RESEARCH STATEMENT

BOAZ TSABAN

Most of my research is focused on two research topics. Within general and set theoretic topology, I study selection principles and their relations to real analysis and Ramsey theory. Within mathematical cryptology, I study the computational problems of public key protocols based on nonabelian groups. I have solved several central problems in each of these topics and, to this end, developed methods with impact beyond the motivating problems.

1. Selection principles

The theory of *selection principles* deals with mathematical properties and notions defined by selections from sequences of structured sets. For example, recall that a space is *compact* if every open cover of the space has a finite subcover. Compactness is a very useful property, but most spaces, including very important examples such as subsets of the real line, are not compact. A weaker restriction is provided by *Menger's property*, defined by Karl Menger in 1924. Motivated by his studies in dimension theory, Menger formulated his property as a basis property in metric spaces. In 1925, Witold Hurewicz observed that Menger's property is equivalent to the following covering property: For each sequence of open covers of the space, there are finite subsets of these covers that, *taken together*, cover the space.

Menger's property is one of several selective covering properties, which evolved in independent contexts such as measure theory (Borel's strong measure zero and Rothberger's closely related property C″) and function spaces (Fréchet–Urysohn property, Alexander Arhangel'skiĭ's countable fan tightness and Masami Sakai's stronger notion, Lev Bukovsky's, Ireneusz Recław's, and Miroslav Repicky's weak quasinormal convergence, etc.). Until the 1990's, these properties were studied in isolation. In a sequence of papers beginning in 1996, Marion Scheepers and others shaped a unified approach to the study of the major classic selective properties, and the identification of additional, natural ones. During these years big progress was made on some of the fundamental problems.

My approach to selection principles is to make their underlying combinatorics more transparent, and use this to develop methods for addressing the major problems and their surrounding theory. I am presently consolidating my approach to selection principles into a general method that I call *omission of intervals*.[1] I illustrate this by a prominent example.

A topological space is *Fréchet–Urysohn* if every point in the closure of a set in the space is actually a limit of a sequence of points from that set. Every metric (or first countable) space is Fréchet–Urysohn, but some very concrete spaces are not. The most prominent example is the space $C(X)$, the set of continuous real-valued functions on a subset X of the real line, equipped with the topology of pointwise convergence (equivalently, with the

Date: January 13, 2019.

[1]For brevity, I do not include here any exposition of two other methods that I co-developed, namely, the *projection method* and the *two worlds lemma*. These methods are used to establish selective properties of product spaces [4, 9].

topology inherited from the Tychonoff product $\mathbb{R}^X$). Unless the set X is countable, the space $C(X)$ is never metrizable. Could it be Fréchet–Urysohn? In a seminal 1982 paper, Gerlits and Nagy proved that this is the case if, and only if, the real set X has an elegant covering property. They called sets X with this property γ-*sets*. By a clever argument, they reformulated this property as a selective one, and used this to prove that γ-sets have Borel's strong measure zero. This implied that, consistently, uncountable γ-sets do not exist. Using a combinatorial reasoning, they proved that it is also consistent (and thus independent of ZFC) that uncountable γ-sets exist. To do this, they proved that the minimal cardinality of a *non*-γ-set is equal to the combinatorial cardinal number $\mathfrak{p}$.[2] Consistently, $\aleph_1 < \mathfrak{p}$, and in this case, every real set of cardinality $\aleph_1$ is a γ-set. Call such examples (stemming from cardinality only, without any analytic structure) *trivial*.

The first example for *nontrivial* γ-sets was given by Fred Galvin and Arnold Miller (1984), using the Continuum Hypothesis, or just $\mathfrak{p} = \mathfrak{c}$, where $\mathfrak{c}$ is the cardinality of the continuum. Their construction uses the hypothesis $\mathfrak{p} = \mathfrak{c}$ in an essential manner, since it diagonalizes over all potential open covers. Since then, many attempts were made at proving that a weaker axiom ($\aleph_1 = \mathfrak{b}$, or maybe even $\mathfrak{p} = \mathfrak{b}$) suffices. The documented attempts include ones by Just–Miller–Scheepers–Szeptycki (1996), Scheepers (1998), Miller (2005), and Gruenhage–Szeptycki (2005). We will return to this problem shortly.

By addressing all classic properties together, the theory of selection principles makes it convenient to study a specific property by transporting knowledge from related properties, or by addressing more amenable, related properties first. In a 2001 work essentially independent of the selection principles thread, Tomek Bartoszyński and Saharon Shelah considered a property that is equivalent to the Hurewicz covering property. Hurewicz's property is a selective property stronger than Menger's property and weaker than being a γ-set. Bartoszyński and Shelah used a certain compactification of the Baire space to prove the existence of a nontrivial Hurewicz subset of the real line, in ZFC. By uncovering the combinatorial essence of their proof, I realized that it can be recast in a language very similar to that of Galvin and Miller in their above-mentioned work. Using this unified approach, I arrived (via a sequence of intermediate results of independent interest [10]) at a proof that the hypothesis $\mathfrak{p} = \mathfrak{b}$ implies the existence of a nontrivial γ-set, solving the above-mentioned problem in the positive. The hypothesis $\mathfrak{p} = \mathfrak{b}$ is optimal in the sense that this sort of examples are, in particular, examples of so-called $\mathfrak{p}$-concentrated sets, and by a classic result of Lawrence, the hypothesis $\mathfrak{p} = \mathfrak{b}$ is necessary for the existence of $\mathfrak{p}$-concentrated sets.

My solution of the "γ-set problem" shows that *all* real sets with a certain combinatorial structure provided by the equality $\mathfrak{p} = \mathfrak{b}$ (namely, unions of unbounded towers of height $\mathfrak{b}$ with the set of finite sets of natural numbers, viewed as a subset of the Cantor set) are γ-sets. In general, my method is not only a method for proving the existence of extraordinary subsets of the real line, but also a method for establishing these properties for all given sets with an appropriate, purely combinatorial structure. This type of results is not standard in the field.

I included the mentioned main result in a paper with my MSc student, Tal Orenshtein [7]. Recently, I arrived at a more comprehensible proof. I presented the complete proof in my plenary lecture at the 31st Summer Conference on Topology and its Applications, to an audience from all branches of topology.

[2] A good exposition of the cardinal number $\mathfrak{p}$ and related combinatorial cardinals mentioned here is available in Andreas Blass's chapter in the Handbook of Set Theory (Springer, 2010).

The method is called *omission of intervals* since its arguments boil down to certain sets of natural numbers being disjoint to certain sequences of long intervals. My paper on Menger's and Hurewicz's problems [10] provides details of some easier applications of this method, and can demonstrate how the treatment of related problems helps in addressing a more difficult one, such as the one on γ-sets.

Additional results. I mention briefly some of my other main results in the realm of selection principles:

(1) My post-doctoral student, Lyubomyr Zdomskyy, and I proved that quasi-normal convergence of continuous real-valued functions on a real set X (known to be equivalent to Arhangel'skiĭ's property α_1) implies the same for *Borel* functions on X [13]. This resulted in a collapse of many properties in the literature into a single property, with very simple proofs, and left no problem from the classic literature concerning these properties open.
(2) My MSc student, Tal Orenshtein, and I obtained a resolution of the Gerlits–Nagy problem in the Borel case [8].
(3) Arnold Miller, Lyubomyr Zdomskyy and I obtained a complete solution of the question which real sets remain Hurewicz in extensions of the universe by Cohen forcing [5]. The answer: The Hurewicz sets that are also Rothberger, and only them.
(4) Viewing Hindman's Finite Sums Theorem as a theorem on open covers of a canonical countable set, I proved that it generalizes to arbitrary Menger spaces, and essentially only to them [12]. The proof uses a novel combination of idempotents in the Stone–Čech compactification and topological games.

2. Nonabelian cryptology

Present-day secure communication is mostly based on commutative mathematical structures and problems: the discrete logarithm problem in finite cyclic groups (Diffie–Hellman), integer factorization (RSA) and, more recently, lattice-based problems. To reduce the dependence of cyber-security on a small number of problems, it is desirable to also have candidate problems of substantially different types. On the practical side, this would make it easier to tailor optimal implementations in constrained environments, such as RFID tags.

Serious consideration of nonabelian algebraic structures as a source of computational problems for cryptography essentially began with the seminal proposals of Iris Anshel, Michael Anshel, and Dorian Goldfeld (1999), and of K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, and C. Park (2000). A parallel approach within complexity theory is recently developed by Avi Wigderson and others. A summary of the early attempts in the nonabelian cryptographic realm is provided in the textbooks by Alexei G. Myasnikov, Vladimir Shpilrain, and Sasha Ushakov (AMS, 2011), and by Maribel González–Vasco and Rainer Steinwandt (Chapman and Hall/CRC Press, 2015). Several devastating cryptanalyses were discovered, based on concurrent mathematical breakthroughs such as the establishment of the linearity of Braid groups. These cryptanalyses indicate that the early proposals were not ripe, and further research is needed in order to identify potentially secure instantiations of the proposed protocols.

The security of a protocol based on a nonabelian structure (in the passive adversary model, assuming for simplicity a random oracle is available) boils down to a clean computational problem concerning the nonabelian structure. Some of these problems, notably the problem

underlying the Anshel–Anshel–Goldfeld *commutator key exchange* protocol, stood out and were advocated by mathematicians such as Alexei G. Myasnikov (a co-developer of the algebraic solution to the Tarski problem on elementary equivalence of free groups) as a potentially hard, new computational problem.

A computational solution of a problem is far more challenging than a cryptanalytic solution. The former should, *provably*, solve the problem efficiently in all, not only most probable, cases. After several years of developing heuristic approaches to the commutator key-exchange problem, I arrived at a definitive computational solution [11]. The solution is structural, and the method was demonstrated to solve several other major problems in nonabelian cryptology. Later, I arrived at the *algebraic span* method [1], a much simpler method applicable in greater generality, which applies to essentially all major protocols based on nonabelian groups.

Some of the applications of the algebraic span method were arrived at jointly with my post-doctoral student Arkadius Kalka, my doctoral student Adi Ben Zvi, and my colleague Simon Blackburn [1, 2]. These include a provable cryptanalysis of an ISO standard proposal for the Internet of Things [2]. The cited reference contains most of the ingredients of this solution. We are presently finalizing a journal version of this paper, where we use methods of Babai and others to make the cryptanalysis fully provable. Provability is based on using uniform i.i.d. distributions on the chosen secret generators. SecureRF, the company that developed this protocol, is presently developing some variations that resist our cryptanalysis, and we may consider them in the future.

Additional results. I also consider hash functions based on nonabelian structures, such as random walks on Cayley graphs. In a joint work with Ciaran Mullan, I obtained the first random self-reducibility results for these functions [6]. This research led me to the discovery of a new candidate for a family of cryptographic hash function that may turn out useful for low-resource processors. I plan to consider this family from a cryptanalytic point of view, in order to estimate its efficiency and security.

From a mathematical aspect, my major result in computational mathematics is a complete, effectively computable invariant for the simultaneous conjugacy problem in Artin's braid groups [3]. This work, joint with my post-doctoral student Arkadius Kalka and my MSc student Gary Vinokur, includes:

(1) The introduction of high-dimensional super summit sets, generalizing Frank A. Garside's one-dimensional notion.
(2) A high-dimensional cycling theorem, providing a method and a bound on its complexity, for conjugating a tuple into its high-dimensional super summit set. This extends the one-dimensional cycling theorem of Joan Birman, Ki Hyoung Ko, and Sang Jin Lee (1998). The algorithm and proof are different than the one-dimensional ones.
(3) A development of minimal simple elements for conjugating tuples inside high-dimensional super summit sets, generalizing Juan González–Meneses's (2005) one-dimensional notion.

The most important future challenge in this direction is finding a high-dimensional extension of Volker Gebhardt's *ultra summit sets* (2005), presently the best invariant in the one-dimensional case. We already have the main ingredient, a high-dimensional cyclic (and cyclic sliding) operation with the requested provable properties, and it remains to find the appropriate transportation maps among the various cycles in the cyclic (sliding) graph.

References

[1] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via algebraic spans, CRYPTO 2018 – Lecture Notes in Computer Science **10991** (2018), 255–274.

[2] A. Ben Zvi, S. Blackburn, B. Tsaban, *A Practical Cryptanalysis of the Algebraic Eraser*, CRYPTO 2016, Lecture Notes in Computer Science **9814** (2016), 179–189.

[3] A. Kalka, B. Tsaban, G. Vinokur, *A complete simultaneous conjugacy invariant in Garside groups*, submitted for publication, 22 pages.

[4] A. Miller, B. Tsaban, L. Zdomskyy, *Selective covering properties of product spaces*, Annals of Pure and Applied Logic **165** (2014), 1034–1057.

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

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

[7] T. Orenshtein, B. Tsaban, *Linear σ-additivity and some applications*, Transactions of the American Mathematical Society **363** (2011), 3621–3637.

[8] T. Orenshtein, B. Tsaban, *Pointwise convergence of partial functions: The Gerlits–Nagy Problem*, Advances in Mathematics **232** (2013), 311–326.

[9] P. Szewczak, B. Tsaban, *Products of Menger spaces: A combinatorial approach*, Annals of Pure and Applied Logic **168** (2017), 1–18.

[10] B. Tsaban, *Menger's and Hurewicz's Problems: Solutions from "The Book" and refinements*, Contemporary Mathematics **533** (2011), 211–226.

[11] B. Tsaban, *Polynomial-time solutions of computational problems in noncommutative algebraic cryptography*, Journal of Cryptology **28** (2015), 601–622.

[12] B. Tsaban, *Algebra, selections, and additive Ramsey theory*, Fundamenta Mathematicae **240** (2018), 81–104.

[13] B. Tsaban, L. Zdomskyy, *Hereditarily Hurewicz spaces and Arhangel'skiĭ sheaf amalgamations*, Journal of the European Mathematical Society **12** (2012), 353–372.