Bounded Truth Table Reductions of P

Jin-yi Cai *   Ashish V. Naik †   D. Sivakumar ‡

Abstract

If there is a sparse set hard for P under bounded truth table reductions computable in LOGSPACE or NC^2, then $P = NC^2$. We give the details of the proof to this theorem.

1 Introduction

Recently a 1978 conjecture by Hartmanis [Har78] was resolved [CS95a], following a breakthrough by [Ogi95]. It was shown that there is no sparse set that is hard for P under logspace many-one reductions, unless P = LOGSPACE. Bounded truth table reductions are a natural extension of many-one reductions and it is natural to ask what consequences can be drawn assuming there is a sparse set hard for P under bounded truth table reductions computable in LOGSPACE. In this note we give the details of the proof of the theorem that if such a sparse set exists, then a very unlikely consequence follows, namely $P = NC^2$. This theorem is even valid for bounded truth table reductions computable in NC^2.

The proof for the case of 1-truth table reductions, which already generalizes the many-one reductions, has been given in the paper [CNS95]. The proof for the general case was announced in [CNS95], but since that paper was already pretty long, the details of the proof for the general case was not included there. The proof extending the case from 1-truth table reductions to general bounded truth table reductions requires several new ideas, and is given here. We believe the proof ideas are interesting. It uses error correcting codes and may be useful in computational learning.

We first include a proof for the 1-tt case as an introduction to the setup of the proof. We refer readers to [CS95a] and [CNS95] for background.

2 Derandomization for the 1-tt Reductions

Fix a circuit C and an input z. We assume the 1-tt reduction assigns, for every I, the same string to $\langle C, z, I, 0\rangle$ and $\langle C, z, I, 1\rangle$ with a "flipped" truth table. If the tuple $\langle C, z, I\rangle$

*Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grants CCR-9057486 and CCR-9319093, and an Alfred P. Sloan Fellowship. Email: `cai@cs.buffalo.edu`

†Computer Science Department, University of Chicago, Chicago, IL 60637. Research supported in part by NSF grant CCR 92-53582. Email: `naik@cs.uchicago.edu`

‡Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grant CCR-9409104. Email: `sivak-d@cs.buffalo.edu`

is assigned the string w then we say that I *receives the color* w. We will identify a subset $I \subseteq [n]$ with its characteristic vector in $\mathbf{Z_2}^n$. Let $p(n)$ be a polynomial such that there are at most $p(n)$ many distinct strings w assigned by the reduction that belong to S.

Suppose two tuples $\langle C, z, I\rangle$ and $\langle C, z, J\rangle$ receive the same color w. Then according to the actual truth table by the evaluator for the reduction on $\langle C, z, I\rangle$ and $\langle C, z, J\rangle$, we get an equation of the form

$$\bigoplus_{i \in I \Delta J} g_i(z) = b,$$

for some appropriate boolean value b, independent of whether the color $w \in S$. On the other hand, if we know the membership for "$w \in S$?", then we can get two equations,

$$\bigoplus_{i \in I} g_i(z) = b_I, \qquad \bigoplus_{i \in J} g_i(z) = b_J,$$

where b_I and b_J depend on the actual truth tables for I and J.

Let $m = 10 + 3\log n + 2\log p(n) = O(\log n)$. Let $\mathbf{F} = GF(2^m)$ be a Galois field of 2^m elements. Let

$$D = \{(\langle 1, v\rangle, \langle u, v\rangle, \ldots, \langle u^{n-1}, v\rangle) \mid u, v \in \mathbf{F}\}.$$

D is technically a multi-set. Note that $|D| = 2^{2m} = n^{O(1)}$. Let

$$D_S = \{y \in D \mid \text{ color}(y) \in S\}.$$

Let D_S and D be decomposed into color classes

$$D_S = C_1 \cup C_2 \cup \ldots \cup C_p,$$

and

$$D = C_1 \cup C_2 \cup \ldots \cup C_p \cup \ldots \cup C_q,$$

where the number of color classes p is at most $p(n)$, and $q \leq |D|$.

Let the affine span of C_i be denoted as $L_i + d_i$, where L_i is a linear subspace, and d_i is a displacement vector. Let $L = L_1 + L_2 + \cdots + L_q$ be the sum of the linear subspaces. We call L the span of the color classes. The difference of each pair of vectors in any color class C_i gives us an equation mod 2 of the values of the gates of the circuit C with the given input. If we collect a generating set of vectors for each L_i, together they span L. Thus, if $\dim L \geq n - O(\log n)$, we would succeed since by sampling exhaustively in D, we would have obtained a system of linear equations of rank $\geq n - O(\log n)$, which can be solved in NC^2 (cf. [CS95a]).

Let $k = 5 + \log n + \log p(n) = O(\log n)$. We now consider two cases.

Case 1. $\dim L \geq n - k$. Then we can solve the problem, as illustrated in [CS95a].

Case 2. $\dim L < n - k$. Then, we note that $D_S \subseteq \bigcup_{i=1}^{p}(L_i + d_i) \subseteq \bigcup_{i=1}^{p}(L + d_i)$. Replacing L by a higher dimensional subspace if necessary, we can assume that L is defined by a set of k linearly independent equations,

$$\sum_{j=0}^{n-1} a_{ij} x_j = 0,$$

where $a_{ij} \in \mathbf{Z_2}$, and $i = 1, \ldots, k$. Each affine space $L + d$ is then defined by the linear system

$$\sum_{j=0}^{n-1} a_{ij} x_j = b_i \tag{1}$$

for some $b(d) = (b_1, \ldots, b_k)^T \in \mathbf{Z_2}^k$, a right hand side (RHS) vector depending on d.

Now consider any such system of k independent linear equations with an arbitrary RHS vector b. Denote this affine space by Π. Denote the point in D specified by u, v as $D(u, v)$. It can be shown that each equation in the linear system (1) cuts down the sample set D successively into two roughly equal subsets, so that the fraction of the points of D that fall in Π is roughly $1/2^k$. More precisely,

$$\left| \Pr_{u,v \in \mathbf{F}} [D(u, v) \in \Pi] - 1/2^k \right| \leq \frac{(2^k - 1)(n - 1)}{2^m} \left(1 - \frac{1}{2^k}\right).$$

As D_S is covered by at most $p(n)$ many affine translations of L, we have

$$\frac{|D_S|}{|D|} \leq p(n) \cdot \left(\frac{1}{2^k} + \frac{n}{2^{m-k}}\right),$$

which by our choice of values for k and m, is $< 1/(8n)$.

Now for each I we will *assume* the target $w \notin S$, which gives us an equation with a certain RHS. For precisely those $I \in D_S$ we get an incorrect RHS. For $I \in D - D_S$, the assumption that $w \notin S$ is correct and thus the RHS for that equation is correct.

For each $u \in \mathbf{F}$, we will first try to obtain a correct equation of the form

$$\sum_{j=0}^{n-1} u^j x_j = \gamma,$$

for some $\gamma \in \mathbf{F}$. We do it by taking a majority vote for each bit.

Let v' range over $\{0, 1\}^{m-1}$. Let $v = 0v'$ and $1v'$ denote the corresponding elements in $\mathbf{F}$ with the specified bit pattern. Then we will set the 1st bit of γ to 0 if the majority of the RHS of $\sum_{j=0}^{n-1} \langle u^j, 0v' \rangle x_j$ and $\sum_{j=0}^{n-1} \langle u^j, 1v' \rangle x_j$ agree, and we set it to 1 otherwise. Similarly we set the other $m - 1$ bits of γ.

Note that, for the given $u \in \mathbf{F}$, if less than 1/4 of the RHS bit b_{uv} in the equation

$$\sum_{j=0}^{n-1} \langle u^j, v \rangle x_j = b_{uv} \in \mathbf{Z_2},$$

are incorrect, as v ranges over all $\mathbf{F}$, then our correction scheme succeeds in finding a correct RHS γ in

$$\sum_{j=0}^{n-1} u^j x_j = \gamma.$$

Now among the 2^m equations $\sum_{j=0}^{n-1} u^j x_j = \gamma$ as u ranges over $\mathbf{F}$, less than a fraction of $1/(2n)$ of them could have an incorrect RHS γ. For, otherwise, the fraction of incorrect equations in the original system is $\geq 1/(8n)$, contradicting the fact that

$$\frac{|D_S|}{|D|} < \frac{1}{8n}.$$

Finally we will correct those remaining values γ via polynomial self-reducibility.

Note that if we set the polynomial $f(U) = \sum_{j=0}^{n-1} \alpha_i U^i$, where α_i is the actual value of the ith gate in the circuit C with input z, then the equations are valuations of f at various points $u \in \mathbf{F}$.

Fix any $u_0 \in \mathbf{F}$. We will break all 2^m equations of the form

$$\sum_{j=0}^{n-1} u^j x_j = \gamma,$$

as u varies over $\mathbf{F}$, into $2^m/n$ blocks of n equations each. Then we use polynomial interpolation formula to evaluate f at u_0 within each block of n equations, and then take a majority vote. Since the fraction of incorrect RHS is $< 1/(2n)$, the majority vote is guaranteed to be correct for $f(u_0)$. Note that u_0 is arbitrary. We can then solve a Vandermonde system for the actual values of the gates, after we have evaluated at n points $u_1, u_2, \ldots, u_n$ in parallel.

This completes our treatment of Case 2.

To summarize, our NC^2 deterministic algorithm works as follows. It constructs D and forms two sets of linear equation systems in parallel. One set of equations is formed similar to the many-one reducibility case by considering all pairs of (I, J) which are mapped to the same string w. The second set of equations is formed by *assuming* all queried strings $w \notin S$. We try to solve both systems and then check out the results, using local information of the circuit such as $z_i = 0$, or $z_i = 1$, or $g_j(z) = g_k(z) \wedge g_\ell(z)$, etc. If the first set of equations has sufficiently high rank $n - O(\log n)$, then it will succeed. Otherwise the second set of equations will succeed.

3 From 1-tt to general bounded truth table reductions

We consider the proof for the 2-tt case. As seen in the 1-tt case, some new ideas were needed to carry through the proof from the many-one reduction case to the proof for the truth table reductions. In particular the idea of error correction plays an important role. This is still a main ingredient of the proof for the 2-tt case. However, the proof is not a straightforward extension from the 1-tt case; a new idea is required.

The extra difficulty can be described as follows: While nested logically in the various cases for the truth tables, we need to reconstruct linear functions defined on various linear subspaces L, each of logarithmic dimension. However, unlike in the case of 1-truth table reductions, we no longer have a reliable set of samples from the whole space L, but rather only a set of samples which may be all from a smaller linear subspace of L.

To overcome this difficulty, we need to suitably "shrink" the linear subspace L to a linear subspace $L' \subseteq L$, which is smaller than L, and yet not too much smaller. On L' we can uniquely reconstruct the linear function from sample data that are "essentially correct". We then apply similar procedures as in the 1-tt case to finish the proof.

The proof for the 2-tt case is combinatorially complicated. The general bounded truth table case is even more convoluted combinatorially. However, all the mathematical difficulties in the proof for the general bounded truth table case is contained in the proof of the 2-tt case.

Theorem 1 *If there is a sparse set that is hard for* P *under bounded truth table reductions computable in* NC^2*, then* $P \subseteq \mathrm{NC}^2$.

3.1 Two lemmas

We will need two essential lemmas for the proof.

Let $GF(2^m)$ be the Galois field of 2^m elements. As usual, we consider it as a vector space over $\mathbf{Z}_2$ of dimension m. Recall the definition of the multiset D,

$$D = \{(\langle 1, v\rangle, \langle u, v\rangle, \ldots, \langle u^{n-1}, v\rangle) \in B \mid u, v \in GF(2^m)\},$$

where $B = \{0,1\}^n$. As a multiset $|D| = 2^{2m}$. Denote the point $(\langle 1, v\rangle, \langle u, v\rangle, \ldots, \langle u^{n-1}, v\rangle)$ by $D(u, v)$, and let $D(u)$ be the sub(multi)set of D defined as,

$$D(u) = \{(\langle 1, v\rangle, \langle u, v\rangle, \ldots, \langle u^{n-1}, v\rangle) \in B \mid v \in GF(2^m)\}.$$

Without loss of generality we will assume n is a power of 2.

Lemma 2 *Let* $u_1, u_2, \ldots, u_{n^{\ell+1}}$ *be* $n^{\ell+1}$ *distinct elements in* $GF(2^m)$*. For every* i*, let* $\tilde{D}(u_i) \subseteq D(u_i)$ *be a sub(multi)set, such that*

$$|\tilde{D}(u_i)| > \frac{2^m}{n^\ell}.$$

Let $\tilde{D}$ *be the union* $\bigcup_{i=1}^{n^{\ell+1}} \tilde{D}(u_i)$*. Then,*

$$\dim(\text{span }(\tilde{D})) \geq \dim(\text{affine span }(\tilde{D})) > n - \ell \log_2 n.$$

Proof. For a contradiction, suppose $\dim(\text{affine span }(\tilde{D})) \leq n - \ell \log_2 n$. Then there exist $s = \ell \log_2 n$ many linearly independent equations

$$\begin{pmatrix} a_{1,0} & a_{1,1} & \ldots & a_{1,n-1} \\ a_{2,0} & a_{2,1} & \ldots & a_{2,n-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{s,0} & a_{s,1} & \ldots & a_{s,n-1} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix},$$

such that all of $\tilde{D}$ satisfy.

Let $Q = \{\sum_{i=1}^{s} \beta_i [\sum_{j=0}^{n-1} a_{ij} X^j] \mid \beta_i \in \mathbf{Z}_2, \text{ but not all } 0\}$ be the set of $2^s - 1$ non-zero polynomials used before, each of degree at most $n-1$.

For any $D(u_i, v) \in \tilde{D}(u_i)$, satisfaction of the above linear equation system is the same as the m bits of v satisfying the linear equation system

$$(*) \qquad \left\{ \begin{array}{rcl} \langle f_1(u_i), v \rangle & = & b_1 \\ \langle f_2(u_i), v \rangle & = & b_2 \\ \vdots & \vdots & \vdots \\ \langle f_s(u_i), v \rangle & = & b_s \end{array} \right. ,$$

where the polynomial $f_\rho(X) = \sum_{j=0}^{n-1} a_{\rho j} X^j$, for $1 \leq \rho \leq s$.

However, these equations, over the m bits of v, are linearly independent over $\mathbf{Z}_2$, as long as u_i is not a root of any polynomial in Q.

There can be at most $(2^s - 1) \cdot (n-1)$ roots for the polynomials in Q, which is $< n^{\ell+1}$.

Since there are $n^{\ell+1}$ many u_i's, some u_i is not a root of any polynomial in Q. Then for this u_i, it can not be the case that all points of $\tilde{D}(u_i)$ satisfy the linear equation system. For, $|\tilde{D}(u_i)|$, which is the same as the number of v's in $\tilde{D}(u_i)$, is $> \frac{2^m}{n^\ell}$, while the linear equation system $(*)$, for any given right hand side $b_1, b_2, \ldots, b_s$, has exactly $2^m/2^s = 2^m/n^\ell$ solutions. This proves that not all points in $\tilde{D}$ satisfy any given s independent linear equations. $\square$

The next lemma gives a uniqueness criterion for the reconstruction of a linear function defined on a vector space over $\mathbf{Z}_2$.

Lemma 3 *Suppose V is a vector space over $\mathbf{Z}_2$ of dimension n, and $\tilde{V}$ is a non-empty subset in V such that no linear subspace of V of co-dimension 1 has a fraction of $1 - 1/n$ of the points of $\tilde{V}$. Then, for any function α defined on $\tilde{V}$, if linear functions ℓ_1 and ℓ_2 on V both agree with α on at least a fraction of $1 - 1/(2n)$ points of $\tilde{V}$, then $\ell_1 = \ell_2$.*

Proof. Suppose ℓ_1 and ℓ_2 are two distinct linear functions on V, both agree with α on at least a fraction of $1 - 1/(2n)$ points of $\tilde{V}$.

The linear subspace V_1 of V determined by the equation $\ell_1 = \ell_2$ is of co-dimension 1. Thus,

$$\frac{|\{x \in \tilde{V} \mid \ell_1(x) = \ell_2(x)\}|}{|\tilde{V}|} < 1 - \frac{1}{n}.$$

Therefore, more than a fraction of $1/n$ of points in $\tilde{V}$ are in the complement of V_1,

$$V_1^c = \{x \in V \mid \ell_1(x) \neq \ell_2(x)\}.$$

For each point x in V_1^c, if $x \in \tilde{V}$ then the function $\alpha(\cdot)$ is defined there, and $\alpha(x)$ must either disagree with $\ell_1(x)$ or disagree with $\ell_2(x)$. Wolog assume α has at least as much disagreement with ℓ_1 as with ℓ_2 on $V_1^c \cap \tilde{V}$. Then the total disagreement between α and ℓ_1 must be more than $1/(2n)$, a contradiction.

Hence, there could be at most one linear function which agrees with α on at least a fraction of $1 - 1/(2n)$ points of $\tilde{V}$. $\square$

Lemma 3 is a special case of the following more general lemma, which we include here for its own interest. The reader can skip it without loss of continuity, as we shall not need this more general form in the subsequent proofs.

Lemma 2.2e *Suppose V is a vector space over any finite field $\mathbf{F}$ of dimension n, and $\tilde{V}$ is a non-empty subset in V such that no linear (respectively, affine linear) subspace of V of co-dimension 1 has a fraction of $1 - 1/n$ of the points of $\tilde{V}$. Then, for any function α defined on $\tilde{V}$, if linear (respectively, affine linear) functions ℓ_1 and ℓ_2 on V both agree with α on at least a fraction of $1 - 1/(2n)$ points of $\tilde{V}$, then $\ell_1 = \ell_2$.*

Proof. The proof in the case of linear subspaces and linear functions is the same as Lemma 3. Let's consider the affine case.

Assume ℓ_1 and ℓ_2 are two distinct affine linear functions on V. Consider the affine linear function $\ell_1 - \ell_2$. By our assumption, $\ell_1 - \ell_2$ is not identically zero.

We claim that it is not identically a constant $c \in \mathbf{F}$ either. Suppose it is a constant $c \neq 0$. Then on $\tilde{V}$, α agrees with at most one of ℓ_1 and ℓ_2. The fraction of agreement with one of them must be at most $1/2$. However, this fraction of agreement is assumed to be $\geq 1 - 1/(2n)$. Hence $n = 1$. But even that is impossible, because of our assumption on the set $\tilde{V}$. In fact if we take any point $v \in \tilde{V}$, and let $V_1 = \{v\}$ be the 0-dimensional affine space, V_1 is of co-dimension 1, and yet the fraction of points from $\tilde{V}$ is

$$\frac{|\tilde{V} \cap V_1|}{|\tilde{V}|} > 0,$$

and not less than $1 - 1/1 = 0$ as assumed.

Hence, $\ell_1 - \ell_2 = 0$ defines an affine subspace V_1 of V of co-1 dimension. Thus, by assumption,

$$\frac{|\tilde{V} \cap V_1|}{|\tilde{V}|} < 1 - \frac{1}{n},$$

which is the same as

$$\frac{|\tilde{V} \cap V_1^c|}{|\tilde{V}|} > \frac{1}{n},$$

here V_1^c denotes the complement of V_1.

On $\tilde{V} \cap V_1^c$, α agrees with at most one of ℓ_1 and ℓ_2. Let's say there is at least as much disagreement bwteen α and ℓ_1 on $\tilde{V} \cap V_1^c$ as that between α and ℓ_2. Now

$$\frac{|\{x \in \tilde{V} \mid \alpha(x) \neq \ell_1(x)\}|}{|\tilde{V}|} \geq \frac{|\{x \in \tilde{V} \cap V_1^c \mid \alpha(x) \neq \ell_1(x)\}|}{|\tilde{V} \cap V_1^c|} \cdot \frac{|\tilde{V} \cap V_1^c|}{|\tilde{V}|}.$$

The second fraction is $> 1/n$ as stated earlier. The first fraction is at least $1/2$, for, otherwise,

$$\frac{|\{x \in \tilde{V} \cap V_1^c \mid \alpha(x) \neq \ell_1(x)\}|}{|\tilde{V} \cap V_1^c|} < \frac{1}{2},$$

and thus

$$\frac{|\{x \in \tilde{V} \cap V_1^c \mid \alpha(x) \neq \ell_2(x)\}|}{|\tilde{V} \cap V_1^c|} \leq \frac{|\{x \in \tilde{V} \cap V_1^c \mid \alpha(x) \neq \ell_1(x)\}|}{|\tilde{V} \cap V_1^c|} < \frac{1}{2},$$

as well, and yet on $\tilde{V} \cap V_1^c$ either $\alpha(x) \neq \ell_1(x)$ or $\alpha(x) \neq \ell_2(x)$, a clear contradiction.

It follows that

$$\frac{|\{x \in \tilde{V} \mid \alpha(x) \neq \ell_1(x)\}|}{|\tilde{V}|} > \frac{1}{2n},$$

contradicting the assumption that α agrees with ℓ_1 on at least a fraction of $1 - 1/(2n)$ points of $\tilde{V}$. $\square$

3.2 The proof

We assume that on any input $\langle C, x, I, b\rangle$, the reduction produces in logspace two strings w and w', and a truth table such that memberships for "$w \in S$?" and "$w' \in S$?" determine whether the tuple $\langle C, x, I, b\rangle$ satisfies $\bigoplus_{i \in I} g_i(x) = b$. As in the 1-tt case, wolog, we may assume that on the tuple $\langle C, x, I, b\rangle$ and the complementary tuple $\langle C, x, I, 1-b\rangle$, the reduction produces the same two strings w and w', and the truth tables are complementary to each other.

We will use the set D as defined earlier. For notational simplicity we will denote by $f^1(u,v)$ and $f^2(u,v)$ respectively the two strings w and w', produced by the reduction on the tuple $\langle C, x, D(u,v), b\rangle$. We consider such a string w (respectively w') gives the point (u,v) a 1-color (respectively 2-color).

As we will only query strings of length bounded by a fixed polynomial in n, and the reduction can stretch the length of queried strings by a fixed polynomial factor, and *since the sparse set S has density bounded by a fixed polynomial*, we can assume that there can be at most n^d many strings from S queried by the reduction, for some constant $d \geq 1$. (Technically, we should define the language first, but it only changes a logarithmic factor as in the NC^1 proof.) Let $\Delta = 18 + 9d$. We will let our finite field $\mathbf{F} = GF(2^m)$ have exactly n^Δ many elements. Thus $2^m = n^\Delta$, and $m = O(\log n)$.

For any 1-color w, and for any u, define

$$V_u^w = \{v \in \mathbf{F} \mid f^1(u,v) = w\}.$$

Define

$$U^w = \{u \in \mathbf{F} \mid |V_u^w| > n^{14+7d}\}.$$

The intuitive meaning is that U^w consists of those u's in $GF(2^m)$ such that there is a relatively large subset ($> n^{14+7d}$) of $v \in GF(2^m)$ for which $f^1(u,v) = w$.

Now we have the following cases.

- Case 1. There exists a w such that $|U^w| \geq n^{13+6d}$.

  Intuitively this means that there is a popular string w such that there is a fairly large subset ($\geq n^{13+6d}$) of $u \in GF(2^m)$ which all have a relatively large subset ($> n^{14+7d}$) of $v \in GF(2^m)$ for which $f^1(u,v) = w$.

  In this Case 1, we need the following further definitions.

$$V_u^{w,w'} = \{v \in V_u^w \mid f^2(u,v) = w'\},$$

and

$$U^{w,w'} = \{u \in U^w \mid |V_u^{w,w'}| > n^{12+6d}\}.$$

Intuitively, this is the set of $u \in U^w$, which all have a relatively large subset ($> n^{14+7d}$) of $v \in GF(2^m)$ for which $f^1(u,v) = w$, which, further among those v's have a pretty large subset ($> n^{12+6d}$) of v's with the second color $f^2(u,v) = w'$.

The following cases need to be examined.

- Case 1.1. There exists a w' such that $|U^{w,w'}| \geq n^{7+3d}$.

  Intuitively, there is a 2-color w' which is popular in the sense that a still large ($\geq n^{7+3d}$) set of u from U^w of size $\geq n^{13+6d}$, each has a pretty large subset ($> n^{12+6d}$) of v having the same 1-color w as well as the 2-color w'.

  Assume each of all 4 possibilities for the memberships of "$w \in S$?" and "$w' \in S$?", we get a set of equations for each $u \in U^{w,w'}$ and for such a u for all $v \in V_u^{w,w'}$. The left hand side of such an equation is

$$\sum_{j=0}^{n-1} \langle w^j, v \rangle x_j.$$

  The right hand side of the equation is determined individually for each equation by the truth table evaluator for the reduction.

  Letting $\ell = 6 + 3d$ in Lemma 2. There are $n^{\ell+1}$ many u's, and for each u, there are strictly more than n^{12+6d} many v's, that is, more than $2^m/n^\ell = n^{\Delta-\ell} = n^{18+9d-(6+3d)} = n^{12+6d}$. Thus Lemma 2 applies. Therefore we can solve for a potential solution of all the gate values, with $O(\log n)$ free variables, in all 4 separate cases in parallel. As before we then check for all the $n^{O(1)}$ assignments and verify the unique correct solution using local informations of the circuit C.

  This finishes Case 1.1.

- Case 1.2. While there exists a w such that $|U^w| \geq n^{13+6d}$, for all w', $|U^{w,w'}| < n^{7+3d}$.

  Intuitively, there is a popular 1-color w, but no color w' is a popular 2-color, *among* $u \in U^w$. Note that, w' being a non-popular 2-color does not mean that no $u \in U^w$ will take it as the 2-color for some v. In fact, it is possible that every $u \in U^w$ will take it as the 2-color for some v; however, the number of u's in U^w which has a pretty large subset ($> n^{12+6d}$) of v having the 2-color w' is not large ($< n^{7+3d}$).

  We will break all elements in U^w into n^{7+4d} disjoint "blocks", each block consists of $\geq n^{6+2d}$ many u's. As the size of U^w is at least n^{13+6d}, this partition is allowed.

  We will say that a 2-color w' "names" a u in U^w, if this $u \in U^{w,w'}$. Intuitively such a u is among the small number ($< n^{7+3d}$) of u's in U^w, which have a pretty large subset ($> n^{12+6d}$) of v having the same 1-color w as well as the 2-color w'.

  Each w' can name less than n^{7+3d} many u's, and there are at most n^d strings that can be from S, so that the total number of u's that can be named by a string from S is less than n^{7+4d}. Hence less than n^{7+4d} many blocks can contain some u which is named by some string from S. Since there are n^{7+4d} many blocks, at least one block is free from any u named by strings from S. We call such a block a "clean" block.

Thus, in a clean block, let's consider an arbitrary u and its set of v's, V_u^w. Each $w' \in S$ may still appear in this "clean" block, but each $w' \in S$ can be the 2-color $f^2(u,v)$ for at most n^{12+6d} many (u,v), for $v \in V_u^w$. Thus, for each $u \in U^w$ within this clean block, at most n^{12+7d} many (u,v), for $v \in V_u^w$, can be 2-colored by some string $w' \in S$. At the same time, each $|V_u^w| > n^{14+7d}$.

Hence, if we just *assume* that the second color $f^2(u,v) \notin S$ for all $v \in V_u^w$, we will have made some error with the ratio of error less than $1/n^2$. This is true for all u in this clean block.

By assuming each of the two possibilities of "$w \in S$" or "$w \notin S$", (and all second colors $w' \notin S$), we can then formulate a system of equation for the values of the gates. The left hand side of such an equation has the form $\sum_{j=0}^{n-1} \langle u^j, v \rangle x_j$, and the right hand side of each equation is determined individually, as before, by the truth table evaluator for the reduction.

Clearly not all such equations can be expected to have a correct right hand side, even if we are in the correct case regarding "$w \in S$" or "$w \notin S$". However, for each u in the clean block, and in the correct case regarding membership of "$w \in S$?", we have a set of linear equation systems, one system of equations for each u,

$$\langle \sum_{j=0}^{n-1} u^j x_j, v \rangle = b_{u,v},$$

where v varies over V_u^w. And in this case, each u has a system of equations with an incorrectness ratio $< 1/n^2$. (The unknowns of such an equation system for a fixed u are the m bits of $\sum_{j=0}^{n-1} u^j g_j \in GF(2^m)$, where g_j is the true value of the jth gate.)

Our next task is to correct all the errors in these equations. We would have liked to reconstruct $\sum_{j=0}^{n-1} u^j g_j$ for each u. However, this is too much to be hoped for. The v's from V_u^w may be all from a proper subspace of $GF(2^m)$. Clearly the equations only give us information concerning the projection of $\sum_{j=0}^{n-1} u^j g_j$ in the dual space of the linear space spanned by V_u^w, $\mathrm{span}(V_u^w)$. Even the more modest goal of reconstructing only the projections of $\sum_{j=0}^{n-1} u^j g_j$ over the dual of the linear span of V_u^w may be too much to ask for. For example, the majority of the samples from V_u^w may be all concentrated in a proper subspace of the span of V_u^w, and yet, the correctness ratio is over all sample points.

However, the following technique will allow us to circumvent this difficulty. We will suitably "shrink" V_u^w to a smaller set $\widetilde{V_u^w}$, where, we maintain a sufficiently small incorrectness ratio, and at the same time the samples in $\widetilde{V_u^w}$ are well distributed so that Lemma 3 applies. The new subset $\widetilde{V_u^w}$ is smaller than V_u^w but not too much smaller. We then will take advantage of the fact that the linear space $\mathrm{span}(\widetilde{V_u^w}) \subseteq GF(2^m)$ has logarithmic dimension ($\leq m = O(\log n)$), and therefore there are only a polynomial number $n^{O(1)}$ of linear functions all together. We may try them all in parallel against the data on the sample points, and the linear function $v \mapsto \langle \sum_{j=0}^{n-1} u^j g_j, v \rangle$ which uniquely agrees with the given samples on a sufficiently high proportion, its uniqueness guaranteed by Lemma 3, will be found unambiguously.

To carry out this process, of shrinking V_u^w, we start with $\tilde{V} = V_u^w$. Within space $\mathrm{span}(\tilde{V})$ we repeatedly ask if there is a co-1 dimensional subspace V_1 on which at least a fraction of $1 - 1/\dim(\mathrm{span}(\tilde{V}))$ points of $\tilde{V}$ lie; and if so, we replace $\tilde{V}$ by $\tilde{V} \cap V_1$.

Let $m' = \dim(\mathrm{span}(V_u^w))$; clearly $m' \leq m$. But as $|V_u^w| > n^{14+7d}$ the dimension $m' = \Theta(\log n)$. The above "shrinking" process surely must terminate no later than at dimension 2. In fact, if this process were to continue to dimension 2, we would have obtained a set $\tilde{V}$ with cardinality at least

$$\left(1 - \frac{1}{m'}\right)\left(1 - \frac{1}{m'-1}\right)\cdots\left(1 - \frac{1}{2}\right) \cdot |V_u^w|,$$

all contained in a one dimensional subspace. This is clearly false, since

$$\left(1 - \frac{1}{m'}\right)\left(1 - \frac{1}{m'-1}\right)\cdots\left(1 - \frac{1}{2}\right) = \frac{1}{m'},$$

and $1/m' = \Omega\left(\frac{1}{\log n}\right)$, and yet $|V_u^w| > n^{14+7d}$.

Thus, this process can go on no more than $O(\log n)$ times, in fact it terminates at dimension no later than $(14 + 7d)\log n - \log m'$, and we end up with a set $\tilde{V}$ such that it has more than

$$\prod_{j=2}^{m'}\left(1 - \frac{1}{j}\right)|V_u^w| = \Omega\left(\frac{n^{14+7d}}{\log n}\right),$$

points.

On the other hand, the incorrectness ratio on this sub-sample set is at most

$$O\left(\frac{n^d \cdot n^{12+6d} \cdot \log n}{n^{14+7d}}\right) < \frac{1}{2n} < \frac{1}{2\dim(\mathrm{span}(\tilde{V}))},$$

for large n. Let $m^* = \dim(\mathrm{span}(\tilde{V}))$. Now Lemma 3 applies, since there is no co-1 dimensional subspace of the span of $\tilde{V}$ with at least a fraction of $1 - 1/m^*$ points of $\tilde{V}$. Hence there is at most one linear function defined on the span of $\tilde{V}$ which agrees with the data with a correctness ratio of at least $1 - 1/(2m^*)$.

As described earlier, using the fact that there are only a polynomial number of linear functions all together on a logarithmic dimensional space, we can exhaustively find the correct one (in the correct case for membership of "$w \in S$?").

Finally, we end up with the set of u's in a clean block of size $\geq n^{6+2d}$. For each u in the block, we know a set of values

$$\langle \sum_{j=0}^{n-1} u^j g_j, v \rangle,$$

for all $v \in \mathrm{span}(\tilde{V})$, where $\tilde{V}$ is the shrunken version of V_u^w with size $|\mathrm{span}(\tilde{V})| \geq |\tilde{V}| = \Omega\left(\frac{n^{14+7d}}{\log n}\right)$. Now if we set the parameter $\ell = 5 + 2d$ in Lemma 2, we have

$$2^m/n^\ell = n^{\Delta-(5+2d)} = n^{18+9d-(5+2d)} = n^{13+7d} < |\mathrm{span}(\tilde{V})|,$$

and the block size $\geq n^{6+2d} = n^{\ell+1}$. Apply Lemma 2, we will be able to solve as before. This finishes Case 1.

- Case 2. For every first color w, $|U^w| < n^{13+6d}$. That is, there are no popular first colors. More precisely, for every w as a first color, except for $< n^{13+6d}$ many u's, all other u's have $|V_u^w| \leq n^{14+7d}$, i.e., for at most n^{14+7d} many v's in $GF(2^m)$, $f^1(u,v) = w$.

  Break all elements in $GF(2^m)$ into n^{13+7d} disjoint "blocks", each block consists of n^{5+2d} many u's. As $GF(2^m)$ has $n^\Delta = n^{18+9d}$ many elements, this partition is allowed.

  Now we say a w "names" a u if $u \in U^w$. These are the u's in $GF(2^m)$ with $> n^{14+7d}$ many v's for which $f^1(u,v) = w$. Then, each $w \in S$ can name $< n^{13+6d}$ many u's, so that the total number of u's named by some $w \in S$ is $< n^{13+7d}$ as there are at most n^d strings from S. Hence the total number of blocks which contain some u named by some $w \in S$ is $< n^{13+7d}$. Consequently, a "clean" block which contains no such u exists.

  Let's focus on such a clean block B. For every u in the block, u is not named by any w from S, i.e., among $n^\Delta = n^{18+9d}$ many v's from $GF(2^m)$, only $\leq n^{14+7d}$ many can be 1-colored by any $w \in S$, hence a total of $\leq n^{14+8d}$ many can be 1-colored by colors from S.

  Define
  $$V_u'^{w'} = \{v \in GF(2^m) \mid f^2(u,v) = w'\},$$
  and
  $$U'^{w'} = \{u \in B \mid |V_u'^{w'}| > n^{16+8d}\}.$$

  Now we have the following two cases.

  - Case 2.1 There exists a second color w' such that $|U'^{w'}| \geq n^{4+d}$.

    We will form equations by assuming all first colors $w \notin S$ and assuming each of the two possibilities for this w', as to whether "$w' \in S$" or "$w' \notin S$". The equations are formed for each $u \in U'^{w'}$ and for each such u, for all $v \in V_u'^{w'}$. There are $\geq n^{4+d}$ many u's, and each has $> n^{16+8d}$ many equations.

    As before not all equations formed are valid equations, even in the case with the correct assumption with respect to whether "$w' \in S$?". However in the case of correct assumption on "$w' \in S$?", by assuming all first colors $w \notin S$, we have made errors for at most n^{14+8d} many v's, among more than n^{16+8d} many v's from $V_u'^{w'}$. Thus the ratio of error is $< 1/n^2$.

    By shrinking the subset $V_u'^{w'}$ to a smaller subset $\widetilde{V_u'^{w'}}$, we can insure the following are satisfied:

    1. the sample size is still quite large, namely $|\widetilde{V_u'^{w'}}| = \Omega\left(\frac{n^{16+8d}}{\log n}\right)$;
    2. the error ratio among the smaller sample set is still small, $< 1/(2\dim(\mathrm{span}(\widetilde{V_u'^{w'}})))$; and
    3. there are no co-1 dimensional subspace of $\mathrm{span}(\widetilde{V_u'^{w'}})$ with at least a fraction of $1 - 1/\dim(\mathrm{span}(\widetilde{V_u'^{w'}}))$ of all the points from $\widetilde{V_u'^{w'}}$.

Hence Lemma 3 applies, and as before, taking advantage of the fact that we are in a logarithmic dimensional space, we can reconstruct the unique linear function on span($\widetilde{V_u'^{w'}}$), defined by $\langle \sum_{j=0}^{n-1} u^j g_j, \cdot\rangle$. We do this for all $u \in U'^{w'}$ separately in parallel. Finally, we obtain a set of $\geq n^{4+d}$ many u, each with $\Omega\left(\frac{n^{16+8d}}{\log n}\right)$ equations corresponding to all v's in span($\widetilde{V_u'^{w'}}$).

Let the parameter $\ell = 3+d$ in Lemma 2, then we have $n^{\ell+1}$ many u's, and for each u, the number of v's for which we have an equation is more than $2^m/n^\ell = n^{\Delta-(3+d)} = n^{15+8d}$. Hence Lemma 2 applies, and we solve and verify the linear equations as before.

This finishes Case 2.1.

- Case 2.2. In the clean block B chosen under the assumption of Case 2, it is the case that for all second color w', $|U'^{w'}| < n^{4+d}$.

  We say a 2-color w' "claims" a $u \in B$, if $u \in U'^{w'}$. Each color w', in particular $w' \in S$, can only claim $< n^{4+d}$ many u's, and therefore all together $< n^{4+2d}$ many u's can be claimed by some $w' \in S$.

  Now we will further break the block B into n^{4+2d} subblocks B', each consisting of exactly n many u's. As the block B has size $\geq n^{5+2d}$, such a partition is allowed. As the number of subblocks is greater than the number of u that can be claimed by some $w' \in S$, some subblock B' is "clean" in the sense that B' is free of any u claimed by strings from S.

  We focus our attention on this clean subblock B' of a clean block B. For any $u \in B'$, and any $w' \in S$, as $u \notin U'^{w'}$, we have by definition $|V_u'^{w'}| \leq n^{16+8d}$. Thus at most n^{16+9d} many $v \in GF(2^m)$ can have $f^2(u,v) \in S$. Meanwhile, since this is a clean block B, at most n^{14+7d} many v from $GF(2^m)$ can have $f^1(u,v) = w$ for any fixed $w \in S$, thus, at most n^{14+8d} many $v \in GF(2^m)$ can have $f^1(u,v) \in S$. The combined total of $v \in GF(2^m)$ with either $f^1(u,v) \in S$ or $f^2(u,v) \in S$ is $< 2n^{16+9d}$.

  So, by assuming all first and second colors $f^1(u,v)$ and $f^2(u,v)$ both $\notin S$, we make errors with an error ratio $< 2/n^2$, over all $v \in GF(2^m)$.

  We can apply our Lemma 3 again (In Lemma 3 we would set $\tilde{V} = V$ here). But in fact, in this case we don't need to shrink our sample space; this is similar to the 1-tt case, where we can directly recover all $\sum_{j=0}^{n-1} u^j g_j$ for $u \in B'$. Thus, we can just solve the Vandermonde system as there are n distinct u's.

  This handles the Case 2.2.

Of course we don't know in advance which case we are in, and more than one cases might be true. For instance, assuming we are in Case 2, within a block, we don't know whether we are in a clean block, there might be more than one clean blocks B_1 and B_2, and finally it might be the case that within clean block B_1, Case 2.1. holds, and within clean block B_2, it is Case 2.2 with several clean subblocks, (again we may not know which subblock is clean.)

The solution to this difficulty is just parallelism. We will assume all possible cases as enumerated here, and attempt to solve the linear systems. Some such assumption must be correct all the way as demonstrated above. Note that we will always verify in the end using local information about the circuit we will never produce an erroneous final output.

This completes our proof.

4 Conclusions

Recently Melkebeek has informed us that he can improve our result in [CNS95] from the collapse of P = NC^2 to P = NC^1 [vM95]. The idea is to do away with randomization and derandomization, as our proof is based on. But rather, Melkebeek goes directly to the Vandermonde system approach of the original paper by Cai and Sivakumar [CS95a], bypassing the explicit derandomization. This is very interesting mathematically as well as philosophically. The point philosophically is, platonically speaking, whether randomization is truly necessary to computation of deterministic problems. It is amusing to note that in the final stage of the Cai-Sivakumar proof [CS95a] all traces of randomization disappeared: there is no underlying randomized computation to be simulated. Randomization only makes its presence felt in its former shadow: one probably would never have arrived at the final proof had it not been for the randomization and derandomization in the earlier stages. However, Melkebeek shows us that the randomization and derandomization doctrine can also go the other way, and blind us from seeing the true and ultimate goal.

In any case, though, the proof presented here should be mathematically interesting since some new ideas are developed and are potentially useful elsewhere.

References

[BH77] L. Berman and J. Hartmanis. On isomorphisms and density of NP and other complete sets. *SIAM J. Comput.*, 6(2):305–322, 1977.

[CNS95] J. Cai, A. Naik, and D. Sivakumar. On the existence of hard sparse sets under weak reductions. Tech. Report 95-31, Department of Computer Science, State University of New York at Buffalo, Buffalo, NY, July 1995.

[CS95a] J. Cai and D. Sivakumar. The resolution of a Hartmanis conjecture. In *Proc. 36th Symp. on Found. of Comp. Sci.* IEEE, 1995. To appear.

[Har78] J. Hartmanis. On log-tape isomorphisms of complete sets. *Theoret. Comput. Sci.*, 7(3):273–286, 1978.

[Ogi95] M. Ogihara. Sparse hard sets for P yield space-efficient algorithms. In *Proc. 36th Symp. on Found. of Comp. Sci.* IEEE, 1995. To appear.

[OW91] M. Ogiwara and O. Watanabe. On polynomial time bounded truth-table reducibility of NP sets to sparse sets. *SIAM J. Comput.*, 20(3):471–483, 1991.

[vM95] D. van Melkebeek. On truth-table reductions of P sets to sparse sets. Manuscript, 1995.