

# The BNS Lower Bound for Multi-Party Protocols is Nearly Optimal

Vince Grolmusz

Department of Computer Science  
Eötvös University, Budapest

## ABSTRACT

We present a *multi-party protocol* which computes the *Generalized Inner Product* (GIP) function, introduced by *Babai, Nisan and Szegedy* [BNS]. Our protocol shows that the lower bound for the multi-party communication complexity of the GIP function, given by [BNS], cannot be improved significantly.

*keywords: multi-party communication, communication protocols*

## 1. INTRODUCTION

In the two-party communication game, introduced by Yao [Y], there are two players,  $P_0$  and  $P_1$ , and a function  $f : \{0, 1\}^{2n} \rightarrow \{0, 1\}$ . The goal of the players is to compute the value of  $f(A_0, A_1)$  cooperatively, for some  $A_0, A_1 \in \{0, 1\}^n$ , where  $A_0$  is known only to  $P_1$ , and  $A_1$  is known only to  $P_0$ , and after the computation both players should know the value  $f(A_0, A_1)$ . The players have unlimited computational power, and both know the definition of  $f$ .  $P_0$  and  $P_1$  communicate via a blackboard, which is seen by both of them: they are allowed to write bits on the blackboard. The cost of the computation is the number of bits communicated. Since the players have unlimited computational power, every function can be computed by communicating  $n + 1$  bits.

The following generalization of the two-party communication game by *Chandra, Furst and Lipton* [CFL] has lead some nice results in the complexity theory (c.f. [BNS], [GH]): In the multi-party communication game,  $k$  players:  $P_0, P_1, \dots, P_{k-1}$  intend to compute the value of  $g(A_0, A_1, \dots, A_{k-1})$  cooperatively, where  $g : \{0, 1\}^{kn} \rightarrow \{0, 1\}$  and  $A_i \in \{0, 1\}^n$ , for  $i = 0, 1, \dots, k - 1$ . Player  $P_i$  knows the value of each variable, except  $A_i$ , for  $i = 0, 1, \dots, k - 1$ . As in the two-party game, the players have unlimited computational power, and they communicate with the help of a blackboard, viewed by all players. Only one player may write on the blackboard at a time. The goal is to compute  $g(A_0, A_1, \dots, A_{k-1})$ , such that at the end of the computation, all players know this value. The cost of the computation is the number of bits written on the blackboard for the given  $A = (A_0, A_1, \dots, A_{k-1}) \in \{0, 1\}^{nk}$ . The cost of a multi-party protocol is the maximum number of bits communicated for any  $A$  from  $\{0, 1\}^{n \times k}$ . The  $k$ -party communication complexity,  $C(g)$  of a function  $g$  is the minimum of costs of those  $k$ -party protocols which compute  $g$ .

---

Address: Múzeum krt.6-8, H-1088 Budapest, HUNGARY; current address: Max Planck Institute for Computer Science, Im Stadtwald, W-6600 Saarbruecken, GERMANY

As in the two-party case, every function can be computed by communicating  $n + 1$  bits. The theory of the two-party communication games is well developed (c.f. [LS], or [L] for a survey), but much less is known about the multi-party communication complexity of functions. *Babai, Nisan and Szegedy* examined the *Generalized Inner Product* (GIP) function in [BNS].

**Definition 1.** Let  $A \in \{0, 1\}^{n \times k}$ . We shall refer to the  $i^{\text{th}}$  column of  $A$  as  $A_i$ , the  $j^{\text{th}}$  row of  $A$  as  $A^j$ , and to the  $i^{\text{th}}$  entry in row  $j$  as  $A_i^j$ . Let  $GIP(A)$  denote the number of the all-1 rows of matrix  $A$ , modulo 2.

In other words, if column  $A_i$  is considered to be the characteristic vector of a subset  $Y_i$  of a fixed  $n$ -element set for  $i = 0, 1, \dots, k - 1$ , then

$$GIP(A) = | Y_0 \cap Y_1 \cap Y_2 \cap \dots \cap Y_{k-1} | \pmod{2}.$$

In [BNS], the following important lower bound is proved for the multi-party communication complexity of GIP:

**Theorem 2.** [BNS, Theorem 2]

$$C(GIP) = \Omega\left(\frac{n}{4^k}\right).$$

■

For several interesting applications of Theorem 2 in Turing machine simulation trade-offs or in circuit complexity theory, see [BNS] or [GH].

We describe a protocol, named “TELESCOPE”, in Section 2, which shows that the lower bound of Theorem 2 is close to the optimal:

**Theorem 3.**

$$C(GIP) \leq (2k - 1) \left\lceil \frac{n}{2^{k-1} - 1} \right\rceil.$$

**Remarks.** Independently from us, *Nisan and Szegedy* have also shown that the lower bound in Theorem 2 cannot be improved significantly (unpublished) [B].

*Babai, Nisan and Szegedy* prove another  $\Omega(n/c^k)$  lower bound for the  $k$  party communication complexity of the *quadratic character* (Legendre symbol) of the mod  $p$  sum of  $k$  variables [BNS]. They also mention that it would be important to find functions where the lower bound does not deteriorate exponentially as a function of  $k$ , e.g. a lower bound  $\Omega(n/k^c)$  would be most desirable. Here we show that no such lower bound holds for the GIP function; but we do not know whether or not the other function of [BNS] may satisfy such a stronger bound.

## 2. THE PROTOCOL

Consider an  $n \times k$  binary matrix  $A$  with columns  $A_0, A_1, A_2, \dots, A_{k-1}$ , where player  $P_i$  knows every column vector, except  $A_i$ ,  $i = 0, 1, 2, \dots, k-1$ .

We note that if it is known to  $P_0$  that  $A$  has no row of the form  $(0, 1, 1, \dots, 1)$ , then  $P_0$  can simply announce the result by counting (mod 2) the number of rows of the form  $(*, 1, 1, \dots, 1)$ . (All such rows must now begin with “1”.)

The following lemma generalizes this idea:

**Lemma 4.** *Let  $\alpha \in \{0, 1\}^k$ . Suppose it is known to each player that  $\alpha$  does not occur as a row of  $A$ . Then there exists a  $k$ -party protocol which computes  $GIP(A)$  with a communication of at most  $k$  bits.*

**Proof.** If  $\alpha$  contains only 1's,  $GIP(A) = 0$ , and they are done, without communicating a bit.

Suppose now, that  $\alpha$  has some 0-coordinates. Without loss of generality we may assume, that its first  $\ell \geq 1$  coordinates are 0:

$$\alpha_0 = \alpha_1 = \dots = \alpha_{\ell-1} = 0; \quad \alpha_\ell = \alpha_{\ell+1} = \dots = \alpha_{k-1} = 1.$$

Only the first  $k$  players, with corresponding 0 coordinates in  $\alpha$ , will participate in the communication game. The game is played as follows:

### PROTOCOL TELESCOPE

Let  $y_i$  denote the number of those rows of  $A$  of the form  $(0, \dots, 0, 1, \dots, 1)$ , where the first 1 occurs in position  $i$ .

For every  $i$ ,  $0 \leq i \leq \ell - 1$ , player  $P_i$  announces the parity of the number of rows of the form  $(0, \dots, 0, *, 1, \dots, 1)$ , where the  $*$  is at place  $i$ .

Observation: This number is  $y_i + y_{i+1}$ .

Subsequently, each player privately computes the mod 2 sum of all numbers announced.

Observation: The result of this telescoping sum is  $y_0 + y_\ell \pmod 2$ . But, by assumption,  $y_\ell = 0$ ; therefore the result is the desired quantity,  $y_0 \pmod 2$ .

The cost was  $\ell$  bits of communication. ■

**Proof of Theorem 3.** Let us divide the rows of matrix  $A$  into blocks of  $2^{k-1} - 1$  contiguous rows plus a leftover of at most  $2^{k-1} - 1$  rows. The players cooperatively determine the number of all-1 rows in each block, and then privately add up the results to obtain  $GIP(A)$ .

Next we show how to obtain the number of all-1 rows for a single block at the cost of  $2k - 1$  bits of communication.  $P_0$  knows all the columns, except the first, so he knows at most  $2^{k-1} - 1$  rows of length  $k - 1$ , so he can find an  $\alpha' \in \{0, 1\}^{k-1}$ ,  $\alpha' = (\alpha_1, \alpha_2, \dots, \alpha_{k-1})$

which is not a row of the  $k - 1$  column wide part of the block seen by  $P_0$ . Let  $\alpha = (0, \alpha_1, \alpha_2, \dots, \alpha_{k-1})$ . Then  $\alpha$  does not occur as a row in this block. So if  $P_0$  communicates  $\alpha'$  with  $k - 1$  bits, then every player exchanges it to  $\alpha$  privately, and they play the TELESCOPE protocol with at most  $k$  bits, exchanging at most  $2k - 1$  bits in total. ■

**ACKNOWLEDGMENT.** The author thanks for many helpful comments to Laci Babai.

## REFERENCES

- [B] L. Babai: oral communication.
- [BNS] L. Babai, N. Nisan, M. Szegedy: Multiparty Protocols and Pseudorandom Sequences, Proc. 21st ACM STOC, 1989, pp. 1-11.
- [CFL] A. K. Chandra, M. L. Furst, R. J. Lipton: Multi-party Protocols, Proc. 15th ACM STOC, 1983, pp. 94-99.
- [GH] M. Goldmann, J. Håstad: On the Power of Small-Depth Threshold Circuits, 31st IEEE FOCS, 1990, pp. 610-618.
- [L] L. Lovász: Communication Complexity: A Survey, Technical Report CS-TR-204-89, Princeton University, 1989
- [LS] L. Lovász, M. Saks: Lattices, Moebius Functions and Communication Complexity, Proc. 29th IEEE FOCS, pp. 81-90.
- [Y] A.C. Yao: Some Complexity Questions Related to Distributive Computing, Proc. 11th ACM STOC, 1979, pp. 209-213.