UNIVERSITÄT TRIER
Mathematik / Informatik

Forschungsbericht Nr. 95–11

On communication games with more than two players

Stasys Jukna

Electronic copies of technical reports are available:

Via FTP: Host ftp.informatik.uni-trier.de, directory /pub/reports

Via gopher: Host gopher.informatik.uni-trier.de, port 70, type 1, pathes 1/TechReports/Abstracts and 1/TechReports/FullText

Via WWW: URL http://www.informatik.uni-trier.de/Reports/List

Via email: Send a mail to ftpmail@ftp.informatik.uni-trier.de, subject 'MAIL ME CLEAR', body 'TechReports.HowTo' followed by an empty line, for detailed instructions

Printed copies:

Trierer Forschungsberichte
Fachbereich IV -
Mathematik / Informatik
Universität Trier
D-54286 Trier

ISSN 0944-0488

ON COMMUNICATION GAMES WITH MORE THAN TWO PLAYERS

STASYS JUKNA[1 2]

Abstract. A *k-player game* is a communication game between k parties, each of which has an access to a half of input bits. 2-player games were introduced by Yao (1981) and are known as best-partition two-party games. We first describe a lower bounds argument for this case, based on computing the *term-rank* and *clique-number* of communication matrices. Using this argument we exhibit an explicit function on n variables such that any 2-players protocol for it requires $\Omega(\sqrt{n})$ bits of communication, whereas 3 players need to communicate only constant number of bits. We then consider another restriction: we allow any number of players but require that every singular input bit is accessable to $\leq k$ of these players. We prove that, for small values of k, no such protocol can recognize codewords of some linear codes of length n using less than $\Omega(\sqrt{n})$ bits of communication.

1. Introduction

A communication game is specified by a family (called the *support* of the game) $\mathcal{F} = \{S_1, \ldots, S_t\}$ of subsets of $[n] = \{1, \ldots, n\}$. To avoid the trivial cases we suppose that $S_i \not\subseteq S_j$ and $|S_i| \leq n-1$ for all $1 \leq i \neq j \leq t$. There are t players - one for each set in $\mathcal{F}$ - who wish to evaluate a Boolean function $f(x_1, \ldots, x_n)$. Each player knows the function f and has unlimited computational power. The only restriction is that the i-th player can see only arguments x_j with $j \in S_i$. They share a blackbord, viewed by all players, where they can exchange messages. The objective is to minimize the number of bits written on the board. The game proceeds in rounds. In each round

[1]Research supported by DFG-project Me 1077/5-2.

some player writes a string of bits on the board. The last bit written is the outcome of the game and should be $f(x_1,\ldots,x_n)$. The *protocol* specifies which player does the writing and what is written in each round. The *cost* is the number of bits written on the board for the worst case input. The *communication complexity* of f w.r.t. $\mathcal{F}$, denoted $\mathtt{cc}_{\mathcal{F}}(f)$, is the minimal cost of an $\mathcal{F}$-protocol that computes f. Different families $\mathcal{F}$ define different games.

1. *Fixed-partition* game of Abelson (1978) and Yao (11979) when $\mathcal{F}$ consists of one *fixed* partition of $[n]$ into two equal parts.

2. *Best-partition* game of Yao (1981) when $\mathcal{F}$ can be *any* partition of $[n]$ into two equal parts. Only few lower bounds are known for this game.

3. *Card game* of Edmonds & Impagliazzio (1994) when $\mathcal{F}$ contains only sets $S \subseteq [n]$ that $i \in S \iff i + \frac{n}{2} \notin S$. Impressing upper bound $\mathtt{cc}_{\mathcal{F}}(f) \leq (\log n)^2$ was obtained by Pudlák & Sgál (1995) for the Sequence Equality function. (This function is hard for the fixed-partition model and is easy in the best-partition model). No non-trivial lower bounds are known for card games.

4. *k-Party* game of Chandra, Furst & Lipton (1983). The support $\mathcal{F}$ of this game is defined as follows: fix a partition of $[n]$ into k mutually disjoint blocks $B_1,\ldots,B_k$, each of cardinality n/k, and let $\mathcal{F} = \{S_1,\ldots,S_k\}$ where $S_i = B_1 \cup \ldots \cup B_{i-1} \cup B_{i+1} \cup \ldots B_k$. Thus, the i-th player can see all the input bits exept those in the block B_i. No non-trivial lower bounds are known here for $k \geq \log n$. Best remains an $\Omega\left(n/c^k\right)$ lower bound of Babai, Nissan & Szegedy (1992).

In this paper we consider the following two types of games

- *k-player game* when $\mathcal{F}$ consists of k subsets of $[n]$, each of cardinality $\frac{n}{2}$. (Thus, we get k-player game from the card game if we relax the condition $i \in S \iff i + \frac{n}{2} \notin S$ to $|S| = \frac{n}{2}$.) For $k = 2$ this is exactly the best-partition game of Yao (1981).

- *degree-k game* when $\deg(\mathcal{F}) \leq k$ where $\deg(\mathcal{F}) = \max\{|\mathcal{F}'| : \mathcal{F}' \subseteq \mathcal{F}, \cap\mathcal{F}' \neq \emptyset\}$ is the maximum number of sets in $\mathcal{F}$ containing a common point. Put otherwise, the only restriction is that every input bit is accessable to at most k players.

In Section 2 we describe a lower bounds argument for the 2-players games, i.e. for the case of best-partition two-party games. The argument is very simple and is based on the *term-rank* and *clique-number* of communication matrices. In Section 3 we establish an exponential gap in communication complexity between 2-player and 3-player games: we exhibit an explicit function on n variables such that any 2-players protocol for it requires $\Omega(\sqrt{n})$ bits of communication, whereas 3 players, each seeing only half of inputs, need to communicate only *constant* number of bits. In Section 4 we prove that bounded-degree protocol cannot recognize codewords of some linear codes of length n using less than $\Omega(\sqrt{n})$ bits of communication.

2. Lower bounds for 2-player games

In this section we consider 2-players game. As pointed above, this is exactly the best-partition model introduced by Yao (1981) where he proved a $\Omega(n)$ lower bound for graph isomorphism [3] and rised the problem of proving lower bounds for other functions, noting that this "seems to be a difficult problem in general". Ja'Ja' (1984) proved $\theta(\sqrt{n}\log n)$ bound for the function which outputs all the connected components in the input graph. His methods do not seem to work for decision problems. Papadimitriou & Sipser (1984) proved that $\Omega(n)$ bits are necessary to recognize triangle-free graphs. This was the first result showing that in the best-partition model (unlike the fixed-partition case) non-determinism has an exponential power. Hajnal, Maass & Turán (1988) proved the bound $\Omega(\sqrt{n}\log n)$ for connectivity, s-t–connectivity and bipartitness properties of graphs. Krause, Meinel & Waack (1992) have proved the bound $\Omega(\sqrt{n})$ for the s-t–connectivity restricted to degree-1 graphs.

All these proofs follow one general schema: they reduce the lower bounds problem for the best partition model to that in the fixed partition model where the lower bound is easy. The reduction step in all these proofs requires non-trivial combinatorics: the Ramsey like combinatorial lemma about bicolored graphs in (Papadimitriou & Sipser 1984), the Regularity Lemma of Szemeredi in (Hajnal *et al.* 1986) and the Ramsey-type lemma about triangles in (Krause *et al.* 1992). Using these facts, the desired lower bounds are obtained via reduction to the set disjointness or to sequence equality problems.

Bellow we describe a lower bounds argument[4] which may be of independent interest.

[3]Throughout for graph problems, n is the number of edges, not vertices

[4]This argument was actually used in (Jukna 1987) to get lower bounds for alteranting switching networks.

Instead of reducing the lower bounds problem to the fixed-partition case (as it is done in all lower bound proofs mentioned above), we reduce the problem to the computation of two combinatorial characteristics – term rank and clique number – of $(0,1)$-matrices. We demonstrate the method by lower bounds on several explicit functions.

For a $(0,1)$ matrix A, let $\kappa(A)$ denote the minimal number of (not necessarily disjoint) all-1 submatrices of A covering all 1's in A. In particular, $\kappa(A) \geq \frac{|A|}{w(A)^2}$ where $|A|$ is the number of 1's in A and $w(A)$ denotes the maximum number of 1's in a line (row or column) of A. It is a folklore that for every partition $\mathcal{F} = \{S, T\}$, $\mathsf{cc}_{\mathcal{F}(f)} \geq \log_2 \kappa\left(A_{f,\mathcal{F}}\right)$, where $A_{f,\mathcal{F}} = \{f(a, \beta)\}$ with $a \in \{0,1\}^S$ and $\beta \in \{0,1\}^T$, is the standard (0,1) matrix, called a *communication matrix* of f.

We will use another characteristic of $(0,1)$ matrices to bound their communication complexity. The *term-rank* $tr(A)$ of A is the maximum number t such that A contains t entries equal 1, no two of which lie on the same line (row or column) of A. The *clique-number* of A, $cl(A)$, is the maximum number k such that A has a $k \times k$-submatrix, with all entries equal 1. The fraction $\rho(A) = tr(A)/cl(A)$ is the *cover number* of A. Since we clearly need at least $tr(A)/cl(A)$ all-1 submatrices to cover all the 1's lying in different lines and defining the term-rank of A, it follows that $\kappa(A) \geq \rho(A)$, which gives the lower bound $\mathsf{cc}_{\mathcal{F}}(f) \geq \log \rho\left(A_{f,\mathcal{F}}\right)$. The lower bound becomes even more tractable if one uses the estimate

$$\rho(A) \geq \frac{|A|}{w(A) \cdot cl(A)}. \tag{1}$$

This estimate follows immediately from the classical result of König-Egervary saying that the term-rank of a $(0,1)$ matrix A is exactly the minimum number of lines covering all 1's in A.

The main advantage of using the product $w(A) \cdot cl(A)$ instead of $w(A)^2$ is that now we have to consider only *square* submatrices. Sometimes $cl(A) \ll w(A)$ (see e.g. the bound in Section 3), which gives non-trivial lower bounds also in the cases where the bound $|A|/w(A)^2$ is trivial.

3. Three players versus two

In this section we exhibit a Boolean function g_n on n variables such that: any 2-players protocol for f requires $\Omega(\sqrt{n})$ bits, whereas 3 players, each seeing only half of inputs, can compute g_n with only $O(1)$ bits of communication.

Let $n = q^2$ where $q \geq 2$ is a prime power. Let $X = \{x_{u,v}\}$ be the set of k Boolean variables labeled by the pairs of elements of the field $\mathbf{F}_q$. Consider the Boolean function $g_n(X)$ whose value is 1 if and only if there exists a polynomial p of degree at most $d = q/2 - 1$ over $\mathbf{F}_q$ such that for all $u, v \in \mathbf{F}_q$, $x_{u,v} = 1 \iff v = p(u)$. Put otherwise, given a subset M of points in the plane $\mathbf{F}_q \times \mathbf{F}_q$, $g_n(M) = 1$ iff M is exactly the graph of some degree $\leq d$ polynomial over $\mathbf{F}_q$.

Theorem 1. *Three players, each seeing only half of inputs, can compute g_n with only $O(1)$ bits of communication. Any 2-players protocol for g_n requires at least $\sqrt{n}/2$ bits of communication.*

Upper bound. Recall that inputs for g_n are $q \times q$ matries X over $GF(q)$. Take $\mathcal{F} = \{S, T, U\}$ where S (T) consists the first (last) $d + 1$ columns of X (recall that $d = q/2 - 1$), and U consists of $d + 1$ columns in the middle of X. Thus, we have 3 players, one for each of these sets. Given a $(0, 1)$ matrix X, every player checks if he can draw exactly one polynomial of degree $\leq d$ throw all the 1's in the part he can see, and responds a one–bit answer. If X was a graph of some polynomial then all they write "yes'. If not, then at least one of the players must answer "no" since parts of graphs they see have only one extension (because we consider only polynomials of degree $\leq d < |S| = |T| = |U|$). ▯

Lower bound. Take an optimal best-partition protocol for g_n, and let $\mathcal{F} = \{S, T\}$ be the corresponding partition of inputs. The corresponding communication matrix $A = A_{\mathcal{F}, g_n}$ has exactly q^{d+1} ones. We have only to estimate the cover number $\rho(A)$.

Let us first estimate $w(A)$, i.e. the maximum number of $1'$s in a line of A. Put otherwise, we must answer the following question. Suppose we have set to constants a half of entries in the matrix X. In how many ways we can set the remaining $n/2$ entries of X so that g_n outputs 1 on the resulting $(0,1)$ matrix? Since our polynomials have degree at most d, this number of ways is clearly at most $\max\{0, q^{d+1-t}\}$ where t is the number of 1's in the first assignment. For $t = 0$ this upper bound on $w(A)$ becomes trivial, and we need better bound. We will show that actually

$$w(G) \leq \left(\frac{q}{2}\right)^{d+1}. \tag{2}$$

To prove this, take an arbitrary assignment $a \in \{0,1\}^S$ of constants to variables in S. Set $\phi(t) := \left(\frac{n}{2(q-t)}\right)^{d+1-t}$. We will prove that there are at most $\phi(|a|)$ assignments $b \in \{0,1\}^T$ of constants to the remaining variables for which $g_n(a,b) = 1$, where $|a|$ is the number of $1'$s in a.

Indeed, if $w(A) = 0$ then we are done, so assume that there is at least one $b \in \{0,1\}^T$ for which $g_n(a,b) = 1$. Let $t = |a|$. If $t \geq d+1$, then $g_n(a,b) = 1$ for at most one b. Suppose now that $0 \leq t \leq d$ and let $C_1, \ldots, C_l$ be those columns of X, no entry of which was set by a to 1. In every column of X the assignment a can set to 1 at most one entry (since otherwise we would have no extensions), hence $l = q - t$. For $i = 1, \ldots, q-t$, let s_i denote the number of entries in the i-th column C_i which a leaves unassigned. Assume w.l.o.g. that $s_1 \leq \ldots \leq s_{q-t}$. Set $r = d+1-t$, and let $h(s_1, \ldots, s_r)$ be the number of all r-tuples $(j_1, \ldots, j_r)$ with $1 \leq j_i \leq s_i$, for $i = 1, \ldots, r$. Since $|a| + r = d+1$, this number $h(s_1, \ldots, s_r)$ is an upper bound for the number of possible b for which $g_n(a,b) = 1$. On the other hand, we know that $s_1 + \cdots + s_{q-t} \leq n/2$, so h achieves its maximum on $s_1 = \ldots = s_r = \frac{n}{2(q-t)}$, and this maximum is equal $\phi(t)$. Thus, $w(A) \leq \max_{0 \leq t \leq n/2} \phi(t) = \phi(0) = (q/2)^{d+1}$, which completes the proof of (2).

Next, observe that for our concrete matrix A, we have that $cl(A) = 1$. Indeed, if $cl(G) \geq 2$ then there are vectors $a \neq a' \in \{0,1\}^S$ and $b \neq b' \in \{0,1\}^T$ such that $g_n(a,b) = g_n(a,b') = g_n(a',b) = g_n(a',b') = 1$. Assume w.l.o.g. that $|a| \geq |b|$. Then $|a| \geq q/2 = d+1$, which means that $g_n(a,b) = 1$ for at most one b, a contradiction.

By (2) and (1) [5] we conlcude that every $\mathcal{F}$-protocol for g_n requires at least $\log \rho(A) \geq \log |A| - \log w(A) \geq d+1 = \sqrt{n}/2 + 1$ bits of communication. ▯

[5] If we would try to apply the standard estimate $\kappa(G) \geq |A|/w(A)^2$ we would get only trivial lower bound since $q^{d+1}\left(\frac{q}{2}\right)^{-2(d+1)} \leq 1$ for $q \geq 4$.

4. A lower bound for linear codes

In this section we prove that many players cannot compute linear codes with few bits of communication if each of input bits is accessable to relatively small number of players.

Recall that a linear (n, m, d)-*code* is an $(n-m)$–dimensional subspace $C \subseteq \mathbf{F}_2^n$ (thus, $|C| = 2^{n-m}$), the Hamming distance between any two vectors of which is at least $2d+1$. A boolean function $f : \{0,1\}^n \to \{0,1\}$ is an (n, m, d) *code* function if $f^{-1}(1)$ is a linear (n, m, d) code.

For a family of sets $\mathcal{F}$, its *rank*, $\mathrm{rk}(\mathcal{F})$, is the maximum cardinality of a set in $\mathcal{F}$, and the *degree*, $\deg(\mathcal{F})$, is the maximum number of sets in $\mathcal{F}$ containing a common point, i.e. $\deg(\mathcal{F}) = \max\{|\mathcal{F}'| : \mathcal{F}' \subseteq \mathcal{F}, \cap\mathcal{F}' \neq \emptyset\}$. Note that small-degree families cannot be too large, namely, we always have that

$$|\mathcal{F}| \leq \frac{n \cdot \deg(\mathcal{F})}{\mathrm{rk}(\mathcal{F})}.$$

THEOREM 2. *Let f be a linear (m, n, d) code function. Then for every family $\mathcal{F} \subseteq 2^{[n]}$, any $\mathcal{F}$-protocol computing f requires at least*

$$d \log\left(\frac{\alpha\beta n^2}{d^2}\right) - m$$

bits of communication, where

$$\alpha = \alpha(\mathcal{F}) = \binom{|\mathcal{F}|}{k}^{-1} \qquad \textit{and} \qquad \beta = \beta(\mathcal{F}) = 1 - \frac{\deg(\mathcal{F}) \cdot \mathrm{rk}(\mathcal{F})}{n}.$$

Using the same argument as in (Jukna 1995, Lemma 4) one can easily reduce any $\mathcal{F}$-protocol to a protocol with only two (overlaping!) players S and T such that $|S \setminus T| \geq \alpha(\mathcal{F})n$ and $|T \setminus S| \geq \beta(\mathcal{F})n$. Thus, Theorem 2 follows directly from the the following lemma.

4.1. Lower bound for two overlaping players.

LEMMA 3. *Let f be (n, m, d) linear code function and let $\mathcal{F} = \{S, T\}$ with $S, T \subseteq [n]$, $s = |S \setminus T|$ and $t = |T \setminus S|$. Then any $\mathcal{F}$-protocol (i.e. any 2-player protocol, where Player 1 sees only bits in S and Player 2 sees only bits in T), requires $\geq d \log \frac{st}{d^2} - m$ bits of communication.*

Proof. We reduce the problem to the case of *disjoint* players. Namely, there is an assignment $\alpha \to S \cap T$ of constants to the common part $S \cap T$, so that the resulting set $C := f_\alpha^{-1}(1) \subseteq \{0,1\}^{(S\setminus T)\cup(T\setminus S)}$ still has the following two properties: (i) $|C| = 2^{n-r-m}$ where $r = |S \cap T|$, and (ii) the Hamming distance between any two vectors in C is at least $2d+1$.

After the assignment α we actually have a 2 player protocol for the subfunction f_α: Player 1 can see the bits in $S \setminus T$ and Player 2 the bits in $T \setminus S$. Recall that $|S \setminus T| = s$ and $|T \setminus S| = t$. The corresponding communication matrix $A = \{f_\alpha(u,v)\}$ has $|C| = 2^{n-r-m}$ ones. From Section 2 we know that any $\{S \setminus T, T \setminus S\}$-protocol computing f_α requires at least

$$\log \kappa(A) \geq \log |C| - \log sq(A)$$

bits of communication, where $sq(A)$ is the maximum of $u \cdot v$ over all monochromatic (i.e. "all-1") $u \times v$ submatrices of A.

For any fixed vector $a \in \{0,1\}^{S\setminus T}$, there are at most $L_1 := 2^t / \sum_{i=0}^{d} \binom{t}{i} < 2^t / \left(\frac{t}{d}\right)^d$ vectors $b \in \{0,1\}^{T\setminus S}$ for which $f_\alpha(a,b) = 1$ (since the Hamming distance between any two such vectors b must be at least $2d+1$). Similary, for any fixed vector $b \in \{0,1\}^{T\setminus S}$, there are at most $L_2 := 2^s / \sum_{i=0}^{d} \binom{s}{i} < 2^s / \left(\frac{s}{d}\right)^d$ vectors $a \in \{0,1\}^{S\setminus T}$ for which $f_\alpha(a,b) = 1$ Thus $sq(A) \leq L_1 \cdot L_2 \leq 2^{t+s} / \left(\frac{s \cdot t}{d^2}\right)^d$, and (since $s + t = n - r$) we get

$$\log \kappa(A) \geq n - r - m - \log sq(A) \geq d \log \frac{s \cdot t}{d^2} - m$$

as desired. ▯

For Bose-Chaudhury codes (BCH-codes) Theorem 2 yields the following lower bound. Recall, that for any $d \leq n/2 - 1$ there is a BCH-code $C \subseteq \mathbf{F}_2^n$ which is a linear (n,m,d)-code with $m \leq d \log(n+1)$.

Corollary 4. *Let $f(x_1, \ldots, x_n)$ be the characteristic function of a BCH-code of with $d = \Theta(\sqrt{n})$. Let $\mathcal{F} \subseteq^{[n]}$ be a family satisfying*

$$\left(\frac{\mathrm{rk}(\mathcal{F})}{en}\right)^{\deg(\mathcal{F})} \left(1 - \frac{\deg(\mathcal{F}) \cdot \mathrm{rk}(\mathcal{F})}{n}\right) = \Omega(1).$$

Then any $\mathcal{F}$-protocol for f requires $\Omega(\sqrt{n})$ bits of communication.

For example, 5 players, each seeing $n/3$ of input bits, need $\Omega(\sqrt{n})$ bits of communication, if no 3 of them can see one and the same input bit.

Acknowledgment I am thankfull to Jan Roßman for interesting comments.

References

H. Abelson, Lower bounds on information transfere in ditributed computing, *19th FOCS*, (1978), 151–158.

Babai L., Nisan N. and Szegedy M. (1992), Multiparty protocols, pseudorandom generators for Logspace, and time-space trade-offs. *J. of Comput. Syst. Sci.*, **45**, 204-232.

Chandra A. K., Furst M. L. and Lipton R. J. (1983), Multi-party protocols. Proc. 15*th* STOC 94-99.

Duris P., and P. Pudlák, On the communication complexity of planarity, In *Proc. of Int. Conf. on Fundamentals of Computation Theory* (Szeged, Hungary, August 1989), Springer Lecture Notes in Comput Sci., vol 380 (1989), 145–147.

Edmonds J., and R. Impagliazzo. Towards time-space lower bounds on branching programs. *Manuscript*, 1994.

A. Hajnal, W. Maass and G. Turán, On the communication complexity of graph properties, *20th STOC*, (1988), 186–191.

J. Ja'Ja', The VLSI complexity of selected graph problems, *JACM*, **31** (1984), 377–391.

S. Jukna, Lower bounds on communication complexity, In: *Math. Logic and Appl.*, **5** (Vilnius, 1987), 22–31.

M. Krause, Ch. Meinel and S. Waack, Separating cpmplexity classes related to certain input oblivious logarithmic space–bounded Turing machines, *RAIRO Theor. Inf. and Applications*, **26**:4 (1992), 345–362.

C.H. Papadimitriou and M. Sipser, Communication complexity, *JCSS*, **28** (1984), 260–269.

Púdlak, P. and J. Sgáll. An upper bound for a communication game related to time-space tradeoffs. *El. Colloquium on Comput. Complexity,* Report Nr. 95-010.

A. Yao, Some complexity questions related to distributed computing, *11th STOC*, (1979), 209–213.

A. Yao, The entropic limitations of VLSI computations, *13th STOC*, (1981), 308–311.