An Exposition of an Upper Bound in Multiparty Communication Complexity
By William Gasarch

1 Introduction

Def 1.1 Let $f : \{\{0,1\}^n\}^k \rightarrow X$. Assume, for $1 \le i \le k$, 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. At the end of the protocol all parties must know the answer. 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 $d(f) \ll n$.

2 Connections Between Multiparty Comm. Comp. and Ramsey Theory

In this section we review the connections between the multiparty communication complexity of f and Ramsey Theory that was first established in [2].

Def 2.1 Let $c, T \in \mathbb{N}$. We think of $[T]$ as being $\{1, \ldots, T\}$ mod T.

1. A *proper c-coloring of* $[T] \times [T]$ is a function COL : $[T] \times [T] \rightarrow [c]$ such that there do not exist $x, y \in [T]$ and $\lambda \in [T-1]$ such that

$$\text{COL}\,(x,y) = \text{COL}\,(x+\lambda, y) = \text{COL}\,(x, y+\lambda)$$

   (all of the additions are mod T). Another way to look at this: 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 $\chi(T)$ be the least c such that there is a proper c-coloring of $[T] \times [T]$.

We will study the following function.

Def 2.2 Let $n \in \mathbb{N}$. Let $N(n) : \mathbb{N} \rightarrow \mathbb{N}$. We define $\text{MOD}_n^{N(n)}$ as follows.

$$\text{MOD}_n^{N(n)}(x,y,z) = \begin{cases} YES & \text{if } x+y+z \equiv 0 \pmod{N(n)} \\ NO & \text{if } x+y+z \not\equiv 0 \pmod{N(n)} \end{cases} \tag{1}$$

Note 2.3 Chandra, Furst, Lipton actually examined the function $\mathrm{EQ}_n^{N(n)}$ which is defined as

$$\mathrm{EQ}_n^{N(n)}(x,y,z) = \begin{cases} YES & \text{if } x+y+z = N(n) \\ NO & \text{if } x+y+z \neq N(n) \end{cases} \tag{2}$$

However, everything we do here is an easy modification of what they have done (unless otherwise noted).

Theorem 2.4 *Let $N(n) : \mathbb{N} \to \mathbb{N}$.*

1. $d(\mathrm{MOD}_n^{N(n)}) \leq \lg(\chi(N(n))) + O(1)$.
2. $d(\mathrm{MOD}_n^{N(n)}) \geq \lg(\chi(N(n)) + \Omega(1)$.

Proof:
1) Let COL be a proper c-coloring of $[N(n)] \times [N(n)]$. We represent elements of $[c]$ by $\lg(\chi(N(n))) + O(1)$ bit strings. P_1, P_2, P_3 will all know COL ahead of time. We present a protocol for this problem for which the communication is $2\lg(\chi(N(n))) + O(1)$. We will then show that it is correct.

1. P_1 has y, z. P_2 has x, z. P_3 has x, y.
2. P_1 calculates x' such that $x' + y + z \equiv 0 \pmod{N(n)}$. P_1 broadcasts $\sigma_1 =$ COL (x', y).
3. P_2 calculates y' such that $x + y' + z \equiv 0 \pmod{N(n)}$. P_2 broadcasts 1 if $\sigma_2 =$ COL (x, y'), 0 otherwise.
4. P_3 looks up $\sigma_3 =$ COL (x, y). P_3 broadcasts YES if $\sigma_1 = \sigma_2 = \sigma_3$ and NO otherwise. (We will prove later that these answers are correct.)

Claim 1: If $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$ then P_1, P_2, P_3 will all think $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$.

Proof: If $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$ then $x_1' = x_1$, $x_2' = x_2$, and $x_3' = x_3$. Hence $\sigma_1 = \sigma_2 = \sigma_3$
Therefore P_1, P_2, P_3 all think $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$.
End of proof of Claim 1.

Claim 2: If P_1, P_2, P_3 all think that $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$ then $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$.

Proof: Assume that P_1, P_2, P_3 all think $\mathrm{MOD}_n^{N(n)}(x,y,z) = YES$.
Hence

$$\text{COL } (x_1, x_2) = \text{ COL } (x_1', x_2) = \text{ COL } (x_1, x_2').$$

We call this **The Coloring Equation.**
Assume

$$x_1 + x_2 + x_3 \equiv \lambda \pmod{N(n)}.$$

We show that $\lambda \equiv N(n) \equiv 0 \pmod{N(n)}$.

By the definition of x_1'

$$x_1' + x_2 + x_3 \equiv 0 \pmod{N(n)}.$$

Hence

$$x_1' + x_1 + x_2 + x_3 - x_1 \equiv 0 \pmod{N(n)}.$$

$$x_1' - x_1 \equiv \lambda \pmod{N(n)}$$

$$x_1' \equiv x_1 + \lambda \pmod{N(n)}$$

By the same reasoning

$$x_2' \equiv x_2 + \lambda \pmod{N(n)}.$$

Hence we can rewrite The Coloring Equation as

$$\text{COL}\ (x_1, x_2) = \text{COL}\ (x_1 + \lambda, x_2) = \text{COL}\ (x_1, x_2 + \lambda).$$

Since COL is a proper coloring, $\lambda \equiv 0 \pmod{N(n)}$.

End of proof of Claim 2.

2) Let P be a protocol for $\text{MOD}_n^{N(n)}$. Let d be the maximum number of bits communicated. Note that the number of transcripts is bounded by 2^d. We use this protocol to create a proper 2^d-coloring of $[N(n)] \times [N(n)]$.

We define COL (x, y) as follows. First find z such that $x+y+z \equiv 0 \pmod{N(n)}$. Then run the protocol on (x, y, z). The color is the transcript produced.

Claim 3: COL is a proper coloring of $[N(n)] \times [N(n)]$.

Proof: Let $\lambda \in [N(n)]$ be such that

$$\text{COL}\ (x, y) = \text{COL}\ (x + \lambda, y) = \text{COL}\ (x, y + \lambda).$$

We denote this value $TRAN$ (for Transcript). We show that $\lambda \equiv 0 \pmod{N(n)}$.

Let z be such that

$$x + y + z \equiv 0 \pmod{N(n)}.$$

Since

$$\text{COL}\ (x, y) = \text{COL}\ (x + \lambda, y) = \text{COL}\ (x, y + \lambda).$$

We know that the following tuples produce the same transcript $TRAN$ (all arithmetic is mod $N(n)$):

- (x, y, z).
- $(x + \lambda, y, z - \lambda)$.
- $(x, y + \lambda, z - \lambda)$.

All of these input produce the same transcript $TRAN$ and this transcript ends with a YES. By an easy communication complexity Lemma the tuple $(x, y, z - \lambda)$ also goes to $TRAN$. Hence $x + y + z - \lambda \equiv 0 \pmod{N(n)}$. Since $x + y + z \equiv 0 \pmod{N(n)}$ we have $\lambda \equiv 0 \pmod{N(n)}$.
End of Proof of Claim 3 ▮

Note 2.5 The lower bound (in the genreal k case) can be used to get lower bounds on Branching Programs, which was the original motivation for the Chandra-Furst-Lipton paper. However, this exposition is only concerned with the upper bound.

3 Upper Bounds: Connection to 3-free Sets

We bound $\chi(N(n))$ and hence, by Theorem 2.4, bound $d(\text{MOD}_n^{N(n)})$.
We first find bounds on $\chi^*(N(n))$ which is the following.

Def 3.1 Let $c, T \in \mathbb{N}$. We think of $[T]$ as being $\{1, \ldots, T\}$ (*not* mod T).

1. A *proper' c-coloring of* $[T] \times [T]$ is a function COL $: [T] \times [T] \to [c]$ such that there do not exist $x, y, z \in [T]$ and $\lambda \in [T - 1]$ such that

$$\text{COL }(x, y, z) = \text{ COL }(x + \lambda, y, z) = \text{ COL }(x, y + \lambda, z) = \text{ COL }(x, y, z + \lambda)$$

   (all of the additions are NOT mod T). Another way to look at this: 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 $\chi^*(T)$ be the least c such that there is a proper' c-coloring of $[T] \times [T]$.

We will need the following definition from Ramsey Theory.

Def 3.2

1. A 3-AP is an arithmetic progression of length 3.

2. Let ψ_3^T be the minimum number of colors needed to color $\{1, \ldots, T\}$ such that there are no monochromatic 3-AP's.

3. A set $A \subseteq [T]$ is 3-*free* if there do not exist any 3-AP's in A.

4. Let $\mathrm{r}_3(T)$ be the size of the largest 3-free subset of $[T]$.

Lemma 3.3

1. $\chi^*(T) \le \psi_3^{3T}$.

2. There exists a constant c such that $\psi_3^T \le c\frac{T \log T}{\mathrm{r}_3(T)}$.

3. There exists a constant c such that $\chi^*(T) \le c\frac{T \log(T)}{\mathrm{r}_3(T)}$. (This follows from 1 and 2.)

Proof:

1) Let $c = \psi_3^{3T}$. Let COL' be a c-coloring of $[3T]$ with no monochromatic 3-AP's. Let COL be the following c-coloring of $[T] \times [T]$.

$$\text{COL }(x, y) = \text{ COL' }(x + 2y).$$

Assume, by way of contradiction, that COL is not a proper' c-coloring. Hence there exist $x, y, z \in [T]$ and $\lambda \neq 0$ such that

$$\text{COL }(x, y) = \text{ COL }(x + \lambda, y) = \text{ COL }(x, y + \lambda).$$

By the definition of COL the following are equal.

$$\text{COL' }(x + 2y) = \text{ COL' }(x + \lambda + 2y) = \text{ COL' }(x + 2\lambda + 2y)$$

Hence $x + 2y, x + 2y + \lambda, x + 2y + 2\lambda$ form a monochromatic 3-AP. which yields a contradiction.

2) Let $A \subseteq [T]$ be a set of size $r_k(T)$ with no 3-AP's. We use A to obtain a 3-free coloring of $[T]$. The main idea is that we use randomly chosen translations of A to cover all of $[T]$.

Let $x \in [T]$. Pick a translation of A by picking $t \in [T]$. The probability that $x \in A + t$ is $\frac{|A|}{T}$. Hence the probability that $x \notin A + t$ 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

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

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 T 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 3-APs. Note that it uses $\frac{T \ln T}{|A|} = O(\frac{T \log T}{\mathrm{r}_k(T)})$ colors. ∎

4 Three Free Sets

In this section we review two constructions of 3-free sets. Our notation will be to take them to be subsets of $\{1, \ldots, n\}$. In particular, $\mathrm{r}_3(n)$ will be the largest 3-free subset of $\{1, \ldots, n\}$. Do not confuse this n with the n we have used before.

We present constructions in order of how large a 3-free set they give us. This is not the same order they were discovered.

The following are trivial to prove; however, since we use it throughout the paper we need a shorthand way to refer to it:

Fact 4.1 *Let $x \le y \le z$. Then x, y, z is a 3-AP iff $x + z = 2y$.*

4.1 $\mathrm{r}_3(n) = \Omega(n^{0.63}$: The Base 3 Method

The following theorem appeared in [3] but they do not take credit for it; hence we can call it folklore.

Theorem 4.2 $\mathrm{r}_3(n) \ge n^{\log_3 2} \approx n^{0.63}$.

Proof:

$A_n = \{m \mid 0 \le m \le n$ and all the digits in the base 3 representation of m are in the set $\{0,1\}$ $\}$.

The following is a (large) subset of A_n: every number in base 3 of length $\lfloor \log_3 n \rfloor$ that only yas 0's and 1's. Hence

$$|A_n| \ge \Omega(2^{\log_3 n}) = \Omega(n^{\log_3 2}) \ge n^{0.63}.$$

We show that A_n is 3-free. Let $x, y, z \in A_n$ form a 3-AP. Let x, y, z in base 3 be $x = x_{k-1} \cdots x_0$, $y = y_{k-1} \cdots y_0$, and $z = z_{k-1} \cdots a_0$, By the definition of A_n, for all i, $x_i, y_i, z_i \in \{0,1\}$. By Fact 4.1 $x+z = 2y$. Since $x_i, y_i, z_i \in \{0,1\}$ the addition is done *without carries*. Hence we have, for all i, $x_i + z_i = 2y_i$. Since $x_i, y_i, z_i \in \{0,1\}$ we have $x_i = y_i = z_i$, so $x = y = z$. ∎

4.2 $\mathrm{r}_3(n) \ge \Omega(n^{1-\frac{c}{\sqrt{\lg n}}})$: The Sphere Methods

The result and proof in this section are a minor variant of what was done by Behrend [1, 4]. We will express the number in a base and put a condition on the representation so that the numbers do not form a 3-AP. It will be helpful to think of the numbers as vectors.

Def 4.3 Let $x, b \in \mathbb{N}$ and $k = \lfloor \log_b x \rfloor$. Let x be expressed in base b as $\sum_{i=0}^{k} x_i b^i$. Let $\vec{x} = (x_0, \ldots, x_k)$ and $|\vec{x}| = \sqrt{\sum_{i=0}^{k} x_i^2}$.

Behrend used digits $\{0, 1, 2 \ldots, d\}$ in base $2d + 1$. We use digits $\{-d, -d+1, \ldots, d\}$ in base $4d + 1$. This choice gives slightly better results since there are more coefficients to use. Every number can be represented uniquely in base $4d + 1$ with these coefficients. There are no carries since if $a, b \in \{-d, \ldots, d\}$ then $-(4d+1) < a + b < (4d+1)$.

We leave the proof of the following lemma to the reader.

Lemma 4.4 *Let* $x = \sum_{i=0}^{k} x_i(4d+1)^i$, $y = \sum_{i=0}^{k} y_i(4d+1)^i$, $z = \sum_{i=0}^{k} z_i(4d+1)^i$, *where* $-d \le x_i, y_i, z_i \le d$. *Then the following hold.*

1. $x = y$ *iff* $(\forall i)[x_i = y_i]$.
2. *If* $x + y = 2z$ *then* $(\forall i)[x_i + z_i = 2y_i]$

The set $A_{d,s,k}$ defined below is the set of all numbers that, when interpreted as vectors, have norm s (norm is the square of the length). These vectors are all on a sphere of radius $\sqrt{s}$. We will later impose a condition on k so that $A_{d,s,k} \subseteq [-n/2, n/2]$.

Def 4.5 Let $d, s, k \in \mathbb{N}$.

$$A_{d,s,k} = \left\{ x : x = \sum_{i=0}^{k-1} x_i(4d+1)^i \wedge (\forall i)[-d \le x_i \le d] \wedge (|\vec{x}|^2 = s) \right\}$$

Def 4.6 Let $d, s, m \in \mathbb{N}$.

$$B_{d,s,k} = \left\{ x : x = \sum_{i=0}^{k-1} x_i(4d+1)^i \wedge (\forall i)[0 < x_i \le d] \wedge (|\vec{x}|^2 = s) \right\}$$

Lemma 4.7 *Let* $n, d, s, k \in \mathbb{N}$.

1. $A_{d,s,k}$ *is 3-free.*
2. *If* $n = (4d+1)^k$ *then* $A_{d,s,k} \subseteq \{-n/2, \ldots, n/2\}$.

Proof: a) Assume, by way of contradiction, that $x, y, z \in A_{d,s,k}$ form a 3-AP. By Fact 4.1, $x + z = 2y$. By Lemma 4.4 $(\forall i)[x_i + z_i = 2y_i]$. Therefore $\vec{x} + \vec{z} = 2\vec{y}$, so $|\vec{x} + \vec{z}| = |2\vec{y}| = 2|\vec{y}| = 2\sqrt{s}$. Since $|\vec{x}| = |\vec{z}| = \sqrt{s}$ and $\vec{x}$ and $\vec{z}$ are not in the same direction $|\vec{x} + \vec{z}| < 2\sqrt{s}$. This is a contradiction.

b) The largest element of $A_{d,s,k}$ is at most

$$\sum_{i=0}^{k-1} d(4d+1)^i = d\sum_{i=0}^{k-1}(4d+1)^i = \frac{(4d+1)^k - 1}{2} = \frac{n-1}{2} \le n/2.$$

Similarly, the smallest element is $\ge -n/2$. ▮

Lemma 4.8 *For all d, s, k*

$$|A_{d,s,k}| = \sum_{m=0}^{k} \binom{k}{m} 2^m |B_{d,s,m}|.$$

Proof:

Define

$$A^m_{d,s,k} = \Big\{ x : x = \sum_{i=0}^{k-1} x_i (4d+1)^i \wedge (\forall i)[-d \le x_i \le d]$$

$$\wedge(\text{ exactly } m \text{ of the } x_i\text{'s are nonzero }) \wedge (|\vec{x}|^2 = s) \Big\}$$

Clearly $|A_{d,s,k}| = \sum_{m=0}^{k} |A^m_{d,s,k}|$.

Note that $|A^m_{d,s,k}|$ can be interpreted as first choosing m places to have non-zero elements (which can be done in $\binom{k}{m}$ ways), then choosing the absolute values of the elements (which can be done in $|B_{d,s,m}|$ ways) and then choosing the signs (which can be done in 2^m ways). Hence $|A^m_{d,s,k}| = \binom{k}{m} 2^m |B_{d,s,m}|$. So

$$|A_{d,s,k}| = \sum_{m=0}^{k} \binom{k}{m} 2^m |B_{d,s,m}|.$$

▮

Theorem 4.9 *There is a c such that* $\mathrm{r}_3(n) \ge \Omega(n^{1-\frac{c}{\sqrt{\lg n}}})$.

Proof:

Let d, s, k be parameters to be specified later. We use the set $A_{d,s,k}$ which, by Lemma 4.7, is 3-free. We seek values of d, k, s such that $|A_{d,s,k}|$ is large and contained in $[-n/2, n/2]$. Note that once k, d are set the only possibly values of s are $\{0, 1, \ldots, kd^2\}$.

A calculation shows that if $k \approx \sqrt{\lg n}$ and d is such that $n = (4d+1)^k$ then $\bigcup_{s=0}^{kd^2} |A_{d,s,k}|$ is so large that *there exists* a value of s such that $|A_{d,s,k}| \ge n^{1-\frac{c}{\sqrt{\lg n}}}$ for some value of c. Note that the proof is nonconstructive in that we do not specify s; we merely show it exists. ▮

5 The Upper Bound

We leave the following lemma to the reader.

Lemma 5.1 *For all $N(n)$ there is a constant c such that $\chi(N(n)) \le c\chi^*(N(n))$.*

Theorem 5.2 $d(\mathrm{MOD}_n^{N(n)}) =$

Proof: By Theorem 2.4

$$d(\mathrm{MOD}_n^{N(n)}) \le 2\lg(\chi(N(n))) + O(1).$$

By Lemma 5.1 there exists a constant c such that $\chi(N(n)) = c\chi^*(N(n))$. Hence

$$d(\mathrm{MOD}_n^{N(n)}) \le 2\lg(\chi^*(N(n))) + O(1).$$

By Lemma 3.3 there exists a constant c such that

$$\chi^*(N(n)) \le c\frac{N(n)\log(N(n))}{\mathrm{r}_3(N(n))} + O(1).$$

Hence

$$d(\mathrm{MOD}_n^{N(n)}) \le 2\lg\Big(\frac{N(n)\log(N(n))}{\mathrm{r}_3(N(n))}\Big) + O(1).$$

By Theorem 4.9 there exists a constant c such that

$$\mathrm{r}_3(N(n)) \ge \Omega(N(n)^{1-\frac{c}{\sqrt{\lg N(n)}}}).$$

Hence

$$d(\mathrm{MOD}_n^{N(n)}) \le 2\lg\Big(\frac{N(n)\log(N(n))}{\mathrm{r}_3(N(n))}\Big) + O(1).$$

∎

References

[1] 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.

[2] 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. `http://portal.acm.org/citation.cfm?id=808737`.

[3] P. Erdös and P. Turan. On some sequences of integers. *Journal of the London Mathematical Society*, 11(2):261–264, 1936. `http://jlms.oxfordjournals.org/`.

[4] R. Graham, B. Rothchild, and J. Spencer. *Ramsey Theory.* Wiley, 1990.