The Journal of Symbolic Logic
Volume 00, Number 0, XXX 0000

QUASI-POLYNOMIAL SIZE FREGE PROOFS OF FRANKL'S THEOREM ON THE TRACE OF SETS

JAMES AISENBERG, MARIA LUISA BONET, AND SAM BUSS

Abstract. We extend results of Bonet, Buss and Pitassi on Bondy's Theorem and of Nozaki, Arai and Arai on Bollobás' Theorem by proving that Frankl's Theorem on the trace of sets has quasi-polynomial size Frege proofs. For constant values of the parameter t, we prove that Frankl's Theorem has polynomial size AC^0-Frege proofs from instances of the pigeonhole principle.

§1. Introduction. This paper extends results of Bonet, Buss, and Pitassi [2] and Nozaki, Arai, and Arai [16] by proving that Frankl's Theorem [7] has quasi-polynomial size Frege proofs. A Frege system is a "textbook" style proof system for propositional logic based on schematic axioms and inferences such as *modus ponens*. An extended Frege system is a Frege system augmented with the extension rule allowing the introduction of abbreviations, cf. Cook-Reckhow [6]. Lines in a Frege proof are Boolean formulas, whereas lines in an extended Frege proof can express Boolean circuits. It is generally conjectured that some Boolean circuits can only be expressed by exponentially larger Boolean formulas. For this reason, it is also generally conjectured that Frege proofs cannot polynomially simulate extended Frege proofs; however this is an open question.

Bonet, Buss, and Pitassi [2] looked for examples of tautologies that might be conjectured to provide exponential separations between the Frege and extended Frege proof systems. They found only a small number of examples other than partial consistency statements. The first type of examples were based on linear algebra, and included the Oddtown Theorem, the Graham-Pollack Theorem, the Fisher Inequality, and the Ray-Chaudhuri-Wilson Theorem. The remaining example was Frankl's Theorem on the trace of sets.

The four principles based on linear algebra all have short extended Frege proofs using facts about determinants and eigenvalues. The same is true for the "$AB{=}I \Rightarrow BA{=}I$" tautologies about square matrices A and B over GF_2 that was subsequently suggested by S. Cook. Recently, Hrubeš and Tzameret [10] showed that determinant identities such as $\det(A)\det(B) = \det(AB)$ and $AB = I \Rightarrow$

Supported in part by NSF grants DMS-1101228 and CCF-1213151.
Supported in part by grant TIN2010-20967-C04-02.
Supported in part by NSF grants DMS-1101228 and CCF-1213151 and by the Simons Foundation award 306202.

0022-4812/00/0000-0000/$00.00

$BA = I$ have quasi-polynomial size Frege proofs. Thus it seems highly likely (as was already conjectured by [2]) that all these principles have quasi-polynomial size Frege proofs.

The remaining principle, Frankl's Theorem, was shown to have polynomial size extended Frege proofs by [2]. The main result of the present paper, Theorem 8, shows that the propositional formulations of Frankl's Theorem also have quasi-polynomial size Frege proofs.

Very few other other candidates (other than partial consistency principles) for exponentially separating Frege and extended Frege systems have been proposed. Kołodziejczyk, Nguyen, and Thapen [13] suggested the propositional translations of various local improvement principles LI, $\mathrm{LI}_{\log}$ and LLI as candidates, motivated by results on their provability in the bounded arithmetic theory V_2^1. They proved the LI principle is equivalent to partial consistency statements for extended Frege systems, but the other two remained as candidates. However, Beckmann and Buss [1] 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. Therefore the former is equivalent to a partial consistency statement, and the latter has quasi-polynomial size Frege proofs. Thus neither of these provide good candidates for exponentially separating Frege and extended Frege systems. The rectangular local improvement principles RLI_k ([13, 1] for $k \geq 2$ are possible candidates for separation, as they are neither known to be provable in U_2^1 nor known to be many-complete for the provably total NP search problems of V_2^1.

Another family of propositional tautologies based on the Kneser-Lovász Theorem was recently proposed by Istrate and Crãciun [11]. 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, subsequent work of Aisenberg, Bonet, Buss, Crãciun, and Istrate [in preparation] has established that the Kneser-Lovász tautologies have polynomial size extended Frege proofs and quasi-polynomial size Frege proofs.

We thus lack many good candidates for super-quasipolynomially separating Frege and extended Frege systems, apart from partial consistency principles (cf., [6, 4]) or principles such as LI and $\mathrm{LI}_{\log}$ which are equivalent to partial consistency principles. This raises the question of whether Frege systems can quasi-polynomially simulate extended Frege systems. This seems very unlikely since none of the cases where Frege proofs (quasi-)polynomially simulate extended Frege proofs use methods that generalize to simulate arbitrary extended Frege proofs. The known simulations, such as the results of the present paper, may instead be useful to help show what kinds of techniques will be needed to separate Frege and extended Frege proofs.

The two restricted cases of Frankl's Theorem (Theorem 1) where the parameter t is equal to 1 or 2 have already been shown to have polynomial size Frege proofs. The $t = 1$ case is Bondy's Theorem, which Bonet, Buss, and Pitassi [2] proved to have polynomial size Frege proofs. They proved more than this in fact; namely, Bondy's Theorem is equivalent over AC^0-Frege to the pigeonhole principle PHP_n^{n+1}. Their proof involved showing that the bounded arithmetic theories $I\Delta_0 + \Delta_0$-PHP and $I\Delta_0 + \Delta_0$-BONDY are equivalent. Nozaki, Arai, and Arai [16] improved this by showing that the $t = 2$ case of Frankl's Theorem (known as

Bollobás' Theorem) also has polynomial size Frege proofs. They did not explicitly address the question of AC^0-Frege reducibility to the pigeonhole principle, but it is easy to see that their constructions give such a reduction. In other words, their proof shows that there are polynomial size AC^0-Frege proofs of the propositional translations of Bollabás' Theorem from instances of the pigeonhole principle, and that Bollobás' Theorem is provable in $I\Delta_0 + \Delta_0$-PHP.

We extend these results to general t. Theorem 9 states that, for any fixed value of t, Frankl's Theorem has polynomial size Frege proofs. In fact, for a fixed value of t, Frankl's Theorem has polynomial size AC^0-Frege proofs from the Δ_0-PHP formulas. Likewise, for fixed values of t, Frankl's Theorem is provable in $I\Delta_0 + \Delta_0$-PHP.

Our proof methods substantially extend the constructions of [7, 2]. Like the original proof of Frankl [7], we reduce from the general case of Frankl's Theorem to the case where the matrix is hereditary. However, the direct transformation to a hereditary matrix as described by Frankl does not yield quasi-polynomial size propositional formulas. Thus, we need to use a different, more complicated construction that builds a hereditary matrix that is AC^1-definable. This construction can be translated into quasi-polynomial size Frege proofs and is the main new contribution of the present paper. The prior constuction of [7, 2] could only be translated to polynomial size extended Frege proofs, but required exponential size Frege proofs. Surprisingly, our more complicated construction produces the same hereditary matrix as the prior construction, at least if the Frankl construction is carried out column by column.

Once the general case of Frankl's Theorem has been reduced to the case of hereditary matrices, the remainder of the proof of Frankl's Theorem is carried out by using the Kruskal-Katona Theorem [12, 15] in the same way as was done by both Frankl and Bonet-Buss-Pitassi. Additional work is need for the case of constant t, where we show that Frankl's theorem has AC^0-Frege + PHP proofs. For this, we use a sharpened "functional" form (Theorem 7) of the Kruskal-Katona Theorem, which is based on AC^0-definable bijections. For constant values of t, we show that the functional form of the Kruskal-Katona Theorem has polynomial size AC^0-Frege proofs, and this allows us to construct the needed AC^0 reduction to the pigeonhole principle.

1.1. Frankl's Theorem and the Kruskal-Katona Theorem. Throughout the paper, A is an $m \times n$ 0/1 matrix with m distinct rows. We identify rows r of A with strings in $\{0,1\}^n$.

THEOREM 1. (Frankl [7]) *Let t be a positive integer and $m \leq n\frac{2^t-1}{t}$. Then for any $m \times n$ 0/1 matrix with distinct rows, there is a column such that if this column is deleted, the resulting $m \times (n-1)$ matrix will contain fewer than 2^{t-1} pairs of equal rows.*

We can rephrase this theorem using the following terminology.

DEFINITION 2. Let r_1 and r_2 be two rows of A, and $j \in \{0, \ldots, n-1\}$. Row r_1 is *equivalent modulo column j to* row r_2 if r_1 and r_2 differ in exactly column j. We define P_j to be the set of rows r_1 for which there exists such a row r_2.

Note that $j \in \{0, \ldots, n-1\}$; columns are numbered from left to right, starting with $j = 0$. Since the rows of A are distinct, there can be at most one row equivalent to r_1 modulo column j; thus, $|P_j|$ is even. When column j is deleted, there are $|P_j|/2$ pairs of equal rows in the resulting $m \times (n-1)$ matrix. Frankl's Theorem can be rephrased as follows.

THEOREM 3. *Let t be a positive integer, and let $m \leq n^{\frac{2^t-1}{t}}$. Then for any $m \times n$ 0/1 matrix with distinct rows, there is a j such that $|P_j| < 2^t$.*

Theorem 3 is trivial if $m < 2^t$ since $|P_j| \leq m$. Also, if $m \leq n$, we can take $t = 1$ and then Theorem 3 follows from Bondy's Theorem; and we already know Bondy's theorem has polynomial size Frege proofs. Thus we may assume that $m \geq 2^t$ and $m > n$.

Our proof, like the usual proof of Frankl's Theorem, goes through hereditary matrices and the Kruskal-Katona Theorem.

DEFINITION 4. Let $\mathcal{F} = \{S_1, \ldots, S_m\}$ be a family of subsets of $\{0, \ldots, n-1\}$. The *incidence matrix* for $\mathcal{F}$ is an $m \times n$ 0/1 matrix with matrix element $a_{i,j} = 1$ iff $j \in S_i$. The family $\mathcal{F}$ is *hereditary* if $X \subset Y \in \mathcal{F}$ implies $X \in \mathcal{F}$. A 0/1 matrix is *hereditary* if it is the incidence matrix of some hereditary family.

Equivalently, a 0/1 matrix A is hereditary provided that, for any row r, changing any entry 1 in r to 0 yields another row of A.

DEFINITION 5. If $r \in \{0,1\}^n$, we write $|r|_1$ to denote the number of ones in r. If A is an $m \times n$ 0/1 matrix and $k \geq 0$, we write $|A_{\leq k}|$ to denote the number of rows r of A such that $|r|_1 \leq k$.

For $r \in \mathbb{N}$, we let $|r|_1$ denote the number of 1's in the binary representation of r. For X a set of natural numbers, we write $|X_{\leq k}|$ to denote the number of $r \in X$ such that $|r|_1 \leq k$.

We next state the Kruskal-Katona Theorem needed for the proof of Frankl's theorem. This is actually only a corollary to the Kruskal-Katona Theorem, see [7, 2], but we henceforth refer to it as the "Kruskal-Katona Theorem".

THEOREM 6. *Let A be an $m \times n$ 0/1 hereditary matrix with distinct rows, and $k \geq 0$. Then*

$$|A_{\leq k}| \;\geq\; |\{0, 1, 2, \ldots, m-1\}_{\leq k}|. \tag{1}$$

Theorem 6 was shown to have polynomial size Frege proofs by [2]. When discussing AC^0-Frege proofs of Frankl's Theorem, we need the following functional form of the Kruskal-Katona Theorem.

THEOREM 7. *Let A be an $m \times n$ 0/1 hereditary matrix with distinct rows. Then there is a bijection f from $\{0, 1, 2, \ldots, m-1\}$ onto the rows of A such that for every i, $|i|_1 \geq |f(i)|_1$.*

Theorem 7 is an immediate consequence of Theorem 6. Its advantage is that, for constant values of m, the bijection f can be defined with a constant depth formula.

1.2. Frege, extended Frege, and the main theorems. *Frege proof systems* are implicationally sound and complete propositional proof systems formalized with a finite set of schematic axioms and the inference rule *modus ponens* using, without loss of generality, the connectives $\neg$, $\wedge$, $\vee$, and $\rightarrow$. The length of a Frege proof is defined to be the total number of symbols in the proof. *Extended Frege systems* can be defined to be the same as Frege systems, but with proof length equal to the number of formulas (lines) in the proof instead of the number of symbols. An AC^0-Frege proof is a Frege proof in which all lines have alternation depth $O(1)$. For more information on Frege and extended Frege systems, see [6] or [2, 3, 14].

Frankl's Theorem, in the form of Theorem 3, is formalized as an infinite family of propositional tautologies as follows. Fix positive values n, m and t such that $m \leq n \cdot (2^t - 1)/t$. For $0 \leq i < m$ and $0 \leq j < n$, let $p_{i,j}$ be a propositional variable with the intended interpretation that $p_{i,j}$ is true iff the (i, j) entry of A is equal to 1. For $i \neq i'$, the formula $\textsc{Eq}(i, i', j)$ expresses that rows i and i' differ only in column j as

$$\textsc{Eq}(i, i', j) \ := \ \bigwedge_{j' \neq j} (p_{i,j'} \leftrightarrow p_{i',j'}).$$

By [3], there are polynomial size formulas expressing counting which allow polynomial size Frege proofs to reason about sizes of sets. This enables us to define the cardinality of P_j as

$$\textsc{CardP}(j) \ := \ \Big|\big\{i : 0 \leq i < m \text{ and } \bigvee_{i' \neq i} \textsc{Eq}(i, i', j)\big\}\Big|.$$

The size of $\textsc{CardP}(j)$ is polynomially bounded by the total size of the m many formulas $\bigvee_{i'} \textsc{Eq}(i, i', j)$; hence polynomially bounded by m and n. Letting DistinctRows be the formula $\bigwedge_{i \neq i'} \bigvee_j (\neg p_{i,j} \leftrightarrow p_{i',j})$, Frankl's Theorem (for these values of m, n, t) can be expressed by the polynomial size propositional formula

$$\textsc{DistinctRows} \rightarrow \bigvee_j (\textsc{CardP}(j) < 2^t).$$

This formula has size polynomially bounded by m, n and t. We next state our two main results precisely. A proof is said to be *quasi-polynomially bounded* if it is quasi-polynomially bounded by the size of the formula that is proved.

Theorem 8. *There are quasi-polynomial size Frege proofs $P_{m,n,t}$ of the propositional translations of Frankl's Theorem.*

As already remarked, Theorem 8 is trivial if $m < 2^t$, and is known (via Bondy's Theorem) for $m \leq n$. In other cases, the Frege proof $P_{m,n,t}$ will have quasi-polynomially (in m) many steps, and each formula in $P_{m,n,t}$ will be equivalent to an AC^1-circuit. Namely, each formula will have only polynomially many distinct subformulas, and will have only $O(\log m)$ many alternations of $\wedge$'s and $\vee$'s.

For the next theorem, we assume t is constant. In this case, there are polynomial size formulas with $O(1)$ alternations of $\wedge$'s and $\vee$'s (that is, AC^0-circuits) that express the condition "$\textsc{CardP}(j) < 2^t$". To see this, note that its negation "$\textsc{CardP}(j) \geq 2^t$" can be expressed as the disjunction over all 2^t-tuples

$i_1 < i_2 < \cdots < i_{2^t}$ of the assertions that every $i_\ell \in P_j$. Thus, for a constant value for t, the propositional translations of Frankl's Theorem can be expressed as constant depth, polynomial size formulas.

As is customary (cf. [5]), we let AC^0-Frege+PHP denote the Frege proof system augmented with all substitution instances of the $n+1$ into n pigeonhole principle for all $n \geq 1$, and restricted so that all formulas have alternation depth $O(1)$.

THEOREM 9. *Fix $t > 0$. There are AC^0-Frege+PHP proofs $P^t_{m,n}$ of the propositional translations of Frankl's Theorem which have polynomial size (in m, n) and in which all formulas have alternation depth $O(t) = O(1)$.*

The outline of the paper is as follows. Sections 2.1 through 2.3 give our new reduction to the hereditary case of Frankl's Theorem. The general strategy of the proof is as follows. Given a 0/1 matrix A, we let T be the prefix tree for the rows of A. The nodes of T are sets of rows of A that share a common prefix, and the ancestor relation for T is set inclusion. We define a function χ that takes as input a node of T and a list of column indices, and produces another node in T. This χ function is used to define another $m \times n$ 0/1 matrix A', which is hereditary. Furthermore, if A violates the conditions of Frankl's Thoerem, then so does A', From here, we are in the situation for the usual proof of Frankl's Theorem, and we conclude our proof by using the Kruskal-Katona Theorem. Section 2.4 describes the functional form of the Kruskal-Katona Theorem which will be needed for polynomial size Frege proofs of the constant t case.

Section 3.1 discusses how to formalize this proof of Frankl's Theorem in propositional logic. The key point is that (the graph of) the χ function can be defined with AC^1-circuits, and that the properties of the χ function can be established with quasi-polynomial size Frege proofs. Section 3.2 discusses the formalization of the constant t case of Frankl's Theorem with AC^0-Frege + PHP proofs. The key new tool is that the bijective form of the Kruskal-Katona Theorem can be formulated and proved in AC^0-Frege.

Section 4 shows that the matrix A' is identical to the hereditary counterexample produced in the usual proof of Frankl's Theorem when the reduction to a hereditary matrix is carried out column by column.

§2. Proof of Frankl's Theorem. This section gives our reduction from the general case of Frankl's Theorem to the hereditary case. We define the reduction and prove its correctness in detail, so that it will be clear in Section 3 that the arguments can be formalized with quasi-polynomial size Frege proofs. Section 2.1 builds the prefix tree for the rows of A, Section 2.2 defines the χ function and establishes its properties. Section 2.3 uses the χ function to construct hereditary matrix, culminating with Theorem 25. Section 2.4 proves the bijective version of the Kruskal-Katona Theorem as will be needed for the AC^0-Frege + PHP proofs. We assume henceforth that A is an $m \times n$ 0/1 matrix with distinct rows and $m \leq n^{\frac{2^t-1}{t}}$.

2.1. The prefix tree for A. Recall that a row r is identified with a string in $\{0,1\}^n$. A binary string x is a *prefix* of r when r equals the concatenation xy for some y.