Compositionality and Proof Complexity

Gabriel Istrate, Cosmin Bonchiş, Adrian Crãciun
West University of Timişoara and the e-Austria Research Institute

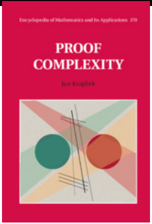
gabrielistrate@acm.org

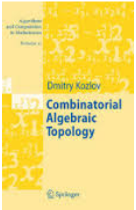
ICALP 2021 paper + subsequent research.

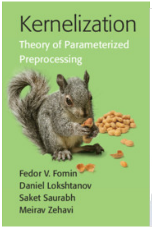
Take-home message

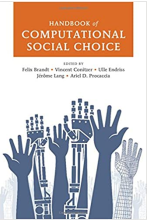
- Proof complexity is often compositional: if π_1 is a proof of $P \models Q$ and π_2 a proof of $Q \models R$ then $[\pi_1; \pi_2]$ is (often) a proof of $P \models R$.
- Caution: **"composition of proofs" (especially size) not that trivial.**
- This often allows to turn kernelizations (parameterized complexity) into proofs in various propositional proof systems.
- Technically interesting part: **what kind** of kernelizations needed to obtain "efficient" proofs ("theory A")

A Tapas of Prerequisites









- How notions from parameterized complexity can help us obtain efficient propositional proofs.
- Application to proof complexity of statements from computational social choice

Caution: Emphasis on philosophy, rather than technical details. Only present <u>some</u> of the results.

Reminder: Propositional proof complexity

- Proof systems for unsatisfiability, e.g. resolution
- $C \vee x, D \vee \overline{x} \rightarrow (C \vee D)$; $x, \overline{x} \rightarrow \Box$. Complexity = minimum length of a proof.
- More powerful proof system @ boundaries of proof complexity: Frege proofs. For concreteness [Hilbert Ackermann]
  - propositional variables $p_1, p_2, \ldots$., connectives $\neg, \vee$.
  - Axiom schematas:
    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.
- Other systems, sequent calculus (LK), etc. All Frege proof systems equivalent (polynomially simulate eachother) S.A.

Cook,R. Reckhow. *"The relative efficiency of propositional proof systems."* J. Symb. Logic 44.1(1979):36-50.

Frege versus extended Frege

- extended Frege: Frege + variable substitutions $X \leftrightarrow \Phi(\overline{Y})$. Proves same formulas, perhaps more efficiently.
- **Open:** $\boxed{\text{Is extended Frege more powerful than Frege ?}}$

  Bonet, M.L., S. Buss, T. Pitassi. "Are there hard examples for Frege systems?." Feasible Mathematics II. Birkhauser, 1995. 30-56.
- Most natural formulas turn out to have (quasi)polynomial Frege proofs.
- Some examples: "$(AB = I) \Rightarrow (BA = I)$" tautologies [Hrubeš, Tzameret CCC'2009], Paris-Harrington tautologies [Carlucci, Galesi, Lauria. CCC, 2011], Frankl Theorem [Buss et al. 2014].

Two-minute parameterized complexity

- Many problems in (co)-NP actually parameterized. E.g. Vertex Cover: Given graph G and integer k, decide whether G has VC of size at most k.
- **Parameterized complexity:** (fixed parameter) tractability = time $O(f(k) \cdot poly(n))$.
- Often achieved via **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}.

In practice, **to propositionally simulate proof by data reduction:**

- Φ_i constructed from Φ_{i-1} by "case construction"; cases translate to tautology $\bigvee_{l=1}^{r_i} \eta_i^{(l)}$. **Also need its proof.**
- Data reduction rule with case construction proves $\Phi_{i-1}(X_{i-1}, k_{i-1}) \wedge \eta_i^{(l)} \vdash \Phi_i^{(l)}(Y_i^{(l)}, k_i^{(l)})$ for some variable substitution $Y_i^{(l)} = \Xi_i^{(l)}(X_{i-1}, k_{i-1})$.

Main idea (II)

- Data reduction $\Rightarrow$ tree of propositional entailments. Don't really need tree for individual formulas, but doesn't hurt for our use cases.
- For Frege proofs: height of the tree dictates proof size (need to unwind variable substitutions).
- Proof: proofs of entailments + proofs of case tautologies + proofs of "brute force statements" (kernel instances).
- If tree arity is upper bounded by constant R then $\#$nodes=$\Theta(2^{\Theta(h)})$. As long as $h = O(\log n)$ this is polynomial.
- Formula growth due to unwinding: $\Theta(n^{\Theta(h)})$. As long as $h = O(\log n)$ this is quasipolynomial in n.

Main (meta)Theorem

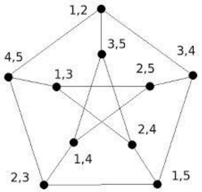
- Somewhat **too complicated to precisely state**.
- If soundness of reduction rules can be witnessed efficiently in Frege, the length of reduction chains is $O(1)$ then unsatisfiable formulas $\Phi(x,k)$ have polynomial size Frege proofs.
- If soundness of reduction rules can be witnessed efficiently in Frege, the length of reduction chains is $O(log(|\Phi(x,k)|))$ then unsatisfiable formulas $\Phi(x,k)$ have quasipolynomial Frege proofs.
- otherwise we normally get polynomial size extended Frege proofs.

Application: Proof Complexity of Schrijver's Theorem

Kneser's Conjecture: 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 $c(A) = c(B)$. M. Kneser(1955). Aufgabe 360. Jahresbericht der Deutschen Mathematiker-Vereinigung, 2, 27.

- $k = 1$ Pigeonhole principle !
- $k = 2, 3$ combinatorial proofs. S. Stahl. *"n-Tuple colorings and associated graphs."* J. Combinatorial Theory, Ser. B 20.2 (1976): 185-203. M. Garey, D.S. Johnson. *"The complexity of near-optimal graph coloring."* J. ACM 23.1 (1976): 43-49.
- $k \geq 4$ only proved in 1977 (Lovász, Baranyi) using Algebraic Topology.
- "Combinatorial" proofs (Matousek, Ziegler). "hide" Alg. Topology
- No efficient, "purely combinatorial" proof was known

Schrijver's Theorem



- Kneser: the chromatic number of a certain graph $Kn_{n,k}$ at least $n-2k+2$. (exact value). V: $\binom{n}{k}$. E: disjoint sets.
- E.g. $k=2$, $n=5$: Petersen's graph has chromatic # 3. Note: inner cycle already chromatic # 3.
- $A \in \binom{n}{k}$ stable if it doesn't contain consecutive elements $i, i+1$ (including $n, 1$).
- Schrijver's Theorem: Chromatic number of **stable Kneser graph** is $n-2k+2$. A. Schrijver. *Vertex-critical Subgraphs of Kneser-graphs.* N. Archief Wiskunde XXVI (1978), 454-461.

Proof Complexity of Schrijver's Theorem

- We proposed to study proof complexity of Kneser-Lovász Theorem in SAT'14 paper. $k = 2$ **poly size Frege proofs**. $k = 3$ **poly size Extended Frege.**
- We showed (ICALP'2015 $\Rightarrow$ Information & Computation'2018): For every fixed k formulas $Kneser_{n,k}$ have **poly size Extended Frege proofs** and **quasipoly size Frege proofs.**
- Proof idea: for every fixed k Kneser's theorem has an easy combinatorial proof that reduces the general case to the (computer verification) of a finite number of cases.

Theorem
Similar results hold for formulas encoding (the stronger) Schrijver theorem.

- Proof idea: data reduction of length $O(\log n)$.

Critical ingredient

We show that $\Theta(n)$ color classes c are star-shaped, i.e. sets colored with color c have an element in common. For that we need a weaker version of a result of Talbot (Intersecting families of separated sets. Journal of the London Mathematical Society, 68(1):37?51, 2003) that can be simulated propositionally:

Theorem
If $\mathcal{C}$ is a color class that is not star-shaped then $|\mathcal{C}| \leq k^2 \cdot \binom{n+k-1}{k-2}$.

Thus if there were a $n - 2k + 1$ coloring c of $SKn_{n,k}$ then we could drop $r = \Theta(n)$ elements of $\{1, 2, \ldots, n\}$ and equally many colors, and reduce the problem to showing that $\chi(SKn_{n-r,k}) > n - r - 2k + 1$.

Applications of Kernelization Techniques to Proof Complexity

- 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 with parameter k extended Frege proofs of poly size .**

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.*

Conclusions

- Theoretically interesting connections between different areas.
- Work in progress:
  - Adapt this program to other techniques from parameterized complexity, e.g. iterative compression.
  - Adapt this program to other proof systems, e.g. SPR^{-} (Heule,Kiesl & Biere HVC'17, J. Autom. Reasoning '19, Buss & Thapen SAT'19).
  - Proof system that only preserves equisatisfiability, **not equivalence**
- Proof complexity lower bounds for hard problems in parameterized complexity ?

Thanks !