Proof complexity of the Kneser-Lovász theorem

James Aisenberg
Joint work with: Maria Luisa Bonet, Sam Buss, Adrian Crăciun, and Gabriel Istrate

University of California, San Diego

Proof Complexity Workshop, St. Petersburg, 2016

Today's topic: Separation problem for Frege and extended Frege.

Open Problem: Is there a family of tautologies $\{\phi_1, \phi_2, \ldots\}$ with polynomial size extended Frege proofs that requires exponential size Frege proofs?

Many people believe the answer is "yes" because they also believe in an exponential separation between Boolean formula/circuit size.

- Each line of a Frege proof is a Boolean formula.
- Each line of an extended Frege proof is a Boolean circuit.
- But, connection to separating formulas/circuits isn't precise.

Question: What tautologies could provide the separation?

Conjectured problems separating Frege and extended Frege

Many combinatorial principles have been proposed to exponentially separate Frege and extended Frege systems:

Tautology	Poly. size extended Frege Proof	(Quasi)poly. size Frege Proof
Pigeonhole principle	[Cook-Reckhow '79]	[Buss '87]
Ramsey's Theorem	[Krishnamurthy '85]	[Pudlák '92]
Frankl's Theorem	[Bonet-Buss-Pitassi '95]	[A-Bonet-Buss '15]
Matrix identities	[Soltys-Kulinicz '01]	[Hruběs-Tzameret '13]
Local Improvement	[Beckmann-Buss '14]	Open
Kneser-Lovász	[Istrate-Crăciun '14]	[ABBCI '15]
Tucker lemma	[ABBCI '15]	Open

Today we'll talk about the last two lines of the table.

Kneser Graphs

Kneser-Lovász bounds the chromatic number of Kneser graphs.

Definition: The (n, k)-*Kneser graph* is the undirected graph with vertex set $\binom{n}{k}$ and $\{S, T\}$ is an edge iff $S \cap T = \emptyset$.

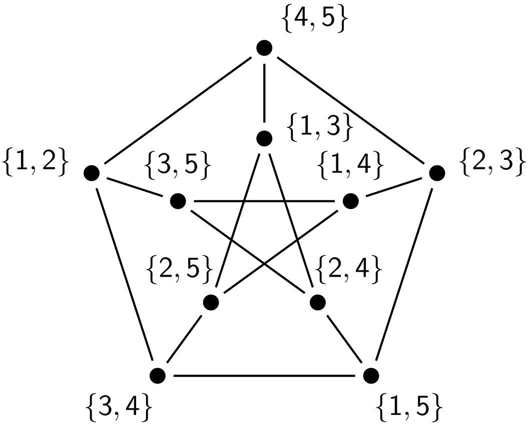

Figure: The $(5, 2)$-Kneser graph.

The Kneser-Lovász theorem

Theorem (Lovász '78)

Let $n \geq 2k > 1$. The (n, k)-Kneser graph has no coloring with $(n - 2k + 1)$ colors.

Lovász's proof:

- goes through the Borsuk–Ulam theorem, and
- pioneered the use of topological methods in combinatorics.

Theorem (Borsuk–Ulam '33)

If $f : S^n \to \mathbb{R}^n$ is continuous, then there is an $x \in S^n$ such that $f(-x) = f(x)$.

[Matoušek '04] gave a more combinatorial proof of KLT using the Tucker lemma, a discrete form of the Borsuk–Ulam theorem.

Propositional translation of the Kneser-Lovász theorem

Propositional variable $p_{S,i} = \top$ means vertex S is assigned color i.

The formula Kneser_k^n is:

$$\bigwedge_{S \in \binom{n}{k}} \bigvee_{i \in [m]} p_{S,i} \rightarrow \bigvee_{\substack{S,T \in \binom{n}{k} \\ S \cap T = \emptyset}} \bigvee_{i \in [m]} (p_{S,i} \wedge p_{T,i}) \,.$$

For fixed k, these formulas are polynomial size in n.

For $m = n - 2k + 1$, these formulas are tautologies.

Prior work and our contribution

Prior work:

Theorem (Istrate-Crăciun)

The formulas Kneser_2^n *have polynomial size Frege proofs and the formulas* Kneser_3^n *have polynomial size extended Frege proofs.*

Our contribution:

Theorem

For fixed $k \geq 1$*, the formulas* Kneser_k^n *have polynomial size extended Frege proofs.*

Theorem

For fixed $k \geq 1$*, the formulas* Kneser_k^n *have quasipolynomial size Frege proofs.*

Proof outline

We prove the Kneser-Lovász theorem by infinite descent.

- For $n > k^4$:
  - Given: $(n - 2k + 1)$-coloring of $\binom{n}{k}$
  - Produce: $((n - 1) - 2k + 1)$-coloring of $\binom{n-1}{k}$
  - How: Eliminate one "star-shaped" color class.
- Repeat until we have a $(k^4 - 2k + 1)$-coloring of $\binom{k^4}{k}$.
- Exhaustively check all possible such colorings of $\binom{k^4}{k}$.
- By the Kneser-Lovász theorem, there are no such colorings.

Key concept: Star-shaped color classes

Fix a coloring of the (n, k)-Kneser graph with m colors.

- Let P_ℓ be the set of vertices assigned color ℓ.
- No two elements of P_ℓ can be disjoint.
- One way for this to happen is if $\cap P_\ell \neq \emptyset$.
- Such P_ℓ's are called *star-shaped*.

Star-shaped color classes allow for one round of infinite descent:

- Suppose P_ℓ is star-shaped, with $i \in \cap P_\ell$.
- Discard vertices containing i. This discards color ℓ.
- Remaining subgraph is $(m-1)$-colorable, isomorphic to $\binom{n-1}{k}$.

Such P_ℓ's exist (next two slides)

Non-stars are small

Theorem

Let P_ℓ be a color class of $\binom{n}{k}$ with $\cap P_\ell = \emptyset$, then $|P_\ell| \leq k^2\binom{n-2}{k-2}$.

Proof.

Take any $S_0 = \{a_1, \ldots, a_k\} \in P_\ell$. Since $\cap P_\ell = \emptyset$, there are $S_1, \ldots, S_k \in P_\ell$ with $a_i \notin S_i$ for $i = 1, \ldots, k$.

To specify an arbitrary element $T \in P_\ell$:

1. Specify some $a_i \in S_0 \cap T \neq \emptyset$.
2. Specify some $b \in S_i \cap T \neq \emptyset$, note: $a_i \neq b$.
3. Specify $k-2$ elements from remaining $n-2$ possible values.

Thus, $|P_\ell| \leq k^2\binom{n-2}{k-2}$. □

We could have also used [Erdős-Ko-Rado '61], which gives slightly worse bounds, or [Hilton–Milner '67], which gives better bounds.

Star-shaped color classes exist.

We just showed that non-star P_ℓ's have $|P_\ell| \in O(n^{k-2})$.

By contrast, if P_ℓ is star-shaped, then $|P_\ell| \in O(n^{k-1})$.

Lemma

For $n > k^4$, any coloring of the (n,k)-Kneser graph with $n - 2k + 1$ colors has at least one star-shaped color class.

Proof: (sketch)

Suppose no color classes are star-shaped.

- $O(n)$ many color classes
- $O(n^{k-2})$ many vertices in each
- But there are $\binom{n}{k} \in \Omega(n^k)$ vertices in total.

Formalization in (extended) Frege

For extended Frege:

- Frege systems can carry out the counting arguments above, using the counting techniques introduced by [Buss '87].
- Extension rule can define a violation of Kneser_k^{n-1} from a violation of Kneser_k^n
- The small instances ($n \leq k^4$) are handled by exhaustive enumeration of cases.

For Frege:

- More careful counting: there are many star-shaped colors.
- Eliminate many star-shaped colors in parallel: requires only logarithmically many rounds of descent

"QED" poly. size extended Frege proofs of KLT, and quasipoly. size Frege proofs of KLT.

But can Frege systems reason topologically?

Our Frege proofs of KLT bypass topological arguments.

So the question remains: can Frege systems reason topologically?

We introduce new principle, the Truncated Tucker lemma:

- Write prop. translations of Truncated Tucker as Tucker_k^n.
- For fixed k, Tucker_k^n is poly. size
- There are poly size. Frege proofs of Kneser_k^n from Tucker_k^n

Special case: Truncated Tucker principle for $k = 1$.

Let A be an $(n+1) \times (n+1)$ matrix with the following properties

- The matrix elements a_{ij} are in the set $\{\pm 1, \ldots, \pm(n-1)\}$
- Every off-diagonal a_{ij} has $a_{ij} = -a_{ji}$.

Say that two matrix elements a_{ij} and $a_{i'j'}$ are *related* if

- Both a_{ij} and $a_{i'j'}$ are off-diagonal,
- $i \leq i'$ and $j \leq j'$, and
- $i \neq j'$ and $j \neq i'$.

Theorem (Truncated Tucker, $k = 1$ case)

For any matrix A as above, there are two related matrix elements a_{ij} and $a_{i'j'}$ with $a_{ij} = -a_{i'j'}$.

Example

Here is an example where $n = 6$.

	1	2	3	4	5	6	7
1	x	-4	5	-4	1	1	-3
2	4	x	**5**	-1	5	3	5
3	-5	**-5**	x	-5	5	2	2
4	4	1	**5**	x	5	5	5
5	-1	-5	-5	-5	x	2	2
6	-1	-3	-2	-5	-2	x	-3
7	3	-5	-2	**-5**	-2	3	x

The red ± 5 's are not related (not what we want).

The blue ± 5 's are related (what we want).

Truncated Tucker, continued

Theorem (ABBCI '15)

Tucker_1^n *has polynomial size extended Frege proofs.*

Open question:

- Does Tucker_1^n have subexponential size Frege proofs?
- Does Tucker_k^n for $k > 1$ have subexponential size (extended) Frege proofs?

Kneser and Truncated Tucker are also TFNP problems. Many open questions there!

Thank you!

Bonus slide: Erdős-Ko-Rado

A set $\mathcal{F} \subseteq \binom{n}{k}$ is an *intersecting family* if $A, B \in \mathcal{F} \Rightarrow A \cap B \neq \emptyset$.

Theorem (EKR '61)

If $n \geq 2k$ and $\mathcal{F} \subseteq \binom{n}{k}$ is an intersecting family, then $|\mathcal{F}| \leq \binom{n-1}{k-1}$. Furthermore, if $\cap\mathcal{F} = \emptyset$, then $|\mathcal{F}| \leq k^3.\binom{n-2}{k-2}$

Theorem (Hilton–Milner '67)

If $n \geq 2k$ and $\mathcal{F} \subseteq \binom{n}{k}$ is an intersecting family with $\cap\mathcal{F} = \emptyset$, then $|\mathcal{F}| \leq 1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1}$