

CURRICULUM VITAE FOR BOAZ TSABAN

Research interests.

Pure mathematics. Applications of discrete methods (infinite combinatorics) in continuous contexts, including: topological algebra, real analysis, and topological covering properties (selection principles).

Computational mathematics. Combinatorial group theory motivated by cryptography (public key cryptology and hash functions).

Personal information. Born in Israel, February 1973; citizen of Israel; married+5.

Education.

Ph.D. (2003, with highest distinction). Mathematics, Bar-Ilan University.
Supervisor: Hillel Furstenberg.
Title: *Infinite Combinatorial Topology.*

M.Sc. (1997, with highest distinction). Mathematics, Bar-Ilan University.
Supervisors: Martin Goldstern and Hillel Furstenberg.
Title: *Special classes of strongly null sets: A journey into the continuum.*

B.Sc. (1994, with highest distinction). Mathematics extended, Bar-Ilan University.

Employment.

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

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

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

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

Date: October 25, 2011.

Grants and Awards. Tenure track: Wolf Foundation's Krill Prize 2009 for Excellence in Scientific Research; United States-Israel Binational Science Foundation (BSF) travel grant for students; Rector's Grants for Excellence in Scientific Research 2008, 2009, 2010, 2011.

Post-Doctoral: Golda Meir, Edmund Landau, Minerva (short-term research visit), Koshland fellowship.

Ph.D.: Bar-Ilan President's Scholarship, Wolf Foundation, Sam Cohen, Rachel Jacobs, Nesyahu Prize for the best doctoral dissertation in mathematics in Israel, in the year 2003.

M.Sc.: Moris Banin.

B.Sc.: Israel Knesset, Rachel and Reuben Jacobs, David Ben-Guryon (Ministry of Science), Salim and Rachel Banin, Wolf Foundation.

Lectures in Conferences and workshops.

Invited and plenary 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 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) *IV Workshop on Coverings, Selections, and Games in Topology*, Seconda Università di Napoli, Caserta, Italy, 2012.
- (16) *Geometric and Combinatorial Group Theory*, Heinrich Heine Universität Düsseldorf, Germany, 2012.

Contributed lectures.

- (1) *BGU symposium in mathematics*, Ben-Guryon University, Israel, 2001.
- (2) *Israel Mathematical Union 2003 meeting*, Zichron Yaakov, Israel, 2003.
- (3) *The Barcelona Conference on Set Theory*, Centre de Recerca Matemàtica, Barcelona, Spain, 2003.
- (4) *Israel Mathematical Union 2005 meeting*, Neve Ilan, Israel, 2005.
- (5) *Boise Extravaganza in Set Theory*, Boise-State University, Idaho, USA, 2006.
- (6) *10th Prague topological symposium*, Prague, Czech Republic, 2006.
- (7) *International Conference on Set-theoretic Topology*, University of Kielce, Poland, 2006.
- (8) *Ultramath 2008*, University of Pisa, Italy, 2008.
- (9) *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 (the parenthesized numbers indicate the number of talks given at each mentioned institution): Bar-Ilan University (> 10); 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).

Students.

M.Sc.

- (1) Dima Ruinskiy (informally), graduated 2007, joint supervision with Adi Shamir.
- (2) Nadav Samet, graduated 2008, joint supervision with Gideon Schechtman.
- (3) Tal Orenstein, graduated 2009, joint supervision with Gady Kozma.
- (4) Tatyana Kovalyova, graduated 2010.
- (5) Garry Vinokor, started 2009.
- (6) Anton Kocherov, started 2009.
- (7) Tomer Yaniv, started 2010.

Ph.D. Adi Jarden, about to graduate.¹

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–present, joint supervision with Mina Teicher.
- (4) Ruthi Lebovitch, 10/2008–9/2009, joint supervision with Malka Schaps.

List of Publications.

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), 107–130.²
- (12) *Products of special sets of real numbers* (with T. Weiss), **Real Analysis Exchange** 30 (2004/5), 819–836.

¹Adi was awarded a 4,000\$ travel grant by U.S.-Israel Binational Science Foundation (BSF).

²Among Elsevier's *Top 25 Downloads* for July–September 2004.

- (13) *Strong γ -sets and other singular spaces*, **Topology and its Applications** 153 (2005), 620–639.³
- (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), 60–71.⁴
- (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. Todorćević, eds.), Trends in Mathematics, Birkhäuser 2006, 225–255.
- (19) *Additivity numbers of covering properties*, in: **Selection Principles and Covering Properties in Topology** (L. Koćinac, 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), 263–276.⁵
- (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 Koćinac α_i properties*, **Topology and its Applications** 155 (2007), 141–145.⁶
- (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.

³Among Elsevier’s *Top 25 Downloads* for January–March 2006.

⁴Among Elsevier’s *Top 25 Downloads* for October 2005–March 2006.

⁵Among Elsevier’s *Top 25 Downloads* for October–December 2007.

⁶Among Elsevier’s *Top 25 Downloads* for October–December 2007.

- (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), 104–109.⁷
- (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) *On the Pytkeev property in spaces of continuous functions (II)* (with L. Zdomskyy), **Houston Journal of Mathematics** 35 (2009), 563–571.
- (34) *Squares of Menger-bounded groups* (with M. Machura and S. Shelah), **Transactions of the American Mathematical Society** 362 (2010), 1751–1764.
- (35) *On a problem of Juhász and van Mill* (with S. Shelah and B. Tsaban), **Topology Proceedings** 36 (2010), 385–392.

Computational mathematics.

- (36) *Guaranteeing the diversity of number generators* (with A. Shamir), **Information and Computation** 171 (2001), 350–363.
- (37) *Efficient linear feedback shift registers with maximal period* (with U. Vishne), **Finite Fields and their Applications** 8 (2002), 256–267.⁸
- (38) *Bernoulli numbers and the probability of a birthday surprise*, **Discrete Applied Mathematics** 127 (2003), 657–663.⁹
- (39) *Permutation graphs fast forward permutations and sampling the cycle structure of a permutation*, **Journal of Algorithms** 47 (2003), 104–121.¹⁰
- (40) *The conjugacy problem and related problems in lattice-ordered groups* (with W. C. Holland), **International Journal of Algebra and Computation** 15 (2005), 395–404.
- (41) *Probabilistic solutions of equations in the braid group* (with D. Garber, S. Kaplan, M. Teicher, and U. Vishne), **Advances in Applied Mathematics** 35 (2005), 323–334.¹¹

⁷Among Elsevier’s *Top 25 Downloads* for October–December 2008.

⁸Among Elsevier’s *Top 25 Downloads* for January–April 2003.

⁹Among Elsevier’s *Top 25 Downloads* for January–April 2003.

¹⁰Among Elsevier’s *Top 25 Downloads* for the whole year 2003.

¹¹Among Elsevier’s *Top 25 Downloads* for July 2005–March 2006.

- (42) *Fast generators for the Diffie-Hellman key agreement protocol and malicious standards*, **Information Processing Letters** 99 (2006), 145–148.¹²
- (43) *Length-based conjugacy search in the Braid group* (with D. Garber, S. Kaplan, M. Teicher, and U. Vishne), **Contemporary Mathematics** 418 (2006), 75–87.
- (44) *Decompositions of graphs of functions and efficient iterations of lookup tables*, **Discrete Applied Mathematics** 155 (2007), 386–393.
- (45) *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.
- (46) *Theoretical cryptanalysis of the Klimov-Shamir number generator TF-1*, **Journal of Cryptology** 20 (2007), 389–392.
- (47) *Length-based cryptanalysis: The case of Thompson’s Group* (with D. Ruinskiy and A. Shamir), **Journal of Mathematical Cryptology** 1 (2007), 359–372.
- (48) *Random strategies with memory for the Robin Hood game*, in: **Foundations of the Formal Sciences V: Infinite Games** (S. Bold, B. Löwe, T. Räscher, J. van Benthem, eds.), Studies in Logic 11, College Publications, London 2007, 271–278.

Recreational mathematics.

- (49) *On the Rabbinical approximation of π* (with D. Garber), **Historia Mathematica** 25 (1998), 75–84.¹³
- (50) *A mechanical derivation of the area of a sphere* (with D. Garber), **The American Mathematical Monthly** 108 (2001), 10–15.
- (51) *The SPM Bulletin*, **Note di Matematica** 27 (2007), 111–117.

Number of pages in papers (Pure mathematics / Computational mathematics). 674 pages in published papers (529 / 145).¹⁴

Teaching. Courses, mini-courses, and seminars at all academic levels (first year B.Sc. up to Ph.D. 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, Weizmann Institute of Science), fractal theory, forcing theory, infinite-combinatorial topology, combinatorial number theory (Weizmann Institute of Science).

Research periods in universities and research institutes outside of Israel. Austria, Canada, Czech Republic, Germany, Italy, Poland, Serbia, Spain, USA. Details in Appendix A.

¹²Among Elsevier’s *Top 25 Downloads* for April–June 2006.

¹³Among Elsevier’s *Top 25 Downloads* for April–June 2005.

¹⁴All of these calculations were kindly performed by L^AT_EX.

Organization of conferences and workshops.

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.)

Membership in organizing committees.

- (1) *Coverings, Selections, and Games in Topology IV*, Caserta, Italy, 2012.
- (2) *Geometric and Combinatorial Group Theory with Applications*, Düsseldorf, Germany, 2012. (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 mathematical occupations

Research seminars. On the academic years 2005–2007 I co-organized the Weizmann Institute’s weekly *Geometric Functional Analysis and Probability* research seminar. Since 10/2007, I co-organize the Bar-Ilan University Colloquium on *Combinatorial Group theory and Cryptography*.

Mathematics books. I wrote books for some of the large mathematics courses at Bar-Ilan University: Linear Algebra, Infinitesimal Calculus, Set Theory, and Mathematical Logic.

Refereeing. I have refereed papers for the following journals. For quite a few of them, I refereed more than one paper.

Pure mathematics.

- (1) Abstract and Applied Analysis.
- (2) Acta Mathematica Sinica.
- (3) Ars Combinatorica.
- (4) Discrete Mathematics.
- (5) Groups–Complexity–Cryptology.
- (6) International Journal of Mathematics, Game Theory and Algebra.
- (7) Journal of Number Theory.
- (8) Journal of Symbolic Logic.
- (9) Lithuanian Mathematical Journal.
- (10) Matematicki Vesnik.
- (11) Note di Matematica.
- (12) Proceedings of the American Mathematical Society.
- (13) Tatra Mountains Mathematical Publications.
- (14) Taiwanese Journal of Mathematics.
- (15) Topology and its Applications.
- (16) Topology Proceedings.
- (17) Transactions of the American Mathematical Society.

Applied Mathematics.

- (18) Applicable Algebra in Engineering, Communication and Computing.
- (19) Contemporary Mathematics.
- (20) Discrete Applied Mathematics.
- (21) IEEE Transactions on Computers.
- (22) IEEE Transactions on Information Security.
- (23) IEEE Transactions on Information Theory.
- (24) Information Processing Letters.
- (25) Information Sciences.
- (26) Journal of Computer Science and Technology.
- (27) Journal of Cryptology.
- (28) Journal of Integer Sequences.
- (29) Journal of Mathematical Cryptology.
- (30) Theoretical Computer Science.
- (31) Theory of Computing Systems (formerly: Mathematical Systems Theory).

Refereeing for conferences.

- (32) LATIN 2004 Conference on Theoretical Computer Sciences.
- (33) SAC (Selected Areas in Cryptography) 2006.
- (34) TCC (Theory of Computer Science) 2007.

- (35) Indocrypt 2007.
- (36) SCC (Symbolic Computation and Cryptography) 2008.
- (37) Inscrypt 2010.

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

Reviewing. I review, on a regular basis, papers for *Mathematical Reviews* and for *Zentralblatt Mathematics*.

Editorship.

Editorial board. **Groups–Complexity–Cryptology**, a Walter de Gruyter journal.

Co-Editor. **Proceedings of the Second Workshop on Coverings, Selections, and Games in Topology**, Note di Matematica, volume 27, 2007.

Newsletter editor. The **SPM Bulletin** on selection principles and diagonalization arguments in mathematics; The **CGC Bulletin** on combinatorial group theory and cryptology.

E-mail. `tsaban@math.biu.ac.il`

APPENDIX A. RESEARCH PERIODS IN UNIVERSITIES AND RESEARCH INSTITUTES
OUTSIDE OF ISRAEL

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

14–22 September 2003. Centre de Recerca Matemàtica, 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.

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 Mathématiques, 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. University of Vienna, Vienna, Austria.