The Communication Complexity of Enumeration, Elimination, and Selection

Andris Ambainis[‡] Univ. of CA at Berkeley
Harry Buhrman[§] CWI
William Gasarch[¶] Univ. of MD at College Park
Bala Kalyanasundaram[‖] Georgetown Univ.
Leen Torenvliet[**] Univ. of Amsterdam

Abstract

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Assume Alice has $x_1, \ldots, x_k \in \{0,1\}^n$, Bob has $y_1, \ldots, y_k \in \{0,1\}^n$, and they want to compute $f(x_1, y_1) \cdots f(x_k, y_k)$ communicating as few bits as possible. The Direct Sum Conjecture of Karchmer, Raz, and Wigderson, states that the obvious way to compute it (computing $f(x_1, y_1)$, then $f(x_2, y_2)$, etc.) is, roughly speaking, the best. This conjecture arose in the study of circuits since a variant of it implies $\mathrm{NC}^1 \neq \mathrm{NC}^2$.

We consider three related problems.

Enumeration: Alice and Bob output $e \leq 2^k - 1$ elements of $\{0,1\}^k$, one of which is $f(x_1, y_1) \cdots f(x_k, y_k)$.

Elimination: Alice and Bob output an element of $\{0,1\}^k$ that is not $f(x_1, y_1) \cdots f(x_k, y_k)$.

Selection: ($k = 2$) Alice and Bob output $i \in \{1,2\}$ such that if $f(x_1, y_1) = 1 \vee f(x_2, y_2) = 1$ then $f(x_i, y_i) = 1$.

We establish lower bounds on $\mathrm{ELIM}(f^k)$ for particular f and connect the complexity of $\mathrm{ELIM}(f^k)$, $\mathrm{ENUM}(k, f^k)$, and $\mathrm{SELECT}(f^2)$ to the direct sum conjecture and other conjectures.

[‡]Dept. of C.S., University of CA at Berkeley, Berkeley, CA 94720, U.S.A Supported in part by Berkeley Fellowship for Graduate Studies and in part NSF grant CCR-98-00024. (Email: ambainis@cs.berkeley.edu)

[§]CWI, P.O. Box 94709, Amsterdamn, The Netherlands. Supported in part by the EU fifth framework program project QAIP IST-1999-11234. (Email: buhrman@cwi.nl.)

[¶]Dept. of C.S. and Inst. for Adv. Comp. Stud., University of MD., College Park, MD 20742, U.S.A. Supported in part by NSF grant CCR–9732692. (Email: gasarch@cs.umd.edu.)

[‖]Dept. of C.S. Georgetown University., Washington, DC 20057, U.S.A. Supported in part by NSF Grant CCR-9734927. (Email: kalyan@cs.georgetown.edu.)

[**]Dept. of C.S., University of Amsterdam, The Netherlands, (Email: leen@wins.uva.nl.)

1 Introduction

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Assume Alice has $x \in \{0,1\}^n$, Bob has $y \in \{0,1\}^n$, and both have unlimited computational power. They want to compute $f(x, y)$ transmiting as few bits as possible. Both need the correct answer at the end of the protocol. Let $\mathrm{D}(f)$ be the minimum number of bits they need to transmit to compute f. $\mathrm{D}(f) \leq n+1$ since Alice can transmit x to Bob, Bob can compute $f(x, y)$ and transmit it to Alice. Communication complexity investigates $\mathrm{D}(f)$ and variants thereof [21, 23, 33].

Let $k \in \mathsf{N}$ and let $f^k(x_1 \cdots x_k, y_1 \cdots y_k) = f(x_1, y_1) \cdots f(x_k, y_k)$ (where $|x_i| = |y_i| = n$). Now Alice has $x_1, \ldots, x_k$, Bob has $y_1, \ldots, y_k$, and they want to compute $f^k(x_1, \ldots, x_k, y_1, \ldots, y_k)$. Clearly $\mathrm{D}(f^k) \leq k\mathrm{D}(f)$. Does $\mathrm{D}(f^k) = k\mathrm{D}(f)$? There is a counterexample: For $x \in \{0,1\}^n$ let $|x|_1$ be the number of 1's in x. Let $f(x, y) = 1$ iff $|x|_1 + |y|_1 \geq n$. Let $n = 2^m$. One can show $\mathrm{D}(f) = m + 2$. (The $2^{m+1} + 1$ inputs in $\{(1^i 0^{2^m - i}, 1^{2^m - i} 0^i) \mid 0 \leq i \leq 2^m\} \cup \{(1^i 0^{2^m - i}, 1^{2^m - i - 1} 0^i) \mid 0 \leq i \leq 2^m - 1\}$ form a fooling set [21] so there is some branch of length $\lceil \log(2^{m+1} + 1) \rceil = m + 2$). For f^k consider that Bob need only transmit to Alice k numbers that are between 0 and $n = 2^m + 1$ (which takes $\lceil \log(2^m + 1)^k \rceil = \lceil k \log(2^m + 1) \rceil$) and Alice then has to transmit back the answers (using k bits). Hence $\mathrm{D}(f^k) \leq \lceil k \log(2^m + 1) \rceil + k$. For m large enough $\log(2^m + 1) \leq m + \frac{1}{k}$ hence we get $\mathrm{D}(f^k) \leq km + k + 1$. However $k\mathrm{D}(f) = km + 2k$, so $k\mathrm{D}(f) - \mathrm{D}(f^k) \geq k - 1$.

Despite the counterexample there is a general notion that $\mathrm{D}(f^k)$ should be close to $k\mathrm{D}(f)$. This notion is refered to as the *Direct Sum Conjecture*, however the literature does not seem to have a formal statement.

Convention 1.1 A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is actually a family of functions, one for each n. We think of n as growing.

0-7695-0674-7/00 $10.00 © 2000 IEEE

We take the following formal statement which is implicit in [17] to be the Direct Sum Conjecture:

Direct Sum Conjecture: If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ then $\mathrm{D}(f^k) = k(\mathrm{D}(f) - O(1))$.

This conjecture arose in the study of circuits since a variant of it implies $\mathrm{NC}^1 \neq \mathrm{NC}^2$ (see [17] for connections to circuits, and see [21, Pages 42-48] for a more recent discussion). While there are no counterexamples to this conjecture there is some evidence against it [12].

What if Alice and Bob scale down their goals? We consider three such downscalings.

Notation 1.2 The notation $x \in \{\{0,1\}^n\}^k$ is used to emphasize that x is thought of as a concatenation of k strings of length n. The notation $x = x_1 x_2 \ldots x_k$ is understood to imply that $|x_1| = |x_2| = \cdots = |x_k| = n$. Similar conventions hold for $\{\{0,1\}^n\}^i$, $\{\{0,1\}^{n-1}\}^i$, and $\{\{0,1\}^n\}^{k-i}$.

Def 1.3 Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let $\mathcal{E}$ be the set of nonempty subsets of $\{0,1\}^k$ of size $\leq e$.

1. *Enumeration:* Alice and Bob output $e \leq 2^k - 1$ possibilities, one of which is the answer. Formally let $\mathrm{ENUM}(e, f^k) \subseteq \{\{0,1\}^n\}^k \times \{\{0,1\}^n\}^k \times \mathcal{E}$ be defined by $(x, y, E) \in \mathrm{ENUM}(e, f^k)$ iff $f^k(x, y) \in E$.

2. *Elimination:* Alice and Bob output a vector that is *not* the answer. Formally let $\mathrm{ELIM}(f^k) \subseteq \{\{0,1\}^n\}^k \times \{\{0,1\}^n\}^k \times \{0,1\}^k$ be defined by $(x, y, b) \in \mathrm{ELIM}(f^k)$ iff $f^k(x, y) \neq b$.

3. *Selection:* $(k = 2)$ Alice and Bob output $i \in \{1,2\}$ such that if $f(x_1, y_1) = 1 \vee f(x_2, y_2) = 1$ then $f(x_i, y_i) = 1$. Formally let $\mathrm{SELECT}(f^2) \subseteq \{\{0,1\}^n\}^2 \times \{\{0,1\}^n\}^2 \times \{1,2\}$ be defined by $(x_1x_2, y_1y_2, i) \in \mathrm{SELECT}(f^2)$ iff $(f(x_1, y_1) = 1 \vee f(x_2, y_2) = 1) \Rightarrow f(x_i, y_i) = 1$.

Let $i \leq k$. Clearly $\mathrm{D}(\mathrm{ENUM}(2^{k-i}, f^k)) \leq i\mathrm{D}(f)$: Alice and Bob can transmit $i\mathrm{D}(f)$ bits to compute $b_1 b_2 \cdots b_i = f^i(x_1 x_2 \cdots x_i, y_1 y_2 \cdots y_i)$ and output $b_1 b_2 \cdots b_i \{0,1\}^{k-i}$ as the set of possibilities. We state (for the first time) the following conjecture which generalizes the Direct Sum Conjecture.

Enum. Conjecture: If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $i \leq k$ then $\mathrm{D}(\mathrm{ENUM}(2^{k-i} - 1, f^k)) = (i+1)(\mathrm{D}(f) - O(1))$.

Elim. Conjecture: If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ then $\mathrm{D}(\mathrm{ELIM}(f^k)) = \mathrm{D}(f) - O(1)$.

One approach to the Direct Sum Conjecture would be to prove the Enumeration Conjecture by induction on i, with the Elimination Conjecture as base case.

2 Definitions, Results, and Lemmas

In the following definition a protocol is a decision tree where, at each node, one of the players uses the knowledge of the string he has and the bits he has seen to transmit one bit to the other player. See [21] for details.

Def 2.1 Let $S \subseteq X \times Y \times Z$ such that, $(\forall x \in X, y \in Y)(\exists z \in Z)[S(x, y, z)]$. Let $0 \leq \epsilon \leq 1$.

1. $\mathrm{D}(S) \leq t$ if there is a t-bit deterministic protocol that will, on input (x, y), output some z such that $S(x, y, z)$.

2. $\mathrm{N}(S) \leq t$ if there is a t-bit non-deterministic protocol such that on input (x, y) some leaf outputs a z such that $S(x, y, z)$. Different leaves could output different correct answers, and some leaves may output I DON'T KNOW. The leaves that do not output I DON'T KNOW are called *real leaves*. The nondeterministic moves are binary and cost 1-bit of communication each. This definition is equivalent to saying that there exists sets $X_1, \ldots, X_{2^t} \subseteq X$, and $Y_1, \ldots, Y_{2^t} \subseteq Y$, and $z_1, \ldots, z_i \in Z$ such that (1) $X \times Y \subseteq \bigcup_{i=1}^{2^t} X_i \times Y_i$, and (2) $(\forall i)(\forall x \in X_i)(\forall y \in Y_i)[S(x, y, z_i)]$. The collection $X_1 \times Y_1$, ..., $X_{2^t} \times Y_{2^t}$ is called a *covering*.

3. $\mathrm{R}_\epsilon^{\mathrm{pub}}(S) \leq t$ if there is a t-bit protocol such that (1) There exists N such that Alice and Bob get to observe N coin flips of a referee without being charged any bits for the privilege, and (2) the probability that the protocol outputs some z with $\neg S(x, y, z)$ is $\leq \epsilon$.

We state a subset of our results in weak form for readability.

Def 2.2

1. $\mathrm{EQ} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined by $\mathrm{EQ}(x, y) = \begin{cases} 1 & \text{if } x = y; \\ 0 & \text{if } x \neq y. \end{cases}$

2. $\mathrm{NE} : \{0,1\}^n \times n \to \{0,1\}$ is defined by $\mathrm{NE}(x, y) = 1 - \mathrm{EQ}(x, y)$.

3. $\mathrm{IP} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined by $\mathrm{IP}(x, y) = x \cdot y \pmod 2$. (Inner Prod mod 2.)

4. We can view $x \in \{0,1\}^n$ as a bit vector representation of a subset of $\{1, \ldots, n\}$. With this in mind $\mathrm{DISJ}(x, y) = \begin{cases} 1 & \text{if } x \cap y = \emptyset; \\ 0 & \text{if } x \cap y \neq \emptyset. \end{cases}$

5. $\text{INTER}(x,y) = 1 - \text{DISJ}(x,y)$.

For $f = \text{EQ}, \text{NE}, \text{IP}, \text{DISJ}$ and INTER it is known that $\text{D}(f) = n+1$ (see [21]).

Results about Particular Functions

1. $\text{D}(\text{ELIM}(\text{EQ}^k)) \geq n$ and $\text{D}(\text{ELIM}(\text{NE}^k)) \geq n$ (Theorem 3.3 and Corollary 3.4).
2. $\text{D}(\text{ELIM}(\text{DISJ}^k)) \geq n - O(\log n)$ and $\text{D}(\text{ELIM}(\text{INTER}^k)) \geq n - O(\log n)$. (Theorem 3.5 and Corollary 3.6).
3. $\text{D}(\text{ELIM}(\text{IP}^k)) \geq n$. (Theorem 5.4)
4. For several graph properties f, $\text{D}(f) \leq O(n \log n)$ and $\text{D}(\text{ELIM}(f^k)) \geq \Omega(n)$ (Theorem 4.8,4.9). Note— n is *not* length of input, it is the number of vertices. Length of input is $\binom{n}{2}$.
5. If k is constant then any randomized (public coin) protocol for $\text{ELIM}(\text{INTER}^k)$ or $\text{ELIM}(\text{IP}^k)$ with error $< \frac{1}{2^k}$ must transmit $\Omega(\frac{n}{(\log\log(n))(\log(n))})$ bits. (Theorems 6.4 and 6.5)

These results establish the Elimination Conjecture for f = EQ, NE , DISJ, INTER and IP. Result 4 can be restated as follows: for several graph properties f, $D(f^k) \geq \Omega(\frac{\text{D}(f)}{\log \text{D}(f)})$, which is a weak form of the Elimination Conjecture. Hence results 1,2,3 and 4 can be seen as evidence for the conjecture in that it holds or almost holds for several natural functions.

Results about General Functions

1. Assume that computing f^m but allowing one mistake requires $\frac{m}{2}\text{D}(f)$ bits for some (even) m. Then $\text{D}(\text{ELIM}(f^2)) = \Omega(\text{D}(f))$ bits. (Corollary 7.10)
2. $\text{N}(\text{SELECT}(f^2)) \geq \text{N}(f) - \log(n) - 1$. (Theorem 10.1)
3. If the Direct Sum Conjecture is true then $\text{D}(\text{SELECT}(f^2)) \geq \frac{\text{D}(f)}{3} - O(1)$. (Corollary 10.4)
4. If the Direct Sum Conjecture is true then $\text{D}(\text{ENUM}(k, f^k)) \geq \text{D}(f) - O(1)$.

These results link the Elimination Conjecture (and variants) to other conjectures that seem reasonable, and thus also provides evidence for its truth.

The complexity of doing k instances of a problem has been looked at in a variety of fields including decision trees [6, 25], computability [5, 13], complexity [2, 7, 19], straightline programs [10], and circuits [28].

Lemma 2.3 *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let $C \subseteq \{\{0,1\}^n\}^k \times \{\{0,1\}^n\}^k$. If $\text{N}(\text{ELIM}(f^k)) \leq t$ then there is $A \subseteq \{\{0,1\}^n\}^k$ and $B \subseteq \{\{0,1\}^n\}^k$ such that*

1. *$|C \cap (A \times B)| \geq |C|/2^t$, and*
2. *$(\exists b \in \{0,1\}^k)(\forall x \in A)(\forall y \in B)[f^k(x,y) \neq b]$.*

Pr: Since $\text{N}(\text{ELIM}(f^k)) \leq t$ we can cover $\{\{0,1\}^n\}^k \times \{\{0,1\}^n\}^k$ with a set of 2^t sets of the form $A \times B$ (which may overlap). These sets also cover C (and of course may also cover points outside of C). Since every element of C is covered, some set must cover $|C|/2^t$ elements of C. ∎

Lemma 2.4 *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, let $g = 1 - f$, and let $k \in \mathsf{N}$. Then $\text{D}(\text{ELIM}(f^k)) = \text{D}(\text{ELIM}(g^k))$.*

3 ELIM(EQ^k) and ELIM(DISJ^k)

Lemma 3.1 *Let $A, B \subseteq \{\{0,1\}^n\}^i$ be such that $(\forall x_1 \cdots x_i \in A)(\forall y_1 \cdots y_i \in B)(\exists j)[\text{EQ}(x_j, y_j) = 1]$. Then $|A||B| \leq 2^{2n(i-1)}$.*

Lemma 3.2 *If $D \subseteq \{\{0,1\}^n\}^k$ and $|D| > 2^{(k-1)n}$ then $(\forall b \in \{0,1\}^k)(\exists x, y \in D)[\text{EQ}^k(x,y) = b]$.*

Pr: By reordering the components of both b and the strings in D we need only consider $b = 1^{k-i}0^i$ for $0 \leq i \leq k$. Fix such an i, and hence such a b.

For each $z \in \{\{0,1\}^n\}^{k-i}$ let $D_z = z\{\{0,1\}^n\}^i \cap D$. Since $|D| > 2^{(k-1)n}$ and the D_z's partition D into at most $2^{(k-i)n}$ parts, there exists z such that $|D_z| > 2^{(i-1)n}$. Let $A = \{w \in \{\{0,1\}^n\}^i : zw \in D\}$. Note that $|A| = |D_z| > 2^{(i-1)n}$. By (the contrapositive of) Lemma 3.1 $(\exists x', y' \in A)(\forall j)[\text{EQ}(x'_j, y'_j) = 0]$. Clearly $\text{EQ}^k(zx', zy') = 1^{k-i}0^i$. ∎

Thm 3.3 *For all $k, n \in \mathsf{N}$, $\text{N}(\text{ELIM}(\text{EQ}^k)) \geq n$.*

Pr: Assume, by way of contradiction, that $\text{N}(\text{ELIM}(\text{EQ}^k)) = t < n$ via protocol P.

Let $C = \{(x,x) \mid x \in \{\{0,1\}^n\}^k\}$. By Lemma 2.3 there exists $A \subseteq \{\{0,1\}^n\}^k$ and $B \subseteq \{\{0,1\}^n\}^k$ such that (1) $|C \cap (A \times B)| \geq 2^{-t}|C| = 2^{kn-t}$ and (2) there is a real leaf L such that for all $(x,y) \in A \times B$ there is a nondeterministic computation path of $P(x,y)$ that terminates at L. Let the label of L be $b \in \{0,1\}^k$. Hence we know that $(\forall x \in A)(\forall y \in B)[\text{EQ}^k(x,y) \neq b]$.

Let $D = A \cap B$. Note that $|D| = |C \cap (D \times D)| = |C \cap (A \times B)| \geq 2^{kn-t} > 2^{kn-n} = 2^{n(k-1)}$. We can now apply Lemma 3.2 to obtain that $(\exists x, y \in D)[\text{EQ}^k(x,y) = b]$. This is a contradiction. ∎

Cor 3.4 *For all* $k, n \in \mathsf{N}$, $\mathrm{D}(\mathrm{ELIM}(\mathrm{NE}^k)) \geq n$.

Thm 3.5 *For all* $k, n \in \mathsf{N}$, $\mathrm{N}(\mathrm{ELIM}(\mathrm{DISJ}^k)) \geq n - O(\log n)$.

Pr: Let $L = \left\lceil \log(\binom{n}{\lceil n/2 \rceil}) \right\rceil \sim n - O(\log n)$. Let $\mathrm{ELIM}(\mathrm{EQ}_L^k)$ be $\mathrm{ELIM}(\mathrm{EQ}^k)$ on k-tuples of $\{0,1\}^L$. By Theorem 3.3 $\mathrm{N}(\mathrm{ELIM}(\mathrm{EQ}_L^k)) \geq L$. We show that $\mathrm{N}(\mathrm{ELIM}(\mathrm{EQ}_L^k)) \leq \mathrm{N}(\mathrm{ELIM}(\mathrm{DISJ}^k))$.

There are $\binom{n}{\lceil n/2 \rceil}$ subsets of $\{1, \ldots, n\}$ of size $\lceil \frac{n}{2} \rceil$. Each one can be represented as a string in $\{0,1\}^L$. Let F map $\{0,1\}^L$ to $\{0,1\}^n$ by mapping a represenation of an $\lceil \frac{n}{2} \rceil$-sized subset of $\{1, \ldots, n\}$ to its bit vector form. Let $G(x)$ be the complement of $F(x)$. Note that $\mathrm{EQ}(x,y)$ iff $\mathrm{DISJ}(F(x), G(y))$. Hence $\mathrm{EQ}^k(x_1 \cdots x_k, y_1 \cdots y_k) \neq b$ iff $\mathrm{DISJ}^k(F(x_1) \cdots F(x_k), G(y_1) \cdots G(y_k)) \neq b$.

The following protocol for $\mathrm{N}(eleqL)$ transmits $\mathrm{N}(\mathrm{ELIM}(\mathrm{DISJ}^k))$ bits, and hence shows that $\mathrm{N}(\mathrm{ELIM}(\mathrm{EQ}_L^k)) \leq \mathrm{N}(\mathrm{ELIM}(\mathrm{DISJ}^k))$. On input $(x_1 x_2 \cdots x_k, y_1 y_2 \cdots y_k) \in \{\{0,1\}^L\}^k \times \{\{0,1\}^L\}^k$ Alice and Bob run a protocol for $\mathrm{ELIM}(\mathrm{DISJ}^k)$ on $(F(x_1) \cdots F(x_k), G(y_1) \cdots G(y_k))$, and output its result. ∎

Cor 3.6 *For all* $k, n \in \mathsf{N}$, $\mathrm{D}(\mathrm{ELIM}(\mathrm{INTER}^k)) \geq n - O(\log n)$.

4 Graph Properties

Notation 4.1 In this section n is *not* the length of the input; it is the number of vertices. Formally Alice and Bob will both be given graphs on $\{1, \ldots, n\}$ and they will try to determine if some property holds of the union of the two graphs.

Def 4.2 If H and G are graphs then H is a *minor* of G if one can obtain H from G by removing vertices, removing edges, or contracting an edge (removing the edge and merging the two endpoints). We denote this by $H \preceq G$.

Def 4.3 Let $\mathrm{TRIV}_{a,b}$ be the graph that is a isolated vertices unioned with b disjoint edges.

We will show graph properties are hard by reduction. We first need to define reduction formally.

Def 4.4 [3] Let $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $g_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be infinite families of functions. $f \leq_{\mathrm{cc}} g$ means that there are functions T_1, T_2 and L such that $L : \mathsf{N} \to \mathsf{N}$, $L(n) \leq 2^{\mathrm{polylog}\, n}$, and $T_1, T_2 : \{0,1\}^n \to \{0,1\}^{L(n)}$ such that $f(x,y) = 1$ iff $g(T_1(x), T_2(y)) = 1$. If $L(n) = O(n)$ then L we say that $f \leq_{\mathrm{cc}} g$ *via a linear reduction.*

The following lemma we leave to the reader.

Lemma 4.5 *If* $f \leq_{\mathrm{cc}} g$ *by a linear reduction then (1)* $\mathrm{D}(g) = \Omega(\mathrm{D}(f))$, *(2)* $\mathrm{N}(g) = \Omega(\mathrm{N}(f))$, *(3)* $\mathrm{D}(\mathrm{ELIM}(g^k)) = \Omega(\mathrm{D}(\mathrm{ELIM}(f^k))$, *and (4)* $\mathrm{N}(\mathrm{ELIM}(g^k)) = \Omega(\mathrm{N}(\mathrm{ELIM}(f^k))$.

Notation 4.6 Let $V(G)$ be the set of vertices in G and $E(G)$ be the set of edges in G.

Using a theorem of Mader ([24] but see [8, Chapter 7, Theorem 1.16]) we can proof the following.

Lemma 4.7 *If* f *is a property of graphs closed under minors then for all* G *such that* $f(G) = 1$, $|E(G)| = O(|V(G)|)$.

Thm 4.8 *Let* f *be a property of graphs closed under minors. If* $(\forall a, b)[f(\mathrm{TRIV}_{a,b}) = 1]$ *then the following occur. Let* $g = 1 - f$.

1. $\mathrm{D}(f) \leq O(n \log n)$.
2. $\mathrm{DISJ} \leq_{\mathrm{cc}} f$ *by a linear reduction.*
3. $\mathrm{N}(f) \geq \Omega(\mathrm{N}(\mathrm{DISJ})) = \Omega(n)$.
4. $\mathrm{N}(\mathrm{ELIM}(f^k)) \geq \Omega(\mathrm{N}(\mathrm{ELIM}(\mathrm{DISJ}^k))) = \Omega(n)$.
5. $\mathrm{D}(g) \leq O(n \log n)$.
6. $\mathrm{INTER} \leq_{\mathrm{cc}} g$ *by a linear reduction.*
7. $\mathrm{D}(g) \geq \Omega(\mathrm{N}(\mathrm{DISJ})) = \Omega(n)$.
8. $\mathrm{D}(\mathrm{ELIM}(g^k)) \geq \Omega(\mathrm{N}(\mathrm{ELIM}(\mathrm{INTER}^k))) = \Omega(n)$.

Pr: We show $\mathrm{D}(f) \leq O(n \log n)$. By Lemma 4.7 there exists a constant c such that any graph with $f(G) = 1$ has $\leq cn$ edges.

Here is the protocol: Alice looks at how many edges she has. If she has more than cn edges then she sends Bob a 0, and they both know $f(G) = 0$. If not she sends Bob a 1 and then sends him a list of the edges she has. Since each edge takes $2 \log n$ bits to send and there are only cn edges, this takes $2cn \log n = O(n \log n)$ bits.

We show that $\mathrm{DISJ} \leq_{\mathrm{cc}} f$ by a reduction that maps a pair of n-bit strings to an $O(n)$-node graph. For any splitting of the graph the reduction works.

By the Graph Minor Theorem [30] there exists graphs $H_1, \ldots, H_k$ such that $f(G) = 0$ iff $(\exists i)[H_i \preceq G]$. Note that the H_i's could be disconnected; however, none of the H_i's can be $\text{TRIV}_{a,b}$.

Let H_1 be the graph that has the smallest largest component, where we measure size by number-of-edges. We view H_1 as being in two parts: $\text{TRIV}_{a,b} \cup A$ where A does not share any edges or vertices with $\text{TRIV}_{a,b}$. It is possible $a = 0$ or $b = 0$ or both. The graph A must have a component with ≥ 2 edges in it. Break up the edge set of A into two disjoint sets such that every connected graph of A with ≥ 2 edges is broken up. Call these two parts A_1 and A_2.

We define T_1 (respectively T_2). On input $T_1(x_1 \cdots x_n)$ (respectively $T_2(y_1 \cdots y_n)$) is defined as follows:

1. Put $\text{TRIV}_{a,b}$ on the first $a + 2b$ vertices. (Same with T_2). Break up the remaining vertices into n groups of $|V(A)|$ vertices each. (Same with T_2.)
2. For all $i \in \{1, \ldots, n\}$ do the following. If $x_i = 1$ then put A_1 on the ith group of vertices. If $x_i = 0$ then do not put those edges in. (If $y_i = 1$ then put A_2 on the ith group of vertices. If $y_i = 0$ then do not put those edges in.)

If $\text{DISJ}(x_1 \cdots x_n, y_1 \cdots y_n) = 0$ then there exists i such that $x_i = y_i = 1$. Hence G will have $\text{TRIV}_{a,b} \cup A = H_1$ as a minor so $f(G) = 0$.

If $\text{DISJ}(x_1 \cdots x_n, y_1 \cdots y_n) = 1$ then there is no such i. G will be $\text{TRIV}_{a,b}$ unioned with graphs all of whose components are smaller than the smallest largest component of a forbidden minor. Hence G cannot have any of $H_1, \ldots, H_k$ as minors, so $f(G) = 1$.

Items 3 and 4 follow from item 2, Theorem 3.5, and Lemma 4.5. Items 5,6, and 7 are easy consequences of items 1,2,3. Item 8 follows from item 4, Corollary 3.6, and Lemma 2.4. ∎

Thm 4.9 *Let f be a property of graphs. Assume that, for all n, there exists a graph $G = G_n$ such that (1) G has n vertices, (2) $f(G) = 1$, (3) for every proper subgraph H of G $f(H) = 0$, and (4) $|E(G)| \geq n$. Let $g = 1 - f$.*

1. $\text{DISJ} \leq_{\text{cc}} f$ *by a linear reduction.*
2. $\text{N}(f) \geq \Omega(\text{N}(\text{DISJ})) = \Omega(n)$.
3. $\text{N}(\text{ELIM}(f^k)) \geq \Omega(\text{N}(\text{ELIM}(\text{DISJ}^k))) = \Omega(n)$.
4. $\text{INTER} \leq_{\text{cc}} g$ *by a linear reduction.*
5. $\text{D}(g) \geq \Omega(\text{N}(\text{DISJ})) = \Omega(n)$.
6. $\text{D}(\text{ELIM}(g^k)) \geq \Omega(\text{N}(\text{ELIM}(\text{DISJ}^k))) = \Omega(n)$.

5 The Complexity of $\text{ELIM}(\text{IP}^k)$

Lemma 5.1 *Let $A, B \subseteq \{0,1\}^n - 0^n$ and let $i \in \{1, \ldots, n+1\}$. If $|A| \geq 2^i$ and $|B| \geq 2^{n-i-1}$ then $(\exists x \in A)(\exists y \in B)[\text{IP}(x, y) = 1]$.*

Pr: Let A' be the linear subspace of $\{0,1\}^n$ spanned by A. Then, $|A'| \geq |A| + 1 \geq 2^i + 1$ because $A \subseteq A'$ and $0^n \in A' - A$. Therefore, the dimension of A' is at least $i + 1$. This means that the dimension of $(A')^{\perp}$ is at most $n - i - 1$ and $|(A')^{\perp} - 0^n| \leq 2^{n-i-1} - 1$. Hence, there is an $x \in B$ and $y_1, \ldots, y_k \in A$ such that x and $\sum_{i=1}^{k} y_i \in A'$ are not perpendicular. Hence there must be an i such that $\text{IP}(x, y_i) = 1$. ∎

Lemma 5.2 *Let $A, B \subseteq \{0,1\}^n - 0^n$ and let $i \in \{1, \ldots, n+1\}$. If $|A| \geq 2^{i-2} + 1$ and $|B| \geq 2^{n-i} + 1$ then $(\exists x \in A)(\exists y \in B)[\text{IP}(x, y) = 0]$.*

Pr: Assume, by way of contradiction, that for every $x \in A$ and $y \in B$ we have $\text{IP}(x, y) = 1$. Fix $x_0 \in A$ and $y_0 \in B$. Let $A' = \{x - x_0 \mid x \in A\}$ and $B' = \{y - y_0 \mid y \in B\}$. For every $y \in B$, $\text{IP}(x - x_0, y) = \text{IP}(x, y) - \text{IP}(x_0, y) = 1 - 1 = 0$ and $\text{IP}(x - x_0, y - y_0) = \text{IP}(x - x_0, y) - \text{IP}(x - x_0, y_0) = 0$. Therefore, A' and $B'' = B \cup B'$ are perpendicular. Moreover, the subspaces spanned by A' and B'' are perpendicular.

The sets B and B' do not overlap: if $y \in B$ and $y - y_0 \in B$ then $\text{IP}(x_0, y - y_0) = 1$, so $\text{IP}(x_0, y) - \text{IP}(x_0, y_0) = 1$, and since $\text{IP}(x_0, y_0) = 1$ we get $\text{IP}(x_0, y) = 0$. The sets B and B' are the same size since the function $y \to y - y_0$ is a bijection between them.

The dimension of the subspace spanned by A' is at least $i-1$ because $|A'| = |A| \geq 2^{i-2}+1$. The dimension of the subspace spanned by B'' is at least $n - i + 2$ because $|B''| = |B| + |B'| = 2|B| = 2^{n-i+1} + 2$. The sum of these two dimensions is at least $(i-1)+(n-i+2) = n+1$. However, if two subspaces are perpendicular, the sum of their dimensions is at most n. This is a contradiction. ∎

Lemma 5.3 *Let $A, B \subseteq \{\{0,1\}^n - 0^n\}^k$ be such that $|A||B| > pH^{2k}$ where $p = \frac{1}{2^n - 4}$ and $H = 2^n - 1$. Then, for any $z \in \{0,1\}^k$, there are $x \in A$, $y \in B$ such that $\text{IP}^k(x, y) = z$.*

Proof sketch: By induction. The base case is $k = 1$: $A, B \subseteq \{\{0,1\}^n - 0^n\}$. and $|A||B| > pH^2 \geq 2^n$. By Lemmas 5.1 and 5.2, this implies that there are $x_1, x_2 \in A$, $y_1, y_2 \in B$ with $f(x_1, y_1) = 0$ and $f(x_2, y_2) = 1$.

For the induction step there are two cases: $z_k = 0$ and $z_k = 1$.

I) What if $z_k = 0$? Assume $k > 1$. Let A_1 be $\{x_1 \cdots x_{k-1} \mid x_1 \cdots x_k \in A \text{ for } \geq 1\ x_k\}$. For $i \in \{2, \ldots, n+1\}$ let A_i be $\{x_1 \cdots x_{k-1} \mid x_1 \cdots x_k \in A \text{ for } \geq 2^{i-2}+1\ x_k\}$.

The sets B_i are defined similarly.

We consider two cases:

Case 1: $|A_i||B_{n+2-i}| > pH^{2(k-1)}$ for some $i \in \{1, \ldots, n+1\}$. Then, by inductive assumption, there are $x_1 \cdots x_{k-1} \in A_i$ and $y_1 \cdots y_{k-1} \in B_{n-i}$ such that $\mathrm{IP}(x_1, y_1) = z_1$, ..., $\mathrm{IP}(x_{k-1}, y_{k-1}) = z_{k-1}$. We fix $x_1, y_1, \ldots, x_{k-1}, y_{k-1}$ with this property. Let $C = \{x_k \mid x_1 \cdots x_k \in A_i\}$, $D = \{y_k \mid y_1 \cdots y_k \in B_{n-i}\}$. Then, $|C| \geq 2^{i-2}+1$ and $|D| \geq 2^{n-i}+1$. By Lemma 5.2, this means that there are $x_k \in C, y_k \in D$ such that $\mathrm{IP}(x_k, y_k) = 0 = z_k$.

Case 2: For all $i \in \{1, \ldots, n+1\}$, $|A_i||B_{n+2-i}| \leq pH^{2(k-1)}$. We will show that this implies $|A||B| \leq pH^{2k}$, and hence cannot occur.

Note that $A_1 \supseteq A_2 \supseteq \cdots \supseteq A_{n+1}$. For every $x_1 \cdots x_k \in A$ we know that $x_1 \cdots x_{k-1}$ is either in $A_1 - A_2$ or $A_2 - A_3$ or $\cdots$ or $A_n - A_{n+1}$ or A_{n+1}. For $1 \leq i \leq n$, for every $x_1 \cdots x_{k-1} \in A_i - A_{i+1}$ there are at most 2^{i-1} extensions of it that are in A (by the definition of A_{i+1}). For every $x_1 \cdots x_{k-1} \in A_{n+1}$ there are at most $2^n - 1$ extensions of it that are in A since there are only $2^n - 1$ elements in $\{0,1\}^n - 0^n$. Clever algebra, which we omit, shows this cannot occur.

II) What if $z_k = 1$? Similar to the $z_k = 0$ case. ∎

Thm 5.4 *For all k, for all $n \geq 4$, $\mathrm{N}(\mathrm{ELIM}(\mathrm{IP}^k)) \geq n$.*

Pr: Let p and H be as in Lemma 5.3. Assume that $\mathrm{N}(\mathrm{ELIM}(\mathrm{IP}^k)) = t$. Let $C = (\{0,1\}^n - 0^n)^k \times (\{0,1\}^n - 0^n)^k$. Note that $|C| = H^{2k}$. By Lemma 2.3 there is an $A \subseteq \{\{0,1\}^n\}^k$, a $B \subseteq \{\{0,1\}^n\}^k$, and a vector $b \in \{0,1\}^k$, such that $|C \cap (A \times B)| \geq |H|^{2k}/2^t$ and $(\forall x \in A)(\forall y \in B)[\mathrm{IP}^k(x,y) \neq b]$. By the nature of C we can assume $A, B \subseteq (\{0,1\}^n - 0^n)^k$. By Lemma 5.3 if $|A||B| > pH^{2k}$ then $(\exists x \in A)(\exists y \in B)[\mathrm{IP}^k(x,y) = b]$. Since b is eliminated from being $\mathrm{IP}^k(x,y)$ we have $|A||B| \leq pH^{2k}$. Therefore $\frac{H^{2k}}{2^t} \leq pH^{2k}$, $\frac{1}{p} \leq 2^t$, and $2^n - 4 \leq 2^t$. Since $n \geq 4$ we have $t \geq n$. ∎

6 Lower Bounds on Rand. Protocols

Amplfiying probabilities in randomized communication complexity protocols is non-trivial since repeating a protocol n times (which is standard for randomized poly time) multplies complexity by n which is very large in this context. The next lemma shows how to amplify, though at a cost.

Lemma 6.1 *Let k and $\epsilon < \frac{1}{2^k}$ be constants. Let S be a relation on $\{0,1\}^n \times \{0,1\}^n \times Z$ such that $(\forall x)(\forall y)(\exists z)[S(x,y,z)]$. If $\mathrm{R}^{\mathrm{pub}}_{\epsilon}(S) \leq t$ then $\mathrm{R}^{\mathrm{pub}}_{1/\log n}(S) \leq O(t \log\log n)$.*

The next lemma applies a techniques from [1, Theorem 3.5][7, Lemma 4.3][26, Theorem 5.1] in a novel way.

Lemma 6.2 *Let $x_1, \ldots, x_{2^k-1}, y_1, \ldots, y_{2^k-1} \in \{0,1\}^*$ such that $(\forall i)[|x_i| = |y_i|]$. Let $X = x_1 \cdots x_{2^k-1}$ and $Y = y_1 \cdots y_{2^k-1}$. For $i = 1, \ldots, k$ let X_i (Y_i) be the concatenation of all x_j (y_j) such that the ith bit of j is 1. For example $X_1 = x_1 x_3 x_5 \cdots x_{2^k-1}$ and $X_2 = x_2 x_3 x_6 x_7 \cdots x_{2^n-2} x_{2^n-1}$. Assume $\mathrm{INTER}^k(X_k X_{k-1} \cdots X_1, Y_k Y_{k-1} \cdots Y_1) \neq b$ and $b \neq \vec{0}$. View b as a k-bit binary number (leading bits may be 0). Let X' (Y') be X with the x_b (y_b) removed. Then $\mathrm{INTER}(X,Y) = 1 \Rightarrow \mathrm{INTER}(X',Y') = 1$.*

Pr: If $\mathrm{INTER}(X,Y) = 1$ and $\mathrm{INTER}(x_b, y_b) = 0$ then clearly $\mathrm{INTER}(X',Y') = 1$. Hence we assume $\mathrm{INTER}(X,Y) = 1$ and $\mathrm{INTER}(x_b, y_b) = 1$.

Let $b = b_k b_{k-1} \cdots b_1$. Let $1 \leq j \leq k$. If $b_j = 1$ then x_b is a substring of X_j and y_b is a substring of Y_j and they are in the same position. Since $\mathrm{INTER}(x_b, y_b) = 1$ we obtain $\mathrm{INTER}(X_j, Y_j) = 1 = b_j$. Since $\mathrm{INTER}^k(X_k X_{k-1} \cdots X_1, Y_k Y_{k-1} \cdots Y_1) \neq b$ we have $\bigvee_{1 \leq i \leq k} \mathrm{INTER}(X_i, Y_i) \neq b_i$. Since $\mathrm{INTER}(X_i, Y_i) = b_i$ this reduces to $\bigvee_{1 \leq i \leq k, b_i = 0} \mathrm{INTER}(X_i, Y_i) \neq b_i$ hence $\bigvee_{1 \leq i \leq k, b_i = 0} \mathrm{INTER}(X_i, Y_i) = 1$. Let i_0 be such that $b_{i_0} = 0$ and $\mathrm{INTER}(X_{i_0}, Y_{i_0}) = 1$. Note that X_{i_0} (Y_{i_0}) does not have x_b (y_b) placed in it. Hence $\mathrm{INTER}(X',Y') = 1$. ∎

Lemma 6.3 ([16, 29]) $\mathrm{R}^{\mathrm{pub}}_{1/4}(\mathrm{INTER}) = \Omega(n)$ *even when restricted to*

$$D = \{(x,y) \in \{0,1\}^n \times \{0,1\}^n : \text{ for } \leq 1\ i\ x_i = y_i\}.$$

Thm 6.4 *Let k and $\epsilon < 1/2^k$ be constants. $\mathrm{R}^{\mathrm{pub}}_{\epsilon}(\mathrm{ELIM}(\mathrm{INTER}^k)) = \Omega(\frac{n}{\log(n)\log\log(n)})$.*

Pr: Assume $\mathrm{R}^{\mathrm{pub}}_{\epsilon}(\mathrm{ELIM}(\mathrm{INTER}^k)) = t(n)$ via protocol P'. By Lemma 6.1 we can obtain a protocol P such that $\mathrm{R}^{\mathrm{pub}}_{1/\log n}(\mathrm{ELIM}(\mathrm{INTER}^k)) = O(t(n)\log\log n)$ via P. We can also apply the protocol to k-tuples of inputs of length $\leq n$ by having both Alice and Bob pad with 0's. We will still assume it costs $t(n)\log\log n$.

We use P to obtain a randomized protocol for INTER that shows $\mathrm{R}^{\mathrm{pub}}_{1/4}(\mathrm{INTER}) = O(\frac{t(n)}{\log(n)\log\log(n)})$.

By Lemma 6.3 $R^{pub}_{1/4}(\text{INTER}) = \Omega(n)$, hence we have $t(n) = \Omega(n/\log n \log\log n)$.

Let X and Y be two strings of length n. Let Alice have X and Bob have Y. Alice and Bob divide X and Y into $2^k - 1$ parts that are roughly of the same length, so that $X = x_1 \dots x_{2^k-1}$ and $Y = y_1 \dots y_{2^k-1}$. Now $x_1, ..., x_{2^k-2}$ are of length $\lfloor n/(2^k-1) \rfloor$ and x_{2^k-1} has length $n - (2^k-2)\lfloor n/(2^k-1) \rfloor \geq \left\lfloor \frac{n}{2^k-1} \right\rfloor$. Let X_i (Y_i) be a string obtained from X (Y) as in Lemma 6.2. Note that $|X_i| = |Y_i| \leq n$ so we can apply the protocol P to $(X_k \cdots X_1, Y_k \cdots Y_1)$.

Run protocol P on $(X_k \cdots X_1, Y_k \cdots Y_1)$. If the protocol returns 0^k then Alice and Bob stop and reject. Note that if this happens then $Pr(\bigvee_{i=1}^k \text{INTER}(X_i, Y_i) = 1) \leq \frac{1}{\log n}$, so the probability of error is $\leq \frac{1}{\log n}$. If the protocol returns $b = b_1 \cdots b_k$ then by Lemma 6.2 with probability greater than $1 - \frac{1}{\log n}$ we have $\text{INTER}(X, Y) = 1 \Rightarrow \text{INTER}(X', Y')$ where X' is X with the x_b cut out (and Y' is similar). Next, Alice and Bob remove x_b and y_b from their strings and reiterate the process. Repeat up to $\log n$ times if needed.

A careful analysis shows that the probability that all steps are correct is $(1 - 1/\log n)^{O(\log n)}$, which is about e^{-c} for some constant c. By a variant of Lemma 6.1 we can iterate the algorithm a constant number of times to get the probability of error down to $\frac{1}{4}$. This constant gets absorbed into the big O. ∎

Thm 6.5 *Let k and $\epsilon < 1/2^k$ be constants.* $R^{pub}_{\epsilon}(\text{ELIM}(\text{IP}^k)) = \Omega(n/\log n \log\log n)$.

Pr: By Lemma 6.3 $R^{pub}_{1/4}(\text{INTER}) = \Omega(n)$ even when restricted to $D = \{(x, y) \in \{0,1\}^n \times \{0,1\}^n : \text{for} \leq 1\ i\ x_i = y_i\}$. On D, IP = DISJ. The proof of Theorem 6.4 can now be viewed as a lower bound on $R^{pub}_{\epsilon}(\text{ELIM}(\text{IP}^k))$. ∎

7 $D(\text{ELIM}(f^2))$ and $D(\text{ALMOST}(f^m))$

Def 7.1 If $\sigma, \tau \in \{0,1\}^*$ are strings of the same length then $\sigma =^1 \tau$ means that σ and τ are either identical or differ on one bit.

Def 7.2 Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ $\text{ALMOST}(f^k) \subseteq \{\{0,1\}^n\}^k \times \{\{0,1\}^n\}^k \times \{0,1\}^k$ is defined by $\{(x, y, b) \mid f^k(x, y) =^1 b\}$

Clearly $D(\text{ALMOST}(f^k)) \leq (k-1)D(f)$. We believe this is optimal but put forth a far weaker conjecture.

Conjecture 7.3 *For any function f, for any $k \in \mathsf{N}$,* $D(\text{ALMOST}(f^k)) \geq \frac{k}{2}D(f)$.

We establish some connections between the complexity of $\text{ALMOST}(f^k)$ and the complexity of enumeration.

Def 7.4 If $X \subseteq \{0,1\}^m$ and $1 \leq i_1, \dots, i_k \leq m$ then $X[i_1, \dots, i_k]$ is the projection of X onto those coordinates.

Lemma 7.5 *Let $X \subseteq \{0,1\}^m$. Let $b \in X$ be unknown. If $(\forall i, j)[|X[i, j]| \leq 3]$ then there is an algorithm that requests $\leq \lceil \frac{m}{2} \rceil - 1$ bits of b that produces $b' =^1 b$.*

Pr: We show the weaker theorem that there is an algorithm that requests $\leq \lceil \frac{m}{2} \rceil$ bits of b. We then show how to modify the algorithm to request $\leq \lceil \frac{m}{2} \rceil - 1$.

Let $\text{U} = \{1, \dots, m\}$, $\text{K} = \text{G} = \emptyset$. Throughout the algorithm U will be the set of indices i such that b_i is Unknown, nor have we ventured a Guess, K will be the set of indices i such that we Know b_i, and G will be the set of indices i such that we have made a Guess for b_i. At the end of the algorithm we will have $\text{U} = \emptyset$, $\text{K} \cup \text{G} = \{1, \dots, m\}$, and at most one of our guesses is wrong.

At all times U, K, and G are a partition of $\{1, \dots, m\}$. The expression "$\text{K} = \text{K} \cup \{a, i\}$" means that wherever a, i are, they leave those sets and go into K. Similar for other sets. Our final output will be $b' = b'_1 \cdots b'_m$. Initially $b'_1, \dots, b'_m$ are undefined. They may get set and reset several times; however at the end of the algorithm they will all be defined.

ALGORITHM

For i=1 to m
  If $X[i] = \{c\}$ then $b'_i = c$, $\text{K} = \text{K} \cup \{i\}$
For $i = 1$ to m, For $j = i + 1$ to m
  If $X[i, j] \subseteq \{00, 11\}$ then
    ASK(b_i =??)
    If $b_i = 1$ then $b'_i = 1$, $b'_j = 1$, $\text{K} = \text{K} \cup \{i, j\}$
    If $b_i = 0$ then $b'_i = 0$, $b'_j = 0$, $\text{K} = \text{K} \cup \{i, j\}$
  Else
  If $X[i, j] \subseteq \{01, 10\}$ then
    ASK(b_i =??)
    If $b_i = 1$ then $b'_i = 1$, $b'_j = 0$, $\text{K} = \text{K} \cup \{i, j\}$
    If $b_i = 0$ then $b'_i = 0$, $b'_j = 1$, $\text{K} = \text{K} \cup \{i, j\}$
End For loop (Note $|X[i, j]| \leq 2 \Rightarrow i, j \in \text{K}$.)
While $\text{U} \neq \emptyset$
  $i = \min(\text{U})$
  If $(\exists j, k \in \text{U} \cup \text{G} - \{i\})(\exists c_1, c_2 \in \{0,1\})[0c_1 \notin X[i, j] \wedge 1c_2 \notin X[i, k]]$ then (CASE 1)
    ASK(b_i =??)
    If $b_i = 0$ then $b'_i = 0$, $b'_j = 1 - c_1$, $\text{K} = \text{K} \cup \{i, j\}$

If $b_i = 1$ then $b'_i = 1$, $b'_k = 1 - c_2$, $K = K \cup \{i, k\}$

(Note that If $b_i = 0$ then since $b_i b_j \in X[i,j]$ and $0c_1 \notin X[i,j]$, we have $b_j = 1 - c_1$.

Similarly, If $b_i = 1$ we have $b_k = 1 - c_2$.)

Else (CASE 2- will prove below this must occur)

find $d \in \{0,1\}$ such that $(\forall j \in U \cup G - \{i\})[|\{d0, d1\} \cap X[i,j]| \leq 1]$

$b'_i = 1 - d$, $G = G \cup \{i\}$

End While

END OF ALGORITHM

It is easy to see that the algorithm (a) requests $\leq \lceil \frac{m}{2} \rceil$ coordinates, (b) sets all the b'_i, and (c) $(\forall i \in K)[b_i = b'_i]$.

Claim 1: Either Case 1 or Case 2 occurs.

Proof: Assume Case 1 does not occur. We show that Case 2 does. Intuitively Case 1 is saying that there is j, k such that $X[i,j]$ and $X[i,k]$ *exclude* elements of $\{0,1\}^2$ that begin with different bits. The negation is that, for all j, k, $X[i,j]$ and $X[i,k]$ *exclude* elements of $\{0,1\}^2$ that begin with the same bit. This bit is the d in case 2. We proceed more formally. Fix $j_0 \in U \cup G - \{i\}$. Since $|X[i,j_0]| \leq 3$ either $(\exists c \in \{0,1\})[0c \notin X[i,j_0]]$ or $(\exists c \in \{0,1\})[1c \notin X[i,j_0]]$. We consider the first scenario (the second is similar)

Assume $(\exists c_1 \in \{0,1\})[0c_1 \notin X[i,j_0]$. (We call it "$c_1$" because it will later play the role of c_1 in Case 1, leading to a contradiction.) We have $|\{00,01\} \cap X[i,j_0]| \leq 1$ which looks like Case 2 for j_0 with $d = 0$. We show that $(\forall j \in U \cup G - \{i\})[|\{00,01\} \cap X[i,j]| \leq 1]$. Assume, by way of contradiction, that $(\exists j)[|\{00,01\} \cap X[i,j]| = 2]$. Since $|X[i,j]| \leq 3$ we have $(\exists c_2 \in \{0,1\})[1c_2 \notin X[i,j]]$. Hence

$$(\exists j_0, j \in U \cup G - \{i\})(\exists c_1, c_2 \in \{0,1\})$$

$$[0c_1 \notin X[i,j_0] \wedge 1c_2 \notin X[i,j]].$$

This *is* Case 1 with different names for the variables; hence it is really Case 1, a contradiction.

End of Proof of Claim 1

Claim 2: There is at most one $i \in G$ such that $b_i \neq b'_i$.

Proof: Assume, by way of contradiction, that there exists $i_1, i_2 \in G$ with $b_{i_1} \neq b'_{i_1}$ and $b_{i_1} \neq b'_{i_1}$. Since $i_1, i_2 \in G$ we know that (1) they are both the chosen i in some phase, (2) when they are chosen Case 2 occurs, and (3) they are both always in $U \cup G$. Since $b_{i_1} \neq b'_{i_1}$ when $i = i_1$ we get Case 2 with $d = b_{i_1}$. Since $i_2 \in U \cup G$ we get $|\{b_{i_1}0, b_{i_1}1\} \cap X[i_1, i_2]| \leq 1$. Similarly, $|\{b_{i_2}0, b_{i_2}1\} \cap X[i_2, i_1]| \leq 1$ which we rewrite as $|\{0b_{i_2}, 1b_{i_2}\} \cap X[i_1, i_2]| \leq 1$.

We prove that $|X[i_1, i_2]| \leq 2$ and hence it must have been dealt with before the while loop even started, which contradicts $i_1, i_2 \in U$. Clearly $b_{i_1}b_{i_2} \in X[i_1, i_2]$. Since $|\{b_{i_1}0, b_{i_1}1\} \cap X[i_1, i_2]| \leq 1$ we get $b_{i_1}(1 - b_{i_2}) \notin X[i_1, i_2]$. Since $|\{0b_{i_2}, 1b_{i_2}\} \cap X[i_1, i_2]| \leq 1$ we get $(1 - b_{i_1})b_{i_2} \notin X[i_1, i_2]$. Since $b_{i_1}(1 - b_{i_2}) \neq (1 - b_{i_1})b_{i_2}$ we have eliminated two elements from $X[i_1, i_2]$. Hence $|X[i_1, i_2]| \leq 2$.

End of Proof of Claim 2

Claim 3: The algorithm can be modified to request $\lceil m/2 \rceil - 1$ bits.

Proof: Run the algorithm keeping track of how many queries it makes. If it stops before making $\lceil m/2 \rceil$th queries then we are done. If it is about to make its $\lceil m/2 \rceil$th query then stop it. Each of the first $\lceil m/2 \rceil - 1$ queries lead to 2 indices being placed in the K set. Hence $m - 2$ bits are known for certain. Let the unknown bits be indexed i and j. Let $c_i c_j \notin X[i,j]$. Set $b'_i = 1 - c_i$ and $b'_j = 1 - c_j$. They cannot both be incorrect since $b_i b_j \neq c_i c_j$.

End of Proof of Claim 3 ∎

Lemma 7.6 *Let $X \subseteq \{0,1\}^m$. Let $b \in X$ be unknown. Let $2 \leq k \leq m$. If $(\forall i_1, \ldots, i_k)[|X[i_1, \cdots, i_k]| \leq k + 1]$ then there is an algorithm that requests $\leq \max\{\lceil \frac{m}{2} \rceil - 1, k - 1\}$ bits of b that produces $b' =^1 b$.*

Pr: We prove this by induction on k. Lemma 7.5 gives the base case of $k = 2$. Assume $k \geq 3$ and that the lemma holds for $k - 1$. Assume $X \subseteq \{0,1\}^m$ and $(\forall i_1, \ldots, i_k)[|X[i_1, \cdots, i_k]| \leq k + 1]$. If $(\forall i_1, \ldots, i_{k-1})[|X[i_1, \cdots, i_{k-1}]| \leq k]$ then we are done by induction. If not then $(\exists i_1, \ldots, i_{k-1})[|X[i_1, \cdots, i_{k-1}]| \geq k + 1]$. Let $i \in \{1, \ldots, m\} - \{i_1, \ldots, i_{k-1}\}$. Since $|X[i_1, \ldots, i_{k-1}, i]| \leq k + 1$ and $|X[i_1, \cdots, i_{k-1}]| \geq k + 1$ for every $c \in X[i_1, \ldots, i_{k-1}]$ exactly one of $c0$ or $c1$ is in $X[i_1, \ldots, i_{k-1}, i]$. Hence if we ask for the values of $b_{i_1}, \ldots, b_{i_{k-1}}$ we can determine the values of all the other b_i. This takes $k - 1$ questions. ∎

Note 7.7 In addition to its use here, Lemma 7.6 can also be used to prove the following new theorem: if C_k^A is $k + 1$-enumerable then, for all m, one can compute C_m^A with at most one error using $\max\{\lceil \frac{m}{2} \rceil, k - 1\}$ of the queries given.

Thm 7.8 *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Then $D(ALMOST(f^m)) \leq \binom{m}{k} D(ENUM(k+1, f^k)) + \max\{\lceil \frac{m}{2} \rceil - 1, k - 1\} D(f)$.*

Pr: We exhibit a protocol for ALMOST(f^m) that will invoke a D(ENUM($k + 1, f^k$)) protocol $\binom{m}{k}$ times, and an f protocol at most $\max\{\lceil \frac{m}{2} \rceil - 1, k - 1\}$ times.

1) Alice has $x = x_1x_2\cdots x_m$, Bob has $y = y_1y_2\cdots y_m$.

2) For all $i_1 < \cdots < i_k \subseteq \{1,\ldots,m\}$ Alice and Bob compute a set of $k+1$ possibilities for $f^k(x_{i_1}x_{i_2}\cdots x_{i_k}, y_{i_1}y_{i_2}\cdots y_{i_k})$. This invokes a $\mathrm{D}(\mathrm{ENUM}(k+1, f^k))$ protocol $\binom{m}{k}$ times.

3) Let $X \subseteq \{0,1\}^m$ be the set of possibilities for $f^m(x,y)$ that are consistent with the information gathered in step 2. (That is, $b \in X$ iff for every $i_1,\ldots,i_k$ the string $b_{i_1}\cdots b_{i_k}$ was output when Alice and Bob enumerated $f^k(x_{i_1}\cdots x_{i_k}, y_{i_1}\cdots y_{i_k})$. Note that X is nonempty since $f(x_1,y_1)\cdots f(x_m,y_m) \in X$.) Note that Alice and Bob both know X and that X satisfies Lemma 7.6.

4) Alice and Bob perform the algorithm in Lemma 7.6.2 with X as in the previous step and $b = f^k(x,y)$. Whenever they need to find a particular bit $f(x_i,y_i)$, they invoke an f protocol. This will happen at most $\max\{\lceil \frac{m}{2} \rceil - 1, k-1\}$ times.

∎

Cor 7.9 *Let $m,n \in \mathsf{N}$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Then* $\mathrm{D}(\mathrm{ALMOST}(f^m)) \leq \binom{m}{2}\mathrm{D}(\mathrm{ELIM}(f^2)) + (\lceil \frac{m}{2} \rceil - 1)\mathrm{D}(f)$.

Cor 7.10 *Let $m,n \in \mathsf{N}$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Assume Conjecture 7.3 holds for some even m. Then* $\mathrm{D}(\mathrm{ELIM}(f^2)) \geq \Omega(\mathrm{D}(f))$.

8 $\mathrm{N}(\mathrm{ENUM}(e, f^k))$, $\mathrm{N}(f)$, and $\mathrm{R}^{\mathrm{pub}}_{\epsilon}$

The next theorem uses ideas from the proof that p-superterse sets are in P/poly from [2].

Lemma 8.1 *Let $e,k,n \in \mathsf{N}$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Either* $\mathrm{N}(\mathrm{ENUM}(e-1, f^{k-1})) \leq \mathrm{N}(\mathrm{ENUM}(e, f^k)) + \log(kn) + O(1)$ *or* $\mathrm{R}^{\mathrm{pub}}_{1/4}(f) \leq \mathrm{N}(\mathrm{ENUM}(e, f^k))$.

Thm 8.2 *Let $e,k,n \in \mathsf{N}$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Either*

1. $\mathrm{R}^{\mathrm{pub}}_{1/4}(f) \leq \mathrm{N}(\mathrm{ENUM}(e, f^k))$ *or*
2. $\mathrm{N}(f) \leq \frac{\mathrm{N}(\mathrm{ENUM}(e,f^k))}{k-e+1} + e\log(kn) + O(e)$.

Cor 8.3 *Let $e,k,n \in \mathsf{N}$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Either* $\mathrm{R}^{\mathrm{pub}}_{1/4}(f) \leq \mathrm{N}(\mathrm{ENUM}(k, f^k))$ *or* $\mathrm{N}(f) \leq \mathrm{N}(\mathrm{ENUM}(k, f^k)) + \log(kn)$.

9 $\mathrm{D}(\mathrm{ENUM}(e, f^k))$ and Direct Sum Conj

Lemma 9.1 ([4, 9, 27]) *Let $X \subseteq \{0,1\}^k$ such that $|X| \leq k$. Let $b \in X$ be unknown. There is an algorithm that requests $\leq k-1$ bits of b that produces b.*

Thm 9.2 *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. For all k,* $\mathrm{D}(f^k) \leq \mathrm{D}(\mathrm{ENUM}(k, f^k)) + (k-1)\mathrm{D}(f)$

Pr: This is proven using a protocol that uses Lemma 9.1 in a manner similar to how Theorem 7.8 used Lemma 7.6. ∎

Cor 9.3 *If the Direct Sum conjecture holds at k then* $\mathrm{D}(\mathrm{ENUM}(k, f^k)) \geq \mathrm{D}(f) - O(k)$.

10 The Comm. Comp. of Selection

The next theorem uses ideas from the proof in [18] that p-selective sets are in P/poly.

Thm 10.1 *Let $n \in \mathsf{N}$ and $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Then* $\mathrm{N}(\mathrm{SELECT}(f^2)) \geq \mathrm{N}(f) - \log(n) - 1$ *and* $\mathrm{N}(\mathrm{SELECT}(f^2)) \geq \mathrm{coN}(f) - \log(n) - 1$.

By $\mathrm{N}(\mathrm{SELECT}(f^2)) \geq \mathrm{N}(\mathrm{ELIM}(f^2))$ and Theorem 3.5 we have $\mathrm{N}(\mathrm{SELECT}(\mathrm{DISJ}^2)) \geq n - O(\log n)$. By Theorem 10.1 and $\mathrm{N}(\mathrm{DISJ}) \geq n+1$ (a fooling set argument) we have $\mathrm{N}(\mathrm{SELECT}(\mathrm{DISJ}^2)) \geq n - \log(n)$. We improve this.

Thm 10.2 $\mathrm{N}(\mathrm{SELECT}(\mathrm{DISJ}^2)) \geq n$.

Pr: Assume that $\mathrm{N}(\mathrm{SELECT}(\mathrm{DISJ}^2)) = t$ via protocol P. Let x_1 and x_2 be strings of length n such that $C(x_1|P,x_2) \geq n$ and $C(x_2|P,x_1) \geq n$. Let Alice have x_1x_2 and Bob have $\overline{x_1x_2}$. Let $b = b_1b_2\cdots b_t$ be a sequence of bits that form a possible path to a real leaf L that Alice and Bob could go down. (Note that b includes both the nondeterministic choice bits and the communication bits by the definition of nondeterministic protocols.) Assume that the leaf outputs 2 (the 1 case is similar).

We show that x_1 can be directly recovered from x_2, P, b. This shows $t \geq n$ since $C(x_2|P,x_1) \geq n$. Recovery algorithm: Enumerate all x such that $P(xx_2, \overline{xx_2})$ could end up at leaf L. There will only be one such x (proven below) and that one x is x_1.

Assume that x and x', get enumerated in the above recovery algorithm. Since $P(xx_2, \overline{xx_2})$ and $P(x'x_2, \overline{x'x_2})$ both end up at L, by a basic theorem in communication complexity [21, Propostion 1.14], the inputs $(xx_2, \overline{x'x_2})$ and $(x'x_2, \overline{xx_2})$ will end up

at L. Hence $\mathrm{DISJ}(x, \overline{x'})\mathrm{DISJ}(x_2, \overline{x_2}) \neq 01$. Since $\mathrm{DISJ}(x_2, \overline{x_2}) = 1$ we have $\mathrm{DISJ}(x, \overline{x'}) = 1$. We also get $\mathrm{DISJ}(x', \overline{x})\mathrm{DISJ}(x_2, \overline{x_2}) \neq 01$. Since $\mathrm{DISJ}(x_2, \overline{x_2}) = 1$ we have $\mathrm{DISJ}(x', \overline{x}) = 1$ Since x and $\overline{x'}$ are disjoint sets and x' and $\overline{x}$ are disjoint sets, $x = x'$. ∎

Thm 10.3 $\mathrm{D}(f^3) \leq 2\mathrm{D}(f) + 3\mathrm{D}(\mathrm{SELECT}(f^2))$.

Pr: For this theorem we use the definition $(x_1x_2, y_1y_2, b_1b_2) \in \mathrm{SELECT}(f^2)$ if $f(x_1, y_1) = b_1$ or $f(x_2, y_2) = b_2$ and $b_1 \neq b_2$. This is easily seen to be equivalent to the usual definition. We present a protocol for $\mathrm{D}(f^3)$ which transmits at most $2\mathrm{D}(f) + 3\mathrm{D}(\mathrm{SELECT}(f^2))$ bits. Assume Alice has $x_1x_2x_3$ and Bob has $y_1y_2y_3$. For $i, j \in \{1, 2, 3\}$ and $i < j$, Alice with inputs x_i, x_j and Bob with inputs y_i, y_j run the $\mathrm{SELECT}(f^2)$ protocol and produce output $b^1_{i,j}, b^2_{i,j}$. For each i, observe that Alice and Bob predict $f(x_i, y_i)$ exactly twice while running $\mathrm{SELECT}(f^2)$ thrice. Since the output of the $\mathrm{SELECT}(f^2)$ protocol is limited to 01 or 10, it must be the case that for some i, the two predictions of Alice and Bob on $f(x_i, y_i)$ do not match. Without loss of generality, let us assume that the mismatch happens for $i = 1$. Now Alice and Bob compute $f(x_1, y_1)$ by exchanging at most $\mathrm{D}(f)$ bits. Without loss of generality, let us assume that $b^1_{1,2} \neq f(x_1, y_1)$. Knowing this, Alice and Bob will correctly conclude that $f(x_2, y_2) = b^2_{2,1}$. Finally, Alice and Bob computes $f(x_3, y_3)$ by exchanging at most $\mathrm{D}(f)$ bits. ∎

Cor 10.4 *If the Direct Sum Conjecture holds then* $\mathrm{D}(\mathrm{SELECT}(f^2)) \geq \frac{1}{3}\mathrm{D}(f) - O(1)$.

11 Acknowledgments

We want to thank László Babai, Richard Chang, Steve Fenner, Anna Gal, Steve Homer, Vladik Kreinovich, Eyal Kushilevitz, Luc Longpre, Jacob Lurie, Noam Nisan, Michael Saks, and Frank Stephan for helpful discussions. The third author wants to thank Eyal Kushilevitz and Noam Nisan whose book [21] introduced him to the field.

References

[1] Agrawal and Arvind. Poly-time tt reductions to P-selective sets. STRUCTURES94.

[2] Amir, Beigel, Gasarch. Some connections between bounded query classes and non-uniform complexity. *STRUCTURES90*

[3] Babai, Frankl, Simon. Complexity classes in communication complexity theory *FOCS86*

[4] Beigel. Bounded queries to SAT and the Boolean hierarchy. *TCS*, 84:199–223, 1991.

[5] Beigel, Gasarch, Gill, Owings. Terse, superterse, and verbose sets. *I&C*, 103(1):68–85, 1993.

[6] Beigel, Hirst. One help bit doesn't help. *STOC98*

[7] Beigel, Kummer, Stephan. Approximable sets. *I&C*, 120(2):304–314, 1995.

[8] Bollobás. *Extremal Graph Theory.* Acad. Press, 1978.

[9] Bondy and Murty. *Graph Theory with applications.* American Elsevier, 1977.

[10] Bshouty. On the direct sum conjecture in the straight line model. *J. of Complexity*, 14, 1998.

[11] Cai, Hemachandra. Enumerative counting is hard. *I&C*, 82(1):34–44, 1989.

[12] Feder, Kushilevitz, Naor, Nisan. Amortized communication complexity. *SICOMP*, 24(4):736–750, 1995.

[13] Gasarch, Martin. *Bounded Queries in Recursion Theory.* Birkhäuser, 1999.

[14] Halstenberg, Reischuk. Relations between complexity classes. *JCSS*, 41:402–429, 1990.

[15] Jockusch. Semirecursive sets and positive reducibility. *Tran. of the AMS*, 131:420–436, 1968.

[16] Kalyanasundaram, Schnitger. The prob. communication complexity of set intersection. *SIAM J. on Disc. Math.*, 5:545–557, 1992. Earlier–STRUCTURES87.

[17] Karchmer, Raz, Wigderson. Super-log depth lower bounds via the direct sum in comm. comp. *Comp. Comp.*, 5, 1995. Earlier–STRUCTURES91.

[18] Ko. On self-reducibility and weak P-selectivity. *JCSS*, 26:209–221, 1983.

[19] Krentel. The complexity of optimization problems. *JCSS*, 36(3):490–509, 1988.

[20] Kummer. A proof of Beigel's cardinality conjecture. *JSL*, 57(2):677–681, 1992.

[21] Kushilevitz, Nisan. *Communication Complexity.* Camb. Univ. Press, 1997.

[22] Li, Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications.* Addison-Wesley, 1991.

[23] Lovász. Communications complexity: A survey. In B. Korte, editor, *Paths, Flows, and VLSI layout*, 1990. Springer-Verlag. Also CS-TR-204-89, Princeton Univ.

[24] Mader. Homomorphieeigenschaften und mittlere kantendichte von graphen. *Math. Ann.*, V. 174, 1967.

[25] Nisan, Rudich, Saks. Products and help bits in decision trees. *SICOMP*, 28, 1998.

[26] Ogihara. Polynomial-time membership comparable sets. *SICOMP*, 24, 1995. Earlier–STRUCTURES94.

[27] Owings. A cardinality version of Beigel's Nonspeedup Theorem. *JSL*, 54(3):761–767, 1989.

[28] Paul. Realizing Boolean functions on disjoint sets of variables. *TCS*, 2(3):383–396, 1976.

[29] Razborov. On the distributional complexity of disjointness. *TCS*, 106:385–390, 1992. Earlier–ICALP90.

[30] Robertson, Seymour. Graph minors XV: Wagner's conjecture. to appear in J. of Comb. Theory (B).

[31] Selman. P-selective sets, tally langs, and the behavior of p-time reducibilities on NP. *MST*, 13:55–65, 1979.

[32] Sivakumar. On membership comparable sets. *JCSS*, pages 270–280, 1999. Earlier–COMPLEXITY98.

[33] Yao. Some complexity questions related to distributive computing. *STOC79*