Are there Hard Examples for Frege Systems?

Maria Luisa Bonet   Samuel R. Buss*   Toniann Pitassi†

Abstract

It is generally conjectured that there is an exponential separation between Frege and extended Frege systems. This paper reviews and introduces some candidates for families of combinatorial tautologies for which Frege proofs might need to be superpolynomially longer than extended Frege proofs. Surprisingly, we conclude that no particularly good or convincing examples are known. The examples of combinatorial tautologies that we consider seem to give at most a quasipolynomial speed-up of extended Frege proofs over Frege proofs, with the sole possible exception of tautologies based on a theorem of Frankl.

It is shown that Bondy's theorem and a version of the Kruskal-Katona theorem actually have polynomial-size Frege proofs. Bondy's theorem is shown to have constant-depth, polynomial-size proofs in Frege+PHP, and to be equivalent in $I\Delta_0$ to the pigeonhole principle.

1 Introduction

Frege systems are schematic, propositional proof systems; for instance, a Frege system can have modus ponens as its sole rule of inference. Extended Frege systems are Frege systems augmented with the ability to introduce new variables which abbreviate long formulas. As usual, the length of a propositional proof is defined to be equal to the number of symbols appearing in the proof. Most researchers conjecture that a Frege system cannot polynomially simulate an extended Frege system; that is to say, that there is no polynomial $p(n)$ so that for every extended Frege proof of length n there is a Frege proof of the same conclusion with length $\leq p(n)$. Indeed, the usual conjecture is that there is an exponential separation of Frege and extended Frege systems; more precisely, that for some $\epsilon > 0$, there are extended Frege proofs of arbitrarily large length n, so that any Frege proof of the same conclusion requires length at least 2^{n^ϵ}. On the other hand, no *super-linear* lower bounds on Frege proof lengths have yet been established for *any* tautology. See [11, 12, 31] for background material on Frege and extended Frege proof systems.

* Supported in part by NSF grant DMS-9205181.
† Supported by NSF postdoctoral fellowship and UC Presidential fellowship.

Although the authors tend to support these conjectures on the separation of Frege and extended Frege systems, the purpose of this paper is to cast doubt on these conjectures by pointing out that there are hardly any good examples to support them. This is in marked contrast to the situation for analogous open questions in computational complexity such as "$P\!=?NP$" and "$NC\!=?P$". For these open questions, there are a large number of candidates which are conjectured to separate the two classes. In particular, there are a large number of combinatorial problems that are known to be NP-complete (or P-complete) and therefore are not in P (or not in NC, respectively) if $P \neq NP$ (or $NC \neq P$, respectively). In fact, the widely accepted conjecture that NC, P and NP are distinct is largely based upon the existence and apparent intractability of these combinatorial problems.

Consider also the problem of separating constant-depth Frege proofs from Frege proofs. In this situation, there are several natural combinatorial principles, including the pigeonhole principle and various matching principles, which are known to have polynomial-size Frege proofs and yet require exponential-size constant-depth Frege proofs [4, 1, 27, 19].

It is thus desirable to seek natural, *combinatorial* problems that are candidates for separating Frege and extended Frege proof systems. By this we mean tautologies based on combinatorial principles which are known to have polynomial-size extended Frege proofs, and for which the shortest known Frege proofs are exponential (or at least superpolynomial) in length. In addition, we wish the tautologies to be "natural"; of course, the naturalness of a family of tautologies is a matter of personal opinion, but at the very least it should mean that they are uniform in some strong sense, such as being polynomial-time recognizable, or, even better, the family of tautologies should consist of the propositional translations of an arithmetic formula with existential, universal and/or counting (bounded) quantifiers. The latter kind of uniform tautologies can sometimes have strongly uniform proofs which are obtained from proofs in bounded arithmetic: in particular, Paris-Wilkie [25] gave a translation of $I\Delta_0$-proofs into polynomial-size (quasipolynomial-size), constant depth Frege proofs; Cook [10] gave a translation of PV-proofs (and thus S^1_2-proofs, by conservativity) into polynomial-size extended Frege proofs; and Krajíček [17] gave a translation of U^1_1-proofs into quasipolynomial-size Frege proofs.

In order to give a superpolynomial separation of Frege and extended Frege proofs, it is of course necessary to give superpolynomial lower bounds for Frege proofs. Already, the problem of finding natural, combinatorial principles which require superpolynomial-size Frege proofs seems difficult. It is well-known that there are tautologies that require superpolynomial Frege (and extended Frege) proofs, unless $NP = coNP$ [11]. However, the set of all tautologies does not yield a natural, combinatorial family of candidates for superpolynomial Frege proofs; because it is neither combinatorial nor believed to be a polynomial-time recognizable set.

A number of authors have already investigated the problem of finding natural, combinatorial tautologies which separate Frege and extended Frege systems. Foremost among these is the pigeon-hole principle introduced in [12, 20]: in [12] is was shown to have polynomial-size extended Frege proofs and only later, in [4], was it shown to have polynomial-size Frege proofs. Krishnamurthy and Noll [22] suggested the Ramsey theorem as a source of hard tautologies and Krishnamurthy [21] established that a version of Ramsey's theorem has polynomial-size extended Frege proofs. Recently, Pudlák has shown that a version of Ramsey's theorem also has polynomial-size Frege proofs [28]. Krishnamurthy [21] also showed that a number of other tautologies, such as the parity principle, have polynomial-size extended Frege proofs; however, it is now known that these also have polynomial-size Frege proofs (using the counting techniques of [4]). Thus none of these examples provide any evidence for an exponential separation of Frege and extended Frege proof systems.

There is a well-known analogy between the question of separating Frege and extended Frege systems and the question of separating NC^1 from P. Namely, the lines in a polynomial-size Frege proof consist of polynomial-size propositional formulas and it is known that polynomial-size formulas can express precisely properties in (nonuniform) NC^1 [30, 3, 7, 6]. Likewise, because of the ability to use abbreviations for long formulas, the lines in a polynomial-size extended Frege proof are essentially polynomial-size circuits and thus can express properties that are in nonuniform P [23]. Thus, one can intuitively view polynomial-size Frege proofs as proofs with polynomially many steps which can reason with NC^1 properties; whereas polynomial-size extended Frege proofs are proofs with polynomially many steps which can reason with properties in nonuniform P. Of course this analogy between Frege and extended Frege systems and NC^1 and P does not entail any actual implication, that is to say it is possible that Frege and extended Frege are polynomially equivalent and NC^1 and P are unequal (or vice-versa). Nonetheless, one might be able to use this analogy to search for combinatorial principles which can be conjectured to separate Frege and extended Frege systems; namely, by considering combinatorial principles whose proofs depend on properties that are P-complete.

We consider in this paper various candidates for separating Frege and extend Frege and discuss their relative merits and disadvantages. In section 2, we consider tautologies based on consistency statements. In section 3.1, we discuss a number of combinatorial properties whose proofs are based on linear algebra: since matrix inversion and determinant computation are not known to be in NC^1, these are thus candidates for a superpolynomial separation of Frege and extended Frege systems. However, since matrix inverses and determinates are in NC^2, these candidates are conjectured to have quasipolynomial-size Frege proofs, where 'quasipolynomial' means $2^{(\log n)^{O(1)}}$. Note that quasipolynomial-sizes are both subexponential and superpolynomial. In section 3.2, we introduce Frankl's theorem; this is the *only* example we have of combinatorial tautologies which are known to have polynomial-size extended Frege proofs and for which we have no reason to suspect that they have subexponential-size Frege proofs. In section 3.3, some tautologies based on a formalization of the "P vs. NP" problem are discussed. In section 4, we approach the problem in a different direction, by giving polynomial-size Frege proofs for some combinatorial tautologies, thereby showing they are not good examples for separating Frege and extended Frege systems. In section 4.1, we give a polynomial-size Frege proofs for Bondy's principle. Bondy's principle was originally suggested to us by Krajíček [16, 9] as a candidate for an exponential separation between Frege and extended Frege systems; however, we give a new proof of Bondy's theorem which, unlike prior proofs, translates into polynomial-size Frege proofs. In section 4.2, we further discuss Frankl's theorem, which is a generalization of Bondy's theorem. Although we have been unable to find polynomial-size Frege proofs of Frankl's theorem, we are able to give polynomial-size Frege proofs of a version of the Kruskal-Katona theorem which is used in the usual proof of Frankl's theorem.

2 Hard examples based on Consistency

Given any propositional proof system, S, one can write out a tautology, $Con_S(n)$, which expresses the partial consistency of S in a natural fashion; namely, this tautology expresses the fact that there are no proofs of length at most n in S of a contradiction. For commonly used proof systems, a partial consistency statement is expressed as a tautology by letting a proof of length n be encoded as a string of binary digits of length $O(n)$; the tautology contains propositional variables representing the bits in the encoded string and expresses the property that the bits do not encode a correct S-proof ending with a contradiction. Since valid S-proofs are, by definition, recognizable in polynomial time, the partial consistency tautologies can always be formulated to have length polynomially bounded by n. Partial consistency tautologies of this type for propositional logic were first described by Cook [10] in the setting of extended Frege provability. Cook established that if S is any schematic propositional proof system such that there are polynomial-size extended Frege proofs of $Con_S(n)$, then extended Frege systems can polynomially simulate S. Later, one of the authors extended this theorem to apply to Frege systems as well, by establishing that the existence of polynomial-size Frege proofs of $Con_S(n)$ implies that a Frege system can polynomially simulate S [5]. These theorems establish that for sufficiently powerful proof systems such as Frege systems, there are sparse families of *complete* tautologies (see also [18]). In particular, we have that the family of tautologies $Con_{eF}(n)$ are complete tautologies for Frege systems with respect to extended Frege systems:

Theorem 1 [5] *There are polynomial-size Frege proofs of the tautologies $Con_{eF}(n)$ if and only if Frege systems can polynomially simulate extended Frege systems.*

Cook showed that the statements $Con_{eF}(n)$ have polynomial-size extended Frege proofs, thus Theorem 1 implies that the partial consistency statements $Con_{eF}(n)$ separate Frege and extended Frege systems, unless the systems are actually equivalent. In fact, it is clear that, up to polynomial factors, these tautologies provide the best separation of Frege and extended Frege systems that is possible. However, we do not view these tautologies as providing evidence for a superpolynomial separation of Frege and extended Frege systems. Instead, we are seeking more natural, combinatorial principles which are hard for Frege systems but not extended Frege systems. Of course, it is possible to take any $coNP$-complete combinatorial property and encode a tautology as an instance of that combinatorial property; for instance, one can encode a tautology as a graph which is not 3-colorable, then reexpress the non-3-colorability of this graph as a tautology. But, this is not what we consider a natural combinatorial problem.

3 Hard Combinatorial Candidates

3.1 Examples based on Linear Programming

There are several combinatorial theorems which are simple to state, but all known proofs rely on the powerful tools of linear algebra. These theorems are prime candidates for tautologies that should require superpolynomial-size Frege proofs. Many examples from this section, including Theorems 2-8, can be found in the excellent expository monograph by Babai and Frankl [2].

3.1.1 The Odd-town Theorem

The Odd-town Theorem is perhaps the original example of the power of linear algebra in combinatorics:

Theorem 2 *Suppose a town has n citizens and that there is a set of clubs, each consisting of citizens, such that each club has an odd number of members and such that every two clubs have an even number of members in common. Then there are no more than n clubs.*

To express this theorem propositionally for a particular n, we use underlying variables v_i^j, $i \leq n+1$, $j \leq n$, where the n-bit vector v_i is intended to describe the i^{th} club. The propositional formula OT_n states that either some vector contains an even number of 1's, or there are two vectors with an odd number of 1's in common. (This formula requires nonconstant depth to express, but the size is still polynomial in n.)

The simplest proof of this theorem uses linear algebra. Assume there are m clubs, $C_1, \ldots, C_m$. We represent the m clubs by an n by m incidence matrix, M, where the i^{th} row vector, v_i, is the incidence vector for club C_i. The inner product modulo 2 of v_i and v_j, $\langle v_i, v_j \rangle$, is equal to 1 if size of the intersection of C_i and C_j is odd, and is equal to 0 otherwise. According to the Odd-town rules, $\langle v_i, v_j \rangle$ is odd whenever $i = j$, and $\langle v_i, v_j \rangle$ is even whenever $i \neq j$. We claim that the vectors $v_1, \ldots, v_m$ must therefore be linearly independent. If not, there exist numbers λ_i such that $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0$ with some $\lambda_k \neq 0$. Taking the inner product of both sides of the equation with v_k, it follows that $\lambda_k = 0$, which is a contradiction. Since the v_i's are linearly independent, m is at most n.

The key point of the above proof is that it relies on linear algebra, and despite considerable effort, there are no known simpler proofs that circumvent the use of linear algebra. In order to carry out the above proof propositionally, one would need to prove the fact that if $m > n$, m vectors cannot be linearly independent. In the most straightforward approach, this would involve giving polynomial-size formulas defining the values λ_i in terms of entries of the incidence vectors. Furthermore, the smallest known formulas defining these values are quasipolynomial-size, i.e., $2^{(\log n)^{O(1)}}$ size, since operations such as finding determinants and matrix inverses are in NC, but are not known to be in NC^1. Thus, our *conjecture* is that the Odd-town Theorem tautologies have quasipolynomial-size Frege proofs. This is only a conjecture, since we have not verified that Frege proofs can formalize properties about the NC-computable functions of linear algebra.

On the other hand, there are polynomial-size extended Frege proofs of the propositional tautologies expressing the Odd-town Theorem. This is because an extended Frege system can easily simulate Gaussian elimination on a matrix, and thereby can prove that $m > n$ vectors must be linearly dependent.

The Odd-town Theorem thus serves as a good combinatorial candidate for quasipolynomially separating Frege and extended Frege systems. There has reportedly been a great deal of effort made to find proofs that do not depend on linear algebra; and this provides at least some evidence that the shortest Frege proofs of the Odd-town Theorem tautologies require quasipolynomial-size.

In sections 3.1.2-3.1.4, we give a number of combinatorial principles that have proofs based on linear algebra. Like the Odd-town Theorem, the tautologies based on these combinatorial principles all have polynomial-size extended Frege proofs and we conjecture that they have quasipolynomial-size Frege proofs.

3.1.2 The Graham-Pollak Theorem

This candidate was suggested to us by Mauricio Karchmer (personal communication).

Theorem 3 *[15] The number of edge disjoint, complete bipartite graphs needed to edge cover K_n (the complete graph on n vertices) is at least $n-1$.*

To express this theorem propositionally, we introduce $2n(n-2)$ propositional variables, A^i_j, B^i_j, $i \leq n$, $j \leq n-2$, where for each $j \leq n-2$, the pair of vectors A_j and B_j describe the j^{th} bipartite graph. (The edge (k_1, k_2) is present in the j^{th} bipartite graph if and only if $A^{k_1}_j \wedge B^{k_2}_j$ or $A^{k_2}_j \wedge B^{k_1}_j$.) The Graham-Pollak tautology for a fixed n, GP_n, states (informally) that either: (1) one of the pairs A_j, B_j does not describe a proper bipartite graph; or (2) there exists $i, j \leq n-2$, $i \neq j$ and an edge e such that e is present both in (A_i, B_i) and in (A_j, B_j); or (3) there exists an edge e that is not present in any (A_i, B_i), $i \leq n-2$. It can be verified that this tautology has size $O(n^4)$.

The known proof of the Graham-Pollak theorem, presented below, does not seem to be formalizable with polynomial-size Frege proofs.

Proof Associate with each vertex i of K_n a variable x_i. Assume (A_i, B_i) $i = 1, .., r$ are the bipartite graphs partitioning K_n and $r \leq n-2$. Then we have

$$\begin{aligned} (\sum_i x_i)^2 &= (\sum_i x_i^2) + 2(\sum_{i<j} x_i x_j), && (1) \\ &= (\sum_i x_i^2) + 2[\sum_\ell (\sum_{i \in A_\ell} x_i)(\sum_{j \in B_\ell} x_j)]. && (2) \end{aligned}$$

Now consider the following system of $r+1$ linear equations: (a) $\sum_i x_i = 0$ and (b) $\sum_{i \in A_\ell} x_i = 0$ for $\ell = 1, .., r$, $r \leq n-2$. The number of underlying variables is n, and the number of equations is $r+1$ which is less than n. Therefore, there exists a nontrivial solution. But this cannot be since the left hand side of (2) is zero, and the second term of the right hand side of (2) is zero, but a nontrivial solution would imply that the remaining term, $\sum_i x_i^2$ is not equal to zero. □

3.1.3 The Fisher Inequality

Theorem 4 (Fischer Inequality) *Let $F_1, \ldots, F_m$ be a system of distinct, nonempty subsets of $\{1,..,n\}$ such that for all F_i, F_j, $|F_i \cap F_j| = k$, for some fixed k. Then $m \leq n$.*

Proof Associate a vector v_i with each F_i, where v_i is the incidence vector of F_i. Let $\langle v_i, v_j \rangle$ denote the inner product of v_i and v_j. The inner product will equal the size of $F_i \cap F_j$. Therefore when $i \neq j$, $\langle v_i, v_j \rangle = k$, and when $i = j$, then $\langle v_i, v_i \rangle$ equals the size of F_i. Without loss of generality, we can assume that $|F_i| > k > 0$, for all i, and therefore $\langle v_i, v_i \rangle = k + \gamma_i$, where $\gamma_i > 0$.

Claim: The vectors $v_1, .., v_m$ are linearly independent.

Proof of claim: Assume for sake of contradiction that the claim does not hold. Then $\sum_i \alpha_i v_i = 0$, where not all α_i's are zero. But then we have $\sum_{k=1}^n \langle \alpha_k v_k, v_j \rangle = 0$. This can be written as $\beta k + \alpha_j \gamma_j = 0$, where $\beta = \sum_i \alpha_i$. Now if β is zero, then $\alpha_j = 0$ for all j, which contradicts our assumption. Therefore, $\beta \neq 0$; but since $k, \gamma_i > 0$, we have that each α_j is non-zero and has sign opposite the sign of β. This is impossible since $\beta = \sum_i \alpha_i$.

It follows from the above claim that $m \leq n$. □

3.1.4 Ray-Chaudhuri–Wilson theorem

The following theorem is a generalization of the Fischer Inequality. Let $[n]$ denote $\{1, \ldots, n\}$. Let F be a set of subsets of $[n]$, and let $L \subset [n]$, $|L| = s$. F is L*-intersecting* if for all $F_1 \neq F_2$, $|F_1 \cap F_2| \in L$. For example, in the previous Fischer theorem, $L = \{k\}$.

Theorem 5 (Nonuniform Ray-Chaudhuri–Wilson) *For any $L \subset Z$, $|L| = s$, if F is L-intersecting, then $|F| \leq \sum_{i=0}^s \binom{n}{i}$.*

We say that F is k*-uniform* provided every member of F has cardinality k. In this case, we get a better upper bound on the size of F:

Theorem 6 (Uniform Ray-Chaudhuri–Wilson) *Let* L *be a set of integers,* $|L| = s$ *, and* F *be an* L*-intersecting* k*-uniform family. Then* $|F| \leq \binom{n}{s}$ *.*

The following theorem is a modular form of the Ray-Chaudhuri–Wilson theorem.

Theorem 7 (Modular Ray-Chaudhuri–Wilson) *Let* p *be a prime number and* $L \subset \{0, \ldots, p-1\}$ *have cardinality* $s \leq p-1$ *. Let* $0 \leq k < p$ *be an integer,* $k \notin L$ *. Let* F *be a family of subsets of* n *elements,* $n \geq s+k$ *, such that for all* i *,* $|F_i| \equiv k \bmod p$ *, and for all* $i \neq j$ *,* $(|F_i \cap F_j| \bmod p) \in L$ *. Then* $|F| \leq \binom{n}{s}$ *.*

Note that the Odd-town Theorem is a special case of the above theorem where $p = 2$, $k = 0$ and $L = \{1\}$. Our final potentially hard tautology based on linear algebra proofs is a generalization of the Odd-town Theorem. This example was suggested to us by L. Babai.

Theorem 8 (Skew Odd-town Theorem) *Suppose there are* m *red clubs* $R_1, \ldots, R_m$ *, and* m *blue clubs,* $B_1, \ldots, B_m$ *in a town of* n *citizens. Assume that these clubs satisfy: (a)* $|R_i \cap B_i|$ *is odd for every* i *; (b)* $|R_i \cap B_j|$ *is even for* $1 \leq i < j \leq m$ *. Then* $m \leq n$ *.*

3.1.5 When can linear algebra be avoided?

While all known proofs of the above theorems rely on linear algebra at some point, it appears to be a difficult problem to determine when a theorem inherently requires the use of linear algebra. In fact, it may be that all of the above examples actually have short, direct proofs. The following theorem, known as the Friendship Theorem, is another example of a combinatorial principle whose standard proof relies on linear algebra. In fact, the authors originally believed that this was another potentially hard example.

Theorem 9 *[13] In a party of* n *people, suppose that every pair of people has exactly one friend in common. Then there is a person at the party who is friends with everyone.*

For a fixed n, we encode the Friendship Theorem using $n(n-1)$ propositional variables, F_{ij} , $1 \leq i < j \leq n$, where F_{ij} indicates whether or not persons i and j are friends. The propositional Friendship Theorem, $Friend_n$, states that either there exists two people with zero or more than 1 friend in common, or there exists a person who is friends with everyone.

The original proof of this theorem is due to Erdős, Rényi and Sós [13]. This proof relies heavily on linear algebra and is not known to be formalizable with polynomial-size Frege proofs. For some years, no completely elementary proof was known, despite considerable effort. But in 1972, such a proof was found by Longyear and Parsons [24]. This proof builds upon an earlier paper of Herbert Wilf [32] where it is shown that the the negation of the Friendship Theorem implies that the group of friends forms a finite projective geometry. Then using elementary properties of finite projective geometry, the Friendship Theorem can be reduced to the special case where every person has the same number of friends. This case is simpler, and in [24], it is shown using elementary reasoning that if every person has the same number of friends, then the conditions of the Friendship Theorem fail to hold. Because this proof only uses direct reasoning, and a counting argument, it can be formalized with polynomial-size Frege proofs.

3.2 Frankl's Theorem

Another potential hard example is the propositional version of Frankl's theorem [14] stated next.

Theorem 10 *Let t be a positive integer and let $m \leq n^{\frac{(2^t-1)}{t}}$. Then for any $m \times n$ matrix of distinct rows of 0's and 1's, there is a column such that, if this column is deleted, the resulting $m \times (n-1)$ matrix will contain at most $2^{t-1}-1$ pairs of equal rows.*

The tautologies based on Frankl's theorem do have polynomial-size extended Frege proofs; however, it is an open question whether they have polynomial- or quasipolynomial-size Frege l-oofs. The only proof of Frankl's Theorem that we know of is due to Frankl [14], and a brief outline of his proof can be given as follows. Define a 0/1 matrix to be *hereditary* if all its rows are distinct and changing any 1 entry to a 0 causes two rows to become identical. Frankl first argues that it suffices to prove Theorem 10 for hereditary matrices by proving that any matrix violating the theorem can be transformed into a hereditary matrix violating the theorem (this is Theorem 1 of [14]). He then gives a proof of the theorem for hereditary matrices, based a corollary to the Kruskal-Katona theorem and on a counting argument.

We have examined Frankl's proof carefully, and have been able to show that the propositional tautologies based on the corollary to the Kruskal-Katona theorem do have polynomial-size Frege proofs (we present this in detail in section 4.2 below), and the counting argument likewise has a polynomial-size Frege proofs. Thus there are polynomial-size Frege proofs of Theorem 10 under the extra assumption that the matrix is hereditary. However, the reduction to hereditary matrices is readily seen to be formalizable in extended Frege proofs, but we see no way in which a Frege proof can formalize this reduction (Theorem 1 of [14]) with subexponential-size proofs. The difficult aspect of the reduction to hereditary matrices is that it involves a sequential process of changing 1's to 0's in a column-by-column fashion, repeated until the matrix is hereditary. The sequential nature of this reduction makes it easy to express with polynomial-size extended Frege proofs, but not with small Frege proofs.

There are two special cases of Frankl's theorem worth mentioning. The first is when $t = 1$ and $m \leq n$; this case is Bondy's theorem and is shown in section 4.1 to have polynomial-size Frege proofs. The second is when $t = 2$ and $m \leq 3n/2$: we have not been able to find subexponential-size Frege proofs even for this case.

3.3 Formalizing circuit lower bounds

Our last example comes from tautologies which formalize circuit lower bounds. It has recently been observed by several people [29, 26] that all explicit circuit lower bounds seem to require proof strength that is strictly greater than the circuit family under consideration. Loosely, it can be shown that known lower bounds for a particular circuit class C require reasoning about formulas with complexity greater than C. These observations lead one to ask whether the family of tautologies expressing $P \neq NC^1$ require superpolynomial-size Frege proofs, and similarly, whether the tautologies expressing $P \neq NP$ require superpolynomial-size extended Frege proofs. In this section, we address this possibility.

The first issue is how to express circuit lower bounds such as $P \neq NP$, propositionally. The following approach was suggested by Steve Cook. NP has polynomial circuit size if and only if there is a function f_{SAT} computable with polynomial-size circuits such that given any satisfiable formula F (we can assume that F is in $3CNF$), $f_{SAT}(F)$ is a truth assignment which satisfies F.

To code the above statement, we will code 3SAT on n variables using $O(n^3)$ propositional variables, each variable corresponding to the presence or absence of a particular 3-clause in the formula. We will code a size $O(m)$ circuit, $m = n^c$, $(c > 3)$, with propositional variables p^i_j, $i \leq 2\log m$, $j \leq m$, where variables $p^0_j, \ldots, p^{2\log m}_j$ describe the jth gate of the circuit. We can then express "f_{SAT} does not have polynomial-size circuits" as follows: For all x, $|x| = n$, for all C, $|C| \leq n^c$, there exists a pair (F, T) such that: (a) F codes a 3CNF formula with n variables, (b) T is a satisfying assignment to F, and (c) The circuit coded by C on input F does not output a satisfying truth assignment (i.e., C does not compute

$f_{SAT}(F)$.)

In order to translate this statement into a propositional statement, we need to replace the existentially quantified variable (the pair (F,T)) by the disjunction of all possible values for (F,T). In other words, the tautology expressing "f_{SAT} does not have polynomial-size circuits" has underlying variables p_j^i, $0 \le i \le 2\log m$, $j \le m$, and the formula states that if the p_j^i's code a proper circuit, C, then there exists a formula coded by $f_1, \ldots, f_{n'}$, with satisfying truth assignment $x_1, \ldots, x_n$, such that when we evaluate C on $f_1, \ldots, f_{n'}$, it does not output a satisfying truth assignment. Because the total number of 3CNF formulas on n variables is roughly 2^{n^3}, this takes about $2^{O(n^3)}$ symbols; thus the entire tautology is expressible in $2^{O(n^3)}$ symbols. Let us call the above family of tautologies $NOTPOLY_n$, where n is the number of underlying variables.

The obvious way to prove this tautology is to go through all possible circuits of size m, and for each of them, check all possible $3CNF$ formulas on n variables, and exhaustively check that for each one, the circuit errs on some input. But this proof requires 2^m symbols, which is superpolynomial in the input length $(O(2^{n^3})$, for $m > n^3$. Recently, Razborov and Rudich proved that under certain cryptographic assumptions, a class of proofs of $NOTPOLY_n$ require superpolynomial-size extended Frege proofs. Proofs in this class are defined to be proofs satisfying certain natural properties, and hence are called "natural proofs". But it is still open whether "unnatural proofs" also require superpolynomial-size extended Frege proofs.

In a similar manner, we can generate the tautology which expresses "P does not have polynomial-size formulas", and this family of tautologies is a potential hard candidate for Frege systems.

4 Short Frege proofs for some Combinatorial Principles

In this section, we give new polynomial-size Frege proofs for two families of tautologies for which the previously known proofs were exponential-size. The first family of tautologies are based on Bondy's theorem, and the second family on a variant of the Kruskal-Katona theorem which is used in the proof of Frankl's theorem.

4.1 Bondy's Theorem and the Pigeonhole Principle

Bondy's theorem was suggested by Krajíček [16, 9] as a possible candidate for a combinatorial tautology with polynomial-size extended Frege proofs but with no Frege proofs. However, we give below a new, elementary proof of Bondy's theorem, which can be translated into the setting of propositional logic. This shows that the tautologies expressing Bondy's theorem actually do have polynomial-size Frege proofs. In fact, our proof shows an even stronger result; namely, that there are constant-depth polynomial-size proofs of the Bondy theorem tautologies in a Frege proof system augmented with additional axioms expressing the pigeonhole principle. Since the pigeonhole principle has polynomial-size Frege proofs [4], this implies that the Bondy's theorem tautologies have polynomial-size proofs.*

Bondy's theorem states that, in any $n \times n$ matrix containing n pairwise distinct rows, there exists a column such that, if the column is deleted, the resulting $(n-1) \times n$ matrix still has n pairwise distinct rows. Without loss of generality, we shall formulate Bondy's theorem for 0-1 matrices only (our arguments easily adapt to the general case, anyway). The version of the pigeonhole principle that we use states that, for $a > 0$, there is no one-to-one mapping from $[a]$ to $[a-1]$, where $[a]$ denotes the set $\{1, 2, 3, \ldots, a\}$.

Definition The propositional pigeonhole principle is stated with propositional variables $p_{i,j}$ which are intended to denote the property of pigeon i being mapped to hole j. The propositional pigeonhole principle is the family of tautologies of the form

$$\left(\bigwedge_{i=1}^{n+1} \bigvee_{k=1}^{n} p_{i,k} \right) \to \left(\bigvee_{i=1}^{n} \bigvee_{j=i+1}^{n+1} \bigvee_{k=1}^{n} (p_{i,k} \land p_{j,k}) \right)$$

which state that there is no one-to-one mapping from $[n+1]$ to $[n]$.

The tautologies expressing Bondy's theorem have propositional variables $p_{i,j}$ which have value *True* or *False* depending on whether a 1 or a 0 is in the (i,j) entry of the $n \times n$ matrix. These tautologies are:

$$\left(\bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} \bigvee_{k=1}^{n} \neg(p_{i,k} \leftrightarrow p_{j,k}) \right) \to \left(\bigvee_{k_0=1}^{n} \bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} \bigvee_{\substack{1 \le k \le n \\ k \ne k_0}} \neg(p_{i,k} \leftrightarrow p_{j,k}) \right)$$

We let *PHP* denote all substitution instances of the propositional pigeonhole principle tautologies; that is to say, *PHP* contains every formula obtained from a pigeonhole tautology with the variables $p_{i,j}$ uniformly replaced by arbitrary formulas $A_{i,j}$. Similarly *BONDY* denotes all substitution instances of the propositional tautologies expressing Bondy's

* We have been informed that that T. Arai has independently obtained the results of Theorems 11 and 12.

theorem. $\mathcal{F} + PHP$ and $\mathcal{F} + BONDY$ denote the propositional proof systems obtained by adding all PHP-formulas, or all $BONDY$-formulas, respectively, as additional axioms to the Frege system $\mathcal{F}$.

Theorem 11 *The tautologies (with variables $p_{i,j}$) expressing Bondy's theorem have constant-depth, polynomial-size proofs in $\mathcal{F} + PHP$. Conversely, the pigeonhole tautologies (with variables $p_{i,j}$) have constant-depth, polynomial-size proofs in $\mathcal{F} + BONDY$.*

Recall from [8] that the depth of a propositional formula is defined by counting the alternations of AND's and OR's in the formula (assuming that $\rightarrow$ has been expressed in terms of OR and NOT and that negations are pushed down to the leaves of the formula). A family of proofs is said to be constant-depth if there is a constant bounding the depths of all formulas appearing in the proofs. There is a well-known construction of Paris-Wilkie [25, Theorem 26] which translates proofs in bounded arithmetic into constant-depth Frege proofs; so instead of proving Theorem 11 directly, we shall state and prove the corresponding (and stronger) theorem for bounded arithmetic.

We now consider the equivalence between Bondy's principle and the pigeonhole principle in the setting of provability in $I\Delta_0$. Recall that $I\Delta_0$ is a first-order theory of bounded arithmetic with language containing the non-logical symbols $0, S, +, \cdot, \leq$, which is axiomatized with a finite set of bounded formulas defining the non-logical symbols, plus induction for all bounded formulas. To formulate Bondy's theorem in $I\Delta_0$, we suppose that there is an $a \times a$ matrix M with entries given by a binary relation $g(x, y)$. The relation $g(i, j)$ is intended to be true iff the (i, j) entry in M is 1. Bondy's principle for g is thus the following formula $Bondy(g)$:

$$\begin{aligned}(\forall x < a)(\forall y < a)(x \neq y \rightarrow (\exists z < a)(\neg(g(x,z) \leftrightarrow g(y,z)))) \rightarrow \\ (\exists z_0 < a)(\forall x < a)(\forall y < a)(x \neq y \\ \rightarrow (\exists z < a)(z \neq z_0 \wedge \neg(g(x,z) \leftrightarrow g(y,z)))).\end{aligned}$$

The pigeonhole principle is stated for a unary function h by the following formula $PHP(h)$:

$$(\forall x < a)(h(x) < a - 1) \rightarrow (\exists x < a)(\exists y < a)(h(x) = h(y) \wedge x \neq y).$$

Definition The first-order theory $I\Delta_0 + \Delta_0$-$Bondy$ is defined to be the theory $I\Delta_0$ plus $Bondy(g)$ for every Δ_0-formula g. The first-order theory $I\Delta_0 + \Delta_0$-PHP is defined to be the theory $I\Delta_0$ plus $PHP(h)$ for every Δ_0-defined function h.

Theorem 12 *The theories $I\Delta_0 + \Delta_0$-$Bondy$ and $I\Delta_0 + \Delta_0$-PHP are equivalent.*

Proof We first show the easier direction that the Δ_0 pigeonhole principle is provable in $I\Delta_0 + \Delta_0$-*Bondy* (this was first noted by Krajíček [16]). Suppose that h is a function with graph defined by a Δ_0-formula which maps $[a]$ one-to-one into $[a-1]$. Define an $a \times a$ matrix A by letting its (i,j)-entry equal 1 if and only if $h(j+1) = i+1$. (Note that we are indexing the columns and rows of A starting with zero, so $0 \le i < a$ and $0 \le j < a$.) Then A violates Bondy's principle. Thus we have shown that if the pigeonhole principle fails, then Bondy's theorem fails. This argument is clearly formalizable in $I\Delta_0$, and thus $I\Delta_0 + \Delta_0$-*Bondy* proves $PHP(f)$.

We now prove the harder direction that the Bondy principle *Bondy*(g), for g a Δ_0-predicate, is provable in $I\Delta_0 + \Delta_0$-PHP. For $0 \le x, z < a$, we have $g(x,z)$ is true iff the (x,z) entry of the matrix is equal to 1 (now numbering rows and columns of the matrix starting from zero). We think of each row as a string of 0's and 1's, which read from left-to-right, is the binary representation of a non-negative integer. We write $x \prec y$ to denote the condition that the number coded by row x is less than the number coded by row y; or formally, $x \prec y$ abbreviates the Δ_0-formula

$$(\exists z < a)[g(y,z) \wedge \neg g(x,z) \wedge (\forall z' < z)(g(x,z') \leftrightarrow g(y,z'))].$$

We write $x \preccurlyeq y$ as an abbreviation for

$$x \prec y \vee (\forall z < a)(g(x,z) \leftrightarrow g(y,z)).$$

The intuitive idea of our proof of Bondy's theorem is that if the n rows of the matrix are sorted according to $\prec$, and if, for each row except the first, we choose the first column where that row differs from the immediately preceding row, then those $n-1$ columns suffice to distinguish all n rows. We show next that this intuitive proof can be carried out in $I\Delta_0 + \Delta_0$-PHP; for this, we must avoid sorting the rows, but can still talk about the immediately $\prec$-preceding row.

Lemma 13 *Let $P(x)$ be a Δ_0-property, possibly with additional free variables. Then $I\Delta_0$ can prove*

(a) $(\exists x < a)P(x) \rightarrow (\exists x < a)(P(x) \wedge (\forall y < a)(P(y) \rightarrow x \preccurlyeq y)$, *and*

(b) $(\exists x < a)P(x) \rightarrow (\exists x < a)(P(x) \wedge (\forall y < a)(P(y) \rightarrow y \preccurlyeq x)$.

Of course this lemma says that $I\Delta_0$ can prove the maximization/minimization properties of Δ_0-predicates w.r.t. the $\preccurlyeq$ ordering of the rows.

Proof of Lemma 13. To prove part (a), let $M(a)$ denote the formula to be proved. Clearly $M(a)$ is a Δ_0-formula, and it is easy to see that $I\Delta_0$

can prove $M(1)$ and $(\forall u)(M(u) \to M(u+1))$. Thus, by induction, $I\Delta_0$ can prove $M(a)$. Part (b) is proved similarly. $\Box$

To prove Theorem 12, we shall argue informally in $I\Delta_0 + \Delta_0\text{-}PHP$, assuming that the hypothesis of $Bondy(g)$ holds:

$$(\forall x < a)(\forall y < a)(x \neq y \to (\exists z < a)(\neg(g(x,z) \leftrightarrow g(y,z)))).$$

First, using Lemma 13(a), there must be a row x_0 so that $(\forall x < a)(x_0 \preccurlyeq x)$. Using Lemma 13(b), we see that for all rows $x \neq x_0$, there is a unique row y so that $y \prec x$ and so that there is no row y' such that $y \prec y' \prec x$. We define $Pred(x)$ to be equal to this y. If we further define $Pred(x_0) = x_0$, then $Pred(x)$ is a total, Δ_0-defined function.

Let $x \neq x_0$; clearly there exists at least one column z such that

$$\neg(g(x,z) \leftrightarrow g(Pred(x),z)).$$

We define $Col(x)$ to be equal to the least such column z. We let $Col(x_0)$ be undefined. We write $z \in Col$ as an abbreviation for the Δ_0-formula

$$(\exists x < a)(x \neq x_0 \land z = Col(x)).$$

Claim: There is a $z_0 < a$ so that $z_0 \notin Col$.

Proof of claim: Suppose that the claim fails. Then a total function $h(z)$ can be Δ_0-defined by letting $h(z)$ equal the least $x < a$ such that $z = Col(x)$. But then h is a one-to-one map from $\{0, 1, \ldots, a-1\}$ into $\{0, 1, \ldots, a-1\} \setminus \{x_0\}$, which is easily seen to contradict the $\Delta_0\text{-}PHP$.

We are now ready to prove the conclusion of $Bondy(g)$. Let z_0 be the column from the claim. Let x, y be two rows with $y \prec x$. We must show that there is a column z such that $z \neq z_0$ and such that $\neg(g(x,z) \leftrightarrow g(y,z))$. Let z be the least value such that $\neg(g(x,z) \leftrightarrow g(y,z))$: we must show $z \neq z_0$. By Lemma 13(a), there is $\preccurlyeq$-minimum $x' < a$ such that

$$(\forall u \le z)(g(x',u) \leftrightarrow g(x,u))$$

holds, since x itself satisfies this condition. Note that $y \prec x'$. In particular,

$$y \preccurlyeq Pred(x') \prec x' \preccurlyeq x.$$

Since $(\forall u < z)(g(y,u) \leftrightarrow g(x,u))$, we have also

$$(\forall u < z)(g(Pred(x'),u) \leftrightarrow g(x',u).$$

Thus, from the definition of x', we have $g(x',u)$ and $\neg g(Pred(x'),u)$; which implies that $z = Col(x')$, so $z \in Col$ and $z \neq z_0$. $\Box$

Theorem 11 follows from Theorem 12 by the general Paris-Wilkie method of translating proofs in bounded arithmetic into polynomial-size, constant-depth Frege proofs. The essential idea of this translation in that universal and existential bounded quantifiers become conjunctions and disjunctions, respectively, and that a use of induction becomes a series of uses of modus ponens. In this way, our proof of Theorem 12 can be translated into a direct proof of Theorem 11.

4.2 Kruskal-Katona Theorem

In this section, we give polynomial-size Frege proofs of the corollary to the Kruskal-Katona Theorem that is used in the proof of Frankl's Theorem. We begin by stating the full Kruskal-Katona theorem, and state the corollary as Theorem 15.

Definition The *antilexicographic ordering* of subsets of $[n]$ is given by

$$A \prec B \Leftrightarrow A \subset B \text{ or } (A \not\supseteq B \text{ and } \max\{i : i \in A \backslash B\} < \max\{i : i \in B \backslash A\})$$

Thus, for instance, $\{2,3,4\} \prec \{1,2,5\}$.

Definition We can represent a set $\{S_1, \ldots, S_m\}$ of subsets of $[n]$ by an $m \times n$ matrix $\{a_{ij}\}_{ij}$ of 0's and 1's by letting $a_{ij} = 1$ if $j \in S_i$ and $a_{ij} = 0$ if $j \notin S_i$. This matrix is called *incidence matrix* of $\{S_1, \ldots, S_m\}$. A row representing a subset is called the *incidence vector* of the subset.

For the rest of this section matrices will have rows ordered from top to bottom in antilexicographical order, but will have columns in reverse order from right to left starting with column one. So, column one is the rightmost one and column n the leftmost one. With the columns of the incidence matrix ordered in this way, each incidence vector can be viewed as the binary representation of an integer, and the antilexicographic ordering corresponds to the usual ordering on the integers. For instance, the subset $\{1,2,5\}$ of $\{1,2,3,4,5\}$ is identified with the number with binary representation $(10011)_2$, which is 19 in base 10. Also, $\{2,3,4\}$ would be the integer with binary representation $(01110)_2$, which is 14 in base 10. Thus, $\{2,3,4\} \prec \{1,2,5\}$ holds since the former is less than the latter.

In this way a set of m subsets of $[n]$ can be represented as the set of integers $\{b_1, \ldots, b_m\}$, where b_i is the number with binary representation equal to the i-th row of the incidence matrix.

Notation The size of a row (incidence vector) is the number of 1's in the row. For an integer corresponding to such a row, we let the size of an integer be the number of ones in its binary representation. We write $|\{b_1, \ldots, b_m\}|_{\le k}$ to denote the number of b_i's of size $\le k$.

Definition A family of sets X is called *hereditary* if, whenever S is in X, then all subsets of S are also in X. A matrix is *hereditary* if it is the incidence matrix of a hereditary family of sets.

Theorem 14 (Kruskal-Katona) *Let $0 < \ell < k$. Let A be a collection of k sets of size m. Let B denote the first k sets of size m in the antilexicographic ordering. Then, the number of sets of size ℓ which are subsets of members of A is at least as large as the number of sets of size ℓ which are subsets of members of B.*

An important point is that the Kruskal-Katona theorem stated in the above form cannot be formalized with short propositional formulas; since there may be exponentially many sets of size ℓ which are subsets of members of A and B. However, the following corollary of the Kruskal-Katona theorem can be expressed with polynomial-size propositional formulas. Moreover, we will present a new proof of this second theorem and argue that our proof can be formalized by a uniform polynomial-size Frege proof.

Theorem 15 *Let $0 \le k \le n$. Let X be a hereditary family of subsets of $[n]$ of cardinality m. Then*

$$|X|_{\le k} \ge |\{0, \ldots, m-1\}|_{\le k}$$

We will first explain how to express Theorem 15 propositionally as a family of tautologies KK^n_m. Let X be a family of subsets of $[n]$. We encode X with the underlying variables p_{ij}, $i \le m$ and $j \le n$, where p_{ij} has the value True or False depending on whether a 1 or a 0 is in the (i,j) entry of the incidence matrix of X. The propositional formula, KK^n_m, states that either the set of subsets (described by the p_{ij}'s) is not hereditary, or two subsets are the same, or for all $k \le n$, $|X|_{\le k} \ge |\{0, \ldots, m-1\}|_{\le k}$. We can express the fact that the p_{ij}'s represent a hereditary family by the following formula:

$$\bigwedge_{1 \le i \le m} \bigwedge_{1 \le j \le n} (p_{ij} \to \bigvee_{\substack{1 \le \ell \le m \\ \ell \ne i}} (\neg p_{\ell j} \wedge \bigwedge_{\substack{1 \le k \le n \\ k \ne j}} p_{\ell k} \leftrightarrow p_{ik}))$$

The quantities $|X|_{\le k}$, and $|\{0, \ldots, m-1\}|_{\le k}$ can be expressed by small propositional formulas, using counting formulas (see [4]). Thus, the tautologies KK^n_m are expressible by polynomial-size formulas.

We next give a new, elementary proof of Theorem 15 based on the next two lemmas.

Lemma 16 *For all i, j and k,*

$$|\{0, \dots, i-1\}|_{\leq k} \geq |\{j, \dots, j+i-1\}|_{\leq k}$$

Proof by induction on i. The base case $i = 1$ is obvious. Suppose now that the lemma holds for all integers $< i$. To show the lemma for i, we have two cases depending on whether the sets of sequences $\{0, \dots, i-1\}$ and $\{j, \dots, j+i-1\}$ intersect or not.

Case 1: $j < i$. It clearly suffices to discard the intersection of $\{0, \dots, i-1\}$ and $\{j, \dots, j+i-1\}$ and show that

$$|\{0, \dots, j-1\}|_{\leq k} \geq |\{i, \dots, i+j-1\}|_{\leq k}$$

But this is immediate by the induction hypothesis since $j < i$.

Case 2: $j \geq i$. Choose k so that $2^k < i \leq 2^{k+1}$. The incidence matrix $\{0, \dots, i-1\}$ has 0's in columns $k+2$ through n, and in column $k+1$ it has 2^k 0's and $i - 2^k$ 1's. Choose $\ell \geq k$ so that $2^\ell \leq j < 2^{\ell+1}$. Case 2 divides into two cases depending on whether $i + j \leq 2^{\ell+1}$ or $i + j > 2^{\ell+1}$.

Case 2.1: $i + j \leq 2^{\ell+1}$. So the sequences $\{j, \dots, j+i-1\}$ have 1's in column $\ell+1$, and 0's in columns $\ell+2$ through n:

$$
\begin{array}{c|c|c|c|c|c|}
 & n & \ell+1 & & k+1 & 1 \\
\hline
0 & 0\cdots 0 & 0 & 0\cdots 0 & 0 & 0\cdots 0 \\
 & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & 0\cdots 0 & 0 & 0\cdots 0 & 0 & 1\cdots 1 \\
\cline{6-6}
2^k & 0\cdots 0 & 0 & 0\cdots 0 & 1 & 0\cdots 0 \\
 & \vdots & \vdots & \vdots & \vdots & \vdots \\
i-1 & 0\cdots 0 & 0 & 0\cdots 0 & 1 & \\
\hline
 & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
j & 0\cdots 0 & 1 & & & \\
 & \vdots & \vdots & \vdots & \vdots & \vdots \\
j+i-1 & 0\cdots 0 & 1 & & & \\
\hline
\end{array}
$$

Applying the induction hypothesis to the first 2^k members of $\{0, \dots, i-1\}$ and of $\{j, \dots, j+i-1\}$ yields

$$|\{0, \dots, 2^k - 1\}|_{\leq k} \geq |\{j, \dots, 2^k + j - 1\}|_{\leq k} \tag{3}$$

Also, we apply the induction hypothesis to the last $i - 2^k$ members of $\{0, \dots, i-1\}$ ignoring the $k+1$ column of 1's, and to the last $i - 2^k$ members of $\{j, \dots, j+i-1\}$ ignoring the $\ell+1$ column of 1's using $k-1$ in place of k. This yields

$$|\{0, \dots, i-2^k-1\}|_{\leq k-1} \geq |\{(j+2^k)-2^\ell, \dots, (j+2^k)-2^\ell+(i-2^k)-1\}|_{\leq k-1}$$

Hence,

$$|\{2^k, \dots, i-1\}|_{\leq k} \geq |\{2^k + j, \dots, i+j-1\}|_{\leq k}$$

which together with (3) implies this case of the lemma.

Case 2.2: $i + j > 2^{\ell+1}$. Let $j_2 = i + j - 2^{\ell+1}$ and $j_1 = i - j_2$. Thus, the last j_2 members in $\{j, \dots, j+i-1\}$ contain 1's in column $\ell+2$, and the first j_1 members have 0's in columns $\ell+2$ through n and 1's in column $\ell+1$. Note $j_2, j_1 > 1$.

	n	$\ell{+}2$	$\ell{+}1$		$k{+}1$	1
0	$0\cdots 0$	0	0	$0\cdots 0$	0	$0\cdots 0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$0\cdots 0$	0	0	$0\cdots 0$	0	$1\cdots 1$
2^k	$0\cdots 0$	0	0	$0\cdots 0$	1	$0\cdots 0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i-1$	$0\cdots 0$	0	0	$0\cdots 0$	1	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
j	$0\cdots 0$	0	1			
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j+j_1-1$	$0\cdots 0$	0	1	$1\cdots 1$	1	$1\cdots 1$
$2^{\ell+1}$	$0\cdots 0$	1	0	$0\cdots 0$	0	$0\cdots 0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j+i-1$	$0\cdots 0$	1				

We consider separately the two cases $2^k \geq j_1$ and $2^k < j_1$.

If $2^k \geq j_1$, by the induction hypothesis with $i = 2^k$,

$$|\{0, \dots, 2^k - 1\}|_{\leq k} \geq |\{j, \dots, 2^k + j - 1\}|_{\leq k}$$

We also apply the induction hypothesis to the last $i - 2^k$ members of $\{0, \dots, i-1\}$ ignoring the 1's in column $k+1$ and to the last $i - 2^k$ members of $\{j, \dots, j+i-1\}$ ignoring the 1's in column $\ell+2$, using $k-1$ in place of k. We obtain,

$$|\{0, \dots, i{-}2^k{-}1\}|_{\leq k-1} \geq |\{(j{+}2^k){-}2^{\ell+1}, \dots, (j{+}2^k){-}2^{\ell+1}{+}(i{-}2^k){-}1\}|_{\leq k-1}$$

Hence,

$$|\{2^k, \dots, i-1\}|_{\leq k} \geq |\{2^k + j, \dots, i+j-1\}|_{\leq k}$$

The case $2^k < j_1$ proceeds similarly. Note that if $2^k < j_1$ then $j_2 < 2^k$ since $j_1 + j_2 = i \leq 2^{k+1}$. First we compare the first 2^k members of $\{0, \dots, i{-}1\}$ with the last 2^k of $\{j, \dots, j{+}i{-}1\}$. Then we compare the last $i{-}2^k$ members of $\{0, \dots, i{-}1\}$ with the first $i{-}2^k$ of $\{j, \dots, j{+}i{-}1\}$.
$\square$

Lemma 17 *For all i, j, k, t where $i \leq 2^k$ and $1 \leq j \leq i$,*

$$|\{2^k, \ldots, 2^k + j - 1\}|_{\leq t} \geq |\{i, \ldots, i + j - 1\}|_{\leq t}$$

Proof By induction on j. The base case for $j = 1$ is obvious. Suppose that the lemma holds for numbers $< j$. The induction case has two cases.

Case 1: $i = 2^\ell + s$ and $i + j \leq 2^{\ell+1}$ for some $\ell < k$ and $2^\ell > s \geq 0$. This means that the members of $\{i, \ldots, i+j-1\}$ have 1's in column $\ell+1$ and 0's in columns $\ell+2$ through n, and the members of $\{2^k, \ldots, 2^k+j-1\}$ have 1's in column $k+1$ and 0's in columns $k+2$ through n. Also the members of $\{2^k, \ldots, 2^k+j-1\}$ have 0's in columns $\ell+1$ through k, since $j \leq 2^\ell$. Now we apply Lemma 16 with $t-1$ to both sets of sequences reduced to columns 1 through ℓ and the lemma follows.

Case 2: $i = 2^\ell + s$ and $i + j > 2^{\ell+1}$ for $0 \leq s < 2^\ell$ and $\ell < k$. Let $j_1 = 2^{\ell+1} - i$ and $j_2 = j - j_1$. Thus, j_1 is the number of members of $\{i, \ldots, i+j-1\}$ with 1's in column $\ell+1$ and 0's in columns $\ell+2$ through n, and j_2 is the number of members of $\{i, \ldots, i+j-1\}$ with 1's in column $\ell+2$ and 0's in the columns $\ell+3$ through n. The argument splits into two cases depending on whether any of the members of $\{2^k, \ldots, 2^k+j-1\}$ have 1's in the $\ell+1$ column, i.e., whether $j \leq 2^\ell$ or $j > 2^\ell$.

Case 2.1: $j \leq 2^\ell$. In this case there are no 1's in the $\ell+1$ column of $\{2^k, \ldots, 2^k+j-1\}$.

	n	$k+1$		$\ell+2$	$\ell+1$	1
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	$0\cdots0$	0	$0\cdots0$	0	1	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i+j_1-1$	$0\cdots0$	0	$0\cdots0$	0	1	$1\cdots1$
	$0\cdots0$	0	$0\cdots0$	1	0	$0\cdots0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i+j-1$	$0\cdots0$	0	$0\cdots0$	1	0	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^k	$0\cdots0$	1	$0\cdots0$	0	0	$0\cdots0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^k+j-1	$0\cdots0$	1	$0\cdots0$	0	0	

Consider the last j_2 members of $\{i, \ldots, i+j-1\}$ and the first j_2 members of $\{2^k, \ldots, 2^k+j-1\}$. By the induction hypothesis

$$|\{2^k, \ldots, 2^k + j_2 - 1\}|_{\leq t} \geq |\{i + j_1, \ldots, i + j - 1\}|_{\leq t}$$

Recall that the columns from $\ell+1$ to k in $\{2^k,\ldots,2^k+j-1\}$ contain only 0's. Now consider the first j_1 members of $\{i,\ldots,i+j-1\}$ and the last j_1 in $\{2^k,\ldots,2^k+j-1\}$. Transform these by discarding the columns $\ell+1$ to n and in the rest of the columns interchanging all 0's and 1's. The incidence vector $i+j_1-1$ becomes $0\cdots 0$ and $i+j_1-2$ becomes $0\cdots 01$, etc. This means that $\{i,\ldots,i+j_1-1\}$ is transformed into $\{0,\ldots,j_1-1\}$ and that $\{2^k+j_2,\ldots,2^k+j-1\}$ is transformed into $\{a,a+1,\ldots,a+j_1-1\}$ for some $a>0$. By Lemma 16, $\{0,\ldots,j_1-1\}$ contains fewer members with with $\le t-1$ 0's than $\{a,a+1,\ldots,a+j_1-1\}$ does. When we undo the transformation, by reversing the interchange of 0's and 1's, we get that

$$|\{2^k+j_2,\ldots,2^k+j-1\}|_{\le t}\ge|\{i,\ldots,i+j_1-1\}|_{\le t}.$$

From the last two displayed inequalities, the desired result follows.

Case 2.2: $j>2^\ell$. Choose s' so that $j=2^\ell+s'$, $i=2^\ell+s$ and $s'\le s$.

	n	$k{+}1$		$\ell{+}2$	$\ell{+}1$	1
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
i	$0\cdots0$	0	$0\cdots0$	0	1	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i+j_1-1$	$0\cdots0$	0	$0\cdots0$	0	1	$1\cdots1$
	$0\cdots0$	0	$0\cdots0$	1	0	$0\cdots0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i+j-1$	$0\cdots0$	0	$0\cdots0$	1	0	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^k	$0\cdots0$	1	$0\cdots0$	0	0	$0\cdots0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^k+2^\ell-1$	$0\cdots0$	1	$0\cdots0$	0	0	$1\cdots1$
	$0\cdots0$	1	$0\cdots0$	0	1	$0\cdots0$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^k+j-1	$0\cdots0$	1	$0\cdots0$	0	1	

The argument splits into two subcases depending on whether $s'\le j_1$.

First suppose $s'\le j_1$. Consider the last s' members of $\{2^k,\ldots,2^k+j-1\}$ and the first s' of $\{i,\ldots,i+j-1\}$. Ignore column $k+1$ of 1's of $\{2^k,\ldots,2^k+j-1\}$ and column $\ell+1$ of 1's in the first s' members of $\{i,\ldots,i+j-1\}$, and apply the induction hypothesis to the sets

$$\{i-2^\ell,\ldots,i-2^\ell+s'-1\}\quad\text{and}\quad\{2^\ell,\ldots,2^\ell+s'-1\}$$

with $t-1$. To apply the induction hypothesis, we need $s'\le i-2^\ell\le 2^\ell$, which is easily verified.

Finally we compare the last 2^ℓ members of $\{i,\ldots,i+j-1\}$ and the first 2^ℓ members of $\{2^k,\ldots,2^k+j-1\}$. In this case, by the induction hypothesis,

$$|\{2^k,\ldots,2^k+2^\ell-1\}|_{\le t} \ge |\{i+s',\ldots,i+s'+2^\ell-1\}|_{\le t}$$

Here $2^\ell \le i+s' \le i+j_1 = 2^{\ell+1} \le 2^k$.

Now suppose that $s' > j_1$.Then $s' \le j_2$, since otherwise $2s' > j_1+j_2 = j = 2^\ell + s'$, contradicting $s' < 2^\ell$. The argument is almost the same as when $s' \le j_1$. Take the last s' members of $\{2^k,\ldots,2^k+j-1\}$ and of $\{i,\ldots,i+j-1\}$ and ignore the $k+1$ column of 1's in $\{2^k,\ldots,2^k+j-1\}$ and the $\ell+2$ column of 1's in $\{i,\ldots,i+j-1\}$ and apply the induction hypothesis to the sets

$$\{2^\ell,\ldots,2^\ell+s'-1\} \text{ and } \{i-2^\ell,\ldots,i-2^\ell+s'-1\}$$

with $t-1$. To apply the induction hypothesis, we need $s' \le i+2^\ell-2^{\ell+1} \le 2^\ell$; which holds since $i+2^\ell-2^{\ell+1} = i-2^\ell = s \ge s'$.

Finally we compare the first 2^ℓ members of $\{2^k,\ldots,2^k+j-1\}$ with the first 2^ℓ members of $\{i,\ldots,i+j-1\}$. In this case by the induction hypothesis we get

$$|\{2^k,\ldots,2^k+2^\ell-1\}|_{\le t} \ge |\{i,\ldots,i+2^\ell-1\}|_{\le t} \qquad \square$$

Now we are ready to complete the proof of Theorem 15.

Proof of Theorem 15. By induction on the size of X. If $|X|=1$ it is obvious. Suppose that the theorem holds for $|X|<m$. Let $\ell \in [n]$ be maximum so that ℓ is in some set in X. Let X_1 be the subset of X containing those sets of X that do not contain ℓ, and let X_2 be the set $X \setminus X_1$. Let m_1 and m_2 be the cardinalities of X_1 and X_2, respectively. Since X is hereditary, $m_2 \le m_1 \le 2^{\ell-1}$. Define X_2^* be the set $\{S\setminus\{\ell\} : S \in X_2\}$. Note that X_2^* must be hereditary. By two applications of the induction hypothesis,

$$|X_1|_{\le k} \ge |\{0,\ldots,m_1-1\}|_{\le k}$$

and

$$|X_2^*|_{\le k-1} \ge |\{0,\ldots,m_2-1\}|_{\le k-1}.$$

Now,

$$\begin{array}{rcl} |X|_{\le k} & = & |X_1|_{\le k} + |X_2^*|_{\le k-1} \\ & \ge & |\{0,\ldots,m_1-1\}|_{\le k} + |\{0,\ldots,m_2-1\}|_{\le k-1} \\ & \ge & |\{0,\ldots,m_1-1\}|_{\le k} + |\{2^{\ell-1},\ldots,2^{\ell-1}+m_2-1\}|_{\le k} \\ & \ge & |\{0,\ldots,m_1-1\}|_{\le k} + |\{m_1,\ldots,m_1+m_2-1\}|_{\le k} \\ & = & |\{0,\ldots,m-1\}|_{\le k} \end{array}$$

The third inequality follows from Lemma 17. $\square$

We claim that the above proof can be formalized by polynomial-size Frege proofs. The easiest way to see this is to first notice that Lemma 17 is expressible by polynomial-size propositional formulas, and the proof of Theorem 15 from Lemma 17 is also easily formalized by polynomial-size Frege proofs. The most direct way to see that Lemma 17 has a short Frege proof, is to notive that, since the lemma is true (by the proof provided), a Frege proof can be obtained by exhaustively checking that the formula holds for all possible values of i, j, k and t. Checking that the lemma holds for a particular value of i, j, k, t is polynomial-length Frege provable, and there are less than $(n+m)^4$ possible values of i, j, k, t. Thus, this "brute-force" proof is easily formalizable by a polynomial-size Frege system. With more work, it can be shown that our entire proof of Theorem 15 is actually formalizable by polynomial-size Frege proofs, and this gives polynomial-size Frege proofs of KK_m^n which are uniform, in the sense that the proofs can be straightforwardly described without depending on the truth of the proposition KK_m^n being proved.

5 Conclusion

As we have seen above, there is a dearth of good examples of tautologies that provide convincing evidence of an exponential separation of Frege and extended Frege proof systems. In fact, the only good combinatorial candidates we have found are based on Frankl's theorem (even the $t = 2$ case). However, in the past a similar state of affairs has held for the pigeonhole principle and for Bondy's theorem and, subsequently, polynomial-size Frege proofs for these have been found. Thus, it is not unlikely that further progress will find polynomial-size Frege proofs of the tautologies based on Frankl's theorem.

We also have a large number of examples of combinatorial principles, most notably, the Odd-town Theorem and the Graham-Pollak Theorem, which have fairly simple linear algebra proofs. These have polynomial-size extended Frege proofs and we conjecture that they have quasipolynomial-size Frege proofs. However, combinatorialists have reportedly put significant effort into searching for proofs that are not based on linear algebra, so it may require a significant breakthrough to find polynomial-size Frege proofs of these principles.

In the course of preparing this paper, we considered several other examples based on expander graphs and on matching algorithms; however, none of these ultimately yielded examples which could be conjectured to provide an exponential separation of Frege and extended Frege proof systems.

6 Acknowledgements

We would like to thank the numerous people who have provided stimulating suggestions and input to this line of investigation. In particular, we would like to thank the following people: László Babai, Vašek Chvátal, Stephen Cook, Mauricio Karchmer, Jan Krajíček, Russell Impagliazzo, Steven Rudich, Michael Sipser, Herbert Wilf and two anonymous referees.

REFERENCES

[1] M. Ajtai, *The complexity of the pigeonhole principle*, in Proceedings of the 29-th Annual IEEE Symposium on Foundations of Computer Science, 1988, pp. 346–355.

[2] L. Babai and P. Frankl, *Linear algebra methods in combinatorics.* Preliminary version of book, 1988.

[3] S. R. Buss, *The Boolean formula value problem is in ALOGTIME*, in Proceedings of the 19-th Annual ACM Symposium on Theory of Computing, May 1987, pp. 123–131.

[4] ——, *Polynomial size proofs of the propositional pigeonhole principle*, Journal of Symbolic Logic, 52 (1987), pp. 916–927.

[5] ——, *Propositional consistency proofs*, Annals of Pure and Applied Logic, 52 (1991), pp. 3–29.

[6] ——, *Algorithms for Boolean formula evaluation and for tree contraction*, in Arithmetic, Proof Theory and Computational Complexity, P. Clote and J. Krajíček, eds., Oxford University Press, 1993, pp. 96–115.

[7] S. R. Buss, S. A. Cook, A. Gupta, and V. Ramachandran, *An optimal parallel algorithm for formula evaluation*, SIAM J. Comput., 21 (1992), pp. 755–780.

[8] S. R. Buss and György Turán, *Resolution proofs of generalized pigeonhole principles*, Theoretical Computer Science, 62 (1988), pp. 311–317.

[9] P. Clote and J. Krajíček, *Some open problems in arithmetic, proof theory and computational complexity*, in Arithmetic, Proof Theory and Computational Complexity, Oxford University Press, 1993, pp. 2–19.

[10] S. A. Cook, *Feasibly constructive proofs and the propositional calculus*, in Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[11] S. A. Cook and R. A. Reckhow, *On the lengths of proofs in the propositional calculus, preliminary version*, in Proceedings of the Sixth Annual ACM Symposium on the Theory of Computing, 1974, pp. 135–148.

[12] ———, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic, 44 (1979), pp. 36–50.

[13] P. Erdős, A. Rényi, and V. Sós, *On a problem of graph theory*, Studia Math. Hungar., 1 (1966), pp. 215–219.

[14] P. Frankl, *On the trace of finite sets*, J. Combin. Theory A, 34 (1983), pp. 41–45.

[15] R. Graham and H. Pollak, *On embedding graphs in squashed cubes*, Lecture Notes in Mathematics, 303 (1972), pp. 99–110.

[16] J. Krajíček. Talk presented at *Workshop on Feasible Mathematics II*, Ithaca, NY, May 28-30, 1992.

[17] J. Krajíček, *On Frege and extended Frege proof systems*, in Feasible Mathematics II, P. Clote and J. Remmel, eds., Boston, 1995, Birkäuser, pp. 284–319.

[18] J. Krajíček and P. Pudlák, *Propositional proof systems, the consistency of first-order theories and the complexity of computations*, Journal of Symbolic Logic, 54 (1989), pp. 1063–1079.

[19] J. Krajíček, P. Pudlák, and A. Woods, *Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle*, Random Structures and Algorithms, 7 (1995), pp. 15–39.

[20] G. Kreisel, G. E. Mints, and S. G. Simpson, *The use of abstract language in elementary metamathematics: Some pedagogical examples*, in Logic Colloquium, Lecture Notes in Mathematics #453, Springer-Verlag, 1975, pp. 38–131.

[21] B. Krishnamurthy, *Short proofs for tricky formulas*, Acta Informatica, 22 (1985), pp. 253–275.

[22] B. Krishnamurthy and R. N. Moll, *Examples of hard tautologies in the propositional calculus*, in Proceedings of the 13-th Annual ACM Symposium on Theory of Computing, 1981, pp. 28–37.

[23] R. E. Ladner, *The circuit value problem is log space complete for P*, SIGACT News, 7 (1975), pp. 18–20.

[24] J. Longyear and J. D. Parsons, *The friendship theorem*, Indag. Math., (1972), pp. 257–262.

[25] J. B. Paris and A. J. Wilkie, *Counting problems in bounded arithmetic*, in Methods in Mathematical Logic, Lecture Notes in Mathematics #1130, Springer-Verlag, 1985, pp. 317–340.

[26] T. Pitassi, *The Power of Weak Formal Systems*, PhD thesis, University of Toronto, 1992.

[27] T. Pitassi, P. Beame, and R. Impagliazzo, *Exponential lower bounds for the pigeonhole principle*, Computational Complexity, 3 (1993), pp. 97–140.

[28] P. Pudlák, *Ramsey's theorem in bounded arithmetic*, in Computer Science Logic, Lecture Notes in Computer Science #553, Springer-Verlag, 1992, pp. 308–312.

[29] A. A. Razborov and S. Rudich, *Natural proofs*, in Proceedings of the 26-th Annual ACM Symposium on Theory of Computing, 1994, pp. 204–213.

[30] P. M. Spira, *On time hardware complexity tradeoffs for Boolean functions*, in Proceedings of the Fourth Hawaii International Symposium on System Sciences, 1971, pp. 525–527.

[31] R. Statman, *Complexity of derivations from quantifier-free Horn formulae, mechanical introduction of explicit definitions, and refinement of completeness theorems*, in Logic Colloquium '76, R. Gandy and M. Hyland, eds., Amsterdam, 1977, North-Holland, pp. 505–517.

[32] H. Wilf, *The friendship theorem*, in Combinatorial mathematics and its applications, D. Welsh, ed., Academic Press, New York, 1971, pp. 307–309.

Maria Luisa Bonet
Department of Mathematics
Univ. of Pennsylvania, Philadelphia, PA 19104-6395
bonet@math.upenn.edu

Samuel R. Buss
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112
sbuss@ucsd.edu.

Toniann Pitassi
Departments of Mathematics and Computer Science
University of Pittsburgh
Pittsburgh, PA 15260
toni@cs.pitt.edu.