

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 [15] by proving that Frankl's Theorem [?] 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 [9] showed that determinant identities such as $\det(A)\det(B) = \det(AB)$ and $AB =$

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.

$I \Rightarrow BA = I$ 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 candidates (other than partial consistency principles) for exponentially separating Frege and extended Frege systems have been proposed. Kołodziejczyk, Nguyen, and Thapen [12] suggested the propositional translations of various local improvement principles LI, 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 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 ([12, 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 Crăciun [10]. 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, Crăciun, 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 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 $I\Delta_0 + \Delta_0\text{-PHP}$ and $I\Delta_0 + \Delta_0\text{-BONDY}$ are equivalent. Nozaki, Arai, and Arai [15] 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 Bollobás' Theorem from instances of the pigeonhole principle, and that Bollobás' Theorem is provable in $I\Delta_0 + \Delta_0\text{-PHP}$.

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 $\Delta_0\text{-PHP}$ formulas. Likewise, for fixed values of t , Frankl's Theorem is provable in $I\Delta_0 + \Delta_0\text{-PHP}$.

Our proof methods substantially extend the constructions of [?, 2]. Like the original proof of Frankl [?], 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 construction of [?, 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 [11, 14] in the same way as was done by both Frankl and Bonnet-Buss-Pitassi. Additional work is needed 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 [?]) *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 $j \in \{0, \dots, n-1\}$. 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 $j \in \{0, \dots, n-1\}$; 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 $\mathcal{F} = \{S_1, \dots, S_m\}$ be a family of subsets of $\{0, \dots, n-1\}$. 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 [?, 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*

$$(1) \quad |A_{\leq k}| \geq |\{0, 1, 2, \dots, m-1\}_{\leq k}|.$$

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 $\{0, 1, 2, \dots, m-1\}$ 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, 13].

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 $\text{EQ}(i, i', j)$ expresses that rows i and i' differ only in column j as

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

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

$$\text{CARDP}(j) := |\{i : 0 \leq i < m \text{ and } \bigvee_{i' \neq i} \text{EQ}(i, i', j)\}|.$$

The size of $\text{CARDP}(j)$ is polynomially bounded by the total size of the m many formulas $\bigvee_{i'} \text{EQ}(i, i', j)$; 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

$$\text{DISTINCTROWS} \rightarrow \bigvee_j (\text{CARDP}(j) < 2^t).$$

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 " $\text{CARDP}(j) < 2^t$ ". To see this, note that its negation " $\text{CARDP}(j) \geq 2^t$ " can be expressed as the disjunction over all 2^t -tuples

$i_1 < i_2 < \dots < i_{2^t}$ 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 $\text{AC}^0\text{-Frege+PHP}$ 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 $\text{AC}^0\text{-Frege+PHP}$ proofs $P_{m,n}^t$ 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 Theorem, 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 $\text{AC}^0\text{-Frege+PHP}$ proofs. The key new tool is that the bijective form of the Kruskal-Katona Theorem can be formulated and proved in $\text{AC}^0\text{-Frege}$.

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 $\text{AC}^0\text{-Frege+PHP}$ 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 .

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

$$\llbracket x \rrbracket = \{r : r \text{ is a row of } A, x \text{ is a prefix of } r\}.$$

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

Of course, every non-empty $\llbracket x \rrbracket$ has a unique maximal representative. Whenever we use the notation $[x]$, it is (implicitly) required that $\llbracket x \rrbracket \neq \emptyset$ and x is its maximal representative. For $|x| < n$, we have $\llbracket x \rrbracket = \llbracket x0 \rrbracket \cup \llbracket x1 \rrbracket$. The string x is a maximal representative for $\llbracket x \rrbracket$ iff $\llbracket x \rrbracket \neq \emptyset$ and either $|x| = n$ or both $\llbracket x0 \rrbracket$ and $\llbracket x1 \rrbracket$ 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 $\llbracket \epsilon \rrbracket$, where ϵ is the empty string and thus $\llbracket \epsilon \rrbracket$ is the set of all rows of A . The root $\llbracket \epsilon \rrbracket$ 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 $\llbracket x0 \rrbracket$ and its right child $\llbracket x1 \rrbracket$. Thus T is an ordered binary tree, and since T has m leaves, it has $m - 1$ internal nodes.

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

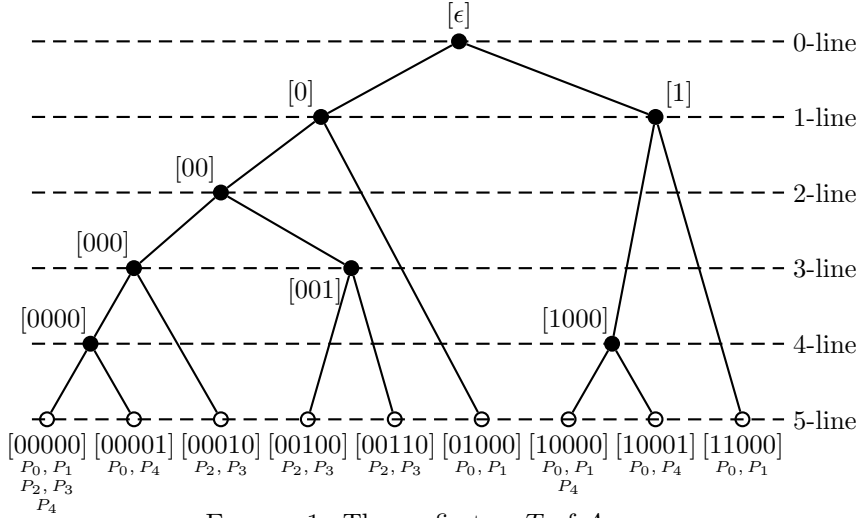
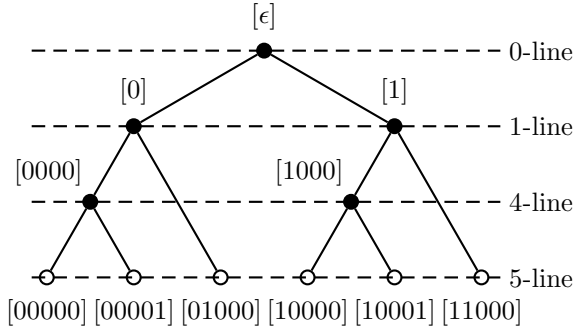
$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Our single/double bracket notation means, for instance, that the rightmost leaf $[11000]$ of the tree is also equal to $\llbracket 11 \rrbracket = \llbracket 110 \rrbracket = \llbracket 1100 \rrbracket$. 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:

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

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

DEFINITION 11. Let $j \in \{0, \dots, n - 1\}$. 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 is inherited from T .

FIGURE 1. The prefix tree T of A .FIGURE 2. The prefix tree T_0 associated with P_0 .

DEFINITION 12. Let $j \in \{0, \dots, n-1\}$. 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, in that two rows of A which differ first in column j give rise to a node on the j -line. Note that any node on the j -line is in the tree T_j , but T_j has other nodes as well. 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 $j < j'$.

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 subtree of $[x]$ in S* is the subtree of S rooted at the left child of $[x]$ in S . The right subtree of $[x]$ is defined similarly.

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 in the following strong sense: For each node $[x0u]$ in the left subtree, there is a corresponding node $[x1u]$ in the right subtree; and conversely, for each node $[x1u]$ in the right subtree, there is a corresponding node $[x0u]$ in the left subtree.*

PROOF. 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 $r = x0y$ (resp., $r = x1y$). In fact, $[x0y]$ is in P_j if and only if $[x1y]$ is in P_j . The internal nodes of these two subtrees are least common ancestors of these leaves. From this, the lemma follows. \dashv

A consequence 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 node $[x0u]$ of T_j has a corresponding node $[x1u]$ in T_j , and their least common ancestor is $[x]$ on the j -line.

2.2. The χ function. The χ_S function takes a node $[x]$ of a tree S and a sequence of columns, and produces a node in the subtree of S 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 $j_1 < j_2 < \dots < j_\ell$ be a (possibly empty) sequence of columns with $\ell \geq 0$. The function $\chi_S([x], j_1, j_2, \dots, j_\ell)$, with $\ell + 1$ arguments, is defined by induction on ℓ , and will equal either $[x]$ or a node below $[x]$ in S . 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 $\chi_S([y], j_2, \dots, j_\ell)$ is defined. Let $[y]$ be the leftmost such node in the right subtree of $[x]$ in S . Then $\chi_S([x], j_1, \dots, j_\ell)$ is defined (written $\chi_S([x], j_1, \dots, j_\ell) \downarrow$) and

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

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

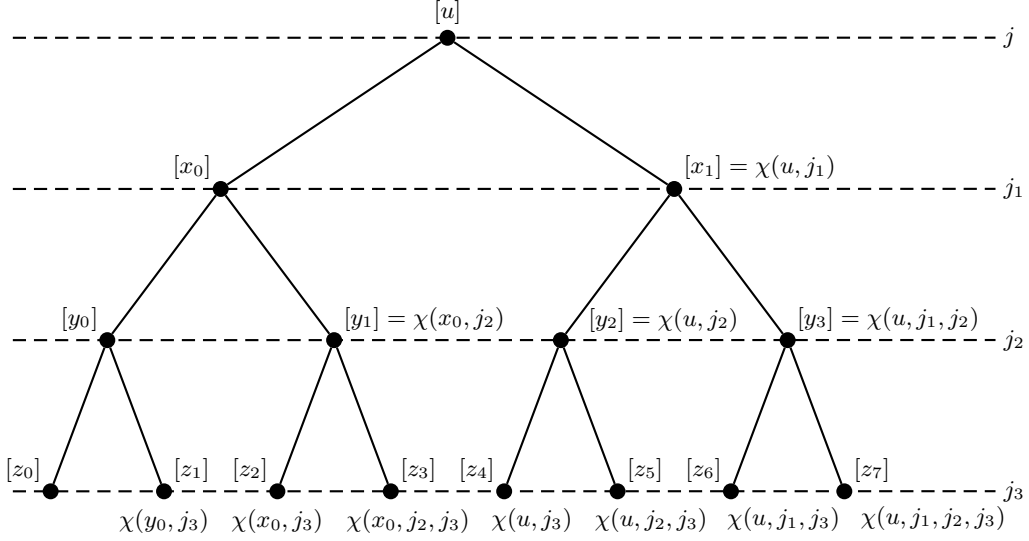
When $S = T$, we write $\chi([x], j_1, \dots, j_\ell)$ instead of $\chi_T([x], j_1, \dots, j_\ell)$. Additionally, to simplify the notation, $\chi([x], j_1, \dots, j_\ell) = [z]$ will be written as $\chi(x, j_1, \dots, j_\ell) = z$.

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

Later, Lemma 36 will describe the meaning of the χ function when A is hereditary. (The reader may skip ahead to read the statement and proof of Lemma 36 if desired.) The general intuition is that when $\chi(x, j_1, \dots, j_\ell) \downarrow$ then the subtree rooted at $[x]$ contains a complete binary subtree of height ℓ as an induced subtree; the internal nodes of this binary tree lie on the j_i -lines for $i = 1, \dots, \ell$.

LEMMA 16. *Let S be T or one of its induced subtrees T_j . For fixed $\ell \geq 0$, the map $(x, j_1, \dots, j_\ell) \mapsto \chi_S(x, j_1, \dots, j_\ell)$ 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, \dots, j_ℓ , the map $x \mapsto \chi(x, j_1, \dots, j_\ell)$ is injective. We prove this by induction. The base case $\ell = 0$ is the injectivity

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

of the identity function. For the induction step, suppose $\ell \geq 1$ and the map $x \mapsto \chi(x, j_2, \dots, j_\ell)$ is injective. Suppose $[x] \neq [x']$ and that $\chi(x, j_1, \dots, j_\ell) = \chi(x', j_1, \dots, j_\ell)$ and these quantities are defined. This means that $\chi(y, j_2, \dots, j_\ell) = \chi(y', j_2, \dots, j_\ell)$, where $[y]$ is the leftmost node on the j_1 -line in $[x]$'s right subtree for which $\chi(y, j_2, \dots, j_\ell) \downarrow$, and similarly for $[y']$ in $[x']$'s right subtree. By the induction hypothesis, $z \mapsto \chi(z, j_2, \dots, j_\ell)$ is injective. Therefore $[y] = [y']$, and $[y]$ is in the right subtrees of both $[x]$ and $[x']$. Thus, one of $[x]$ and $[x']$ is an ancestor of the other, say $[x]$ is an ancestor of $[x']$. Since $\chi(x', j_1, \dots, j_\ell)$ is defined, there must be some element $[u]$ on the j_1 -line in $[x']$'s left subtree for which $\chi(u, j_2, \dots, j_\ell) \downarrow$. 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 $\chi(y, j_2, \dots, j_\ell)$ 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 $(x, j_2, \dots, j_\ell) \mapsto \chi(x, j_2, \dots, j_\ell)$ is injective. Suppose $\chi(x, j_1, \dots, j_\ell) = \chi(x', j_1, \dots, j_\ell)$ (and are defined). Let $[y]$ be the leftmost node on the j_1 -line in $[x]$'s right subtree such that $\chi(y, j_2, \dots, j_\ell) \downarrow$ and $[y']$ be the leftmost node in on the j_1 -line in $[x']$'s right subtree such that $\chi(y', j_2, \dots, j_\ell) \downarrow$. So,

$$\chi(y, j_2, \dots, j_\ell) = \chi(x, j_1, \dots, j_\ell) = \chi(x', j_1, \dots, j_\ell) = \chi(y', j_2, \dots, j_\ell).$$

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

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

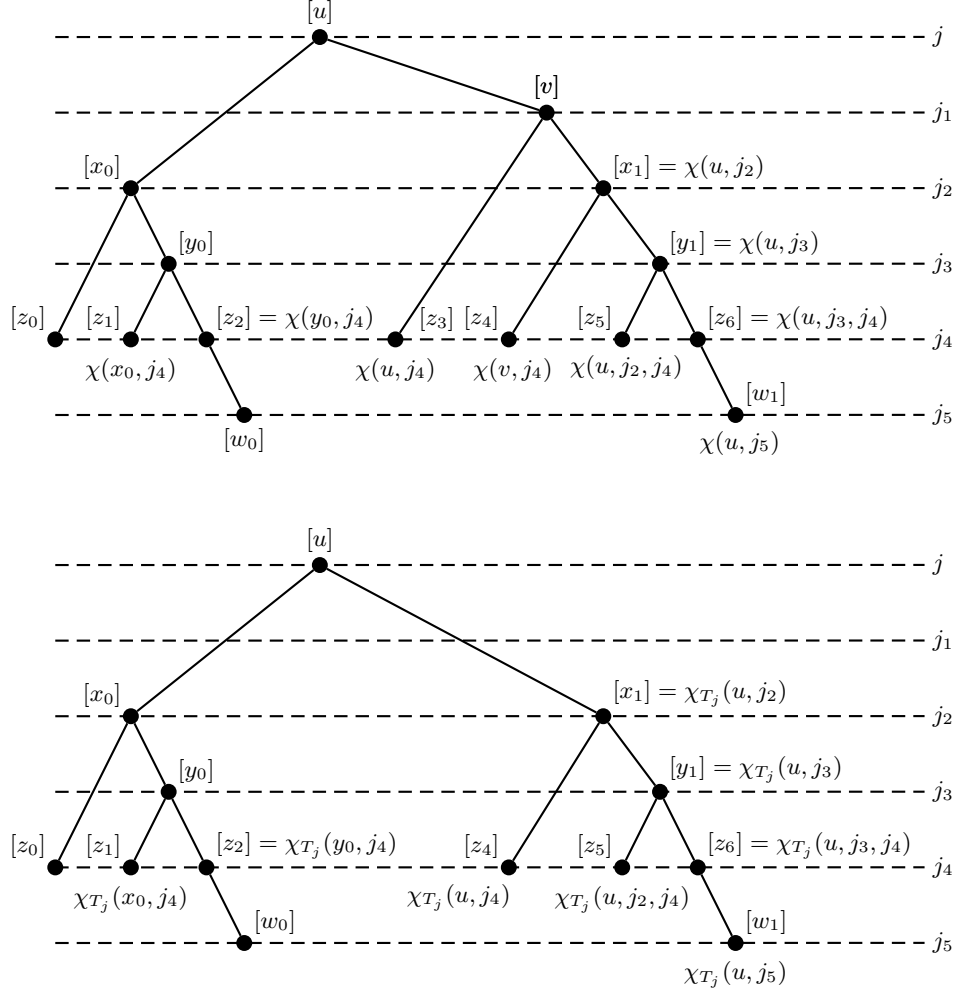


FIGURE 4. An example of a tree T (top) and T_j (bottom) with χ values specified. Each node is an internal node; the leaf nodes are not drawn.

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

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 $\chi(x, j_1, \dots, j_\ell) = z$ and $\chi(x, j'_1, \dots, j'_{\ell'}) = z$. 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 $\chi(y, j_{\ell-\ell'+1}, \dots, j_\ell) = z$. By Lemma 16, $[y] = [x]$, which is a contradiction.

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

Part 4. follows from part 1. and Lemma 16. \dashv

It is an immediate consequence of parts 2. and 3. of Lemma 17 that if $\chi(x, \vec{j}) \downarrow$ then $|\vec{j}| \leq \log m$. In particular, we need only consider values of ℓ which are $\leq \log m$. This is because there are 2^ℓ many $\vec{j}' \subseteq \vec{j}$ and each value $\chi(x, \vec{j}')$ 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 $y = \chi_S(x, j_1, \dots, j_\ell)$ for some $[x], j_1, \dots, j_\ell$.*

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

LEMMA 19. *For fixed $[x] \in T_j$, $[x]$ on the j -line, the function $\vec{j} \mapsto \chi_{T_j}(x, \vec{j})$ 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 $[y] \in T_j$ in the right subtree of $[x]$, let $[\tilde{y}] \in T_j$ denote the corresponding node in the left subtree. Recall that \tilde{y} is the same as y except the $(j+1)$ -st bit is changed from “1” to “0”.

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_ℓ 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, $[\tilde{y}]$ is on the j_0 -line in $[x]$'s left subtree, and by

Lemma 14, $\chi_{T_j}(\tilde{y}, j_1, \dots, j_\ell) \downarrow$. 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 $[\tilde{y}]$ 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 . \dashv

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 . The base case is trivial, since $\chi_{T_j}(x) = \chi(x) = x$. 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. \dashv

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

Later, Corollary 37 will show that if A is hereditary, then $A' = A$. For general A , we have:

LEMMA 22. *If A' is the hereditary matrix associated with A , then A' is hereditary. Moreover, A' has the same dimensions as A .*

PROOF. Let r be a row of A' , with 1's in the $\ell + 1$ columns $j_0 < j_1 < \dots < j_\ell$, 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, \dots, j_ℓ by part 3. of Lemma 17. So, consider replacing the leftmost 1, in column j_0 , with a 0. By definition of A' , $\chi(x, j_1, \dots, j_\ell)$ is defined for some $[x]$ on the j_0 -line. Therefore, there is a node $[y]$ on the j_1 -line such that $\chi(y, j_2, \dots, j_\ell) \downarrow$, and thus A' contains a row with 1's in columns j_1, \dots, j_ℓ 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, \dots, j_ℓ . Let $[x]$ be the leftmost node on the j_0 -line for which $\chi(x, j_1, \dots, j_\ell)$ is defined. Then Θ is defined by $\Theta(r) = \chi(x, j_1, \dots, j_\ell)$.

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 $j_1, \dots, j_{\ell(S)}$ which satisfy all the properties of Lemma 18. Thus, A' contains a row r with 1's in (only) columns $j, j_1, \dots, j_{\ell(S)}$, and $\Theta(r) = y$. By Lemmas 17 and 18, r is the only row with $\Theta(r) = y$. \dashv

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 $\chi(x, j_1, \dots, j_\ell) \downarrow$, then $\Theta^{-1}(\chi(x, j_1, \dots, j_\ell)) \in X_j$. 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 there are at least $|P_j \cap S|/2$ many nodes of the form $\chi(x, \vec{j})$. \dashv

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 .

THEOREM 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 already shown that A' is an $m \times n$ hereditary matrix. Define P'_j for A' in the same way that P_j was defined for A . Since A' is hereditary, $|P'_j| = 2|X_j|$. That A' is a counterexample to Frankl's theorem for t follows immediately from Lemma 24 and the hypothesis that A is a counterexample. \dashv

Theorem 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 quasi-polynomial size Frege proofs of Frankl's Theorem. Section 3.1 will argue that Theorem 25 can be expressed and proved with quasi-polynomial 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 Theorem 25, suffice to prove Theorem 8.

2.4. The functional Kruskal-Katona Theorem. 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

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

such that $g_{m_0, m_1}(a) = \langle 0, b \rangle$ implies $|a|_1 \geq |b|_1$ and such that $g_{m_0, m_1}(a) = \langle 1, b \rangle$ implies $|a|_1 \geq |b|_1 + 1$. We claim that the fact that the Kruskal-Katona Theorem is true implies that g_{m_0, m_1} exists. The range of g_{m_0, m_1} is

$$(\{0\} \times \{0, \dots, m_0-1\}) \cup (\{1\} \times \{0, \dots, m_1-1\})$$

and can be viewed as the set of rows of a hereditary matrix. The inequality (1) of the Kruskal-Katona Theorem thus implies the existence of g_{m_0, m_1} .

This circularity of using the Kruskal-Katona Theorem for its own proof should not be too disturbing however. The point is that we know the Kruskal-Katona Theorem is true. 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 constantly many of the functions g_{m_0, m_1} , and these can just be hard-coded 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

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

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

To define the function $f : \{0, \dots, m-1\} \rightarrow A$, 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 . As before, columns are numbered from left to right, beginning with column $j = 0$.

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

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 $|P_j| \geq 2^t$ for all j . Let D be the least common multiple of the integers $1, 2, 3, \dots, t$. 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 $1, 2, \dots, t$ satisfies $D = O(t)$, see e.g. [8, 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, $|Y_j^*| \geq 2^{t-1}$. The set Y_j^* is hereditary since A is. Let $Z_j \subset Y_j^*$ be a hereditary subset with $|Z_j| = 2^{t-1}$, for example the least 2^{t-1} elements of Y_j^* in the lexicographic ordering. Let $B = \{0, \dots, 2^{t-1} - 1\}$. Define A^+ and B^+ as follows:

$$\begin{aligned} A^+ &= \{\langle a, k \rangle : a \neq \vec{0} \text{ is a row of } A \text{ and } 0 \leq k < D\} \\ B^+ &= \{\langle b, k \rangle : b \in B \text{ and } 0 \leq k < \frac{D}{|b|_1 + 1}\}. \end{aligned}$$

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 $\{0, \dots, n-1\} \times B^+$ to A^+ . By Theorem 7, now with $m = |B| = 2^{t-1}$, there are bijections $f_j : B \rightarrow Z_j$ so that $|f_j(b)|_1 \leq |b|_1$ for all $b \in B$.

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

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

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 $f_j(b) + 2^j \neq \vec{0}$ 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 , we can recover j ; and from j and a , we can recover $b = f_j^{-1}(a - 2^j)$. \dashv

§3. Formalization in the Frege system. This section sketches the proofs of Theorems 8 and 9 by showing how to transform the above proofs of Theorem 25 and Lemma 26 into families of quasi-polynomial size Frege proofs (respectively, polynomial size, constant depth Frege proofs).

3.1. Quasi-polynomial 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 quasi-polynomial 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 for i and i' unique, we always use the least values i and i' . Accordingly, we define

$$\begin{aligned} \text{EQTO}(i, i', j) &:= \bigwedge_{j'=0}^{j-1} (p_{i,j'} \leftrightarrow p_{i',j'}) \\ \text{FIRSTEQTO}(i, j) &:= \bigwedge_{i'=0}^{i-1} \neg \text{EQTO}(i, i', j). \end{aligned}$$

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:

$$\text{EQTO}(i, i', j) \wedge \text{FIRSTEQTO}(i, j+1) \wedge \text{FIRSTEQTO}(i', j+1) \wedge \neg p_{i,j} \wedge p_{i',j}.$$

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) iff

$$\begin{aligned} \text{INLEFT}(i_1, i'_1; i_2, i'_2) &:= \\ &\bigvee_{j_1 < j_2} \left(\text{TNODELN}(i_1, i'_1, j_1) \wedge \text{TNODELN}(i_2, i'_2, j_2) \right. \\ &\quad \left. \wedge \text{EQTO}(i_1, i_2, j_1) \right) \wedge \neg p_{i_2, j_1}. \end{aligned}$$

INRIGHT is defined similarly, but with $\neg p_{i_2, j_1}$ replaced with p_{i_2, j_1} .

The rows of A are ordered by

$$\text{LEFTOF}(i, i') := \bigvee_{j=0}^{n-1} \left(\neg p_{i,j} \wedge p_{i',j} \wedge \text{EQTO}(i, i', j) \right)$$

which expresses that row i precedes row i' in lexicographic order. Since nodes of T correspond to (prefixes of) rows of A , LEFTOF also induces a left to right ordering on T .

We now give quasi-polynomial size formulas defining the graph of the χ functions. $\text{CHI}(i_1, i'_1; j_1, \dots, j_\ell; i_2, i'_2)$ defines the property $\chi(x, j_1, \dots, j_k) = z$ where (i_1, i'_1) and (i_2, i'_2) represent nodes $[x]$ and $[z]$ in T . For $\ell = 0$, $\text{CHI}(i_1, i'_1; i_2, i'_2)$ is

true iff $i_1 = i_2$, $i'_1 = i'_2$, $i_1 \neq i'_1$, and $\text{TNode}(i_1, i'_1)$. Then, inductively for $\ell \geq 1$, define (the indices k, k', k_1, k'_1, \dots range over rows, i.e., are in $\{0, \dots, m-1\}$):

$$\begin{aligned} \text{CHI}(i_1, i'_1; j_1, \dots, j_\ell; i, i') := & \\ & \bigvee_{k_1 < k'_1} \bigvee_{k_2 < k'_2} \left[\text{TNodeLN}(k_1, k'_1, j_1) \wedge \text{INLEFT}(i_1, i'_1; k_1, k'_1) \right. \\ & \wedge \text{TNodeLN}(k_2, k'_2, j_1) \wedge \text{INRIGHT}(i_1, i'_1; k_2, k'_2) \\ & \wedge \text{CHI}(k_2, k'_2; j_2, \dots, j_\ell; i, i') \wedge \bigvee_{k < k'} \text{CHI}(k_1, k'_1; j_2, \dots, j_\ell; k, k') \\ & \wedge \neg \left(\bigvee_{k_3 < k'_3} [\text{TNodeLN}(k_3, k'_3, j_1) \wedge \text{INRIGHT}(i_1, i'_1; k_3, k'_3) \right. \\ & \quad \left. \wedge \text{LEFTOF}(k_3, k_2) \wedge \bigvee_{k < k'} \text{CHI}(k_3, k'_3; j_2, \dots, j_\ell; k, k') \right] \bigg). \end{aligned}$$

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 $\text{PJ}(i, j)$ be $\bigvee_{i' \neq i} \text{EQ}(i, i', j)$. The formula $\text{TJNode}(i, i', j)$ that defines the property of (i, i') being a node in T_j can be defined similarly to $\text{TNode}(i, i')$ 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 $\text{CHITJ}(i_1, i'_1; j_1, \dots, j_\ell; i, i'; j)$ 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 $O(\ell)$ using AND and OR gates with fan-in as large as n or m^2 (for example, the AND gate in FIRSTEQTO and the big OR gates in the definition of CHI, respectively). Thus, these formulas have size bounded by $(m+n)^{O(\ell)} = (m+n)^{O(\log m)}$. In other words, CHI and CHITJ are quasi-polynomial size formulas, and the χ function is NC^2 -definable. In fact, since the values of j_1, \dots, j_ℓ 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 different formulas CHI and CHITJ that need to be constructed is 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 many parameters j_1, \dots, j_ℓ ($\ell + 1$ many 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 quasi-polynomially many formulas $\text{CHI}(\dots)$ and $\text{CHITJ}(\dots)$.

We have shown how to express concepts such as the trees T and T_j and the χ and χ_j functions with quasi-polynomial size formulas. It is now straightforward to formulate and prove the propositional translations of Lemmas 14-24 and Theorem 25 with quasi-polynomial size Frege proofs. Indeed the proofs of these lemmas are all very concrete and constructive, and they are readily translated 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 with a “brute-force induction” or “exhaustive” enumeration of cases. For example, the propositional translation of Lemma 16 becomes the propositional formulas

$$\neg(\text{CHI}(i_1, i'_1; j_1, \dots, j_\ell; i_3, i'_3) \wedge \text{CHI}(i_2, i'_2; j'_1, \dots, j'_\ell; i_3, i'_3))$$

for all choices of sequences $i_1, i'_1, j_1, \dots, j_\ell$ not identical to $i_2, i'_2, j'_1, \dots, j'_\ell$. The propositional proof derives all these statements, for all such values, successively for ℓ equal to 0 up to $\log m$. Second, note that the hereditary matrix A' , as defined in Definition 21 has quasi-polynomially many possible rows. The proof of Theorem 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 case of Frankl's Theorem. This completes the proof of Theorem 8 that the propositional translations of Frankl's Theorem have quasi-polynomial 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 $\chi(x, j_1, \dots, j_\ell)$ is 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, and we prove an analogue of Lemma 22.

DEFINITION 27. The matrix $A'_{\leq t}$ is the 0/1 matrix that contains as rows exactly those rows of A' with no more than t many 1's.

LEMMA 28. $A'_{\leq t}$ 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 fewer than 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 , and prove an analogue of Lemma 24.

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

PROOF. This is similar to the proof of Lemma 24, but now we reason with only the rows of $A'_{\leq t}$, not the rows of A' . The argument splits into two cases. First suppose there is some row r of $X_{j, \leq t}$ that contains t many 1's. There are 2^{t-1} many rows that 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 Theorem 25, we obtain the following.

THEOREM 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 and 30 and Theorem 31, the entire proof of Frankl's Theorem for constant t can be formalized by 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 ϕ_1, \dots, ϕ_n be formulas. The condition that at least s of the ϕ_i 's are true can be expressed by letting \mathcal{I} range over subsets of $\{1, \dots, n\}$ 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 restricted 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, 28 and 30 and Theorem 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 Lemma 28 and Theorem 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 define an injection 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 $\{0, \dots, m-1\}$ onto the rows of A , and since m is constant, there are only finitely many possibilities for f . It is now convenient to work with

¹Recall 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 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 $\{0, \dots, m-1\}$ 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 $\{0, \dots, |E_{\ell,i}| - 1\}$.

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 Lemma 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 Lemma 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 Theorem. This construction as described in [?, 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 this construction yields the same matrix as our matrix A' from Section 2.3.

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 , respectively A_1 , denote the set of rows of A with a 0, respectively a 1, in column j . The *downshift* of A in column j is the matrix $\text{DownShift}(A, j)$ 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 $\text{DownShift}(A, j)$ is hereditary in column j .

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

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

PROOF. The proof is by induction on $j = n, \dots, 1, 0$. The base case of $j = n$ is trivial. For the induction step, suppose $A^{(j+1)}$ is hereditary in columns $j+1, \dots, n-1$. 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 $x1y$ where $|x| = j$ and $i \in \{0, 1\}$ and $|y| = k - j - 1$. Thus w is equal to $x1y1z$. First suppose $i = 1$ and $w = x1y1z$. 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, $i = 0$ and $w = x0y1z$. 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 $A^{(j)}$. \dashv

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

$$(2) \quad x10^{j_1-j_0-1}10^{j_2-j_1-1}1 \dots 10^{j_\ell-j_{\ell-1}-1}10^{n-j_\ell-1}.$$

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

PROOF. Suppose $\chi(x, j_1, \dots, j_\ell) \downarrow$. We argue by induction on ℓ . For the base case, $\ell = 0$, 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 $\chi(y, j_2, \dots, j_\ell) \downarrow$. We have $y = x1w$ for some $w \in \{0, 1\}^{j_1-j_0-1}$. By the induction hypothesis,

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

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 $[y_0]$ and $[y_1]$ exist as nodes of A . Using the hereditary property of A with respect to the row u , and applying the induction hypothesis twice, both $\chi(y_0, j_2, \dots, j_\ell) \downarrow$ and $\chi(y_1, j_2, \dots, j_\ell) \downarrow$. Since $[y_0]$ and $[y_1]$ lie on the j_1 -line in the left and right subtrees of $[x]$, respectively, $\chi(x, j_1, \dots, j_\ell) \downarrow$. \dashv

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, \dots, j_ℓ and 0's elsewhere, then by the definition of A' , there is a node $[x]$ on the j_0 -line such that $\chi(x, j_1, \dots, j_\ell) \downarrow$. By Lemma 36, A contains a row of the form (2) with 1's in columns j_0, \dots, j_ℓ . 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, $A' = A$. \dashv

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 $\chi_{T^{(j+1)}}(x, j_1, \dots, j_\ell) \downarrow$. Then there exists a node $[x']$ of $T^{(j)}$ on the j_0 -line such that $\chi_{T^{(j)}}(x', j_1, \dots, j_\ell) \downarrow$. 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, \dots, j_ℓ that are less than or equal to j . For the first base case (when $j_0 > j$), we have $j_0 \geq j + 1$, so Lemmas 35 and 36 and the fact that $\chi_{T^{(j+1)}}(x, j_1, \dots, j_\ell) \downarrow$ imply that the u of Equation (2) is a row of $A^{(j+1)}$. Let x' be x , except modified to have a 0 in column j . By definition of DownShift,

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

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

The second base case is when $j_0 = j$. Since $\chi_{T^{(j+1)}}(x, j_1, \dots, j_\ell) \downarrow$, 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 $\chi_{T^{(j+1)}}(y_i, j_2, \dots, j_\ell) \downarrow$ 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 $u_i = xiw_i1\bar{0} \dots \bar{0}1\bar{0}$ for $i = 0, 1$, where the indicated 1's are in columns j_1, \dots, j_ℓ . $A^{(j+1)}$ is hereditary in columns $j+1, \dots, n-1$, therefore the presence of the row u_1 implies that $v = x1\bar{0}1\bar{0}1 \dots \bar{0}1\bar{0}$ with the indicated 1's in columns j_0, \dots, j_ℓ 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 DownShift, v is a row of $A^{(j)}$. So by Lemmas 35 and 36, $\chi_{T^{(j)}}(x, j_1, \dots, j_\ell) \downarrow$.

In the final base case, $j_0 < j < j_1$. Since $\chi_{T^{(j+1)}}(x, j_1, \dots, j_\ell) \downarrow$, 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 $\chi_{T^{(j+1)}}(y_i, j_2, \dots, j_\ell) \downarrow$ for $i = 0, 1$. So by Lemmas 35 and 36,

$$y_i10^{j_2-j_1-1}10^{j_3-j_2-1}1 \dots 10^{j_\ell-j_{\ell-1}-1}10^{n-j_\ell-1}$$

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 DownShift,

$$y'_i10^{j_2-j_1-1}10^{j_3-j_2-1}1 \dots 10^{j_\ell-j_{\ell-1}-1}10^{n-j_\ell-1}$$

for $i = 0, 1$ are elements of $A^{(j)}$. By Lemmas 35 and 36 again, $\chi_{T^{(j)}}(y'_i, j_2, \dots, j_\ell) \downarrow$ 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 $\chi_{T^{(j)}}(x, j_1, \dots, j_\ell) \downarrow$.

For the induction step we have $j_0 < j_1 < j$. Since $\chi_{T^{(j+1)}}(x, j_1, \dots, j_\ell) \downarrow$, 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 $\chi_{T^{(j+1)}}(y_i, j_2, \dots, j_\ell) \downarrow$ for $i = 0, 1$. By the “more-over” clause of the induction hypothesis, $\chi_{T^{(j)}}(y_i, j_2, \dots, j_\ell) \downarrow$ for $i = 0, 1$. Thus $\chi_{T^{(i)}}(x, j_1, \dots, j_\ell) \downarrow$. \dashv

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 Corollary 37, since $A^{(0)}$ is hereditary, $A^{(0)} = (A^{(0)})' = A'$. \dashv

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). 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 [7], 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