The Multiparty Communication Complexity of Exact-T: Improved Bounds and New Problems

Richard Beigel [*]
Temple University

William Gasarch [†]
Univ. of MD at College Park

James Glenn [‡]
Loyola College in Maryland

Abstract

Let $x_1, \ldots, x_k$ be n-bit numbers and $T \in \mathbb{N}$. Assume that $P_1, \ldots, P_k$ are players such that P_i knows all of the numbers *except* x_i. The players want to determine if $\sum_{j=1}^{k} x_j = T$ by broadcasting as few bits as possible. Chandra, Furst, and Lipton obtained an upper bound of $O(\sqrt{n})$ bits for the $k = 3$ case, and a lower bound of $\omega(1)$ for $k \geq 3$ when $T = \Theta(2^n)$. We obtain (1) for general $k \geq 3$ an upper bound of $k + O(n^{1/(k-1)})$, (2) for $k = 3$, $T = \Theta(2^n)$, a lower bound of $\Omega(\log \log n)$, (3) a generalization of the protocol to abelian groups, (4) lower bounds on the multiparty communication complexity of some regular languages, (5) lower bounds on branching programs, and (6) empirical results for the $k = 3$ case.

1 Introduction

Multiparty communication complexity was first defined by Chandra, Furst, and Lipton [8] and used to obtain lower bounds on branching programs. Since then it has been used to get additional lower bounds and tradeoffs for branching programs [1, 5], lower bounds on problems in data structures [5], time-space tradeoffs for restricted Turing machines [1], and unconditional pseudorandom generators for logspace [1].

Def 1.1 Let $f : \{\{0,1\}^n\}^k \to \{0,1\}$. Assume, for $1 \leq i \leq k$, P_i has all of the inputs *except* x_i. Let $d(f)$ be the total number of bits broadcast in the optimal deterministic protocol for f. This is called the *multiparty communication complexity* of f. The scenario is called the *forehead model.*

Note 1.2 Note that there is always the $n+1$-bit protocol of (1) P_1 broadcasts x_2, (2) P_2 computes and broadcasts $f(x_1, \ldots, x_k)$. The cases of interest are when $d(f) \ll n$.

The multiparty communication complexity of the following function was used by Chandra, Furst, and Lipton to obtain superlinear lower bounds on constant width branching programs (since improved by [2, 4, 18]).

[*] Temple University, Dept. of Computer and Information Sciences, 1805 N Broad St Fl 3, Philadelphia, PA 19122. professorB@gmail.com

[†] University of Maryland, Dept. of Computer Science and Institute for Advanced Computer Studies, College Park, MD 20742. gasarch@cs.umd.edu, Partially supported by NSF grant CCR-01-05413

[‡] Dept. of Computer Science, Loyola College in Maryland, 4501 N. Charles St, Baltimore, MD 21210. jglenn@cs.loyola.edu

Def 1.3 Let $k, n, T \in \mathbb{N}$. (T stands for Target.) We interpret elements of $\{0,1\}^n$ as numbers. Let $f_{k,T} : \{\{0,1\}^n\}^k \rightarrow \{0,1\}$ be defined as

$$f_{k,T}(x_1, \ldots, x_k) = \begin{cases} 1 & \text{if } \sum_{j=1}^{k} x_j = T; \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

We refer to $f_{k,T}$ as *the Exact-T problem.*

Chandra, Furst, and Lipton [8] (see also [14]) show that determining $d(f_{k,T})$ is equivalent to a problem in combinatorics. From this they obtained the following:

1. If $T = \Theta(2^n)$ then $d(f_{3,T}) = O(\sqrt{n})$.
2. For all k, for $T = \Theta(2^n)$, $d(f_{k,T})$ is not constant in n. The nonconstant function they obtained grew very slowly and had no name (e.g., it was not "inverse Ackerman").

This paper contains the following.

1. For $k \geq 4$ we generalize the upper bound to, when $T = \Theta(2^n)$, $d(f_{k,T}) \leq k + O(n^{1/(k-1)})$.
2. For $k = 3$, for $T = \Theta(2^n)$, we improve the lower bound to $d(f_{3,T}) \geq \Omega(\log \log n)$. The proof uses an interesting Ramsey-theoretic combinatorial lemma (Lemma 5.2).
3. We introduce a group-theoretic version of the Exact-T problem. This version is cleaner than the Exact-T problem and lower bounds on it yield lower bounds on Exact-T. We denote this problem $f_{k,T}^{\mathcal{G}}$ where $\mathcal{G}$ is a group. We show that
   (a) For all finite abelian groups $\mathcal{G}$ of size g, $d(f_{3,T}^{\mathcal{G}}) \geq \Omega(\log \log \log g)$.
   (b) For almost all finite abelian groups $\mathcal{G}$ there is a nontrivial protocol for $f_{k,T}^{\mathcal{G}}$.
   (c) $d(f_{k,T}^{\mathbb{Z}_m}) \leq k + O((\log m)^{1/(k-1)})$. ($\mathbb{Z}_m$ is $\{0, \ldots, m-1\}$ under mod arithmetic.)
4. We use the lower bound for $d(f_3^{\mathcal{G}})$ ($d(f_k^{\mathcal{G}})$) to obtain lower bounds of $\Omega(\log \log n)$ ($\omega(1)$) on multiparty communication complexity of several regular languages.
5. We use our results to obtain alternate proofs of known lower bounds on branching programs. Our results are weaker than what is known; however, the technique may be interesting.
6. We have some empirical results about 3-free sets that lead to concrete upper bounds on $d(f_{3,T})$ for $T = 2^n$.

Notation 1.4 If $T \in \mathbb{N}$ then $[T]$ denotes the set $\{1, \ldots, T\}$.

We will need the following notion of reduction.

Def 1.5 Let $f : \bigcup_{n=1}^{\infty} \{\{0,1\}^n\}^k \rightarrow \{0,1\}$ and $g : \bigcup_{n=1}^{\infty} \{\{0,1\}^n\}^k \rightarrow \{0,1\}$.

1. We say $f \leq_{\text{cc}}^{O(1)} g$ if there exists a protocol for f that has the following properties.

(a) The protocol may invoke a protocol for g once on an input of length $O(n)$.

(b) Before and after the invocation, the players may broadcast $O(1)$ bits.

(c) $f \equiv_{\text{cc}}^{O(1)} g$ if $f \leq_{\text{cc}}^{O(1)} g$ and $g \leq_{\text{cc}}^{O(1)} f$.

The following lemma is obvious.

Lemma 1.6

1. *$\leq_{\text{cc}}^{O(1)}$ is transitive.*
2. *If $f \leq_{\text{cc}}^{O(1)} g$ then $d(f) \leq d(g) + O(1)$.*

Note 1.7 The definition $\leq_{\text{cc}}^{O(1)}$ is not commonly used. The standard definition of a reduction in communication complexity allows polylog(n) instead of $O(1)$ extra bits. Usually in Communication Complexity n is big and $\log n$ is small. For our work, even $\log n$ is big. So we take $O(1)$ to be small.

2 Connections Between Multiparty Communication Complexity and Combinatorics

In this section we review the connections between the multiparty communication complexity of $f_{3,T}$ and combinatorics that was first established in [8]. We also review the upper and lower bounds that they obtained. We state a more detailed upper bound than they did which is useful for our empirical work in Section 10.

Def 2.1 Let $c, k, T \in \mathbb{N}$ with $k \geq 3$.

1. A *proper c-coloring of* $[T]^{k-1}$ is a function $C : [T]^{k-1} \to [c]$ such that there do not exist $x_1, \ldots, x_{k-1} \in [T]$ and $\lambda[T]$ with
   - For all i, $x_i + \lambda \in [T]$,
   - $C(x_1, x_2, x_3, \ldots, x_{k-1}) = C(x_1 + \lambda, x_2, x_3, \ldots, x_{k-1}) = \cdots = C(x_1, x_2, x_3, \ldots, x_{k-1} + \lambda)$ (Consider the case of $k = 3$, so we are coloring the plane. In a proper coloring there cannot be three vertices that (a) are the same color, and (b) are the corners of a right isosceles triangle with legs parallel to the axes and hypotenuse parallel to the line $y = -x$.)
2. Let $\chi_k(T)$ be the least c such that there is a proper c-coloring of $[T]^{k-1}$.

Theorem 2.2 *[8]*

1. *$d(f_{k,T}) \leq k - 1 + \lceil \lg(\chi_k(T) + 1) \rceil = k + \lg(\chi_k(T)) + O(1)$.*
2. *If $x_1, \ldots, x_k \in \{0, \ldots, T\}$ then $d(f_{k,T}) \geq \lg(\chi_k(\lfloor \frac{T}{k} \rfloor)) + \Omega(1)$.*

Chandra, Furst, and Lipton related their bounds to concepts in extremal combinatorics.

Def 2.3

1. A k-AP is an arithmetic progression of length k.
2. Let ζ_k^T be the minimum number of colors needed to color $\{1,\ldots,T\}$ such that there are no monochromatic k-AP's.
3. A set $A \subseteq [T]$ is *k-free* if there do not exist any k-AP's in A.
4. Let $\mathrm{r}_k(T)$ be the size of the largest k-free subset of $[T]$.

The next theorem states combinatorial facts that are needed for the upper and lower bounds, and then the bounds themselves.

Theorem 2.4 *[8]*

1. $\chi_k(T) \le \zeta_k^{kT}+1$.
2. $\zeta_k^T \le \frac{2T\ln(T)}{r_k(T)}$.
3. $\chi_k(T) \le \frac{2kT\ln(kT)}{\mathrm{r}_k(kT)} + 1 = O\big(\frac{kT\log(kT)}{\mathrm{r}_k(kT)}\big)$.
4. $d(f_{k,T}) \le k-1+\lg(\chi_k(T)) \le k-1+\left\lceil \lg\big(\frac{2kT\ln(kT)}{\mathrm{r}_k(kT)}\big)+1\right\rceil = k+O\big(\log\big(\frac{kT\log(kT)}{\mathrm{r}_k(kT)}\big)\big)$
5. *For all k, $\chi_k(2^n)$ is an increasing function of n.*
6. *If $T=\Theta(2^n)$ then $d(f_{k,T})=\omega(1)$.*

Chandra, Furst, and Lipton used the fact that there are 3-free sets of $[T]$ of size $T2^{-O(\log T)^{1/2}}$. (Due to [6], but see [16] for a constructive version and [10] for an exposition) to obtain the following.

Corollary 2.5 $d(f_{3,T}) \le O(\sqrt{\log T})$. *When $T=\Theta(2^n)$, $d(f_{3,T})=O(\sqrt{\log T})=O(\sqrt{n})$.*

3 New Upper Bounds

The following lemma yields large k-free sets. We will use these sets to obtain new explicit upper bounds for $\chi_k(T)$ when $k \ge 4$, which will in turn yield new explicit upper bounds on $d(f_{k,T})$. This lemma was first proven in [19] but see also [15].

Lemma 3.1 $\mathrm{r}_k(T) \ge T2^{-O((\log T)^{1/(k-1)})}$.

Theorem 3.2

1. $\chi_k(T) = 2^{O((\log(kT))^{1/(k-1)})}$.
2. $d(f_{k,T}) \le k + O((\log kT)^{1/(k-1)})$.
3. *If $T=\Theta(2^n)$ then $d(f_{k,T}) = k+O(n^{1/(k-1)})$.*

Proof:
1) Follows directly from Theorem 2.4.3 and Lemma 3.1.
2) Follows from Theorem 2.2 and part 1 of this theorem.
3) Follows from part 2 of this theorem. ▮

4 Group Theoretic Version

We define a group-theoretic version of the Exact-T problem. This version is cleaner than the Exact-T problem and lower bounds on it yield lower bounds on Exact-T. We obtain lower bounds in Section 5 which yield our main result: if $T = \Theta(2^n)$ then $d(f_{3,T}) = \Omega(\log\log n)$.

We define the problem on a group.

Def 4.1 Let $\mathcal{G} = (G, \odot)$ be a group. Let $T \in G$. Let $f^{\mathcal{G}}_{k,T} : G^k \to \{0,1\}$ be defined by

$$f^{\mathcal{G}}_{k,T}(x_1,\ldots,x_k) = \begin{cases} 1 & \text{if } \bigodot_{j=1}^{k} x_j = T; \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Def 4.2 Let $\mathcal{G} = (G, \odot)$ be a group. Let ID denote the identity element. Let $T \in G$. Let $c, k \in \mathbb{N}$.

1. An *$\mathcal{G}$-proper c-coloring of G^{k-1}* is a function $C : G^{k-1} \to [c]$ such that there does not exist $x_1, \ldots, x_{k-1} \in G$ and $\lambda \in G - \{ID\}$ with
   $C(x_1,\ldots,x_{k-1}) = C(x_1 \odot \lambda, x_2, x_3, \ldots, x_{k-1}) = \cdots = C(x_1, x_2, x_3, \ldots, x_{k-1} \odot \lambda)$.
2. If $\mathcal{M}$ is a finite group then let $\chi^*_k(\mathcal{G})$ be the least c such that there is an $\mathcal{G}$-proper c-coloring of G^{k-1}.

Theorem 4.3 *Let $\mathcal{G} = (G, \odot)$ be a group. Let $T_1, T_2 \in G$. Then $f^{\mathcal{G}}_{k,T_1} \equiv^{O(1)}_{\mathrm{cc}} f^{\mathcal{G}}_{k,T_2}$. Hence $d(f^{\mathcal{G}}_{k,T_1}) = d(f^{\mathcal{G}}_{k,T_2})$.*

Proof: We show $f^{\mathcal{G}}_{k,T_2} \le^{O(1)}_{\mathrm{cc}} f^{\mathcal{G}}_{k,T_1}$. Given $(x_1,\ldots,x_k)$ we map it to

$$(x_1,\ldots,x_{k-1}, x_k \odot T_2^{-1} \odot T_1).$$

Note that $x_1 \odot \cdots \odot x_k = T_2$ iff $x_1 \odot \cdots x_{k-1} \odot x_k \odot T_2^{-1} \odot T_1 = T_1$. ▮

Since $d(f^{\mathcal{G}}_{k,T}) = d(f^{\mathcal{G}}_{k,ID})$ we only study the case $T = ID$.

Def 4.4 Let $\mathcal{G} = (G, \odot)$ be a group. $f^{\mathcal{G}}_k$ is $f^{\mathcal{G}}_{k,ID}$ where ID is the identity element of $\mathcal{G}$.

The proof of the following theorem is a modification of a proof from [8].

Theorem 4.5 *Let $\mathcal{G} = (G, \odot)$ be a finite abelian group.*

1. $d(f^{\mathcal{G}}_k) \le k - 1 + \lceil \lg(\chi^*_k(\mathcal{G})) \rceil = k + \lg(\chi^*_k(\mathcal{G})) + O(1)$.
2. $d(f^{\mathcal{G}}_k) \ge \lg(\chi^*_k(\mathcal{G})) + \Omega(1)$.

Proof: 1) Let ID be the identity element of $\mathcal{G}$. Let C be a $\mathcal{G}$-proper c-coloring of G^{k-1} where $c = \chi^*_k(\mathcal{G})$. We represent elements of $[c]$ by bit strings. Hence we need $\lceil \lg(\chi^*_k(\mathcal{G})) \rceil$ bits. $P_1, P_2, \ldots, P_k$ will all know C ahead of time. The following protocol shows $d(f^{\mathcal{G}}_k) \le k - 1 + \lceil \lg(\chi^*_k(\mathcal{G})) \rceil$.

1. For $1 \le i \le k$ P_i has all x_j except x_i.

2. For $1 \le i \le k-1$ P_i calculates $x_i' = (x_1 \odot \cdots \odot x_{i-1} \odot x_{i+1} \odot \cdots \odot x_k)^{-1}$. Note that since $\mathcal{G}$ is a an abelian group x_i' exists and is the *unique* string such that

$$x_1 \odot \cdots \odot x_{i-1} \odot x_i' \odot x_{i+1} \odot \cdots \odot x_k = ID.$$

   For $1 \le i \le k-1$ let $\sigma^i = C(x_1, x_2, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_{k-1})$. Let $\sigma^k = C(x_1, x_2, \ldots, x_{k-1})$. Note that, for $1 \le i \le k$, P_i knows σ^i.

3. P_k broadcasts σ^k.

4. For $i = 1$ to $k-1$: If $\sigma^k = \sigma^i$ then P_i broadcasts 1, else P_i broadcasts 0. (Note that this takes $k-1$ bits total.)

5. If $P_1, \ldots, P_{k-1}$ all broadcast a 1 then $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 1$, otherwise $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 0$.

Claim 1: If $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 1$ then $P_1, \ldots, P_{k-1}$ will all broadcast 1.

Proof: If $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 1$ then, for all i, $x_i' = x_i$. (We are using that x_i' is unique and hence we are using that $\mathcal{G}$ is a group.) Hence $(\forall i, j)[\sigma^i = \sigma^j]$. Therefore $P_1, \ldots, P_{k-1}$ all broadcast 1.
End of proof of Claim 1.

Claim 2: If $P_1, \ldots, P_{k-1}$ all broadcast 1 then $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 1$.

Proof: Assume that $P_1, \ldots, P_{k-1}$ all broadcast 1. Then

$$C(x_1, x_2, \ldots, x_{k-1}) = C(x_1', x_2, x_3, \ldots, x_{k-1}) = \cdots = C(x_1, x_2, \ldots, x_{k-1}').$$

where

$$x_i' = (x_1 \odot \cdots \odot x_{i-1} \odot x_{i+1} \odot \cdots \odot x_k)^{-1}.$$

Let $\lambda = \bigodot_{i=1}^k x_i^{-1}$. Note that $x_i' = x_i \odot \lambda$. (We are using that $\mathcal{G}$ is abelian.) Hence

$$C(x_1, x_2, \ldots, x_{k-1}) = C(x_1 \odot \lambda, x_2, x_3, \ldots, x_{k-1}) = \cdots = C(x_1, x_2, \ldots, x_{k-1} \odot \lambda).$$

Since the coloring is proper we must have $\lambda = ID$ so $\bigodot_{i=1}^k x_i^{-1} = ID$. Since $\mathcal{G}$ is abelian we have $\bigodot_{i=1}^k x_i = ID$. Hence $f_k^{\mathcal{G}}(x_1, \ldots, x_k) = 1$.
End of proof of Claim 2.

2) Let P be a protocol for $f_k^{\mathcal{G}}$. We use this protocol to create a $\mathcal{G}$-proper coloring of G^{k-1}.

We define $C(x_1, \ldots, x_{k-1})$ as follows. First find x such that $(\bigodot_{i=1}^{k-1} x_i) \odot x = ID$. Then run the protocol on $(x_1, \ldots, x_{k-1}, x)$. The color is the transcript produced.

Claim 3: C is a $\mathcal{G}$-proper coloring.
Proof: Assume there exists $\lambda \ne ID$ such that

$$C(x_1, x_2, \ldots, x_{k-1}) = C(x_1 \odot \lambda, x_2, x_3, \ldots, x_{k-1}) = C(x_1, x_2, \ldots, x_{k-1} \odot \lambda).$$

We denote this value $TRAN$ (for Transcript).

Let x be such that $(\bigodot_{i=1}^{k-1} x_i) \odot x = ID$. Let y be such that $\lambda \odot (\bigodot_{i=1}^{k-1} x_i) \odot y = ID$. By the definition of C (and using that $\mathcal{G}$ is abelian) the following inputs produce the transcript $TRAN$.

- $(x_1, \ldots, x_{k-1}, x)$,
- $(x_1 \odot \lambda, \ldots, x_{k-1}, y)$,
- $(x_1, x_2 \odot \lambda, \ldots, x_{k-1}, y)$,
- $\vdots$
- $(x_1, x_2, \ldots, x_{k-1} \odot \lambda, y)$.

By a standard result in communication complexity, this implies that $(x_1, \ldots, x_{k-1}, y)$ also produces $TRAN$. But $f_k^{\mathcal{G}}(x_1, \ldots, x_{k-1}, x) = 1$ and $f_k^{\mathcal{G}}(x_1, x_2, \ldots, x_{k-1}, y) = 0$. This is a contradiction.
End of Proof of Claim 3 ▮

Note 4.6 In the group case we just obtained $d(f_k^{\mathcal{G}}) \geq \lg(\chi_k^*(\mathcal{G})) + \Omega(1)$. In the original case Chandra, Furst, and Lipton obtained $d(f_{k,T}) \geq \lg(\chi_k(\lfloor \frac{T}{k} \rfloor)) + \Omega(1)$. The reason they had a factor of $\frac{1}{k}$ and we do not comes from the fact that, in the group case, for any $x_1, \ldots, x_{k-1} \in G$ there is an $x \in G$ such that $f_k^{\mathcal{G}}(x_1, \ldots, x_{k-1}, x) = 1$; by contrast, there are $x_1, \ldots, x_{k-1} \in [T]$ such that, for all $x \in [T]$, $f_{k,T}(x_1, \ldots, x_{k-1}, x) = 0$.

The next lemma shows a relation between $d(f_k^{\mathcal{G}})$ and $d(f_{k,T})$ that we will use to obtain bounds on one from bounds on the other.

Def 4.7 $\mathbb{Z}_T$ is the group with set $\{0, 1 \ldots, T-1\}$ under modular addition.

Lemma 4.8 *Let $T \in \mathbb{N}$ and $k \geq 3$. Then the following hold.*

1. *For all $a, b \in \mathbb{N}$, $a \leq b$, $d(f_{k,aT}) \leq d(f_{k,bT})$ (easy proof omitted).*
2. *$\chi_k(T) \leq \chi_k^*(\mathbb{Z}_T)$.*
3. *$d(f_{k,T}) \leq k + d(f_k^{\mathbb{Z}_T}) + O(1)$.*
4. *$d(f_k^{\mathbb{Z}_T}) \leq kd(f_{k,kT}) + O(1)$.*

Proof:
2) Let C be a proper $\mathbb{Z}_T$-coloring of $\mathbb{Z}_T^{k-1}$. It is easy to see that C is also a proper coloring of $[T]^{k-1}$. Hence $\chi_k(T) \leq \chi_k^*(\mathbb{Z}_T)$.

3) By Theorem 2.2.1, part 2 of this lemma, and Theorem 4.5.2 we obtain

$$d(f_{k,T}) \le k + \lg(\chi_k(T)) + O(1) \le k + \lg(\chi_k^*(\mathbb{Z}_T)) + O(1) \le k + d(f_k^{\mathbb{Z}_T}) + O(1).$$

4) It is easy to see that

$$f_k^{\mathbb{Z}_T}(x_1, \ldots, x_k) = 1 \text{ iff } (\bigvee_{i=1}^{k} f_{k,iT}(x_1, \ldots, x_k) = 1) \vee (\forall i)[x_i = 0].$$

Hence

$$d(f_k^{\mathcal{G}}) \le (\sum_{i=1}^{k} d(f_{k,iT})) + O(1) \le kd(f_{k,kT}) + O(1).$$

(We use part (1) for second inequality.) ▮

5 Lower Bounds

5.1 An $\omega(1)$ Lower Bound for $d(f_k^{\mathbb{Z}_T})$

Theorem 5.1 *Let $T = \Theta(2^n)$. $d(f_k^{\mathbb{Z}_T}) \ge \omega(1)$ ($d(f_k^{\mathbb{Z}_T})$ is nonconstant in T).*

Proof: By Lemma 4.8.3 $d(f_k^{\mathbb{Z}_T}) \ge d(f_{k,T}) - k$. By Theorem 2.4, $d(f_{k,T}) \ge \omega(1)$. Hence $d(f_k^{\mathbb{Z}_T}) \ge \omega(1)$. ▮

5.2 An $\Omega(\log\log\log g)$ Lower Bound for $d(f_3^{\mathbb{Z}_T})$ and $d(f_{3,T})$

The following combinatorial lemma will allow us to prove a lower bound on $d(f_3^{\mathcal{G}})$ for a variety of $\mathcal{G}$. This lemma is a reworking of a theorem of Graham and Solymosi [12].

Lemma 5.2 *There exist absolute constants g_0, d_0 such that the following is true. Let $\mathcal{G} = (G, \odot)$ be any finite abelian group and let $g = |G|$. If $g \ge g_0$ and $c \le d_0 \log\log g$ then there are no $\mathcal{G}$-proper c-colorings of $G \times G$. Hence $\chi_3^*(\mathcal{G}) \ge \Omega(\log\log g)$.*

Proof: Assume that C is a $\mathcal{G}$-proper c-coloring of $G \times G$. We will find sets $X_1, Y_1 \subseteq G$ such that C restricted to $X_1 \times Y_1$ uses $c - 1$ colors. We will iterate this process to obtain X_c, Y_c such that C restricted to $X_c \times Y_c$ uses 0 colors. Hence $|X_c| = 0$ which will yield $c = \Omega(\log\log g)$.

Let $X_0 = G$, $Y_0 = G$, $h_0 = |X_0| = |Y_0| = g$, $COL_0 = [c]$. At stage s the subset will be $X_s \times Y_s$, the size of X_s will be $h_s = |X_s| = |Y_s|$, and COL_s will be the colors used by $X_s \times Y_s$.

Assume X_s, Y_s, h_s are defined and inductively $COL_s = [c-s]$ (we will be renumbering to achieve this). Partition $X_s \times Y_s$ into sets P_a indexed by $a \in G$ defined by

$$P_a = \{(x, y) \in X_s \times Y_s \mid x \odot y = a\}.$$

(Think of P_a as the ath anti-diagonal.) There exists an a such that $|P_a| \ge \lceil h_s^2/g \rceil$. There exists a color, which we will take to be $c - s$ by renumbering, such that at least $\lceil \lceil h_s^2/g \rceil / c \rceil$ of the elements of P_a are colored $c - s$. (We could use $c - s$ in the denominator but we do not need to.) Let

$m = \lceil \lceil h_s^2/g \rceil /c \rceil$. Let $\{(x_1, y_1), \ldots, (x_m, y_m)\}$ be m elements of P_a such that, for $1 \le i \le m$, $C(x_i, y_i) = c - s$.

Claim 1: For all $i \ne j$, $x_i \ne x_j$ and $y_i \ne y_j$.

Proof: If $x_i = x_j$ then

$$x_j \odot y_j = a = x_i \odot y_i = x_j \odot y_i.$$

Hence $y_j = y_i$. Therefore $(x_i, y_i) = (x_j, y_j)$. This contradicts P_a having m distinct points.

The proof that $y_i \ne y_j$ is similar.

End of Proof of Claim 1

Claim 2: For all $i \ne j$, $C(x_i, y_j) \ne c - s$.

Proof: Assume, by way of contradiction, that $C(x_i, y_j) = c - s$. Note that

$$C(x_i, y_j) = C(x_i, y_i) = C(x_j, y_j) = c - s.$$

We want a $\lambda \ne ID$ such that $y_i = y_j \odot \lambda$ and $x_j = x_i \odot \lambda$. Using that $x_i \odot y_i = x_j \odot y_j = a$ we can take $\lambda = (a^{-1} \odot x_j \odot y_i)$. The element $\lambda \ne ID$: if $\lambda = ID$ then one can show $y_i = y_j$, which contradicts Claim 1.

We now have

$$C(x_i, y_j) = C(x_i \odot \lambda, y_j) = C(x_i, y_j \odot \lambda).$$

This violates C being a proper coloring.

End of Proof of Claim 2

Let

$$\begin{aligned} h_{s+1} =&\ m' = \lceil m/3 \rceil \\ X_{s+1} =&\ \{x_1, x_2, \ldots, x_{m'}\} \\ Y_{s+1} =&\ \{y_{m+1-m'}, \ldots, y_m\} \\ COL_{s+1} =&\ [c - (s+1)] \end{aligned}$$

Note that, by Claim 2 above

$$\{C(x, y) \mid x \in X_{s+1}, y \in Y_{s+1}\} \subseteq COL_{s+1}.$$

We iterate the process c times to obtain X_c, Y_c with $|X_c| = |Y_c| = h_c$ such that COL restricted to $X_c \times Y_c$ uses 0 colors. The only way this is possible is if $h_c = 0$. This will yield $c = \Omega(\log \log g)$.

We have $h_0 = g$ and

$$h_{s+1} = \left\lceil \left\lceil \left\lceil \frac{h_s^2}{g} \right\rceil /c \right\rceil /3 \right\rceil \ge \frac{h_s^2}{3cg}.$$

We show that for $s \in \mathbb{N}$, $h_s \ge \frac{g}{(3c)^{2^s - 1}}$.

Claim 3: $(\forall s)[h_s \ge \frac{g}{(3c)^{2^s-1}}]$.

Base Case: $h_0 = g \ge \frac{g}{(3c)^0} = g$.

Induction Step: Assume $h_s \ge \frac{g}{(3c)^{2^s-1}}$. Since $h_{s+1} \ge (h_s)^2/3cg$ we have, by the induction hypothesis

$$h_{s+1} \geq (h_s)^2/3cg \geq \frac{\frac{g^2}{(3c)^{2^{s+1}-2}}}{3cg} \geq \frac{g}{(3c)^{2^{s+1}-1}}.$$

End of proof of Claim 3

Taking $s = c$ we obtain $h_c \geq \frac{g}{(3c)^{2^c-1}}$. Hence there is a set of h_c^2 points that are 0-colored. Therefore $h_c < 1$. This yields $c = \Omega(\log\log g)$. ▮

The following is a variant of a statement that Solymosi claims “Analysts believe”[22].

BILL- MOVE CONJ TO OPEN PROBLEM SECTION. DELETE ALL THOSE ‘IF CONJ HOLDS...’ RESULTS.

Conjecture 5.3 *There is a function $c : \mathbb{N} \to \mathbb{N}$ such that, for all $k \geq 3$, $\chi^*_k(\mathcal{G}) \geq \Omega(c(k)\log\log g)$.*

Theorem 5.4 *Let $\mathcal{G}$ be any finite abelian group. Let $|G| = g$.*

1. *$d(f_3^{\mathcal{G}}) \geq \Omega(\log\log\log g)$. Note that $\log g$ is the length of all the players inputs, so this should be considered an $\Omega(\log\log n)$ bound.*

2. *Assume Conjecture 5.3 holds. There exists $c : \mathbb{N} \to \mathbb{N}$ such that, for all k, $d(f_k^{\mathcal{G}}) \geq \Omega(c(k)\log\log\log g)$.*

Proof:
1) By Lemma 5.2 $\chi^*_3(\mathcal{G}) \geq \Omega(\log\log g)$. By Theorem 4.5, $d(f_3^{\mathcal{G}}) \geq \lg(\chi^*_3(\mathcal{G})) \geq \Omega(\log\log\log g)$.

2) If Conjecture 5.3 is true then there exists $c : \mathbb{N} \to \mathbb{N}$ such that $\chi^*_k(\mathcal{G}) \geq \Omega(c(k)\log\log g)$. By Theorem 4.5, $d(f_k^{\mathcal{G}}) \geq \lg(\chi^*_k(\mathcal{G})) \geq \Omega(c(k)\log\log\log g)$. ▮

Theorem 5.5 *Let $T \in \mathbb{N}$.*

1. *$d(f_{3,T}) \geq \Omega(\log\log\log T)$. If $T = \Theta(2^n)$ then $d(f_{3,T}) \geq \Omega(\log\log n)$.*

2. *Assume Conjecture 5.3 holds. There exists $c' : \mathbb{N} \to \mathbb{N}$ such that, for all k, $d(f_{k,T}) \geq \Omega(c'(k)\log\log\log T)$. If $T = \Theta(2^n)$ then $d(f_{k,T}) \geq \Omega(c'(k)\log\log n)$.*

Proof:
1) We assume 3 divides T. The general case is similar. Let $T = 3T'$. By Lemma 4.8.3 $d(f_{3,3T'}) \geq \Omega(d(f_3^{\mathbb{Z}_{T'}}))$. By Theorem 5.4 $d(f_3^{\mathbb{Z}_{T'}}) \geq \Omega(\log\log\log T') = \Omega(\log\log\log T)$.

2) We assume k divides T. The general case is similar. Let $T = kT'$. By Lemma 4.8.3 $d(f_{k,kT'}) \geq \Omega(d(f_k^{\mathbb{Z}_{T'}})/k)$. Assuming the conjecture, by Theorem 5.5, there exists a function $c(k)$ such that $d(f_k^{\mathbb{Z}_{T'}}) \geq \Omega(c(k)\log\log\log T/k)$. Hence there is another function which we call $c'(k)$ such that $d(f_k^{\mathbb{Z}_{T'}}) \geq \Omega(c'(k)\log\log\log T)$. ▮

5.3 An $\omega(1)$ Lower Bound for General $\mathcal{G}$ and k

Def 5.6 Fix k. The phrase $d(f_k^{\mathcal{G}}) = \omega(1)$ means that, for all constants d, there exists g_0, such that for all finite abelian groups G of size $g \geq g_0$, $d(f_k^{\mathcal{G}}) \geq d$.

Def 5.7 $\mathrm{PART}_{m,k} : \{\{0,1\}^m\}^k \rightarrow \{0,1\}$ is the following function. Interpret the input as k subsets of $\{1,\ldots,m\}$. Output 1 if these sets form a partition of $\{1,\ldots,m\}$, and 0 otherwise.

Tesson [23, 24] proved the following. He used the Hales-Jewitt Theorem (see [11]) which is why the bound is $\omega(1)$ instead of something more concrete. We use this lemma to obtain $d(f_k^{\mathcal{G}}) = \omega(1)$.

Lemma 5.8 *For all k, $d(\mathrm{PART}_{m,k}) \geq \omega(1)$.*

Lemma 5.9 *Let $k \geq 3$. Let $h_1,\ldots,h_m \geq 2$. Let $\mathcal{G} = \mathbb{Z}_{h_1} \times \cdots \times \mathbb{Z}_{h_m}$ For all k, $d(\mathrm{PART}_{m,k}) \leq d(f_k^{\mathcal{G}}) + O(1)$.*

Proof: We show that $\mathrm{PART}_{m,k} \leq_{\mathrm{cc}}^{O(1)} f_k^{\mathcal{G}}$ and then use Lemma 1.6.

1. Input $(x_1,\ldots,x_k)$. Think of each x_i as a subset of $\{1,\ldots,m\}$ which we denote by X_i.

2. Player k broadcasts 0 if

$$(\exists i_1, i_2 \in \{1,\ldots,k-1\})(\exists j \in \{1,\ldots,m\})[j \in X_{i_1} \cap X_{i_2}].$$

and a 1 otherwise. If he broadcasts a 0 then the protocol stops because everyone knows the answer is 0.

3. Player $k-1$ broadcasts 0 if

$$(\exists i_1, i_2 \in \{1,\ldots,k-2,k\})(\exists j \in \{1,\ldots,m\})[j \in X_{i_1} \cap X_{i_2}].$$

and a 1 otherwise. If he broadcasts a 0 then the protocol stops because everyone knows the answer is 0.

4. Player $k-2$ broadcasts 0 if

$$(\exists i_1, i_2 \in \{1,\ldots,k-3,k-1,k\})(\exists j \in \{1,\ldots,m\})[j \in X_{i_1} \cap X_{i_2}].$$

and a 1 otherwise. If he broadcasts a 0 then the protocol stops because everyone knows the answer is 0.

5. The players now view the input $(X_1,\ldots,X_k)$ as being k elements of $Z_{h_1} \times \cdots \times Z_{h_m}$ where all of the coordinates are 0 or 1. If the protocol got to this point then, for every $j \in \{1,\ldots,m\}$ there is at most one i such that the jth coordinate of the ith input is 1. The original X_i form a partition iff these elements add up to $(1,\ldots,1)$ (there are n 1's). Hence $\mathrm{PART}_{m,k}(x_1,\ldots,x_k) = f_{k,1^n}^{\mathcal{G}}(x_1,\ldots,x_k)$ (Recall from Definition 4.1 that $f_{k,1^n}^{\mathcal{G}}(x_1,\ldots,x_k)$ asks if $x_1 \odot \cdots \odot x_k = 1^n$.) By Theorem 4.3 $f_{k,1^n}^{\mathcal{G}}$ can be transformed to an instance of $f_k^{\mathcal{G}}$ with no increase in communication. The players do the transformation and then run the protocol for $f_k^{\mathcal{G}}$.

▮

Lemma 5.10 *If $\mathcal{G}_1$ and $\mathcal{G}_2$ are groups, $k \ge 3$, $d(f_k^{\mathcal{G}_1}) \le d(f_k^{\mathcal{G}_1 \times \mathcal{G}_2})$.*

Proof: Let ID_1 be the identity in $\mathcal{G}_1$ and ID_2 be the identity in $\mathcal{G}_2$. Note that if $x_1, \ldots, x_k \in G_1$ then

$\prod_{i=1}^{k} x_i = ID_1$ iff $\prod_{i=1}^{k}(x_i, ID_2) = (ID_1, ID_2)$, where the first product is in $\mathcal{G}_1$ and the second product is in $\mathcal{G}_2$.

Hence $f_k^{\mathcal{G}_1} \le_{\text{cc}}^{O(1)} f_k^{\mathcal{G}_1 \times \mathcal{G}_2}$. ▮

Theorem 5.11 *For all d, k there exists g_0 such that for all finite abelian groups $\mathcal{G}$, $|G| \ge g_0$, $d(f_k^{\mathcal{G}}) \ge d$. In short, the bigger the group, the larger $d(f_k^{\mathcal{G}})$, without bound.*

Proof: Fix d, k. We define g_0 such that, for all finite abelian groups $\mathcal{G}$ such that $|G| \ge g_0$, $d(f_k^{\mathcal{G}}) \ge d$. We define m_0 first and then g_0. The theorem demands a value of g_0, the proof demands a value of m_0.

- Let m_0 be such that, for all $m \ge m_0$, $\text{PART}_{m,k} > d + d'$ where d' will be named later. Such an m_0 exists by Lemma 5.8.
- Let g_0 be such that, for all $g \ge g_0$, if $\mathcal{G} = \mathbb{Z}_{g^{1/m_0}}$ then $d(f_k^{\mathcal{G}}) \ge d$. Such a g_0 exists by Theorem 5.1.

Let $\mathcal{G}$ be a finite abelian group of size $g \ge g_0$. By the classification of finite abelian groups $\mathcal{G} = \mathbb{Z}_{h_1} \times \cdots \times \mathbb{Z}_{h_m}$ for some factorization $g = \prod_{i=1}^{m} h_i$.

There are two cases. They depend on m.

Case 1: $m \ge m_0$. By the definition of m_0,

$$d(\text{PART}_{m,k}) > d + d'.$$

By Lemma 5.9

$$d(f_k^{\mathcal{G}}) + O(1) \ge d(\text{PART}_{m,k}).$$

Hence

$$d(f_k^{\mathcal{G}}) \ge d + d' - \Omega(1).$$

Let d' be such that d' is greater than the constant in the $\Omega(1)$. Hence $d(f_k^{\mathcal{G}}) \ge d$.

Case 2: $m \le m_0$. By Lemma 5.10 $d(f_k^{\mathcal{G}}) \ge \max_{1 \le i \le m} d(f_k^{\mathcal{G}_i})$ where $\mathcal{G}_i = \mathbb{Z}_{h_i}$. Since $\prod_{i=1}^{m} h_i = g$ and $m \le m_0$, there exists h_i such that $h_i \ge g^{1/m} \ge g^{1/m_0}$. Hence, by Lemma 5.10, $d(f_k^{\mathcal{G}}) \ge d(f_k^{\mathcal{G}_i})$ where $\mathcal{G}_i = \mathbb{Z}_{h_i}$. By the choice of g_0 we have $d(f_k^{\mathcal{G}}) \ge d(f_k^{\mathcal{G}_i}) \ge d$. ▮

5.4 Lack of Lower Bounds on Monoids

Our lower bounds on $d(f_k^{\mathcal{G}})$ used that $\mathcal{G}$ is a group. One can define $f_k^{\mathcal{M}}$ for $\mathcal{M}$ a monoid. The next theorem shows that the lower bound in Theorems 4.5.2 and 5.11 would not hold.

Theorem 5.12 *Let $\mathcal{M} = (\{0,1\}^n, \wedge)$ where $\wedge$ is bitwise AND. Let $T = 1^n$. Then $d(f_{k,T}^{\mathcal{G}}) = 2$.*

Proof: The protocol is as follows

1. Player P_1 broadcasts 1 if $x_2 = x_3 = \cdots = x_k = 1^n$ and 0 otherwise.
2. Player P_2 broadcasts 1 if $x_1 = 1^n$.
3. The answer is 1 iff both P_1 and P_2 broadcast 1.

▮

6 Applications to the Multiparty Communication Complexity of Regular Languages

In this section we use Theorems 5.4 and Theorem 5.11 to obtain lower bounds on the multiparty communication complexity of many regular languages.

The 2-party communication complexity of regular languages has been defined and solved completely [20, 26, 25]. The multiparty communication complexity of regular languages (defined initially in [20]) still has many open problems. The standard problem in this field is as follows.

Def 6.1 Let L be a regular language and k be the number of players. $R_{k,L}$ is the following problem.

1. Let $x = a_1 a_2 \cdots a_{kn}$ be a string such that $(\forall i)[a_i \in \Sigma \cup \{\epsilon\}]$.
2. Player P_i gets all a_j such that $j \not\equiv i \pmod{k}$.
3. The players want to determine if $a_1 a_2 \cdots a_{kn} \in L$.

Notation 6.2 The multiparty communication complexity of $R_{k,L}$ is denoted $d(R_{k,L})$.

Notation 6.3 Let $\sigma \in \Sigma$, $m \in \mathbb{N}$, and $r \in \mathbb{N}$ such that $0 \le r \le m-1$.

1. $\#_\sigma(w)$ is the number of occurences of σ in w.
2. $L_{\sigma,r,m} = \{w \mid \#_\sigma(w) \equiv r \mod m\}$.

Lemma 6.4 *Let $k, r, m \in \mathbb{N}$ such that $0 \le r \le m-1$. Let $|\Sigma| \ge 2$ and $\sigma \in \Sigma$ and $L = L_{\sigma,r,m}$. Then $f_k^{\mathbb{Z}_m} \le_{\rm cc}^{O(1)} R_{k,L}$.*

Proof: We show $f_{k,r}^{\mathbb{Z}_m} \leq_{\text{cc}}^{O(1)} R_{k,L}$. By Theorem 4.3 $f_k^{\mathbb{Z}_m} \equiv_{\text{cc}}^{O(1)} f_k^{\mathbb{Z}_m}$, hence we will have $f_k^{\mathbb{Z}_m} \leq_{\text{cc}}^{O(1)} R_{k,L}$.

We map $(q_1, \ldots, q_k)$ to a string w of length km such that $f_{k,r}^{\mathbb{Z}_m}(q_1, \ldots, q_k) = 1$ iff $\#_\sigma(w) \equiv r \mod m$.

For each i, $1 \leq i \leq k$, there are m positions in w that are $\equiv i \pmod k$. Set q_i of those positions to σ, and the rest of them to a letter that is not σ.

If w is the resulting word then $\#_\sigma(w) = \sum_{i=1}^{k} q_i$. Hence $q_1 + \cdots + q_k \equiv r \pmod m$ iff $w \in L$. ▮

Theorem 6.5 *Let $k, r, m \in \mathbb{N}$ such that $0 \leq r \leq m-1$. Let $|\Sigma| \geq 2$ and $\sigma \in \Sigma$. Let $L = L_{\sigma,r,m}$.*

1. *$d(R_{3,L}) \geq \Omega(\log\log\log m)$.*
2. *For all $k \geq 4$, $d(R_{k,L}) = \omega(1)$.*
3. *Assume Conjecture 5.3 is true. Then there exists a function c such that, for all $k \geq 4$, $d(R_{k,L}) \geq \Omega(c(k) \log\log\log m)$.*
4. *$d(R_{k,L}) \leq O(\log m)$.*

Proof: By Lemma 6.4 $d(f_k^{\mathcal{G}}) \leq d(R_{k,L})$.
1) By Theorem 5.4 $d(f_3^{\mathcal{G}}) = \omega(\log\log\log m)$. Hence $d(R_{3,L}) = \omega(\log\log\log m)$.
2) By Theorem 5.11 $d(f_3^{\mathcal{G}}) = \omega(1)$. Hence $d(R_{k,L}) = \omega(1)$.
3) If Conjecture 5.3 holds then, by Theorem 5.4, there exists a function c such that $d(f_k^{\mathcal{G}}) \geq \Omega(c(k) \log\log m) = \Omega(c(k) \log\log\log m)$. Hence $d(R_{k,L}) = \Omega(c(k) \log\log\log m)$.
4) The following protocol establishes the upper bound: Player k broadcasts the number of σ's he sees, mod m. Player $k-1$ broadcasts the number of σ's on Player k's forehead, mod m. Now everyone knows the number of σ mod m. ▮

7 Applications to Lower Bounds on Branching Programs

7.1 Lower Bounds for MAJ_m and MOD_m

Branching programs are a model of computation that are like decision trees except that nodes can be gotten to by several paths; hence they are 'skinny decision trees'. If a function $h : \{0,1\}^m \to \{0,1\}$ is computed by a branching program the key questions to ask are (1) what is its length? and (2) what is its width? It is somewhat surprising that all sets in NC^1 can be decided with poly-length, width 5, branching programs [3]. See [3, 27] or a paper on Branching Programs for a formal definition.

The function MAJ_m defined below has been of particular interest.

Def 7.1 Let $\text{MAJ}_m : \{0,1\}^m \to \{0,1\}$ be the function

$$\text{MAJ}_m(x_1, \ldots, x_m) = \begin{cases} 1 & \text{if } \sum_{i=1}^{m} x_i \geq m/2; \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

We will also look at the function MOD_m.

Def 7.2 Let $\mathrm{MOD}_m : \{0,1\}^m \rightarrow \{0,1\}$ be the function

$$\mathrm{MOD}_m(x_1,\ldots,x_m) = \begin{cases} 1 & \text{if } \sum_{i=1}^{m} x_i \equiv 0 \pmod{m}; \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

The following Theorem is from [2, 18].
BILL- CHECK THIS, IT LOOKS WRONG.

Theorem 7.3 *Any branching program for* MAJ_m *must have length at least* $\Omega(m \log m/(\log\log m))$. *Note that this is independent of the width.*

Their proof uses a *difficult* reduction to the 2-player communication complexity of $\mathrm{MAJ}_{\alpha m}$, which had an *easy-to-prove* lower bound. We obtain alternative proofs of weaker results. Our lower bound on MAJ_m uses an *easy-to-prove* reduction to the 3-player communication complexity of $\mathrm{MAJ}_{\alpha m}$, which has a *difficult* lower bound (this paper's Theorem 5.4).

We state the known upper bounds for comparison.

Theorem 7.4

1. *For every m there is a branching program for* MAJ_m *of length*

$$O(m(\log m)^3/((\log\log m)(\log\log\log m)))$$

and width $O(\log m)$.

2. *There is a function w such that, for every $\delta > 0$, there is a BP for* MAJ_m *of width $w(\delta)$ and length $O(n^{4.95+\delta})$. Note that there is a constant width BP for* MAJ_m *of length $O(n^5)$.*

Proof:
1) This is from [21].
2) By [17] there is a bounded fan-in circuit for MAJ_m that has $O(n)$ size and depth $4.95 \log n + O(1)$. By [9] any circuit of bounded fan-in, poly size, and depth $d \log n$ can be simulated by a Branching Program of constant width, and length $n^{d(1+\epsilon)}$. The larger w is the smaller ϵ is. Hence there is a Branching Program for MAJ_m with constant width, and length $n^{4.95+\delta}$. ▮

The following (easy) lemma can be proven by techniques similar to those of Lemma 5.1 and Theorem 5.2 from [8].

Lemma 7.5 *Let $m \in \mathbb{N}$, $\alpha < 1$, and $k \geq 3$. Let $g(x_1,\ldots,x_m) : \{0,1\}^m \rightarrow \{0,1\}$. Assume g can be computed by a branching program of length L and width w. Let $k = \lfloor L/(\alpha m) \rfloor$, $n = \lceil (0.5) \lg m \rceil$, and $T = \lceil (\sqrt{m})/2) \rceil$.*

- *If $g = \mathrm{MAJ}_m$ then $d(f_{k,T}) \leq O(k \log w)$.*

- *If $g = \mathrm{MOD}_m$ then $d(f_k^{\mathbb{Z}_m}) \leq O(k \log w)$.*

Theorem 7.6 *Let $\epsilon > 0$.*

1. *If there is a length $(3-\epsilon)m$, width w BP for MAJ_m (MOD_m) then $w \geq \log\log m$.*
2. *Assume Conjecture 5.3 is true. Then there exists a function $d : \mathbb{N} \to \mathbb{N}$ such that if there is a length am, width w BP for MAJ_m (MOD_m) then $w \geq \Omega(d(a)\log\log m)$.*

Proof: We assume throughout that m is a power of 2 and a square (the proof in the general case is similar). We proof the theorem for MAJ_m. The proof for MOD_m is similar.
1) Assume there is a length $L = (3-\epsilon)m$, width w BP for MAJ_m. By Lemma 7.5 with $\alpha = \frac{3-\epsilon}{3} < 1$, we obtain $d(f_{3,T}) \leq O(\log w)$ (with $n = (0.5)\log m$ and $T = (\sqrt{m})/2$). By Theorem 5.5.1

$$d(f_{3,T}) \geq \Omega(\log\log\log T) = \Omega(\log\log\log m).$$

Hence $\log\log\log m \leq O(\log w)$, so $w \geq \Omega(\log\log m)$.

2) Assume there is a length $L = am$, width w, BP for MAJ_m. By Lemma 7.5 with $\alpha = \frac{a}{a-1} < 1$ we obtain $d(f_{k,T}) \leq O(k\log w)$ where $k = a-1$, $n = (0.5)\lg m$, and $T = (\sqrt{m})/2$. By Theorem 5.5.2, assuming the conjecture, $d(f_{k,T}) \geq \Omega(c(k)\log\log\log T) = \Omega(c(k)\log\log\log m)$. Hence $c(k)\log\log\log m \leq O(\log w)$, so $w \geq \Omega((\log\log m)/c(k))$. Let $d(a) = 1/c(k-1) = 1/c(a-2)$. ▌

7.2 Lower Bounds for f^*

Babai, Nisan and Szegedy [1] have proven a theorem that enables one to go from lower bounds for $d(f)$ to lower bounds for oblivious branching programs for f^* where f^* is related to f (see definition below). An oblivious branching program is one where the questions asked do not depend on previous answers.

Def 7.7 Let $f : (\{0,1\}^n)^k \to \{0,1\}$. Let $c \in \mathbb{N}$ be any natural number (it may depend on n or k). Then f^*_c is defined as follows

- *Input:* k strings over the ternary alphabet $\{00, 11, 01\}$ of length $2n3^m$ (so there are $2n3^m$ symbols, each one is 2 bits long). Note that the total input size is $4nk3^m$ bits. We denote these strings by $X_1, \ldots, X_k$.
- *Output:* For $1 \leq i \leq k$ let $x_i \in \{0,1\}^*$ be obtained by removing the letters 01 from X_i, and then replacing the letters 00 with 0 and the letters 11 with 1. If any of the x_i are not in $\{0,1\}^n$, then output 0. If all of the x_i are in $\{0,1\}^n$ then output $f(x_1, \ldots, x_k)$.

Theorem 7.8 *[1] Let $f : (\{0,1\}^n)^k \to \{0,1\}$. Let $c \in \mathbb{N}$ be a parameter. If there is an oblivous branching program for f^*_c with length $L = O(kn3^c)$ then it has width $W \geq 2^{d(f)/kc}$. (Recall that $d(f)$ is the multiparty communication complexity of f.)*

Corollary 7.9 *Let $f = f_{3,T}$ where $T = \Theta(2^n)$ or $f = f_k^{\mathbb{Z}_{2^n}}$. Let $c \in \mathbb{N}$. If there is a branching program for f^*_c of length $L = O(3^c n)$ then it must have width $W = (\log n)^{\Omega(1/c)}$.*

Proof: This follows from Theorem 7.8, 5.4 and 5.5. ▌

8 Upper Bounds

8.1 Upper Bounds for $\mathcal{G} = \mathbb{Z}_m$

The proofs in this section are a reworking of those in [8].

Notation 8.1 If $\mathcal{M} = (M, \odot)$ is a monoid and $d \in M$, $k \in \mathbb{N}$, then d^k means $d \odot \cdots \odot d$ where there are k d's.

Def 8.2 Let $\mathcal{M} = (M, \odot)$ be a monoid. Let $T = |M|$.

1. A k-AP$^{\mathcal{M}}$ is a multiset of the form $\{a, a \odot d, a \odot d^2, \ldots, a \odot d^{k-1}\}$ where $a, d \in M$.
2. Let $\zeta_k^{\mathcal{M}}$ be the minimum number of colors needed to color M such that there are no monochromatic k-AP$^{\mathcal{M}}$'s.
3. A set $A \subseteq M$ is *k-free* if there do not exist any k-AP$^{\mathcal{M}}$'s in A.
4. Let $\mathrm{r}_k(\mathcal{M})$ be the size of the largest k-free subset of M.

The following lemma is proven for all finite commutative monoids. We will only be using it for finite abelian groups; however, this generalization is no harder to prove and may be useful at some later time.

Lemma 8.3 *Let $\mathcal{M} = (M, \odot)$ be a finite commutative monoid. Let $T = |M|$.*

1. $\chi_k^*(\mathcal{M}) \le \zeta_k^{\mathcal{M}}$.
2. $\zeta_k^{\mathcal{M}} \le O\big(\frac{T \log T}{\mathrm{r}_k(T)}\big)$.
3. $\chi_k^*(\mathcal{M}) \le O\big(\frac{T \log(T)}{\mathrm{r}_k(\mathcal{M})}\big)$. *(This follows from 1 and 2.)*

Proof:
1) Let $c = \zeta_k^{\mathcal{M}}$. Let C' be an c-coloring of M with no monochromatic k-AP$^{\mathcal{M}}$'s. Let C be the following c-coloring of M^{k-1}.

$$C(x_1, \ldots, x_{k-1}) = C'(x_1 \odot x_2^2 \odot x_3^3 \odot \cdots \odot x_{k-1}^{k-1}).$$

Assume, by way of contradiction, that C is not an $\mathcal{M}$-proper coloring. Hence there exist $x_1, \ldots, x_{k-1} \in M$ and $\lambda \in M - \{ID\}$ such that
$C(x_1, \ldots, x_{k-1}) = C(x_1 \odot \lambda, x_2, x_3, \ldots, x_{k-1}) = \cdots = C(x_1, x_2, x_3, \ldots, x_{k-1} \odot \lambda)$.
By the definition of C and the fact that $\mathcal{M}$ is commutative we have that the following are equal.

- $C'(x_1 \odot x_2^2 \odot x_3^3 \odot \cdots \odot x_{k-1}^{k-1})$
- $C'(x_1 \odot \lambda \odot x_2^2 \odot x_3^3 \odot \cdots \odot x_{k-1}^{k-1})$
- $C'(x_1 \odot (x_2 \odot \lambda)^2 \odot x_3^3 \odot \cdots \odot x_{k-1}^{k-1})$

- $C'(x_1 \odot x_2^2 \odot (x_3 \odot \lambda)^3 \odot \cdots \odot x_{k-1}^{k-1})$
- $\vdots$
- $C'(x_1 \odot x_2^2 \odot x_3^3 \cdots \odot (x_{k-1} \odot \lambda)^{k-1})$

This is a monochromatic k-AP$^{\mathcal{M}}$ in C', which yields a contradiction.

2) Let $A \subseteq M$ be a set of size $r_k(\mathcal{M})$ with no k-AP$^{\mathcal{M}}$'s. We use A to obtain a coloring of M. The main idea is that we use randomly chosen translations of A to cover all of M.

Let $x \in M$. Pick a translation of A by picking $t \in M$. The probability that $x \in A \odot t$ is $\frac{|A|}{T}$. Hence the probability that $x \notin A \odot t$ is $1 - \frac{|A|}{T}$. If we pick s translations $t_1, \ldots, t_s$ at random (s to be determined later) then the expected number of x that are not covered by any $A + t_i$ is

$$T\left(1 - \frac{|A|}{T}\right)^s \leq Te^{-s\frac{|A|}{T}}.$$

We need to pick s such that this quantity is < 1 We take $s = 2\frac{T \ln T}{|A|}$ which yields

$$Te^{-s\frac{|A|}{T}} = Te^{-2\ln T} = 1/T < 1.$$

We color M by coloring each of the s translates a different color. If a number is in two translates then we color it by one of them arbitrarily. Clearly this coloring has no monochromatic k-APs. Note that it uses $\frac{T \ln T}{|A|} = O(\frac{T \log T}{\mathrm{r}_k(\mathcal{M})})$ colors. ▮

Lemma 8.4 *Let $T \in \mathbb{N}$. $\chi_k^*(\mathbb{Z}_T) \leq 2^{O((\log T)^{1/(k-1)})}$.*

Proof: By Lemma 3.1 $\mathrm{r}_k(T) \leq T2^{-O((\log T)^{1/(k-1)})}$, so $\mathrm{r}_k(T/2) \leq T2^{-O((\log T)^{1/(k-1)})}$. Let A be the k-free subset of $[T/2]$ of this size. View it as a subset of $\{1, \ldots, T\}$. This set has no k-AP$^{\mathcal{G}}$'s in it. Hence $\mathrm{r}_k(\mathcal{G}) \leq T2^{-O((\log T)^{1/(k-1)})}$. The bound on $\chi_k^*(\mathcal{G})$ follows from this bound and Lemma 8.3.3. ▮

Theorem 8.5 *Let $T \in \mathbb{N}$. $d(f_k^{\mathbb{Z}_T}) \leq k + O((\log T)^{1/(k-1)})$. Since the length of the input is $\log T$ this really an upper bound of $k + n^{1/(k-1)}$.*

Proof: By Theorem 4.5

$$d(f_k^{\mathbb{Z}_T}) \leq k + \lg(\chi_k^*(\mathbb{Z}_T)) + O(1).$$

By Lemma 8.4

$$\chi_k^*(\mathbb{Z}_T) \leq 2^{O((\log T)^{1/(k-1)})}$$

so

$$d(f_k^{\mathcal{G}}) \leq k + \lg(\chi_k^*(\mathbb{Z}_T)) \leq k + O((\log T)^{1/(k-1)}).$$

▮

8.2 Upper Bounds for General Groups

If $\mathcal{G}$ is a group of low characteristic then it does not have large k-free sets, so the technique of Lemma 8.3 does not improve upon a trivial upper bound. Hence other techniques must be used to obtain nontrivial upper bounds. We show that, for all groups $\mathcal{G}$, for almost all k, there is a nontrivial protocol for $f_k^{\mathcal{G}}$.

Lemma 8.6 *Let $\mathcal{G}_1 = (G_1, \odot_1)$ and $\mathcal{G}_2 = (G_2, \odot_2)$ be any two finite groups. Let n_1, n_2 be such that, for $i = 1, 2$, $2^{n_i - 1} < |G_i| \le 2^{n_i}$. Assume $n_1 \le n_2$. We represent elements of G_i by a subset of $\{0,1\}^{n_2}$. Let $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$.*

1. *$\chi_3^*(\mathcal{G}) \le 2^{n_2} = \Theta(|G_2|)$.*
2. *$d(f_3^{\mathcal{G}}) \le 2 + n_2 = \Theta(\log(|G_2|))$.*

Proof:
1) Let $\oplus : \{0,1\}^{n_2} \times \{0,1\}^{n_2} \to \{0,1\}^{n_2}$ be the bitwise XOR function. For $i = 1, 2$ Let ID_i be the identify in $\mathcal{G}_i$.

The following coloring shows that $\chi_3^*(\mathcal{G}) \le 2^{n_2}$. Let $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$. Let

$$C((a_1, a_2), (b_1, b_2)) = a_1 \oplus b_2 \in \{0,1\}^{n_2}.$$

Note that C uses $\le 2^{n_2}$ colors.

$$C((a_1, a_2), (b_1, b_2)) = C((a_1 \odot_1 c_1, a_2 \odot_2 c_2), (b_1, b_2)) = C((a_1, a_2), (b_1 \odot_1 c_1, b_2 \odot_2 c_2)).$$

By the definition of C we have

$$a_1 \oplus b_2 = (a_1 \odot_1 c_1) \oplus b_2.$$

Hence, by the nature of $\oplus$, $a_1 = a_1 \odot_1 c_1$. Therefore, since $\mathcal{G}_1$ is a group, $c_1 = ID_1$.

By the definition of C we have

$$a_1 \oplus b_2 = a_1 \oplus (b_2 \odot_2 c_2).$$

Hence, by the nature of $\oplus$, $b_2 = b_2 \odot_2 c_2$. Therefore, since $\mathcal{G}_2$ is a group, $c_2 = ID_2$.

Hence (c_1, c_2) is the identity in G.

2) Since $\chi_3^*(\mathcal{G}) \le 2^{n_2}$ we have, from Theorem 4.5, $d(f_3^{\mathcal{G}}) \le 2 + n_2$. ▮

Lemma 8.7 *If $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_a$ then $\chi_k^*(\mathcal{G}) \le \prod_{i=1}^a \chi_k^*(\mathcal{G}_i)$.*

Proof: Let C_i be a proper $\chi_k^*(\mathcal{G}_i)$-coloring of $\mathcal{G}_i^{k-1}$. Let C be the coloring of the product of the $\mathcal{G}_i^{k-1}$'s obtained by taking the product of the colorings. Formally C is the $\prod_{i=1}^a \chi_k^*(\mathcal{G}_i)$-coloring of $\mathcal{G}^{k-1}$

$$C((z_1^1, \ldots, z_a^1), \ldots, (z_1^{k-1}, \ldots, z_a^{k-1})) = C_1(z_1^1, \ldots, z_1^{k-1}) \cdots C_a(z_a^1, \ldots, z_a^{k-1}).$$

It is routine to check that this is a $\mathcal{G}$-proper coloring. ▮

Lemma 8.8 *If $\mathcal{G} = (G, \odot)$ is any finite abelian group and $k \geq 3$ then $d(f_k^{\mathcal{G}}) \leq d(f_{k-1}^{\mathcal{G}})$.*

Proof: We show a protocol for $f_k^{\mathcal{G}}$ that uses $d(f_{k-1}^{\mathcal{G}})$ bits.

1. For $1 \leq i \leq k$, Player i has $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$.
2. Players $1, \ldots, k-1$ replace x_1 with $x_1 \odot x_k$. Note that this takes no communication.
3. Players $1, \ldots, k-1$ execute a protocol for $k-1$ players on their new inputs. This takes $d(f_{k-1}^{\mathcal{G}})$ bits.

▮

Theorem 8.9 *For all $k \geq 3$ there exists $\alpha < 1$ such that for all finite abelian groups $\mathcal{G}$ $d(f_k^{\mathcal{G}}) < k + \alpha \lg(|G|) + O(1)$. (Hence there is a nontrivial protocol for $f_k^{\mathcal{G}}$.)*

Proof: Fix k. Let $\mathcal{G}$ be a finite abelian group of size g. By the classification of finite abelian groups $\mathcal{G} = \mathbb{Z}_{h_1} \times \cdots \times \mathbb{Z}_{h_b}$ for some factorization $g = \prod_{i=1}^{b} h_i$. We assume $h_1 \leq \cdots \leq h_b$. By Lemma 8.4, for all i, $\chi_k^*(\mathbb{Z}_{h_i}) \leq 2^{O((\lg h_i)^{1/(k-1)})}$.

There are two cases. They depend on a constant β to be picked later.

Case 1: $b \leq \beta \lg g$.

By Lemma 8.7

$$\chi_k^*(\mathcal{G}) = \chi_k^*(\mathbb{Z}_{h_1}) \cdots \chi_k^*(\mathbb{Z}_{h_b}) \leq \prod_{i=1}^{b} 2^{O((\lg h_i)^{1/(k-1)})}.$$

So

$$\lg(\chi_k^*(\mathcal{G})) \leq \sum_{i=1}^{b} O((\lg h_i)^{1/(k-1)}) \leq O(\sum_{i=1}^{b}((\lg h_i)^{1/(k-1)}).$$

The quantity $\sum_{i=1}^{b}(\lg h_i)^{1/(k-1)}$, where $\prod_{i=1}^{b} h_i = g$, is maximized when $h_1 = \cdots = h_b = g^{1/b}$. Hence

$$\sum_{i=1}^{b}(\lg h_i)^{1/(k-1)} \leq \sum_{i=1}^{b}(\lg g^{1/b})^{1/(k-1)} \leq b(1/b)^{1/(k-1)}(\lg g)^{1/(k-1)} \leq b^{(k-2)/(k-1)}(\lg g)^{1/(k-1)}.$$

Since $b \leq \beta \lg g$ we have

$$\begin{aligned} b^{(k-2)/(k-1)}(\lg g)^{1/(k-1)} \leq (\beta \lg g)^{(k-2)/(k-1)}(\lg g)^{1/(k-1)} &\leq \beta^{(k-2)/(k-1)}(\lg g)^{(k-2)/(k-1)}(\lg g)^{1/(k-1)} \\ &\leq \beta^{(k-2)/(k-1)}(\lg g). \end{aligned}$$

Hence there exists a constant c such that $\lg(\chi_k^*(\mathcal{G})) \leq c\beta^{(k-2)/(k-1)}(\lg g)$. Note that

$$d(f_k^{\mathcal{G}}) \leq k + \lg(\chi_k^*(\mathcal{G})) + O(1) \leq k + c\beta^{(k-2)/(k-1)}(\lg g).$$

Pick $\beta < 1$ such that $\alpha = c\beta^{(k-2)/(k-1)} < 0.9$.

Case 2: $b \geq \beta \lg g$.

Since all $h_i \geq 2$ we have

$$\prod_{i=1}^{b/2} h_i \geq 2^{b/2} \geq 2^{\beta \lg g/2} = g^{\beta/2}.$$

So

$$\prod_{i=b/2+1}^{b} h_i \leq g^{1-(\beta/2)}.$$

Let $\mathcal{G}_1 = \mathbb{Z}_{h_1} \times \cdots \times \mathbb{Z}_{h_{b/2}}$ and $\mathcal{G}_2 = \mathbb{Z}_{h_{b/2+1}} \times \cdots \times \mathbb{Z}_{h_b}$ Note that $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and that $|G_2| \geq |G_1|$. By Lemmas 8.8 and 8.6

$$d(f_k^{\mathcal{G}}) \leq d(f_3^{\mathcal{G}}) \lg(|G_2|) + O(1) \leq \lg(g^{1-\beta/2}) + O(1) \leq (1-\beta/2) \lg g + O(1).$$

Since $0 < \beta < 1$ we have $(1 - (\beta/2)) < 1$.

Take α to be the max of

- 0.9.
- $1 - (\beta/2)$

■

9 Open Problems

1. If $T = \Theta(2^n)$ then
$$\Omega(\log \log n) \leq d(f_{3,T}) \leq \sqrt{n}.$$
It is open to improve this. Speculations:
   (a) One way to improve the upper bounds is to find larger 3-free sets. It is known [7] (see also [13]) that if $A \subseteq [T]$ and $|A| \geq \Omega\left(T\sqrt{\frac{\log \log T}{\log T}}\right)$ then A has a 3-AP. If 3-free sets of this size exist then $d(f_{3,T}) \leq O(\log \log T)$, so if $T = \Theta(2^n)$ then $d(f_{3,T}) \leq O(\log n)$.
   (b) If proper colorings that do not induce 3-free sets exist then this may improve the upper bounds. By contrast, if proper colorings must induce 3-free sets then this may improve the lower bounds.

2. If $T = \Theta(2^n)$ and $k \geq 4$ then
$$\omega(1) \leq d(f_{k,T}) \leq k + O((n \log k)^{1/(k-1)}).$$
It is open to improve either side. Speculations:
   (a) If proper colorings that do not induce k-free sets exist this may improve the upper bounds. By contrast, if proper colorings must induce k-free sets this may improve the lower bounds.

(b) If Conjecture 5.3 is true then this would improve the lower bound to $c(k) \log\log\log T$ for some $c(k)$.

3. Theorem 4.5 gives upper and lower bounds for $d(f_k^{\mathcal{G}})$ that differ by $k + O(1)$; however, the bounds are in terms of $\chi_k^*(\mathcal{G})$. For a variety of abelian groups $\mathcal{G}$ find upper and lower bounds on $\chi_k^*(\mathcal{G})$ so that we can obtain upper and lower bounds on $d(f_k^{\mathcal{G}})$.

4. Let p be a prime. Theorem 4.5 holds if $\mathcal{G}$ is $\mathbb{Z}_p$ under modular multiplication. Hence the complexity of $f_3^{\mathcal{G}}$ and $f_k^{\mathcal{G}}$ is very close to a function in combinatorics. This function should be studied.

5. Let $k, T \in \mathbb{N}$. Let $g_{k,T} : \{\{0,1\}^n\}^k \rightarrow \{0,1\}$ be defined by $g(x_1, \ldots, x_m) = 1$ iff $\prod_{i=1}^k x_i = T$. The multiparty communication complexity of g can probably be studied with the tools we have devised.

6. The premise of Theorem 4.5 is that $\mathcal{G}$ is a finite abelian group. What if $\mathcal{G}$ is a nonabelian group? A Monoid? Infinite? Theorem 5.12 illustrates that there are large monoids $\mathcal{M}$ with $d(f_k^{\mathcal{M}}) \leq 2$, so there may be a wide range of possibilities.

7. Empirical studies could be done to see if there are colorings that use substantially fewer than the number of colors induced by 3-free sets.

10 Appendix: Empirical Results

Gasarch and Glenn [10] survey several constructions of 3-free sets and use them to produce actual 3-free sets. The table below Appendix was produced using their software. The table gives n, a lower bound on $\mathrm{r}_3(3N)$, $n = \lg N$, and $d(f_{3,T}) = 3 + \left\lceil \lg\left(\frac{6N \ln(3N)}{\mathrm{r}_3(3N)} + 1\right) \right\rceil$ (from Theorem 2.4.1). We also give the ratio of $d(f_{3,T})$ to $\sqrt{n}$ since $O(\sqrt{n})$ is what the analysis gives.

1. The lowest value where we know that the main protocol beats the trivial one is around 10^4. This is fairly small.

2. The ratio seems to be around 0.31. This is a small number.

N	$\mathrm{r}_3(3N)$	df	n	$\lceil\sqrt{n}\rceil$	ratio
10	10	7	4	2	0.286
100	48	9	7	3	0.333
1000	210	10	10	4	0.4
10000	1024	12	14	4	0.333
100000	4096	13	17	5	0.385
10^6	16384	15	20	5	0.333
10^7	65536	16	24	5	0.312
10^8	262144	18	27	6	0.333
10^9	1.28×10^6	19	30	6	0.316
10^{10}	6.32×10^6	20	34	6	0.3
10^{11}	3.83×10^7	21	37	7	0.333
10^{12}	2.12×10^8	22	40	7	0.318
10^{13}	1.31×10^9	23	44	7	0.304
10^{14}	8.36×10^9	24	47	7	0.292
10^{15}	5.23×10^{10}	24	50	8	0.333
10^{16}	3.41×10^{11}	25	54	8	0.32
10^{17}	2.12×10^{12}	26	57	8	0.308
10^{18}	1.34×10^{13}	27	60	8	0.296
10^{19}	9.20×10^{13}	27	64	8	0.296
10^{20}	6.00×10^{14}	28	67	9	0.321
10^{21}	4.11×10^{15}	29	70	9	0.31
10^{22}	2.82×10^{16}	29	74	9	0.31
10^{23}	1.92×10^{17}	30	77	9	0.3
10^{24}	1.31×10^{18}	30	80	9	0.3
10^{25}	9.13×10^{18}	31	84	10	0.323
10^{26}	6.34×10^{19}	32	87	10	0.312
10^{27}	4.60×10^{20}	32	90	10	0.312
10^{28}	3.19×10^{21}	33	94	10	0.303
10^{29}	2.25×10^{22}	33	97	10	0.303
10^{30}	1.61×10^{23}	34	100	10	0.294
10^{31}	1.19×10^{24}	34	103	11	0.324
10^{32}	8.57×10^{24}	35	107	11	0.314
10^{33}	6.20×10^{25}	35	110	11	0.314
10^{34}	4.61×10^{26}	36	113	11	0.306
10^{35}	3.38×10^{27}	36	117	11	0.306
10^{36}	2.50×10^{28}	37	120	11	0.297
10^{37}	1.83×10^{29}	37	123	12	0.324
10^{38}	1.36×10^{30}	38	127	12	0.316
10^{39}	1.03×10^{31}	38	130	12	0.316
10^{40}	7.70×10^{31}	39	133	12	0.308

N	$\mathrm{r}_3(3N)$	df	n	$\lceil\sqrt{n}\rceil$	ratio
10^{41}	5.81×10^{32}	39	137	12	0.308
10^{42}	4.36×10^{33}	39	140	12	0.308
10^{43}	3.33×10^{34}	40	143	12	0.3
10^{44}	2.54×10^{35}	40	147	13	0.325
10^{45}	1.94×10^{36}	41	150	13	0.317
10^{46}	1.48×10^{37}	41	153	13	0.317
10^{47}	1.13×10^{38}	42	157	13	0.31
10^{48}	8.70×10^{38}	42	160	13	0.31
10^{49}	6.74×10^{39}	42	163	13	0.31
10^{50}	5.22×10^{40}	43	167	13	0.302
10^{51}	4.04×10^{41}	43	170	14	0.326
10^{52}	3.13×10^{42}	44	173	14	0.318
10^{53}	2.43×10^{43}	44	177	14	0.318
10^{54}	1.91×10^{44}	44	180	14	0.318
10^{55}	1.50×10^{45}	45	183	14	0.311
10^{56}	1.18×10^{46}	45	187	14	0.311
10^{57}	9.24×10^{46}	45	190	14	0.311
10^{58}	7.24×10^{47}	46	193	14	0.304
10^{59}	5.72×10^{48}	46	196	14	0.304
10^{60}	4.54×10^{49}	47	200	15	0.319
10^{61}	3.61×10^{50}	47	203	15	0.319
10^{62}	2.87×10^{51}	47	206	15	0.319
10^{63}	2.28×10^{52}	48	210	15	0.312
10^{64}	1.81×10^{53}	48	213	15	0.312
10^{65}	1.44×10^{54}	48	216	15	0.312

References

[1] Babai, Nisan, and Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *Journal of Computer and System Sciences*, 45, 1992. Prior version in STOC89.

[2] L. Babai, P. Pudlak, V. Rodl, and E. Szemeredi. Lower bounds to the complexity of symmetric boolean functions. *Theoretical Computer Science*, 74:313–323, 1990.

[3] D. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38, 1989.

[4] D. Barrington and H. Straubing. Superlinear lower bounds for bounded width branching programs. *Journal of Computer and System Sciences*, 50, 1995.

[5] P. Beame and E. Vee. Time-space tradeoffs, multiparty communication complexity and nearest neighbor problems. In *Proceedings of the Thirty-fourth Annual ACM Symposium on the Theory of Computing,* Montreal, Canada, 2002.

[6] F. Behrend. On set of integers which contain no three in arithmetic progression. *Proc. of the National Acadamy of Science (USA)*, 23:331–332, 1946.

[7] J. Bourgain. On triples in arithmetic progression. *Geometric and Functional Analysis*, 9:968–984, 1999.

[8] A. Chandra, M. Furst, and R. Lipton. Multiparty protocols. In *Proceedings of the Fifteenth Annual ACM Symposium on the Theory of Computing,* Boston MA, pages 94–99, 1983.

[9] R. Cleve. Towards optimal simulations of formulas by bounded-width programs. *Computational Complexity*, 1:91–105, 1991. Earlier version in STOC90.

[10] W. Gasarch and J. Glenn. Finding large sets without arithmetic progressions of length three: An empirical view, 2005.

[11] R. Graham, A. Rothchild, and J. Spencer. *Ramsey Theory.* Wiley, 1990.

[12] R. Graham and J. Solymosi. Monochromatic equilateral right triangles on the integer grid, 2005. `www.math.ucsd.edu/~sbutler/ron/06_03_righttriangles.pdf` or `www.cs.umd.edu/~gasarch/vdw/graham-solymosi.pdf`.

[13] B. Green. On triples in arith. prog., 1999. `www.dpmms.cam.ac.uk/~bjg23/papers/bourgain.pdf`.

[14] E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, 1997.

[15] I. Laba and M. T. Lacey. On sets of integers not containing long arithmetic progressions, 2001. Website `arxiv.org/pdf/math.CO/0108155` or `www.math.ubc.ca/~ilaba/preprints`.

[16] L. Moser. On non-averaging sets of integers. *Canadian Journal of Mathematics*, 5:245–252, 1953.

[17] M. Paterson, N. Pippenger, and U. Zwick. Optimal carry save networks. In *PATBOOL: Paterson (Ed), Boolean Function Complexity*, pages 174–201, 1992.

[18] P. Pudlak. A lower bound on complexity of branching programs. In *MFCS84*, pages 480–489, 1984.

[19] R. Rankin. Sets of integers containing not more than a given number of terms in an arithmetic progression. *Proceedings of the Royal Society of Edinburgh Sect. A 65*, pages 332–344, 1960—1961.

[20] J.-F. Raymond, P. Tesson, and D. Therien. An algebraic approach to communication complexity. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming ICALP 1998,* Aalborg, Denmark, volume 1443 of *Lecture Notes in Computer Science*, pages 29–40, Berlin, 1998. Springer-Verlag. `www.cs.mcgill.ca/~ptesso`.

[21] R. Sinha and J. Thathachar. Efficient oblivous branching programs. *Journal of Computer and System Sciences*, 55:373–384, 1997.

[22] J. Solymosi. Personal communication, 2005.

[23] P. Tesson. *Computational complexity questions realted to finite monoids and semigroups.* PhD thesis, McGill University, 2003.

[24] P. Tesson. An application of the Hales-Jewitt Theorem to multiparty communication complexity, 2004. Unpublished manuscript, but available at `www.cs.umd.edu/~gasarch/ramsey/ramsey.html`.

[25] P. Tesson and D. Therien. Monoids and computations. *International Journal of Algebra and Computation*, pages 115–163, 2004. `www.cs.mcgill.ca/~ptesso`.

[26] P. Tesson and D. Therien. Complete classification of the communication complexity of regular languages. *Theory of computing systems*, pages 135–159, 2005.

[27] I. Wegener. *Branching Programs and Binary Decision Diagrams: Theory and Application.* SIAM, 2000.

11 Acknowledgments

We would like to thank Jozsef Solymosi who directed us to [12], and Paul Pudlak who directed us to [2]. We would also like to thank Adam Bender, Walid Gomma, Jon Katz, Clyde Kruskal, Martin Ma and Brian Postow for proofreading.