CURRICULUM VITAE FOR BOAZ TSABAN

Research interests.

Pure mathematics. In general and set theoretic topology, I study *selection principles*: selective covering and local properties, via infinite-combinatorial methods, with applications to real analysis (extraordnary sets of real numbers; function spaces) and Ramsey theory of open covers. I also worked extensively on applications of infinite-combinatorial methods in Pontryagin–van Kampen duality of topological groups.

Computational mathematics. In mathematical cryptology, I study computational questions that form the basis of nonabelian cryptology; especially group-theory based public key protocols.

Education.

PhD. Infinite Combinatorial Topology, Department of Mathematics, Bar-Ilan University, 2003, with highest distinction. Supervisor: Hillel Furstenberg.

MSc. Special classes of strongly null sets: A journey into the continuum, Department of Mathematics, Bar-Ilan University, 1997, with highest distinction. Supervisors: Martin Goldstern and Hillel Furstenberg.

BSc. Mathematics Extended, Department of Mathematics, Bar-Ilan University, 1994, with highest distinction.

Employment.

4/2012–present. Associate Professor, Department of Mathematics, Bar-Ilan University.

10/2013–9/2014. Sabbatical leave, Faculty of Mathematics and Computer Science, Weizmann Institute of Science.

10/2007–3/2012. Senior Lecturer, Department of Mathematics, Bar-Ilan University.

10/2007–9/2009. Consultant, Faculty of Mathematics and Computer Science, Weizmann Institute of Science.

10/2004–9/2007. Koshland Fellow, Faculty of Mathematics and Computer Science, Weizmann Institute of Science.

10/2002–9/2004. Post-doctoral student, Einstein Institute of Mathematics, Hebrew University of Jerusalem.

Date: October 15, 2018.

Research grants. Details and sums available at the enclosed Research Authority page.

(1) Council for Higher Education, PBC Fellowship for Outstanding Chinese and Indian Post-doctoral Fellows, *Selection Principles and Combinatorial Cardinal Characteristics of the Continuum*, 2018 and 2019. Support for a post-doctoral student.
(2) BIU Center for Research in Applied Cryptography and Cyber Security, *Algebraic lightweight cryptography*, 2016–2018.
(3) Ministry of Defense, *Group theory based homomorphic encryption*, 2015–2016.
(4) Cyber Defense and Advanced Computing grant, Ministry of Science and Technology, Israel, 2014.
(5) Ministry of Science and Technology, Women in Science. (Support for a PhD student.)
(6) Ministry of Defense, *Hard problems in infinite groups*, 2012, 2013.
(7) United States–Israel Binational Science Foundation (BSF), Prof. Rahamimoff Grant, 2011 and 2013.
(8) Rector and Vice President for Research Grants for Excellence in Scientific Research 2008, 2009, 2010, 2011, 2012, 2015.

Awards.

Tenure track: Wolf Foundation's *Krill Prize* for Excellence in Scientific Research, 2009.
Post-Doctoral: Golda Meir; Edmund Landau; Minerva (short-term research visit); Koshland fellowship.
PhD: *Nessyahu Prize* for the best doctoral dissertation in mathematics in Israel, in the year 2003 (shared with Irit Dinur); BIU President Scholarship; Wolf Foundation; Sam Cohen; Rachel Jacobs.
MSc: Moris Banin Prize.
BSc: Israel Knesset; Rachel and Reuben Jacobs; David Ben Gurion (Ministry of Science); Salim and Rachel Banin; Wolf Foundation.

Lectures in Conferences and Workshops.

Invited Lectures.

(1) Coverings, selections, and games in topology, University of Lecce, Italy, 2002.
(2) Foundations of the Formal Sciences V: Infinite Games, University of Bonn, Germany, 2004.
(3) Algebraic Methods in Cryptography, Ruhr Universität Bochum, Germany, 2005.
(4) Coverings, selections, and games in topology, II, University of Lecce, Italy, 2005.
(5) Boise Workshop on Selection Principles in Mathematics, Boise State University, Idaho, USA, 2006.
(6) Geometric and Asymptotic Group Theory with Applications, Universitat Politècnica de Catalunya, Barcelona, Spain, 2006.
(7) Workshop on Set Theory and its Applications, Weizmann Institute of Science, Israel, 2007.
(8) III-rd Workshop on Coverings, Selections, and Games in Topology, Vrnjacka Banja, Serbia, 2007.
(9) Combinatorial and Geometric Group Theory with Applications, University of Dortmund, Germany, 2007.
(10) 44th annual Spring Topology and Dynamics Conference, Mississippi State University, Mississippi State, USA, 2010.

(11) Annual Israel Mathematical Union meeting, Weizmann Institute of Science, Israel, 2010.
(12) International Functional Analysis Meeting in Valencia, University of Valencia, Valencia, Spain, 2010.
(13) Algebra Meets Topology: Advances and Applications, Universitat Politècnica de Catalunya, Barcelona, Spain, 2010.
(14) Workshop on Complexity and Group-based Cryptography, Centre de Recherches Mathématiques, Université de Montréal, Canada, 2010.
(15) Topology Day, University of Messina, Messina, Italy, 2012: *Diagonalizations of dense families*. Plenary lecture.
(16) IV Workshop on Coverings, Selections, and Games in Topology, Seconda Universitá di Napoli, Caserta, Italy, 2012: *Coherent omission of intervals: A method for constructing special sets of reals and associated topological spaces*. Plenary lecture.
(17) Geometric and Combinatorial Group Theory, Heinrich Heine Universität Düsseldorf, Germany, 2012:
   (a) *The Conjugacy Problem: cryptoanalytic approaches to a problem of Dehn*. Invited minicourse for all participants.
   (b) *Finite invariants for the multiple conjugacy problem in Garside groups*. Invited lecture.
(18) Symbolic Computations and Post-Quantum Cryptography, Stevens Institute of Technology, USA, 2012: *Polynomial time cryptanalysis of the Commutator Key Exchange Protocol and related protocols*. Invited lecture.
(19) Interactions between Logic, Topological structures and Banach spaces theory, Ben Gurion University of the Negev, Israel, 2013: *Coherent omission of intervals*. Invited lecture.
(20) Summer Undergraduate Research in Complexity in Algebra, Geometry and Applications, Boise, Idaho, USA, 2013: *Nonabelian cryptography*. Invited lecture.
(21) 13th Serbian Mathematical Congress, Vrnjačka Banja, Serbia, 2014: *Pontryagin–van Kampen duality and PCF theory*. Invited lecture.
(22) Analysis, Topology and Applications, Vrnjačka Banja, Serbia, 2014: *Product spaces, through the lens of selection theory*. Invited lecture.
(23) Second Joint International Meeting of the American Mathematical Society and the Israel Mathematical Union, Ramat Gan and Tel Aviv, Israel, 2014: *Polynomial time solutions of the main problems of noncommutative algebraic cryptography*. Invited lecture.
(24) International Conference on Topology, Messina, Italy, 2015: *Algebra, selections, and additive Ramsey theory*. Plenary lecture.
(25) Compactness, Incompactness and Canonical Structures, Israel Institute for Advanced Studies, Jerusalem, 2015: *Applications of PCF theory and forcing theory to free topological groups*. Plenary lecture.
(26) Galway Topology Colloquium, Leicester, UK, 2016: *Wide selection!* Invited lecture.
(27) 31st Summer Conference on Topology and its Applications, Leicester, UK, 2016: *On the existence of real Fréchet–Urysohn function spaces*. Plenary lecture.
(28) Workshop on Selection Principles, Chengdu, China, 2016: *Omission of intervals*. Invited minicourse for all participants.

(29) Workshop on Secure Implementation of Post-Quantum Cryptography, Tel Aviv, 2016: *Nonabelian cryptography* Invited lecture.
(30) Frontiers of Selection Principles, Warsaw, 2017: *An introduction to omission of intervals*. Plenary lecture.
(31) Set Theory, Model Theory and Applications, Eilat, 2018: *On the Haar measure problem*. Invited lecture.
(32) Summer Conference on Topology and its Applications, Bowling Green, USA, 2018: *A complete classification of the cofinal structure of precompacta in metric spaces*. Invited lecture.
(33) CRYPTO, Santa Barbara, USA, 2018: *Cryptanalysis via algebraic spans*. Invited lecture.
(34) Workshop on Cryptography and Network Security, Kanpur, 2018: *TBD*. Invited lecture.
(35) European Set Theory Conference, Vienna, Austria, 2019. *Selection principles in set theory*. Invited lecture.
(36) Geometric and Asymptotic Group Theory with Applications, Ramat Gan, Israel, 2019: *Foundations of nonabelian cryptanalysis*. Plenary lecture.

Contributed lectures (until 2008). *BGU symposium in mathematics*, Ben Gurion University, Israel, 2001; *Israel Mathematical Union 2003 meeting*, Zichron Yaakov, Israel, 2003; *The Barcelona Conference on Set Theory*, Centre de Recerca Matematica, Barcelona, Spain, 2003; *Israel Mathematical Union 2005 meeting*, Neve Ilan, Israel, 2005; *Boise Extravaganza in Set Theory*, Boise State University, Idaho, USA, 2006; *10th Prague topological symposium*, Prague, Czech Republic, 2006; *International Conference on Set-theoretic Topology*, University of Kielce, Poland, 2006; *Ultramath 2008*, University of Pisa, Italy, 2008; *Compression and Combinatorial Algorithms (CCA) 2008*, CRI, University of Haifa, and Ashkelon Academic College, Haifa, 2008.

Other lectures. Colloquia and research seminars in Israel and abroad (number of talks indicated): Bar-Ilan University (> 10); Ben Guryon University (1); Hebrew University (8); Technion (1); Haifa University (2); Tel Aviv University (1); Holon Institute of Technology (1); Weizmann Institute of Science (8); Warsaw University (3); Katowice University (1); Wrocław University (1); Bonn University (2); University of Kragujevac (1); University Jaume I (2); Kurt Gödel Research Center (2).

Students. Graduation date indicated.

MSc.

(1) (Informally) Dima Ruinskiy, 2007. Joint supervision with Adi Shamir.
(2) Nadav Samet, 2008. Joint supervision with Gideon Schechtman.
(3) Tal Orenstein, 2009. Joint supervision with Gady Kozma.
(4) Tatyana Kovalyova, 2010.
(5) Gili Goloan, 2011.
(6) Gary Vinokur, 2012. Joint supervision with David Garber.
(7) Matan Banin, 2014.
(8) Achiya Bar-On, 2015. Joint supervision with Nathan Keller. Awards: Cyber Defense and Advanced Computing grant, Ministry of Science and Technology; Check Point Institute for Information Security grant.

(9) Efrat Taub, 2015. Joint supervision with Adi Jarden.
(10) Adi Ben Zvi , 2015.
(11) Ayelet Amsalem, 2017. Joint supervision with Adi Jarden.
(12) Itay Bookstein, 2018.
(13) Asaf Cohen, present.
(14) Idan Sulami, present.

PhD.

(1) Adi Jarden, 2012. Awards: Prof. Rahamimoff Travel Grant of the U.S.–Israel Binational Science Foundation (BSF). Adi accepted a tenure-track position at Ariel University.
(2) Gili Golan, 2015. Joint supervision with Mark Sapir. Awards: Women in Science, Israel Ministry of Science and Technology, 2012; Prof. Rahamimoff Travel Grant of the U.S.–Israel Binational Science Foundation (BSF); Wolf Foundation grant for PhD students; Fulbright Israeli Post-doctoral Scholar Fellowship. Finishing her post-doctoral studies at Vanderbilt, Gili accepted a tenure-track position at Ben-Gurion University.
(3) Adi Ben-Zvi, present. Awards: Check Point Institute for Information Security grant.

Post-doctoral.

(1) Michał Machura, 10/2004–9/2005 (informally). Joint supervision with Boris Kunyavski.
(2) Lyubomyr Zdomskyy, 10/2006–9/2007 (informally). Joint supervision with Gideon Schechtman.
(3) Arkadius Kalka, 10/2007–12/2011 and 5/2013–9/2015. Joint supervision with Mina Teicher.
(4) Piotr Szewczak, 1–6/2015; 2/1016–1/2017.
(5) Jialiang He, 10/2018–9/2020.

Publications. Links available at: `math.biu.ac.il/~tsaban/papers.html`
Citations available at: `math.biu.ac.il/~tsaban/citing.html`

Pure Mathematics.

(1) *A topological interpretation of* $\mathfrak{t}$, **Real Analysis Exchange** 25 (1999/2000), 391–404.
(2) *A diagonalization property between Hurewicz and Menger*, **Real Analysis Exchange** 27 (2001/2002), 757–763.
(3) *The combinatorics of Borel covers* (with M. Scheepers), **Topology and its Applications** 121 (2002), 357–382.
(4) *Additivity properties of topological diagonalizations* (with T. Bartoszyński and S. Shelah), **Journal of Symbolic Logic** 68 (2003), 1254–1260.
(5) *Critical cardinalities and additivity properties of combinatorial notions of smallness* (with S. Shelah), **Journal of Applied Analysis** 9 (2003), 149–162.
(6) *Selection principles and the minimal tower problem*, **Note di Matematica** 22 (2003), 53–81.
(7) *Topological diagonalizations and Hausdorff dimension* (with T. Weiss), **Note di Matematica** 22 (2003), 83–92.

(8) *Selection principles in Mathematics: A milestone of open problems*, **Note di Matematica** 22 (2003), 179–208.
(9) *The minimal cardinality where the Reznichenko property fails*, **Israel Journal of Mathematics** 140 (2004), 367–374.
(10) *The Hurewicz covering property and slaloms in the Baire space*, **Fundamenta Mathematicae** 181 (2004), 273–280.
(11) *The combinatorics of splittability*, **Annals of Pure and Applied Logic** 129 (2004), 107–130.
(12) *Products of special sets of real numbers* (with T. Weiss), **Real Analysis Exchange** 30 (2004/5), 819–836.
(13) *Strong γ-sets and other singular spaces*, **Topology and its Applications** 153 (2005), 620–639.
(14) *Hereditary topological diagonalizations and the Menger–Hurewicz Conjectures* (with T. Bartoszyński), **Proceedings of the American Mathematical Society** 134 (2006), 605–615.
(15) *o-bounded groups and other topological groups with strong combinatorial properties*, **Proceedings of the American Mathematical Society** 134 (2006), 881–891.
(16) *Covering the Baire space by families which are not finitely dominating* (with H. Mildenberger and S. Shelah), **Annals of Pure and Applied Logic** 140 (2006), 60–71.
(17) *Menger's covering property and groupwise density* (with L. Zdomskyy), **Journal of Symbolic Logic** 71 (2006), 1053–1056.
(18) *Some new directions in infinite-combinatorial topology*, in: **Set Theory** (J. Bagaria and S. Todorčevic, eds.), Trends in Mathematics, Birkhäuser 2006, 225–255.
(19) *Additivity numbers of covering properties*, in: **Selection Principles and Covering Properties in Topology** (L. Kočinac, ed.), Quaderni di Matematica 18, Seconda Universita di Napoli, Caserta 2006, 245–282.
(20) *The combinatorics of τ-covers* (with H. Mildenberger and S. Shelah), **Topology and its Applications** 154 (2007), 263–276.
(21) *Selection Principles and special sets of reals*, in: **Open Problems in Topology II** (E. Pearl ed.), Elsevier B.V. 2007, 91–108.
(22) *On the Kočinac α_i properties*, **Topology and its Applications** 155 (2007), 141–145.
(23) *A new selection principle*, **Topology Proceedings** 31 (2007), 319–329.
(24) *On the Pytkeev property in spaces of continuous functions* (with P. Simon), **Proceedings of the American Mathematical Society** 136 (2008), 1125–1135.
(25) *Several comments about the combinatorics of τ-covers*, **Note di Matematica** 27 (2007), 47–53.
(26) *Scales, fields, and a problem of Hurewicz* (with L. Zdomskyy), **Journal of the European Mathematical Society** 10 (2008), 837–866.
(27) *The combinatorics of the Baer–Specker group* (with M. Machura), **Israel Journal of Mathematics** 168 (2008), 125–151.
(28) *Hurewicz sets of reals without perfect subsets* (with D. Repovš and L. Zdomskyy), **Proceedings of the American Mathematical Society** 136 (2008), 2515–2520.
(29) *Combinatorial images of sets of reals and semifilter trichotomy* (with L. Zdomskyy), **Journal of Symbolic Logic** 73 (2008), 1278–1288.

(30) *Continuous selections and σ-spaces* (with D. Repovš and L. Zdomskyy), **Topology and its Applications** 156 (2008), 104–109.
(31) *Null sets and games in Banach spaces* (with J. Duda), **Topology and its Applications** 156 (2008), 56–60.
(32) *Partition relations for Hurewicz-type selection hypotheses* (with N. Samet and M. Scheepers), **Topology and its Applications** 156 (2009), 616–623.
(33) *Superfilters, Ramsey theory, and van der Waerden's Theorem* (with N. Samet), **Topology and its Applications** 156 (2009), 2659–2669.
(34) *On the Pytkeev property in spaces of continuous functions (II)* (with L. Zdomskyy), **Houston Journal of Mathematics** 35 (2009), 563–571.
(35) *Squares of Menger-bounded groups* (with M. Machura and S. Shelah), **Transactions of the American Mathematical Society** 362 (2010), 1751–1764.
(36) *On a problem of Juhász and van Mill* (with S. Shelah), **Topology Proceedings** 36 (2010), 385–392.
(37) *Point-cofinite covers in Laver's model* (with A. Miller), **Proceedings of the American Mathematical Society** 138 (2010), 3313–3321.
(38) *Sequential properties of function spaces with the compact-open topology* (with Gary Gruenhage and L. Zdomskyy), **Topology and its Applications** 158 (2011), 387–391.
(39) *Menger's and Hurewicz's Problems: Solutions from "The Book" and refinements*, **Contemporary Mathematics** 533 (2011), 211–226.
(40) *Linear σ-additivity and some applications* (with T. Orenshtein), **Transactions of the American Mathematical Society** 363 (2011), 3621–3637.
(41) *On productively Lindelöf spaces* (with F. Tall), **Topology and its Applications** 158 (2011), 1239–1248.
(42) *Hereditarily Hurewicz spaces and Arhangel'skiĭ sheaf amalgamations* (with L. Zdomskyy), **Journal of the European Mathematical Society** 12 (2012), 353–372.
(43) *Pointwise convergence of partial functions: The Gerlits–Nagy Problem* (with T. Orenshtein), **Advances in Mathematics** 232 (2013), 311–326.
(44) *Hindman's Coloring Theorem in arbitrary semigroups* (with G. Golan), **Journal of Algebra** 395 (2013), 111–120.
(45) *On the cardinality of the θ-closed hull of sets* (with F. Cammaroto, A. Catalioto, B. Pansera), **Topology and its Applications** 160 (2013), 2371–2378.
(46) *Selective covering properties of product spaces* (with A. Miller, L. Zdomskyy), **Annals of Pure and Applied Logic** 165 (2014), 1034–1057.
(47) *Diagonalizations of dense families* (with M. Bonanzinga, F. Cammaroto, B. Pansera), **Topology and its Applications** 165 (2014), 12–25.
(48) *Additivity of the Gerlits–Nagy property and concentrated sets* (with L. Zdomskyy), **Proceedings of the American Mathematical Society** 142 (2014), 2881–2890.
(49) *The character of topological groups, via bounded systems, Pontryagin–van Kampen duality and pcf theory* (with C. Chis, M. V. Ferrer, S. Hernández), **Journal of Algebra** 420 (2014), 86–119.
(50) *Combinatorial aspects of selective star covering properties in Ψ-spaces*, **Topology and its Applications** 192 (2015), 198–207.
(51) *Arhangel'skiĭ sheaf amalgamations in topological groups* (with L. Zdomskyy), **Fundamenta Mathematicae** 232 (2016), 281–293.

(52) *Selective covering properties of product spaces, II: γ spaces* (with A. Miller, L. Zdomskyy), **Transactions of the American Mathematical Society** 368 (2016), 2865–2889.

(53) *The linear refinement number and selection theory* (with M. Machura, S. Shelah), **Fundamenta Mathematicae** 234 (2016), 15–40.

(54) *Products of Menger spaces: A combinatorial approach* (with P. Szewczak), **Annals of Pure and Applied Logic** 168 (2017), 1–18.

(55) *Algebra, selections, and additive Ramsey theory*, **Fundamenta Mathematicae** 240 (2018), 81–104.

(56) *The Haar Measure Problem* (with P. Szewczak, A. Przeździecki), **Proceedings of the American Mathematical Society**, to appear, 8 pages.

(57) *Products of general Menger spaces* (with P. Szewczak), submitted for publication, 14 pages.

(58) *A classification of the cofinal structures of precompacta* (with A. Eshed, M. Ferrer, S. Hernández, P. Szewczak), submitted for publication, 17 pages.

Computational mathematics.

(59) *Guaranteeing the diversity of number generators* (with A. Shamir), **Information and Computation** 171 (2001), 350–363.

(60) *Efficient linear feedback shift registers with maximal period* (with U. Vishne), **Finite Fields and their Applications** 8 (2002), 256–267.

(61) *Bernoulli numbers and the probability of a birthday surprise*, **Discrete Applied Mathematics** 127 (2003), 657–663.

(62) *Permutation graphs fast forward permutations and sampling the cycle structure of a permutation*, **Journal of Algorithms** 47 (2003), 104–121.

(63) *The conjugacy problem and related problems in lattice-ordered groups* (with W.C. Holland), **International Journal of Algebra and Computation** 15 (2005), 395–404.

(64) *Probabilistic solutions of equations in the braid group* (with D. Garber, S. Kaplan, M. Teicher, U. Vishne), **Advances in Applied Mathematics** 35 (2005), 323–334.

(65) *Fast generators for the Diffie–Hellman key agreement protocol and malicious standards*, **Information Processing Letters** 99 (2006), 145–148.

(66) *Length-based conjugacy search in the Braid group* (with D. Garber, S. Kaplan, M. Teicher, U. Vishne), **Contemporary Mathematics** 418 (2006), 75–87.

(67) *Decompositions of graphs of functions and efficient iterations of lookup tables*, **Discrete Applied Mathematics** 155 (2007), 386–393.

(68) *Cryptanalysis of group-based key agreement protocols using subgroup distance functions* (with D. Ruinskiy and A. Shamir), **PKC07, Lecture Notes In Computer Science** 4450 (2007), 61–75.

(69) *Theoretical cryptanalysis of the Klimov–Shamir number generator TF-1*, **Journal of Cryptology** 20 (2007), 389–392.

(70) *Length-based cryptanalysis: The case of Thompson's Group* (with D. Ruinskiy and A. Shamir), **Journal of Mathematical Cryptology** 1 (2007), 359–372.

(71) *Random strategies with memory for the Robin Hood game*, in: **Foundations of the Formal Sciences V: Infinite Games** (S. Bold, B. Löwe, T. Räsch, J. van Benthem, eds.), Studies in Logic 11, College Publications, London 2007, 271–278.

(72) *Solving random equations in Garside groups using length functions* (with M. Hock), in: **Combinatorial and Geometric Group Theory** (O. Bogopolski, I. Bumagin, O. Kharlampovich, E. Ventura), Trends in Mathematics, Birkhäuser 2010, 149–169.

(73) *The Discrete Logarithm Problem in Bergman's non-representable ring* (with M. Banin), **Journal of Mathematical Cryptology** 6 (2012), 171–182.

(74) *Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser* (with A. Kalka, M. Teicher), **Advances in Applied Mathematics** 49 (2012), 57–76.

(75) *Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme* (with N. Lifshitz), **Journal of Mathematical Cryptology** 9 (2015), 75–78.

(76) *Cryptanalysis of SP networks with partial non-linear layers* (with A. Bar-On, I. Dinur, O. Dunkelman, N. Keller, V. Lallemand), **EUROCRYPT 2015, Lecture Notes in Computer Science** 9056 (2015), 315–342.

(77) *Polynomial-time solutions of computational problems in noncommutative algebraic cryptography*, **Journal of Cryptology** 28 (2015), 601–622.

(78) SL_2 *homomorphic hash functions: Worst case to average case reduction and short collision search* (with C. Mullan), **Designs Codes and Cryptography** 81 (2016), 83–107.

(79) *A reduction of Semigroup DLP to classic DLP* (with M. Banin), **Designs Codes and Cryptography** 81 (2016), 75–82.

(80) *A Practical Cryptanalysis of the Algebraic Eraser* (with A. Ben Zvi, S. Blackburn), **CRYPTO 2016 – Lecture Notes in Computer Science** 9814 (2016), 179–189.

(81) *Cryptanalysis via algebraic spans* (with A. Ben-Zvi, A. Kalka), **CRYPTO 2018 – Lecture Notes in Computer Science** 10991 (2018), 255–274.

(82) *A complete simultaneous conjugacy invariant in Garside groups* (with A. Kalka, G. Vinokur), submitted for publication, 22 pages.

Recreational mathematics and history of mathematics.

(83) *On the Rabbinical approximation of* π (with D. Garber), **Historia Mathematica** 25 (1998), 75–84.

(84) *A mechanical derivation of the area of a sphere* (with D. Garber), **American Mathematical Monthly** 108 (2001), 10–15.

(85) *The* $\mathcal{SPM}$ *Bulletin*, **Note di Matematica** 27 (2007), 111–117.

(86) *The mathematics of Ljubiša D.R. Kočinac*, **Topology and its Applications** 160 (2013), 2234–2242.

Book editorship.

(87) L. Babinkostova, C. Guido, L. Kočinac, M. Scheepers, B. Tsaban, eds., **Proceedings of the Second Workshop on Coverings, Selections and Games in Topology**, Note di Matematica 27, suppl. 1 (2007), 117 pp.

(88) G. Di Maio, B. Tsaban, eds., **Fourth Workshop on Coverings, Selections and Games in Topology**, on the occasion of Ljubiša D.R. Kočinac's 65th birthday, Topology and its Applications 160 (2013), 334 pp.

(89) A. Bella, M. Bonanzinga, B. Tsaban, eds., **International Conference on Topology**, on the occasion of Filippo Cammaroto's 65th birthday, Topology and its Applications 224 (2017), 82 pp.

(90) P. Szweczak, B. Tsaban, L. Zdomskyy, eds., **Frontiers of Selection Principles**, on the occasion of Marion Scheepers's 60th birthday, Topology and its Applications, to appear.

Published pages (calculated by LaTeX). 1174 pages in published papers: 858 in pure mathematics; 316 in computational mathematics.

Teaching. Courses, mini-courses, and seminars from first year BSc up to PhD level, in universities (Bar-Ilan University, Hebrew University, Weizmann Institute of Science) and colleges (Jerusalem College of Technology); academic courses for gifted high-school students; advanced courses, including: Set theory (Bar-Ilan University, Weizmann Institute of Science), fractal theory, forcing theory, infinite-combinatorial topology, combinatorial number theory (Bar-Ilan University, Weizmann Institute of Science).

Teaching evaluations. Always above the course average (including service courses). Almost always above the departmental average in departmental courses. Typically, among the highest in the department.

Travel to research institutes. Austria, Canada, China, Czech Republic, Germany, Italy, Poland, Serbia, Spain, United Kingdom, USA. Details in Appendix A.

Conferences and workshops committees.

Membership in scientific committees.

(1) *Coverings, Selections, and Games in Topology II*, Lecce, Italy, December 2005.
(2) *Coverings, Selections, and Games in Topology III*, Vrnjacka Banja, Serbia, 2007.
(3) *First International Conference on Symbolic Computation and Cryptography*, Beijing, China, 2008.
(4) *Second International Conference on Symbolic Computation and Cryptography*, Egham, UK, 2010.
(5) *Coverings, Selections, and Games in Topology IV*, Caserta, Italy, 2012. (Scientific and organizing committees.)
(6) *Third International Conference on Symbolic Computation and Cryptography*, Castro Urdiales, Spain, 2012.
(7) *13th Serbian Mathematical Congress*, Vrnjačka Banja, Serbia, 2014.
(8) *Analysis, Topology and Applications*, Vrnjačka Banja, Serbia, 2014.
(9) *International Conference on Topology*, Messina, Italy, 2015.
(10) *Frontiers of Selection Principles*, Warsaw, Poland, 2017.

Membership in organizing committees.

(1) *Coverings, Selections, and Games in Topology IV*, Caserta, Italy, 2012. (Scientific and organizing committees.)
(2) *Geometric and Combinatorial Group Theory with Applications*, Düsseldorf, Germany, 2012.
(3) *International Conference on Topology*, Messina, Italy, 2015. (Scientific and organizing committees.)
(4) *Frontiers of Selection Principles*, Warsaw, Poland, 2017. (Scientific and organizing committees.)

Organizer.

(1) *Workshop on Set Theory and its Applications*, Weizmann Institute of Science, Israel, 2007.
(2) *Israel Mathematical Union special session on Set Theory and its Applications*, Israel, 2009.

Additional professional occupations

Departmental teaching committee. 2008–present. Took part in a major departmental curriculum revision.

Co-organization of research seminars. Weizmann Institute's *Geometric Functional Analysis and Probability* seminar, 2005–2007; Bar-Ilan University *Combinatorial Group theory and Cryptography* seminar, 10/2007–6/2013; Bar-Ilan University *Infinite combinatorics* seminar, 2015.

Journal refereeing. The number of refereed papers, when greater than 1, is indicated. The journals are sorted by number of reports completed, and then by name.

Pure mathematics.

(1) Topology and its Applications (14).
(2) Matematicki Vesnik (4).
(3) Colloquim Mathematicum (2).
(4) Contemporary Mathematics (2).
(5) European Journal of Mathematics (2).
(6) Note di Matematica (2).
(7) Proceedings of the American Mathematical Society (2).
(8) Quaestiones Mathematicae (2).
(9) Abstract and Applied Analysis.
(10) Acta Mathematica Sinica.
(11) Annales Mathematicae Silesianae.
(12) Ars Combinatorica.
(13) Bollettino dell'Unione Matematica Italiana.
(14) Discrete Mathematics.
(15) Filomat.
(16) International Journal of Mathematics, Game Theory and Algebra.
(17) Journal of Logic and Analysis.
(18) Journal of Mathematical Analysis and Applications.
(19) Journal of Number Theory.
(20) Journal of Symbolic Logic.
(21) Lithuanian Mathematical Journal.
(22) Mathematical Bulletin of the Shevchenko Scientific Society.
(23) Monatshefte für Mathematik.
(24) Open Mathematics (formerly: Central European Journal of Mathematics).
(25) Publicationes Mathematicae Debrecen.
(26) Tatra Mountains Mathematical Publications.
(27) Taiwanese Journal of Mathematics.

(28) Topology Proceedings.
(29) Transactions of the American Mathematical Society.
(30) Turkish Journal of Mathematics.

Computational mathematics.

(31) Applicable Algebra in Engineering, Communication and Computing (4).
(32) Journal of Mathematical Cryptology (4).
(33) IEEE Transactions on Information Theory (3).
(34) Groups Complexity Cryptology (3).
(35) Journal of Cryptology (2).
(36) Theoretical Computer Science, Series A (2).
(37) Contemporary Mathematics.
(38) Cryptography.
(39) Discrete Applied Mathematics.
(40) IEEE Transactions on Computers.
(41) IEEE Transactions on Information Security.
(42) Information Processing Letters.
(43) Information Sciences.
(44) Journal of Algebra and its Applications.
(45) Journal of Computer Science and Technology.
(46) Journal of Integer Sequences.
(47) Journal of Symbolic Computation.
(48) Theory of Computing Systems (formerly: Mathematical Systems Theory).

Refereeing for conferences.

(49) LATIN 2004 Conference on Theoretical Computer Sciences.
(50) SAC (Selected Areas in Cryptography) 2006.
(51) TCC (Theory of Computer Science) 2007.
(52) Indocrypt 2007.
(53) SCC (Symbolic Computation and Cryptography) 2008.
(54) Inscrypt 2010.
(55) SCC (Symbolic Computation and Cryptography) 2010.
(56) CCC (IEEE Conference on Computational Complexity) 2012.
(57) PKC (Public Key Cryptography) 2013, 2014.
(58) Eurocrypt 2018.
(59) Asiacrypt 2018.
(60) ProvSec 2018.

I also refereed several grant applications in my fields of research, for USA and EU grant agencies.

Reviewing. *Mathematical Reviews* (16 items); *Zentralblatt Mathematics* (20 items).

Editorship. Editorial board member, **Groups, Complexity, and Cryptology**, Walter de Gruyter. Informal newsletters editor: The **SPM Bulletin** on selection principles in mathematics; The **CGC Bulletin** on combinatorial group theory and cryptology.

Appendix A. Visits to universities and research institutes outside of Israel

23–30 June 2002. University of Lecce, Italy.

14–22 September 2003. Centre de Recerca Matematica, Barcelona, Spain.

14 November–2 December 2004. University of Warsaw, Poland (15–17 November); University of Katowice, Poland (18–23 November); University of Wrocław, Poland (24–25 November); University of Bonn, Germany (25 November–2 December).

16–20 November 2005. Ruhr-Universität Bochum, Germany.

18–25 December 2005. University of Lecce, Italy.

19 March–5 April 2006. Boise State University, Idaho, USA.

13–19 August 2006. Mathematical Institute of Czechoslovak Academy of Sciences, Czech Republic.

20–28 August 2006. University of Kielce, Poland.

29 August–4 September 2006. Universitat Politècnica de Catalunya, Spain.

23–29 April 2007. University of Niš, Serbia.

4–6 July 2007. University of Warsaw, Poland.

8–13 July 2007. Stefan Banach International Mathematical Center, Poland.

26 August–2 September 2007. University of Dortmund, Germany.

1–6 June 2008. University of Pisa, Italy.

1–19 December 2008. University Jaume I, Castellon, Spain.

23 August–3 September 2009. Royal Holloway, University of London, Egham, United Kingdom.

25 January–12 February 2010. University Jaume I, Castellon, Spain.

15–21 March 2010. Mississippi State University, USA.

6–13 June 2010. University of Valencia, Spain.

18–25 July 2010. Universitat Politècnica de Catalunya, Barcelona, Spain.

29 August–6 September 2010. Centre de Reserches Mathèmatiques, Montreal, Canada.

19–30 June 2011. University of Manitoba, Winnipeg, Canada.

18–27 July 2011. University of Messina, Messina, Italy.

28 August–16 September 2011. Kurt Gödel Research Center, Vienna, Austria.

11–29 June 2012. University of Messina, Sicily; Seconda Universitá di Napoli, Caserta, Italy.

24 July–4 August 2012. Heinrich Heine Universität Düsseldorf, Germany.

2–14 September 2012. Kurt Gödel Research Center, Vienna, Austria.

29 September–24 October 2013. Kurt Gödel Research Center, Vienna, Austria.

21–29 May 2014. University of Niš, Serbia.

6–11 September 2015. University of Messina, Messina, Italy.

1–5 Aug 2016. Leicester University, Leicester, UK, 2016.

4–23 Sep 2016. Sichuan University, Chengdu, China, 2016.

25 Oct–4 Nov 2016. Kurt Gödel Research Center, Vienna, Austria.

20 Aug–8 Sep 2017. Cardinal Stephan Wyszyński University, Warsaw.