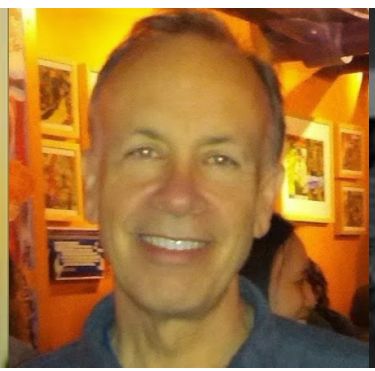
On the proof complexity and (un)satisfiability of several combinatorial principles

Gabriel Istrate
West University of Timişoara, Romania

Disclaimer

- Somewhat older work, newer research more algorithmic.
- This presentation: Combines multiple papers (SAT, ICALP), plus work in progress, multiple topics.
- Coauthors (chronologically): Adrian Crãciun (Timişoara), James Aisenberg, Sam Buss (both San Diego), Maria-Luisa Bonet (Barcelona), Cosmin Bonchiş(Timişoara).





"Philosophical" Summary

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

Can we make them "small"/constructive ?

This work: very combinatorial, finitistic formalization of this problem.

Outline

- What is Proof Complexity and why do we care about it.

Outline

- What is Proof Complexity and why do we care about it.
- Combinatorial principles and their propositional translation.

Outline

- What is Proof Complexity and why do we care about it.
- Combinatorial principles and their propositional translation.
- Proof complexity results

Outline

- What is Proof Complexity and why do we care about it.
- Combinatorial principles and their propositional translation.
- Proof complexity results
- Experimental benchmarking of Kneser formulas.

Outline

- What is Proof Complexity and why do we care about it.
- Combinatorial principles and their propositional translation.
- Proof complexity results
- Experimental benchmarking of Kneser formulas.
- Complexity of the (Truncated) Tucker Lemma.

Outline

- What is Proof Complexity and why do we care about it.
- Combinatorial principles and their propositional translation.
- Proof complexity results
- Experimental benchmarking of Kneser formulas.
- Complexity of the (Truncated) Tucker Lemma.
- ~~Future~~ Current work and open problems.

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
- ... or difficulty of finding it
- Proof systems: e.g. resolution ...
- (extended) Frege systems
- cutting planes, polynomial calculus, nullenstellensatz, sums of squares, semi-algebraic proofs, IPS
- ...the list goes on and on.

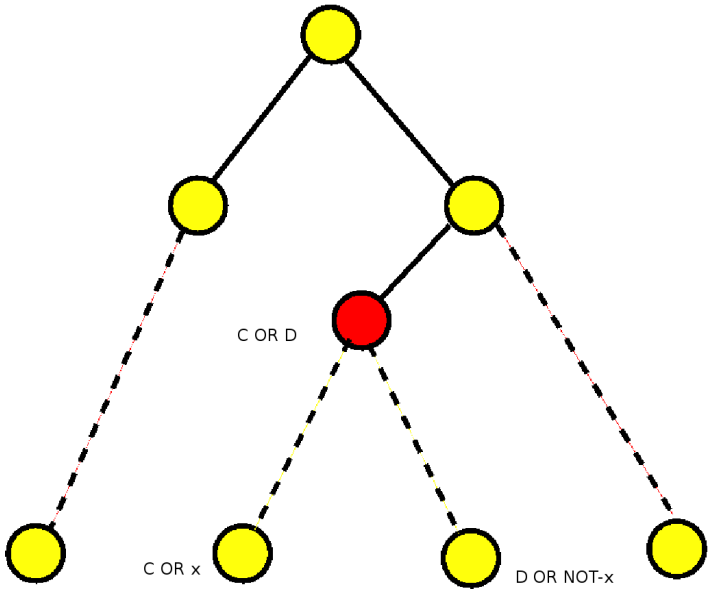
Why care about proof complexity ?

- academic reasons.
- applications to SAT solving and Integer Programming.

Applications: SAT solving - Complexity of DPLL

Resolution length: L.B. running time of all DPLL algorithms !

- resolution $C \vee x$, $D \vee \overline{x} \rightarrow (C \vee D)$, $x, \overline{x} \rightarrow \square$.
- Complexity= minimum length of a resolution proof.



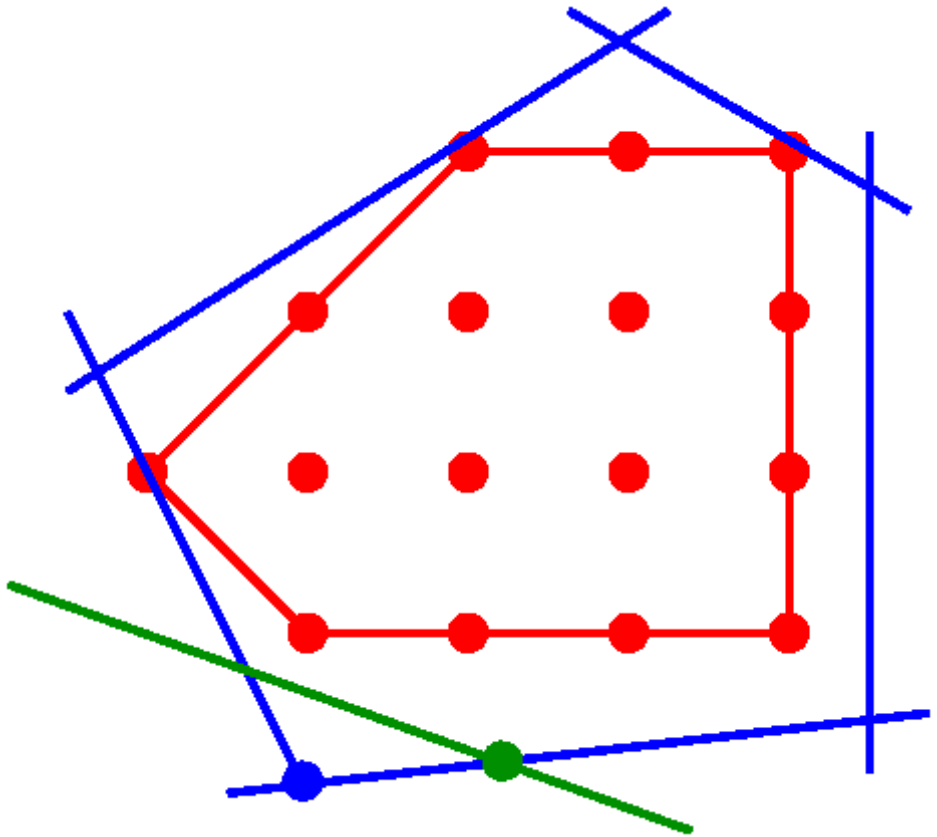
Applications: SAT solving - Complexity of DPLL

Most successful SAT solvers: DPLL + clause learning (CDCL)

Proof complexity theorists called up by practitioners to explain the success of CDCL (Banff, Dagstuhl,VSL, etc)

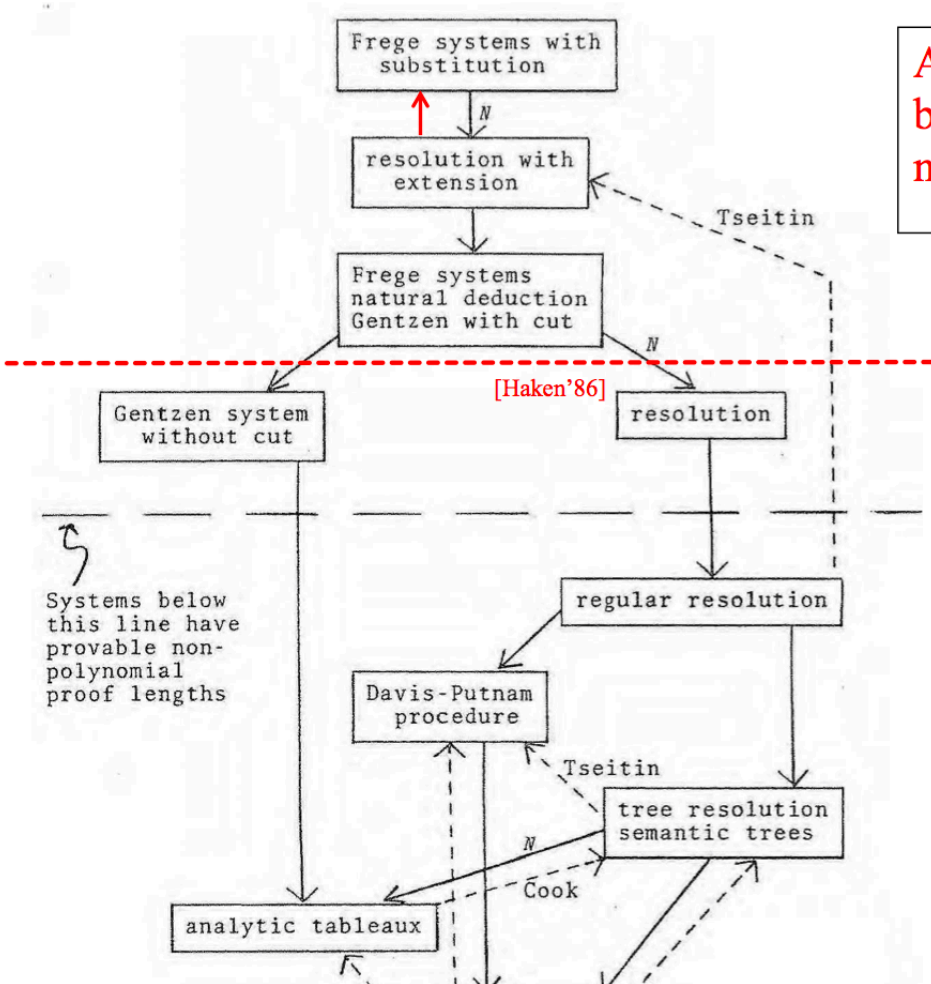
Beyond CPLEX/GUROBI: branch and bound + cutting planes.

Many B& B. algs simulated by cutting plane proofs



Proof complexity: frontiers of tractability

Image credit: Sam Buss ⇐ R. Reckow



As of 2014, proof systems below the line are known to not be polynomially bounded:

Constant-depth (AC^0) Frege
[Ajtai'88; Pitassi-Beame-Impagliazzo'93; Krajicek-Pudlak-Woods'95]

Constant-depth Frege with counting mod *m* axioms
[Ajtai'94; Beame-Impagliazzo-Krajicek-Pitassi-Pudlak'96; B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Cutting Planes
[Pudlak'97]

Nullstellensatz
[B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Boundaries of proof complexity: Frege proofs

"Textbook-style" proof systems.

Cook-Reckhow: all Frege proof sys polynomially simulate eachother

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

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

Proof complexity of the pigeonhole principle

n pigeons in n − 1 holes ⇒ 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".
- $X_{i,1} \vee X_{i,2} \vee \ldots \vee X_{i,n-1}$, $1 \leq i \leq n$ (each pigeon goes to (at least) one hole)
- $\overline{X_{k,j}} \vee \overline{X_{l,j}}$ (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.

E. g.: usual inductive proof for PHP: poly-size extended Frege proof.

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

Poly-size Frege proofs for PHP

- Buss proof: by counting
- $Z = \text{Count}(X_1, X_2, \ldots, X_n)$ = the number of TRUE vars. among $X_1, X_2, \ldots, X_n$.
- Can be "computed by Frege proofs" (bits of Z = truth status of propositional formulas)
- Given $f : [n] \to [n-1]$, counterexample to PHP:
  - Count $|A_i|$, where $A_i = f^{-1}([i])$.
  - $|A_1| \leq 1$.
  - $|A_i| \leq |A_{i-1}| + 1$.
  - so $n = |A_n| \leq n - 1$, contradiction.

Wishful thinking

- Open question: Is extended Frege more powerful than Frege ?
- Perhaps translating into SAT a mathematical statement that is (mathematically) hard to prove would yield a natural candidate for the separation.

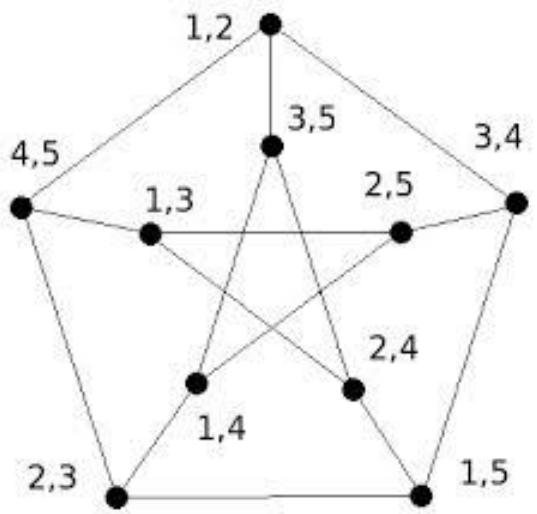
Kneser's Conjecture

- 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 $c(A) = c(B)$.

- 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
- No "purely combinatorial" proof known

Kneser's Conjecture (II)

- the chromatic number of a certain graph $\mathrm{Kn}_{n,k}$ (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.



Stronger form: Schrijver's Theorem

- inner cycle in Petersen's graph already chromatic number three.
- $A \in \binom{n}{k}$ stable if it doesn't contain consecutive elements i, $i+1$ (including $n, 1$).
- Schrijver's Theorem: Kneser's conjecture holds when restricted to stable sets only.

Lovász-Kneser's Thm. as an (unsatisfiable) propositional formula

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

Our results in a nutshell

- Kneser_n^k reduces to (is a special case of) $\text{Kneser}_{n-2}^{k+1}$.
- Thus all known lower bounds that hold for PHP (resolution, bd. Frege) hold for any Kneser_k.
- Cases with combinatorial proofs:
  - $k = 2$: polynomial size Frege proofs
  - $k = 3$: polynomial size 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, completely bypassing Algebraic Topology !

Reducing Kneser_n^{k+1} to Kneser_{n-2}^{k}

THM: There exists a var. subst.
$\Phi_k : \text{Var}(\text{Kneser}_n^{k+1}) \to \text{Var}(\text{Kneser}_{n-2}^{k})$ s.t. $\Phi_k(\text{Kneser}_n^{k+1})$ consists precisely of the clauses of Kneser_{n-2}^{k} (perhaps repeated and in a different order)

Proof: Let $A \in \binom{n}{k+1}$. Define $\Phi_k(X_{A,i})$ by:

- Case 1: $A_{\leq k} \subseteq [n-2]$: $\Phi_k(X_{A,i}) = Y_{A_{\leq k},i}$
- Case 2: $A_{\leq k} \not\subseteq [n-2]$: $(n-1, n \in A)$ Let $A = P \cup \{n-1, n\}$, $|P| = k-1$. Let $\lambda = \max\{j : j \leq n-2, j \notin P\}$. Define $\Phi_k(X_{A,i}) = Y_{P \cup \{\lambda\},i}$

Clause $X_{A,1} \vee X_{A,2} \vee \ldots \vee X_{A,n-2k+1}$ maps to $Y_{B,1} \vee Y_{B,2} \vee \ldots \vee Y_{B,n-2k+1}$, $B = A$ (Case 1). Clauses $\overline{X_{A,i}} \vee \overline{X_{B,i}}$ $(A \cap B = \emptyset)$ map to $\overline{Y_{C,i}} \vee \overline{Y_{D,i}}$ Case 2 cannot happen for both A and B. By case analysis $C \cap D = \emptyset$.

Poly-size Frege proofs for Kneser_n^2

- For any color class $c^{-1}(\lambda)$ one of the following is true (assuming conclusion of Kneser does not hold):
  - $|c^{-1}(\lambda)| \leq 3$.
  - All sets $B \in c^{-1}(\lambda)$, $|c^{-1}(\lambda)| \geq 4$, have one element in common (call such color class star-shaped, and the element special).
- Frege systems can "count" (á lá Buss) many things.
- Assuming said coloring exists, contradiction: $\binom{n}{2} \leq \ldots$ (something smaller)

Proof: $D = \{a, b\} \in c^{-1}(l)$, $E \in c^{-1}(l)$, $a \notin E$, then either $D \cap E = \emptyset$ or $E = \{b, c\}$, for some c. If $\bigcap_{A \in c^{-1}(l)} A = \emptyset$ then there exists another set F with $b \notin F$. F has to intersect both D and E, thus $F = \{a, c\}$. Hence $|c^{-1}(l)| \leq 3$.

Poly-size Frege proofs for Kneser_n^2

Count:

- large star-shaped color classes

$$p_r = |\{1 \le \lambda \le r : |c^{-1}(\lambda)| \ge 4 \text{ and } \bigcap_{A \in c^{-1}(\lambda)} A \neq \emptyset\}|,$$

- Nodes colored with the first r colors.

$$M_r = \sum_{i=1}^{r} |c^{-1}(i)|$$

Let

$$N_r = p_r(n-1) - \frac{p_r(p_r-1)}{2} + 3(r-p_r)$$

(upper bound on the # elements covered by the first r color classes)

Poly-size Frege proofs for Kneser_n^2

Prove (in poly-size Frege):

- $M_r \leq M_{r+1}$.
- $N_r \leq N_{r+1}$.
- $M_r \leq N_r$.

Assume by contradiction a coloring exists.

$$\binom{n}{2} = M_n \leq N_n \leq \max_p p(n-1) - \frac{p(p-1)}{2} + 3(r-p) \leq \binom{n}{2} - 3.$$

Intermezzo: Benchmarking Kneser (+Schrijver) formulas with SAT

- glucose, lingeling, one of the best SAT solvers (SAT'2016).
- Same timeout as in SAT competition, better hardware.

Dim. Probl.	Kneser	Schrijver
$\binom{2}{10}$	171.2 sec, 16.9 MB	152.2 sec, 14.1 MB
$\binom{2}{11}$	6393.0 sec, 91.8 MB	6281.6 sec, 57.8 MB
$\binom{2}{12}$	> 32400.1 sec (timeout)	> 33562.5 sec (timeout)
$\binom{3}{10}$	17.7 sec, 8.1 MB	16.9 sec, 7.2 MB
$\binom{3}{11}$	4273.3 sec, 57.6 MB	4314.5 sec, 41.7 MB
$\binom{3}{12}$	>32400.2 sec (timeout)	> 34530.4 sec (timeout)
$\binom{4}{11}$	3.8 sec, 5.9 MB	5.5 sec, 4.7 MB
$\binom{4}{12}$	>32400.2 sec (timeout)	> 34530.4 sec (timeout)
$\binom{5}{12}$	0.2 sec, 2.2 MB	0.0 sec, 0.2 MB
$\binom{5}{13}$	2085.2 sec, 64.2 MB	398.0 sec, 20.1 MB
$\binom{5}{14}$	>32400.2 sec (timeout)	> 34530.4 sec (timeout)

Intermezzo: Benchmarking Schrijver formulas with IP

- lingeling maxes out on PHP at n = 18.
- To give algorithms a chance, we use IP/Gurobi.
- Gurobi solves PHP well up to n = 50.
- Similar max-out on Sch_n^2 !

Conclusion:

Kneser/Schrijver formulas are ridiculously hard for current SAT/IP solvers.

Conjecture

Sch_n^2 has superpolynomial (lower bounds on) cutting-plane proofs.

Not true for PHP.

The plot thickens

Theorem (ABBCI)

For every fixed k, formulas Kneser_n^k have poly-size extended Frege proofs and quasi-poly-size Frege proofs.

In other words: One can reduce all Kneser_n^k to a finite number of values of n. No algebraic topology required !

Proof idea

Assume there is 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 $|C_l \leq k^2\binom{n-2}{k-2}$.

$n > k^4$, $\binom{n}{k} > (n-2k+1)\binom{n-2}{k-2}$, 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

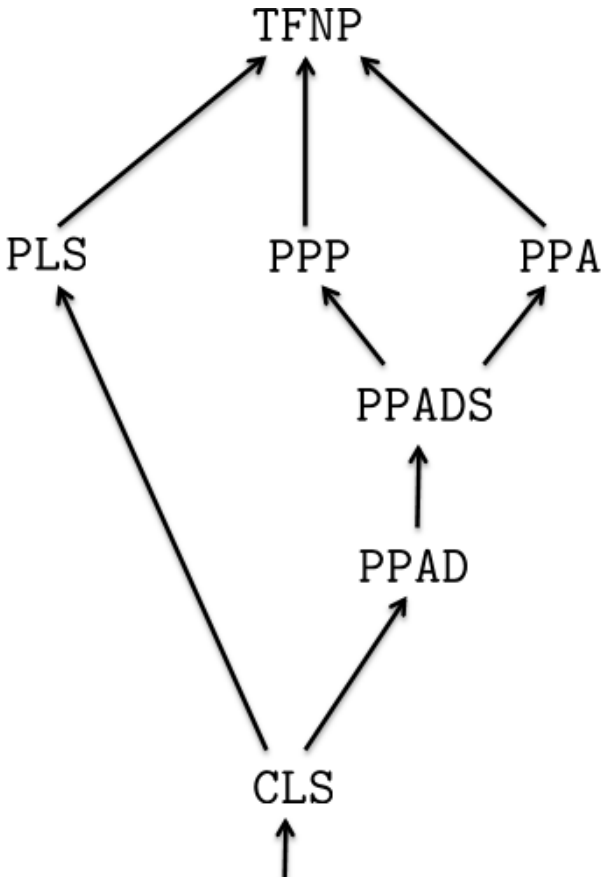
Let C_l be a non-star-shaped color class.

- Fix some $S = \{a_1, ..., a_k\} \in C_l$.
- For every a_i let $S_i \in P_l$, $a_i \notin C_l$ (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 ?

- Mathematically: Kneser follows from Borsuk-Ulam. (octahedral Tucker-lemma)
- Sperner: PPAD-complete, Borsuk-Ulam: PPAD(?)-complete.



Complexity of (nonconstructive) search principles

PPA:

Any undirected graph with degrees ≤ 2 which has a vertex of degree 1 has another vertex of degree 1.

PPAD:

Any directed graph with in-/out-degrees ≤ 1which has a vertex of total degree 1 has another vertex of total degree 1.

Graph: exponential size, given implicitly by a circuit/oracle which computes the adj. list of a given vertex.

A 20 year-old mistake in a classic paper of Papadimitriou.

Found by Aisenberg, Buss, Bonet.

Borsuk-Ulam not complete for PPAD, but for harder class PPA !

Mistake: BU $\notin$ PPAD.

on the complexity of the parity argument and other inefficient... https://scholar.google.ro/scholar?q=on+the+complexity+of+t...

On the complexity of the parity argument and other inefficient proofs of existence

CH Papadimitriou - Journal of Computer and system Sciences, 1994 - Elsevier

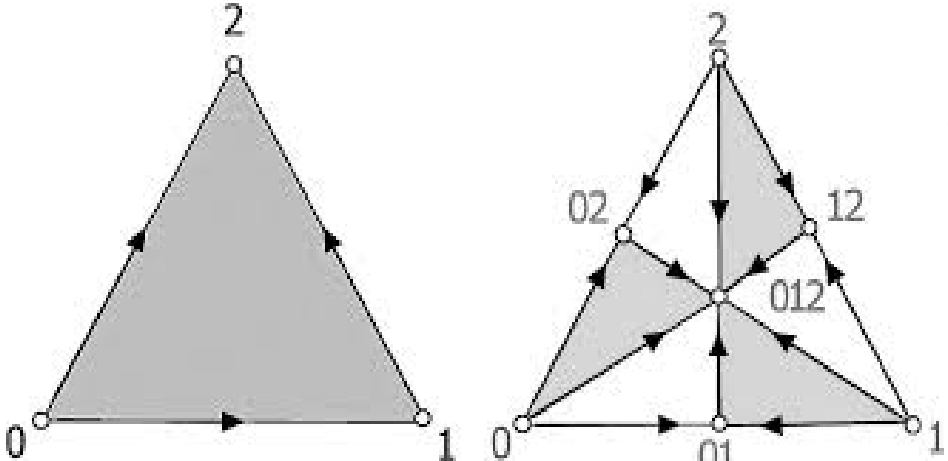
We define several new complexity classes of search problems," between" the classes FP and FNP. These new classes are contained, along with factoring, and the class PLS, in the class TFNP of search problems in FNP that always have a witness. A problem in each of these new classes is defined in terms of an implicitly given, exponentially large graph. The existence of the solution sought is established via a simple graph-theoretic argument with ...

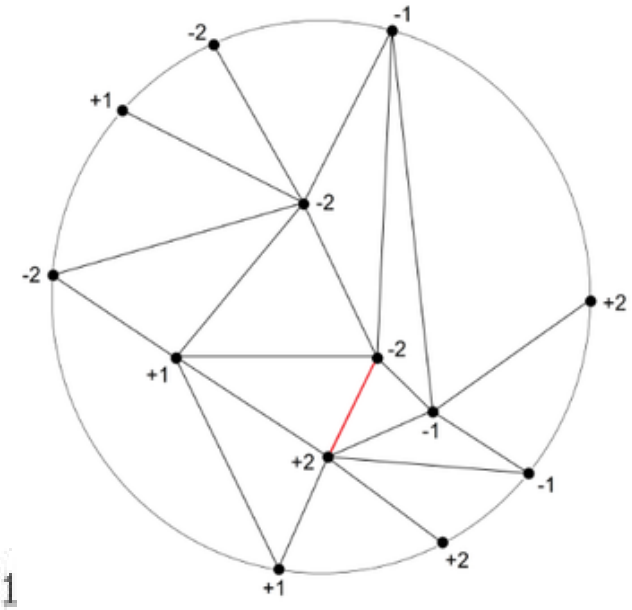
Citat de 565 ori Articole cu conţinut similar Toate cele 15 versiuni Citaţi Salvat Mai multe

Se afișează cel mai bun rezultat pentru această căutare. Afișați toate rezultatele

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

- Antipodally Symmetric Triangulation T of the n-ball. Barycentric subdivision, one vertex for each face
- 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 $c(v) = -c(w)$.
- Intuition: no continuous (a.k.a simplicial) antipodal map from the n-ball to the n-sphere.





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 $A_1 \subseteq A_2$, $B_1 \subseteq B_2$ 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 dimension $\Rightarrow$ exponentially large formula !

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

- Kneser follows from a new "low dim." 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:

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

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

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.

- Follows from "ordinary" octahedral Tucker lemma.
- k-truncated Tucker Implies Kneser_k.
- Translates (naturally) to formulas Truncated^k_n.
- Generates search problem Truncated_k.

Complexity of Truncated Tucker Lemma

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

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

THEOREM: (Aisenberg) Tucker_k hard for PPP.

CONCLUSION: Kneser_k may not be "hard", but Tucker_k (that encodes the topological principle) probably is !

Further work & Open 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 ?

Philosophical Open problem

Proof complexity for SMT ?

Thank you. Questions ?