Electronic Colloquium on Computational Complexity - Reports Series 1995 - available via:

ECCC
TR95-034

FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Lower Bounds for the Majority Communication Complexity of Various Graph Accessibility Problems

Christoph Meinel[1] and Stephan Waack[2]

[1] Theoretische Informatik, Fachbereich IV, Universität Trier, D–54286 Trier
[2] Inst. für Num. und Angew. Mathematik, Univ. Göttingen, Lotzestr. 16–18, D–37083 Göttingen

Abstract. We investigate the probabilistic communication complexity (more exactly, the majority communication complexity,) of the graph accessibility problem GAP and its counting versions MOD_k-GAP, $k \geq 2$. Due to arguments concerning matrix variation ranks and certain projection reductions, we prove that, for any partition of the input variables, GAP and MOD_m-GAP have majority communication complexity $\Omega(n)$, where n denotes the number of nodes of the graph under consideration.

Topics: Computational Complexity, Probabilistic Communication Protocols, Majority Accepting Mode, Projection Reductions, *GAP*, *MOD_k-GAP*

Introduction

The *graph accessibility problem* $\mathrm{GAP} = (\mathrm{GAP}_n)_{n\in\mathbb{N}}$ consists in the decision whether there is a path in a given directed, acyclic n-node graph $G = (V, E)$, $V = \{1, \ldots, n\}$ and $E \subseteq V \times V$, that leads from vertex 1 to vertex n. As usual, let G be given by its adjacency matrix $G = (a_{ij})_{1\leq i,j\leq n, i\neq j}$ with

$$a_{ij} = a(i,j) = \begin{cases} 1 & \text{if } (i,j) \in E\,; \\ 0 & \text{otherwise.} \end{cases}$$

$\mathrm{GAP}_n : \{0,1\}^{n^2} \longrightarrow \{0,1\}$, is defined by

$$(a_{ij}) \longrightarrow \begin{cases} 1 & \text{if there is a path in the graph described by } (a_{ij}) \text{ from 1 to } n; \\ 0 & \text{otherwise.} \end{cases}$$

The major property of GAP is the following one.

Theorem 1. GAP *is complete for the complexity class* NL *of languages acceptable by nondeterministic logarithmic space-bounded Turing machines via logspace reductions (see [15]), via projection translations (see [6]), and via p-projection reductions for nonuniform* NL *(see [8]).* □

Soon it was realized (see, e.g.,[9]) that certain modified GAPs, denoted by MOD_k-GAP, $k \geq 2$, have similar properties for the complexity classes MOD_k–L, defined by logarithmic space–bounded Turing machines equipped with the

counting acceptation mode MOD_k. Here, an input is accepted, if and only if the number of accepting computations is *not* congruent 0 modulo k.

$\text{MOD}_k\text{-GAP}_n : \{0,1\}^{n^2} \longrightarrow \{0,1\}$, is defined by

$$(a_{ij}) \longrightarrow \begin{cases} 1 & \text{the number of paths in } (a_{ij}) \text{ from 1 to } n \text{ is not divisible by } k; \\ 0 & \text{otherwise.} \end{cases}$$

A generalization of Theorem 1 yields the following theorem which is true for the various reduction notions. (For a proof, e.g. of the p-projection completeness, we refer to [10].)

Theorem 2. $\text{MOD}_k\text{-GAP}$ *is complete for* $\text{MOD}_k\text{–L}$, $k \geq 2$. □

From Theorems 1 and 2 it becomes clear why it is an important goal in complexity theory to characterize the complexity of graph accessibility problems. In [17], Yao started the study of the communication complexity of graph problems. In [5], the deterministic communciation complexity of *connectivity* and *s-t-connectivity* (for undirected graphs) was investigated. There the problem of proving lower bounds on the *probabilistic communication complexity* of graph problems was raised. In the following we contribute to the solution of this problem by investigating the *majority communication complexity* of the graph accessibility problems GAP and $\text{MOD}_k\text{-GAP}$, $k \geq 2$.

Let a graph $G = (V, E)$ be given, in arbitarily distributed form, to two processors P_1 and P_2 with unbounded computational power. In order to solve GAP or $\text{MOD}_k\text{-GAP}$, both processors have to communicate via a common communication tape. The computation of the whole structure, which is called a *communication protocol* or simply a *protocol*, is going on in *rounds*. Starting with P_1, the processors write alternatingly bits on the communication tape. These bits depend on the input available to the processor which is to move and on the bits already written on the communication tape before. We assume without loss of generality that in each round exactly one bit is written on the communication tape and that all (nondeterministic) computations of a protocol are of equal length, say L. If the last bit written on the communication tape is "1" or "0", the particular computation is called *accepting* or *rejecting*, respectively. (Since we shall assume the processors to be nondeterministic, this last bit need not to coincide with the output of the protocol.) So co-operative computations can be thought of as to be Boolean strings. The length L of the string is the *communication complexity* of the computation. (For more reading on communciation complexity we refer, e.g., to [1], [2], [3], [4], [7]). Since our processors are nondeterministic we have to define the *output of* of a protocol by means of a certain *acception mode*. In this paper we consider the probabilistic *majority acception mode* in which a protocol *accepts* an input, if the number of accepting computations is greater than the number of rejecting ones.

We prove that all graph accessibility problems, defined before, have majority communication complexity $\Omega(n)$, where n is the number of nodes of the graph under consideration.

Simular bounds could be proved recently for the modular communication complexity of GAP and MOD_m-GAP [11]. For the nondeterministic communication complexity Raz and Spieker derived the lower bound $\Omega(n \log\log n)$ [14]. However, the optimal lower bound $\theta(n \log n)$ could be proved up to now merely for the deterministic communication complexity [5].

1 The Computational Model

In order to be able to receive our results we need a precise formal definition of the considered computational model which was described informally already in the introduction. Let $f : S_1 \times S_2 \to \{0,1\}$ be given in distributed form. (Throughout this paper, S_1 and S_2 are either $\{0,1\}^n$ or $\mathbb{Z}/m\mathbb{Z}$.) A *protocol of length* L consisting of two processors P_1 and P_2 which access inputs of S_1 and S_2, respectively, can be described by two functions

$$\Phi_i : S_i \times \{0,1\}^{\leq L} \to \{0,1\},$$

$i = 1, 2$. The interpretation is as follows. Let $\gamma = \gamma_1 \ldots \gamma_j$, $\gamma_k \in \{0,1\}$. If $\Phi_i(s_i, \gamma) = 1$, and if $|\gamma| - i$ is even, then the corresponding processor P_i is able to write γ_j on the communication tape provided that it has read $\gamma_1 \ldots \gamma_{j-1}$ on the communication tape and that it has s_i as input. If, however, $\Phi_i(s_i, \gamma) = 0$, then P_i is not able to write γ_j.

The work of a protocol P of length L can be described in terms of two $\#S_1 \times \#S_2$–matrices Acc^P and Rej^P. For $(s_1, s_2) \in S_1 \times S_2$, $Acc^P_{s_1,s_2}$ gives the number of accepting computations of the protocol P on the input (s_1, s_2), and $Rej^P_{s_1,s_2}$ gives the number of rejecting computations.

In order to make this approach unique, we agree that $\Phi_i(s_i, \gamma) = 1$, if $|\gamma| - i$ is odd, for $i = 1, 2$.

$$Acc^P_{s_1,s_2} \stackrel{def}{=} \sum_{\gamma_1 \ldots \gamma_L \in \{0,1\}^L, \gamma_L = 1} \prod_{j=1}^{L} \Phi_{(1+(j+1) \bmod 2)}\big(s_{(1+(j+1) \bmod 2)}, \gamma_1 \ldots \gamma_j\big) \quad (1)$$

$$Rej^P_{s_1,s_2} \stackrel{def}{=} \sum_{\gamma_1 \ldots \gamma_L \in \{0,1\}^L, \ \gamma_L = 0} \prod_{j=1}^{L} \Phi_{1+((j+1) \bmod 2)}\big(s_{1+((j+1) \bmod 2)}, \gamma_1 \ldots \gamma_j\big) \quad (2)$$

Increasing the length of P by at most two, it can be achieved that $Acc^P_{s_1,s_2} \neq Rej^P_{s_1,s_2}$ for all inputs (s_1, s_2). In the following, we assume that all protocols will have this property.

A *counting accepting mode* μ for a protocol P is a function $\mu : \mathbb{N}^2 \to \{0,1\}$ such that P accepts a distributed input (s_1, s_2) if and only if

$$\mu(Acc^P_{s_1,s_2}, Rej^P_{s_1,s_2}) = 1.$$

Otherwise P rejects the input. In the following we consider the probabilistic *majority accepting mode*

$$\mathrm{MAJ}(n_1, n_2) = 1 \quad \stackrel{def}{\Longleftrightarrow} \quad n_1 > n_2,$$

which leads to an acception of a given input if the number of accepting computations exeeds that of rejecting computations.

Definition 3. *A protocol P equipped with the accepting mode* MAJ *is called a* majority-protocol. *The* majority communication complexity MAJ-Comm(f) *of a function $f : S_1 \times S_2 \to \{0,1\}$ is defined by*

$$\text{MAJ-Comm}(f) \stackrel{def}{=} \min\{\, length(P) \mid \; f_P = f \,\},$$

where f_P denotes the function computed by the majority-protocol P.

Investigating communication complexity, the appropriate type of reduction is that of rectangular reductions which are defined as follows: Let $F = (F_{2n} : \Sigma^n \times \Sigma^n \to \{0,1\})_{n\in\mathbb{N}}$ and $G = (G_{2n} : \Gamma^n \times \Gamma^n \to \{0,1\})_{n\in\mathbb{N}}$ be two decision problems. F is *rectangularly reducible* to G with respect to q (denoted by $F \leq^q_{rec} G$), where $q : \mathbb{N} \to \mathbb{N}$ is a nondecreasing function, if, for each n, there are two transformations l_n, $r_n : \Sigma^n \to \Gamma^{q(n)}$ such that for all $\mathbf{x}, \mathbf{y} \in \Sigma^n$ $F_{2n}(\mathbf{x}, \mathbf{y}) = G_{2q(n)}(l_n(\mathbf{x}), r_n(\mathbf{y}))$.

Rectangular reductions can be used for proving lower bounds on the majority communication complexity in the following way: Let $q : \mathbb{N} \to \mathbb{N}$ be an unbounded nondecreasing function. Then we define $q^{(-1)}$ by $q^{(-1)}(i) = \max\{j \mid \; q(j) \leq i\}$. Standard arguments yield

Lemma 4. *Assume there are given two sequences of functions $F = (F_{2n} : \Sigma^n \times \Sigma^n \to \{0,1\})_{n\in\mathbb{N}}$ and $G = (G_{2n} : \Gamma^n \times \Gamma^n \to \{0,1\})_{n\in\mathbb{N}}$. If $c(n) \leq$* MAJ-Comm(F) *and $F \leq^q_{rec} G$, then $c \circ q^{(-1)}(n) \leq$* MAJ-Comm(G). □

One efficient way to get rectangular reductions is to work with projection reductions [16] which are defined as follows.

Definition 5. Let $F = (F_n : \Sigma^n \to \{0,1\})_{n\in\mathbb{N}}$ and $G = (G_n : \Gamma^n \to \{0,1\})_{n\in\mathbb{N}}$. The mapping $\pi_n : \{y_1, \ldots, y_m\} \to \{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\} \cup \Gamma$ is called a *projection reduction* from F_n to G_m if $F_n(x_1, \ldots, x_n) = G_m(\pi(y_1), \ldots, \pi(y_m))$. If F_n and G_m are given in distributed form,

$$F_{2n} : \Sigma^n \times \Sigma^n \to \{0,1\} \;\text{ and }\; G_{2m} : \Gamma^m \times \Gamma^m \to \{0,1\}$$

then a projection reduction π_n is said to *respect the distribution* of the variables if

$$\pi_n^{-1}\{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\} \subseteq \{y_1, \ldots, y_m\}$$

and

$$\pi_n^{-1}\{x_{n+1}, \ldots, x_{2n}, \neg x_{n+1}, \ldots, \neg x_{2n}\} \subseteq \{y_{m+1}, \ldots, y_{2m}\}.$$

A sequence $\pi = (\pi_n)_n \in \mathbb{N}$ of reduction projections π_n is called a *$p(n)$–projection reduction* and we write $F \leq^p_\pi G$ if $p(n)$ is a nondecreasing function with $m \leq p(n)$.

From Lemma 4 we immediately get

Lemma 6. *Assume that we are given two sequences of functions* $F = (F_{2n} : \Sigma^n \times \Sigma^n \to \{0,1\})_{n\in\mathbb{N}}$ *and* $G = (G_{2m} : \Gamma^m \times \Gamma^m \to \{0,1\})_{m\in\mathbb{N}}$ *with* $F \leq^p_\pi G$, *where* p *is increasing and* $\pi = (\pi_n)_{n\in\mathbb{N}}$ *is a sequence of projection reductions that respects the distribution of the variables. If* $c(n) \leq$ MAJ-Comm(F), *then* $c \circ q^{(-1)}(n) \leq$ MAJ-Comm(G). □

2 Rank Arguments for Lower Bounds

Following an approach of Mehlhorn and Schmidt, rank arguments can be used for proving lower bounds on the length of communication protocols. Throughout this section, f denotes a function $f : S_1 \times S_2 \to \{0,1\}$ with $N = \#S_1 = \#S_2$. M^f denotes the *communication matrix* of f, which is defined by $M^f_{s_1,s_2} = f(s_1, s_2)$.

Lemma 7. [12] *Let* R *be any semiring. Let* P *be a protocol of the length* L *on the input set* $S_1 \times S_2$, $\#S_1 = \#S_2 = N$, *and let* Acc^P *and* Rej^P *be the* $N \times N$*–matrices defined in equations 1, and 2. Then*

$$\text{rank}_R(Acc^P) \leq 2^{L-1}, \tag{3}$$

$$\text{rank}_R(Rej^P) \leq 2^{L-1}. \ \square \tag{4}$$

In order to derive lower bounds on the length of protocols equipped with the *majority* acceptance mode, we adopt the concept of variation ranks of communication matrices first developed in [7].

Definition 8. *Two real* $N \times N$*–matrices* A *and* B *with nonzero coefficients are called* order–equivalent *if, for all indices* i *and* j, $a_{ij} \cdot b_{ij} \geq 0$. *Let* θ *be a positive natural number, and let* A *be a real matrix with non-zero coefficients. The* variation rank var-rank$_{\leq,\theta}(A)$ *is the minimum over all numbers* rank$_{\mathbb{R}}B$, *where* B *is a* $N \times N$*–matrix with* $b_{ij} \in \{0, \pm 1, \pm 2, \ldots, \pm\theta\}$ *that is order–equivalent to* A.

If J denotes the $N \times N$–matrix whose coefficients are equal to 1, then Lemma 7 implies the following corollary.

Corollary 9. $\log_2\left(\text{var-rank}_{\leq,2^L}(2M^f - J)\right) \leq L$, *where* L *is the length of any* MAJ*-protocol computing* f. □

In order to estimate the variation rank of the matrix $(2M^f - J)$, some linear algebraic considerations and computations are nessecary. Recall that if $\mathbb{R}^N$ is the N–dimensional real vector space of column vectors and if $\mathbf{x}^T\mathbf{y}$ denotes the standard scalar product, then $\|\mathbf{x}\| = \sqrt{\mathbf{x}^T\mathbf{x}}$ is the norm induced by this scalar product. Let $A = (a_{ij})$ be a real $N \times N$–matrix. Then $\|A\| := \sup\{\|A\mathbf{x}\| \mid \|\mathbf{x}\| = 1\}$ is the *spectral norm*, and $\|A\|_2 := \sqrt{\sum_{i,j} |a_{ij}|^2}$ is the l_2*–norm* of the matrix A. The matrix A is called *orthogonal* if and only if $A^{-1} = A^T$. The following theorem, which is well–known in linear algebra, relates these notions to each other.

Theorem 10. *1.* $\frac{1}{\sqrt{N}}\|A\|_2 \leq \|A\| \leq \|A\|_2$.

2. $\frac{1}{\sqrt{N}}\|A\|_2 = \|A\|$ *if and only if* $A = d \cdot U$, *where* $0 \leq d \in \mathbb{R}$ *and* U *is an orthogonal matrix.* □

Due to the next lemma, the variation rank of a matrix M with coefficients from $\{-1, 1\}$ can be estimated in terms of the norms of certain matrices A which are order–equivalent to M.

Lemma 11. **[7]** *Let* M *be an* $N \times N$*–matrix with* $m_{i,j} \in \{-1, 1\}$ *If* $A = (a_{ij})$ *is any* $N \times N$*–matrix over* $\mathbb{R}$ *that is order–equivalent to* M *with* $1 \leq |a_{ij}| \leq \theta$ *for all* $1 \leq i, j \leq N$, *then* $\frac{\|A\|_2^2}{\theta^2 \cdot \|A\|^2} \leq \text{var-rank}_{\leq,\theta}(M)$. □

A straightforward computation using Lemma 11 together with Corollary 9 yields

Lemma 12. *Let* A *be a real matrix which is order equivalent to* $2M^f - J$, *where* $1 \leq |a_{ij}| \leq \theta$, *for all* $1 \leq i, j \leq N$. *Let* $\tilde{A}$ *be a square submatrix of* A. *Then*

$$\frac{2}{3}\log_2\left(\frac{\|\tilde{A}\|_2}{\|\tilde{A}\|}\right) - 2\log_2\theta \leq \text{MAJ-Comm}(f) \ . \quad \square$$

Due to Theorem 10, a matrix $\tilde{A}$ is optimal in Lemma 12 if $\tilde{A} = d \cdot \tilde{U}$, where $\tilde{U}$ is orthogonal.

Corollary 13. *If, moreover,* $\tilde{A}$ *is assumed to be an* $\tilde{N} \times \tilde{N}$*–submatrix of the matrix* A, *and if there are a real number* $d > 0$ *and an orthogonal matrix* $\tilde{U}$ *such that* $\tilde{A} = d \cdot \tilde{U}$, *then* $\frac{1}{3}\log_2 \tilde{N} - 2\log_2\theta \leq \text{MAJ-Comm}(f)$. □

Using Corollary 13, we start to prove lower bounds on the length of majority protocols for some concrete functions. We consider the *MOD_m-orthogonality-test-function* $\text{ORT}^{[m]} = (\text{ORT}^{[m]}_{2n})_{n\in\mathbb{N}}$, $m \geq 2$, which is defined by

$$\text{ORT}^{[m]}_{2n} : (\mathbb{Z}/m\mathbb{Z})^n \times (\mathbb{Z}/m\mathbb{Z})^n \to \{0,1\}_{n\in\mathbb{N}},$$

$$(x_1, \ldots, x_n, y_1, \ldots, y_n) \mapsto \begin{cases} 1 \text{ if } \sum x_i y_i = 0 \text{ in } \mathbb{Z}/m\mathbb{Z}; \\ 0 \text{ otherwise.} \end{cases}$$

The problem is to find a quadratic submatrix M' of $M^{\text{ORT}^{[m]}}$ with large degree, and to find an optimal comparison matrix $\tilde{A}$ of M' in the sense of Corollary 13.

First we look for an appropriate submatrix M' of M. We describe M' by giving its set $\mathcal{R}$ of column indices,

$$\mathcal{R} \subset (\mathbb{Z}/m\mathbb{Z})^n \cong \left(\mathbb{Z}/p_1^{l_1}\mathbb{Z}\right)^n \times \cdots \times \left(\mathbb{Z}/p_r^{l_r}\mathbb{Z}\right)^n .$$

Let us assume that the elements of $(\mathbb{Z}/m\mathbb{Z})^n$ and $\left(\mathbb{Z}/p^l\mathbb{Z}\right)^n$ are column vectors. We adopt the usual definition of $\mathbb{Z}/p^l\mathbb{Z}$–linear independence. The following lemma characterizes those sets of vectors that are linearly independent in $\left(\mathbb{Z}/p^l\mathbb{Z}\right)^n$.

Lemma 14. *Let $A = (a_{ij})$ be an integer $n \times k$–matrix. Then the vectors*

$$((a_{1j} \bmod p^l), \ldots, (a_{nj} \bmod p^l))^T,$$

for $j = 1, \ldots k$, are linearly independent over $\mathbb{Z}/p^l\mathbb{Z}$ if and only if the vectors

$$((a_{1j} \bmod p), \ldots, (a_{nj} \bmod p))^T,$$

for $j = 1, \ldots k$, are linearly independent over $\mathbb{Z}/p\mathbb{Z}$.

Proof. ($\Rightarrow$) Assume that the columns $\mathbf{a}_{\cdot j}$, $j = 1, \ldots, k$, are linearly dependent over $\mathbb{Z}/p\mathbb{Z}$, i.e., there are integers $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}$ such that, for all $i \in \{1, \ldots, n\}$, $\sum_{j=1}^{k} \lambda_j a_{ij} \equiv 0 \pmod{p}$ and there is an j_0 such that $\lambda_{j_0} \not\equiv 0 \pmod{p}$. It follows that, for all $i \in \{1, \ldots, n\}$, $\sum_{j=1}^{k} p^{l-1} \lambda_j a_{ij} \equiv 0 \pmod{p^l}$ and there is an j_0 such that $p^{l-1}\lambda_{j_0} \not\equiv 0 \pmod{p^l}$.

($\Leftarrow$) Assume that the columns $a_{\cdot j}$, $j = 1, \ldots, k$, are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, there is a $k \times k$ submatrix A' of A such that $\det(A') \not\equiv 0 \pmod{p}$. It follows that $\det(A' \bmod p^l)$ is a unit in $\mathbb{Z}/p^l\mathbb{Z}$ and consequently $A' \bmod p^l$ is an invertible matrix over $\mathbb{Z}/p^l\mathbb{Z}$. It follows from

$$A' \cdot (\lambda_1, \lambda_2, \ldots, \lambda_k)^T \equiv (0, 0, \ldots, 0)^T \pmod{p^l}$$

that $\lambda_1 \equiv \lambda_2 \equiv \ldots \equiv \lambda_k \equiv 0 \pmod{p^l}$. □

Now we define on the set $\{\mathbf{x} | \, \mathbf{x} \in \left(\mathbb{Z}/p^l\mathbb{Z}\right)^n, \mathbf{x} \text{ linearly independent}\}$ the equivalence relation

$$\mathbf{x} \sim \mathbf{y} \overset{def}{\iff} \mathbf{x} \text{ and } \mathbf{y} \text{ are linearly dependent over } \mathbb{Z}/p^l\mathbb{Z}.$$

Let, for $p_i = p$, $\mathcal{R}_i$ denote an arbitrary but fixed system of representatives, and let $\mathcal{R} \overset{def}{=} \mathcal{R}_1 \times \cdots \times \mathcal{R}_r$. Then we get

Corollary 15. $\#\mathcal{R} = \frac{p_1^n - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_r^n - 1}{p_r - 1}$. □

After having found via $\mathcal{R}$ an appropriate quadratic submatrix M' of $M^{\mathrm{ORT}^{[m]}}$ that is of large degree, we have to construct an optimal comparison matrix $\tilde{A}$ in the sense of Corollary 13. In order to do this, we use the following fact which is trivial merely in the case $l = 1$.

Lemma 16.
Let $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \left(\mathbb{Z}/p^l\mathbb{Z}\right)^n$ be linear independent over $\mathbb{Z}/p^l\mathbb{Z}$. Then

$$\left\{\mathbf{x} \,|\, \mathbf{x} \in \left(\mathbb{Z}/p^l\mathbb{Z}\right)^n, \, \mathbf{x}^T\mathbf{x}_1 = \ldots = \mathbf{x}^T\mathbf{x}_k = 0\right\} \simeq \left(\mathbb{Z}/p^l\mathbb{Z}\right)^{n-k}.$$

Proof. We consider the $n \times k$ matrix $X = \left(\mathbf{x}_1, \ldots \mathbf{x}_k\right)$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, there is an unimodular $n \times n$ matrix U and an unimodular $k \times k$ matrix V over $\mathbb{Z}/p^l\mathbb{Z}$ such that $X' = \left(x'_{ij}\right) \overset{def}{=} U \cdot X \cdot V = \left(\epsilon_i\delta_{ij} + z_{ij}\right)$, where the ϵ_i are units in $\mathbb{Z}/p^l\mathbb{Z}$, the z_{ij} are zero divisors in $\mathbb{Z}/p^l\mathbb{Z}$, and δ_{ij} is Kronecker's function. Consequently, there are unimodular matrices U' and V' such that $X'' = \left(x''_{ij}\right) \overset{def}{=} U' \cdot X \cdot V' = \left(\delta_{ij}\right)$. The claim follows now. □

Lemma 17. *Let* $\mathbf{x}, \mathbf{y} \in \mathcal{R}$, $\mathbf{x} \neq \mathbf{y}$.

1. $\omega_1^{(n)} \stackrel{def}{=} \#\{\mathbf{z} \mid (\mathbf{z}^T\mathbf{x} = 0) \wedge (\mathbf{z}^T\mathbf{y} = 0)\}/\#\mathcal{R} = \prod_{i=1}^{r} \frac{p_i^{n-2}-1}{p_i^n-1}$,
2. $\omega_2^{(n)} \stackrel{def}{=} \#\{\mathbf{z} \mid (\mathbf{z}^T\mathbf{x} \neq 0) \wedge (\mathbf{z}^T\mathbf{y} \neq 0)\}/\#\mathcal{R} =$
$= 1 - 2 \cdot \prod_{i=1}^{r} \frac{p_i^{n-1}-1}{p_i^n-1} + \prod_{i=1}^{r} \frac{p_i^{n-2}-1}{p_i^n-1}$. □

Proof. The claims follow from Lemma 14, Lemma 16, and Corollary 15. □

Now we are able to prove a lower bound on the the majority communication complexity of $\mathrm{ORT}^{[m]}$.

Proposition 18. *If* $m = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$, *where the* p_i *are pairwise different prime numbers, then, for sufficiently large* n,

$$\text{MAJ-Comm}(\mathrm{ORT}_{2n}^{[m]}) \geq \frac{n-7}{3} \log_2(p_1 \cdot \ldots \cdot p_r).$$

Proof. We consider first the following quadratic equation and one of its solutions $t^{(n)}$.

$$0 = T^2 - \frac{1 - (\omega_1^{(n)} + \omega_2^{(n)})}{\omega_1^{(n)}} T + \frac{\omega_2^{(n)}}{\omega_1^{(n)}}$$

$$t^{(n)} = \frac{1 - (\omega_1^{(n)} + \omega_2^{(n)})}{2\omega_1^{(n)}} + \sqrt{D^{(n)}}$$

The numbers $\omega_i^{(n)}$ were defined in Lemma 17. An easy calculation yields that the discriminant $D^{(n)}$ of Equation 5 is nonnegative if and only if $\sqrt{\omega_1^{(n)}} + \sqrt{\omega_2^{(n)}} \leq 1$. The latter inequality holds. Observe that it follows easily from Lemma 17 that $\lim_{n\to\infty} \omega_1^{(n)} = \left(\prod_{i=1}^{r} \frac{1}{p_i}\right)^2$, and $\lim_{n\to\infty} \omega_2^{(n)} = \left(1 - \prod_{i=1}^{r} \frac{1}{p_i}\right)^2$. Consequently, $\lim_{n\to\infty} t^{(n)} = \frac{p_1 \cdot \ldots \cdot p_r - 1}{p_1 \cdot \ldots \cdot p_r}$, since $\lim_{n\to\infty} D^{(n)} = 0$.

Now we define the following matrix $\tilde{A}$ indexed by $\mathcal{R} \times \mathcal{R}$.

$$\tilde{a}_{\mathbf{xy}} \stackrel{def}{=} \begin{cases} t^{(n)} \cdot p_1 \cdot \ldots \cdot p_r & \mathbf{x}^T\mathbf{y} = 0; \\ -p_1 \cdot \ldots \cdot p_r & \text{otherwise,} \end{cases}$$

which is order–equivalent to the corresponding submatrix of $2M^{\mathrm{ORT}^{[m]}} - J$. It can be show that $\tilde{A}^T A = d \cdot I$, for sufficiently large n. The claim follows from Corollary 13 now. □

3 Graph Accessibility Problems

In order to make graph accessibility problems tractable for the model of distributed computation, we assume that the set of input variables is partitioned in an arbitrary way into two sets of equal size. If we speak about projection reductions to GAPs in the sequel, we always mean ones which respect the preassigned partition. As usual, the graphs under consideration are represented by adjacency vectors of $\{0,1\}^{n^2}$, where n denotes the number of nodes. We visualize the graph, which is the transpose[3] $\pi_n^t(\boldsymbol{\sigma})$ of a vector $\boldsymbol{\sigma} \in \Sigma^n$, in such a way that the edges which are not constant are drawn as thin lines and are labelled by the corresponding predicates (see Figure 2). All other edges are drawn as thick lines.

We start with an easy graph theoretical lemma which shows that any partition of the complete graph provides "enough space" to define a projection reduction that respects a given partition.

Lemma 19. *[10] Let $E_1 \cup E_2$ be any partition of the set of all edges $\{1,\ldots,n\} \times \{1,\ldots,n\}$ into two sets of equal size $\frac{n(n-1)}{2}$. Then there are subsets $E_1' \subseteq E_1$ and $E_2' \subseteq E_2$ such that*

- *$\#E_i' \geq \lfloor n/8 - 1 \rfloor$*
- *the edges from $E_1' \cup E_2'$ are pairwise vertex–disjoint*
- *neither vertex 1 nor vertex n is incident with any edge from $E_1' \cup E_2'$.* □

Now we give some projection reductions from $\neg ORT^{[m]}$ to GAP (Proposition 20) and from $\neg ORT^{[m]}$ to MOD_m-GAP (Proposition 21) which seem to be interesting on their own.

Proposition 20. *Assume that the input variable set of* GAP *is partitioned in an arbitrary way into two subsets of equal size. Then $\neg\mathrm{ORT}^{[2]} = (\neg\mathrm{ORT}_N)_{N\in\mathbb{N}}$ is reducible to* GAP *via a $(O(n^4))$–projection reduction which respects that partition.* □

Proof. The basic idea is very similar to that of computing parity by means of branching programs in linear size. We have to construct a directed graph of width 2 which counts modulo 2 for each problem instance of $\sum_{i=1}^{n} t_i \cdot u_i$ the number of indices i for which $t_i u_i = 1$. □

Proposition 21. *Let $m \in \mathbb{N}$. Assume that the input variables of* MOD_m-GAP *are partitioned in an arbitrary way into two subsets of equal size. Then $\neg\mathrm{ORT}^{[m]} = (\neg\mathrm{ORT}_N^{[m]})_{N\in\mathbb{N}}$ is reducible to* MOD_m-GAP *via a $\left((4\binom{m}{2}+1)^2 \cdot n^4\right)$–projection reduction which respects that partition.*

[3] The *transpose* $\pi_n^t : \{0,1\}^n \to \{0,1\}^m$ of the projection reduction π is defined by $\pi_n^t(\mathbf{u}) = (\pi_n(y_1)(\mathbf{u}),\ldots,\pi_n(y_m)(\mathbf{u}))$, where $\mathbf{u} = (x_1(\mathbf{u}),\ldots,x_n(\mathbf{u})) \in \{0,1\}^n$.

Proof. Let $Y \cup Z$ be the preassigned partition of the set of variables of $\text{MOD}_m\text{-GAP}_{n(n-1)}$ and let

$$Y \supseteq Y' \stackrel{def}{=} \left\{ x_{i_{\kappa,\nu} j_{\kappa,\nu}} \mid \kappa = 1, \ldots, r/\binom{m}{2}, \nu = 1, \ldots, \binom{m}{2} \right\}$$
$$Z \supseteq Z' \stackrel{def}{=} \left\{ x_{k_{\kappa,\nu} l_{\kappa,\nu}} \mid \kappa = 1, \ldots, r/\binom{m}{2}, \nu = 1, \ldots, \binom{m}{2} \right\}$$

be the two subsets whose existence is insured by Lemma 19. Then we have $r = \lfloor n/8 - 1 \rfloor$ and we assume w.l.o.g. that r is divisible by $\binom{m}{2}$, since m is a universal constant. The projection reduction

$$\pi_{2r/\binom{m}{2}} : \{x_{i,j}\} \to \left\{ 0, 1, (t_\nu = a), (u_\nu = a) \mid \nu = 1, \ldots, r/\binom{m}{2}, a \in \mathbb{Z}/m\mathbb{Z} - \{0\} \right\}$$

is defined by means of Figure 2 and Figure 1, in which the transpose $\pi^t_{2r/\binom{m}{2}}$ is shown.

If $(\mathbf{t}, \mathbf{u}) \in \{0,1\}^{2r/\binom{m}{2}}$, then an easy calculation reveals that for the number $\left[1 \stackrel{\pi^t(\mathbf{t},\mathbf{u})}{\longrightarrow} n\right]$ of directed paths from vertex 1 to vertex n in the graph $\pi^t(\mathbf{t}, \mathbf{u})$ holds

$$\left[1 \stackrel{\pi^t(\mathbf{t},\mathbf{u})}{\longrightarrow} n\right] \equiv \mathbf{t}^T \mathbf{u} \pmod{m},$$

where $\mathbf{t}^T \mathbf{u}$ denotes the standard inner product. □

Putting altogether one obtain the announced main theorem of this paper.

Theorem 22.

1. *It holds* $\text{MAJ-Comm}(\text{GAP}_n) = \Omega(n)$.
2. *Let m be an arbitrary number. Then* $\text{MAJ-Comm}(\text{MOD}_m\text{-GAP}_n) = \Omega(n)$. □

References

1. A. V. Aho, J. D. Ullman, M. Yannakakis, *On notions of information transfer in VLSI circuits*, in: Proc. 15th ACM STOC 1983, pp. 133–183.
2. L. Babai, P. Frankl, J. Simon, *Complexity classes in communication complexity theory*, in: Proc. 27th IEEE FOCS, pp. 337–347, 1986.
3. B. Halstenberg, R. Reischuk, *Relations between Communication Complexity Classes*, in: Proc. 3rd IEEE Structure in Complexity Theory Conference, pp. 19–28, 1988.
4. C. Damm, M. Krause, Ch. Meinel, St. Waack, *Separating counting communication complexity classes*, in: Proc. 9th STACS, Lecture Notes in Computer Science **577**, Springer Verlag 1992, pp. 281–293.
5. A. Hajnal, W. Maass, G. Turan, *On the communication complexity of graph problems*, in: Proc. 20th ACM STOC 1988, pp. 186–191.
6. N. Immerman, *Languages that capture complexity classes*, SIAM J. Comput., **16**(4)(1978), pp. 760–778.
7. M. Krause, St. Waack, *Variation ranks of communication matrices and lower bounds for depth two circuits having symmetric gates with unbounded fan–in*, in: Proc. 32nd IEEE FOCS 1991, pp. 777–782.
8. Ch. Meinel, *p-Projection reducibility and the complexity classes L(nonuniform) and NL(nonuniform)*, in: Proc. 12th MFCS, 1986, LNCS 233, 527–535.
9. Ch. Meinel, *Modified branching programs and their computational power*, LNCS 370, Springer-Verlag, 1989.
10. Ch. Meinel, St. Waack, *Upper and lower bounds for certain graph-accessibility problems on bounded alternating ω-branching programs*, in: Complexity Theory - current research, Eds. K. Ambos-Spies, S. Homer, U. Schöning, Cambridge University Press 1993, 273–290.
11. Ch. Meinel, St. Waack, *Lower Bounds on the Modular Communication Complexity of various graph-accessibility problems*, in: Proc. LATIN'95, LNCS 911, 427–435.
12. K. Mehlhorn, E. M. Schmidt, *Las Vegas is better than determinism in VLSI and distributed computing*, in: Proc. 14th ACM STOC 1982, pp. 330–337.
13. R. Paturi, J. Simon, *Probabilistic communication complexity*, Journ. of Computer and System Science **33**(1986), pp. 106–124.
14. R. Raz, B. Spieker, *On the "log rank"–conjecture in communication complexity*, in: Proc. 34th IEEE FOCS 1993, pp. 168–176.
15. W. Savitch, *Relationship between nondeterministic and deterministic tape complexities*, J. Comput. System Sci. **4**(1970), pp. 244–253.
16. Skyum, L. V. Valiant, *A complexity theory based on Boolean algebra*, Proc. 22nd IEEE FOCS, pp. 244-253.
17. A. Yao, *The entropic limitations of VLSI computations*, Proc. 13th ACM STOC 1981, pp. 308–311.

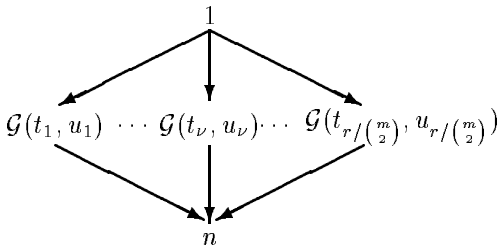

Figure 1. The graph transposed to the instance $(\mathbf{t}, \mathbf{u})$ of $\neg\mathrm{ORT}^{[m]}$

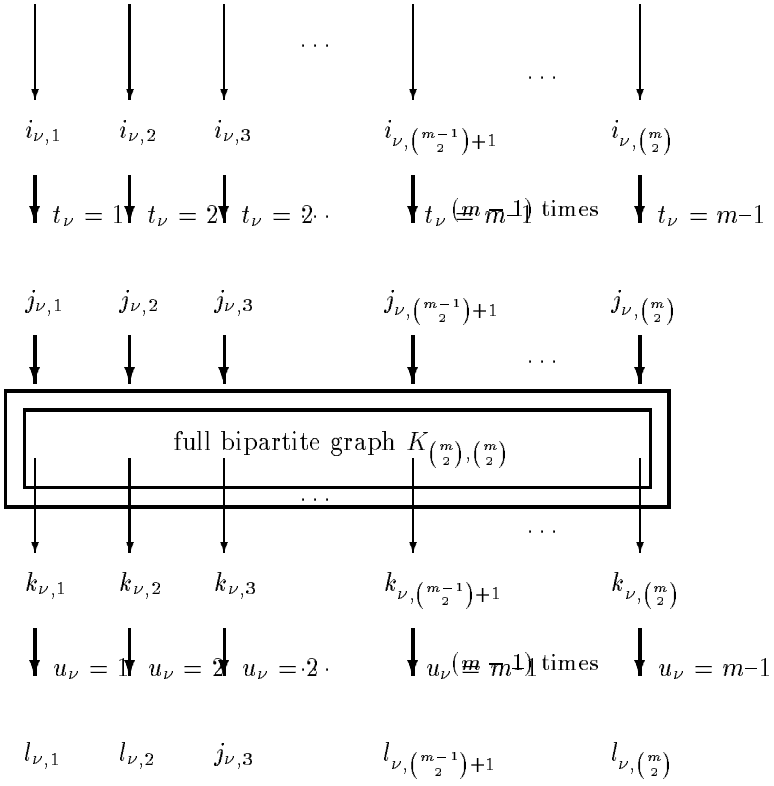

Figure 2. *The subgraph $\mathcal{G}(t_\nu, u_\nu)$ of Figure 1.*

This article was processed using the LaTeX macro package with LLNCS style