Efficient (Propositional) Proofs of Statements in Combinatorial Topology and Related Areas

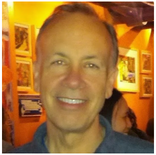
Gabriel Istrate
gabrielistrate@acm.org

University of Bucharest
Virtute et Sapientia

Acknowledgment

- Research program. Multiple papers (SAT'14, ICALP 2015, 2021), plus work in progress.
- Coauthors (chronologically): Adrian Crãciun (Timişoara), James Aisenberg (Seattle), Sam Buss (San Diego), Maria-Luisa Bonet (Barcelona), Cosmin Bonchiş (Timişoara).





"Philosophical" Summary/Outline

Mathematics (in particular Algebraic Topology) often works with exponential size objects (nonconstructive proofs).

(When) can we make them "small"/constructive ?

- Concrete statement: Kneser-Lovász Theorem, hard to prove (mathematically). Is its propositional encoding hard in proof complexity ?
- Surprise: easy to prove (mathematically) (with disclaimers)
- How ? Why ?
- **Spoiler:** versions of notions of kernelization/data reduction from parameterized complexity theory.

Proof Complexity

Given a class of unsatisfiable propositional formulas, how hard it is to refute them in a certain proof system ?

- **Hardness:** length/"complexity" of the proof
- ... difficulty of finding it also relevant.
- Proof systems: e.g. resolution ...
- (extended) Frege systems
- cutting planes, polynomial calculus, nullenstellensatz, sums of squares, semi-algebraic proofs, IPS ....

Boundaries of proof complexity: Frege proofs

"Textbook-style" proof systems.

Cook-Reckhow: all Frege proof sys poly simulate eachother

- Example, for concreteness [Hilbert Ackermann]
  - propositional variables $p_1, p_2, \ldots.$
  - Connectives $\neg$, **or** .
  - Axiom schemas:
    1. $\neg(A \textbf{ or } A) \textbf{ or } A$
    2. $\neg A \textbf{ or } (A \textbf{ or } B)$
    3. $\neg(A \textbf{ or } B) \textbf{ or } (B \textbf{ or } A)$
    4. $\neg(\neg A \textbf{ or } B) \textbf{ or } (\neg(C \textbf{ or } A) \textbf{ or } (C \textbf{ or } B))$
  - Rule: From A and $\neg A$ **or** B derive B.

Superpolynomial lower bounds: restricted (e.g. depth) versions of Frege.

Proof complexity of the pigeonhole principle

n pigeons in $n-1$ holes $\Rightarrow$ at least two pigeons in same hole !

- E.g. Pigeonhole formula(s): PHP_n^{n-1}
- $X_{i,j} = 1$ "pigeon i goes to hole j".
- $X_{i,1}$ **or** $X_{i,2}$ **or** $\ldots$ **or** $X_{i,n-1}$, $1 \leq i \leq n$ (each pigeon goes to (at least) one hole)
- $\overline{X_{k,j}}$ **or** $\overline{X_{k,i}}$ (pigeon k goes to at most one hole).
- $\overline{X_{k,j}}$ **or** $\overline{X_{l,j}}$ (pigeons k and l do not go together to hole j).
- Resolution complexity: exponential ! (Haken)

Theorem (Buss): PHP_n has poly-size Frege proofs.

Extended Frege proofs

Frege proofs + variable substitutions.

We may introduce variable names for formulas $X \Leftrightarrow \Phi(Y)$. Proves the same formulas but potentially with great reductions in size.

OPEN PROBLEM: Is extended Frege **strictly** more powerful than Frege ? Most natural candidates for separation turned out to have subexponential Frege proofs.

Wishful thinking: Perhaps translating into SAT a mathematical statement that is (mathematically) hard to prove would yield a natural candidate for the separation.

Kneser's Conjecture

- Stated in 1955 (Martin Kneser, Jaresbericht DMV)

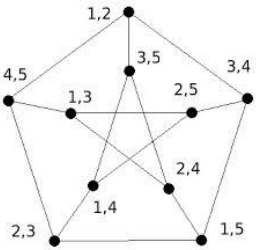
> Let $n \geq 2k - 1 \geq 1$. Let $c : \binom{n}{k} \to [n - 2k + 1]$. Then there exist two disjoint sets A and B with $c(A) = c(B)$.

- $k = 1$ Pigeonhole principle!
- $k = 2, 3$ combinatorial proofs (Stahl, Garey & Johnson)
- $k \geq 4$ only proved in 1977 (Lovász) using Algebraic Topology.
- Combinatorial proofs known (Matousek, Ziegler). "Hide" Alg. Topology in combinatorics.

> No "purely combinatorial" proof was known

Kneser's Conjecture (II)

- the chromatic number of a certain graph $Kn_{n,k}$ (at least) $n - 2k + 2$. (exact value)
- Vertices: $\binom{n}{k}$. Edges: disjoint sets.
- E.g. $k = 2$, $n = 5$: Petersen's graph has chromatic number (at least) three.
- "Internal graph" also chromatic number $n - 2k + 2$ (Schrijver's theorem).



Lovász-Kneser as an (unsatisfiable) SAT formula

- naïve encoding $X_{A,k} = TRUE$ iff A colored with color k.
- $X_{A,1}$ **or** $X_{A,2}$ **or** $\ldots$ **or** $X_{A,n-2k+1}$ "every set is colored with (at least) one color"
- $\overline{X_{A,j}}$ **or** $\overline{X_{B,j}}$ $(A \cap B = \emptyset)$ "no two disjoint sets are colored with the same color"
- $\overline{X_{A,j}}$ **or** $\overline{X_{A,k}}$ "no set has two colors".
- Fixed k: $Kneser_{k,n}$ has poly-size (in n).
- Extends encoding of PHP

Our results in a nutshell

- $Kneser_n^k$ reduces to (is a special case of) $Kneser_{n-2}^{k+1}$.
- Thus all known lower bounds that hold for PHP hold for any $Kneser_k$.
- Cases with combinatorial proofs:
  - $k = 2$: polynomial size Frege proofs
  - $k = 3$: polynomial size extended Frege proofs
- $k \geq 4$: surprisingly, quasipoly Frege/poly extended Frege proofs.

Most important, "take-home" message: for every fixed k, $Kneser_*^k$ can be proved (mathematically) by an easy-to-describe reduction to a finite set of values of n, (to be checked, perhaps on a computer) completely bypassing Algebraic Topology !

(ICALP 2015/Information and Computation 2018, but written in the language of proof complexity)

Proof idea

Assume there was a $(n-2k+1)$-coloring of $Kneser_n^k$.

A color class C_l is star shaped if the intersection of all members is nonempty.

Theorem: If C_l is **not** star-shaped then $|C_l| \leq k^2\binom{n-2}{k-2}$.

Reduction, assuming theorem:
If $n > k^4$ then $\binom{n}{k} > (n-2k+1)k^2\binom{n-2}{k-2}$, hence some color class is star-shaped C_l. Remove C_l and the central element of class C_l.

Conclusion: We get a $(n-2k)$-coloring of $Kneser_{n-1}^k$.

Proof of the theorem

Let C_l be a non-star-shaped color class.

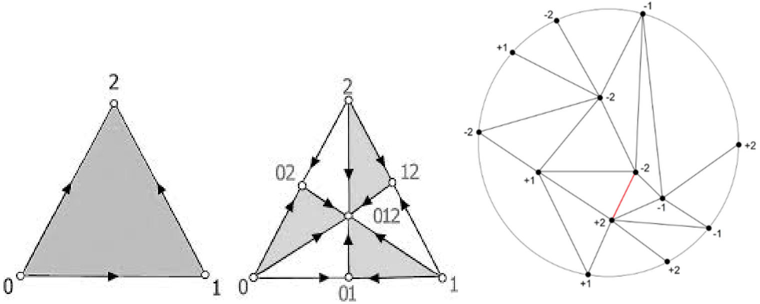
- Fix some $S = \{a_1, ..., a_k\} \in C_l$.
- For every a_i let $S_i \in P_l$, $a_i \notin S_i$ (C_l not star-shaped)
- To specify arbitrary $T \in C_l$:
  - Specify $a_i \in T$ ($S \cap T \neq \emptyset$)
  - Specify $x \in S_i \cap T$.
  - Specify the remaining $k - 2$ elements.

Nr. of choices: $k \cdot k \cdot \binom{n-2}{k-2}$.

If *Kneser* is not difficult, then what is ?

Discrete version of Borsuk-Ulam: Octahedral Tucker's lemma.

- Intuition: Borsuk-Ulam - no continuous (a.k.a simplicial) antipodal map from the n-ball to the n-sphere.
- For any labeling of T with vertices from $\{\pm 1, \ldots, \pm(n-1)\}$ antipodal on the boundary there exist two adjacent vertices $v \sim w$ with $c(v) = -c(w)$.



Octahedral Tucker Lemma

Definition: Let $n \geq 1$. The *octahedral ball* $\mathcal{B}^n$ is:

$$\mathcal{B}^n := \{(A, B) : A, B \subseteq [n] \text{ and } A \cap B = \emptyset\}.$$

Definition: Two pairs (A_1, B_1) and (A_2, B_2) in $\mathcal{B}^n$ are *complementary* with respect to λ if $\mathbf{A_1} \subseteq \mathbf{A_2}$, $\mathbf{B_1} \subseteq \mathbf{B_2}$ and $\lambda(A_1, B_1) = -\lambda(A_2, B_2)$.

Theorem (Octahedral Tucker lemma)

If $\lambda : \mathcal{B}^n \to \{1, \pm 2, \ldots, \pm n\}$ is antipodal, then there are two elements in $\mathcal{B}^n$ that are complementary.

- barycentric subdivision $\Rightarrow$ exponentially large formula !

A class of "hard" formulas based on Octahedral Tucker Lemma

- Kneser follows from a new "low dimensional" Tucker lemma.
- Avoid barycentric subdivision. Instead "truncated version".

Definition: Let $1 \leq k \leq n$. The *truncated octahedral ball* $\mathcal{B}^n_{\leq k}$ is:

$$\mathcal{B}^n_{\leq k} \; := \; \Big\{(A, B) \in \mathcal{B}^n : |A| \leq k, \; |B| \leq k\Big\}.$$

Definition: Let $\preceq$ be the partial order on sets in $\binom{n}{\leq k}$ defined by $\mathbf{A} \preceq \mathbf{B}$ iff $(\mathbf{A} \cup \mathbf{B})_{\leq \mathbf{k}} = \mathbf{B}$.

Definition: For (A_1, B_1) and (A_2, B_2) in $\mathcal{B}^n_{\leq k}$, write $(A_1, B_1) \preceq (A_2, B_2)$ when $A_1 \preceq A_2$, $B_1 \preceq B_2$, and $A_i \cap B_j = \emptyset$ for $i, j \in \{1, 2\}$. The pairs (A_1, B_1) and (A_2, B_2) are k-complementary with respect to an antipodal map λ on $\mathcal{B}^n_{\leq k}$ if $(A_1, B_1) \preceq (A_2, B_2)$ and $\lambda(A_1, B_1) = -\lambda(A_2, B_2)$.

Truncated Octahedral Tucker Lemma

THEOREM: Let $n \geq k \geq 1$. If $\lambda : \mathcal{B}^n_{\leq k} \to \{1, \pm 2 \ldots, \pm n\}$ is antipodal, then there are two elements in $\mathcal{B}^n_{\leq k}$ that are k-complementary.

- (Mathematically) follows from "ordinary" octahedral Tucker lemma.
- k-truncated Tucker Implies $Kneser_k$.
- Translates (naturally) to formulas $Truncated^k_n$, whose proof complexity unknown.
- Generates search problem $Truncated_k$.

Complexity of Truncated Tucker Lemma

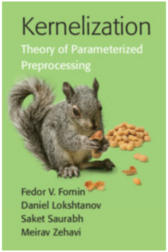
THEOREM: [ABCCI, journal version] Formulas Tucker_n^1 have poly-size extended Frege proofs.

THEOREM: (Aisenberg) $\mathit{Tucker}_k \preceq_m \mathit{Tucker}_{k+1}$.

THEOREM: (Aisenberg) Tucker_k hard for PPP.

CONCLUSION: Kneser_k may not be "hard", but Tucker_k (which encodes the topological principle used to prove it) probably is!

Why is Kneser easy? What else is?



- **kernelization:** reduce instance (x, k) to "kernel instance" (x', k'), s.t. $(x, k) \in L$ iff $(x', k') \in L$ and $|x'|, k' \leq g(k)$ for some computable g.
- **data reduction:** algorithm A that maps in time poly$(|x| + k)$ (x, k) to (x', k') s.t. $(x, k) \in L$ iff $(x', k') \in L$ and $|x'| \leq |x|$.
- given r data reductions $A_1, \ldots, A_r$, a **data reduction chain** for instance (x, k) of L: seq. $(x_0, k_0), (x_1, k_1), \ldots, (x_m, k_m)$, where $(x_0, k_0) = (x, k)$, $A_t(x_m, k_m) = (x_m, k_m)$ for $t = 1, \ldots r$ and, for $i = 1, \ldots, m$ $\exists j \in 1, \ldots, r$ s.t. $(x_i, k_i) = A_j(x_{i-1}, k_{i-1})$.

Main idea

- **"Negative" instance** (x, k) of parameterized problem in NP **maps "canonically" to formula** $\Phi(x, k) \in \overline{SAT}$**.**

- If Π_i proof for soundness of the reduction rule $(x_i, k_i) = A_j(x_{i-1}, k_{i-1})$ and Π_{m+1} is a "brute force proof of unsatisfiability" for the kernel instance then one can prove $\Phi(x, k) \in \overline{SAT}$ by "concatenating" $\Pi_1, \ldots, \Pi_m$ and Π_{m+1}.

- Need: data reduction of length $O(\log(n))$ to unwind variable substitutions.

Applications of Kernelization Techniques to Proof Complexity

- Extend results on Kneser to Schrijver's theorem.
- classical (ad-hoc) kernelization for **VertexCover** $\Rightarrow$ for every fixed k, negative instances of VC with parameter k have poly-size Frege proofs.
- **crown decomposition** for **DualColoring** $\Rightarrow$ negative instances of VC with parameter k poly-size Frege proofs.
- improved (ad-hoc) kernelization for **EDGE CLIQUE COLOR** $\Rightarrow$ negative instances (G,k) of EDGE CLIQUE COVER have extended Frege proofs of poly size and Frege proofs of quasipoly size.
- **sunflower lemma**-based kernelization of d-**HittingSet**$\Rightarrow$ **negative instances of** d**-HittingSet extended Frege proofs of poly size .**
- **NEW Turing kernelization: Instances of CLIQUE(VC) have poly-size Frege proofs.**

Applications to Computational Social Choice

- **Arrow, Gibbard-Satterthwaite:** Fundamental impossibility results on ranking m objects by n agents.
- Tang & Lin (Artificial Intelligence, 2009): Arrow's Theorem has computer-assisted propositional proofs by reducing the general case to the case $n = 2, m = 3$. Similar results (2008) for the Gibbard-Satterthwaite theorem.
- Their proofs: data reductions of length $\Theta(n + m)$.

We give: **data reductions of length $O(n)$**, whose soundness can be witnessed by efficient Frege proofs.

Theorem
Formulas $Arrow_{m,n}, GS_{m,n}$ have:

- *quasipoly size Frege proofs*
- *poly size Frege proofs for fixed n.*

Further work & Open problems

- Proof complexity of parameterized intractable (W[1] and higher) problems ?
- Open problem: search complexity of the Octahedral Tucker Lemma ?
- Open problem Proof complexity of cutting planes for $Kneser_n^2$?
- Logics for implicit proof systems ? Other combinatorial principles ?

Thank you. Questions ?