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

QUASIPOLYNOMIAL 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 quasipolynomial 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 quasipolynomial size Frege proofs. A Frege system is a textbook 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 p-simulate extended Frege proofs. This is an open question however.

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, Hrubes and Tzameret [10] showed

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

that determinantal identities such as $det(A)det(B) = det(AB)$ have quasipolynomial size Frege proofs. Thus it seems highly likely (as was already conjectured by [2]) that these principles all have quasipolynomial 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 quasipolynomial 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, $\text{LI}_{\log}$ 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 $\text{LI}_{\log}$ 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 quasipolynomial 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 Lovász-Kneser 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 Lovász-Kneser tautologies have polynomial size extended Frege proofs and quasipolynomial size Frege proofs.

We thus now 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 $\text{LI}_{\log}$ which are equivalent to partial consistency principles. This raises the question of whether Frege systems can quasipolynomially simulate extended Frege systems, but this seems very unlikely.

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 principles 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 method 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 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 cannot does not yield quasipolynomial size propositional formulas. Thus, we need to use a different, more complicated construction that builds a hereditary matrix that is AC^1-definable. Surprisingly, this more complicated construction produces the same hereditary matrix as the Frankl construction, at least if the Frankl construction is carried out column by column.

We also use the Kruskal-Katona Lemma [12, 15], as was done by both Frankl and Bonet-Buss-Pitassi. For the case of constant t, we use a sharpened "functional" form (Theorem 7) of the Kruskal-Katona Lemma, which is based on AC^0-definable bijections. For constant values of t, 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.

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 $|P_j| < 2^t$.*

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 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 integers, we write $|X_{\leq k}|$ to denote the number of $r \in X$ such that $|r|_1 \leq k$.

The version of the Kruskal-Katona Lemma needed for the proof of Frankl's theorem can be stated as follows:

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

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

This version of the Kruskal-Katona Theorem was shown to have polynomial size Frege proofs by [2]. When discussing AC^0-Frege proofs, 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 of course. 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 proofs, and the main theorems. *Frege proof systems* are implicationally sound and complete propositional proof systems formalized with a finite set of schematic axioms and *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. 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 $\mathrm{EQ}(i,i',j)$ expresses that rows i and i' differ only in column j as

$$\mathrm{EQ}(i,i',j) \;:=\; \bigwedge_{j' \neq j} (p_{i,j'} \leftrightarrow p_{i',j'}).$$

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

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

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

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

We can now state our two main results precisely.

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

The Frege proof $P_{m,n,t}$ will have quasipolynomially many steps (lines), 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. (Here we assume that $m > n$, w.l.o.g.)

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 "$\textsc{CardP}(j) \ge 2^t$" 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, 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. Section 2 gives, informally, our new proof 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 finish up by using the Kruskal-Katona Theorem.

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 quasipolynomial 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 Frankl reduction is carried out column by column.

§2. Proof of Frankl's Theorem. This section gives the informal proof of Frankl's Theorem in the form of Theorem 3. Although the proof is designed to be formalizable with polynomial size Frege proofs, we do not discuss this aspect until Section 3. 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 the hereditary matrix A', and Section 2.4 finishes up the proof of Frankl's Theorem and proves the bijective version of the Kruskal-Katona Theorem as will be needed for the constant depth Frege 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. The prefix tree of A will be defined with nodes corresponding to rows of A.

DEFINITION 10. Let $x \in \{0,1\}^*$. Then $[\![x]\!]$ denotes the collection of the rows of A that have prefix x:

$$[\![x]\!] \;=\; \{r : r \text{ is a row of } A,\, x \text{ is a prefix of } r\}.$$

We call x the *maximal length representative* for $[\![x]\!]$ if there is no y with $|y| > |x|$ and $[\![y]\!] = [\![x]\!]$. The notation $[x]$ is used to denote $[\![x]\!]$ in this case.

Of course, every non-empty $[\![x]\!]$ has a unique maximal representative. Whenever we use the notation $[x]$, it is (implicitly) required that $[\![x]\!] \neq \emptyset$ and x is its maximal representative. For $|x| < n$, we have $[\![x]\!] = [\![x0]\!] \cup [\![x1]\!]$. The string x is a maximal representative for $[\![x]\!]$ iff $[\![x]\!] \neq \emptyset$ and either $|x| = n$ or both $[\![x0]\!]$ and $[\![x1]\!]$ are non-empty.

The classes $[x]$ are the nodes of a binary tree T called the *prefix tree* of A. The root of T is $[\![\epsilon]\!]$, where ϵ is the empty string and thus $[\![\epsilon]\!]$ is the set of all rows of A. The root $[\![\epsilon]\!]$ is equal to $[y]$ for y the longest common initial substring of the rows. The leaves of T are the singleton nodes $[r]$, where $r \in \{0,1\}^n$ is a row of A.

The parent-child relationships of T are defined so that $[x]$ is an ancestor of $[y]$ in T precisely when $[x] \neq [y]$ and x is a prefix of y. In more detail, if $[x]$ is not a leaf node (in other words $|x| < n$) then the only two children of $[x]$ are its left child $[\![x0]\!]$ and its right child $[\![x1]\!]$. Thus T is an ordered binary tree, and since T has m leaves, it has $m-1$ internal nodes.

The edges of T are decorated with labels in $\{0,1\}^*$. If $[y]$ is a child of $[x]$, then x is a proper prefix of y, and the edge from $[x]$ to $[y]$ is labeled with the nonempty string z such that $y = xz$. As a maximal length representative, x is equal to the concatenation of the labels on the edges along the branch of T leading to $[x]$.

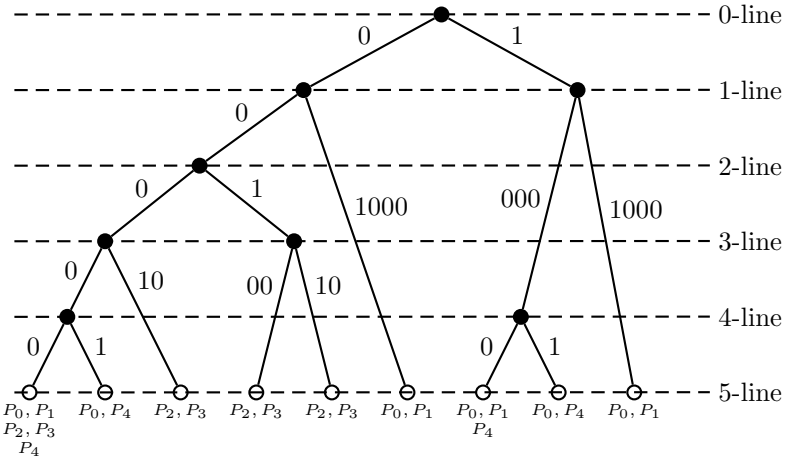

FIGURE 1. The prefix tree T of A.

As an example, Figure 1 shows the prefix tree for the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

For example, $[\![11]\!] = [\![110]\!] = [\![1100]\!] = [11000]$ is the rightmost leaf of the tree. The sets P_j of rows which are equivalent modulo column j were defined in Section 1.1. In this example, the sets P_j are:

$$\begin{aligned} P_0 &= \{00000, 10000, 00001, 10001, 11000, 01000\} \\ P_1 &= \{00000, 01000, 10000, 11000\} \\ P_2 = P_3 &= \{00000, 00100, 00010, 00110\} \\ P_4 &= \{00000, 10000, 00001, 10001\}. \end{aligned}$$

Each set P_j has prefix tree T_j. Formally, the nodes of T_j will identified with nodes of T, making it an induced subtree of T.

DEFINITION 11. Let $j \in \{0, \ldots, n-1\}$. The tree T_j has leaves $[r]$ for $r \in P_j$, and has as internal nodes the least common ancestors of every pair of $[r]$'s. The ancestor relationship and edge labels are inherited from T.

The edges of T_j are labeled with strings in $\{0,1\}^*$ using the same definition as for labels on T, but now interpreting the definition relative to T_j. That is, if $[y]$ is a child of $[x]$ in T_j, then the edge from $[x]$ to $[y]$ is labeled with z where $y = xz$. For example, in the tree T_0 shown in Figure 2, the edge from [1] to [1000] is labeled 000.

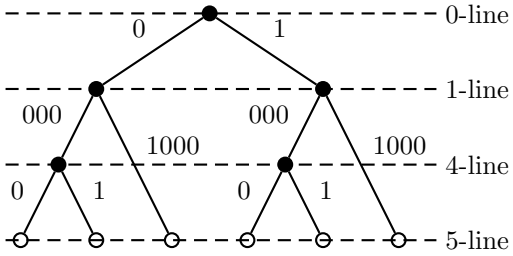

FIGURE 2. The prefix tree T_0 associated with P_0.

DEFINITION 12. Let $j \in \{0, \ldots, n-1\}$. The *j-line* through the tree T is defined to be

$$\{[x] : [x] \in T \text{ and } |x| = j\}.$$

In other words, the j-line is the set of nodes $[x]$ in T such that $[\![x0]\!] \neq [\![x1]\!]$ with $|x| = j$. In the above, $[\![10]\!] = [1000]$ is on the 4-line.

The j-line corresponds to column j of the matrix. We picture the tree T with root at the top and j-lines ordered accordingly, and say that the j-line and its nodes in T are *above* the j'-line if $j < j'$.

Two trees are defined to be *isomorphic* provided they are isomorphic as graphs and, in addition, the isomorphism preserves the edge labels.

In Figure 2, the tree T_0 has one node on the 0-line, $[\epsilon]$. Its two children are roots of isomorphic subtrees of T_0. The next lemma shows this property always holds.

DEFINITION 13. Let S be T or one of its induced subtrees T_j. Let $[x]$ be an internal node of S. The *left (right) subtree of* $[x]$ *in* S is the subtree of S rooted at the left (respectively, right) child of $[x]$ in S.

LEMMA 14. *Let $[x] \in T_j$ lie on the j-line. Then the right and left subtrees of $[x]$ in T_j are isomorphic. Moreover, the labels on the edges from $[x]$ to the roots of its right and left subtrees in T_j differ only in their first bit.*

PROOF. (Sketch) The leaves of the left (resp., right), subtrees of $[x]$ in T_j are the classes $[r]$ for r a row of A of the form $r = x0u$ (resp., $r = x1u$). In fact, for fixed u, $[x0u]$ is in P_j if and only if $[x1u]$ is in P_j. The internal nodes of these two subtrees are least common ancestors of these leaves. From this, the lemma follows. ⊣

A consequence of (the proof of) Lemma 14 is that every leaf node of T_j has a ancestor on the j-line. Indeed, every node of T_j below the j-line has an ancestor on the j-line. This is because every leaf $[x0u]$ of T_j has a corresponding leaf $[x1u]$ in T_j, and their least common ancestor is $[x]$ on the j-line.

2.2. The χ function. The χ function takes a node x of a tree S and a sequence of columns, and produces a node in the subtree rooted at x:

DEFINITION 15. Let S be either T or one of its induced subtrees T_j. Let $[x]$ be an internal node of S and let $j_1 < j_2 < \cdots < j_\ell$ be a (possibly empty) sequence

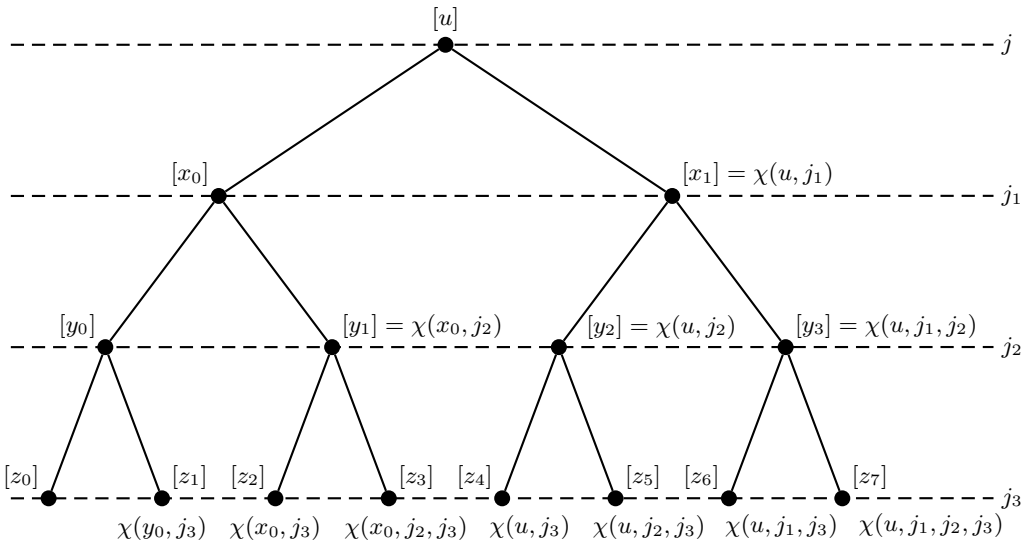

FIGURE 3. An example of a tree T with χ values specified.

of lines with $\ell \geq 0$. The function $\chi_S([x], j_1, j_2, \ldots, j_\ell)$, with $\ell + 1$ arguments, is defined by induction on ℓ. For the base case $\ell = 0$, define $\chi_S([x]) = [x]$.

Now let $\ell \geq 1$. Suppose $[x]$ has the property that its left and right subtrees in S each contain a node $[y]$ on the j_1-line for which $\chi_S([y], j_2, \ldots, j_\ell)$ is defined. Let $[y]$ be the leftmost such node in the right subtree of $[x]$ in S. Then $\chi_S([x], j_1, \ldots, j_\ell)$ is defined (written $\chi_S([x], j_1, \ldots, j_\ell)\!\downarrow$) and

$$\chi_S([x], j_1, \ldots, j_\ell) \;=\; \chi_S([y], j_2, \ldots, j_\ell).$$

In all other cases, $\chi_S([x], j_1, \ldots, j_\ell)$ is undefined.

When $S = T$, we write $\chi([x], j_1, \ldots, j_\ell)$ instead of $\chi_T([x], j_1, \ldots, j_\ell)$. Additionally, to simplify the notation, $\chi([x], j_1, \ldots, j_\ell) = [z]$ will be written as $\chi(x, j_1, \ldots, j_\ell) = z$.

We use the notation $\vec{\jmath}$ to stand for an increasing sequence $j_1, \ldots, j_\ell$. Additionally, $|\vec{\jmath}| = \ell$ is the length of the sequence $\vec{\jmath}$. Finally, we write $\vec{\jmath}' \subseteq \vec{\jmath}$ to denote that the sequence $\vec{\jmath}'$ is a subsequence of $\vec{\jmath}$. Note that $\chi_S(x, \vec{\jmath})$ is defined only for *internal* nodes $[x]$, and its value is also an internal node of S.

LEMMA 16. *Let S be T or one of its induced subtrees T_j. For fixed $\ell \geq 0$, the map $(x, j_1, \ldots, j_\ell) \mapsto \chi_S(x, j_1, \ldots, j_\ell)$ is injective.*

PROOF. We will suppress the subscript S from χ_S in what follows. First we prove the following subclaim: For fixed $j_1, \ldots, j_\ell$, the map $x \mapsto \chi(x, j_1, \ldots, j_\ell)$ is injective. We prove this by induction. The base case $\ell = 0$ is the injectivity of the identity function. For the induction step, suppose $\ell \geq 1$ and the map $x \mapsto \chi(x, j_2, \ldots, j_\ell)$ is injective. Suppose $[x] \neq [x']$ and that $\chi(x, j_1, \ldots, j_\ell) = \chi(x', j_1, \ldots, j_\ell)$ and these quantities are defined. This means that $\chi(y, j_2, \ldots, j_\ell) = \chi(y', j_2, \ldots, j_\ell)$, where $[y]$ is the leftmost node on the j_1-line in $[x]$'s right subtree for which $\chi(y, j_2, \ldots, j_\ell)\!\downarrow$, and similarly for $[y']$ in $[x']$'s right subtree. By

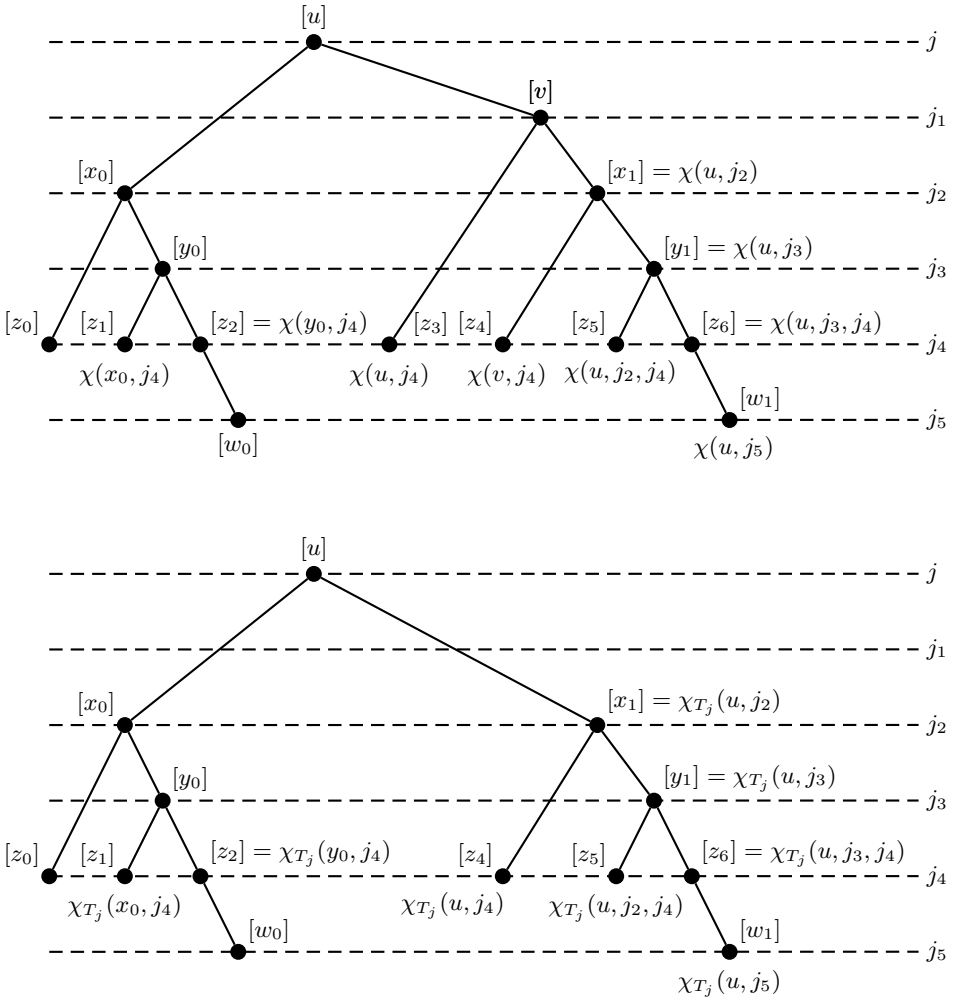

FIGURE 4. An example of a tree T (top) and T_j (bottom) with χ values specified. Each node is an internal node; the leaf nodes are not drawn.

the induction hypothesis, $z \mapsto \chi(z, j_2, \ldots, j_\ell)$ is injective. Therefore $[y] = [y']$, and $[y]$ is in the right subtrees of both $[x]$ and $[x']$. Thus, since $[x] \neq [x']$, one of $[x]$ and $[x']$ is an ancestor of the other, say $[x]$ is an ancestor of $[x']$. Since $\chi(x', j_1, \ldots, j_\ell)$ is defined, there must be some element, $[u]$, on the j_1-line in $[x']$'s left subtree for which $\chi(u, j_2, \ldots, j_\ell)\downarrow$. This element is to the left of $[y]$ on the j_1-line, and, since it is in the left subtree of $[x']$, it is in $[x]$'s right subtree. This is a contradiction, because $[y]$ is the leftmost node on the j_1-line in $[x]$'s right subtree for which $\chi(y, j_2, \ldots, j_\ell)$ is defined. This completes the proof of the subclaim.

To prove the lemma from the subclaim, we again argue by induction. The base case $\ell = 0$ is again the injectivity of the identity map. For the induction step, suppose that $(x, j_2, \ldots, j_\ell) \mapsto \chi(x, j_2, \ldots, j_\ell)$ is injective. Suppose $\chi(x, j_1, \ldots, j_\ell) = \chi(x', j'_1, \ldots, j'_\ell)$ (and are defined). Let $[y]$ be the leftmost node on the j_1-line in $[x]$'s right subtree such that $\chi(y, j_2, \ldots, j_\ell)\downarrow$ and $[y']$ be the leftmost node in on the j'_1-line in $[x']$'s right subtree such that $\chi(y', j'_2, \ldots, j'_\ell)\downarrow$. So,

$$\chi(y, j_2, \ldots, j_\ell) = \chi(x, j_1, \ldots, j_\ell) = \chi(x', j'_1, \ldots, j'_\ell) = \chi(y', j'_2, \ldots, j'_\ell)$$

By the induction hypothesis, $[y] = [y']$, and $j_k = j'_k$ for $k = 2, \ldots, \ell$. Since $[y] = [y']$ and these are on the j_1- and j'_1-lines, it follows that $j_1 = j'_1$. Therefore, $\chi(x, j_1, \ldots, j_\ell) = \chi(x', j_1, \ldots, j_\ell)$. By the subclaim, it follows that $[x] = [x']$. ⊣

LEMMA 17. *Let S be T or one of its induced subtrees T_j.*

1. *Suppose $\chi_S(x, j_1, \ldots, j_\ell) = z$, and $0 \leq k \leq \ell$. Then there is a $[y]$ such that $\chi_S(y, j_{k+1}, \ldots, j_\ell) = z$.*
2. *For fixed $[x]$, the map $\vec{\jmath} \mapsto \chi_S(x, \vec{\jmath})$ is injective.*
3. *Suppose $\chi_S(x, \vec{\jmath})\downarrow$ and that $\vec{\jmath}' \subseteq \vec{\jmath}$. Then also $\chi_S(x, \vec{\jmath}')\downarrow$.*
4. *Suppose $\chi_S(x, j_1, \ldots, j_\ell) = \chi_S(y, j'_1, \ldots, j'_{\ell'})$ with $[x]$ on the j_0-line, and $\ell < \ell'$. Then $j_0, \ldots, j_\ell$ is a suffix of $\vec{\jmath}$. That is, $j_i = j'_{i+\ell'-\ell}$ for $0 \leq i \leq \ell$.*

PROOF. In what follows, we suppress the subscript from χ_S.

Part 1. is proved by induction on k. When $k = 0$, just use $[y] = [x]$. The induction step is immediate from the definition of χ. Note that the $k = \ell$ case corresponds to $[y] = [z]$.

Suppose part 2. fails with $\chi(x, j_1, \ldots, j_\ell) = z$ and $\chi(x, j'_1, \ldots, j'_{\ell'}) = z$. By Lemma 16, $\ell \neq \ell'$; w.l.o.g., $\ell > \ell'$. By part 1., there is a y on the $j_{\ell-\ell'}$-line such that $\chi(y, j_{\ell-\ell'+1}, \ldots, j_\ell) = z$. By Lemma 16, $[y] = [x]$, which is a contradiction.

Part 3. is proved by induction on $|\vec{\jmath}'|$. If $\vec{\jmath}'$ is the empty sequence, $\chi(x, \vec{\jmath}')$ is equal to $[x]$ and hence defined. Otherwise, let k be such that j_k is the first entry in $\vec{\jmath}'$, namely $\vec{\jmath}'$ is the sequence $j_k, \vec{\jmath}''$. The value $\chi(x, j_k, \vec{\jmath}'')$ is defined if and only if there are nodes $[u]$ and $[v]$, on the j_k-line in the left and right subtrees of $[x]$ respectively, such that both $\chi(u, \vec{\jmath}'')\downarrow$ and $\chi(v, \vec{\jmath}'')\downarrow$. By part 1. and since $\chi(x, \vec{\jmath})\downarrow$, there are nodes $[u']$ and $[v']$ on the j_k-line such that $\chi(u', j_k, j_{k+1}, \ldots, j_\ell)\downarrow$ and $\chi(v', j_k, j_{k+1}, \ldots, j_\ell)\downarrow$. Thus, applying the the induction hypothesis twice, $\chi(u', \vec{\jmath}'')\downarrow$ and $\chi(v', \vec{\jmath}'')\downarrow$. Letting $u = u'$ and $v = v'$, this proves part 3.

Part 4. follows immediately by part 1. and Lemma 16. ⊣

It is an immediate consequence of parts 2. and 3. of Lemma 17 that if $\chi(x, \vec{\jmath})\downarrow$ then $|\vec{\jmath}| \leq \log m$. This is because there are 2^ℓ many $\vec{\jmath}' \subseteq \vec{\jmath}$ and each value $\chi(x, \vec{\jmath}')$ maps to a distinct node of the tree T, and T has only $m - 1$ internal nodes.

LEMMA 18. *Let S be T or one of its induced subtrees T_j. For $[y]$ a node in S, let $\ell_S(y)$ be the largest value ℓ such that $y = \chi_S(x, j_1, \ldots, j_\ell)$ for some $[x], j_1, \ldots, j_\ell$.*

1. *If $y = \chi_S(x, j_1, \ldots, j_\ell)$ and $[x]$ is the leftmost node on the j-line such that $\chi(x, j_1, \ldots, j_\ell)\downarrow$, then $\ell = \ell_S(y)$.*

2. *Conversely, if* $\chi_S(x, j_1, \dots, j_{\ell_S(y)}) = y$ *with* $[x]$ *on the* j*-line, then* $[x]$ *is the leftmost node on the* j*-line such that* $\chi_S(x, j_1, \dots, j_{\ell_S(y)})\downarrow$.

PROOF. To prove part 1., suppose there are $[x']$ and $j'_1, \dots, j'_{\ell'}$ with $\ell' > \ell$ such that $\chi_S(x', j'_1, \dots, j'_{\ell'}) = y$. By Lemma 17, part 4., $j_1, \dots, j_\ell$ is a proper suffix of $j'_1, \dots, j'_{\ell'}$ By the definition of χ, there is a $[z]$ in the left subtree of $[x']$ such that $\chi_S(z, j'_2, \dots, j'_{\ell'})\downarrow$. Thus, by Lemma 17, part 1., and the suffix property, there is a node $[v]$ in the left subtree of x such that $\chi_S(v, j_1, \dots, j_\ell)\downarrow$. This $[v]$ is on the same j-line as x, and is to the left of $[x]$.

For part 2., suppose there is a node $[x']$ on the j-line to the left of $[x]$ such that $\chi_S(x', j_1, \dots, j_{\ell_S}(y))\downarrow$. Pick $[x']$ to be the rightmost such node to the left of $[x]$. Let $[z]$ be the least common ancestor of $[x]$ and $[x']$. Then $\chi_S([z], j, j_1, \dots, j_{\ell_S(y)}) = y$, and this contradicts the definition of $\ell_S(y)$. ⊣

LEMMA 19. *For* $[x] \in T_j$, $[x]$ *on the* j*-line, the function* $\vec{\jmath} \mapsto \chi_{T_j}(x, \vec{\jmath})$ *maps surjectively onto the internal nodes of the right subtree of* T_j *rooted at* $[x]$.

PROOF. The left and right subtrees of $[x]$ in T_j are isomorphic by Lemma 14. For each $[z] \in T_j$ in the right subtree of $[x]$, let $[\widetilde{z}] \in T_j$ denote the corresponding node in the left subtree.

Fix an internal node $[z]$ in the right subtree of $[x]$. Let ℓ be the maximum value such that there exists $[y]$ in the subtree rooted at $[x]$ and exists $j_1, \dots, j_\ell$ so that $\chi_{T_j}(y, j_1, \dots, j_\ell) = z$. We claim that $[y] = [x]$ for the maximum value of ℓ. Suppose $[y] \neq [x]$. The node $[y]$ is on some line $j_0 < j_1$. Since $[y] \neq [x]$, $[y]$ is in $[x]$'s right subtree. Furthermore, $[\widetilde{y}]$ is on the j_0-line in $[x]$'s left subtree, and by Lemma 14, $\chi_{T_j}(\widetilde{y}, j_1, \dots, j_\ell)\downarrow$. Let $[u]$ be the rightmost node on the j_0-line to the left of $[y]$ such that $\chi_{T_j}(u, j_1, \dots, j_\ell)\downarrow$. There must exist such a $[u]$ since $[\widetilde{y}]$ has these properties. Let $[v]$ be the least common ancestor of $[u]$ and $[y]$. From the choice of $[u]$, it follows that $\chi_{T_j}(v, j_0, j_1, \dots, j_\ell) = z$. This contradicts the maximality of ℓ. ⊣

An example of Lemma 19 can be seen in Figure 4. Observe that every node in the right subtree of $[u]$ in the tree T_j (bottom) is of the form $\chi(u, \dots)$.

LEMMA 20. *If* $[x] \in T_j$ *and* $\chi_{T_j}(x, j_1, \dots, j_\ell)$ *is defined, then* $\chi(x, j_1, \dots, j_\ell)$ *is defined (in* T*).*

PROOF. The claim is proved by induction on ℓ. For the base case is trivial as $\chi_{T_j}(x) = \chi(x) = x$. For the induction step, suppose $\chi_{T_j}(x, j_1, \dots, j_\ell)$ is defined. The left and right subtrees of $[x]$ in T_j both contain nodes $[y]$ on the j_1-line such that $\chi_{T_j}(y, j_2, \dots, j_\ell)\downarrow$. By the induction hypothesis, $\chi(y, j_2, \dots, j_\ell)\downarrow$ for both $[y]$'s. Thus $\chi(x, j_1, \dots, j_\ell)$ is defined. ⊣

An example of Lemma 20 can be seen in Figure 4. Observe that $\chi_{T_j}(u, j_4)$ is defined, and equals z_4. So the lemma guarantees that $\chi(u, j_4)$ is defined. However, $\chi(u, j_4) = z_3 \neq \chi_{T_j}(u, j_4)$.

2.3. The hereditary matrix A'. We use the χ function to define a hereditary matrix associated with A.

DEFINITION 21. The *hereditary matrix* A' *associated with* A is the 0/1 matrix with n columns such that:

- For all $x, j_0, \ldots, j_\ell$, if $[x]$ is on the j_0-line, and $\chi(x, j_1, \ldots, j_\ell)$ is defined, then there is a row in A' with 1's in columns $j_0, \ldots, j_\ell$ and 0's elsewhere.
- A' consists only of these rows, together with the zero row.

LEMMA 22. *If A' is the hereditary matrix associated with A, then A' is hereditary. Moreover, A' is an $m \times n$ matrix, and thus is the same size as A.*

PROOF. Let r be a row of A', with 1's in the $\ell+1$ columns $j_0 < j_1 < \cdots < j_\ell$, and 0's in all other columns. We must show that the row obtained by replacing any 1 in r with a 0 is also in A'. This holds for the 1's in any of the columns $j_1, \ldots, j_\ell$ by part 3. of Lemma 17. So, consider replacing the leftmost 1, in column j_0, with a 0. By definition of A', $\chi(x, j_1, \ldots, j_\ell)$ is defined for some $[x]$ on the j_0-line. Therefore, there is a node $[y]$ on the j_1-line such that $\chi(y, j_2, \ldots, j_\ell)\downarrow$, and thus A' contains a row with 1's in columns $j_1, \ldots, j_\ell$ and 0's elsewhere.

To prove that A' has m rows, we define a bijection Θ from the non-zero rows of A' onto the internal nodes of T. Let r be a row of A' with 1's in (only) columns, $j_0, \ldots, j_\ell$. Let $[x]$ be the leftmost node on the j_0-line for which $\chi(x, j_1, \ldots, j_\ell)$ is defined. Then Θ is defined by $\Theta(r) = \chi(x, j_1, \ldots, j_\ell)$.

To prove that Θ is a bijection, we show it has an inverse. Let $[y]$ be an internal node of T. Then there are $[x]$ on the j-line, and $j_1, \ldots, j_{\ell(S)}$ which satisfy all the properties of Lemma 18. Thus, A' contains a row r with 1's in (only) columns $j, j_1, \ldots, j_{\ell_S(y)}$, and $\Theta(r) = y$. By Lemmas 17 and 18, r is the only row with $\Theta(r) = y$. ⊣

DEFINITION 23. For $0 \leq j < n$, let X_j denote the set of rows of A' with a 1 in column j.

LEMMA 24. $|X_j| \geq |P_j|/2$.

PROOF. Recall the bijection Θ defined in the proof of Lemma 22, which maps rows of A' to internal nodes of T. By part 4. of Lemma 17, if $[x]$ is on the j-line, and $\chi(x, j_1, \ldots, j_\ell)\downarrow$, then $\Theta^{-1}(\chi(x, j_1, \ldots, j_\ell)) \in X_j$. So it suffices to show that there are at least $|P_j|/2$ many nodes $[z]$ such that $\chi(x, \vec{j}) = z$ for some $[x]$ on the j-line, and some sequence $\vec{j}$.

Let $[x]$ be an internal node of T on the j-line. and let S be the subtree of T rooted at $[x]$. We claim that there are at least $|P_j \cap S|/2$ many distinct nodes of the form $\chi(x, \vec{j})$. This will prove the lemma, because P_j is the union over all such S's of $P_j \cap S$.

The claim is trivial if $P_j \cap S = \emptyset$. Otherwise, we have $|P_j \cap S| \geq 2$. The subtree of T_j rooted at $[x]$ has $|P_j \cap S| - 1$ many internal nodes. Thus, by Lemma 14, the right subtree has $(|P_j \cap S| - 2)/2 = |P_j \cap S|/2 - 1$ many internal nodes. By Lemma 19, it follows that there are $|P_j \cap S|/2 - 1$ many $\vec{j}$'s for which $\chi_{T_j}(x, \vec{j})$ is defined. By Lemma 20, it follows that there are at least that many $\vec{j}$'s for which $\chi(x, \vec{j})$ is defined (in T). Furthermore, the node $\chi(x)$ is also defined, so the number of nodes of the form $\chi(x, \vec{j})$ is at least $|P_j \cap S|/2$. ⊣

The results above are summarized in the following lemma. An $m \times n$ counterexample to Frankl's Theorem for t is an $m \times n$ 0/1 matrix A of distinct rows such that $|P_j| \geq 2^t$ for all j.

LEMMA 25. *If A is an $m \times n$ counterexample to Frankl's Theorem for t. Then A' is an $m \times n$ hereditary counterexample to Frankl's Theorem for t.*

PROOF. We have shown that A' is $m \times n$ and hereditary. Define P'_j for A' in the same way that P_j was defined for A. Since A' is hereditary, $|P'_j| = 2|X_j|$. And, the fact that A' is a counterexample for Frankl's theorem for t follows immediately from Lemma 24 and the hypothesis that A is a counterexample. $\dashv$

2.4. The functional Kruskal-Katona Theorem. Lemma 25 brings us back to the usual proof of Frankl's Theorem. Namely the usual proof of Frankl's Theorem is by contradiction and constructs a hereditary matrix violating the conditions of Frankl's Theorem and then gives a simple argument based on the Kruskal-Katona Theorem to show that no such hereditary matrix exists.

We are interested in quasipolynomial size Frege proofs of Frankl's Theorem. Section 3.1 will argue that Lemma 25 can be expressed and proved with quasipolynomial size Frege proofs. Furthermore, Bonet, Buss, and Pitassi [2] showed that there are polynomial size Frege proofs of the Kruskal-Katona Theorem (in the form of Theorem 6), and from this, that there are polynomial size Frege proofs of Frankl's Theorem for hereditary matrices. These constructions, with Lemma 25, suffice to prove Theorem 8.

To prove Theorem 9 with t constant we need to use the functional form of the Kruskal-Katona Theorem (Theorem 7). This allows proving Theorem 7 with an argument that that can be formalized with constant-depth Frege proofs. In addition, we restructure the proof of Frankl's Theorem to use the pigeonhole principle instead of a counting argument; this will allow us to prove Frankl's Theorem from the Kruskal-Katona Theorem with arguments that can be formalized with constant-depth Frege proofs.

We next prove Theorem 7. Our argument will be somewhat circular: for $m = m_0 + m_1 > 1$ with $m_0 \geq m_1$, we will assume the existence of a function

$$g_{m_0,m_1}(x) : \{0, \ldots, m-1\} \to (\{0\} \times \{0, \ldots, m_0 - 1\}) \cup (\{1\} \times \{0, \ldots, m_1 - 1\})$$

such that $g(a) = \langle 0, b\rangle$ implies $|a|_1 \geq |b|_1$ and such that $g(a) = \langle 1, b\rangle$ implies $|a|_1 \geq |b|_1 + 1$. The existence of these functions follows immediately from the Kruskal-Katona Theorem of course! This circularity should not be too disturbing, however: the point is that we know the Kruskal-Katona Theorem is true, we only want to give arguments that can be formalized with constant depth Frege proofs. As it turns out, we only need the Kruskal-Katona Theorem for small values of m, namely the parameter m of the Kruskal-Katona Theorem will be equal to the value 2^{t-1} of Frankl's Theorem (not the value m of Frankl's Theorem!). Thus, we only need to appeal to polynomially many of the functions g_{m_0,m_1}, and these can just be hardcoded into the Frege proofs.

PROOF OF THEOREM 7. We argue by induction on m. Let j be the leftmost column in A with a 1 appearing column j. Let A_0 be the set of rows in A with a 0 in column j. Let A_1 be all the other rows in A. Let A_1^* be the strings in $\{0,1\}^n$ which are obtained from rows of A_1 by replacing the 1's in column j with 0's.

Let $m_0 = |A_0|$ and $m_1 = |A_1^*| = |A_1|$. By choice of j and the fact that A is hereditary, $m > m_0 \geq m_1$. By two applications of the induction hypothesis, there are maps

$$f_0 : \{0, \ldots, m_0 - 1\} \to A_0 \text{ and } f_1 : \{0, \ldots, m_1 - 1\} \to A_1^*$$

with the property that $f_i(b) = a$ implies $|a|_1 \leq |b|_1$.

Consider the function g_{m_0,m_1} discussed above. To define the function $f : \{0,\ldots,m-1\} \to A$, set

$$f(b) \;=\; \begin{cases} f_0(x) & \text{if } g_{m_0,m_1}(b) = \langle 0,x\rangle \\ f_1(x) + 2^j & \text{if } g_{m_0,m_1}(b) = \langle 1,x\rangle \end{cases}$$

where $f_1(x) + 2^j$ denotes the row $f_1(x)$, with a 1 replacing the 0 in column j.

To finish the proof, we claim that $f(b) = a$ implies $|a|_1 \le |b|_1$. If $g_{m_0,m_1}(b) = \langle 0,x\rangle$, then $|a|_1 = |f_0(x)|_1 \le |x|_1 \le |b|_1$. And if $g_{m_0,m_1}(b) = \langle 1,x\rangle$, then $|a|_1 = |f_1(x)|_1 + 1 \le |x|_1 + 1 \le |b|_1$. ⊣

Frankl's Theorem for hereditary matrices follows as an immediate consequence of the next lemma and the pigeonhole principle.

LEMMA 26. *Let A be an $m \times n$ 0/1 hereditary matrix with distinct rows and with $|P_j| \ge 2^t$ for all j. Let D be the least common multiple of the integers $1,2,3,\ldots,t$. Then there is an injection from a set of size $\frac{2^t-1}{t} \cdot D \cdot n$ to a set of size $(m-1)\cdot D$.*

The least common multiple $D = D(t)$ of $1,2,\ldots,t$ satisfies $|D| = O(t)$, see e.g. [9, Thm. 414].

PROOF. Let Y_j be the set of rows in A with a 1 in column j. Let Y_j^* be the strings $r \in \{0,1\}^n$ obtained from rows of Y_j by replacing the 1's in column j with 0's. By hypothesis, $|Y_j^*| \ge 2^{t-1}$. The set Y_j^* is hereditary since A is. Let $Z_j \subset Y_j^*$ be a canonical hereditary subset with $|Z_j| = 2^{t-1}$, for example the least 2^{t-1} elements of Y_j^* in the lexicographic ordering. Let $B = \{0,\ldots,2^{t-1}-1\}$. Define A^+ and B^+ as follows:

$$A^+ = \{\langle a,k\rangle : a \ne \vec{0} \text{ is a row of } A \text{ and } 0 \le k < D\}$$
$$B^+ = \{\langle b,k\rangle : b \in B \text{ and } 0 \le k < \tfrac{D}{|b|_1+1}\}.$$

The matrix A is hereditary with m distinct rows, $\vec{0}$ is a row of A, and so,

$$|A^+| = (m-1)\cdot D.$$

Since B can be viewed as the set of all strings in $\{0,1\}^{t-1}$,

$$|B^+| \;=\; \sum_{i=0}^{t-1} \binom{t-1}{i} \frac{D}{i+1} \;=\; \sum_{i=1}^{t} \binom{t}{i} \frac{D}{t} \;=\; \frac{(2^t-1)\cdot D}{t}.$$

We show there is an injection from $\{0,\ldots,n-1\} \times B^+$ to A^+. By Theorem 7, now with $m = |B| = 2^{t-1}$, there are bijections $f_j : B \to Z_j$ so that $|f_j(b)|_1 \le |b|_1$ for all $b \in B$.

Define $\Phi : \{0,\ldots,n-1\} \times B^+ \to A^+$ by

$$(j,b,k) \mapsto \left(f_j(b) + 2^j,\; \frac{D}{|f_j(b)|_1 + 1} \cdot j' + k \right),$$

where j' is the number of 1's to the left of column j in $f_j(b)$. Note that the fraction is always an integer by choice of D. To see that Φ maps into A^+, observe that $f_j(b) + 2^j \ne \vec{0}$ and

$$\frac{D}{|f_j(b)|_1 + 1} \cdot j' + k \;<\; D.$$

since $j' \leq |f_j(b)|_1$ and $k < \frac{D}{|b|_1+1} \leq \frac{D}{|f_j(b)|_1+1}$.

We show that Φ is injective by showing that it has an inverse. Given $\Phi(j,b,k) = \langle a, k' \rangle$, we show how to recover j, b and k. We have $a = f_j(b) + 2^j$, and $k' = \frac{D}{|a|_1} j' + k$ with j' the number of 1's to the left of column j in a.

From a, we compute $\frac{D}{|a|_1}$. Since $k < \frac{D}{|a|_1}$, we can obtain j' and k using $k' = \frac{D}{|a|_1} j' + k$. Then, from j' and $a + 2^j$, we can recover j, and from j and a, we can recover $b = f_j^{-1}(a - 2^j)$. $\dashv$

§3. Formalization as Frege proofs. This section sketches the proofs of Theorems 8 and 9 by showing how to transform the above proofs of Theorem 3 into families of quasipolynomial size Frege proofs (respectively, polynomial size, constant depth Frege proofs).

3.1. Quasipolynomial size Frege proofs. Recall that an $m \times n$ 0/1 matrix A is represented by propositional variables $p_{i,j}$ where $0 \leq i < m$ and $0 \leq j < n$. Section 1.2 already introduced the formulas $\text{EQ}(i,i',j)$, $\text{CARDP}(j)$, and DISTINCTROWS. We shall argue that the other concepts used in the proof of Theorem 3 can all be expressed by polynomial or quasipolynomial size Boolean formulas.

First, we need formulas that define the tree T. The leaves of T are just the rows of A. Accordingly, a leaf is specified by a value i with $0 \leq i < m$. An internal node $[x]$ of T will be specified by giving a pair (i,i') of leaves, one in each of the two subtrees of $[x]$ in T. In order to make the choices the choices for i and i' unique, we always use the least values i and i'. Accordingly, we define

$$\text{EQTO}(i,i',j) := \bigwedge_{j'=0}^{j-1} (p_{i,j'} \leftrightarrow p_{i',j'})$$

$$\text{FIRSTEQTO}(i,j) := \bigwedge_{i'=0}^{i-1} \neg\text{EQTO}(i,i',j).$$

Then, for $i \neq i'$, we define $\text{TNODELN}(i,i',j)$ to mean that the rows i and i' define a node $[x] \in T$ on the j-line, as

$$\text{TNODELN}(i,i',j) := \text{EQTO}(i,i',j) \wedge \text{FIRSTEQTO}(i,j+1) \wedge \text{FIRSTEQTO}(i',j+1) \wedge \overline{p}_{i,j} \wedge p_{i',j}.$$

For $i = i'$, $\text{TNODELN}(i,i,n)$ is defined to be the constant *True*. For $j < n$, $\text{TNODELN}(i,i,j)$ is the constant *False*. Finally, the nodes of T are defined by the pairs (i,i') satisfying

$$\text{TNODE}(i,i') := \bigvee_{j=0}^{n} \text{TNODELN}(i,i',j).$$

It is straightforward to give formulas defining structural properties of T. For instance, the node (i_2, i_2') is in the left subtree below the node $(i_1, i_1\prime)$ iff

$$\begin{aligned}&\textsc{InLeft}(i_1, i_1'; i_2, i_2') \ :=\\ &\bigvee_{j_1<j_2}\Big(\textsc{TNodeLn}(i_1, i_1', j_1) \wedge \textsc{TNodeLn}(i_2, i_2', j_2)\\ &\qquad\wedge\textsc{EqTo}(i_1, i_2, j_1)\Big) \wedge \overline{p}_{i_2,j_1}\Big).\end{aligned}$$

InRight is defined similarly, but with $\overline{p}_{i_2,j_1}$ replaced with p_{i_2,j_1}.

The rows of A are lexicographically ordered by

$$\textsc{ToLeft}(i, i') \ := \bigvee_{j=0}^{n-1}\Big(\overline{p}_{i,j} \wedge p_{i',j} \wedge \textsc{EqTo}(i, i', j)\Big)$$

ToLeft also permits us to order nodes of T from left to right.

We can now give quasipolynomial size formulas defining the (graph of the) χ functions. $\textsc{Chi}(i_1, i_1'; j_1, \dots, j_\ell; i_2, i_2')$ will define the property $\chi(x, j_1, \dots, j_k) = z$ where the (i_1, i_1') and (i_2, i_2') represent nodes $[x]$ and $[z]$ in T. For $\ell = 0$, $\textsc{Chi}(i_1, i_1'; i_2, i_2')$ is true iff $i_1 = i_2$, $i_1' = i_2'$, $i_1 \neq i_1'$, and $\textsc{TNode}(i_1, i_1')$. Then, inductively for $\ell \geq 1$, define

$$\begin{aligned}&\textsc{Chi}(i_1, i_1'; j_1, \dots, j_\ell; i, i') \ :=\\ &\bigvee_{k_1,k_1'}\bigvee_{k_2,k_2'}\Bigg[\textsc{TNodeLn}(k_1, k_1', j_1) \wedge \textsc{InLeft}(i_1, i_1'; k_1, k_1')\\ &\quad\wedge \textsc{TNodeLn}(k_2, k_2', j_1) \wedge \textsc{InRight}(i_1, i_1'; k_2, k_2')\\ &\quad\wedge \textsc{Chi}(k_2, k_2'; j_2, \dots, j_\ell; i, i') \wedge \bigvee_{k,k'} \textsc{Chi}(k_1, k_1'; j_2, \dots, j_\ell; k, k')\\ &\quad\wedge \neg\Big(\bigvee_{k_3,k_3'}\Big(\textsc{TNodeLn}(k_3, k_3', j_1) \wedge \textsc{InRight}(i_1, i_1'; k_3, k_3')\\ &\qquad\qquad\wedge\textsc{ToLeft}(k_3, k_2) \wedge \bigvee_{k,k'} \textsc{Chi}(k_3, k_3'; j_2, \dots, j_\ell; k, k')\Big)\Big)\Bigg].\end{aligned}$$

The Chi formulas are readily modified to define the functions χ_T, for $T = T_j$. The leaves of T that are in P_j are definable by letting $\textsc{Pj}(i, j)$ be $\vee_{i'\neq i}\textsc{Eq}(i, i', j)$. The formula $\textsc{TjNode}(i, i', j)$ that defines the property of (i, i') being a node in T_j can be defined similarly to $\textsc{TNode}(i, i')$ but restricting to leaves that lie in T_j. The χ_{T_j} function can be defined similarly to the χ function by a formula $\textsc{ChiTj}(i_1, i_1'; j_1, \dots, j_\ell; i, i'; j)$ which has j as an extra parameter. We leave the details of formalizing TjNode and ChiTj to the reader.

All of the formulas defined above, except Chi and ChiTj, are constant depth and have polynomial size (in m, n). The formulas Chi and ChiTj, however, are defined inductively on ℓ, and have depth $O(\ell)$ and thus quasipolynomial formula size. In other words, the χ function is NC^2-definable. In fact, since the values of $j_1, \dots, j_\ell$ are fixed, the Chi and ChiTj have polynomial size, unbounded fan-in *circuits* of depth $O(\ell)$, so (the graph of) the function χ is even in AC^1.

The number of distinct propositional formulas CHI and CHITJ formulas that need to be constructed can be bounded by $m^4 n^{O(\log m)}$. This is because the CHI formula has four parameters i_1, i_1', i, i' that range over the m rows of A and ℓ parameters ($\ell+1$ for CHITJ) that range over the n columns of A. The value ℓ is bounded by $\log m$ by part 3. of Lemma 17 and the injectivity of the χ function (Lemma 16). This means there are quasipolynomially many formulas $\text{CHI}(\cdots)$ and $\text{CHITJ}(\cdots)$.

We have shown how to express concepts such as the trees T and T_j and the χ and χ_j functions with quasipolynomial size formulas. It is now straightforward to formulate and prove the propositional translations of Lemmas 14 through 25 with quasipolynomial size Frege proofs. Indeed the proofs of these lemmas are all very concrete and constructive, and they are straightforward to translate into propositional logic.

Although it is left to the reader to verify that the translations to propositional logic can be carried out straightforwardly, we do mention a couple points. First, as usual, the propositional proofs replace the use of induction in the proofs of Lemmas 14-25 with a "brute-force induction" or "exhaustive" enumeration of cases. For example, the propositional translation of Lemma 16 becomes the propositional formulas

$$\neg\big(\text{CHI}(i_1, i_1'; j_1, \dots, j_\ell; i_2, i_2') \wedge \text{CHI}(i_1, i_1'; j_1, \dots, j_\ell; i_3, i_3')\big)$$

for all values of the parameters with (i_2, i_2') not equal to (i_3, i_3'). The propositional proof proves all the statements, for all such values, successively for ℓ equal to 0 up $\log m$. Second, note that the hereditary matrix A', as defined in Definition 21 has quasipolynomially many possible rows. The proof of Lemma 25 gives an injection from the rows of A' to the rows of A, and, with this injection, propositional proofs can be used to bound the number of rows of A.

As already discussed, [2] showed that polynomial size Frege proofs can prove the hereditary version of Frankl's Theorem. This completes the proof of Theorem 8 that the propositional translations of Frankl's Theorem have quasipolynomial size Frege proofs.

3.2. Polynomial size constant-depth proofs. For t fixed, Theorem 9 asserts the existence of polynomial size, constant depth Frege proofs of Frankl's Theorem. The first difficulty is that the predicates CHI and CHITJ are defined with formulas of depth $O(\log m)$, since the function $\chi(x, j_1, \dots, j_\ell)$ might be invoked with ℓ as large as $\log m$. To avoid this, we modify Definition 21 of the hereditary matrix A' to restrict attention to rows that have at most t many 1's:

DEFINITION 27. The matrix $A'_{\leq t}$ is the 0/1 matrix which contains as rows exactly those rows of A' which have $\leq t$ many 1's.

We have the following analogue of Lemma 22:

LEMMA 28. *A' is an $m' \times n$ hereditary matrix, where $m' \leq m$ and $m' < n^t$.*

PROOF. The fact that $A'_{\leq t}$ is hereditary follows immediately by the same argument that showed A' is hereditary. The fact that $m < n^t$ follows from the fact that there are $< n^t$ many subsets of $\{1, \dots, n\}$ of size $\leq t$. Finally, $m' \leq m$ is proved by showing, as in the proof of Lemma 22, that the function Θ is an

injective map from the nonzero rows of $A'_{\leq t}$ into the internal nodes of T. (It may not be surjective, however.) $\dashv$

We also need to modify the definition of X_j:

DEFINITION 29. For $0 \leq j < n$, let $X_{j,\leq t}$ denote the set of rows of $A'_{\leq t}$ with a 1 in column j.

LEMMA 30. $|X_{j,\leq t}| \geq \min\{|P_j|/2, 2^{t-1}\}$.

Clearly, this is related to Lemma 24. The point is that the proof of Lemma 30 only needs to reason with rows of $A'_{\leq t}$, not with rows of A'.

PROOF. The argument splits into two cases. First suppose there is some row r of $X_{j,\leq t}$ which contains t many 1's. There are 2^{t-1} many rows which can be obtained from r by deleting 1's from columns other than column j. These all lie in $X_{j,\leq t}$, so $|X_{j,\leq t}| \geq 2^{t-1}$.

Second suppose that all rows in $X_{j,\leq t}$ contain fewer than t many 1's. Then the argument used in the proof of Lemma 24 applies to show that $|X_{j,\leq t}| \geq |P_j|/2$. $\dashv$

Similarly to Lemma 25, we now get the following:

LEMMA 31. *If A is an $m \times n$ counterexample to Frankl's Theorem for t. Then $A'_{\leq t}$ is an $m' \times n$ hereditary counterexample to Frankl's Theorem for t with $m' \leq m$.*

We claim that, using Lemmas 28, 30 and 31, the entire proof of Frankl's theorem for constant t can by formalized by a constant depth, polynomial size Frege proofs in which all formulas have depth $O(t)$. We sketch the proof of this claim below.

First, the basic properties of the tree T, using formulas TNODELN, TNODE, INRIGHT, etc., can be expressed with constant depth, polynomial size formulas. Second, counting sets up to a constant cardinality, say $s = O(t)$ or $s = O(2^t)$, can be done with polynomial size formulas (for fixed t). To see this, let $\phi_1, \ldots, \phi_n$ be formulas. Expressing that $\geq s$ of the ϕ_i's are true can be expressed by letting $\mathcal{I}$ range over subsets of $\{1, \ldots, n\}$ of size exactly s, and writing $\bigvee_{\mathcal{I}} \bigwedge_{i \in \mathcal{I}} \phi_i$. This allows the statement $\text{CARDP}(j) < 2^t$ to be expressed by a constant depth, polynomial size formula. Therefore, for fixed t, Frankl's Theorem can be stated with constant depth, polynomial size formulas.

Thirdly, as can be straightforwardly checked, the predicates CHI and CHITJ, when retricted to $\ell \leq t$ can be expressed by Boolean formulas of depth $O(t)$ and size $n^{O(t)}$.

These considerations allow Lemmas 14-20 and 28-31 to be expressed with constant depth, polynomial size Boolean formulas, and proved with constant depth, polynomial size Frege proofs. The assertion "$m' \leq m$" of Lemmas 28 and 31 cannot be expressed explicitly as constant depth polynomial size formulas. Instead, it is formalized by defining an injection from the rows of $A'_{\leq t}$ into the rows of A. Recall that Θ is an injection from the nonzero rows of $A'_{\leq t}$ into the internal nodes of T. The rows of A are the same as the leaves of T, and it is easy to explicitly give between the internal nodes of T and the leaves of T, omitting one leaf (say, the leftmost leaf). By composition, there is an injection from the

rows of $A'_{\leq t}$ into the rows of A. Constant depth, polynomial size Frege proofs can define this injection, and prove its properties.

Finally, we need to argue that the arguments in Section 2.4 can be formalized as polynomial size, constant depth Frege proofs.

We sketch how to formalize Section 2.4's proof of Theorem 7 as polynomial size, constant depth Frege proofs, when m is a constant.[1] The difficulty is that the proof given above defines the function f by induction in a way that is not readily formalizable with constant depth formulas. However, the key point is that f is a map from $\{0, \ldots, m-1\}$ onto the rows of A, and since m is constant, there are only finitely many possibilities for f. It is convenient to now work with the inverse of f, which we denote F. Theorem 7 is proved by using "brute-force" induction, for ℓ ranging from n down to 1 to prove the following assertion. We let $E_{\ell,i}$ denote the set of rows of A that agree with row i in their first ℓ entries. We let $r_{\ell,i}$ be the last $n - \ell$ columns of row i (that is, discarding the first ℓ columns).

> There is a function F_ℓ (not necessarily injective) from the m many rows of A into $\{0, \ldots, m-1\}$ such that: for each row i, $0 \leq i < m-1$, (a) $|F(i)|_1 \geq |r_{\ell,i}|_1$, and (b) F_ℓ restricted to $E_{\ell,i}$ is a bijection onto $\{0, \ldots, |E_{\ell,i}| - 1\}$.

This assertion is expressible as a polynomial size, constant depth formula, since m is constant and there are only finitely many possibilities for F_ℓ. Furthermore, the argument from the proof of Theorem 7 readily shows that the existence of F_ℓ follows from the existence of the F_k's for $k > \ell$ (and from the finitely many functions g_{m_0,m_1}). Finally, the f of Theorem 7 is just the inverse of F_0.

The proof of Theorem 26 is straightforward to formalize with polynomial size, constant depth Frege proofs. This follows from the facts that, since t is constant, the value $D = D(t)$ is a fixed constant, and that the proof of Theorem 26 gives an explicit construction of the injection and only involves counting up to a constant.

This completes the proof of Theorem 9.

§4. Equivalent definitions of the hereditary matrix. The usual proof of Frankl's theorem uses a much simpler construction of a hereditary counterexample matrix than the χ-function procedure of Definition 21. The construction starts with a matrix A which, by hypothesis, violates Frankl's theorem. If A is not hereditary, there is some entry 1 in A, such that if this 1 is replaced with a 0 the matrix still contains distinct rows. A hereditary counterexample matrix is formed by iteratively replacing such 1's with 0's until a hereditary matrix is obtained. It is easy to verify that this process preserves the property that the matrix violates Frankl's thoerem. This construction as described in [7, 2] did not specify the order in which 1's are to be replaced with 0's. We shall prove that there is some order for changing 1's to 0's such that the Frankl construction yields the same matrix as our matrix A' constructed in Section 2.3.

[1] Recall that the variable m is used in different ways for Frankl's Theorem and the Kruskal-Katona Theorem. In our applications, the value for the Kruskal-Katona Theorem is $m = 2^{t-1}$ and this is constant since t is.

The next definition describes the effect of replacing all 1's in column j with 0's which do not identify any pair of rows. Recall that if $r \in \{0,1\}^n$ is a row with a 1 in column j, then $r - 2^j$ represents the same row but with that 1 replaced with 0. Throughout this section, let A be an $m \times n$ 0/1-matrix with distinct rows.

DEFINITION 32. Let $0 \leq j < n$, and let A_0, resp. A_1, denote the rows of A with a 0, resp. 1, in column j. The *downshift* of A in column j is the matrix DownShift(A, j) containing the rows

$$A_0 \cup \{r : r \in A_1,\, r - 2^j \in A_0\} \cup \{r - 2^j : r \in A_1,\, r - 2^j \notin A_0\}.$$

DEFINITION 33. Let $0 \leq j < n$. Then A is *hereditary in column j* if, for any row r of A with a 1 in column j, $r - 2^j$ is also a row in A.

By definition, the matrix DownShift(A, j) is hereditary in column j.

DEFINITION 34. Define the sequence of matrices $A^{(n)}$, $A^{(n-1)}, \ldots, A^{(1)}, A^{(0)}$ by letting $A^{(n)}$ equal A, and $A^{(j)}$ equal DownShift$(A^{(j+1)}, j)$ for each $j < n$.

LEMMA 35. *The matrix $A^{(j)}$ is hereditary in columns $j, j{+}1, \ldots, n{-}1$. In particular, $A^{(0)}$ is hereditary.*

PROOF. The proof is by induction on $j = n, \ldots, 1, 0$. The base case of $j = n$ is trivial. For the induction step, suppose $A^{(j+1)}$ is hereditary in columns $j{+}1, \ldots, n{-}1$. By the definition of DownShift, $A^{(j)}$ is hereditary in column j, so we need to prove that it is hereditary in all columns $k > j$. Consider a row $w = u1z$ is in $A^{(j)}$, where $|u| = k > j$. We need to prove that $u0z$ is a row of $A^{(j)}$.

Write u in the form xiy where $|x| = j$ and $i \in \{0,1\}$ and $|y| = k - j - 1$. Thus w is equal to $xiy1z$. First suppose $w = x1y1z$. Since $x1y1z$ is a row of $A^{(j)}$ and has a 1 in column j, both $x1y1z$ and $x0y1z$ are present as rows in $A^{(j+1)}$. Since $A^{(j+1)}$ is hereditary in column k, $x1y0z$ and $x0y0z$ are rows of $A^{(j+1)}$. Thus, by the definition of DownShift, $x1y0z = u0z$ is also a row of $A^{(j)}$.

Otherwise, $w = x0y1z$. If w is also a row of $A^{(j+1)}$, then since $A^{(j+1)}$ is hereditary in column k, $x0y0z$ is also a row of $A^{(j+1)}$. Therefore, $x0y0z = u0z$ is a row of $A^{(j)}$. Otherwise, $x1y1z$ is a row of $A^{(j+1)}$, but $x0y1z$ is not. Since $A^{(j+1)}$ is hereditary in column k, $x1y0z$ is a row of $A^{(j+1)}$. Therefore, by the definition of DownShift, $x0y0z = u0z$ is a row of $A^{(j)}$. ⊣

LEMMA 36. *Let A be hereditary in columns $j, \ldots, n-1$, let $[x]$ be a node of T on the j_0-line, $j \leq j_0$, and let u be the string*

$$x10^{j_1 - j_0 - 1}10^{j_2 - j_1 - 1}1 \cdots 10^{j_\ell - j_{\ell-1} - 1}10^{n - j_\ell - 1}. \tag{1}$$

In other words, u is x plus 1's in columns $j_0, \ldots, j_\ell$. Then $\chi(x, j_1, \ldots, j_\ell)\!\downarrow$ iff u is a row of A.

PROOF. Suppose $\chi(x, j_1, \ldots, j_\ell)\!\downarrow$. We argue by induction on ℓ. For the base base, $\ell = 0$, we have u equal to $x10^{n - j_0 - 1}$ and since x is a maximal representative for $[x]$, A has a row $x1w$ for some $w \in \{0,1\}^{n - j_0 - 1}$ By the hereditary property, u is also a row of A. For the induction step, suppose $\ell > 0$. Then there is a

$[y]$ in the right subtree of $[x]$ on the j_1-line such that $\chi(y, j_2, \ldots, j_\ell)\downarrow$. We have $y = x1w$ for some $w \in \{0,1\}^{j_1 - j_0 - 1}$. By the induction hypothesis,

$$x1w10^{j_2 - j_1 - 1}1 \cdots 10^{j_\ell - j_{\ell-1} - 1}10^{n - j_\ell - 1}$$

is a row of A. Thus, by the hereditary property, u is also a row of A.

For the converse, suppose u is a row of A. We again argue by induction on ℓ. First suppose $\ell = 0$. By the hereditary property, $x0^{n-j_0-1}$ is a row of A. Thus, $[x]$ exists as an internal node of T, and we have $\chi(x)\downarrow$. Second, suppose $\ell > 0$. Let $y_0 = x0^{j_1 - j_0}$ and, $y_1 = x10^{j_1 - j_0 - 1}$. Using the hereditary property of A, both of $[y_0]$ and $[y_1]$ exist as nodes of A. Applying the induction hypothesis twice and using the hereditary property of A, $\chi(y_0, j_2, \ldots, j_\ell)\downarrow$ and $\chi(y_1, j_2, \ldots, j_\ell)\downarrow$. Since $[y_0]$ and $[y_1]$ lie on the j_1-line in the left and right subtrees of $[x]$, respectively, $\chi(x, j_1, \ldots, j_\ell)\downarrow$. ⊣

COROLLARY 37. *If A is hereditary, and A' is the hereditary matrix associated with A, then $A' = A$.*

PROOF. If v is a non-zero row of A' with 1's in columns $j_0, \ldots, j_\ell$ and 0's elsewhere, then by the definition of A', there is a node $[x]$ on the j_0-line such that $\chi(x, j_1, \ldots, j_\ell)\downarrow$. By Lemma 36, A contains a row of the form (1) with 1's in columns $j_0, \ldots, j_\ell$. Since A is hereditary, v is also a row of A. Therefore every row of A' is a row of A, and since the matrices have the same number of rows, $A' = A$. ⊣

LEMMA 38. *Let $T^{(j+1)}$ and $T^{(j)}$ be the prefix trees for $A^{(j+1)}$ and $A^{(j)}$. Let $[x]$ be a node of $T^{(j+1)}$ on the j_0-line with $\chi_{T^{(j+1)}}(x, j_1, \ldots, j_\ell)\downarrow$. Then there exists a node $[x']$ of $T^{(j)}$ on the j_0-line such that $\chi_{T^{(j)}}(x', j_1, \ldots, j_\ell)\downarrow$. Moreover, if $j_0 \leq j$, then we can take $[x'] = [x]$.*

PROOF. If $\ell = 0$, then the claim is trivial, so assume that $\ell > 0$. The proof is by induction on the number of elements of $j_0, \ldots, j_\ell$ that are less than or equal to j. For the base case (when $j_0 > j$), we have $j_0 \geq j + 1$, so Lemmas 35 and 36 and the fact that $\chi_{T^{(j+1)}}(x, j_1, \ldots, j_\ell)\downarrow$ imply that the u of Equation (1) is a row of $A^{(j+1)}$. Let x' be x, except modified to have a 0 in column j. By definition of down-shift,

$$x'10^{j_1 - j_0 - 1}10^{j_2 - j_1 - 1}1 \cdots 10^{j_\ell - j_{\ell-1} - 1}10^{n - j_\ell - 1}$$

is a row of $A^{(j)}$. By Lemmas 35 and 36, $\chi_{T^{(j)}}(x', j_1, \ldots, j_\ell)\downarrow$.

The next base case is when $j_0 = j$. Since $\chi_{T^{(j+1)}}(x, j_1, \ldots, j_\ell)\downarrow$, there are nodes $[y_0]$ and $[y_1]$ in $[x]$'s left and right subtrees on the j_1-line in $T^{(j+1)}$ such that $\chi_{T^{(j+1)}}(y_i, j_2, \ldots, j_\ell)\downarrow$ for $i = 0, 1$. We have $y_0 = x0w_0$ and $y_1 = x1w_1$ for some strings w_0, w_1 of length $j_1 - j_0 - 1$. By Lemma 36, $A^{(j+1)}$ contains the rows $u_i = xiw_i1\vec{0}\cdots\vec{0}1\vec{0}$ for $i = 0, 1$, where the indicated 1's are in columns $j_1, \ldots, j_\ell$. $A^{(j+1)}$ is hereditary in columns $j+1, \ldots, n-1$, therefore the presence of the row u_1 implies that $v = x1\vec{0}1\vec{0}1\cdots\vec{0}1\vec{0}$ with the indicated 1's in columns $j_0, \ldots, j_\ell$ is a row of $A^{(j+1)}$. Similarly the presence of u_0 implies that $v - 2^j$ is a row of $A^{(j+1)}$. Because v and $v - 2^j$ are rows of $A^{(j+1)}$, by definition of down-shift, v is a row of $A^{(j)}$. So by Lemmas 35 and 36, $\chi_{T^{(j)}}(x, j_1, \ldots, j_\ell)\downarrow$.

In the final base case, $j_0 < j < j_1$. Since $\chi_{T^{(j+1)}}(x, j_1, \ldots, j_\ell)\!\downarrow$, there are nodes $[y_0]$ and $[y_1]$ in $[x]$'s left and right subtrees on the j_1-line in $T^{(j+1)}$ such that $\chi_{T^{(j+1)}}(y_i, j_2, \ldots, j_\ell)\!\downarrow$ for $i = 0, 1$. So by Lemmas 35 and 36,

$$y_i 10^{j_2 - j_1 - 1} 10^{j_3 - j_2 - 1} 1 \cdots 10^{j_\ell - j_{\ell-1} - 1} 10^{n - j_\ell - 1}$$

for $i = 0, 1$ are rows of $A^{(j+1)}$. Let y_i' be y_i modified to have a 0 in column j. By definition of down-shift,

$$y_i' 10^{j_2 - j_1 - 1} 10^{j_3 - j_2 - 1} 1 \cdots 10^{j_\ell - j_{\ell-1} - 1} 10^{n - j_\ell - 1}$$

for $i = 0, 1$ are elements of $A^{(j)}$. By Lemmas 35 and 36 again, $\chi_{T^{(j)}}(y_i', j_2, \ldots, j_\ell)\!\downarrow$ for $i = 0, 1$. Since $j_0 < j$, it follows that $[y_0']$ and $[y_1']$ are in the left and right subtrees of $[x]$, therefore $\chi_{T^{(j)}}(x, j_1, \ldots, j_\ell)\!\downarrow$.

For the induction step we have $j_0 < j_1 < j$. Since $\chi_{T^{(j+1)}}(x, j_1, \ldots, j_\ell)\!\downarrow$, it follows that $T^{(j+1)}$ has nodes $[y_0]$ and $[y_1]$ on the j_1-line in $[x]$'s left and right subtrees such that $\chi_{T^{(j+1)}}(y_i, j_2, \ldots, j_\ell)\!\downarrow$ for $i = 0, 1$. By the "moreover" clause of the induction hypothesis, $\chi_{T^{(j)}}(y_i, j_2, \ldots, j_\ell)\!\downarrow$ for $i = 0, 1$. Thus $\chi_{T^{(j)}}(x, j_1, \ldots, j_\ell)\!\downarrow$. ⊣

Recall that Definition 21 defined the matrix A' associated with A.

THEOREM 39. $A^{(0)} = A'$.

PROOF. Define $(A^{(j)})'$ to be the hereditary matrix associated with $A^{(j)}$ in the sense of Definition 21. By Lemma 38, Definition 21, and the fact that $(A^{(j+1)})'$ and $(A^{(j)})'$ both have m rows, $(A^{(j+1)})' = (A^{(j)})'$. Therefore, $(A^{(0)})' = (A^{(n)})' = A'$. Moreover, by the corollary to Lemma 36, since $A^{(0)}$ is hereditary, $A^{(0)} = (A^{(0)})' = A'$. ⊣

REFERENCES

[1] A. BECKMANN AND S. R. BUSS, *Improved witnessing and local improvement principles for second-order bounded arithmetic*, ACM Transactions on Computational Logic, 15 (2014), pp. Article 2, 35 pages.

[2] M. L. BONET, S. R. BUSS, AND T. PITASSI, *Are there hard examples for Frege systems?*, in Feasible Mathematics II, P. Clote and J. Remmel, eds., Boston, 1995, Birkhäuser, pp. 30–56.

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

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

[5] S. A. COOK AND P. NGUYEN, *Foundations of Proof Complexity: Bounded Arithmetic and Propositional Translations*, ASL and Cambridge University Press, 2010. 496 pages.

[6] S. A. COOK AND R. A. RECKHOW, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic, 44 (1979), pp. 36–50.

[7] P. FRANKL, *On the trace of finite sets*, Journal of Combinatorial Theory, Series A, 34 (1983), pp. 41–45.

[8] I. GESSEL AND G.-C. ROTA, eds., *Classic Papers in Combinatorics*, Birkhäuser, 1987.

[9] G. HARDY AND E. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford University Press, 6 ed., 2008.

[10] P. HRUBEŠ AND I. TZAMERET, *The proof complexity of polynomial identities*, in Proc. 24th IEEE Conf. on Computational Complexity (CCC), 2009, pp. 41–51.

[11] G. ISTRATE AND A. CRĂCIUN, *Proof complexity and the Kneser-Lovász theorem*, in Theory and Applications of Satisfiability Testing (SAT), Lecture Notes in Computer Science 8561, Springer Verlag, 2014, pp. 138–153.

[12] G. O. Katona, *A theorem of finite sets*, in Theory of Graphs: Proc. Coll. Tihany, Hungary, Sept. 1966, Akadémiai Kiadó and Academic Press, 1966, pp. 187–207. Reprinted in [8], pp. 361-380.

[13] L. A. Kołodziejczyk, P. Nguyen, and N. Thapen, *The provably total NP search problems of weak second-order bounded arithmetic*, Annals of Pure and Applied Logic, 162 (2011), pp. 419–446.

[14] J. Krajíček, *Bounded Arithmetic, Propositional Calculus and Complexity Theory*, Cambridge University Press, Heidelberg, 1995.

[15] J. B. Kruskal, *The number of simplices in a complex*, in Mathematical Optimization Techniques, R. Bellman, ed., University of California Press, 1963, pp. 251–278.

[16] A. Nozaki, T. Arai, and N. H. Arai, *Polynomial-size Frege proofs of Bollobás' theorem on the trace of sets*, Proceedings of the Japan Academy, Series A. Math. Sci., 84 (2008), pp. 159–161.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CA 92093-0112, USA
E-mail: jaisenberg@math.ucsd.edu

LENGUAJES Y SISTEMAS INFORMÁTICOS
UNIVERSIDAD POLITÉCNICA DE CATALUÑA
BARCELONA, SPAIN
E-mail: bonet@lsi.upc.edu

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, SAN DIEGO
LA JOLLA, CA 92093-0112, USA
E-mail: sbuss@math.ucsd.edu