Propositional Proofs in Frege and Extended Frege Systems (Abstract)

Sam Buss*

Department of Mathematics
University of California, San Diego
La Jolla, California 92130-0112, USA
sbuss@math.ucsd.edu
http://math.ucsd.edu/~sbuss

Abstract. We discuss recent results on the propositional proof complexity of Frege proof systems, including some recently discovered quasipolynomial size proofs for the pigeonhole principle and the Kneser-Lovász theorem. These are closely related to formalizability in bounded arithmetic.

Keywords: Proof complexity, Frege proofs, pigeonhole principle, Kneser-Lovász theorem, bounded arithmetic

1 Introduction

The complexity of propositional proofs has been studied extensively both because of its connections to computational complexity and because of the importance of propositional proof search for propositional logic and as an underpinning for stronger systems such as SMT solvers, modal logics and first-order logics. Frege systems are arguably the most important fully expressive, sound and complete proof system for propositional proofs: Frege proofs are "textbook" propositional proof systems usually formulated with modus ponens as the sole rule of inference. Extended Frege proofs allow the use of the extension rule which permits new variables to be introduced as abbreviations for more complex formulas [27].

(This abstract cannot do justice to the field of propositional proof complexity. There are several surveys available, including [25, 4, 12, 13, 5, 23].)

We will measure proof complexity by counting the number of symbols appearing in a proof. We are particularly interested in polynomial and quasipolynomial size Frege and extended Frege proofs, as these represent proofs of (near) feasible size. Frege proofs are usually axiomatized with modus ponens and a finite set of axiom schemes. However, there are a number of other natural ways to axiomatize Frege proofs, and they are all polynomially equivalent [15, 24]. Thus, Frege proof

* Supported in part by NSF grants CCF-121351 and DMS-1101228, and a Simons Foundation Fellowship 306202.

systems are a robust notion for proof complexity. The same holds for extended Frege proofs.

Formulas in a polynomial size Frege proof are polynomial size of course, and hence express (nonuniform) NC^1 properties. By virtue of the expressiveness of extension variables, formulas in polynomial size extended Frege proofs represent polynomial size Boolean *circuits*.[1] Boolean circuits express nonuniform polynomial time (P) predicates. It is generally conjectured $\mathrm{NC}^1 \neq \mathrm{P}$ and that Boolean circuits are more expressive than Boolean formulas, namely that converting a Boolean circuit to a Boolean formula may cause an exponential increase in size. For this reason, it is generally conjectured that Frege proofs do not polynomially or quasipolynomially simulate extended Frege proofs:

Definition 1. *The* size $|P|$ *of a proof P is the number of occurrences of symbols in P. Frege proofs* polynomially simulate *extended Frege proofs provided that there is a polynomial $p(n)$ such that, for every extended Frege proof P_1 of a formula φ there is a Frege proof P_2 of the same formula φ with $|P_2| \leq p(|P_1|)$.*

Frege proofs quasipolynomially simulate *extended Frege proofs if the same holds but with $p(n) = 2^{\log n^{O(1)}}$.*

However, the connection between the proof complexity of Frege and extended Frege systems and the expressiveness of Boolean formulas and circuits is only an analogy. There is no known direct connection. It could be that Frege proofs can polynomially simulate extended Frege proofs but Boolean formulas cannot polynomially express Boolean circuits. Likewise, it could be that Boolean formulas can express Boolean circuits with only a polynomial increase in size, but Frege proofs cannot polynomially simulate extended Frege proofs.

Bonet, Buss, and Pitassi [7] considered the question of what kinds of combinatorial tautologies are candidates for exponentially separating proof sizes for Frege and extended Frege systems, that is for showing Frege systems do not polynomially or quasipolynomially simulate extended Frege systems. Surprisingly, only a small number of examples were found. The first type of examples were based on linear algebra, and included the Oddtown Theorem, the Graham–Pollack Theorem, the Fisher Inequality, the Ray-Chaudhuri–Wilson Theorem, and the $AB = I \Rightarrow BA = I$ tautology (the last was suggested by S. Cook). The remaining example was Frankl's Theorem on the trace of sets.

The five principles based on linear algebra were known to have short extended Frege proofs using facts about determinants and eigenvalues of 0/1 matrices. Since there are quasipolynomial size formulas defining determinants over 0/1 matrices, [7] conjectured that all these principles have quasipolynomial size Frege proofs. This was only recently proved by Hrubeš and Tzameret [16], who showed that the five linear-algebra-based tautologies have quasipolynomial size Frege proofs by showing that there are quasipolynomial size definitions of determinants whose properties can be established by quasipolynomial Frege proofs.

[1] See Jeřábek [18] for an alternative formulation of extended Frege systems based directly on Boolean circuits.

The remaining principle, Frankl's Theorem, was shown to have polynomial size extended Frege proofs by [7], but it was unknown whether it had polynomial size Frege proofs. Recently, Aisenberg, Bonet and Buss [1] showed that it also has quasipolynomial size Frege proofs. Thus, Frankl's theorem does not provide an example of tautologies which exponentially separate Frege and extended Frege proofs.

Istrate and Crãciun [17] recently proposed the Kneser-Lovász Theorem as a family of tautologies that might be hard for (extended) Frege systems. They showed that the $k = 3$ versions of these tautologies have polynomial size extended Frege proofs, but left open whether they have (quasi)polynomial size Frege proofs. However, as stated in Definition 3 and Theorem 5 below, [2] have now given polynomial size extended Frege proofs and quasipolynomial size Frege proofs for the Kneser-Lovász tautologies, for each fixed k. Thus these also do not give an exponential separation of Frege from extended Frege systems.

Other candidates for exponentially separating Frege and extended Frege systems arose from the work of Kołodziejczyk, Nguyen, and Thapen [19] in the setting of bounded arithmetic [9]. They proposed as candidates various forms of the local improvement principles LI, $\mathrm{LI}_{\log}$ and LLI. The results of [19] include that the LI principle is many-one complete for the NP search problems of V_2^1; it follows that LI is equivalent to partial consistency statements for extended Frege systems. Beckmann and Buss [6] subsequently proved that $\mathrm{LI}_{\log}$ is provably equivalent (in S_2^1) to LI and that the linear local improvement principle LLI is provable in U_2^1. The LLI principle thus has quasipolynomial size Frege proofs. Combining the results of [6, 19] shows that $\mathrm{LI}_{\log}$ and LLI are many-one complete for the NP search problems of V_2^1 and U_2^1, respectively, and thus equivalent to partial consistency statements for extended Frege and Frege systems, respectively.

Cook and Reckhow [14] showed that the partial consistency statements for extended Frege systems characterize the proof theoretic strength of extended Frege systems; Buss [11] showed the same for Frege systems. For this reason, partial consistency statements do not provide satisfactory *combinatorial* principles for separating Frege and extended Frege systems. The same is true for other statements equivalent to partial consistency statements. (But, compare to Avigad [3].)

This talk will discuss a pair of recently discovered families of quasipolynomial size Frege proofs. The first is based on the pigeonhole principle; the second on the Kneser-Lovász principle.

Definition 2. *The propositional pigeonhole principle* PHP_n^{n+1} *is the tautology*

$$\bigwedge_{i=0}^{n} \bigvee_{j=0}^{n-1} p_{i,j} \quad \rightarrow \quad \bigvee_{0 \le i_1 < i_2 \le n} \bigvee_{j=0}^{n-1} (p_{i_1,j} \wedge p_{i_2,j}).$$

Theorem 1. (Cook-Reckhow [15]) PHP_n^{n+1} *has polynomial size extended Frege proofs.*

Theorem 1 was proved by a induction proof. Later, the following was proved by using a "counting" proof:

Theorem 2. ([10]) PHP_n^{n+1} *has polynomial size Frege proofs.*

Since the proofs of Theorems 1 and 2 were so different, this was sometimes taken as evidence that Frege proofs cannot polynomially simulate extended Frege proofs. However, recently the present author showed that the proof of Theorem 1 can be carried out with Frege proofs, and established a weaker result, but with a proof based on the proof of [15]:

Theorem 3. ([8]) PHP_n^{n+1} *has quasipolynomial size Frege proofs.*

This is weaker than Theorem 2: the point is that its proof shows that the construction underlying the proof of Theorem 1 can be carried by quasipolynomial size Frege proofs.

We next state the results about the Kneser-Lovász principle.

Definition 3. *Fix $k \geq 1$. Let $\binom{n}{k}$ denote the set of subsets of $[n] := \{0, \ldots, n-1\}$ of cardinality k. The* (n,k)-Kneser graph *is the undirected graph (V, E) where the vertex set V is the set $\binom{n}{k}$, and E is the set of edges $\{A, B\}$ such that $A, B \in \binom{n}{k}$ and $A \cap B = \emptyset$.*

It is not hard to show that the (n,k)-Kneser graph can be colored with $n-2k+2$ colors. (That is, so that no two adjacent vertices receive the same color.) This is the optimal number of colors:

Theorem 4. (Lovász [21]) *Let $k \geq 1$ and $n \geq 2k$. The (n,k)-Kneser graph cannot be colored with $n-2k+1$ colors.*

Note that the $k = 1$ case of the Theorem 4 is just the usual pigeonhole principle.

It is straightforward to translate the Kneser-Lovász principle as expressed by Theorem 4 into a family of polynomial size tautologies:

Definition 4. *Let $n \geq 2k > 1$, and let $m = n - 2k + 1$ be the number of colors. For $A \in \binom{n}{k}$ and $i \in [m]$, the propositional variable $p_{A,i}$ has the intended meaning that vertex A of the Kneser graph is assigned the color i. The Kneser-Lovász principle is expressed propositionally by*

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

Theorem 5. ([2]) *For each $k \geq 1$, the tautologies based on the Kneser-Lovász principle have polynomial size extended Frege proofs and quasipolynomial size Frege proofs.*

The proof of Theorem 5 is based on a simple counting argument which avoids the usual topologically-based combinatorial arguments of Matoušek [22] and others.

As already discussed, we now lack many good combinatorial candidates for super-quasipolynomially separating Frege and extended Frege systems, apart from partial consistency principles or principles which are equivalent to partial consistency principles. At the present moment, we have only a couple potential combinatorial candidates. The first candidate is the rectangular local improvement principles RLI_2 (or more generally, RLI_k for any constant $k \geq 2$). For the definitions of these in the setting of bounded arithmetic, plus characterizations of the logical strengths of the related principles RLI_1, $\mathrm{RLI}_{\log}$ and RLI, see Beckmann-Buss [6]. RLI_1 is provable in U_2^1 and is many-one complete for the NP search problems of U_2^1, and thus has quasipolynomial size Frege proofs (for the latter connection, see Krajíček [20]). $\mathrm{RLI}_{\log}$ and RLI are provable in V_2^1 and are many-one complete for the NP search problems of V_2^1; hence they are equivalent to partial consistency statements for extended Frege. The second candidate is the truncated Tucker lemma defined by [2]. These are actively under investigation as this abstract is being written; some special cases are known to have extended Frege proofs [Aisenberg-Buss, work in progress], but it is still open whether they has quasipolynomial size Frege proofs.

It seems very unlikely however that Frege proofs can quasipolynomially simulate extended Frege proofs.

We thank Lev Beklemishev and Vladimir Podolskii for helpful comments.

References

1. Aisenberg, J., Bonet, M.L., Buss, S.: Quasi-polynomial size Frege proofs of Frankl's theorem on the trace of finite sets (201?), to appear in Journal of Symbolic Logic
2. Aisenberg, J., Bonet, M.L., Buss, S., Crăciun, A., Istrate, G.: Short proofs of the Kneser-Lovász principle (2015), to appear in Proc. 42th International Colloquium on Automata, Languages, and Programming (ICALP'15)
3. Avigad, J.: Plausibly hard combinatorial tautologies. In: Beame, P., Buss, S.R. (eds.) Proof Complexity and Feasible Arithmetics, pp. 1–12. American Mathematical Society (1997)
4. Beame, P.: Proof complexity. In: Computational Complexity Theory, pp. 199–246. IAS/Park City Mathematical Series, Vol. 10, American Mathematical Society (2004), lecture notes scribed by Ashish Sabharwal
5. Beame, P., Pitassi, T.: Propositional proof complexity: Past, present and future. In: Paun, G., Rozenberg, G., Salomaa, A. (eds.) Current Trends in Theoretical Computer Science Entering the 21st Century, pp. 42–70. World Scientific (2001), earlier version appeared in *Computational Complexity Column*, Bulletin of the EATCS, 2000.
6. Beckmann, A., Buss, S.R.: Improved witnessing and local improvement principles for second-order bounded arithmetic. ACM Transactions on Computational Logic 15(1) (2014), article 2, 35 pages

7. Bonet, M.L., Buss, S.R., Pitassi, T.: Are there hard examples for Frege systems? In: Clote, P., Remmel, J. (eds.) Feasible Mathematics II. pp. 30–56. Birkhäuser, Boston (1995)
8. Buss, S.: Quasipolynomial size proofs of the propositional pigeonhole principle (201?), to appear in *Theoretical Computer Science*
9. Buss, S.R.: Bounded Arithmetic. Bibliopolis (1986), revision of 1985 Princeton University Ph.D. thesis
10. Buss, S.R.: Polynomial size proofs of the propositional pigeonhole principle. Journal of Symbolic Logic 52, 916–927 (1987)
11. Buss, S.R.: Propositional consistency proofs. Annals of Pure and Applied Logic 52, 3–29 (1991)
12. Buss, S.R.: Propositional proof complexity: An introduction. In: Berger, U., Schwichtenberg, H. (eds.) Computational Logic, pp. 127–178. Springer-Verlag, Berlin (1999)
13. Buss, S.R.: Towards NP-P via proof complexity and proof search. Annals of Pure and Applied Logic 163(9), 1163–1182 (2012)
14. Cook, S.A., Reckhow, R.A.: On the lengths of proofs in the propositional calculus, preliminary version. In: Proceedings of the Sixth Annual ACM Symposium on the Theory of Computing. pp. 135–148 (1974)
15. Cook, S.A., Reckhow, R.A.: The relative efficiency of propositional proof systems. Journal of Symbolic Logic 44, 36–50 (1979)
16. Hrubeš, P., Tzameret, I.: Short proofs for determinant identities. SIAM J. Computing 44(2), 340–383 (2015)
17. Istrate, G., Crăciun, A.: Proof complexity and the Kneser-Lovász theorem. In: Theory and Applications of Satisfiability Testing (SAT). pp. 138–153. Lecture Notes in Computer Science 8561, Springer Verlag (2014)
18. Jeřábek, E.: Dual weak pigeonhole principle, boolean complexity, and derandomization. Annals of Pure and Applied Logic 124, 1–37 (2004)
19. Kołodziejczyk, L.A., Nguyen, P., Thapen, N.: The provably total NP search problems of weak second-order bounded arithmetic. Annals of Pure and Applied Logic 162(2), 419–446 (2011)
20. Krajíček, J.: Bounded Arithmetic, Propositional Calculus and Complexity Theory. Cambridge University Press, Heidelberg (1995)
21. Lovász, L.: Kneser's conjecture, chromatic number, and homotopy. Journal of Combinatorial Theory, Series A 25(3), 319 – 324 (1978)
22. Matoušek, J.: A combinatorial proof of Kneser's conjecture. Combinatorica 24(1), 163–170 (2004)
23. Pudlák, P.: Twelve problems in proof complexity. In: Computer Science — Theory and Applications. pp. 13–27. Lecture Notes in Computer Science #5010, Springer, Berlin, Heidelberg (2008)
24. Reckhow, R.A.: On the Lengths of Proofs in the Propositional Calculus. Ph.D. thesis, Department of Computer Science, University of Toronto (1976), technical Report #87
25. Segerlind, N.: The complexity of propositional proofs. Bulletin of Symbolic Logic 13(4), 417–481 (2007)
26. Siekmann, J., Wrightson, G.: Automation of Reasoning, vol. 1&2. Springer-Verlag, Berlin (1983)
27. Tsejtin, G.S.: On the complexity of derivation in propositional logic. Studies in Constructive Mathematics and Mathematical Logic 2, 115–125 (1968), reprinted in: [26, vol 2], pp. 466-483.