An Application of Ramsey Theory to in Multiparty Communication Complexity
Exposition By William Gasarch

1 Introduction

Multiparty communication complexity was first defined by Chandra, Furst, and Lipton [4] 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, 2], lower bounds on problems in data structures [2], time-space tradeoffs for restricted Turing machines [1], and unconditional pseudorandom generators for logspace [1].

All results in this paper are from [4] or can be easily derived from their techniques unless otherwise specified.

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 $d(f) \ll n$.

We will need the following lemmas about multiparty protocols. The first one is the $k=3$ case of the second one. We leave it for an exercise.

Lemma 1.3 *Let P be a multiparty protocol for a function $f : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \rightarrow X$.*

1. *Let $TRAN$ be a possible transcript of the protocol P. There exists $A_1, A_2, A_3 \subseteq \{0,1\}^n$ such that, for all $x_1, x_2, x_3 \in \{0,1\}^n$ the following holds: The protocol P on input (x_1, x_2, x_3) produces transcript $TRAN$ iff $(x_1, x_2, x_3) \in A_1 \times A_2 \times A_3$.*
2. *Let $x_1, x_2, x_3 \in \{0,1\}^n$, $\sigma_1, \sigma_2, \sigma_3 \in \{\{0,1\}^n\}^3$, $TRAN$ be a transcript. Assume that σ_1 has x_1 as its first element, σ_2 has x_2 as its second element, σ_3 has x_3 as its third element. (In symbols, if $*$ means we don't care about the element, then*

$$\begin{aligned} \sigma_1 &= (x_1, *, *) \\ \sigma_2 &= (*, x_2, *) \\ \sigma_3 &= (*, *, x_3). \end{aligned}$$

) Further assume that $\sigma_1, \sigma_2, \sigma_3$ all produces transcript $TRAN$. Then (x_1, x_2, x_3) produces transcript $TRAN$.

Lemma 1.4 *Let P be a multiparty protocol for a function $f : \{\{0,1\}^n\}^k \rightarrow X$.*

1. *Let $TRAN$ be a possible transcript of the protocol P. There exists $A_1, \ldots, A_k \subseteq \{0,1\}^n$ such that, for all $x_1, \ldots, x_k \in \{0,1\}^n$ the following holds: The protocol P on input $(x_1, \ldots, x_k)$ produces transcript $TRAN$ iff $(x_1, \ldots, x_k) \in A_1 \times \cdots \times A_k$.*

2. *Let $x_1, \ldots, x_k \in \{0,1\}^n$, $\sigma_1, \ldots, \sigma_k \in \{\{0,1\}^n\}^k$, $TRAN$ be a transcript. Assume that σ_i has x_i as its ith element. Further assume that each σ_i produces transcript $TRAN$. Then $(x_1, \ldots, x_k)$ produces transcript $TRAN$.*

We will study the following function.

Def 1.5 Let $n \in \mathbb{N}$. We define $\mathrm{EQ}_n^{2^n} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$ as follows (interpreting the three inputs as numbers in binary):

$$\mathrm{EQ}_n^{2^n}(x,y,z) = \begin{cases} YES & \text{if } x+y+z = 2^n \\ NO & \text{if } x+y+z \neq 2^n \end{cases} \tag{1}$$

We will first establish a connection between $d(\mathrm{EQ}_n^{2^n})$ and some concepts in Ramsey Theory. We will then use results from Ramsey Theory to obtain upper and lower bounds on $d(\mathrm{EQ}_n^{2^n})$. The lower bounds will be applied to obtain lower bounds on branching programs.

Here is what we will show.

1. $d(\mathrm{EQ}_n^{2^n}) \leq \sqrt{\log(2^n)} = \sqrt{n}$ (First proven by Chandra, Furst, Lipton [4].) (This is somewhat surprising since it would seem the best you could do is have Alice yell to Bob what her bits are.)

2. $d(\mathrm{EQ}_n^{2^n}) \geq \omega(1)$ (First proven by Chandra, Furst, Lipton [4].)

3. $d(\mathrm{EQ}_n^{2^n}) \geq \log\log\log 2^n + \Omega(1) = \log\log n + \Omega(1)$ (First proven by Beigel, Gasarch, Glenn [3].)

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 [4].

Def 2.1 Let $c, T \in \mathbb{N}$.

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

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

   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 $[T] \times [T]$.

Theorem 2.2 *Let* $2^n : \mathbb{N} \rightarrow \mathbb{N}$.

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

Proof:
1) Let COL be a proper c-coloring of $[2^n] \times [2^n]$. We represent elements of $[c]$ by $\lg(\chi(2^n)) + O(1)$ 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 $2\lg(\chi(2^n)) + O(1)$. 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 $x' + y + z = 2^n$. (If no such x' exists then output NO and thats the end of the protocol.) P_1 broadcasts $\sigma_1 =$ COL (x', y).
3. P_2 calculates y' such that $x + y' + z = 2^n$. (If no such y' exists then output NO and thats the end of the protocol.) P_2 broadcasts $\sigma_2 =$ COL (x, y').
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 $\mathrm{EQ}_n^{2^n}(x, y, z) = YES$ then P_1, P_2, P_3 will all think $\mathrm{EQ}_n^{2^n}(x, y, z) = YES$.

Proof: If $\mathrm{EQ}_n^{2^n}(x, y, z) = YES$ 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 $\mathrm{EQ}_n^{2^n}(x, y, z) = YES$.
End of proof of Claim 1.

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

Proof: Assume that P_1, P_2, P_3 all think $\mathrm{EQ}_n^{2^n}(x, y, z) = YES$.
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

$$x_1 + x_2 + x_3 = \lambda.$$

We show that $\lambda = 2^n$.
By the definition of x_1'

$$x_1' + x_2 + x_3 = 2^n.$$

Hence

$$x_1' + (x_1 + x_2 + x_3) - x_1 = 2^n.$$

$$x_1' + \lambda - x_1 = 2^n.$$

$$x_1' - x_1 = 2^n - \lambda$$

$$x_1' = x_1 + 2^n - \lambda$$

By the same reasoning

$$x_2' = x_2 + 2^n - \lambda.$$

Hence we can rewrite The Coloring Equation as

$$\text{COL}(x_1, x_2) = \text{COL}(x_1 + 2^n - \lambda, x_2) = \text{COL}(x_1, x_2 + 2^n - \lambda).$$

Since COL is a proper coloring, $2^n - \lambda = 0$, so $\lambda = 2^n$.
End of proof of Claim 2.

2) Let P be a protocol for $\text{EQ}_n^{2^n}$. 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 $[2^n] \times [2^n]$.

We define COL (x, y) as follows. First find z such that $x + y + z = 2^n$. Then run the protocol on (x, y, z). The color is the transcript produced.

Claim 3: COL is a proper coloring of $[2^n] \times [2^n]$.
Proof: Let $\lambda \in [2^n]$ 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 $\lambda = 0$.

Let z be such that

$$x + y + z = 2^n.$$

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 $TRAN$:

- (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 Lemma 1.3.2 the tuple $(x, y, z - \lambda)$ also goes to $TRAN$. Hence $x + y + z - \lambda = 2^n$. Since $x + y + z = 2^n$ we have $\lambda = 0$.
End of Proof of Claim 3 ▮

We now have a really odd situation. We have $d(\mathrm{EQ}_n^{2^n}) = \Theta(\lg(\chi(2^n)))$
YEAH: We we have upper and lower bounds that match up to a multiplicative constant!
BOO: We don't know that the function IS.
In the next two sections we get upper bounds and lower bounds on $\lg(\chi(2^n))$.

3 Upper Bounds

We need to properly color $[2^n] \times [2^n]$ and keep the number of colors down. We will prove lower bounds on $W(3, c)$ on the way there.

Def 3.1 A *3-free set* is a set with no 3-AP's.

If X is a 3-free set and $X \subseteq [T]$ then X could be a color in a c-coloring of $[T]$ that has no mono 3-AP's. How can we get the other colors?

4 Lower Bounds

4.1 An $\omega(1)$ Lower Bound for $d(\mathrm{EQ}_n^{2^n})$

We will need the following theorem from Ramsey Theory.

Theorem 4.1 *For all c there exists T such that, there are no proper c-colorings of $[T] \times [T]$.*

Theorem 4.1 can be proven several ways. We enumerate them:

1. This can be proven from van der Waerden's theorem.
2. This can be proven by the same techniques as van der Waerden's theorem.
3. This follows from the Galai-Witt Theorem. This generalizes to coloring $[T]^k$.
4. We will give a concrete lower bound (rather than $\omega(1)$) and is in Section 4.2. Other ways generalize to k variables.

Theorem 4.2 *If* $\lim_{n\to\infty} 2^n = \infty$ *then* $d(\mathrm{EQ}_n^{2^n}) = \omega(1)$.

Proof: By Theorem 2.2
$$d(\mathrm{EQ}_n^{2^n}) \ge \lg(\chi(2^n)) + \Omega(1).$$
Hence we need to show that $\chi(T)$ is not bounded by a constant (as T goes to infinity).

Assume, by way of contradiction, that there exists c such that, for all T, there is a proper c-coloring of $[T] \times [T]$. This contradicts Theorem 4.1. ∎

We will need to look at k-party protocols for the following function.
$\mathrm{MOD}_{n,k}^{2^n} : (\{0,1\}^n)^k \to \{0,1\}$

$$\mathrm{MOD}_{n,k}^{2^n}(x_1,\ldots,x_k) = \begin{cases} 1 & \text{if } \sum_{i=1}^k x_i = 2^n \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

The following can be proven in a manner similar to the $k = 3$ case.

Theorem 4.3 *Fix* k*. If* $\lim_{n\to\infty} 2^n = \infty$ *then* $d(\mathrm{MOD}_{n,k}^{2^n}) = \omega(1)$.

4.2 An $\Omega(\log\log\log 2^n)$ Lower Bound for $d(\mathrm{EQ}_n^{2^n})$

The following combinatorial lemma will allow us to prove a lower bound on $d(\mathrm{EQ}_n^{2^n})$. This lemma is a reworking of a theorem of Graham and Solymosi [5].

Lemma 4.4

1. $\chi(2^n) \ge \Omega(\log\log 2^n)$.
2. $d(\mathrm{EQ}_n^{2^n}) \ge \log\log\log 2^n + \Omega(1)$. *(This follows from part 1 and Theorem 2.2.)*

Proof: Assume that COL is a proper c-coloring of $[2^n] \times [2^n]$. We find sets $X_1, Y_1 \subseteq [2^n] \times [2^n]$ such that COL restricted to $X_1 \times Y_1$ uses $c-1$ colors. We will iterate this process to obtain X_c, Y_c such that COL restricted to $X_c \times Y_c$ uses 0 colors. Hence $|X_c| = 0$ which will yield $c = \Omega(\log\log\log 2^n) = \Omega(\log\log n)$.

For $0 \le s \le c$ we define X_s, Y_s, h_s, USED-COL$_s$.

1. $X_0 = Y_0 = [2^n]$. $h_0 = |X_0| = |Y_0| = 2^n$. USED-COL$_0 = [c]$.
2. Assume X_s, Y_s, h_s are defined and inductively USED-COL$_s = [c - s]$ (we will be renumbering to achieve this). Also assume that Partition $X_s \times Y_s$ (which is of size h_s^2) into sets P_a indexed by $a \in [2^n]$ defined by
$$P_a = \{(x,y) \in X_s \times Y_s \mid x + y = a\}.$$
(P_a is the ath anti-diagonal.) There exists an a such that $|P_a| \ge \lceil h_s^2/2^n \rceil$. There exists a color, which we will take to be $c - s$ by renumbering, such that at least $\lceil \lceil h_s^2/2^n \rceil / c \rceil$

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 $m = \lceil \lceil h_s^2/2^n \rceil /c \rceil$. Let $\{(x_1, y_1), \ldots, (x_m, y_m)\}$ be m elements of P_a such that, for $1 \le i \le m$, COL $(x_i, y_i) = c - s$. We will later show that, for all $i \ne j$, COL $(x_i, y_j) \ne c - s$.

3. Let

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

Note that for all $(x_i, y_j) \in X_{s+1} \times y_j \in Y_{s+1}$, $i < j$ hence $i \ne j$. Since we will show that for all $i \ne j$, COL $(x_i, y_j) \ne c - s$, we will have that, for all $(x, y) \in X_{s+1} \times y_j \in Y_{s+1}$, COL $(x, y) \ne c - s$.

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

$$x_j + y_j = a = x_i + y_i = x_j + y_i.$$

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 $i \ne j$, COL $(x_i, y_j) \ne c - s$.

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

$$\text{COL } (x_i, y_j) = \text{ COL } (x_i, y_i) = \text{ COL } (x_j, y_j) = c - s.$$

We want a $\lambda \ne 0$ such that $y_i = y_j + \lambda$ and $x_j = x_i + \lambda$. Using that $x_i + y_i = x_j + y_j = a$ we can take $\lambda = (x_j + y_i - a)$. The element $\lambda \ne 0$: if $\lambda = 0$ then one can show $y_i = y_j$, which contradicts Claim 1.

We now have

$$\text{COL } (x_i, y_j) = \text{ COL } (x_i + \lambda, y_j) = \text{ COL } (x_i, y_j + \lambda).$$

This violates COL being a proper coloring.

End of Proof of Claim 2

Note that, by Claim 2 above

$$\{ \text{ COL } (x, y) \mid x \in X_{s+1}, y \in Y_{s+1}\} \subseteq \text{ USED-COL}_{s+1}.$$

Look at what happens at stage c. $|X_c| = |Y_c| = h_c$ and COL restricted to $X_c \times Y_c$ uses 0 colors. The only way this is possible is if $h_c = 0$. We will see that this implies $c = \Omega(\log \log 2^n)$.

We have $h_0 = 2^n$ and

$$h_{s+1} = \left\lceil \left\lceil \left\lceil \frac{h_s^2}{2^n} \right\rceil /c \right\rceil /3 \right\rceil \geq \frac{h_s^2}{3c2^n}.$$

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

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

Base Case: $h_0 = 2^n \geq \frac{2^n}{(3c)^0} = 2^n$.

Induction Step: Assume $h_s \geq \frac{2^n}{(3c)^{2^s-1}}$. Since $h_{s+1} \geq (h_s)^2/3c2^n$ we have, by the induction hypothesis

$$h_{s+1} \geq (h_s)^2/3c2^n \geq \frac{\frac{(2^n)^2}{(3c)^{2^{s+1}-2}}}{3c2^n} \geq \frac{2^n}{(3c)^{2^{s+1}-1}}.$$

End of proof of Claim 3

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

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] 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. `http://www.cs.washington.edu/homes/beame/publications.html`.

[3] R. Beigel, W. Gasarch, and J. Glenn. The multiparty communication complexity of exact-t: improved bounds and new problems. In *Proceedings of the 31th International Symposium on Mathematical Foundations of Computer Science 2001,* Stara Lesna, Slovakia, pages 146–156, 2006.

[4] 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`.

[5] R. Graham and J. Solymosi. Monochromatic equilateral right triangles on the integer grid. *Topics in Discrete Mathematics, Algorithms and Combinatorics*, 26, 2006. `www.math.ucsd.edu/~/ron/06\_03\_righttriangles.pdf` or `www.cs.umd.edu/~/vdw/graham-solymosi.pdf`.