A Note on Non-Deterministic Communication Complexity with Few Witnesses

Vince Grolmusz * Gábor Tardos †

Abstract

We improve both main results of the paper "Non-Deterministic Communication Complexity with Few Witnesses " by M. Karchmer, I. Newman, M. Saks and A. Wigderson, appeared in JCSS Vol. 49, pp. 247-257.

1 Introduction

Randomness is an often studied resource in a wide variety of computation models. Non-determinism is another important computational resource: for example, the P vs. NP question addresses the power of non-determinism in Turing-machine computation. In communication games non-determinism is proven to be stronger than determinism (see [7], [5], [2]). Analogously to the study of the power of the bounded randomness, the study of the power of the bounded non-determinism has nice results [4] or [3]. In [4] Karchmer, Newman, Saks and Wigderson examined communication games with bounded non-determinism: for a positive integer k they introduced $n_k(f)$ the length of the shortest nondeterministic protocol for computing the function f subject to the condition that each input has at most k witnesses (defined below). They studied how this complexity measure relates to old measures such as the deterministic communication complexity and the rank of the communication matrix of the function f. For the exact statements of their results, see Theorems 3 and 4 below. In this note we prove a tighter relation between these quantities (Theorems 5 and 6) slightly improving on the earlier results.

1.1 Notation and Preliminaries

We follow the notations of [4]:

rk(A) denotes the *rank* of matrix A over the complex numbers.

trk(A) is the *triangular rank* of matrix A: the size of the largest non-singular lower triangular submatrix of A.

A *rectangle* is a rank-1 or rank-0 Boolean matrix. We say that a rectangle *covers* a position if its entry in that position is 1. Notice that the set of positions covered by a rectangle forms a submatrix. A set of rectangles $R_1, R_2, \ldots, R_t$ *covers* the Boolean matrix A if the matrix A and the matrix $\sum_{i=1}^{t} R_i$ has entry 0 exactly in the same positions.

*Department of Computer Science, Eötvös University, Budapest, Pázmány P. stny. 1/C, H-1117 Budapest, Hungary; E-mail: grolmusz@cs.elte.hu

†Rényi Mathematical Institute of the Hungarian Academy of Science, Reáltanoda u. 13-15, H-1055 Budapest, Hungary; E-mail: tardos@renyi.hu

A rectangle-cover $R_1, R_2, \ldots, R_t$ is a *k-cover* if every entry of $\sum_{i=1}^t R_i$ is at most k. (Alternatively, any position is covered by at most k of the rectangles R_i.) Let $\kappa_k(A)$ denote the minimum cardinality of a k-cover of A.

Readers unfamiliar with the basic definitions in communication complexity are referred to the paper [4] or monographs [5] or [2]. We just list here the notations used in paper [4].

For a function $f : \{0,1\}^u \times \{0,1\}^u \to \{0,1\}$, let M_f denote its $2^u \times 2^u$ communication-matrix: this matrix contains the value $f(x, y) \in \{0,1\}$ in the intersection of the row, corresponded to x and the column, corresponded to y, where $x, y \in \{0,1\}^n$. Let $c(f)$ denote the deterministic communication complexity of f, and let $n(f)$ denote its non-deterministic communication complexity.

Every non-deterministic communication protocol for computing f corresponds to a cover of M_f by rectangles [4], [1]. These rectangles are called *witnesses*. Let $n_k(f)$ denote the minimum complexity of a non-deterministic protocol, computing f such that every entry of M_f are covered by at most k rectangles (has at most k witnesses).

We need the following two results, the first from [4]:

Lemma 1 (KNSW) *For $k \geq 1$ and if $\mathrm{rk}(M_f) > 1$ we have $n_k(f) = \lceil \log \kappa_k(M_f) \rceil$.*

□

The second result is the following Lemma of [6] Here $\bar{f}$ denotes the complementary function of f, i.e., $\bar{f} = 1 - f$.

Lemma 2 (Lovász-Saks) $c(f) = O(n(f) \log(\mathrm{trk}(M_{\bar{f}})))$.

□

2 Lower bounds for restricted non-deterministic complexity

Two different lower bounds were given in [4] for $n_k(f)$:

Theorem 3 (KNSW) *For any function $f : X \times Y \to \{0,1\}$ and integer $k \geq 1$:*

$$n_k(f) = \Omega\left(\frac{\sqrt{c(f)}}{k}\right);$$

or, equivalently,

$$c(f) = O((kn_k(f))^2).$$

The other main result of paper [4] is the following

Theorem 4 (KNSW) *For any non-zero function $f : X \times Y \to \{0,1\}$ and integer $k \geq 1$,*

$$n_k(f) \geq \frac{\log \mathrm{rk}(M_f)}{k} - 1.$$

We prove here the following stronger bounds for $n_k(f)$. Our Theorem 5 improves Theorem 3:

Theorem 5 *For any function $f : X \times Y \to \{0,1\}$ and integer $k \geq 1$:*

$$n_k(f) = \Omega\left(\sqrt{\frac{c(f)}{k}}\right);$$

or, equivalently,

$$c(f) = O(k(n_k(f))^2).$$

Our Theorem 6 tightens Theorem 4:

Theorem 6 *For any function $f : X \times Y \to \{0,1\}$ and integer $1 \leq k < \log \mathrm{rk}(M_f)/2$,*

$$n_k(f) \geq \frac{\log \mathrm{rk}(M_f)}{k} + \log k - 2.$$

3 Proofs

Our improvement of Theorem 4 relies on the following improvement of a statement used by Karchmer, Newman, Saks and Wigderson (Lemma 1 in [4]):

Lemma 7 *For any Boolean matrix A and positive integer k:*

$$\mathrm{rk}(A) \leq \binom{\kappa_k(A)}{1} + \binom{\kappa_k(A)}{2} + \cdots + \binom{\kappa_k(A)}{k}.$$

Proof: Consider a set of rectangles R_i. Observe that the intersection of the sets of positions covered by R_i is a (possibly empty) submatrix. We call the rectangle R covering exactly the positions in this intersection the *intersection* of the rectangles R_i.

Note also, that if a matrix M can be given as a linear combination of t rectangles, then $\mathrm{rk}(M) \leq t$, simply by the sub-additivity of the rank function.

Now, let us consider matrix A, and its k-cover by $s = \kappa_k$ rectangles $R_1, \ldots, R_s$. For a $K \subset \{1, 2, \ldots, s\}$ let R_K denote the intersection of the rectangles R_i with $i \in K$.

From the inclusion-exclusion formula:

$$A = \sum_{K\subset\{1,2,\ldots,s\},|K|=1} R_K - \sum_{K\subset\{1,2,\ldots,s\},|K|=2} R_K + \cdots + (-1)^{k+1} \sum_{K\subset\{1,2,\ldots,s\},|K|=k} R_K$$

The right-hand-side of this formula is a combination of $\binom{s}{1} + \cdots + \binom{s}{k}$ rectangles, thus the left-hand-side has rank $\mathrm{rk}(A)$ bounded by this number, as claimed.

□

Proof of Theorem 6. Let $A = M_f$, and apply Lemma 7, with $s = \kappa_k(M_f)$:

$$\mathrm{rk}(M_f) \leq \sum_{i=1}^{k} \binom{s}{i}.$$

Clearly, $\mathrm{rk}(M_f) \leq 2^s$ follows, thus $k < s/2$. Now we use $\binom{s}{i} \leq \binom{s}{k} \leq \left(\frac{se}{k}\right)^k$. Taking logarithms, and applying Lemma 1 we get:

$$\log \mathrm{rk}(M_f) \leq k n_k(f) - k \log k + 2k$$

as claimed.

□

Proof of Theorem 5.

If f is constant (i.e. 0 or 1), then – both deterministic, and non-deterministic – communication complexities of f are 0, so we are done. In what follows, we assume that f is non-constant.

For any $k \geq 1$, $n(f) \leq n_k(f)$, consequently, from Lemma 2:

$$c(f) = O(n(f)\log(\mathrm{trk}(M_{\bar{f}}))) = O(n_k(f)\log(\mathrm{trk}(M_{\bar{f}})) = O(n_k(f)\log(\mathrm{rk}(M_{\bar{f}})).$$

However, since $M_{\bar{f}} = J - M_f$, where J is the all-1 matrix, the ranks of M_f and $M_{\bar{f}}$ may differ by at most 1. Consequently,

$$c(f) = O(n_k(f)\log(\mathrm{rk}(M_f)) = O(kn_k^2),$$

where the last equation comes from Theorem 6.

References

[1] A. Aho, J. D. Ullman, and M. Yannakakis, *On the notions of information transfer in VLSI circuits*, in Proc. 15th Ann. ACM Symp. Theor. Comput., 1983, pp. 151–158.

[2] J. Hromkovič, *Communication Complexity and Parallel Computing*, Springer-Verlag, 1997.

[3] J. Hromkovic and G. Schnitger, *Nondeterministic communication with a limited number of advice bits*, in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, ACM Press, 1996, pp. 551–560.

[4] M. Karchmer, I. Newman, M. E. Saks, and A. Wigderson, *Non-deterministic communication complexity with few witness*, Journal of Computer and System Sciences, 49 (1994), pp. 247–257.

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

[6] L. Lovász and M. Saks, *Lattices, Möbius functions, and communication complexity*, in Proc. 29th Ann. IEEE Symp. Found. Comput. Sci., 1988, pp. 81–90.

[7] A. C. Yao, *Some complexity questions related to distributed computing*, in Proc. 11th Ann. ACM Symp. Theor. Comput., 1979, pp. 209–213.