Discrete Mathematics and Theoretical Computer Science DMTCS vol. **13:4**, 2011, 15–22

Separating the k-party communication complexity hierarchy: an application of the Zarankiewicz problem

Thomas P. Hayes†

Department of Computer Science, University of New Mexico

received 18th February 2011, revised 20th October 2011, accepted 21st October 2011.

For every positive integer k, we construct an explicit family of functions $f : \{0,1\}^n \to \{0,1\}$ which has $(k+1)$-party communication complexity $O(k)$ under every partition of the input bits into $k+1$ parts of equal size, and k-party communication complexity $\Omega\left(\frac{n}{k^4 2^k}\right)$ under every partition of the input bits into k parts. This improves an earlier hierarchy theorem due to V. Grolmusz.

Our construction relies on known explicit constructions for a famous open problem of K. Zarankiewicz, namely, to find the maximum number of edges in a graph on n vertices that does not contain $K_{s,t}$ as a subgraph.

Keywords: communication complexity, extremal combinatorics, expander graphs

The "Number on the Forehead" model of multiparty communication complexity was introduced by Chandra, Furst, and Lipton [4]. In this model, k players, $P_1, \ldots, P_k$, use a communication protocol to collaboratively evaluate a function $f(x_1, \ldots, x_k)$ on a particular input. The components x_i of the input are written on the forehead of player P_i, so that each player sees the values of all components *except* his own. The players then take turns broadcasting strings of bits according to their protocol, at the end of which, all players must know the value of $f(x_1, \ldots, x_k)$.

We will show that there is a real difference in the computational power of k players and $k+1$ players in this model, by constructing explicit functions which are easy for $k+1$ players, and hard for k players. However, before we can begin to discuss this construction, we must first specify how a function of k input strings $x_1, \ldots, x_k$ is to be viewed as a function of $k+1$ input strings.

We think of f as a boolean function $f : \{0,1\}^n \to \{0,1\}$, whose n input bits are partitioned into k parts, and each part of the partition is assigned to a player, so that every bit is seen by exactly $k-1$ players. The communication complexity of a function may vary greatly depending on the partition chosen. Such partition models have already been studied (see, for instance, Kushilevitz and Nisan [12, Ch. 6–7]). Two different methods for defining the communication complexity in this context are:

†Email: `hayes@cs.unm.edu`.

- Worst-case partition: All possible partitions of the input into k parts are considered, and the complexity of f is the maximum of the various complexities.
- Best-case equipartition: All *equipartitions* of the input (partitions into k parts whose sizes differ by at most one) are considered, and the complexity of f is the minimum of the various complexities. (If there were no restriction on the sizes of the parts, the complexity would always be zero.)

Our separation result for the multiparty communication complexity hierarchy holds in the strongest possible sense: our lower bound holds for every equipartition (even the best), and our upper bound holds for every partition (even the worst).

Theorem 1 *Let $k \geq 2$. There exists an explicit family of functions $f : \{0,1\}^n \to \{0,1\}$ such that the $(k+1)$-party communication complexity of f is $O(k)$ under any partition, while the k-party communication complexity is $\Omega\left(\frac{n}{k^4 2^k}\right)$ under any equipartition.*

If k is fixed and $n \to \infty$, then this result is optimal up to constant factors:

Corollary 2 *For every fixed $k \geq 2$, there exists an explicit family of functions having k-party communication complexity $\Omega(n)$ under any equipartition of the inputs, and $(k+1)$-party communication complexity $O(1)$ under any partition of the inputs.*

Our results were inspired by the following result of Grolmusz [8], and by its proof.

Proposition 3 (Grolmusz [8]) *Let k and k' be fixed constants, such that there exists a prime $k < p \leq k'$. There exists an explicit family of functions having k-party communication complexity $\Omega(n)$ under some equipartition of the inputs, and k'-party communication complexity $O(1)$ under any partition of the inputs.*

We have improved this by removing the condition $k < p \leq k'$, and by extending the lower bound to hold for for arbitrary equipartitions.

Related Work

A number of other "communication complexity hierarchies" have been studied previously—see, for instance [14, 2, 9]. These include, for instance, hierarchies based on the number of rounds, and on communication complexity versions of standard complexity theory hierarchies.

Ďuriš *et al.* [6] recently proved a separation result in a two-player multi-partition model of communication complexity. Although their results have some interesting similarities to our own, there does not seem to be any real connection between the models.

Some unpublished notes of T. Pitassi [15] present substantially the same construction and results as ours. Although she has graciously conceded priority, we wish to acknowledge her independent discovery.

1 Preliminaries

In this section, we summarize the definitions and familiar results which form the building blocks of our construction. The family of functions we will construct is defined using a particular class of hypergraphs, which is in turn defined using Zarankiewicz graphs.

Definition 4 Let $\mathcal{H}$ be a hypergraph. The function $\mathrm{GIP}_{\mathcal{H}} : \{0,1\}^{V(\mathcal{H})} \to \{0,1\}$ is defined by

$$\mathrm{GIP}_{\mathcal{H}}(\vec{x}) := \sum_{e \in E(\mathcal{H})} \prod_{v \in e} x_v \pmod 2,$$

and is called the *generalized inner product over $\mathcal{H}$.*

Remark. The mapping $\mathcal{H} \mapsto \mathrm{GIP}_{\mathcal{H}}$ defines a bijection between the set of hypergraphs with vertex set V and the set of all functions $f : V \to \{0,1\}$. Indeed, the edges of $\mathcal{H}$ correspond to the monomial terms when $\mathrm{GIP}_{\mathcal{H}}$ is written as a multilinear polynomial over $GF(2)$.

The following observation has long been known, and has appeared in many contexts.

Observation 5 *If the largest edge in $\mathcal{H}$ contains $k-1$ vertices, then there is a k-party communication protocol evaluating $\mathrm{GIP}_{\mathcal{H}}$ using at most k bits of communication.*

Proof: By definition $\mathrm{GIP}_{\mathcal{H}}$ is a polynomial of degree at most $k-1$ over $GF(2)$. For each monomial, there exists a player who can evaluate it. Assign each monomial to the lowest index player who can evaluate it. Each player evaluates his assigned monomials, then takes their mod 2 sum, adds it to the previous communicated bit, if any, and broadcasts this bit as his message. $\Box$

When $\mathcal{H}$ is a perfect matching, $\mathrm{GIP}_{\mathcal{H}}$ is the usual inner product over $GF(2)$. More generally, when the edges of $\mathcal{H}$ are pairwise disjoint and of size k, $\mathrm{GIP}_{\mathcal{H}} = \mathrm{GIP}_k$ is the generalized inner product function of Babai, Nisan and Szegedy [3]. These authors showed showed that $C_k(GIP_k) = \Omega(n/4^k)$. Their result was improved by Chung and Tetali [5] to:

Proposition 6 *Let $\mathcal{H}$ be a k-uniform perfect matching on n vertices. Then*

$$C_k(\mathrm{GIP}_{\mathcal{H}}) = \Omega\left(\frac{n}{k2^k}\right).$$

Remark. A nearly-matching upper bound of $O(n/2^k)$ is due to Grolmusz [7].

Definition 7 If $\mathcal{H}$ is a hypergraph, and $S \subseteq V(\mathcal{H})$ is a set of vertices, then the *sub-hypergraph of $\mathcal{H}$ induced by S* is the hypergraph $\mathcal{G}$ with vertex set S and edge set $\{e \in E(\mathcal{H}) \mid e \subseteq S\}$.

Proposition 8 *If $\mathcal{G}$ is a vertex-induced sub-hypergraph of $\mathcal{H}$, as defined above, then $C(\mathrm{GIP}_{\mathcal{H}}) \geq C(\mathrm{GIP}_{\mathcal{G}})$.*

Proof: Observe that $\mathrm{GIP}_{\mathcal{G}}$ is the restriction of $\mathrm{GIP}_{\mathcal{H}}$ induced by setting $x_v = 0$ for all $v \in V(\mathcal{H}) - V(\mathcal{G})$. The result is immediate. $\Box$

We will use graphs with the following property in our construction.

Definition 9 Let G be a graph on n vertices, and let $c > 0$. We say G is *c-interconnected* if, for every pair of disjoint sets $S_1, S_2 \subset V$ such that $|S_1|, |S_2| \geq c$, there exists at least one edge from S_1 to S_2. In other words, the complement of G contains no $K_{c,c}$ subgraph.

Remark. Finding the minimum number of edges in a c-interconnected graph is a special case of a notoriously difficult question called the Zarankiewicz problem. This problem is normally phrased as, for positive integers s, t, to find the maximum number of edges in a graph containing no subgraph isomorphic to $K_{s,t}$. Our question is the complemented version of the case $s = t = c$. An explicit construction for the Zarankiewicz problem in the case $s \geq t!$ was found by Kollár, Rónyai and Szabó [10], using sophisticated methods from algebraic geometry. For the case $s = t = c \geq 3$, even the correct order of magnitude for the right answer is not known, and no explicit constructions approach the naive probabilistic bound below, which appears to be folklore.

Proposition 10 *Let G be a random graph on n vertices, with each possible edge independently included with probability $p > 0$. Then G is $(3\ln(n)/p)$-interconnected with probability at least $1 - n^{-3\ln(n)/p}$.*

Proof: The expected number, X, of sets S_1, S_2, of size $c = 3\ln(n)/p$ with no edges between them is

$$\mathbb{E}X = \binom{n}{c}\binom{n-c}{c}(1-p)^{c^2} < n^{2c}\mathrm{e}^{-pc^2} = n^{-3\ln(n)/p},$$

and the claimed result follows by Markov's inequality. □

For explicit constructions of c-interconnected graphs, we rely on explicit constructions of expanders. The best possible expanders are Ramanujan graphs (defined below). The first explicit constructions of these were by Lubotzky, Philips and Sarnak [11] and Margulis [13].

Definition 11 Let G be a d-regular graph on n vertices. Let $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of G. G is called a *Ramanujan graph* if all eigenvalues of G are in the set $\{-d, d\} \cup [-2\sqrt{d-1}, 2\sqrt{d-1}]$.

Remark. When G is connected and non-bipartite, it has a single largest eigenvalue in absolute value, so in this case, the $n-1$ other eigenvalues lie in $[-2\sqrt{d-1}, 2\sqrt{d-1}]$.

The Expander Mixing Lemma, (see, for instance, [1, Corollary 9.2.5]) implies that connected non-bipartite Ramanujan graphs are highly interconnected. We will make use of the following corollary; a proof is included for completeness.

Lemma 12 *Let G be a d-regular connected non-bipartite Ramanujan graph on n vertices. Then G is $\frac{2n}{\sqrt{d+1}}$-interconnected.*

Proof: Let $c = \frac{2n}{\sqrt{d+1}}$, and let $S, T \subset V(G)$ be disjoint sets of vertices such that $|S|, |T| \geq c$. Let $\mathbf{x_S}$ (resp. $\mathbf{x_T}$) be the characteristic vector of the set S (resp. T), with respect to some labelling of $V(G)$. Let A be the adjacency matrix of G, with respect to the same labelling. Then we easily see $m(S,T) = \mathbf{x_S}^t A \mathbf{x_T}$.

Let $d = \lambda_1 > \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_n$ be the eigenvalues of G, and let $\mathbf{v_1}, \ldots, \mathbf{v_n}$ be a corresponding orthonormal basis of eigenvectors. Let us express $\mathbf{x_S} = \sum_{i=1}^n \alpha_i \mathbf{v_i}$ and $\mathbf{x_T} = \sum_{i=1}^n \beta_i \mathbf{v_i}$ in this basis. With this notation, $m(S,T) = \mathbf{x_S}^t A \mathbf{x_T} = \sum_{i=1}^n \alpha_i \beta_i \lambda_i$.

It is easy to see that $\mathbf{v_1} = (1, 1 \ldots, 1)/\sqrt{n}$, from which we observe that $\alpha_1 = |S|/\sqrt{n}$ and $\beta_1 = |T|/\sqrt{n}$. We also note that $|S| = \|\mathbf{x_S}\|^2 = \sum_{i=1}^n \alpha_i^2$ and that $|T| = \|\mathbf{x_T}\|^2 = \sum_{i=1}^n \beta_i^2$.

Substituting, we have

$$\left| m(S,T) - \frac{|S||T|d}{n} \right| = \left| \sum_{i=2}^{n} \alpha_i \beta_i \lambda_i \right| \leq \sum_{i=2}^{n} |\alpha_i \beta_i| 2\sqrt{d-1}$$

By the Cauchy-Schwarz inequality,

$$\left(\sum_{i=2}^{n} |\alpha_i \beta_i| \right)^2 \leq \sum_{i=1}^{n} \alpha_i^2 \sum_{i=1}^{n} \beta_i^2 = |S||T|.$$

It follows that

$$\begin{aligned} m(S,T) &\geq \frac{|S||T|d}{n} - 2\sqrt{|S||T|(d-1)} \\ &= \sqrt{|S||T|(d-1)} \left(\frac{\sqrt{|S||T|}d}{n\sqrt{d-1}} - 2 \right) \\ &> \sqrt{|S||T|(d-1)} \left(\frac{c\sqrt{d+1}}{n} - 2 \right). \end{aligned}$$

By the definition of c, this last term is non-negative. Hence $m(S,T) > 0$, proving that G is c-interconnected. $\square$

Remark. Alon used the same analysis to give a somewhat stronger result, namely that, for somewhat larger sets S and T, the density of edges between S and T is always approximately the same as the density of edges in the entire graph G.

2 Results

The next two lemmas present surprising properties of c-interconnected graphs. These will be used in the proof of Theorem 1, but may also be interesting in their own right.

First, we find it convenient to generalize the concept of c-interconnectedness:

Definition 13 Let c be a positive integer. We say a graph $G = (V, E)$ is *c-starry* if the following holds. Let $S_1, S_2, \ldots, S_m \subset V$ be pairwise disjoint sets, each of size at least c. Then there exist vertices $v_1 \in S_1, v_2 \in S_2, \ldots, v_m \in S_m$ that form a star in G, i.e. there is an index $1 \leq j \leq m$ such that for all $i \neq j$, $(v_j, v_i) \in E$.

Remark. Every c-starry graph is c-interconnected, since we can let $m = 2$ in Definition 13. Surprisingly, the converse is also true:

Lemma 14 *Every c-interconnected graph G is c-starry.*

Proof: Let $G = (V, E)$ and let $S_1, S_2, \ldots, S_m \subset V$ be pairwise disjoint sets, each of size at least c.

For $1 \leq i \leq m$, let $T_i = V \setminus S_i \setminus \Gamma(S_i) = \{v \in V \setminus S_i \mid \forall w \in S_i, (v,w) \notin E\}$. By hypothesis, $|T_i| < c$, since G contains no edge from T_i to S_i. Hence

$$|\cup_i T_i| \leq (c-1)m < cm = |\cup_i S_i|,$$

so by the pigeonhole principle, there exists an element $v_j \in (\cup_j S_j) \setminus (\cup_i T_i)$, which is the center of the desired star. □

The following corollary is incidental to our main result, but may be of independent interest.

Corollary 15 *Let $G = (V,E)$ be a c-interconnected graph. Let T be any tree on m vertices, and denote $V(T) = \{t_1, \ldots, t_m\}$. Let $S_1, S_2, \ldots, S_m \subset V$ be pairwise disjoint sets such that for all i, $|S_i| \geq d_i c$, where d_i is the degree of t_i in T. Then there exist vertices $v_1 \in S_1, v_2 \in S_2, \ldots, v_m \in S_m$ such that if $(t_i, t_j) \in E(T)$, then $(v_i, v_j) \in E(G)$.*

The proof is a straightforward induction, which we omit. We are now ready to begin our construction.

Definition 16 Let $G = (V,E)$ be a graph. We define the *hypergraph of k-stars in G* to be the k-uniform hypergraph on vertex set V, whose edges are all k-tuples in which at least one vertex is adjacent to the other $k-1$.

Lemma 17 *Let $G = (V,E)$ be a c-interconnected regular graph of degree d on n vertices. Let $\mathcal{H}$ be the hypergraph of k-stars in G. Then, for any equipartition of V into k parts, there exists $S \subset V$, with $|S| > \frac{n-kc}{kd}$, such that the sub-hypergraph of $\mathcal{H}$ induced by S consists of pairwise disjoint edges, each of which intersects all k parts nontrivially.*

Proof: We define S recursively. Initially, let S be empty. In each stage, apply Lemma 14 to find a star having one vertex in each set of the partition. Add these k vertices to S. Delete the k vertices, and all their neighbors, from G. Repeat, restricting the given partition to the remaining vertices of G.

After i stages, at most ikd vertices have been removed from G, which means each set in the partition still has size at least $n/k - ikd$. Since G is c-interconnected, Lemma 14 will apply as long as $n/k - ikd \geq c$. Thus, the algorithm will run for at least $(n-kc)/(k^2 d)$ stages.

Because $\mathcal{H}$ is k-uniform, and at each stage we removed all neighbors of the k vertices added, the sub-hypergraph induced by S contains only one edge for each stage, and these are pairwise disjoint. □

Lemma 18 *Let $G = (V,E)$ be a c-interconnected regular graph of degree d on n vertices. Let $\mathcal{H}$ be the hypergraph of k-stars in G. Then, for any equipartition of the inputs into k parts,*

$$C_k(\mathrm{GIP}_{\mathcal{H}}) = \Omega\left(\frac{n-kc}{k^2 d 2^k}\right).$$

But the $k+1$-party communication complexity is at most $k+1$, regardless of how the inputs are partitioned.

Proof: By Lemma 17, $\mathcal{H}$ contains a sub-hypergraph $\mathcal{G}$ of $\Omega\left(\frac{n-kc}{kd}\right)$ vertices, such that $\mathrm{GIP}_{\mathcal{G}}$ is exactly the original GIP function of Babai, Nisan and Szegedy [3]. By Propositions 8 and 6,

$$C_k(\mathrm{GIP}_{\mathcal{H}}) \geq C_k(\mathrm{GIP}_{\mathcal{G}}) = \Omega\left(\frac{n-kc}{k^2 d 2^k}\right).$$

The upper bound for $k+1$ players follows directly from Proposition 5. □

Theorem 19 *Let G be a Ramanujan graph of degree $d \approx 16k^2$. Let $\mathcal{H}$ be the hypergraph of k-stars in G. Then for any partition of the inputs into k equal parts,*

$$C_k(\mathrm{GIP}_{\mathcal{H}}) = \Omega\left(\frac{n}{k^4 2^k}\right).$$

But the $k+1$-party communication complexity is at most $k+1$, regardless of how the inputs are partitioned.

Proof: This follows from composing Lemmas 12 and 18. □

Theorem 19 implies Theorem 1.

3 Conclusions and Open Questions

Although it is intuitive that adding more players can reduce communication complexity, the amount gained is not clear. We have seen that, for $O(1)$ players, adding just one player to the game can cause the communication complexity to plummet from $\Omega(n)$ to $O(1)$; this is the most that could be hoped for. However, what if k is a non-constant function of n?

A simple counting argument shows that, for a randomly chosen boolean function of kn variables, the k-party communication complexity is $\Omega(n)$ with high probability, regardless of the dependence of k on n.

In stark contrast, no explicit family of boolean functions has been shown to have $\omega(\log n)$ communication complexity for $k = \omega(\log n)$ players. Even for weaker models of communication such as the Simultaneous Messages model (cf. [12]), no such construction is known. To narrow this gap even slightly is one of the major challenges in communication complexity theory today.

For the question of separating the k-party communication hierarchy, we do not even know of a *non-constructive* proof that the k-player versus $(k+1)$-player separation extends beyond $k = O(\log n)$ players, in either the best-case or the worst-case partition models. An answer to this question would be welcome.

References

[1] N. Alon and J.H. Spencer. *The probabilistic method, 2nd Ed*. John Wiley & Sons, New York, 2000.

[2] L. Babai, P. Frankl, and J. Simon. *Complexity classes in communication complexity theory.* In: Proceedings of the 27th IEEE FOCS (1986) 337–347.

[3] L. Babai, N. Nisan, and M. Szegedy. *Multiparty Protocols, Pseudorandom Generators for Logspace and Time-Space Trade-offs.* Journal of Computer and System Sciences **45** (1992) 204–232.

[4] A.K. Chandra, M.L. Furst, and R.J. Lipton. *Multiparty Protocols.* In: Proceedings of the 15th ACM STOC (1983) 94–99.

[5] F.R.K. Chung and P. Tetali. *Communication complexity and quasi randomness.* SIAM J. Discrete Math. **6** (1993) 110–123.

[6] P. Ďuriš, J. Hromkovič, S. Jukna, M. Sauerhoff, and G. Schnitger. *On Multi-Partition Communication Complexity.* Information and Computation **194** (2004) 49–75.

[7] V. Grolmusz. *The BNS Lower Bound for Multi-Party Protocols is Nearly Optimal.* Information and Computation **112** (1994) 51–54.

[8] V. Grolmusz. *Separating the Communication Complexities of MOD m and MOD p Circuits.* Journal of Computer and System Sciences **51** (1995) 307–313.

[9] J. Hromkovič, J. Kari, and L. Kari. *Some hierarchies for the communication complexity measures of cooperating grammar systems.* Theoretical Computer Science **127** (1994), 123–147.

[10] J. Kollár, L. Rónyai, and T. Szabó. *Norm-Graphs and Bipartite Turán Numbers.* Combinatorica **16**(1996) 399–406.

[11] A. Lubotzky, R. Phillips, R., and P. Sarnak. *Ramanujan graphs.* Combinatorica **8** (1988) 261–277.

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

[13] G. A. Margulis. *Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators.* Problems of Information Transmission **24** (1988), 39–46.

[14] C. H. Papadimitriou and M. Sipser. *Communication Complexity.* J. Computer and System Sciences **28** (1984), 260–269.

[15] T. Pitassi. *Best-Partition Multiparty Communication Complexity.* Course notes for Foundations of Communication Complexity, Fall 2009. Manuscript online at `http://www.cs.toronto.edu/~toni/Courses/CommComplexity/Papers/bestpartition.ps`