

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, \dots, x_k be n -bit numbers and $T \in \mathbb{N}$. Assume that P_1, \dots, P_k are players such that P_i knows all of the numbers *except* x_i . They want to determine if $\sum_{j=1}^k x_j = T$ by broadcasting as few bits as possible. In [7] an upper bound of $O(\sqrt{n})$ bits was obtained 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 $k \geq 3$ an upper bound of $k + O((n + \log k)^{1/(\lceil \lg(2k-2) \rceil)})$, (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, and (5) empirical. results for $k = 3$,

1 Introduction

Multiparty communication complexity was first defined in [7] and was used to obtain lower bounds on branching programs (BPs). It has been used to get additional lower bounds and tradeoffs for BPs [1, 5], lower bounds on data structures [5], time-space tradeoffs for restricted TMs [1], and unconditional pseudorandom generators for logspace [1].

Def 1.1 Let $f : \{\{0, 1\}^n\}^k \rightarrow \{0, 1\}$. 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 . This scenario is called *the forehead model*.

*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

The multiparty communication complexity of the following function was used [7] to obtain superlinear lower bounds on constant width BPs (improved [2, 4, 14]).

Def 1.2 Let $k, n, T \in \mathbb{N}$. (T stands for Target.) Let $f_{k,T} : \{\{0,1\}^n\}^k \rightarrow \{0,1\}$ be defined as

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

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

Determining $d(f_{k,T})$ is equivalent to a problem in combinatorics. From this one obtains:

1. $d(f_{3,T}) = O(\sqrt{n})$.
2. For all k , for $T = \Theta(2^n)$, $d(f_{k,T})$ is not constant in n .

This paper contains the following.

1. New upper and lower bounds on $d(f_{k,T})$:
 - (a) For $k \geq 4$, $d(f_{k,T}) \leq k + O((n + \log k)^{1/(\lfloor \lg(2k-2) \rfloor)})$.
 - (b) For $k = 3$, for $T = \Theta(2^n)$, $d(f_{3,T}) \geq \Omega(\log \log n)$. The proof uses a Ramsey-theoretic lemma (Lemma 5.1).
2. A group-theoretic version of the Exact- T problem that we denote $f_{k,T}^{\mathcal{G}}$.
 - (a) Bounds on $d(f_3^{\mathcal{G}})$ yield bounds on $d(f_{k,T})$.
 - (b) For all finite abelian groups \mathcal{G} of size g , $d(f_{3,T}^{\mathcal{G}}) \geq \Omega(\log \log \log g)$.
 - (c) For almost all finite abelian groups \mathcal{G} , a nontrivial protocol for $f_{k,T}^{\mathcal{G}}$.
 - (d) $d(f_{k,T}^{\mathbb{Z}_m}) \leq k + O((\log m + \log k)^{1/(\lfloor \lg(2k-2) \rfloor)})$.
3. Application: We use the lower bound on $d(f_k^{\mathcal{G}})$ to obtain lower bounds on the multiparty communication complexity of several regular languages.
4. Empirical results: 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 1.3 If $T \in \mathbb{N}$ then $[T]$ denotes the set $\{1, \dots, T\}$.

Def 1.4 We say $f \leq_{cc}^{O(1)} g$ if there exists a protocol for f that has the following properties. (1) The protocol may invoke a protocol for g once on an input of length $O(n)$, (2) before and after the invocation, the players may broadcast $O(1)$ bits, and (3) $f \equiv_{cc}^{O(1)} g$ if $f \leq_{cc}^{O(1)} g$ and $g \leq_{cc}^{O(1)} f$. Note that $\leq_{cc}^{O(1)}$ is transitive and that if $f \leq_{cc}^{O(1)} g$ then $d(f) \leq d(g) + O(1)$.

2 Multiparty. Comm. Comp. 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 [7]. We also review the upper and lower bounds that they obtained.

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 $C : [T]^{k-1} \rightarrow [c]$ such that there do not exist $x_1, \dots, x_{k-1} \in [T]$ and $\lambda \in \mathbb{Z} - \{0\}$ with (1) for all i , $x_i + \lambda \in [T]$, and (2) $C(x_1, x_2, x_3, \dots, x_{k-1}) = C(x_1 + \lambda, x_2, x_3, \dots, x_{k-1}) = \dots = C(x_1, x_2, x_3, \dots, x_{k-1} + \lambda)$
2. Let $\chi_k(T)$ be the least c such that there is a proper c -coloring of $[T]^{k-1}$.

Theorem 2.2 [7]

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

Def 2.3

1. A k -AP is an arithmetic progression of length k .
2. A set $A \subseteq [T]$ is k -free if there do not exist any k -AP's in A .
3. Let $r_k(T)$ 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 [7]

1. $d(f_{k,T}) \leq k - 1 + \lg(\chi_k(T)) \leq k - 1 + \left\lceil \lg\left(\frac{2kT \ln(kT)}{r_k(kT)}\right) + 1 \right\rceil = k + O\left(\log\left(\frac{kT \log(kT)}{r_k(kT)}\right)\right)$
2. For all k , $\chi_k(2^n)$ is an increasing function of n .
3. 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 [13] for a constructive version and [8] for an exposition) to obtain the following.

Corollary 2.5 $d(f_{3,T}) \leq O(\sqrt{\log T})$. 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 $k \geq 4$, which will in turn yield new explicit upper bounds on $d(f_{k,T})$. This lemma was first proven in [15] but see also [12].

Lemma 3.1 $r_k(T) \geq T2^{-O((\log T)^{1/(\lfloor \lg(2k-2) \rfloor)})}$.

Theorem 3.2

1. $d(f_{k,T}) \leq k + O((\log kT)^{1/(\lfloor \lg(2k-2) \rfloor)})$.
2. If $T = \Theta(2^n)$ then $d(f_{k,T}) = k + O((n + \log k)^{1/(\lfloor \lg(2k-2) \rfloor)})$.

Proof: (1) Follows from Theorem 2.4 and Lemma 3.1. (2) Follows from part 1 of this theorem. ■

4 Group Theoretic Version

We define a group-theoretic version of the Exact- T problem.

Def 4.1 Let $\mathcal{G} = (G, \odot)$ be a group.

1. Let $f_{k,T}^{\mathcal{G}} : G^k \rightarrow \{0, 1\}$ be defined by

$$f_k^{\mathcal{G}}(x_1, \dots, x_k) = \begin{cases} 1 & \text{if } \odot_{j=1}^k x_j = ID; \\ 0 & \text{otherwise.} \end{cases}$$

2. A \mathcal{G} -proper c -coloring of G^{k-1} is a function $C : G^{k-1} \rightarrow [c]$ such that there does not exist $x_1, \dots, x_{k-1} \in G$ and $\lambda \in G - \{ID\}$ with $C(x_1, \dots, x_{k-1}) =$

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

3. $\chi_k^*(\mathcal{G})$ be the least c such that there is a \mathcal{G} -proper c -coloring of G^{k-1} .

The proof of the following theorem is a modification of a proof from [7], hence we omit it.

Theorem 4.2 If \mathcal{G} is a finite abelian group then $\lg(\chi_k^*(\mathcal{G})) + \Omega(1) \leq d(f_k^{\mathcal{G}}) \leq k + \lg(\chi_k^*(\mathcal{G})) + O(1)$.

Note 4.3 In Theorem 4.2 $d(f_k^{\mathcal{G}}) \geq \lg(\chi_k^*(\mathcal{G})) + \Omega(1)$. Chandra, Furst, and Lipton obtained $d(f_{k,T}) \geq \lg(\chi_k(\lfloor \frac{T}{k} \rfloor)) + \Omega(1)$. They have a factor of $\frac{1}{k}$ and we do not because in the group case, for any $x_1, \dots, x_{k-1} \in G$ there is an $x \in G$ such that $f_k^{\mathcal{G}}(x_1, \dots, x_{k-1}, x) = 1$; by contrast, there are $x_1, \dots, x_{k-1} \in [T]$ such that, for all $x \in [T]$, $f_{k,T}(x_1, \dots, x_{k-1}, x) = 0$.

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

Lemma 4.5 Let $T \in \mathbb{N}$ and $k \geq 3$. Then the following hold.

1. $d(f_{k,T}) \leq d(f_k^{\mathbb{Z}_T}) + O(1)$.
2. $d(f_k^{\mathbb{Z}_T}) \leq d(f_{k,T}) + O((\log(k)2^n/T))$.
3. If $T = 2^n$ then $d(f_k^{\mathbb{Z}_T}) \leq d(f_{k,T}) + O(\log k)$.

5 Lower Bounds

5.1 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 [10].

Lemma 5.1 *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 $g \geq g_0$ and $c \leq d_0 \log \log g$ then there are no \mathcal{G} -proper c -colorings of $G \times G$. Hence $\chi_3^*(\mathcal{G}) \geq \Omega(\log \log g)$.*

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 a th anti-diagonal.) There exists an a such that $|P_a| \geq \lceil h_s^2/g \rceil$. 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 $\{(x_1, y_1), \dots, (x_m, y_m)\}$ be m elements of P_a such that, for $1 \leq i \leq m, C(x_i, y_i) = c-s$.

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

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 $y_i \neq y_j$ is similar. *End of Proof of Claim 1*

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

Proof: If $C(x_i, y_j) = c - s$ then $C(x_i, y_j) = C(x_i, y_i) = C(x_j, y_j) = c - s$. If $\lambda = (a^{-1} \odot x_j \odot y_i)$ then $C(x_i, y_j) = C(x_i \odot \lambda, y_j) = C(x_i, y_j \odot \lambda)$. This violates C being a proper coloring. *End of Proof of Claim 2*

Let

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

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 such that COL restricted to $X_s \times Y_s$ uses 0 colors.

We have $h_0 = g$ and

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

One can easily show that $h_s \geq \frac{g}{(3c)^{2^s-1}}$.

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 $c = \Omega(\log \log g)$. \blacksquare

Theorem 5.2 *If \mathcal{G} is a finite abelian group then $d(f_3^{\mathcal{G}}) \geq \Omega(\log \log \log |G|)$.*

Proof: By Lemma 5.1 $\chi_3^*(\mathcal{G}) \geq \Omega(\log \log |G|)$. By Theorem 4.2, $d(f_3^{\mathcal{G}}) \geq \lg(\chi_3^*(\mathcal{G})) \geq \Omega(\log \log \log |G|)$. \blacksquare

From Theorem 5.2 and Lemma 4.5 we obtain the following.

Theorem 5.3 *Let $T \in \mathbb{N}$. $d(f_{3,T}) \geq \Omega(\log \log \log T) - O(\frac{(\log k)2^n}{T})$. If $T = \Theta(2^n)$ then $d(f_{3,T}) \geq \Omega(\log \log n) - O(\log k)$.*

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

From Lemma 4.5 and Theorem 2.4 we obtain the following.

Theorem 5.4 $d(f_k^{\mathbb{Z}_m}) = \omega(1)$.

For other groups we cannot use Lemma 4.5 and hence we develop other techniques.

Def 5.5 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 5.6 $\text{PART}_{n,k} : \{\{0, 1\}^n\}^k \rightarrow \{0, 1\}$ is the following function. Interpret the input as k subsets of $\{1, \dots, n\}$. Output 1 if these sets form a partition of $\{1, \dots, n\}$, and 0 otherwise.

Tesson [17, 18] proved the following. He used the Hales-Jewitt Theorem (see [9]) 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 5.7 For all k , $d(\text{PART}_{n,k}) \geq \omega(1)$.

Lemma 5.8 Let $k \geq 3$. Let $h_1, \dots, h_m \geq 2$. Let $\mathcal{G} = \mathbb{Z}_{h_1} \times \dots \times \mathbb{Z}_{h_m}$. For all k , $d(\text{PART}_{m,k}) \leq d(f_k^{\mathcal{G}}) + O(1)$.

Proof sketch: One can show that $\text{PART}_{n,k} \leq_{\text{cc}}^{O(1)} f_k^{\mathcal{G}}$. (Recall Definition 1.4.) ■

Lemma 5.9 If \mathcal{G}_1 and \mathcal{G}_2 are groups, $k \geq 3$, $d(f_k^{\mathcal{G}_1}) \leq d(f_k^{\mathcal{G}_1 \times \mathcal{G}_2})$.

Theorem 5.10 For all d, k there exists g_0 such that for all finite abelian groups \mathcal{G} , $|\mathcal{G}| \geq g_0$, $d(f_k^{\mathcal{G}}) \geq d$. In short, the bigger the group, the larger $d(f_k^{\mathcal{G}})$, without bound.

6 App. to Multiparty. Comm. Comp. of Reg Languages

In this section we use Theorems 5.2 and Theorem 5.10 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 [16, 20, 19]. The multiparty communication complexity of regular languages (defined initially in [16]) 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 $x = a_1 a_2 \dots a_{kn}$ 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 $a_1 a_2 \dots a_{kn} \in L$.

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 $0 \leq r \leq m - 1$.

1. $\#_{\sigma}(w)$ is the number of σ in w .

$$2. L_{\sigma,r,m} = \{w \mid \#_{\sigma}(w) \equiv r \pmod{m}\}.$$

Lemma 6.4 *Let $k, r, m \in \mathbb{N}$ such that $0 \leq r \leq m - 1$. Let $|\Sigma| \geq 2$ and $\sigma \in \Sigma$ and $L = L_{\sigma,r,m}$. Then $f_k^{\mathbb{Z}_m} \leq_{cc}^{O(1)} R_{k,L}$. (Recall Definition 1.4.)*

Proof: We show $f_{k,r}^{\mathbb{Z}_m} \leq_{cc}^{O(1)} R_{k,L}$. It is easy to show that $f_k^{\mathbb{Z}_m} \equiv_{cc}^{O(1)} f_{k,r}^{\mathcal{G}}$, hence we will have $f_k^{\mathbb{Z}_m} \leq_{cc}^{O(1)} R_{k,L}$.

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

For each i , $1 \leq i \leq k$, there are m positions that are $\equiv i \pmod{k}$. Map to a string such that q_i of those positions are σ and the rest are not σ .

If w is the resulting word then $\#_{\sigma}(w) = \sum_{i=1}^k q_i$. Hence $q_1 + \dots + q_k \equiv r \pmod{m}$ 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 $k \geq 4$, $\omega(1) \leq d(R_{k,L})$.

Proof: By Lemma 6.4 $d(f_k^{\mathcal{G}}) \leq d(R_{k,L})$.

- 1) By Theorem 5.2 $d(f_3^{\mathcal{G}}) = \omega(\log \log \log m)$. Hence $d(R_{3,L}) = \omega(\log \log \log m)$.
- 2) By Theorem 5.10 $d(f_3^{\mathcal{G}}) = \omega(1)$. Hence $d(R_{k,L}) = \omega(1)$. ■

7 Upper Bounds

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

The proofs in this section are a reworking of those in [7].

Notation 7.1 If $\mathcal{G} = (G, \odot)$ is a group and $d \in G$, $k \in \mathbb{N}$, then d^k means $d \odot \dots \odot d$ where there are k d 's.

Def 7.2 Let $\mathcal{G} = (G, \odot)$ be a group. Let $T = |G|$.

1. A k -AP $^{\mathcal{G}}$ is a multiset of the form $\{a, a \odot d, a \odot d^2, \dots, a \odot d^{k-1}\}$ where $a, d \in G$.
2. A set $A \subseteq G$ is k -free if there do not exist any k -AP $^{\mathcal{G}}$'s in A .
3. Let $r_k(\mathcal{G})$ be the size of the largest k -free subset of G .

Lemma 7.3 *If \mathcal{G} is a finite abelian group then $\chi_k^*(\mathcal{G}) \leq O\left(\frac{|G|\log(|G|)}{r_k(\mathcal{G})}\right)$. $\chi_k^*(\mathcal{M}) \leq O\left(\frac{T \log(T)}{r_k(\mathcal{M})}\right)$.*

Lemma 7.4 *Let $T \in \mathbb{N}$. $\chi_k^*(\mathbb{Z}_T) \leq 2^{O((\log T)^{1/(\lfloor \lg(2k-2) \rfloor)})}$.*

Theorem 7.5 *Let $T \in \mathbb{N}$. $d(f_k^{\mathbb{Z}_T}) \leq k + O((\log kT)^{1/(\lfloor \lg(2k-2) \rfloor)})$.*

7.2 Upper Bounds for General Groups

If \mathcal{G} has low characteristic then it does not have large k -free sets, so the technique of Lemma 7.3 does not improve upon a trivial upper bound. Hence we use other techniques.

Lemma 7.6 *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 $i = 1, 2$, $2^{n_i-1} < |G_i| \leq 2^{n_i}$. Assume $n_1 \leq n_2$. 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. $\chi_3^*(\mathcal{G}) \leq 2^{n_2} = \Theta(|G_2|)$.
2. $d(f_3^{\mathcal{G}}) \leq 2 + n_2 = \Theta(\log(|G_2|))$.

Proof:

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

We show that $\chi_3^*(\mathcal{G}) \leq 2^{n_2}$. Let $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$. Let $C((a_1, a_2), (b_1, b_2)) = a_1 \oplus b_2 \in \{0, 1\}^{n_2}$. It is easy to show that C is a $\mathcal{G}_1 \times \mathcal{G}_2$ -proper coloring.

2) Since $\chi_3^*(\mathcal{G}) \leq 2^{n_2}$ we have, from Theorem 4.2, $d(f_3^{\mathcal{G}}) \leq 2 + n_2$. ■

Lemma 7.7 *If $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_a$ then $\chi_k^*(\mathcal{G}) \leq \prod_{i=1}^a \chi_k^*(\mathcal{G}_i)$.*

Proof: Let C_i be a proper $\chi_k^*(\mathcal{G}_i)$ -coloring of \mathcal{G}_i^{k-1} . Let C be the coloring

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

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

Lemma 7.8 *If \mathcal{G} is a finite abelian group, $k \geq 3$, then $d(f_k^{\mathcal{G}}) \leq d(f_{k-1}^{\mathcal{G}})$.*

Theorem 7.9 *For all $k \geq 3$ there exists $\alpha < 1$ such that for all finite abelian groups \mathcal{G} $d(f_k^{\mathcal{G}}) < k + \alpha \lg(|G|) + O(1)$. (There is a nontrivial protocol for $f_k^{\mathcal{G}}$.)*

Proof sketch: 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 7.4, 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 7.7 $\chi_k^*(\mathcal{G}) = \chi_k^*(\mathbb{Z}_{h_1}) \cdots \chi_k^*(\mathbb{Z}_{h_b}) \leq \prod_{i=1}^b 2^{O((\lg h_i)^{1/(k-1)})}$.

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 $\sum_{i=1}^b (\lg h_i)^{1/(k-1)} \leq b^{(k-2)/(k-1)} (\lg g)^{1/(k-1)}$. 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 $\prod_{i=1}^{b/2} h_i > 2^{b/2} \geq 2^{\beta \lg g/2} = g^{\beta/2}$. So $\prod_{i=b/2+1}^b h_i < g^{1-(\beta/2)}$. 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 7.8 and 7.6 $d(f_k^{\mathcal{G}}) \leq d(f_3^{\mathcal{G}_2}) \lg(|G_2|) + O(1) \leq \lg(g^{1-\beta/2}) + O(1) \leq (1-\beta/2) \lg g + O(1)$. Since $0 < \beta < 1$ we have $(1 - (\beta/2)) < 1$. Take $\alpha = \max\{0.9, 1 - (\beta/2)\}$. ■

8 Open Problems

1. If $T = \Theta(2^n)$ then $\Omega(\log \log n) \leq d(f_{3,T}) \leq \sqrt{n}$. Improve either side.
2. If $T = \Theta(2^n)$ and $k \geq 4$ then $\omega(1) \leq d(f_{k,T}) \leq k + O((n + \log k)^{1/(\lfloor \lg(2k-2) \rfloor)})$. Improve either side.
3. Theorem 4.2 shows $\lg(\chi_k^*(\mathcal{G})) + \Omega(1) \leq d(f_k^{\mathcal{G}}) \leq k + \lg(\chi_k^*(\mathcal{G})) + \Omega(1)$. For a variety of abelian groups \mathcal{G} estimate $\chi_k^*(\mathcal{G})$.
4. What happens to $d(f_k^{\mathcal{G}})$ if G is nonabelian? A Monoid? Infinite?
5. 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.

References

- [1] Babai, Nisan, and Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *JCSS*, 45, 1992.
- [2] L. Babai, P. Pudlak, V. Rodl, and E. Szemerédi. Lower bounds to the complexity of symmetric Boolean functions. *TCS*, 74:313–323, 1990.
- [3] D. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 . *JCSS*, 38, 1989.
- [4] D. Barrington and H. Straubing. Superlinear lower bounds for bounded width branching programs. *JCSS*, 50, 1995.

- [5] P. Beame and E. Vee. Time-space tradeoffs, multiparty communication complexity and nearest neighbor problems. In *34th STOC*, 2002.
- [6] F. Behrend. On set of integers which contain no three in arithmetic progression. *Proc. of the Nat. Acad. of Sci. (USA)*, 23:331–332, 1946.
- [7] A. Chandra, M. Furst, and R. Lipton. Multiparty protocols. In *15th STOC*, pages 94–99, 1983.
- [8] W. Gasarch and J. Glenn. Finding large sets without arithmetic progressions of length three: An empirical view, 2005.
- [9] R. Graham, A. Rothchild, and J. Spencer. *Ramsey Theory*. Wiley, 1990.
- [10] R. Graham and J. Solymosi. Monochromatic equilateral right triangles on the integer grid, 2005. See Solymosi’s website
- [11] E. Kushilevitz and N. Nisan. *Comm. Comp.* Camb Univ. Press, 1997.
- [12] I. Laba and M. T. Lacey. On sets of integers not containing long arithmetic progressions, 2001. See arxiv.org
- [13] L. Moser. On non-averaging sets of integers. *Canadian Journal of Mathematics*, 5:245–252, 1953.
- [14] P. Pudlak. A lower bound on complexity of branching programs. In *MFCS84*, pages 480–489, 1984.
- [15] R. Rankin. Sets of integers containing not more than a given number of terms in an arithmetic. progressions. *Proc. of the Royal Soc. of Edinburgh Sect. A* 65, 332–344, 1960–1961.
- [16] J.-F. Raymond, P. Tesson, and D. Therien. An algebraic approach to communication complexity. In *25th ICALP*, vol. 1443 of LNCS pages 29–40. 1998. Also at Tesson Website.
- [17] P. Tesson. *Computational complexity questions related to finite monoids and semigroups*. PhD thesis, McGill University, 2003.
- [18] P. Tesson. An application of the Hales-Jewitt Theorem to multiparty communication complexity, 2004. See Gasarch’s Ramsey Website.
- [19] P. Tesson and D. Therien. Monoids and computations. *Int. J. of Algebra and Computation*, pages 115–163, 2004. www.cs.mcgill.ca/~ptesso.
- [20] P. Tesson and D. Therien. Complete classification of the communication complexity of regular languages. *TOCS*, pages 135–159, 2005.
- [21] I. Wegener. *Branching Programs and Binary Decision Diagrams: Theory and Application*. SIAM, 2000.

N	$r_3(3N)$	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
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
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

9 Appendix: Empirical Results

Gasarch and Glenn [8] produced tables of sizes of 3-free sets. The table below was produced using their software. The table gives n , a lower bound on $r_3(3N)$, $n = \lg N$, and $d(f_{3,T}) = 3 + \lceil \lg(\frac{6N \ln(3N)}{r_3(3N)} + 1) \rceil$ (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. We only show an excerpt of the table- the full table will be in the journal version.

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 fairly small.

10 Acknowledgments

We would like to thank Jozsef Solymosi, Paul Pudlak for refs; and Adam Bender, Walid Gomma, Dov Gordon, Jon Katz, Clyde Kruskal, Martin Ma, Matthew Mah, Brian Postow, and Arkady Yerukhimovich for proofreading.