection of sets $\mathcal{U}$ where each element of $\mathcal{U}$ is a G_δ-set, and $\bigcup\mathcal{U}$ is dense in the space.

A space is said to be *weakly Alster* if each member of $\mathcal{G}_K$ has a countable subset which is a member of $\mathcal{G}_D$.

Using the proof technique of Theorem 4.5 of [6] we find:

Lemma 39. *If X weakly Alster and Y is weakly Lindelöf, then $X \times Y$ is weakly Lindelöf.*

Proof. Let $\mathcal{U}$ be an open cover of $X \times Y$. We may assume that $\mathcal{U}$ is closed under finite unions. For each compact set $C \subset X$ and for each $y \in Y$ we find an open set $U(C, y) \in \mathcal{U}$ such that $C \times \{y\} \subseteq U(C, y)$. For each y we find open sets $V(C, y) \subset X$ and $W(C, y) \subset Y$ such that $C \times \{y\} \subset V(C, y) \times W(C, y) \subset U(C, y)$.

By Theorem 37 $C \times Y$ is weakly Lindelöf. Thus the cover $\{W(C, y)\colon\ y \in Y\}$ of Y contains a countable subset with union dense in Y, say $\{W(C, y_n^C)\colon\ n \in \mathbb{N}\}$. Define $V(C) = \bigcap\{V(C, y_n^C)\colon\ n \in \mathbb{N}\}$, a G_δ subset of X containing the compact set $C \subseteq X$. But then $\mathcal{V} = \{V(C)\colon\ C \subset X \text{ compact}\}$ is a member of $\mathcal{G}_K$ for X. Since X is weakly Alster we find a countable subset $\{V(C_m)\colon\ m \in \mathbb{N}\}$ of $\mathcal{V}$ with union dense in X. But then $\{W(C_m, y_n^{C_m})\colon\ m, n \in \mathbb{N}\} \subset \mathcal{U}$ is countable and its union is dense in $X \times Y$. □

Since an Alster space is a weakly Alster space, we find

Corollary 40 *(CH). Every productively Lindelöf space of weight at most $\aleph_1$ is productively weakly Lindelöf.*

Proof. By Theorem 10, productively Lindelöf spaces of weight at most $\aleph_1$ are Alster spaces, and thus weakly Alster spaces. □

We don't know if the additional hypotheses are necessary in Corollary 40:

Problem 4. Is every productively Lindelöf space productively weakly Lindelöf?

Problem 5. Is every productively weakly Lindelöf space a weakly Alster space?

An argument similar to the one in Theorem 39 shows:

Theorem 41. *If X and Y are weakly Alster, then $X \times Y$ is weakly Alster.*

Additionally, analogous to Lemma 12 and Theorem 15 we find:

Lemma 42. *For a topological space X the following are equivalent*:

(1) *X is a weakly Alster space.*
(2) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_D)$.*
(3) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Omega})$.*
(4) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D^{gp}})$.*
(5) *X satisfies the selection principle $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D^{gp}_\Omega})$.*
(6) *X satisfies the selection principle $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G}_D)$.*

(7) *X satisfies the selection principle* $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G}_{D^{gp}})$.
(8) *X satisfies the selection principle* $\mathsf{S}_{fin}(\mathcal{G}_K, \mathcal{G}_{D^{gp}_{\Omega}})$.

We also leave to the reader the proof of

Lemma 43. *If the T_2-space X has a dense subspace which is a weakly Alster space, then X is a weakly Alster space.*

A stronger version of weakly Alster: $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$

$\mathcal{G}_{D_\Gamma}$ is the family of infinite sets $\mathcal{U}$ where each member of $\mathcal{U}$ is a G_δ subset of X, and for each nonempty open subset U of X, $\{V \in \mathcal{U}\colon\ U \cap V = \emptyset\}$ is finite.

A space with the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$ has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$. Indeed:

Lemma 44. *If a space X has a dense subset which has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$, then X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$.*

Proof. Let X be a space which has a dense subspace Y which has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$. If $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ is a sequence of elements of $\mathcal{G}_K$ for X, then choose for each $n \in \mathbb{N}$ an element $U_n \in \mathcal{U}$ such that $\{U_n\colon\ n \in \mathbb{N}\}$ is an element of $\mathcal{G}_\Gamma$ for Y. Since Y is dense in X, $\{U_n\colon\ n \in \mathbb{N}\}$ is an element of $\mathcal{G}_{D_\Gamma}$ for X. □

Theorem 45. *If X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$, then it is*

(1) *productively weakly Menger.*
(2) *productively weakly Hurewicz.*

Proof. We give the argument for weakly Menger productive. Thus, let Y be a weakly Menger space, and let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. We may assume that each $\mathcal{U}_n$ is closed under finite unions.

For each n: For each compact subset C of X find for each $y \in Y$ a set $U_n(C, y) \in \mathcal{U}_n$ such that $C \times \{y\} \subseteq U_n(C, y)$. Then for each n we find open subsets $V_n(C, y) \subset X$ and $W_n(C, y) \subset Y$ such that

$$C \times \{y\} \subseteq V_n(C, y) \times W_n(C, y) \subset U_n(C, y).$$

For each C define $\mathcal{U}_n(C) = \{W_n(C, y)\colon\ y \in Y\}$, an open cover of Y.

Partition $\mathbb{N}$ into countably many infinite subsets S_m, $m \in \mathbb{N}$.

Since Y is weakly Menger we find for each m and for each $n \in S_m$ a finite set $F(C, n) \subset Y$ such that $\bigcup\{W_n(C, y)\colon\ y \in F(C, n),\ n \in S_m\}$ is dense in Y in the following sense: For each nonempty open $T \subset Y$ there are infinitely many $n \in S_m$ for which $W_n(C, y) \cap T \neq \emptyset$ for some $y \in F(C, n)$.

Then for each C define $V(C) = \bigcap_{n\in\mathbb{N}} \bigcap \{V_n(C, y)\colon\ y \in F(C, n)\}$, a G_δ subset of X that contains C. Then $\mathcal{V} = \{V(C)\colon\ C \subset X \text{ compact}\}$ is a member of $\mathcal{G}_K$ for X. Applying the fact that X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$, we find a countable set $\{V(C_m)\colon\ m \in \mathbb{N}\}$ such that for each nonempty open set $S \subset X$, for all but finitely many n, $S \cap V(C_m) \neq \emptyset$.

For each n find the m with $n \in S_m$ and define $\mathcal{V}_n = \{V_n(C_m, y) \times W_n(C_m, y)\colon\ y \in F(C_m, n)\}$. Then each $\mathcal{V}_n$ is a refinement of a finite subset of $\mathcal{U}_n$. We must show that $\bigcup_{n\in\mathbb{N}}(\bigcup \mathcal{V}_n)$ is dense in $X \times Y$. Thus, let $U \times V$ be a nonempty open subset of $X \times Y$. Choose N so large that for all $m \geqslant N$ we have $V(C_m) \cap U \neq \emptyset$. For such an m there are infinitely many $n \in S_m$ such that $W_n(C_m, y) \cap V \neq \emptyset$ for some $y \in F(C_m, n)$.

Since $V(C_m)$ is a subset of $V_n(C_m)$, it follows that for infinitely many n there are $y \in F(C_m, n)$ for which $V_n(C_m) \times W_n(C_m, y) \cap U \times V \neq \emptyset$. □

As in the case of Lindelöf productiveness, a proof of the following conjectures may depend on a characterization of the properties of being productively Menger or productively Hurewicz.

Conjecture 1. *If a space is productively Menger then it is productively weakly Menger.*

If a space is productively Hurewicz then it is productively weakly Hurewicz.

Theorem 46. *If X is a Rothberger space with the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$, then it is productively weakly Rothberger.*

Proof. Let Y be a weakly Rothberger space. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. We may assume that for each n the elements of $\mathcal{U}_n$ are of the form $U \times V$. Partition $\mathbb{N}$ into infinitely many infinite subsets S_m, $m \in \mathbb{N}$. Then partition each S_m into infinitely many infinite pairwise disjoint subsets $S_{m,k}$, $k \in \mathbb{N}$.

For each m, and for each compact subset C of X, do the following. For each k and for each $y \in Y$ choose $i_i < i_2 < \cdots < i_t$ from $S_{m,k}$ such that for each j, $y \in V_{i_j}$, and such that $C \subseteq U_{i_1} \cup \cdots \cup U_{i_t}$, where now for each j, V_{i_j} corresponds with U_{i_j}. This is possible since C, a compact subset of X is a Rothberger space. Define $V_{m,k}(y, C)$ to be the intersection of these V_{i_j}, and $U_{m,k}(y, C)$ to be the union of these U_{i_j}. Then $\mathcal{W}_{m,k}(C) = \{V_{m,k}(y, C)\colon\ y \in Y\}$ is an open cover of Y for each m and k. Applying the fact that Y is weakly Rothberger to $(\mathcal{W}_{m,k}\colon\ k \in \mathbb{N})$, choose for each k a $y_k \in Y$ such that for each open set $V \subset Y$ there are infinitely many k with $V_{m,k}(y_k, C) \cap V \neq \emptyset$. Define $V_m(C)$ to be the set $\bigcap_{k\in\mathbb{N}} U_{m,k}$.

Then for each compact set $C \subset X$ define $V(C) = \bigcap_{m\in\mathbb{N}} V_m(C)$, a G_δ subset of X which contains C. Now apply $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$ to the member $\{V(C)\colon\ C \subset X \text{ compact}\}$ of $\mathcal{G}_K$. We find a sequence $(V(C_m)\colon\ m \in \mathbb{N})$ of G_δ-sets such that for each nonempty open subset U of X, for all but finitely many n, $V(C_n) \cap U$ is nonempty. Then the sequence $(V_n(C_n)\colon\ n \in \mathbb{N})$ has the same properties.

Now consider the sets $U_{m,k}(y_k, C_m) \times V_{m,k}(y_k, C_m)$ for $k, m \in \mathbb{N}$. For each nonempty open $U \times V \subset X \times Y$ there is an N such that for all $m > N$, $V(C_m) \cap U$ is nonempty, whence $U_{m,k} \cap C_m$ is nonempty for all k. But for such an m, for infinitely many k also $V_{m,k}(y_k, C_m) \cap V$ is nonempty. Thus, for infinitely many m and k, $U_{m,k}(y_k, C_m) \times V_{m,k}(y_k, C_m)$ has nonempty intersection with $U \times V$. But now $U_{m,k}(y_k, C_m)$ is of the form $U_{i_1} \cup \cdots \cup U_{i_t}$ while $V_{m,k}(y_k, C_m)$ is of the form $V_{i_1} \cap \cdots \cap V_{i_t}$, where $i_1 < \cdots < i_t$ are from $S_{m,k}$ and $U_{i_j} \times V_{i_j}$ is an element of $\mathcal{U}_{i_j}$.

It follows that there is a sequence of $S_n \in \mathcal{U}_n$ such that for each nonempty open $U \times V \subset X \times Y$, here are infinitely many n with $S_n \cap U \times V$ nonempty. □

Corollary 47. *Every space which has a dense σ-compact subset has property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$.*

Proof. A σ-compact space has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$. □

Corollary 48. *Every separable space has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$.*

Proof. Let X be a separable space, and let D be a countable dense subset of X. Then D is a dense σ-compact subset of X. □

Corollary 49. *Every separable space is productively weakly Lindelöf, productively weakly Menger and productively weakly Hurewicz.*

Proof. Theorem 45 and Corollary 48. □

Corollary 50. *For each cardinal number κ, $\mathbb{R}^\kappa$ is productively weakly Lindelöf, productively weakly Menger, productively weakly Hurewicz and productively weakly Rothberger.*

Proof. We only consider the case when κ in infinite. By Proposition 4 of [8],

$$\left\{f \in \mathbb{R}^\kappa\colon \left|\left\{i\colon\ f(j) \neq 0\right\}\right| < \aleph_0\right\}$$

is a dense σ-compact subset of $\mathbb{R}^\kappa$. By Lemma 39, Corollary 47 and Theorem 45 $\mathbb{R}^\kappa$ has the claimed properties.

Since $\mathbb{Q}$ is σ-compact and Rothberger, Proposition 4 of [8] implies that the subset

$$S_\kappa = \left\{f \in \mathbb{Q}^\kappa\colon \left|\left\{\alpha \in \kappa\colon\ f(\alpha) = 0\right\}\right| < \aleph_0\right\}$$

of $\mathbb{Q}^\kappa$ is σ-compact. By Corollary 15 of [26], TWO has a winning strategy in the game $\mathsf{G}_1^\omega(\Omega, \Gamma)$ in S_κ, and thus S_κ is a γ-space. It is evident that S_κ is a dense subset of $\mathbb{R}^\kappa$.

But S_κ is dense in $\mathbb{R}^\kappa$ and so as S_κ is productively weakly Rothberger by Theorem 46, also $\mathbb{R}^\kappa$ is productively weakly Rothberger. □

Separable spaces are weakly Alster, and in fact have several additional properties: For example a separable space is also weakly Rothberger. Note that a compact space could be weakly Rothberger without being Rothberger: The closed unit interval is a compact separable space but is not a Rothberger space.

Corollary 51. *If X is a separable space then X is productively weakly Rothberger.*

Proof. Every countable space has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_\Gamma)$, and thus the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$. Since a countable space is Rothberger, Theorem 46 implies that any countable space is productively weakly Rothberger. Apply Theorem 34 to conclude that any separable space is productively weakly Rothberger. □

Lemma 52. *Compact Rothberger spaces are productively weakly Rothberger.*

Proof. Let X be a compact Rothberger space and let Y by weakly Rothberger. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of open covers of $X \times Y$. We may assume each $\mathcal{U}_n$ consist of sets of the form $U \times V$. Write $\mathbb{N} = \bigcup_{n\in\mathbb{N}} S_n$ where the S_n's are infinite and pairwise disjoint.

Fix n as well as $y \in Y$, and choose a finite sequence $U_{i_1}, \ldots, U_{i_k}$ where

(1) $i_1 < \cdots < i_k$ are elements of S_n;
(2) U_{i_j} is an element of $\mathcal{U}_{i_j}$, $1 \leqslant j \leqslant k$;
(3) $X = U_{i_1} \cup \cdots \cup U_{i_k}$;
(4) $y \in V_{i_1} \cap \cdots \cap V_{i_k}$ (and define $V_n(y)$ to be this latter intersection).

This defines for each n an open cover $\mathcal{H}_n = \{V_n(y)\colon\ y \in Y\}$ of Y. Now apply the fact that Y is weakly Rothberger to the sequence $(\mathcal{H}_n\colon\ n \in \mathbb{N})$ and select for each n an $H_n \in \mathcal{H}_n$ such that for each open set $V \subseteq Y$, for infinitely many n, $V \cap H_n$ is nonempty. This produces a sequence of elements $U_n \in \mathcal{U}_n$, $n \in \mathbb{N}$, such that $\bigcup\{U_n\colon\ n \in \mathbb{N}\}$ is dense in $X \times Y$. □

Problem 6. Is it true that if X has the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$ and each compact subset of X is weakly Rothberger, then X is productively weakly Rothberger?

Using techniques from the previous section we can prove:

Lemma 53. *If each compact subspace of X is a weakly Rothberger space and if X satisfies $\mathsf{S}_1(\mathcal{O}_K, \mathcal{D})$, then X it is weakly Rothberger.*

For a space X define an element $\mathcal{U}$ of $\mathcal{D}$ to be *groupable* if there is a partition $\mathcal{U} = \bigcup\{\mathcal{U}_n\colon\ n \in \mathbb{N}\}$ where each $\mathcal{U}_n$ is a finite set, and for each nonempty open $U \subseteq X$, for all but finitely many n we have $U \cap \bigcup \mathcal{U}_n$ is nonempty. Then define

$$\mathcal{D}^{gp} = \{\mathcal{U} \in \mathcal{D}\colon\ \mathcal{U} \text{ is groupable}\}.$$

A space is weakly Gerlits–Nagy space if it satisfies $\mathsf{S}_1(\Omega, \mathcal{D}^{gp})$.

Lemma 54. *Compact Gerlits–Nagy spaces are productively weakly Gerlits–Nagy.*

Proof. Let X be a compact Gerlits–Nagy space and let Y be weakly Gerlits–Nagy. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of ω-covers of $X \times Y$. We may assume each $\mathcal{U}_n$ consists of sets of the form $U \times V$. Write $\mathbb{N} = \bigcup_{n\in\mathbb{N}} S_n$ where the S_n's are infinite and pairwise disjoint.

Fix n and F, a finite subset of Y, and choose a finite sequence $U_{i_1}, \ldots, U_{i_k}$ where:

(1) $i_1 < \cdots < i_k$ are elements of S_n;
(2) U_{i_j} is an element of $\mathcal{U}_{i_j}$, $1 \leqslant j \leqslant k$;
(3) $X = U_{i_1} \cup \cdots \cup U_{i_k}$;
(4) $F \subseteq V_{i_1} \cup \cdots \cup V_{i_k} = V_n(F)$, say.

This defines for each n an ω-cover $\mathcal{H}_n = \{V_n(F)\colon\ F \text{ a finite subset of } Y\}$ of Y.

Now apply the fact that Y is weakly Gerlits–Nagy to the sequence $(\mathcal{H}_n\colon\ n \in \mathbb{N})$ and select for each n an $H_n \in \mathcal{H}_n$ and select an increasing sequence $m_1 < m_2 < \cdots < m_k < \cdots$ in $\mathbb{N}$ such that for each open set $V \subset Y$, for all but finitely many k, $V \cap \bigcup\{H_j\colon\ m_k \leqslant j < m_{k+1}\}$ is nonempty.

This produces a sequence of elements $W_n \in \mathcal{U}_n$, $n \in \mathbb{N}$, such that $\{W_n\colon\ n \in \mathbb{N}\}$ is an element of $\mathcal{D}^{gp}$ for $X \times Y$. □

Problem 7. Is each compact weakly Rothberger space a weakly Gerlits–Nagy space? (Or maybe a weakly γ-space?)

We also don't know if weakly Lindelöf P-spaces have stronger properties in terms of products. They are at least productively weakly Lindelöf as we now show:

Lemma 55. *If X is a weakly Lindelöf P-space, then it has property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_D)$.*

Proof. For each $n \in \mathbb{N}$ let a set $\mathcal{U}_n \in \mathcal{G}_K$ be given. Since X is a P-space, $\mathcal{U}_n$ is an open cover of X. For each compact subset C of X choose for each n a $U_n(C) \in \mathcal{U}_n$ with $C \subseteq U_n(C)$, and then define $V(C) = \bigcap_{n\in\mathbb{N}} U_n(C)$. Then $V(C)$ is a G_δ subset of X and $\mathcal{V} = \{V(C)\colon\ C \subset X \text{ compact}\}$ is an open cover of X as X is a P-space. Since X is weakly Lindelöf, choose a countable subset $\{V(C_n)\colon\ n \in \mathbb{N}\}$ of $\mathcal{U}$ which has the property that there is for each nonempty open $V \subset X$ an infinite number of n with $V \cap V(C_n) \neq \emptyset$. For each n, choose $U_n = U_n(C_n) \in \mathcal{U}_n$. Then $\{U_n\colon\ n \in \mathbb{N}\}$ is a member of $\mathcal{G}_D$. □

It also follows that weakly Lindelöf P-spaces are weakly Rothberger. Since the finite product of P-spaces are P-spaces, Lemma 55 and Lemma 39 imply that the product of finitely many weakly Lindelöf P-spaces is a weakly Lindelöf P-space.

Problem 8. Let X be a weakly Lindelöf P-space.

(a) Does X then have the property $\mathsf{S}_1(\mathcal{G}_K, \mathcal{G}_{D_\Gamma})$?
(b) Is X productively weakly-Rothberger?
(c) Is X weakly-Hurewicz?

For the family $\mathcal{D}$ we introduce

$$\mathcal{D}_\Gamma := \{\mathcal{U} \in \mathcal{D}\colon\ \mathcal{U} \text{ infinite and each infinite subset of } \mathcal{U} \text{ is in } \mathcal{D}\}.$$

A space is *weak γ-space* if it satisfies $\mathsf{S}_1(\Omega, \mathcal{D}_\Gamma)$. A space is *weakly Gerlits–Nagy space* if it satisfies $\mathsf{S}_1(\Omega, \mathcal{D}^{gp})$.

Lemma 56. *Compact γ-spaces are productively weakly γ-spaces.*

Proof. Let X be a compact γ-pace and let Y be a weakly γ-space. Let $(\mathcal{U}_n\colon\ n \in \mathbb{N})$ be a sequence of ω-covers of $X \times Y$. We may assume each $\mathcal{U}_n$ consists of sets of the form $U \times V$. Write $\mathbb{N} = \bigcup_{n\in\mathbb{N}} S_n$ where the S_n's are infinite and pairwise disjoint.

Fix n as well as F finite subset of Y, and choose a finite sequence $U_{i_1}, \ldots, U_{i_k}$ where

(1) $i_1 < \cdots < i_k$ are elements of S_n;
(2) U_{i_j} is an element of $\mathcal{U}_{i_j}$, $1 \leqslant j \leqslant k$;
(3) $X = U_{i_1} \cup \cdots \cup U_{i_k}$;
(4) $F \subseteq V_{i_1} \cap \cdots \cap V_{i_k} = V_n(F)$, say.

This defines for each n an ω-cover $\mathcal{H}_n = \{V_n(F)\colon\ F \text{ finite subset of } Y\}$ of Y. Now apply the fact that Y is weakly γ-space to the sequence $(\mathcal{H}_n\colon\ n \in \mathbb{N})$ and select for each n an $H_n \in \mathcal{H}_n$ such that $\{H_n\colon\ n \in \mathbb{N}\} \in \mathcal{D}_\Gamma$. This produces a sequence of elements $U_n \in \mathcal{U}_n$, $n \in \mathbb{N}$, such that $\{U_n\colon\ n \in \mathbb{N}\}$ is a member of $\mathcal{D}_\Gamma$ for $X \times Y$. □

Acknowledgement

Part of this work was done while B. Pansera was visiting the Department of Mathematics at Boise State University. The Department's hospitality and support during this visit is gratefully acknowledged. We also thank the referee for the careful reading of our paper, and the thoughtful suggestions which improved the readability of the paper.

References

[1] K. Alster, On the class of all spaces of weight not greater than ω_1 whose Cartesian product with every Lindelöf space is Lindelöf, Fundamenta Mathematicae 129 (2) (1988) 133–140.
[2] L.F. Aurichi, F.D. Tall, Lindelöf spaces which are indestructible, productive, or D, Topology and Its Applications 159 (2012) 331–340.
[3] L. Babinkostova, B.A. Pansera, M. Scheepers, Weak covering properties and infinite games, Topology and Its Applications 159 (17) (2012) 3644–3657.
[4] L. Babinkostova, M. Scheepers, Products and selection principles, Topology Proceedings 31 (2007) 431–443.
[5] L. Babinkostova, M. Scheepers, Weakly infinite dimensional subsets of $\mathbb{R}^{\mathbb{N}}$, Topology and Its Applications 157 (2010) 1302–1313.
[6] M. Barr, J.F. Kennison, R. Raphael, On productively Lindelöf spaces, Scientiae Mathematicae Japonicae 65 (3) (2007) 310–332.
[7] F. Cammaroto, G. Santoro, Some counterexamples and properties on generalizations of Lindelöf spaces, International Journal of Mathematics and Mathematical Sciences 19 (4) (1996) 737–746.

[8] H.H. Corson, Normality in subsets of product spaces, American Journal of Mathematics 81 (1959) 784–796.
[9] P. Daniels, Pixley–Roy spaces over subsets of the reals, Topology and Its Applications 29 (1988) 93–106.
[10] R. Engelking, General Topology, 2nd edition, Sigma Series in Pure Mathematics, vol. 6, Heldermann, Berlin, 1989.
[11] J. Gerlits, Zs. Nagy, Some properties of $C(X)$, I, Topology and Its Applications 14 (1982) 151–161.
[12] M.E. Gewand, The Lindelöf degree of scattered spaces and their products, Journal of the Australian Mathematical Society, Series A 37 (1984) 98–105.
[13] A. Hajnal, I. Juhasz, On the products of weakly Lindelöf spaces, Proceedings of the American Mathematical Society 48 (2) (1975) 454–456.
[14] W. Hurewicz, Über eine Verallgemeinerung des Borelschen Theorems, Mathematische Zeitschrift 24 (1925) 401–421.
[15] F. Jordan, There are no hereditary productive γ-spaces, Topology and Its Applications 155 (2008) 1786–1791.
[16] W. Just, A.W. Miller, M. Scheepers, P.J. Szeptycki, The combinatorics of open covers (II), Topology and Its Applications 73 (1996) 241–266.
[17] A. Kilicman, A.J. Fawakhreh, Product property on generalized Lindelöf spaces, preprint.
[18] Lj.D.R. Kočinac, M. Scheepers, Combinatorics of open covers (VII): Groupability, Fundamenta Mathematicae 179 (2) (2003) 131–155.
[19] E.A. Michael, Paracompactness and the Lindelöf property in finite and countable Cartesian products, Compositio Mathematica 23 (2) (1971) 199–214.
[20] A.K. Misra, A topological view of P-spaces, General Topology and Its Applications 2 (1972) 349–362.
[21] N. Noble, Products with closed projections II, Transactions of the American Mathematical Society 160 (1971) 169–183.
[22] F. Rothberger, Eine Verschärfung der Eigenschalft C, Fundamenta Mathematicae 3 (1938) 50–55.
[23] C.T. Scarborough, A.H. Stone, Products of nearly compact spaces, Transactions of the American Mathematical Society 124 (1966) 131–147.
[24] M. Scheepers, Combinatorics of open covers (V): Pixley–Roy spaces of sets of reals, and ω-covers, Topology and Its Applications 102 (2000) 13–31.
[25] M. Scheepers, The length of some diagonalization games, Archive for Mathematical Logic 38 (1999) 103–122.
[26] M. Scheepers, Rothberger bounded groups and Ramsey theory, Topology and Its Applications 158 (13) (2011) 1575–1583.
[27] M. Scheepers, F.D. Tall, Lindelöf indestructibility, topological games and selection principles, Fundamenta Mathematicae 210 (2010) 1–46.
[28] S. Shelah, Can you take Solovay's inaccessible away?, Israel Journal of Mathematics 48 (1984) 1–47.
[29] P. Staynova, A comparison of Lindelöf type covering properties of topological spaces, Rose–Hulman Undergraduate Mathematics Journal 12 (2) (2011) 163–204.
[30] F.D. Tall, A note on productively Lindelöf spaces, manuscript dated March 24, 2010.
[31] F.D. Tall, B. Tsaban, On productively Lindelöf spaces, Topology and Its Applications 158 (2011) 1239–1248.
[32] S. Todorčević, Aronszajn ordering, Publications de L'Institut Mathématique 57 (1) (1995) 29–46.

Research Article

Liljana Babinkostova, Kevin W. Bombardier, Matthew C. Cole, Thomas A. Morrell and Cory B. Scott

Algebraic properties of generalized Rijndael-like ciphers

Abstract: We provide conditions under which the set of Rijndael-like functions considered as permutations of the state space and based on operations of the finite field $\mathrm{GF}(p^k)$ ($p \geq 2$) is not closed under functional composition. These conditions justify using a sequential multiple encryption to strengthen the Advanced Encryption Standard (AES), a Rijndael cipher with specific block sizes. In [39], R. Sparr and R. Wernsdorf provided conditions under which the group generated by the Rijndael-like round functions based on operations of the finite field $\mathrm{GF}(2^k)$ is equal to the alternating group on the state space. In this paper we provide conditions under which the group generated by the Rijndael-like round functions based on operations of the finite field $\mathrm{GF}(p^k)$ ($p \geq 2$) is equal to the symmetric group or the alternating group on the state space.

Keywords: Rijndael cipher, finite fields, symmetric groups, group operation, imprimitivity

MSC 2010: 20B05, 20B30, 94A60, 11T71, 14G50

Liljana Babinkostova: Department of Mathematics, Boise State University, Boise, ID 83725, USA, e-mail: liljanababinkostova@boisestate.edu
Kevin W. Bombardier: Department of Mathematics, Statistics, and Physics, Wichita State University, Wichita, KS 67260, USA, e-mail: kwbombardier@wichita.edu
Matthew C. Cole: Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556, USA, e-mail: mcole5@nd.edu
Thomas A. Morrell: Department of Mathematics, Washington University, St. Louis, MO 63130, USA, e-mail: tmorrell@wustl.edu
Cory B. Scott: Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO 80903, USA, e-mail: cory.scott@coloradocollege.edu

1 Introduction

An $\mathcal{SP}$-network is an iterated block cipher. This means that a certain sequence of computations, constituting a *round*, is repeated a specified number of times. The computations in each round are defined as a composition of specific functions (substitutions and permutations) in a way that achieves Shannon's principle [38] of confusion and diffusion. The *Rijndael* block cipher ([16, 17]) is an example of an $\mathcal{SP}$-network. Rijndael is a block cipher with both a variable block length and a variable key length. The versions for the block size of 128 bits and key length of 128, 192, and 256 bits were adopted by the NIST as the *Advanced Encryption Standard* (AES) [33]. Rijndael has a highly algebraic structure. The cipher round transformations are based on operations of the finite field $\mathrm{GF}(2^8)$. While little research has been done about the structural and algebraic properties of Rijndael before it was adopted as a standard, there has been much research since. Several alternative representations of the AES have been proposed (see, e.g., [2, 14, 27]) and some group theoretic properties of the AES components have been discovered (see, e.g., [12, 32, 39, 41]).

A motivation for investigating the group theoretic structure of a block cipher is to identify and exclude undesirable properties. One such undesirable property is short cycles of the round functions when considered as permutations of the state space. Another undesirable property is nontrivial factor groups of the group generated by the round functions of the cipher. For example, in [36] it was shown that if the group generated by the round functions of a block cipher is imprimitive, then this might lead to the design of trapdoors. Some related results about the cycle structure of the AES round functions are given in [27] and [41].

Knowing the order of the group generated by the round functions is also an important algebraic question about the security of the cipher, because of its connection to the Markov cipher approach to differential cryptanalysis. In [24] it was shown that if the one-round functions of an s-round iterated cipher generate

the alternating or the symmetric group, then for all corresponding Markov ciphers the chains of differences are *irreducible* and *aperiodic*. This means that after sufficiently many rounds of the cipher all differences become equally probable which makes the cipher secure against a differential cryptanalysis attack. In [41], R. Wernsdorf showed that the round functions of Rijndael over $GF(2^8)$ generate the alternating group. In [39], R. Sparr and R. Wernsdorf provided conditions under which the group generated by the Rijndael-like round functions which are based on operations on the finite field $GF(2^k)$ is equal to the alternating group on the state space. Motivated by their work we embark on a formal study of the Rijndael-like functions to determine the extent to which this and other results in [41] hold when we consider an arbitrary finite field. In this paper we provide conditions under which the group generated by the Rijndael-like round functions which are based on operations on the finite field $GF(p^k)$ ($p \geq 2$) is equal to the symmetric group or the alternating group on the state space.

Since the adoption of AES as a standard many papers have been published on the cryptanalysis on this cryptosystem. Initially AES survived several cryptanalytic efforts. The situation started to change in 2009 when [5, 6] presented a key recovery attack on the full versions of AES-256 and AES-192. Since then there have been several other theoretical attacks on these versions of AES and AES-128 (see, e.g., [7]) as well as on reduced-round instances of these versions of AES (see, e.g., [19]). In [4] the authors presented a key recovery attack on version of AES-256 with up to ten rounds that is of practical complexity. However, we must note that all these attacks are of high computational complexity and they do not threaten the practical use of AES in any way.

Theoretical attacks against widely used crypto algorithms often get better over time. The crucial question is how far AES is from becoming practically insecure. One way of strengthening AES is through using sequential multiple encryption, as it has been done with DES (see [9, 26, 34]). If the set of Rijndael round functions is closed under functional composition, then multiple encryption would be equivalent to a single encryption, and so strengthening AES through multiple encryption would not be possible. Thus, it is important to know whether this set is closed under functional composition. Also, it is important to know how changing the underlying finite field in AES will impact this property. In this paper we provide conditions under which the set of Rijndael-like functions considered as permutations of the state space and based on operations of the finite field $GF(p^k)$ ($p \geq 2$) is not closed under functional composition.

The idea of examining block ciphers using different binary operations in their underlying structure has already been considered. For example, E. Biham and A. Shamir [3] examined the security of DES against their differential attack when some of the exclusive-or operations in DES are replaced with addition modulo 2^n. In [35] the authors initiated a study of Luby–Rackoff ciphers when the bitwise exclusive-or operation in the underlying Feistel network is replaced by a binary operation in an arbitrary finite group. They showed that in certain cases these ciphers are completely secure against adaptive chosen plaintext and ciphertext attacks and has better time and space complexity if considered over $GF(p)$ for $p > 2$. Although the study of the $\mathcal{SP}$-network based ciphers over $GF(2^r)$ has already been considered (see, e.g., [41]), we are not aware of such study when the underlying operations are the field operations in $GF(p^r)$ for $p > 2$.

The paper is organized as follows. In Section 2 we give some background from the theory of permutation groups and finite fields as well as block ciphers. In Section 3 we introduce the generalized Rijndael-like $\mathcal{SP}$ network and provide conditions for the parity and the cycle structure of the round functions of such a network when considered as permutations on the state space. Furthermore, we show when the set of round functions in the generalized Rijndael-like $\mathcal{SP}$ network of s-rounds do not constitute a group under functional composition. In Section 4 we derive conditions for Rijndael-like round functions such that the group generated by these functions is equal to the alternating group or the symmetric group on the state space. In Section 5 we conclude the paper.

2 Preliminaries

2.1 Iterated block ciphers

A *cryptosystem* is an ordered 4-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$ where $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$ are called the *message (state) space*, the *ciphertext space*, and the *key space* respectively, and where $T : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is a transformation such that for each $k \in \mathcal{K}$, the mapping $\epsilon_k : \mathcal{M} \to \mathcal{C}$, called an *encryption transformation*, is invertible. For any cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$, let $\mathcal{T}_\Pi = \{\epsilon_k : k \in \mathcal{K}\}$ be the set of all encryption transformations. In addition, for any transformation $\epsilon_k \in \mathcal{T}_\Pi$, let ${\epsilon_k}^{-1}$ denote the inverse of ϵ_k. In a cryptosystem where $\mathcal{M} = \mathcal{C}$ the mapping ϵ_k is a permutation of $\mathcal{M}$. We consider only cryptosystems for which $\mathcal{M} = \mathcal{C}$. The set of all permutations of the set $\mathcal{M}$ is denoted by $\mathcal{S}_\mathcal{M}$. Under the operation of functional composition $\mathcal{S}_\mathcal{M}$ forms a group called *the symmetric group* over $\mathcal{M}$. The symbol $\mathcal{G} = \langle \mathcal{T}_\Pi \rangle$ denotes the subgroup of $\mathcal{S}_\mathcal{M}$ that is generated by the set $\mathcal{T}_\Pi$. The group $\mathcal{G}$ is known as the *group generated by a cipher*. If $\mathcal{T}_\Pi = \mathcal{G}$, that is, the set of permutations $\mathcal{T}_\Pi$ forms a group, then we say the cipher is a group. As $\mathcal{G}$ is finite, by [21, Theorem 3.3] the cipher is a group if and only if its set of encryption transformations $\mathcal{T}_\Pi$ is closed under functional composition. For such a cipher, multiple encryption does not offer better security than single encryption. Computing the group $\mathcal{G}$ generated by a cipher is often difficult. Let $T[k]$ denote the round function of the cipher under the key $k \in \mathcal{K}$ where $\mathcal{K}$ denotes the set of all round keys. Let $\tau = \{T[k] : k \in \mathcal{K}\}$ be the set of all round functions. The round functions $T[k]$ are also permutations of the message space $\mathcal{M}$ and it is often easier to compute the group $\mathcal{G}_\tau = \langle \{T[k] : k \in \mathcal{K}\} \rangle$ generated by these permutations. Suppose we have an s-round cipher with a key schedule $\mathrm{KS} : \mathcal{K} \to \mathcal{K}^s$ so that any key $k \in \mathcal{K}$ produces a set of subkeys $k_i \in \mathcal{K}$, $1 \le i \le s$. It is natural then to consider the following three groups relevant to the block cipher:

$$\begin{aligned}
\mathcal{G}_\tau &= \langle T[k] : k \in \mathcal{K} \rangle, \\
\mathcal{G}_\tau^s &= \langle T[k_s]T[k_{s-1}] \cdots T[k_1] : k_i \in \mathcal{K} \rangle, \\
\mathcal{G} &= \langle T[k_s]T[k_{s-1}] \cdots T[k_1] : \mathrm{KS}(k) = (k_1, k_2, \ldots, k_s) \rangle.
\end{aligned}$$

Thus $\mathcal{G}_\tau$ is the group generated by the round functions and $\mathcal{G}_\tau^s$ is the group generated by the set of all compositions of s (independently chosen) round functions. The group $\mathcal{G}$ is the group generated by the set of all compositions of s round functions using the key schedule KS. This group can also be regarded as the group $\langle \mathcal{T}_\Pi \rangle$ generated by the cipher $\mathcal{T}_\Pi$. It is obvious that $\mathcal{G}$ is a subgroup of $\mathcal{G}_\tau^s$ which is a subgroup of $\mathcal{G}_\tau$. We will show that $\mathcal{G}_\tau^s$ is in fact a normal subgroup of $\mathcal{G}_\tau$.

Lemma 2.1. *For every $s \in \mathbb{N}$, $\mathcal{G}_\tau^s$ is a normal subgroup of $\mathcal{G}_\tau$.*

Proof. Let $T_k \in \mathcal{G}_\tau$ and $T_s \circ \cdots \circ T_1 \in \mathcal{G}_\tau^s$. We see that

$$\begin{aligned}
T_k \circ (T_s \circ \cdots \circ T_1) \circ T_k^{-1} &= T_k \circ (T_s \circ \cdots \circ T_1) \circ (\underbrace{T_k \circ T_k \circ \cdots \circ T_k}_{s-1 \text{ copies}}) \circ (\underbrace{T_k^{-1} \circ T_k^{-1} \circ \cdots \circ T_k^{-1}}_{s-1 \text{ copies}}) \circ T_k^{-1} \\
&= (T_k \circ T_s \circ \cdots \circ T_2) \circ (T_1 \circ \underbrace{T_k \circ T_k \circ \cdots \circ T_k}_{s-1 \text{ copies}}) \circ (\underbrace{T_k \circ T_k \circ \cdots \circ T_k}_{s \text{ copies}})^{-1}.
\end{aligned}$$

It follows that

$$T_k \circ (T_s \circ \cdots \circ T_1) \circ T_k^{-1} \in \mathcal{G}_\tau^s.$$

This completes the proof. □

Thus the group $\mathcal{G}_\tau$ generated by the round functions is an upper bound for the group generated by the cipher.

2.2 Group theoretical background

In this subsection we present some background from the theory of permutation groups and finite fields which are used in this paper.

2.2.1 Permutation groups

For a finite set X, let $|X|$ denote the number of elements of X. For any nonempty finite set X with $|X| = n$, the set of all bijective mappings of X to itself is denoted by $\mathcal{S}_n$ and is called the *symmetric group* on X. A permutation $g \in \mathcal{S}_n$ is a *transposition* if g interchanges two elements $x, y \in X$ and fixes all the other elements of $X \setminus \{x, y\}$. A permutation $g \in \mathcal{S}_n$ is called an *odd* (*even*) permutation if g can be represented as a composition of an odd (even) number of transpositions.[1]

The set of all even permutations is a group under functional composition and is called the *alternating group* on X. The symbol $\mathcal{A}_n$ denotes the alternating group on a set X with $|X| = n$. The *degree* of a permutation group G over a finite set X is the number of elements in X that are moved by at least one permutation $g \in G$.

Theorem 2.2. *For $n \geq 5$, the alternating group $\mathcal{A}_n$ is a simple group.*

For any subgroup $G \leq \mathcal{S}_n$, for any $x \in X$, the set $\mathrm{orb}_G(x) = \{\phi(x) : \phi \in G\}$ is called the *orbit* of x under G. The set $\mathrm{stab}_G(x) = \{\phi \in G : \phi(x) = x\}$ is called the *stabilizer* of x in G. We will make use of the following well-known theorem, often called the Orbit-Stabilizer Theorem.

Theorem 2.3. *Let G be a finite group of permutations of a set X. Then for any $x \in X$,*

$$|G| = |\mathrm{orb}_G(x)| \cdot |\mathrm{stab}_G(x)|.$$

Let l and n denote natural numbers such that $0 < l \leq n$. A group $G \leq \mathcal{S}_n$ is called *l-transitive* if for any pair $(a_1, a_2, \ldots, a_l)$ and $(b_1, b_2, \ldots, b_l)$ with $a_i \neq a_j$, $b_i \neq b_j$ for $i \neq j$, there is a permutation $g \in G$ with $g(a_i) = b_i$ for all $i \in \{1, 2, \ldots, l\}$. A 1-transitive permutation group is called *transitive*.

A subset $B \subseteq X$ is called a *block* of G if for each $g \in G$ either $g(B) = B$ or $g(B) \cap B = \emptyset$. A block B is said to be *trivial* if $B \in \{\emptyset, X\}$ or $B = \{x\}$ where $x \in X$. The group $G \leq \mathcal{S}_n$ is called *imprimitive* if there is a nontrivial block $B \subseteq X$ of G; otherwise G is called *primitive*.

We use the following result from [42] which provides sufficient conditions for a permutation group to be the alternating or the symmetric group.

Lemma 2.4. *Suppose G is a primitive permutation group of degree n on a finite set X of cardinality n. If G contains a cycle of length m with $2 \leq m \leq (n-m)!$, then G is the alternating or the symmetric group on X.*

The following lemma from [15] gives the probability that a random permutation contains a cycle of length m with $2 \leq m \leq (n-m)!$.

Lemma 2.5. *Let A be a subset of the positive integers. The probability that a random permutation does not contain cycles of length in A is*

$$\prod_{i \in A} e^{-1/i} = e^{-\sum_{i \in A} 1/i}.$$

2.2.2 Finite fields

A structure $(\mathbb{F}, +, \cdot)$ is called a *field* if and only if the following hold:

- $(\mathbb{F}, +)$ is an Abelian group with identity element 0_G,
- $(\mathbb{F} \setminus \{0_G\}, \cdot)$ is an Abelian group,
- the law of distributivity of $\cdot$ over $+$ applies.

If the number of elements in $\mathbb{F}$ is finite, then $\mathbb{F}$ is called a *finite field*; otherwise it is called an *infinite field*.

Definition 2.6. Suppose $\mathbb{F}$ and $\mathbb{K}$ are fields. If $\mathbb{F} \subseteq \mathbb{K}$, then $\mathbb{F}$ is called a *subfield* of $\mathbb{K}$, or equivalently $\mathbb{K}$ is called an *extension field* of $\mathbb{F}$.

1 Note that in this terminology a cycle of even length is an odd permutation, while a cycle of odd length is an even permutation.

We can view $\mathbb{K}$ as a vector space over $\mathbb{F}$ if we define the scalar multiplication as follows:

$$\mathbb{F} \times \mathbb{K} \to \mathbb{K}, \quad (a, \alpha) \mapsto a\alpha.$$

Suppose the extension field $\mathbb{K}$ of $\mathbb{F}$ is a finite-dimensional vector space over $\mathbb{F}$. Let $d = \dim_{\mathbb{F}}(\mathbb{K})$ be the dimension of the vector space $\mathbb{K}$ over the field $\mathbb{F}$, and let $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be a basis of the vector space $\mathbb{K}$ over $\mathbb{F}$. Then any element $\beta \in \mathbb{K}$ can be expressed uniquely as a linear combination of $\alpha_1, \alpha_2, \ldots, \alpha_d$ with coefficients in $\mathbb{F}$, that is, $\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_d\alpha_d$ where $a_1, a_2, \ldots, a_d \in \mathbb{F}$.

In field theory the dimension d of the vector space $\mathbb{K}$ over $\mathbb{F}$ is called the *degree* of extension.

It is known that every finite field has order p^n for some prime number p and some positive integer n. Such a field is called a *Galois field* of order p^n and is denoted by $\mathrm{GF}(p^n)$. The following classical fact from the theory of finite fields (see [21]) will be used.

Theorem 2.7. *We have* $\mathrm{GF}(p^{n_1}) \subseteq \mathrm{GF}(p^{n_2})$ *if and only if* n_1 *divides* n_2.

It is also known that a finite field $\mathbb{K}$ of order p^{nd} can be constructed as a quotient ring $\mathbb{F}[x]/\langle f(x)\rangle$ where $\mathbb{F}[x]$ is the polynomial ring over the field $\mathbb{F}$ of order p^n and $f(x) \in \mathbb{F}[x]$ is an irreducible polynomial of degree d over $\mathbb{F}$. The field $\mathbb{K}$ is an extension field of degree d of $\mathbb{F}$, i.e., a vector space of dimension d over $\mathbb{F}$. The equivalence classes modulo $f(x)$ in $\mathbb{F}[x]/\langle f(x)\rangle$ of the polynomials $1, x, x^2, \ldots, x^{d-1}$ over $\mathbb{F}$ form a basis of $\mathbb{K}$ viewed as a vector space over the field $\mathbb{F}$. Thus, using x^i as representative for the equivalence class of x^i modulo $f(x)$ (for $0 \le i \le d-1$), the elements in $\mathbb{K}$ can be represented uniquely as $a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_2x^2 + ax + a_0$ where $a_i \in \mathbb{F}$.

Definition 2.8. A *quadratic field extension* of a field $\mathbb{K}$ is a field extension of degree 2.

In the case where a quadratic extension $\mathbb{K}$ arises as the quotient ring $\mathbb{F}[x]/\langle f(x)\rangle$ for an irreducible polynomial $f(x)$ of the form $x^2 - c$ with $c \in \mathbb{F}$, it is common to replace the equivalence class of x modulo $f(x)$ with the symbol $\sqrt{c}$ when representing the elements of $\mathbb{K}$ as linear combinations of basis elements of the vector space $\mathbb{K}$ over the field $\mathbb{F}$. In this notation, elements of $\mathbb{K}$ are written as $a_0 + a_1\sqrt{c}$ where $a_0, a_1 \in \mathbb{F}$ and $\mathbb{K}$ is usually denoted by $\mathbb{F}(\sqrt{c})$.

We consider the following function on finite fields.

Definition 2.9. Let $\mathbb{F}$ be a finite field of order q and $\mathbb{K}$ be an extension field of $\mathbb{F}$ of degree d. The *trace* function on $\mathbb{K}$ with respect to $\mathbb{F}$ is the function $\mathrm{Tr} : \mathbb{K} \to \mathbb{F}$ defined by $\mathrm{Tr}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{d-1}}$.

For any subset S of a field E write S^{-1} for the set $\{s^{-1} : 0 \neq s \in S\}$. The set S is called *inverse-closed* if $S^{-1} \subseteq S$. The inversion map in finite fields is of cryptographic interest, especially when we study the algebraic structure of the ciphers which are based on substitution-permutation networks. The following theorem is a result by S. Mattarei in [29].

Theorem 2.10. *Let* A *be a nontrivial inverse-closed additive subgroup of the finite field* $E = \mathrm{GF}(p^n)$. *Then either* A *is a subfield of* E *or else* A *is the set of elements of trace zero in some quadratic field extension contained in* E.

Lemma 2.11. *The number of elements of trace zero in a quadratic field extension* $\mathbb{K}(\sqrt{c})$ *of a subfield* $\mathbb{K} \subseteq \mathrm{GF}(p^n)$ *is equal to* $|\mathbb{K}|$.

Proof. The set of elements of trace zero in $\mathbb{K}(\sqrt{c})$ is the set $\{a_0 + a_1\sqrt{c} : a_0, a_1 \in \mathbb{K}, a_0 = 0\}$. This set has $|\mathbb{K}|$ members. □

Theorem 2.12. *Any nontrivial inverse-closed additive subgroup* H *of a finite field* $\mathrm{GF}(p^n)$ *has* p^k *elements for some* k *dividing* n.

Proof. By Theorem 2.10, there are two possibilities: H is a subfield of $\mathrm{GF}(p^n)$, in which case the result follows immediately from Theorem 2.7; or H is the set of elements of trace zero in a quadratic field extension $\mathbb{K}(\sqrt{c})$ of a subfield $\mathbb{K} \subseteq \mathrm{GF}(p^r)$. In the latter case, by Theorem 2.7 we have that $|\mathbb{K}| = p^k$ for some $k|n$, and Lemma 2.11 yields $|H| = |\mathbb{K}| = p^k$. □

3 Cycle structure of the generalized Rijndael-like round functions

In this section we show properties of the cycle structure of the round functions of a Rijndael-like $\mathcal{S}P$-network considered over the field $\mathrm{GF}(p^r)$, which we call *generalized Rijndael-like functions*. The notation of the generalized Rijndael-like functions and their component functions will be similar to the notation in [39]. One exception will be that the underlying field in the generalized Rijndael-like functions and their component functions is the finite field $\mathrm{GF}(p^r)$ of characteristic $p \geq 2$ instead of $\mathrm{GF}(2^r)$.

Let m, n, r be positive integers. The symbol $M_{m,n}(\mathrm{GF}(p^r))$ denotes the set of all $m \times n$-matrices over $\mathrm{GF}(p^r)$. The elements of $\mathrm{GF}(p^r)^{mn}$ are defined as matrices $b \in M_{m,n}(\mathrm{GF}(p^r))$ with the mapping

$$t : \mathrm{GF}(p^r)^{mn} \to M_{m,n}(\mathrm{GF}(p^r))$$

where $t(a) = b$ is defined by $b_{ij} = a_{ni+j}$ for $0 \leq i < m$, $0 \leq j < n$. First we start with the analysis of the cycle structure of the component functions in the generalized Rijndael-like function.

3.1 Analysis of the AddRoundKey-like function ($\sigma[k]$-function)

Definition 3.1. Let $\sigma[k] : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r))$ denote the mapping defined by $\sigma[k](a) = b$ if and only if $b_{ij} = a_{ij} + k_{ij}$ and $k \in M_{m,n}(\mathrm{GF}(p^r))$ for all $0 \leq i < m$, $0 \leq j < n$.

Lemma 3.2. *Let $k \in M_{m,n}(\mathrm{GF}(p^r))$ be given.*
(i) *If $p > 2$, then $\sigma[k]$ is always an even permutation.*
(ii) *If $p = 2$, then $\sigma[k]$ is an even permutation if and only if $r \cdot m \cdot n > 1$.*

Proof. If $k = \mathbf{0}$, then $\sigma[k]$ is the identity permutation. If $k \neq \mathbf{0}$, then $\sigma[k]$ is composed of p-cycles. If p is odd, then there are no cycles of even length. If $p = 2$, then $\sigma[k]$ is composed of 2^{rmn-1} many 2-cycles. □

3.2 Analysis of the SubBytes-like function (λ-function)

Definition 3.3. Let $\lambda : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r))$ denote the mapping defined as a parallel application of $m \cdot n$ bijective S-box mappings $\lambda_{ij} : \mathrm{GF}(p^r) \to \mathrm{GF}(p^r)$ and defined by $\lambda(a) = b$ if and only if $b_{ij} = \lambda_{ij}(a_{ij})$ for all $0 \leq i < m$, $0 \leq j < n$.

Each S-box mapping consists of an inversion, multiplication by a fixed $A \in \mathrm{GF}(p^r)$, and addition of a fixed element $B \in \mathrm{GF}(p^r)$, i.e., it is a mapping of the form $Ax^{-1} + B$ where $A, B \in \mathrm{GF}(p^r)$ are fixed. For convenience we define this map on all of $\mathrm{GF}(p^r)$ so that it maps 0 to B, and any nonzero x to $Ax^{-1} + B$.

Lemma 3.4. *Let $A \in \mathrm{GF}(p^r)$ be the fixed element used in the* S*-box mapping λ_{ij}. If $p = 2$, then the function λ is an odd permutation if and only if $r \geq 2$ and $m \cdot n = 1$. If $p > 2$, then the function λ is an odd permutation if and only if m and n are odd, and either of the following holds:*
(i) *$p \equiv_4 3$, r is odd, and $(p^r - 1)/|\langle A \rangle|$ is odd,*
(ii) *either $p \equiv_4 1$ or r is even, and $(p^r - 1)/|\langle A \rangle|$ is even.*

Proof. Analysis of inversion. We first consider a single S-box inversion

$$f : \mathrm{GF}(p^r) \to \mathrm{GF}(p^r), \quad x \mapsto f(x) = \begin{cases} x^{-1} & \text{if } x \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

If we enumerate the elements of $\mathrm{GF}(p^r)$ as $(0, x_1, \ldots, x_{p^r-1})$, then we can represent f in standard permutation form as

$$f = \begin{pmatrix} 0 & x_1 & x_2 & \ldots & x_i & \ldots & x_{p^r-1} \\ 0 & x_1^{-1} & x_2^{-1} & \ldots & x_i^{-1} & \ldots & x_{p^r-1}^{-1} \end{pmatrix}.$$

Writing this in disjoint cycle form, we see that f consists entirely of 1-cycles and 2-cycles. The 1-cycles correspond to the x for which $x^2 = 1$ or $x = 0$, while 2-cycles correspond to the rest of the elements x.

Assume that $p > 2$. Since $\mathrm{GF}(p^r) \setminus \{0\}$ is a cyclic group under multiplication, it has only $\phi(2) = 1$ elements of order 2, and thus counting the identity also, there are two elements x with $x = x^{-1}$. Thus, there are $p^r - 3$ other nonzero elements, and these form 2-cycles in pairs, giving a total of $\frac{1}{2}(p^r - 3)$ many 2-cycles in the disjoint cycle decomposition of the f function. If $p = 2$, then $p^r - 1$ is odd, and so the cyclic group $\mathrm{GF}(2^r) \setminus \{0\}$ (under multiplication) has no elements of order 2 (since 2 is not a divisor of $2^r - 1$), and so there is only one solution to $x = x^{-1}$ in this case, namely the identity. The remaining $2(2^{r-1} - 1)$ nonzero elements contribute $2^{r-1} - 1$ disjoint 2-cycles in the cycle decomposition of the f function.

Next we analyze the inversion function as a function over $M_{m,n}(\mathrm{GF}(p^r))$.

(a) Consider $p > 2$. When $p > 2$, a fixed position (i, j) S-box inversion defined on $M_{m,n}(\mathrm{GF}(p^r))$ still consists of 1-cycles and 2-cycles. The remaining $mn - 1$ positions in the $m \times n$-matrices in $M_{m,n}(\mathrm{GF}(p^r))$ can be filled in p^{rmn-r} ways, thus producing

$$\frac{1}{2}(p^{rmn-r})(p^r - 1)$$

2-cycles over $M_{m,n}(\mathrm{GF}(p^r))$, leading to a total of

$$\frac{1}{2}(p^{rmn-r})(p^r - 3) \tag{3.1}$$

2-cycles, which is an odd number if $p \equiv_4 1$ or r is even.

(b) Consider $p = 2$. Over $M_{m,n}(\mathrm{GF}(2^r))$, a fixed position (i, j) S-box inversion consists of inversion in one position's subfield $\mathrm{GF}(2^r)$ and the identity on all other $(mn - 1)$ subfields. Therefore, for every 2-cycle over $\mathrm{GF}(2^r)$, there are 2^{rmn-r} many 2-cycles over $\mathrm{GF}(2^{r\,m\,n})$. The total number of 2-cycles is

$$\frac{1}{2}(2^{rmn-r})(2^r - 2),$$

which is even if and only if $mn \geq 2$.

Analysis of multiplication by a fixed polynomial in $\mathrm{GF}(p^r)$. Multiplication by a fixed polynomial (field element) $A \in \mathrm{GF}(p^r)$ produces cycles of length $|\langle A\rangle|$ for multiplication with a nonzero field element, and length one for multiplication with the zero element. Over $M_{m,n}(\mathrm{GF}(p^r))$, there are

$$\frac{(p^{rmn-r})(p^r - 1)}{|\langle A\rangle|} \tag{3.2}$$

of these cycles, each of length $|\langle A\rangle|$ (see equation (3.6)).

(a) Consider $p > 2$. Then (3.2) is an odd number if and only if $(p^r - 1)/|\langle A\rangle|$ is odd, in which case the cycle length $|\langle A\rangle|$ is even. In this case the permutation obtained from multiplication by A is an odd permutation.

(b) Consider $p = 2$. We have that $|\langle A\rangle|$ is odd, so there are no even-length cycles. In this case the permutation obtained from multiplication by the polynomial $A \in \mathrm{GF}(p^r)$ is an even permutation.

Analysis of addition of a constant. If $p > 2$, the addition of a constant is always an even permutation, and if $p = 2$, then it is even if and only if $m \cdot n \cdot r > 1$ (Lemma 3.2).

From the above, we conclude that for p an odd prime the S-box mapping λ_{ij} is odd if $(p^r - 1)/|\langle A\rangle|$ is odd, or $p \equiv_4 1$ or r even, but not both. Thus, the function λ defined as parallel application of all $m \cdot n$ S-box mappings λ_{ij} is odd if and only if each S-box mapping λ_{ij} is odd and m and n are odd. For $p = 2$ the function λ is odd if and only if $r \geq 2$ and $m \cdot n = 1$. □

3.3 Analysis of the ShiftRows-like function (π-function)

Definition 3.5. Let $\pi : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r))$ denote the mapping for which there is a mapping $c : \{0, \ldots, m-1\} \to \{0, \ldots, n-1\}$ such that $\pi(a) = b$ if and only if $b_{ij} = a_{i(j-c(i)) \bmod n}$ for all $0 \leq i < m$, $0 \leq j < n$.

The function π permutes each row of the state matrix, an element of $M_{m,n}(\mathrm{GF}(p^r))$, by shifting that row by a constant offset. To analyze the parity of the whole permutation, we consider it as the composition

of m row permutations. A row permutation shifts a specific row by the corresponding offset, while leaving all other entries of the matrix fixed. Thus for a specific matrix from $M_{m,n}(\mathrm{GF}(p^r))$, such a row permutation leaves $n(m-1)$ entries fixed.

The parity of the function π can be computed from the parity of each row permutation by considering the permutation of $M_{1,n}(\mathrm{GF}(p^r))$ corresponding to the restriction of the row permutation that corresponds to the particular row in question. To analyze the parity of the function π we first identify the possible lengths of cycles in the cycle decomposition of this permutation, and then we count the number of cycles of each length. From this information and the value of the prime number p we then conclude what is the parity of the permutation π.

Analysis of the cycle lengths. We show that the possible lengths of a cycle of the permutation that leaves all entries in the $m \times n$-matrix fixed, except for the i-th row, and which shifts the i-th row's n entries by $c(i)$ units are the divisors of $n/\gcd(n, c(i))$. To determine this consider all the n-vectors whose entries are elements of $\mathrm{GF}(p^r)$. A typical such vector is of the form $(x_0, \ldots, x_{n-1})$ where the x_j are elements of $\mathrm{GF}(p^r)$. A single application of this permutation maps as follows:

$$(x_0, \ldots, x_{n-1}) \mapsto (x_{n-c(i)+0 \bmod n}, \ldots, x_{n-c(i)+n-1 \bmod n}),$$

and k iterations of this permutation maps as follows:

$$(x_0, \ldots, x_{n-1}) \mapsto (x_{k\cdot(n-c(i))+0 \bmod n}, \ldots, x_{k\cdot(n-c(i))+n-1 \bmod n}).$$

The least $k > 0$ which for any n-vector $(x_0, \ldots, x_{n-1})$ of elements of $\mathrm{GF}(p^r)$ produces

$$(x_{k\cdot(n-c(i))+0 \bmod n}, \ldots, x_{k\cdot(n-c(i))+n-1 \bmod n}) = (x_0, \ldots, x_{n-1})$$

gives the order of the cyclic group G generated by this row permutation. For this k we have $k \cdot (n - c(i)) \equiv_n 0$ meaning that $k \cdot c(i)$ is a common multiple of $c(i)$ and n. By minimality of k, this is the least common multiple of $c(i)$ and n, which is $n \cdot c(i)/\gcd(n, c(i))$ and thus $k = n/\gcd(n, c(i))$.

By the Orbit-Stabilizer Theorem we see that for any n-vector $(x_0, \ldots, x_{n-1})$ we have

$$\frac{n}{\gcd(n, c(i))} = |G| = |\mathrm{orb}_G((x_0, \ldots, x_{n-1}))| \cdot |\mathrm{stab}_G((x_0, \ldots, x_{n-1}))|.$$

But the orbit of $(x_0, \ldots, x_{n-1})$ "is" the cycle containing $(x_0, \ldots, x_{n-1})$ in the disjoint cycle decomposition of this row permutation. The length of this cycle is thus a factor of $n/\gcd(n, c(i))$.

For the factor $d = 1$, a fixed point is built by taking a vector $(x_0, \ldots, x_{\gcd(n,c(i))-1})$, and concatenating it $n/\gcd(n, c(i))$ times to form a vector of length n. There are p^r choices of each of the x_i, and thus $p^{r\cdot\gcd(n,c(i))}$ many n-vectors with orbit length equal to 1.

We claim that for each factor $d > 1$, there is an n-vector $(x_0, \ldots, x_{n-1})$ for which the orbit length is d. Indeed, fix an f such that $d \cdot f = n/\gcd(n, c(i))$ and choose two distinct elements $x, y \in \mathrm{GF}(p^r)$. Consider the n-vector which consists of the concatenation of f copies of the vector $(y, \ldots, y, x)$ which has only one entry equal to x,

$$(y, \ldots, y, x) \smile (y, \ldots, y, x) \smile \cdots \smile (y, \ldots, y, x).$$

Note that the vector $(y, \ldots, y, x)$ has length $d \cdot \gcd(n, c(i))$.

Consider the last x of this n-vector. After a minimum number of t applications of the permutation, it is in a position of an x in the n-vector. Then

$$t = \mathrm{lcm}(d \cdot \gcd(n, c(i)), c(i)) = \frac{d \cdot \gcd(n, c(i)) \cdot c(i)}{\gcd(d \cdot \gcd(n, c(i)), c(i))}$$

As d divides $n/\gcd(n, c(i))$, it follows that $\gcd(d, c(i))$ divides $\gcd(n/\gcd(n, c(i)), c(i))$. Since

$$\gcd\Big(\frac{n}{\gcd(n, c(i))}, c(i)\Big) = 1,$$

we have that

$$\gcd(d \cdot \gcd(n, c(i)), c(i)) = \gcd(n, c(i)).$$

It follows that $t = d \cdot c(i)$ applications of the permutation has this n-vector as fixed point. Any iteration of this $d \cdot c(i)$-iterate has this n-vector as fixed point, and the order of this $d \cdot c(i)$-iterate is

$$\frac{\frac{n}{\gcd(n,c(i))}}{\gcd\left(d \cdot c(i), \frac{n}{\gcd(n,c(i))}\right)} = \frac{\frac{n}{\gcd(n,c(i))}}{\gcd\left(d, \frac{n}{\gcd(n,c(i))}\right)} = \frac{\frac{n}{\gcd(n,c(i))}}{d} = \frac{n}{d \cdot \gcd(n, c(i))} = f.$$

It follows that

$$|\mathrm{stab}_G((y, \ldots, y, x) \smile (y, \ldots, y, x) \smile \cdots \smile (y, \ldots, y, x))| = f,$$

and thus the orbit has d elements, meaning that in the cycle decomposition of the permutation the cycle containing this vector has length d.

Analysis of the number of cycles of a given length. Fix a divisor d' of $n/\gcd(n, c(i))$. We now count the number of cycles of length exactly d' in the cycle decomposition of the given permutation. As observed before, for $d' = 1$ there are exactly $p^{r \cdot \gcd(n,c(i))}$ cycles of length 1 for this permutation. Now consider the case when $d' > 1$. It can be shown that if an n-vector $(x_0, \ldots, x_{n-1})$ has an orbit of length dividing d', then it is a concatenation of a number of copies of a vector $(y_1, \ldots, y_{d' \cdot \gcd(n,c(i))})$. Observe that the total number of such vectors that can be constructed using the elements of $\mathrm{GF}(p^r)$ is $p^{r \cdot d' \cdot \gcd(n,c(i))}$. But for $d' > 1$ many of these $(d' \cdot \gcd(n, c(i)))$ vectors have orbits whose cardinality is a proper divisor of d' and thus should be excluded from the count of items producing cycles of length exactly d'. Notice that for d a divisor of d' the vectors producing orbits of cardinality d are obtained by concatenating the vector $(y_1, \ldots, y_{d \cdot \gcd(n,c(i))})$ the appropriate number of times. The vectors among ones of the form $(z_1, \ldots, z_{d' \cdot \gcd(n,c(i))})$ to be excluded are those obtained by concatenating $\frac{d'}{d}$ copies of a vector $(y_1, \ldots, y_{d \cdot \gcd(n,c(i))})$ to obtain the vector $(z_1, \ldots, z_{d' \cdot \gcd(n,c(i))})$. Let $N(d')$ denote the number of $(d' \cdot \gcd(n, c(i)))$ vectors that produce cycles of length exactly d'. Thus, $N(1) = p^{r \cdot \gcd(n,c(i))}$. For $d' > 1$ we find that

$$N(d') = p^{r \cdot d' \cdot \gcd(n,c(i))} - \sum_{d \mid d',\, d \neq d'} N(d).$$

Alternately this can be written

$$p^{r \cdot d' \cdot \gcd(n,c(i))} = \sum_{d \mid d'} N(d).$$

By the Möbius inversion formula ([25, Theorem 2, p. 20]), we have

$$N(d') = \sum_{d \mid d'} p^{r \cdot d \cdot \gcd(n,c(i))} \mu\left(\frac{d'}{d}\right). \tag{3.3}$$

Note that since each orbit contains exactly d' elements, the number of disjoint cycles in the cycle decomposition of the permutation contributed by these vectors is $\frac{N(d')}{d'}$. The question is whether the number $\frac{N(d')}{d'}$ is even, or odd. Since a cycle of odd length is an even permutation, the answer to this question is relevant only when d' is even. Let d' be even and have prime factorization

$$d' = 2^a \cdot p_1^{s_1} \cdot \cdots \cdot p_t^{s_t}, \quad a > 0. \tag{3.4}$$

Since we are interested in only the parity of $\frac{N(d')}{d'}$, we seek to determine if

$$N(d') \bmod 2^{a+1} \tag{3.5}$$

is zero, or positive.

Consider $\mu(\frac{d'}{d})$ for an even d' and a factor d of d'. By the definition of μ, the only case when $\mu(\frac{d'}{d})$ is nonzero is when $\frac{d'}{d}$ is 1, or else square free (i.e., a product of distinct prime numbers). In each of these cases the power of 2 that divides into d is at least 2^{a-1}, so that the factor $p^{r \cdot d \cdot \gcd(n,c(i))}$ of the term corresponding to the factor d is of the form $v^{2^{a-1} \cdot t}$ where t and v are integers. Note that v odd if p is an odd prime number, and even otherwise.

Next, using the preceding analysis we present our analysis of the parity of π. We analyze separately the case when p is an odd prime and when $p = 2$.

Lemma 3.6. *Let $p > 2$ be a prime. If $p \equiv_4 3$, n is even, r is odd, and $\gcd(n, c(i))$ is odd for an odd number of $i \in \{0, \ldots, m-1\}$, then the function π is an odd permutation; otherwise it is even.*

Proof. Let $a > 1$ be an integer. Then for any odd number v we have that $v^{2^{a-1}} \equiv 1 \bmod 2^{a+1}$, by [25, Section 4.1, Theorem 2′]. Then equation (3.5) reduces to

$$\sum_{d \mid d'} p^{r \cdot d \cdot \gcd(n,c(i))} \mu\left(\frac{d'}{d}\right) \bmod 2^{a+1} = \sum_{d \mid d'} 1 \cdot \mu\left(\frac{d'}{d}\right) \bmod 2^{a+1} = 0$$

since for any integer $d' > 1$ we have, by [25, Proposition 2.2.3, p. 19], that $\sum_{d \mid d'} \mu(d) = 0$.

Next, consider $a = 1$. We need to analyze the following two cases.

Case 1: r is even or $p \equiv_4 1$. Since for each odd number v we have $v^2 \equiv_4 1$ and since we have $a = 1$ in equation (3.4), equation (3.5) reduces to

$$\sum_{d \mid d'} p^{r \cdot d \cdot \gcd(n,c(i))} \mu\left(\frac{d'}{d}\right) \bmod 4 = \sum_{d \mid d'} 1 \cdot \mu\left(\frac{d'}{d}\right) \bmod 4 = 0$$

using [25, Proposition 2.2.3, p. 19] as in the previous case and the fact that $a = 1$ and $p \equiv_4 1$ or r is even. This concludes the argument that if p is a prime number such that $p \equiv_4 1$, or if r is even, then for each i the permutation shifting each item in the i-th row of $M_{m,n}(\mathrm{GF}(p^r))$ by $c(i)$ units is an even permutation. As a result the function π is a composition of even permutations, and thus is an even permutation in this case.

Case 2: r is odd and $p \equiv_4 3$. We will start analyzing this case by first assuming that $d' > 2$. The factors of d' are either of the form $2d$ where d is odd, or d where d is odd.

Part 1: factors of the form $2d$ where d is odd. Since $v^2 \equiv_4 1$ for each odd number v, we have

$$\sum_{2d \mid d'} p^{r \cdot 2d \cdot \gcd(n,c(i))} \mu\left(\frac{d'}{2d}\right) \bmod 4 = \sum_{d \mid \frac{d'}{2}} p^{r \cdot 2d \cdot \gcd(n,c(i))} \cdot \mu\left(\frac{d'}{2d}\right) \bmod 4 = \sum_{d \mid \frac{d'}{2}} 1 \cdot \mu\left(\frac{d'}{2d}\right) \bmod 4 = 0$$

again using [25, Proposition 2.2.3, p. 19] as before.

Part 2: factors of the form d where d is odd. First note that if v is an odd number such that $v \equiv_4 3$, then for any odd number r, $v^r \equiv_4 3$. Using this observation and the fact that $a = 1$ in equation (3.4), equation (3.5) reduces to

$$\sum_{d \mid \frac{d'}{2}} p^{r \cdot d \cdot \gcd(n,c(i))} \mu\left(\frac{d'}{d}\right) \bmod 4 = \sum_{d \mid \frac{d'}{2}} 3^{\gcd(n,c(i))} \cdot \left(-\mu\left(\frac{d'}{2d}\right)\right) \bmod 4 = (-3^{\gcd(n,c(i))}) \cdot \sum_{d \mid \frac{d'}{2}} \mu\left(\frac{d'}{2d}\right) \bmod 4 = 0$$

Here we used the fact that μ is multiplicative, so that for odd w, $\mu(2w) = \mu(2)\mu(w) = -\mu(w)$, and we again used [25, Proposition 2.2.3, p. 19]. Taking Parts 1–2 together, we obtain for $d' > 2$ that $N(d') \equiv_4 0$.

Next, assume that $d' = 2$. Then $\frac{N(d')}{d'}$ reduces to

$$\frac{p^{r \cdot 1 \cdot \gcd(n,c(i))}\mu(2) + p^{r \cdot 2 \cdot \gcd(n,c(i))}\mu(1)}{2} = \frac{p^{r \cdot \gcd(n,c(i))} \cdot (p^{r \cdot \gcd(n,c(i))} - 1)}{2}.$$

Since p is odd, the parity of this quantity depends entirely on the parity of $\frac{p^{r \cdot \gcd(n,c(i))}-1}{2}$, which in turn depends on the parity of $r \cdot \gcd(n, c(i))$. For this we consider the parity of $\frac{(4k+3)^m-1}{2}$ (since $p \equiv_4 3$). By the Binomial Theorem, $(4k+3)^m$ has the form $3^m + 4x$ for an appropriate integer x, and so

$$\frac{(4k+3)^m - 1}{2} = \frac{3^m + 4x - 1}{2},$$

and the parity of this quantity depends on the parity of $\frac{3^m-1}{2}$. Applying the Binomial Theorem to $3^m = (2+1)^m$, we see that 3^m is of the form $1 + 2m + 4x$ for an appropriate integer x. Thus, $\frac{3^m-1}{2}$ is of the form $\frac{2m+4x}{2}$, which is even if, and only if, m is even. Thus, as r is odd, we find that

- $\frac{N(2)}{2} \equiv_2 0$ if $\gcd(n, c(i))$ is even,
- $\frac{N(2)}{2} \equiv_2 1$ if $\gcd(n, c(i))$ is odd.

Since for divisors $d' > 2$ of $n/\gcd(n, c(i)$ we have $\frac{N(d')}{d'}$ even, it follows that when $p \equiv_4 3$ the row permutation is even if, and only if, $r \cdot \gcd(n, c(i))$ is even. Since the function π is a composition of these row permutations, we see that for $p \equiv_4 3$, we have that π is an odd permutation if and only if $r \cdot \gcd(n, c(i))$ is odd for an odd number of i and even for the remaining values of i. □

Lemma 3.7. *Let $\pi : M_{m,n}(\mathrm{GF}(2^r)) \to M_{m,n}(\mathrm{GF}(2^r))$. If $m \cdot r \cdot \gcd(n, c(0)) = 1$ and $n = 2$, then π is an odd permutation; otherwise it is an even permutation.*

Proof. We analyze separately the cases when $m > 1$ and $m = 1$.

Case 1: Let $m > 1$. The number $2^{r(m-1)n}$ is an even number, and each cycle length of the permutation π appears a multiple of $2^{r(m-1)n}$ times in its cycle decomposition. Thus in this case π is an even permutation.

Case 2: Let $m = 1$. Then the function π is a single row permutation, and the factor $2^{r(m-1)n}$ is equal to 1, so that the parity argument when $m > 1$ does not apply. Once again apply equations (3.3) and (3.5) for $p = 2$. Considering a factor d' of $n/\gcd(n, c(0))$ with factorization as in equation (3.4), we distinguish between the cases $a > 2$, $a = 1$ and $a = 2$.

For $a > 2$ we have $n > 2$ and the factors $2^{r \cdot d \cdot \gcd(n,c(i))}$ in the nonzero terms of (3.3) have 2^{a-1} as a divisor of d. Write $d = k_d \cdot 2^{a-1}$. We have

$$2^{r \cdot d \cdot \gcd(n,c(i))} = 2^{r \cdot k_d \cdot 2^{a-1} \cdot \gcd(n,c(i))}$$

which for each nonnegative integer a is divisible by $2^{2^{a-1}}$, which in turn is divisible by 2^{a+1}. Thus we find from equation (3.3) that $N(d') \equiv \mu(d')2^{r \cdot \gcd(n,c(i))} \bmod 2^{a+1}$. But since $a > 2$, we must have $\mu(d') = 0$. It follows that $\frac{N(d')}{d'}$ is even in this case.

For $a = 1$ we see that the only contributing terms to the parity of the i-th row permutation are of the form

$$N(d') \equiv \mu(d')2^{r \cdot \gcd(n,c(0))} \bmod 4$$

where d' is an even square-free factor of $n/\gcd(n, c(0))$. If $r \cdot \gcd(n, c(0)) > 1$, then $N(d') \equiv_4 0$ and the factor d' of $n/\gcd(n, c(0))$ contributes an even number of cycles of even length to the cycle decomposition of the row permutation. We see that for $m \cdot r \cdot \gcd(n, c(0)) > 1$ the function π is an even permutation.

Finally consider the case when $m \cdot r \cdot \gcd(n, c(0)) = 1$. For $d' > 2$ a square-free even factor of $n/\gcd(n, c(0))$, we have that $N(d') = \mu(d')2 \equiv_4 2$. Suppose that n has $x + 1$ distinct prime factors, including 2. Thus, as $d' > 2$, we have $x > 0$. The number of square-free even factors of $n/\gcd(n, c(0))$ larger than 2 is $2^x - 1$, an odd number. Thus the square-free even factors of $n/\gcd(n, c(0))$ larger than 2 contribute an odd number of even length cycles to the cycle decomposition of the permutation π. To complete the count of the number of cycles of square-free even length in the cycle decomposition of π, we must still consider $\frac{N(2)}{2}$. By equation (3.3),

$$\frac{N(2)}{2} = \frac{2\mu(2) + 2^2\mu(1)}{2} = \frac{2(2-1)}{2} = 1.$$

Thus, when $a = 1$, the square-free even factors of n contribute an even number of cycles of (square-free) even length. Thus, if $n > 2$ and the largest power of 2 that divides n is equal to 1, we find that π is even.

For $a = 2$ we see that the only contributing terms to the parity of the i-th row permutation are of the form

$$N(d') \equiv \mu(d'/2)2^{2 \cdot r \cdot \gcd(n,c(0))} \bmod 8$$

where $\frac{d'}{4}$ is an odd square-free factor of $n/\gcd(n, c(0))$. If $r \cdot \gcd(n, c(0)) > 1$, then $N(d') \equiv_8 0$. Therefore, we must consider the case when $r \cdot \gcd(n, c(0)) = 1$. In this case $N(d') \equiv_8 4$, and the factor d' contributes an odd number of cycles of length d' to the disjoint cycle decomposition of π. If n has k odd prime factors, then there are 2^k factors d' with, in the notation of equation (3.4), $a = 2$. When $k > 0$, the number of cycles of even length contributed to the disjoint cycle decomposition of π by all these factors combined is an even number (the sum of an even number of odd numbers). When n has no odd prime factors, then there is only one d' with $a = 2$, namely $d' = 4$. In this case we have

$$N(4) = 2^{r \cdot \gcd(n,c(0))}\mu(4) + 2^{2 \cdot r \cdot \gcd(n,c(0))}\mu(2) + 2^{4 \cdot r \cdot \gcd(n,c(0))}\mu(1)$$

and $N(4) \equiv_8 2^{2 \cdot r \cdot \gcd(n,c(0))}\mu(2)$. If $r \cdot \gcd(n, c(0)) > 1$, then $N(4) \equiv_8 0$, and else $N(4) \equiv_8 4$.

Finally, we consider the remaining two cases. In the case when $n = 4$ and $m \cdot r \cdot \gcd(n, c(0)) = 1$, the permutation π has three 4-cycles and one 2-cycle and thus π is an even permutation. In the case when $n = 2$, $m = 1$, $r = 1$ and c odd, the π permutation has one 2-cycle, and two fixed points, and is thus an odd permutation. □

3.4 Analysis of the MixColumns-like function (ρ-function)

Definition 3.8. Let $\rho : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r))$ be a mapping defined as the parallel application of n "column" mappings $\rho_j : M_{m,1}(\mathrm{GF}(p^r)) \to M_{m,1}(\mathrm{GF}(p^r))$ defined by $\rho(a) = b$ if and only if $b_j = \rho_j(a_j)$ for all $0 \le j < n$ where each ρ_j is given by $\rho_j(x) = C \cdot x$ for all $x \in M_{m,1}(\mathrm{GF}(p^r))$ where $C \in M_{m,m}(\mathrm{GF}(p^r))$ is an invertible diffusion matrix.

Lemma 3.9. *The function ρ is a linear transformation of $M_{m,n}(\mathrm{GF}(p^r))$.*

Lemma 3.10. *Let $C \in M_{m,m}(\mathrm{GF}(p^r))$ be an invertible diffusion matrix and $n > 1$. Then the function ρ is an odd permutation if and only if p, n, and $\frac{p^{rm}-1}{|\langle C\rangle|}$ are odd.*

Proof. Consider the function ρ as a composition of n permutations ρ_j, each of which multiplies the j-th column by the invertible $m \times m$-matrix C over $\mathrm{GF}(p^r)$ and fixes the other $n-1$ columns. Fix $j \in \mathbb{N}$. Then ρ_j produces cycles of length $|\langle C\rangle|$. Of the p^{rm} possible states of the j-th column all but the fixed points of C, which is only the all-0 column, are members of cycles. Note that for any state of the j-th column, there correspond $p^{rm(n-1)}$ states of the entire matrix. Therefore, over $M_{m,n}(\mathrm{GF}(p^r))$, the permutation ρ_j consists of

$$\frac{p^{rm(n-1)}(p^{rm}-1)}{|\langle C\rangle|} \tag{3.6}$$

cycles of length $|\langle C\rangle|$. Recall that $n > 1$. This implies that the number of cycles is odd if and only if p is odd and $\frac{p^{rm}-1}{|\langle C\rangle|}$ is odd (in this case $|\langle C\rangle|$ is even). Note that for only an odd number of mappings ρ_j would their composition then be an odd permutation, meaning n must be odd. □

Note that for $p = 2$ the ρ function is odd if and only if $n = 1$. Additionally, for $n = 1$ and $p > 2$ the ρ function is odd if and only if $\frac{p^{rm}-1}{|\langle C\rangle|}$ is odd.

3.5 Analysis of the generalized Rijndael-like round functions

Definition 3.11. Let $m, n, r > 0$ be natural numbers and $k \in \mathcal{K}$. The mapping

$$T[k] : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r)), \quad T[k] = \sigma[k] \circ \rho \circ \pi \circ \lambda,$$

is called a *generalized Rijndael-like round function*.

Corollary 3.12. *Let p be an odd prime. For each $k \in \mathcal{K}$, the generalized Rijndael-like round function $T[k]$ is an odd permutation if and only if exactly one of the functions λ, ρ, and π is odd.*

Proof. By Lemma 3.2, each $\sigma[k]$ is an even permutation. By definition the function, $T[k]$ is odd if and only if each of λ, ρ and π is odd, or else exactly one of these three functions is odd. By Lemmas 3.4, 3.6 and 3.10, these three functions cannot simultaneously be of the same parity. □

Corollary 3.13. *For $n > 2$ the Rijndael-like round function $T[k] : M_{m,n}(\mathrm{GF}(2^r)) \to M_{m,n}(\mathrm{GF}(2^r))$ is an even permutation.*

Corollary 3.14. *The Rijndael-like round function $T[k] : M_{m,2}(\mathrm{GF}(2^r)) \to M_{m,2}(\mathrm{GF}(2^r))$ is an even permutation if and only if π is even.*

Corollary 3.15. *The Rijndael-like round function $T[k] : M_{m,1}(\mathrm{GF}(2^r)) \to M_{m,1}(\mathrm{GF}(2^r))$ is an even permutation if and only if $\sigma[k]$ is odd or λ is odd.*

Note that when $n = 1$ and $m = 2$, the Rijndael-like round function $T[k]$ is an odd permutation.

Definition 3.16. Let $m, n, r > 0$ be natural numbers and $k \in \mathcal{K}$. For $s > 1$ and $2 \le i \le s$ the mapping

$$T_s[k] : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r)), \quad T_s[k] = \sigma[k_{s+1}] \circ \pi \circ \lambda \circ (\sigma[k_s] \circ \rho \circ \pi \circ \lambda) \circ \cdots \circ (\sigma[k_2] \circ \rho \circ \pi \circ \lambda) \circ \sigma[k_1]$$

where $\{k_i : 1 \le i \le s\}$ is the set of subkeys produced by the key k, is called an *s-round generalized Rijndael-like function*.

The AES as well as the actual Rijndael [17] are special s-round Rijndael-like functions for $m = n = 4$, $r = 8$, $p = 2$ and $s = 10, 12,$ or 14 (depending on key size).

Theorem 3.17 ([39]). *Let $m, n > 2$ and $r \geq 2$ be natural numbers. Then the s-round Rijndael-like function*

$$T_s[k] : M_{m,n}(\mathrm{GF}(2^r)) \to M_{m,n}(\mathrm{GF}(2^r))$$

is an even permutation.

Using Corollaries 3.13–3.15, we have the following generalization of the theorem above.

Theorem 3.18. *For $n > 2$ the s-round Rijndael-like function*

$$T_s[k] : M_{m,n}(\mathrm{GF}(2^r)) \to M_{m,n}(\mathrm{GF}(2^r))$$

is an even permutation.

Corollary 3.19. *The s-round Rijndael-like function $T_s[k] : M_{m,2}(\mathrm{GF}(2^r)) \to M_{m,2}(\mathrm{GF}(2^r))$ is an even permutation if and only if π is odd and s is even or π is even.*

Corollary 3.20. *The s-round Rijndael-like function $T_s[k] : M_{m,1}(\mathrm{GF}(2^r)) \to M_{m,1}(\mathrm{GF}(2^r))$ is an even permutation if and only if σ is odd or λ is odd or else s is even.*

The proofs of the theorems below are omitted as they follow directly from the above theorems about the parity of the functions σ, ρ, λ, and π.

Theorem 3.21. *Let $p > 2$ be a prime. Then the s-round generalized Rijndael-like function $T_s[k]$ is an odd permutation if one of the following holds:*
(i) *s is even and ρ is odd,*
(ii) *s is odd and either π or λ is odd.*

Corollary 3.22. *Let $p > 2$ be a prime. Then the set of s-round Rijndael-like functions do not form a group if one of the following holds:*
(i) *s is even and ρ is odd,*
(ii) *s is odd and either π or λ is odd.*

4 Groups generated by the generalized Rijndael-like round functions

In this section we will show properties of groups generated by the round functions of the Rijndael-like $\mathcal{SP}$-network. We provide conditions under which the group generated by the generalized Rijndael-like round functions based on operations of the finite field $\mathrm{GF}(p^k)$ $(p \geq 2)$ is equal to the symmetric group or the alternating group on the state space. Some of the techniques that we use for this result appear in [10].

In our analysis of this group note that by Lemma 3.9 and the fact that π is a linear transformation, the functions ρ and π appearing in $T[k] = \sigma[k] \circ \rho \circ \pi \circ \lambda$ are both linear. Thus the map $\alpha = \rho \circ \pi$ is a linear transformation.

The space $V = M_{m,n}(\mathrm{GF}(p^r))$ is a direct sum

$$V = V_1 \oplus \cdots \oplus V_{mn}$$

where each V_i has dimension r over $\mathrm{GF}(p)$. For any $v \in V$ we write

$$v = v_1 + \cdots + v_{mn}$$

where $v_i \in V_i$. Also, we consider the projections $\mathrm{Proj}_i : V \to V_i$ given by $\mathrm{Proj}_i(v) = v_i$.

Definition 4.1. We say that $\gamma : V \to V$ is a *piecewise Galois field inversion* if $\gamma(v) = (v_1)^{\epsilon_1} \oplus \cdots \oplus (v_{mn})^{\epsilon_{mn}}$ for all $v \in V$ where $\epsilon_{mn} \in \{-1, 1\}$ is such that $\epsilon_i = -1$ if $v_i \neq 0$, and $\epsilon_i = 1$ otherwise.

Lemma 4.2. *Let γ_i denote the restriction of γ to V_i and let $r > 4$. Then:*
(1) $\gamma(0) = 0$ *and* γ^2 *is the identity map.*
(2) *Let* $i \in \mathbb{Z}_{mn}$.
   (a) *For all* $v \in V_i$ *where* $v \neq 0$, *the image of the map* $V_i \to V_i$ *which maps* $x \mapsto \gamma_i(x+v) - \gamma_i(x)$ *has size greater than* p^{r-2}.
   (b) *If a subspace of* V_i *is invariant under* γ_i, *then it has codimension at least* 3.

Proof. The condition (1) is satisfied by construction of γ.

(2, a) Fix $0 \neq v \in \mathrm{GF}(p^r)$ and consider the map $\mathrm{GF}(p^r) \to \mathrm{GF}(p^r)$ which maps $x \mapsto (x+v)^{-1} - x^{-1}$. The size of the image of this map is equal to the number of distinct elements b that solve the equation $(x+v)^{-1} - x^{-1} = b$. If $x \neq \mathbf{0}$ or $-v$, then $(x+v)((x+v)^{-1}) = 1$ and $x(x^{-1}) = 1$, and

$$\begin{aligned}(x+v)^{-1} - x^{-1} = b &\implies x(x+v)((x+v)^{-1} - x^{-1}) = x(x+v)b \\ &\implies x - (x+v) = bx^2 + bvx \\ &\implies bx^2 + bvx + v = 0 \\ &\implies b(x^2 + vx) = -v.\end{aligned}$$

Now as x ranges over $\mathrm{GF}(p^r)$ except $\mathbf{0}$ and $-v$, the quantity $(x^2 + vx)$ ranges over at least $\frac{p^r-2}{2}$ distinct nonzero values, whence solving for b we find at least $\frac{p^r-2}{2}$ distinct values of b. Therefore the map $x \mapsto (x+v)^{-1} - x^{-1}$ has at least $\frac{p^r-2}{2} > p^{r-2}$ distinct values, fulfilling condition (2, a).

(2, b) Assume that U is a proper (vector) subspace of V_i and U is closed under inversion. As subspace, U is an additive subgroup of V_i. Apply Theorem 2.10 and Lemma 2.11 to find that either U is a subfield of V_i, or $|U| = |F|$ for some subfield $F \subset V_i$. Since V_i is isomorphic to $\mathrm{GF}(p^r)$, Theorem 2.7 implies that $|U| = p^k$ where $k \mid r$ and $k \neq r$. Then as k is a proper divisor of r, $k \leq \frac{r}{2}$. But then we have the following implications:

$$\begin{aligned}|U| \leq p^{\frac{r}{2}} &\implies \dim(U) \leq \frac{r}{2} && \text{because } |U| = p^{\dim(U)} \\ &\implies \mathrm{codim}(U) \geq \frac{r}{2} && \text{because } \dim(U) + \mathrm{codim}(U) = \dim(V_i) = r \\ &\implies \mathrm{codim}(U) \geq 3 && \text{provided } r \geq 5.\end{aligned}$$

This completes the proof of condition (2, b) and the theorem. □

Theorem 4.3. *Let $r > 4$ and $V = M_{m,n}(\mathrm{GF}(p^r))$. If $U \neq \{\mathbf{0}\}$ is a subspace of V such that for all $u \in U$ and $v \in V$*

$$(\alpha \circ \gamma)(v+u) - (\alpha \circ \gamma)(v) \in U$$

where $\alpha = \rho \circ \pi$, then U is invariant under α and U is a sum of some of the V_i.

Proof. We already know that α is a permutation of the set V. By Lemma 3.9 and the fact that π is a linear transformation we have that α is an invertible linear transformation of the vector space V over the field $\mathrm{GF}(p^r)$. Thus, $W = \alpha^{-1}[U]$ is a vector subspace of V of the same dimension as U.

Thus, for all $u \in U$ and $v \in V$ we have

$$\gamma(v+u) - \gamma(v) \in \alpha^{-1}[U] = W. \tag{4.1}$$

Setting $v = 0$ in (4.1) and using the fact that $\gamma(0) = 0$, we see that for each $u \in U$ we have $\gamma(u) \in W$. Hence, γ is a function from U to W. Since U and W are finite and $|\gamma[U]| = |U| = |W|$, statement (1) of Lemma 4.2 implies that

$$\gamma[U] = W \quad \text{and} \quad \gamma[W] = U.$$

Using the hypothesis that U is not $\{\mathbf{0}\}$, choose a $u \in U$ and an i such that $u_i = \mathrm{Proj}_i(u) \neq 0$. With i fixed from now on, consider any $v_i \in V_i$ with $v_i \neq 0$. We have that $\gamma(u+v_i) - \gamma(v_i) \in W$ and $\gamma(u) \in W$. Since W is a vector space, $-\gamma(u) + \gamma(u+v_i) - \gamma(v_i) \in W$. Explicitly written $\gamma(u+v_i)$ and $\gamma(u)$ have the form

$$\gamma(u+v_i) = \gamma_1(u_1) \oplus \gamma_2(u_2) \oplus \cdots \oplus \gamma_i(u_i + v_i) \oplus \cdots \oplus \gamma_{mn}(u_{mn})$$

and

$$\gamma(u) = \gamma_1(u_1) \oplus \gamma_2(u_2) \oplus \cdots \oplus \gamma_i(u_i) \oplus \cdots \oplus \gamma_{mn}(u_{mn}).$$

Since V_i is a vector space, $-\gamma_i(u_i) + \gamma_i(u_i + v_i) - \gamma_i(v_i) \in V_i$. Therefore,

$$-\gamma(u) + \gamma(u + v_i) - \gamma(v_i) = -\gamma_i(u_i) + \gamma_i(u_i + v_i) - \gamma_i(v_i) \in W \cap V_i.$$

If for each $v_i \in V_i$ this vector was the zero-vector, then the image of the map $v_i \mapsto \gamma_i(v_i + u_i) - \gamma_i(v_i)$ from V_i to V_i would be $\{\gamma_i(u_i)\}$. This would contradict (2, a) of Lemma 4.2. Thus, $W \cap V_i \neq \{\mathbf{0}\}$.

Since $U \cap V_i = \gamma(W \cap V_i)$ and $\gamma_i(x) = 0$ implies $x = 0$, we have that $U \cap V_i \neq \{\mathbf{0}\}$. Thus there is a nonzero element $u_i \in U \cap V_i$. By the hypothesis that $r > 4$ and (2, a) of Lemma 4.2, the map $x \mapsto \gamma_i(x + u_i) - \gamma_i(x)$ from V_i to V_i has image of cardinality greater than p^{r-2}. But as seen in (4.1), the image of this map is also a subset of W. Thus $W \cap V_i$ is a linear subspace of V_i and has cardinality greater then p^{r-2}. As subspace of V_i the cardinality of $W \cap V_i$ must be factor of the cardinality p^r of V_i and thus is a power of the prime number p. It follows that the cardinality of $W \cap V_i$ is at least p^{r-1}. But then the codimension of $W \cap V_i$ in V_i is at most 1. Similarly, the codimension of $U \cap V_i$ is at most 1. Hence, the subspace $U \cap W \cap V_i$ of V_i has codimension of at most 2 in V_i. In particular, since $r > 2$, we have that $U \cap W \cap V_i \neq \{\mathbf{0}\}$.

Because $\gamma(U) = W$ and $\gamma(W) = U$, we see that $U \cap W \cap V_i$ is invariant under γ. From condition (2), it follows that $U \cap W \cap V_i = V_i$. Hence, $U \supset V_i$.

So if U contains an element of V_i for some i, then $U \supset V_i$. Hence, U is a direct sum of some of the V_i. Since $W = \gamma(U)$ and $\gamma(V_i) = V_i$ for all i, we see that $W = U$, and since $U = \gamma(W)$, it follows that $U = \alpha(U)$ □

Theorem 4.4. *Let $\tau = \{T[k] : k \in \mathcal{K}\}$ be the set of all generalized Rijndael-like functions*

$$T[k] : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r)) \quad (p \geq 2)$$

and $\mathcal{G}_\tau = \langle T[k] : k \in \mathcal{K}\rangle$ be the group generated by the set τ. Assume that the only subspaces of $M_{m,n}(\mathrm{GF}(p^r))$ that are invariant under $\alpha = \rho \circ \pi$ are $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$. Then for all m, n and $r > 4$ the group $\mathcal{G}_\tau$ is primitive.

Proof. Let $V = M_{m,n}(\mathrm{GF}(p^r))$. Suppose that $\mathcal{G}_\tau$ acts imprimitively on V. By [10, Corollary 4.1], there is a proper subspace U of V such that $U \neq \{\mathbf{0}\}$ and such that for all $u \in U$ and $v \in V$ one has $(\alpha \circ \gamma)(v + u) - (\alpha \circ \gamma)(v) \in U$. By Theorem 4.3, U is a direct sum of some of the V_i and an invariant subspace of α (i.e., $U = \alpha(U)$). But this contradicts the hypothesis that α has no nontrivial invariant subspaces. Therefore, G is primitive. □

The following theorem follows directly from Lemma 2.4 and Theorem 4.4.

Theorem 4.5. *Let $\tau = \{T[k] : k \in \mathcal{K}\}$ be the set of all generalized Rijndael-like functions on $M_{m,n}(\mathrm{GF}(p^r))$ and $\mathcal{G}_\tau = \langle T[k] : k \in \mathcal{K}\rangle$ be the group generated by the set τ. If $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$ are the only subspaces of $M_{m,n}(\mathrm{GF}(p^r))$ that are invariant under $\alpha = \rho \circ \pi$ and $\mathcal{G}_\tau$ contains an l-cycle with $2 \leq l \leq (p^{rmn} - l)!$, then for all $m, n > 1$ and $r > 4$ the group $\mathcal{G}_\tau$ is either the alternating group or the symmetric group acting on $M_{m,n}(\mathrm{GF}(p^r))$.*

Lemma 2.5 shows that the probability for a random permutation in $\mathcal{G}_\tau$ to have a cycle of length l with $2 \leq l \leq (p^{rmn} - l)!$ is equal to $1 - e^{-\sum_{i=2}^{L} 1/i}$ where $L = (p^{rmn} - l)! - 1$. This means that the probability that there is an l-cycle in $\mathcal{G}_\tau$ that satisfies the condition of the preceding theorem increases as the values of $m, n, p > 1$ and $r > 4$ increase.

Also, note that the hypothesis that α's only invariant subspaces are $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$ implies that $\gcd(c_1, \ldots, c_m, n) = 1$. Indeed, suppose that $\gcd(c_1, \ldots, c_m, n) = x > 1$. Consider an input $\mathbf{a} \in M_{m,n}(p^r)$ for α with only one nonzero entry

$$\mathbf{a} = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix}.$$

Note that under α, the orbit of $\mathbf{a}$ will have its nonzero entries at column positions of form $1 + k \cdot x \leq n$, $k \in \mathbb{N}$. Thus, no orbit element will have a nonzero entry in the second column. But then as α is linear, it has an invariant subspace consisting of members of $M_{m,n}(\mathrm{GF}(p^r))$ that have no nonzero entries in the second column. This is a subspace different from $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$, contradicting that α's only invariant subspaces are $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$:

Also, note that in general the condition $\gcd(c_1, \ldots, c_m, n) = 1$ is not sufficient to guarantee that α's only invariant subspaces are $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$. To see this, the reader is invited to consider the following.

Example. Consider the vector space $M_{2,8}(\mathrm{GF}(7))$, an irreducible polynomial $f(x) = x^2 + x + 3$ over GF(7) and $c_1 = 1$ and $c_2 = 5$. Since the MixColumns-like function ρ is linear, it can be specified as $\mathbf{d} = M \cdot \mathbf{c}$ for $c, d \in M_{2,8}(\mathrm{GF}(7))$ and M a matrix of dimension 2×2. Let $M = \left[\begin{smallmatrix} 1 & 4 \\ 1 & 0 \end{smallmatrix}\right]$, i.e., the generating polynomial $M(x) = x + 1$ for $\mathrm{GF}(7)/\langle f \rangle$.

Now let $\mathbf{a} \in M_{2,8}(\mathrm{GF}(7))$,

$$\mathbf{a} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

be the input in the function α. It is easy to see that the orbit of $\mathbf{a}$ under α has 48 elements containing a linearly independent subset of at most 15 elements. Thus the subspace W generated by this orbit has dimension $1 < \dim(W) \leq 15$, and as α is linear, this is an invariant subspace of α with dimension less than $\dim(M_{2,8}(\mathrm{GF}(7))) = 16$.

Note that the ShiftRows-like function π for this example (in the sense of [17, Definition 9.4.1]) and the MixColumns-like function ρ (in the sense that the orbit of any nonzero column vector includes all the nonzero column vectors) are diffusion optimal. Thus, merely requiring that ShiftRows is diffusion optimal is not sufficient to guarantee that the only invariant subspaces of α are $\{\mathbf{0}\}$ and $M_{m,n}(\mathrm{GF}(p^r))$.

Next we determine the group $\mathcal{G}_\tau^s = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] : k_i \in \mathcal{K} \rangle$ generated by the set of all compositions of s (independently chosen) generalized Rijndael-like functions.

Theorem 4.6. *Let $\tau = \{T[k] : k \in \mathcal{K}\}$ be the set of all generalized Rijndael-like functions and $\mathcal{G}_\tau = \langle T[k] : k \in \mathcal{K} \rangle$ be the group generated by the set τ. Then:*
(a) *If $\mathcal{G}_\tau = \mathcal{A}_{p^{rmn}}$, then $\mathcal{G}_\tau^s = \mathcal{A}_{p^{rmn}}$.*
(b) *If $\mathcal{G}_\tau = \mathcal{S}_{p^{rmn}}$, then $\mathcal{G}_\tau^s = \mathcal{A}_{p^{rmn}}$ if s is even and $\mathcal{G}_\tau^s = \mathcal{S}_{p^{rmn}}$ if s is odd.*

Proof. Part (a) follows immediately from Lemma 2.1 and Theorem 2.2. To show (b) suppose that $\mathcal{G}_\tau = \mathcal{S}_{p^{rmn}}$. If s is even, then every element of $\mathcal{G}_\tau^s$ must be an even permutation. Hence $\mathcal{G}_\tau^s = \mathcal{A}_{p^{rmn}}$ by Lemma 2.1. If s is odd, then $\mathcal{G}_\tau^s$ must contain an odd permutation. Hence $\mathcal{G}_\tau^s = \mathcal{S}_{p^{rmn}}$, again by Lemma 2.1. □

5 Conclusion

In this paper we provided conditions for which the round functions of a Rijndael-like block cipher deployed over a finite field $\mathrm{GF}(p^r)$ ($p > 2$) do not constitute a group under functional composition – Theorem 3.21. We also provided conditions for which the round functions of a Rijndael-like block cipher over a finite field $\mathrm{GF}(p^r)$ ($p \geq 2$) generate either the alternating group or the symmetric group on the message space – Theorem 4.6.

Acknowledgement: The authors would like to thank Rüdiger Sparr and Ralph Wernsdorf for their valuable remarks. We would also like to thank the anonymous referee for his/her thorough review. We highly appreciate their comments and suggestions, which significantly contributed to improving the quality of the paper.

Funding: Supported by the National Science Foundation grant DMS-1062857.

References

[1] L. Babai, The probability of generating the symmetric group, *J. Combin. Theory* **52** (1989), 148–153.
[2] E. Barkan and E. Biham, In how many ways can you write Rijndael?, in: *Advances in Cryptology – ASIACRYPT 2002*, Lecture Notes in Comput. Sci. 2501, Springer-Verlag, Berlin (2002), 160–175.

[3] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, New York, 1993.
[4] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich and A. Shamir, Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds, in: *Advances in Cryptology – CRYPTO 2010*, Lecture Notes in Comput. Sci. 6110, Springer-Verlag, Berlin (2010), 299–319.
[5] A. Biryukov and D. Khovratovich, Related-key cryptanalysis of the full AES-192 and AES-256, in: *Advances in Cryptology – ASIACRYPT 2009*, Lecture Notes in Comput. Sci. 5912, Springer-Verlag, Berlin (2009), 1–18.
[6] A. Biryukov, D. Khovratovich and I. Nikolic, Distinguisher and related-key attack on the full AES-256, in: *Advances in Cryptology – CRYPTO 2009*, Lecture Notes in Comput. Sci. 5677, Springer-Verlag, Berlin (2009), 231–249.
[7] A. Bogdanov, D. Khovratovich and C. Rechberger, Biclique cryptanalysis of the full AES, in: *Advances in Cryptology – CRYPTO 2011*, Lecture Notes in Comput. Sci. 7073, Springer-Verlag, Berlin (2011), 344–371.
[8] D. K. Branstead, J. Gait and S. Katzke, Report of the workshop on cryptography in support of computer security, Technical report NBSIR 77–1291, National Bureau of Standards, 1977.
[9] K. W. Campbell and M. J. Wiener, DES is not a group, in: *Advances in Cryptology – CRYPTO 1992*, Lecture Notes in Comput. Sci. 740, Springer-Verlag, Berlin (1993), 512–520.
[10] A. Caranti, F. Dalla Volta, M. Sala and F. Villani, Imprimitive permutation groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis, preprint (2006), http://arxiv.org/abs/math/0606022.
[11] C. Cid, S. Murphy and M. J. B. Robshaw, Small scale variants of the AES, in: *Fast Software Encryption – FSE 2005*, Lecture Notes in Comput. Sci. 3557, Springer-Verlag, Berlin (2005), 145–162.
[12] C. Cid, S. Murphy and M. J. B. Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer-Verlag, New York, 2006.
[13] D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, *SIAM J. Appl. Math.* **29** (1975), 624–627.
[14] N. Courtois and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, in: *Advances in Cryptology – ASIACRYPT 2002*, Lecture Notes in Comput. Sci. 2501, Springer-Verlag, Berlin (2002), 267–287.
[15] N. T. Courtois, G. V. Bard and S. V. Ault, Statistics of random permutations and the cryptanalysis of periodic block ciphers, *J. Math. Cryptol.* **2** (2008), 1–20.
[16] J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, preprint (1998), http://www.cryptosoft.de/docs/Rijndael.pdf.
[17] J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer-Verlag, Berlin, 2002.
[18] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), no. 3, 199–205.
[19] O. Dunkelman, N. Keller and A. Shamir, Improved single-key attacks on 8-round AES-192 and AES-256, in: *Advances in Cryptology – ASIACRYPT 2010*, Lecture Notes in Comput. Sci. 6477, Springer-Verlag, Berlin (2010), 158–176.
[20] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner and D. Whiting, Improved cryptanalysis of Rijndael, in: *Proceedings of Fast Software Encryption*, Lecture Notes in Comput. Sci. 1978, Springer-Verlag, Berlin (2001), 213–230.
[21] J. A. Gallian, *Contemporary Abstract Algebra*, Houghton Mifflin, Boston, 1992.
[22] H. Gilbert and M. Minier, A collision attack on 7 rounds of Rijndael, in: *Proceedings of the 3rd AES Candidate Conference*, National Institute for Standards and Technology, Gaithersburg (2000), 230–241.
[23] H. Gilbert and T. Peyrin, Super-sbox cryptanalysis: Improved attacks for AES-like permutations, in: *Fast Software Encryption – FSE 2010*, Lecture Notes in Comput. Sci. 6147, Springer-Verlag, Berlin (2010), 365–383.
[24] G. Hornauer, W. Stephan and R. Wernsdorf, Markov ciphers and alternating groups, in: *Advances in Cryptology – EUROCRYPT 1993*, Lecture Notes in Comput. Sci. 765, Springer-Verlag, Berlin (1994), 453–460.
[25] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer-Verlag, New York, 1990.
[26] B. S. Kaliski, R. L. Rivest and A. T. Sherman, Is the data encryption standard a group? (Results of cycling experiments on DES), *J. Cryptology* **1** (1988), 3–36.
[27] T. V. Le, R. Sparr, R. Wernsdorf and Y. Desmedt, Complementation-like and cyclic properties of AES round functions, in: *Advanced Encryption Standard – AES 2004*, Lecture Notes in Comput. Sci. 3373, Springer-Verlag, Berlin (2005), 128–141.
[28] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall, Upper Saddle River, 2003.
[29] S. Mattarei, Inverse-closed additive subgroups of fields, *Israel J. Math.* **159** (2007), 343–348.
[30] L. Miller, Generators of the symmetric and alternating group, *Amer. Math. Monthly* **48** (1941), 43–44.
[31] S. Murphy, K. G. Paterson and P. Wild, A weak cipher that generates the symmetric group, *J. Cryptology* **7** (1994), 61–65.
[32] S. Murphy and M. J. B. Robshaw, Essential algebraic structure within the AES, in: *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Comput. Sci. 2442, Springer-Verlag, Berlin (2002), 1–16.
[33] National Institute of Standards and Technology (US), Advanced encryption standard (AES), FIPS Publ. 197 (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[34] National Institute of Standards and Technology (US), Recommendation for the triple data encryption algorithm (TDEA) block cipher, Spec. Publ. 800-67 (2004), http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf.
[35] S. Patel, Z. Ramzan and G. S. Sundaram, Luby–Rackof ciphers: Why XOR is not so exclusive, in: *Selected Areas in Cryptography*, Lecture Notes in Comput. Sci. 2595, Springer-Verlag, Berlin (2003), 271–290.
[36] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: *Fast Software Encryption – FSE 1999*, Lecture Notes in Comput. Sci. 1636, Springer-Verlag, Berlin (1999), 201–214.

[37] D. M. Rodgers, Generating and covering the alternating or symmetric group, *Comm. Algebra* **30** (2002), 425–435.
[38] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.*, **27** (1948), 379–423.
[39] R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discrete Appl. Math.* **156** (2008), 3139–3149.
[40] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Pearson Prentice Hall, Upper Saddle River, 2006.
[41] R. Wernsdorf, The round functions of Rijndael generate the alternating group, in: *Fast Software Encryption – FSE 2002*, Lecture Notes in Comput. Sci. 2365, Springer-Verlag, Berlin (2002), 143–148.
[42] A. Williamson, On primitive permutation groups containing a cycle, *Math. Z.* **130** (1973), 159–162.

Received January 9, 2013.

http://topology.auburn.edu/tp/
http://topology.nipissingu.ca/tp/

TOPOLOGY PROCEEDINGS
Volume 47 (2016)
Pages 297-311

E-Published on November 1, 2015

SELECTIVE STRONG SCREENABILITY AND A GAME

LILJANA BABINKOSTOVA AND MARION SCHEEPERS

Abstract. Selective versions of screenability and of strong screenability coincide in a large class of spaces. We show that the corresponding games are not equivalent in even such standard metric spaces as the closed unit interval. We identify sufficient conditions for ONE to have a winning strategy (Theorem 3.3), and necessary conditions for TWO to have a winning strategy (Theorem 4.6) in the selective strong screenability game.

1. Introduction

Unless specified otherwise, all topological spaces in this paper are assumed to be infinite. A collection $\mathcal{A}$ of subsets of a topological space (X,τ) is *discrete* if there is for each $x \in X$ a neighborhood U of x such that $|\{A \in \mathcal{A} : A \cap U \neq \emptyset\}| \leq 1$. Note that a finite family of nonempty sets whose closures are disjoint is a discrete family. An infinite family of sets with pairwise disjoint closures need not be discrete, as illustrated by the family $\{[\frac{1}{2n+1}, \frac{1}{2n}] : n \in \mathbb{N}\}$ of disjoint closed subsets of the real line. A disjoint family of open sets covering a space is automatically a discrete family of open sets.

A family $\mathcal{A}$ of sets *refines* a family $\mathcal{B}$ of sets if there is for each $A \in \mathcal{A}$ a $B \in \mathcal{B}$ such that $A \subseteq B$. The symbol $\mathcal{O}$ denotes the collection of all open covers of the space (X,τ). When Y is a subset of X, then $\mathcal{O}_Y$ denotes the set of covers of Y by sets open in X.

R.H. Bing introduced the notions of *screenable* and *strongly screenable* in [8]. A topological space (X,τ) is *strongly screenable* if there is for each open cover $\mathcal{U}$ of X a sequence $(\mathcal{V}_n : n < \omega)$ such that each $\mathcal{V}_n$ is a *discrete* collection of sets, each $\mathcal{V}_n$ refines $\mathcal{U}$, and $\bigcup\{\mathcal{V}_n : n < \omega\}$ is an open cover of X.

2010 *Mathematics Subject Classification.* 54D20, 91A44.

Key words and phrases. Selection principle, selective screenability, selective strong screenability, infinite game.

We obtain the notion of being *screenable* by replacing "`discrete`" in the definition of strong screenability with "`disjoint`".

Towards defining the selective version of strong screenability let $\mathcal{A}$ and $\mathcal{B}$ be collections of families of subsets of a set S. Assume that the set S is endowed with a topology. Then $\mathsf{S}_d(\mathcal{A},\mathcal{B})$ denotes the selection principle:

> For each sequence $(\mathcal{U}_n : n < \omega)$ of elements of $\mathcal{A}$ there is a sequence $(\mathcal{V}_n : n < \omega)$ such that:
> (1) For each n, $\mathcal{V}_n$ refines $\mathcal{U}_n$;
> (2) For each n, $\mathcal{V}_n$ is a discrete collection of sets;
> (3) $\bigcup\{\mathcal{V}_n : n < \omega\}$ is an element of $\mathcal{B}$.

In this notation the property $\mathsf{S}_d(\mathcal{O},\mathcal{O})$ of a topological space is called *selective strong screenability* of the space. If in (2) of the definition of $\mathsf{S}_d(\mathcal{A},\mathcal{B})$ we replace `discrete` with `disjoint` we obtain the selection principle $\mathsf{S}_c(\mathcal{A},\mathcal{B})$ that was introduced in [2]. The corresponding selection principle $\mathsf{S}_c(\mathcal{O},\ \mathcal{O})$ for a topological space is the selective version of screenability, called *selective screenability*. Selective screenability was introduced by Addis and Gresham in [1] under the name *property* C.

Screenability properties are related to several fundamental topological notions, including paracompactness, metrizability and extensions of covering dimension. A family $\mathcal{A}$ of sets in a topological space (X,τ) has the property of being *locally finite* if there is for each $x \in X$ a neighborhood U of x such that $|\{A \in \mathcal{A} :\ A \cap U \neq \emptyset\}|$ is finite. A topological space is *paracompact* if for each given open cover there is a locally finite open cover refining the given cover. In [13] Michael and, independently, in [14] Nagami proved:

Theorem 1.1 (Michael, Nagami)**.** *A regular space is paracompact if, and only if, it is strongly screenable.*

Theorem 5 of [14] also proves[1]:

Theorem 1.2 (Nagami)**.** *A normal, countably paracompact space is screenable if, and only if, it is strongly screenable.*

The hypothesis of countable paracompactness in Theorem 1.2 is necessary. To justify this we first comment on the terminology *zero dimensional*: According to Sierpinski [9] a space is *zero-dimensional* if each element has a neighborhood basis consisting of sets that are both open and closed. A space has *covering dimension zero* if each *finite* open cover has a refinement by disjoint open sets, still covering the space.

[1]In personal communication Roman Pol and Elzbieta Pol pointed out that Nagami's result can be strengthened to show that selective screenability and selective strong screenability coincide in normal countably paracompact spaces, and thus in metric spaces.

A space is *ultraparacompact* if *each* open cover has a refinement by disjoint open sets still covering the space. Covering dimension zero is also called *strongly zero dimensional*.

Theorem 1.3 (Balogh, [7]). *There is a strongly zerodimensional T_4 space that is screenable*[2] *but not countably paracompact, and thus not strongly screenable.*

In [6] it was shown that for regular spaces paracompactness is equivalent to a selective version of paracompactness. Although in these spaces paracompactness is equivalent to strong screenability, (selective) paracompactness does not imply selective screenability: The Hilbert Cube $\mathbb{H} = [0,\ 1]^{\mathbb{N}}$ is compact and metrizable, but as it is strongly infinite dimensional, it is not selectively screenable.

In separable metric spaces selective screenability is related to dimension theory: With $\mathcal{O}_2$ denoting the family of open covers consisting of two sets each, $\mathsf{S}_c(\mathcal{O}_2, \mathcal{O})$ corresponds to Alexandroff's notion of *weakly infinite dimensional*. It was an open problem whether Hurewicz's notion of countable dimensionality coincides with Alexandroff's notion of weak infinite dimensionality until R. Pol gave an example of a compact selectively screenable metrizable space that is not countable dimensional [17].

In separable metrizable spaces dimension theoretic concepts have been further clarified by the study of the *selective screenability game*: Let an ordinal $\alpha > 0$ be given. Then $\mathsf{G}_c^\alpha(\mathcal{A}, \mathcal{B})$ denotes the following game of length α: In inning $\gamma < \alpha$ player ONE selects an element A_γ of $\mathcal{A}$, and TWO then responds with B_γ, a disjoint collection of sets that is a refinement of A_γ. A play $A_0, B_0, \cdots, A_\gamma, B_\gamma, \cdots \ \ \gamma < \alpha$ is won by TWO if $\bigcup\{B_\gamma : \gamma < \alpha\} \in \mathcal{B}$; otherwise, ONE wins. It was proven in [3] that a separable metrizable space X is

(1) of Lebesgue covering dimension n if, and only if, n is minimal such that TWO has a winning strategy in $\mathsf{G}_c^{n+1}(\mathcal{O}, \mathcal{O})$;
(2) countable dimensional (in the sense of Hurewicz) if, and only if, TWO has a winning strategy in $\mathsf{G}_c^\omega(\mathcal{O}, \mathcal{O})$.

These results inspired the notion of *game dimension*, explored in the papers [4] and [5]. Even though selective screenability and selective strong screenability are equivalent concepts in normal countably paracompact spaces, the corresponding games have very different characteristics, the topic of this paper. In sections 3 and 4 we report findings regarding player ONE and player TWO, respectively, on the length ω version of the selective strong screenability game. In section 5 we consider other ordinal lengths for the game.

[2]Balogh's space is in fact *selectively* screenable.

2. The selective strong screenability game

For ordinal $\alpha > 0$ define the game $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$ as follows: In each inning $\gamma < \alpha$ ONE first selects an A_γ from $\mathcal{A}$, to which TWO responds with a B_γ which is a discrete family of sets refining the family A_γ. A play

$$A_0,\, B_0,\, \cdots,\, A_\gamma,\, B_\gamma,\, \cdots \quad \gamma < \alpha$$

is won by TWO if $\bigcup\{B_\gamma : \gamma < \alpha\} \in \mathcal{B}$; otherwise, ONE wins.

Aside from the following easily verified relationships the games $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$ and $\mathsf{G}_c^\alpha(\mathcal{A}, \mathcal{B})$ are in fact very different from each other:

- If TWO has a winning strategy in $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$, then TWO has a winning strategy in $\mathsf{G}_c^\alpha(\mathcal{A}, \mathcal{B})$.
- If ONE has a winning strategy in $\mathsf{G}_c^\alpha(\mathcal{A}, \mathcal{B})$, then ONE has a winning strategy in $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$.

Moreover, certain monotonicity properties hold for this game:

- Assume that $\mathcal{A}' \supseteq \mathcal{A}$ and $\mathcal{B}' \subseteq \mathcal{B}$: If ONE has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A},\ \mathcal{B})$ then ONE has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A}', \mathcal{B}')$. If TWO has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A}',\ \mathcal{B}')$ then TWO has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$.
- Let $\alpha < \beta$ be ordinal numbers. If ONE has a winning strategy in the game $\mathsf{G}_d^\beta(\mathcal{A},\ \mathcal{B})$ then ONE has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A}, \mathcal{B})$. If TWO has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{A},\ \mathcal{B})$ then TWO has a winning strategy in the game $\mathsf{G}_d^\beta(\mathcal{A}, \mathcal{B})$.

Also the following fact is easy to verify:

Proposition 2.1. *Let (X, τ) be a topological space, let Y be a closed subset of X and let $\alpha > 0$ be an ordinal. If ONE has a winning strategy in the game $G_d^\alpha(\mathcal{O}, \mathcal{O})$ played on Y, then ONE has a winning strategy in this game played on X. If TWO has a winning strategy in the game $G_d^\alpha(\mathcal{O}, \mathcal{O})$ played on X, then TWO has a winning strategy in this game played on Y.*

3. Winning strategies for player ONE

The following version of the Banach-Mazur game on a topological space (X, τ) with specified subspace Y was defined in [16]: There is an inning per finite ordinal. In the n-th inning ONE chooses a nonempty open subset O_n of X and TWO responds with a nonempty open subset T_n of X. The players must obey the rule that for each n, $O_n \supseteq T_n \supseteq O_{n+1}$. ONE wins a play

$$O_0,\, T_0,\, O_1,\, T_1,\, \ldots O_n,\, T_n,\, \ldots$$

if $Y \cap (\bigcap\{O_n : n < \omega\}) \neq \emptyset$. Otherwise, TWO wins the play.

In [10], p. 53, the special case of $Y = X$ of this game is denoted $\mathsf{MB}(X)$. We use the notation $\mathsf{MB}(Y, X)$ to denote this game in the general case.

Lemma 3.1. *If X is a T_1-space and $U \neq X$ is an open subset of X such that $|U| > 1$, then there is an open cover $\mathcal{U}$ of X such that for each $V \in \mathcal{U}$ we have $U \not\subseteq V$.*

Proof. With U and X as given, choose distinct elements x and y in U. Then as X is T_1 the sets $X \setminus \{x\}$ and $X \setminus \{y\}$ are open. The open cover $\mathcal{U} = \{X \setminus \{x\},\ X \setminus \{y\}\}$ is as required. □

Lemma 3.2. *A space is connected if, and only if, it is not a union of a discrete collection consisting of more than one nonempty proper subsets.*

Proof. Suppose X is a space and that $\mathcal{F}$ is a collection of nonempty proper subsets of X such that $\mathcal{F}$ is a discrete family, $|\mathcal{F}| > 1$ and $X = \bigcup \mathcal{F}$. Then also $\mathcal{G} = \{\overline{F} :\ F \in \mathcal{F}\}$ is a discrete family of subsets of X that covers X, and $|\mathcal{G}| > 1$. Choose $U \in \mathcal{G}$. Then U is nonempty and closed, and as $\mathcal{G}$ is a discrete family, also $V = \bigcup(\mathcal{G} \setminus \{U\})$ is closed. But then $X = U \cup V$ and U and V are disjoint nonempty open sets, whence X is not connected. Conversely, if X is not connected then a family $\{U,\ V\}$ of disjoint nonempty open sets with union X is a discrete collection consisting of more than one nonempty set. □

From now on call a connected set *nontrivial* if it has more than one element. Recall that a family $\mathcal{P}$ of nonempty open subsets of a topological space is said to be a *π-base* if there is for each nonempty open subset U of the space an element V of $\mathcal{P}$ such that $V \subseteq U$.

Theorem 3.3. *Let X be a T_1 topological space and let Y be a subspace of X such that*

(1) *X has a π-base consisting of nontrivial connected sets, and*
(2) *ONE has a winning strategy in the game $\mathsf{MB}(Y, X)$.*

Then ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O}_Y)$.

Proof. Let σ be ONE's winning strategy in the game $\mathsf{MB}(Y, X)$. We may assume that σ calls on ONE to play elements of a fixed π-base consisting of nontrivial connected open sets. Define a strategy F for ONE of the game $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O})$ as follows:

To begin, consider $O_0 = \sigma(X)$, and apply Lemma 3.1 to define $F(\emptyset)$, ONE's first move in $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O})$, to be an open cover for which no element contains O_0 as a subset. If TWO's response is the discrete open refinement $\mathcal{T}_0$, by Lemma 3.2 the discrete family $\{\overline{T} : T \in \mathcal{T}_0\}$ does not cover O_0. Let TWO of the game $\mathsf{MB}(Y, X)$ play $T_0 = O_0 \setminus \bigcup\{\overline{T} : T \in \mathcal{T}_0\}$ a nonempty open set.

Let $O_1 = \sigma(T_0)$ be ONE's response in the game $\mathsf{MB}(Y, X)$. ONE's move $F(\mathcal{T}_0)$ in the strong screenability game is an open cover of X for which no member has O_1 as a subset. TWO's response, $\mathcal{T}_1$ is a discrete open refinement of $F(\mathcal{T}_0)$. As $\{\overline{T} : T \in \mathcal{T}_1\}$ does not cover O_1, $T_1 = O_1 \setminus \bigcup\{\overline{T} : T \in \mathcal{T}_1\}$ is a legal move for TWO in the game $\mathsf{MB}(Y, X)$.

In the next inning ONE of the game $\mathsf{MB}(Y, X)$ responds with $O_2 = \sigma(T_0, T_1)$. ONE's move $F(\mathcal{T}_0,\ \mathcal{T}_1)$ in the strong screenability game is an open cover of X (as in Lemma 3.1) for which no member has O_2 as a subset. TWO's response, $\mathcal{T}_2$ is a discrete open refinement of $F(\mathcal{T}_0,\ \mathcal{T}_1)$. By Lemma 3.2 $\{\overline{T} : T \in \mathcal{T}_2\}$ cannot cover O_2, whence $T_2 = O_2 \setminus \bigcup\{\overline{T} : T \in \mathcal{T}_2$ is a legal move for TWO of the game $\mathsf{MB}(Y, X)$. Then $O_3 = \sigma(T_0,\ T_1,\ T_2\}$ is a legal move for ONE in the Banach-Mazur game, and so on.

This outlines a definition of a strategy F for ONE in the strong screenabilty game. Corresponding to an F play we have a sequence

$$O_0 \supseteq T_0 \supseteq O_1 \supseteq T_1 \supseteq O_2 \supseteq T_2 \supseteq O_3 \supseteq \cdots$$

of nonempty open sets such that for each n the open set $\bigcup(\mathcal{T}_1 \cup \ldots \cup \mathcal{T}_n)$ is disjoint from O_{n+1}. Since σ is a winning strategy for ONE of the game $\mathsf{MB}(Y, X)$, $Y \cap (\bigcap_{n<\infty} O_n)$ is nonempty. Thus $\bigcup_{n<\infty} \mathcal{T}_n$ is not a cover of Y, and TWO looses F-plays of $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O}_Y)$. □

Corollary 3.4. *If X is a compact locally connected T_1-space, then ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O})$.*

Examples of compact locally connected spaces abound. A metrizable compact connected locally connected space is called a *Peano space*. The unit interval is an example of a Peano space. By the Hahn-Mazurkiewicz Theorem a T_2 space is a Peano space if, and only if, it is a continuous image of the closed unit interval.

Observe that if Y is a dense G_δ set in the space X, then ONE has a winning strategy in $\mathsf{MB}(X)$ if, and only if, ONE has a winning strategy in $\mathsf{MB}(Y, X)$.

Corollary 3.5. *Let Y be a dense G_δ subspace of the T_1-space X such that*

(1) *X has a π-base consisting of nontrivial connected sets, and*
(2) *ONE has a winning strategy in the game on $\mathsf{MB}(X)$.*

Then ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O}_Y)$ on X.

$\mathbb{P}$, the set of irrational numbers, is a dense G_δ subset of $\mathbb{R}$, the real line. Corollary 3.5 implies that ONE has a winning strategy in the game $\mathsf{G}^{\omega}_{d}(\mathcal{O}, \mathcal{O}_{\mathbb{P}})$ on the real line.

4. Player TWO

Lemma 4.1. *For a topological space X the following are equivalent:*

(1) *X is an ultraparacompact space.*
(2) *TWO has a winning strategy in the game $\mathsf{G}_d^1(\mathcal{O},\mathcal{O})$.*

With $\mathbb{S}$ the Sorgenfrey line, $\mathbb{S}\times\mathbb{S}$ is zero-dimensional and regular, but not normal, thus not paracompact, and thus by the Michael-Nagami Theorem, not strongly screenable. Thus, ONE has a winning strategy in the game $\mathsf{G}_d^\omega(\mathcal{O},\mathcal{O})$ on $\mathbb{S}\times\mathbb{S}$, while TWO has a winning strategy in $\mathsf{G}_d^1(\mathcal{O},\mathcal{O})$ on $\mathbb{S}$. In [18] P. Roy constructed a complete (non-separable) metric space X of cardinality $2^{\aleph_0}$ which is zero-dimensional, has Lebesgue covering dimension 1, and is not ultraparacompact. Roy's example is a complete zero-dimensional metric space for which TWO does not have a winning strategy in $\mathsf{G}_d^1(\mathcal{O},\mathcal{O})$ and thus not in $\mathsf{G}_d^\omega(\mathcal{O},\mathcal{O})$, as we shall see in Theorem 4.6.

Zerodimensional Lindelöf spaces are ultraparacompact. Thus,

Corollary 4.2. *For Lindelöf space X the following are equivalent:*

(1) *X is zero-dimensional.*
(2) *TWO has a winning strategy in $\mathsf{G}_d^1(\mathcal{O},\mathcal{O})$ on X.*

Balogh's space mentioned in Theorem 1.3 and constructed in [7] is a union of countably many open sets, each ultraparacompact. Thus TWO has a winning strategy in $\mathsf{G}_c^\omega(\mathcal{O},\mathcal{O})$. As this space is not strongly screenable ONE has a winning strategy in $\mathsf{G}_d^\alpha(\mathcal{O},\mathcal{O})$ for each countable ordinal α.

The existence of winning strategies for TWO in the relative version of the game seems more delicate. The following fact about extending open sets from a subspace to a containing space can be found in Theorem 3 on p. 227 of [12]. Observe that the metric spaces in Lemma 4.3 are *not* assumed to be separable.

Lemma 4.3. *Let X be a metric space and let Y be a subset of X. For each family $\{U_i : i\in I\}$ of subsets of Y open in the relative topology of Y there exists a family $\{V_i : i\in I\}$ of sets open in X such that*

(1) *For each $i\in I$ we have $U_i = Y\cap V_i$ and*
(2) *For every finite set $J\subseteq I$, if $\bigcap_{j\in J} U_j = \emptyset$, then $\bigcap_{j\in J}\overline{V}_j = \bigcap_{j\in J}\overline{U}_j$, where the closures are computed in X.*

Lemma 4.4. *Let X be a metric space and let Y be a closed, ultraparacompact subspace of X. Then TWO has a winning strategy in the game $\mathsf{G}_d^1(\mathcal{O},\mathcal{O}_Y)$.*

Proof. Let an open cover $\mathcal{U}$ of X be given. Since Y is an ultraparacompact space there is in the relative topology of Y a disjoint family $\{U_i : i \in I\}$ of open sets that refines $\mathcal{U}$ and covers Y. Being disjoint subsets of Y these relatively open sets are in fact closed in Y, and thus in X as Y is closed in X. By Lemma 4.3 we may choose for each i an open subset V_i of X such that $V_i \cap Y = U_i = \overline{U}_i$, such that when $i \neq j$ are elements of I, then $\overline{V}_i \cap \overline{V}_j = U_i \cap U_j = \emptyset$, and as each U_i is a subset of an element of the open cover $\mathcal{U}$ of X, also each V_i may be taken to be an open subset of that same element of $\mathcal{U}$. But then the refinement $\{V_i : i \in I\}$ of $\mathcal{U}$ is an element of $\mathcal{O}_Y$, and is a discrete family. □

Corollary 4.5. *Let X be a metric space and let Y be a subset of a σ-compact zero-dimensional subset of X. Then TWO has a winning strategy in $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$.*

Proof. Let $Y \subseteq C \subseteq X$ be given with C zerodimensional and σ-compact. Write $C = \bigcup_{n<\omega} C_n$ where each C_n is compact. By Lemma 4.4 fix for each n a winning strategy σ_n of TWO in the game $\mathsf{G}_d^1(\mathcal{O}, \mathcal{O}_{C_n})$. Then the strategy of responding to ONE's move in inning n using the strategy σ_n is winning for TWO in $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$. □

The example after Theorem 4.7 shows that game-length ω in Corollary 4.5 is optimal.

Theorem 4.6. *Let X be a metrizable space and let Y be a subspace of X. If TWO has a winning strategy in the game $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$ on X, then Y is a subset of a union of countably many closed, strongly zero-dimensional subsets of X.*

Proof. Let F be a winning strategy for TWO in the game $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$. Let d be a compatible metric for the topology of X, and for each positive integer n let $\mathcal{B}_n$ be the set

$$\{U \subset X : U \text{ open and } \mathsf{diam}_d(U) < \frac{1}{2^n}\}.$$

Define $C_\emptyset := \bigcap\{\overline{\bigcup F(\mathcal{B}_n)} : 0 < n < \omega\}$. And for each sequence $(n_1, \cdots, n_k)$ of positive integers, define $C_{n_1,\cdots,n_k} := \bigcap\{\overline{\bigcup F(\mathcal{B}_{n_1}, \cdots, \mathcal{B}_{n_k}, \mathcal{B}_m)} : 0 < m < \omega\}$.

We claim:

(a) Each $C_{n_1,\cdots,n_k}$, as well as $C_\emptyset$, is a closed, strongly zerodimensional set.
(b) $Y \subseteq \bigcup\{C_\tau : \tau \in {}^{<\omega}\omega\}$.

Towards proving (a): We give an argument for $C_{n_1,\cdots,n_k}$. The argument for $C_\emptyset$ is similar. Write C for $C_{n_1,\cdots,n_k}$. For each positive integer m the

discrete (in X) family $\mathcal{U}_m := \{C \cap \overline{U} : U \in F(\mathcal{B}_{n_1}, \cdots, \mathcal{B}_{n_k}, \mathcal{B}_m)\}$ is a cover of C and is a discrete family of sets clopen in C. It follows that $\bigcup\{\mathcal{U}_m : 0 < m < \omega\}$ is a σ-discrete base of C, consisting of sets clopen in the relative topology of C. By Theorem II.9 in [15], C has covering dimension 0, that is, C is strongly zero-dimensional.

Towards proving (b), suppose that on the contrary $x \in Y \setminus (\bigcup\{C_\tau : \tau \in^{<\omega} \omega\})$. As x is not an element of $C_\emptyset$, choose an n_1 such that x is not in $\overline{\bigcup F(\mathcal{B}_{n_1})}$. Then as x is not an element of C_{n_1}, choose an n_2 such that x is not in $\overline{\bigcup F(\mathcal{B}_{n_1}, \mathcal{B}_{n_2})}$, and so on. In this way we obtain an F-play of the game $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$ in which TWO lost since TWO did not cover $x \in Y$. This contradicts the hypothesis that F is a winning strategy for TWO. □

Note that the argument in the proof of Theorem 4.6 also gives:

Theorem 4.7. *Let X be a metric space and let Y be a subspace of X. If TWO has a winning strategy in $\mathsf{G}_d^1(\mathcal{O}, \mathcal{O}_Y)$, then Y is a subset of a closed, strongly zerodimensional subset of X.*

Proof. By the argument in the proof of Theorem 4.6, $Y \subseteq C_\emptyset$. □

Thus, for example, TWO has a winning strategy in the game $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_\mathbb{Q})$, but does not have a winning strategy in the game $\mathsf{G}_d^1(\mathcal{O}, \mathcal{O}_\mathbb{Q})$.

Corollary 4.8. *If X is a metrizable space, then the following are equivalent:*

(1) *TWO has a winning strategy in $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O})$.*
(2) *X is ultraparacompact.*
(3) *TWO has a winning strategy in $\mathsf{G}_d^1(\mathcal{O}, \mathcal{O})$.*

Proof. (1) ⇒ (2): By Theorem 4.6, X is a union of countably many closed sets, each strongly zerodimensional. By the countable sum theorem - see [15] Theorem II.2 A) - X is strongly zerodimensional. As X is metrizable the Katetov-Morita Theorem - see Theorem II.7 of [15] - implies that X has covering dimension zero. Thus, by Proposition 3.2.2 of [9], X is ultraparacompact.

(2) ⇒ (3): This implication is Lemma 4.4 since X is metrizable.

(3) ⇒ (1): This is left to the reader. □

Corollary 4.9. *Let Y be a subspace of the real line $\mathbb{R}$. Then the following are equivalent:*

(1) *TWO has a winning strategy in $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_Y)$.*
(2) *Y is a first category set of real numbers.*
(3) *TWO has a winning strategy in the game $\mathsf{MB}(Y, \mathbb{R})$.*

Proof. (1)⇒(2): Observe that a closed, zerodimensional set of real numbers is nowhere dense. Apply Theorem 4.6.

(2)⇒(1): As Y is a first category set of real numbers it is a subset of a union, say A, of countably many closed, nowhere dense sets. $\mathbb{R}$ is σ-compact, whence A is a union of countably many compact zerodimensional subsets of $\mathbb{R}$. Since A has empty interior it is zero-dimensional. Thus, Y is a subset of a σ-compact zero-dimensional subset of $\mathbb{R}$. Apply Corollary 4.5.

(2)⇔(3): This is a direct application of Theorem 1 of [16]. □

In [11] Kulesza constructs a complete, zerodimensional metric space K that is not ultraparacompact. Indeed, K has covering dimension 1. On p. 111 of [11] K is represented as $K = P_1 \cup \bigcup_{m\in\mathbb{N}} P_2^m$ where the subspace P_1 is homeomorphic to $D(\aleph_1)^\omega$ and each P_2^m is, by [11] Lemmas 3.3 and 3.4 and the remarks on [11], p. 113, a strongly zerodimensional closed (and nowhere dense) subset of the space K.

Corollary 4.10. *On the space K TWO does not have a winning strategy in $\mathsf{G}_d^\omega(\mathcal{O}, \mathcal{O}_{P_1})$.*

Proof. Suppose that, on the contrary, TWO has a winning strategy. By Theorem 4.6 P_1 is contained in a union of countably many closed, strongly zerodimensional subsets of K. But also each of the subspaces P_2^m is a closed, strongly zerodimensional subset of K. Thus, K is the union of countable many closed, strongly zerodimensional subsets. By Theorem 4.1.9 in [9] K has covering dimension 0, contradicting the fact that K has covering dimension larger than 0. □

5. Longer games

For any space (X, τ) there is an ordinal $\alpha \leq |X|$ such that TWO has a winning strategy in the game $\mathsf{G}_d^\alpha(\mathcal{O}, \mathcal{O})$ on X. Thus, we may define

$$\mathsf{tp}_d(X, \tau) = \min\{\alpha > 0 : \text{ TWO has a winning strategy in } \mathsf{G}_d^\alpha(\mathcal{O}, \mathcal{O})\}.$$

Let α be an infinite ordinal with Cantor normal form $\alpha = \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_m} \cdot n_m + n_{m+1}$ where $\beta_1 > \cdots > \beta_m > 0$ and $n_i < \omega$ for each $i \leq n + 1$. Define α^- as follows:

$$\alpha^- = \begin{cases} \alpha & \text{if } n_{m+1} = 0 \text{ and } \beta_m > 1 \\ \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_m} \cdot (n_m - 1) + 1 & \text{if } n_{m+1} = 0 \text{ and } \beta_m = 1 \\ \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_m} \cdot n_m + 1 & \text{otherwise.} \end{cases}$$

Corollary 5.1. *Let X be a metrizable space and let α be an infinite ordinal. If TWO has a winning strategy in $\mathsf{G}_d^{\alpha}(\mathcal{O},\mathcal{O})$ on X then TWO has a winning strategy in $\mathsf{G}_d^{\alpha^-}(\mathcal{O},\mathcal{O})$ on X.*

Proof. For consider a winning strategy σ of TWO. We need only consider ordinals α for which $\alpha > \alpha^-$.

Case 1: $n_{m+1} = 0$. We may assume that $\beta_m = 1$. After $\omega^{\beta_1}\cdot n_1 + \cdots + \omega^{\beta_m}\cdot(n_m - 1)$ innings TWO has covered a part, U, of the space X, and a closed set $C = X \setminus U$ remains to be covered. Using σ TWO has a winning strategy in the game $\mathsf{G}_d^{\omega}(\mathcal{O},\mathcal{O})$ on C. Now Theorem 4.7 implies that the closed set C is strongly zero-dimensional. Since X is metrizable, C is ultraparacompact. Thus, TWO has a winning strategy that wins $\mathsf{G}_d^{\alpha^-}(\mathcal{O},\mathcal{O})$ on X.

Case 2: $n_{m+1} > 0$. We may assume that $n_{m+1} > 1$. After $\omega^{\beta_1}\cdot n_1 + \cdots + \omega^{\beta_m}\cdot n_m$ innings TWO has covered a part, U, of the space X, and a closed set $C = X \setminus U$ remains to be covered. Using σ TWO has a winning strategy in the game $\mathsf{G}_d^{n_{m+1}}(\mathcal{O},\mathcal{O})$ on C. Now Theorem 4.7 implies that the closed set C is strongly zero-dimensional. As X is metrizable, C is ultraparacompact. Thus, TWO has a winning strategy that wins $\mathsf{G}_d^{\alpha^-}(\mathcal{O},\mathcal{O})$ on X. □

Since the unit interval is a Peano space, Corollary 3.4 implies that ONE has a winning strategy in the game $\mathsf{G}_d^{\omega}(\mathcal{O},\mathcal{O})$. We show that TWO has a winning strategy in $\mathsf{G}_d^{\omega+1}(\mathcal{O},\mathcal{O})$ on the unit interval. The key to the argument is Lebesgue's covering lemma:

Theorem 5.2 (Lebesgue)**.** *If (X,d) is a compact metric space then there is for each open cover $\mathcal{U}$ of X a positive real number δ such that for each set $Y \subset X$ for which the d-diameter is less than δ there is a set $U \in \mathcal{U}$ such that $Y \subseteq U$.*

Lemma 5.3. *Let $[a,\, b]$ be a closed interval of positive length L. Let $\mathcal{U}$ be a cover of $[a,\, b]$ by sets open in $[a,\, b]$. Then there is a finite discrete open refinement $\mathcal{V}$ of $\mathcal{U}$ such that $\bigcup\mathcal{V} \subset [a,\, b]$ and $[a,\, b] \setminus \bigcup\mathcal{V}$ is a union of finitely many disjoint closed intervals whose lengths add up to at most $\frac{L}{2}$.*

Proof. Using the Lebesgue covering lemma and the compactness of $[a,\, b]$, choose a positive real number δ as in Theorem 5.2. Then choose $\epsilon < \delta$ so that $M := \frac{L}{\epsilon}$ is an even integer. Choosing $a_0 = a$ and $a_{i+1} = a_i + \epsilon$ for $i < M$ we find that each of the intervals $[a_i,\, a_{i+1}]$, $0 \le i < M$ is a subset of an element of $\mathcal{U}$. Put $\mathcal{V} = \{(a_i,\, a_{i+1}) : i < M \text{ odd}\}$. Then $\mathcal{V}$ is as required. □

Theorem 5.4. *TWO has a winning strategy in* $\mathsf{G}_d^{\omega+1}(\mathcal{O},\mathcal{O})$ *on the closed unit interval.*

Proof. Player TWO's strategy in $\mathsf{G}_d^{\omega+1}(\mathcal{O},\mathcal{O})$ is as follows: In the first inning player TWO applies Lemma 5.3 to the open cover O_1 of $[0,\,1]$ played by ONE to obtain the open refinement $\mathcal{V}_1$ for which $[0,\,1]\setminus\bigcup\mathcal{V}_1$ is a union of finitely many closed disjoint intervals, $I_1^1,\cdots,I_{n_1}^1$ with lengths adding up to at most $\frac{1}{2}$.

When ONE plays the open cover O_2 next, TWO applies Lemma 5.3 to each I_j^1 to find a discrete open refinement $\mathcal{V}_{2,j}$ of O_2 with all elements subsets of I_j^1, and with $I_j^1\setminus\bigcup\mathcal{V}_{2,j}$ a union of finitely many disjoint closed subintervals of I_j^1 of positive length with lengths adding up to at most $\frac{length(I_j^1)}{2}$, and then TWO responds with $\mathcal{V}_2=\cup_{j\leq n_1}\mathcal{V}_{2,j}$. It follows that $[0,\,1]\setminus(\bigcup\mathcal{V}_1\cup\bigcup\mathcal{V}_2)$ is a union of finitely many closed, disjoint, intervals of positive length $I_1^2,\cdots,I_{n_2}^2$ with length adding up to at most $\frac{1}{4}$.

By applying this strategy to the next open covers chosen by ONE, we find that after countably many moves the set $[0,\,1]\setminus\bigcup\cup_{j=1}^{\infty}\mathcal{V}_j$ is compact and zero dimensional. Then by Lemma 4.4 TWO wins in one more inning. □

6. Remarks and Questions

Also for relative versions of the selective strong screenability game one could define the corresponding length ordinals: For a subspace Y of a topological space (X,τ), define

$\mathsf{tp}_d(X,Y,\tau)=\min\{\alpha\in\mathsf{ON}:$ TWO has a winning strategy in the game $\mathsf{G}_d^{\alpha}(\mathcal{O},\mathcal{O}_Y)\}$.

Thus, $\mathsf{tp}_d(X,\tau)=\mathsf{tp}_d(X,X,\tau)$.

Problem 1. *Is there a topological space* X *and a subspace* Y *for which* $\mathsf{tp}_d(X,Y,\tau)=2$*?*

Problem 2. *Is there a topological space* X *for which* $\mathsf{tp}_d(X,\tau)=2$*?*

There are complete metric spaces that are zero-dimensional but not ultraparacompact. See for example [11] and [18]. In these spaces TWO does not have a winning strategy in the game $\mathsf{G}_d^1(\mathcal{O},\mathcal{O})$. It is not clear whether more can be proven:

Problem 3. *If* X *is a complete metric space that is not ultraparacompact, does ONE have a winning strategy in the game* $\mathsf{G}_d^{\omega}(\mathcal{O},\mathcal{O})$ *on* X*?*

In connection with Theorem 3.3, it would be interesting to know:

Problem 4. *Let* Y *be a set of real numbers. Are the following statements equivalent?*

(1) *ONE has a winning strategy in the game* $\mathsf{MB}(Y, \mathbb{R})$.
(2) *ONE has a winning strategy in the game* $\mathsf{G}_d^{\omega}(\mathcal{O}, \mathcal{O}_Y)$

Our results on the closed unit interval and heuristic arguments suggest:

Conjecture 1. *For each positive integer* n *ONE has a winning strategy in* $\mathsf{G}_d^{\omega \cdot n}(\mathcal{O}, \mathcal{O})$*, and TWO has a winning strategy in* $\mathsf{G}_d^{\omega \cdot n+1}(\mathcal{O}, \mathcal{O})$ *on* $[0, 1]^n$.

Similarly to the ordinal $\mathsf{tp}_d(X, \tau)$ for a space (X, τ) one can define the ordinal $\mathsf{tp}_c(X, \tau)$ to be the least ordinal $\alpha > 0$ such that TWO has a winning strategy in the game $\mathsf{G}_c^{\alpha}(\mathcal{O}, \mathcal{O})$. This ordinal was introduced and studied in [3, 4, 5] as an alternative definition for covering dimension. The inequality $\mathsf{tp}_c(X, \tau) \leq \mathsf{tp}_d(X, \tau)$ holds for all topological spaces.

Now let $\mathcal{C}$ denote a class of topological spaces. If there is an ordinal α such that for each $(X, \tau) \in \mathcal{C}$ we have $\mathsf{tp}_c(X, \tau) \leq \alpha$, then we define $\mathsf{tp}_c(\mathcal{C})$ to be the supremum of the ordinals $\mathsf{tp}_c(X, \tau)$ where (X, τ) ranges over $\mathcal{C}$. The ordinal $\mathsf{tp}_d(\mathcal{C})$ is defined similarly, when it exists. We have that $\mathsf{tp}_c(\mathcal{C}) \leq \mathsf{tp}_d(\mathcal{C})$

Let $\mathcal{S}$ be the class of separable metrizable spaces. Since every separable metric space is a union of at most $\aleph_1$ zerodimensional subsets, for each separable metrizable space (X, τ), $\mathsf{tp}_c(X, \tau) \leq \omega_1$ and thus, $\mathsf{tp}_c(\mathcal{S}) \leq \omega_1$. The Hilbert cube $\mathbb{H}$ is strongly infinite dimensional, and thus $\mathsf{tp}_c(\mathbb{H}) = \omega_1$, meaning that for separable metrizable spaces the upper bound $\mathsf{tp}_c(\mathcal{S}) = \omega_1$ is sharp, *and* achieved.

Towards bounds on $\mathsf{tp}_d(\mathcal{S})$ we recall that $\mathsf{cov}(\mathcal{M})$ is the minimal cardinality of a family of first category subsets of the closed unit interval whose union is equal to the closed unit interval. One can show that $\mathsf{cov}(\mathcal{M})$ is also the least ordinal α such that each separable metrizable space is the union of at most α closed, zerodimensional subsets.

Theorem 6.1. *For the class* $\mathcal{S}$ *of separable metrizable spaces,* $\omega_1 \leq \mathsf{tp}_d(\mathcal{S}) \leq \mathsf{cov}(\mathcal{M})$.

Proof. We have $\omega_1 = \mathsf{tp}_c(\mathcal{S}) \leq \mathsf{tp}_d(\mathcal{S})$. A zerodimensional subset Y of separable metrizable space (X, τ) is ultraparacompact; if it is also closed, then TWO has a winning strategy in the game $\mathsf{G}_d^1(\mathcal{O}, \mathcal{O}_Y)$. Thus, if (X, τ) can be written as a union of κ closed, zerodimensional subsets, then $\mathsf{tp_d}(\mathsf{X}, \tau) \leq \kappa$. □

We suspect that the upper bound of $\mathsf{cov}(\mathcal{M})$ in Theorem 6.1 can be significantly improved. Assuming the Continuum Hypothesis, $\mathsf{tp}_d(\mathcal{S}) = \omega_1$. And as we have shown in Theorem 5.4, TWO has a winning strategy in $\mathsf{G}_d^{\omega+1}(\mathcal{O}, \mathcal{O})$ on the closed unit interval.

Problem 5. *Is it true that* $\mathsf{tp}_d(X, \tau) \leq \omega_1$ *for each separable metrizable space* (X, τ)*?*

7. Acknowledgements

We thank Roman Pol and Rodrigo Dias for very informative communications that improved the contents of this paper. We also thank a very careful referee for feedback that further improved our paper.

References

[1] D. F. Addis and J.H. Gresham, *A class of infinite-dimensional spaces. Part I: Dimension theory and Alexandroff's problem*, Fundamenta Mathematicae **101:3** (1978), 195–205.

[2] L. Babinkostova, *Selection Principles in Topology* (Macedonian), Ph.D. thesis. University of St. Cyril and Methodius, Macedonia, 2001.

[3] L. Babinkostova, *Selective screenability game and covreing dimension*, Topology Proceedings **29:1** (2005), 13–17

[4] L. Babinkostova, *Topological games and covering dimension*, Topology Proceedings **38** (2011), 99–120.

[5] L. Babinkostova, *Topological groups and covering dimension*, Topology and its Applications **158:12** (2011), 1460–1470.

[6] L. Babinkostova, Lj.D.R. Kočinac and M. Scheepers, *Notes on selection principles in topology (I): Paracompactness*, Journal of the Korean Mathematical Society **42:4** (2005), 709–721.

[7] Z. Balogh, *A normal, screenable, nonparacompact space in ZFC*, Proceedings of the American Mathematical Society **126:6** (1998), 1835–1844.

[8] R.H. Bing, *Metrization of topological spaces*, Canadian Journal of Mathematics **3** (1951), 175–186.

[9] R. Engelking, *Dimension Theory*, North-Holland Publishing Company (1978).

[10] F. Galvin and R. Telgarsky, *Stationary strategies in topological games*, Topology and its Applications **22** (1986), 51–69.

[11] J. Kulesza, *An example in the dimension theory of metrizable spaces*, Topology and its Applications **35** (1990), 109–120.

[12] C. Kuratowski, *Topology* Vol. I, Academic Press 1966.

[13] E. Michael, *A note on paracompact spaces*, Proceedings of the American Mathematical Society **4** (1953), 831–838.

[14] K. Nagami, *Paracompactness and Strong Screenability*, Nagoya Mathematics Journal, **8** (1955), 83–88.

[15] J. Nagata, *Modern Dimension Theory*, Biblioteca Mathematica (VI), **John Wiley & Sons Inc**, 1965.

[16] J.C. Oxtoby, *The Banach-Mazur game and Banach category theorem*, in Contributions to the Theory of Games, Volume 3, Princeton University Press (1957), 159– 164.

[17] R. Pol, *A weakly infinite-dimensional compactum which is not countable-dimensional*, Proceedings of the American Mathematical Society **82:4** (1981), 634–636.

[18] P. Roy, *Nonequality of dimensions for metric spaces*, Transactions of the American Mathematical Society **134:1** (1968), 117–132.

Department of Mathematics; Boise State University; Boise, Idaho 83725
E-mail address: liljanababinkostova@boisestate.edu
E-mail address: mscheepe@boisestate.edu