RAIRO-Inf. Theor. Appl. **39** (2005) 687-706
DOI: 10.1051/ita:2005037

ONE-WAY COMMUNICATION COMPLEXITY OF SYMMETRIC BOOLEAN FUNCTIONS*

Jan Arpe[1, 2], Andreas Jakoby[1, 3] and Maciej Liśkiewicz[1, 4]

Abstract. We study deterministic one-way communication complexity of functions with Hankel communication matrices. Some structural properties of such matrices are established and applied to the one-way two-party communication complexity of symmetric Boolean functions. It is shown that the number of required communication bits does not depend on the communication direction, provided that neither direction needs maximum complexity. Moreover, in order to obtain an optimal protocol, it is in any case sufficient to consider only the communication direction from the party with the shorter input to the other party. These facts do not hold for arbitrary Boolean functions in general. Next, gaps between one-way and two-way communication complexity for symmetric Boolean functions are discussed. Finally, we give some generalizations to the case of multiple parties.

Mathematics Subject Classification. 68Q99, 06E30, 94A05, 68R15.

1. Introduction

The communication complexity of two-party protocols was introduced by Yao [17] in 1979. The theory of communication complexity evolved into an important branch of computational complexity (for a general survey of the theory see *e.g.* Kushilevitz and Nisan [10]).

Keywords and phrases. Communication complexity, Boolean functions, Hankel matrices.

* *A preliminary version of these results has been presented at 14th International Symposium on Fundamentals of Computation Theory (FCT 2003) and published in Lect. Notes Comput. Sci.* **2751**, *Springer-Verlag (2003) 158–170.*

[1] Institut für Theoretische Informatik, Universität zu Lübeck, Razeburger Allee 160, 23538 Lübeck, Germany; arpe@tcs.uni-luebeck.de;jakoby@tcs.uni-luebeck.de; liskiewi@tcs.uni-luebeck.de

[2] *Supported by DFG research grant Re 672/3.*

[3] *Part of this work was done while visiting International University Bremen, Germany.*

[4] *On leave from Instytut Informatyki, Uniwersytet Wrocławski, Wrocław, Poland.*

© EDP Sciences 2005

Article published by EDP Sciences and available at http://www.edpsciences.org/ita or http://dx.doi.org/10.1051/ita:2005037

In this paper we consider one-way communication, *i.e.* we restrict the communication to a single round. This simple model has been investigated by several authors for different types of communication such as fully deterministic, probabilistic, nondeterministic, and quantum (see *e.g.* [1,4,8,9,12,13,17]). We study the deterministic setting. One-way communication complexity finds application in a wide range of areas, *e.g.* it provides lower bounds on VLSI complexity and on the size of finite automata (*cf.* [6]). Moreover, one-way communication complexity of symmetric Boolean functions is connected with binary decision diagrams by the following observation due to Wegener [16] (see also [14]): the size of an optimal protocol coincides with the number of nodes at a certain level in a minimal OBDD.

We consider the standard two-party communication model: initially the parties, called Alice and Bob, hold disjoint parts of input data x and y, respectively. In order to compute a function $f(x, y)$, they exchange messages between each other according to a communication protocol.

In a (deterministic) one-way protocol $\mathcal{P}$ for f, one of the parties sends a single message to the other party, and then the latter party computes the output $f(x, y)$. We call $\mathcal{P}$ a protocol of type $A \to B$ if Alice sends to Bob and of type $B \to A$ if Bob sends to Alice. The size of $\mathcal{P}$ is the number of different messages that can potentially be transmitted *via* the communication channel according to $\mathcal{P}$. The one-way communication size $S^{A\to B}(f)$ of f is the size of the best protocol of type $A \to B$. It is clear that the respective one-way communication complexity is $C^{A\to B}(f) = \lceil \log S^{A\to B}(f) \rceil$. For the case when Bob sends messages to Alice, we analogously use the notation $S^{B\to A}$ and $C^{B\to A}$. Note that throughout this paper, log always denotes the binary logarithm.

The main results of this paper deal with one-way communication complexity of symmetric Boolean functions – an important subclass of all Boolean functions. A Boolean function F is called symmetric, if permuting the input bits does not affect the function value. Some examples for symmetric functions are *and, or, parity, majority,* and arbitrary *threshold* functions. We assume that to compute F Alice holds m input bits and Bob holds n bits. As the function value of a symmetric Boolean function only depends on the number of 1's in the input (*cf.* [15]), it is completely determined by the sum of the number of 1's in Alice's input part and the number of 1's in Bob's part. Hence for such functions, we are faced with the problem of determining the one-way communication complexity of a function

$$f : \{0, \ldots, m\} \times \{0, \ldots, n\} \to \{0, 1\}$$

associated to F, where $f(x, y)$ only depends on the sum $x + y$. Note that $S^{A\to B}(F) \leq m + 1$ is a trivial upper bound on the one-way communication size of F.

Let us assume that Alice's input part is at most as large as Bob's is (*i.e.* let $m \leq n$). While for arbitrary functions this property does not imply which communication direction admits the better one-way protocols, we show that the converse is true for symmetric Boolean functions F, namely in this case we have $C^{A\to B}(F) \leq C^{B\to A}(F)$. Moreover, we prove that if some protocol of type $A \to B$

does not require maximal size, *i.e.* if $S^{A\to B}(F) < m+1$, then both directions yield the same complexities, *i.e.* $C^{A\to B}(F) = C^{B\to A}(F)$.

We also present a class of families of symmetric Boolean functions for which one-way communication is *almost* as powerful as two-way communication. More precisely, for any family of symmetric Boolean functions $F_1, F_2, F_3 \ldots$ with

$$F_m : \{0,1\}^{2m} \to \{0,1\},$$

let $f_m : \{0,\ldots,m\} \times \{0,\ldots,m\} \to \{0,1\}$ denote the integer function associated to F_m. We prove that if $f_m \subseteq f_{m+1}$ for all $m \in \mathbb{N}$, then either the one-way communication complexities of $F_1, F_2, F_3 \ldots$ are almost all equal to a constant c or the two-way communication complexities of $F_1, F_2, F_3 \ldots$ are infinitely often maximal. We show that one can easily test whether the first or the second case occurs: The two-way communication complexities are infinitely often maximal if and only if the unary language $\{0^{k+\ell} \mid f_{k+\ell}(k,\ell) = 1,\ k,\ell \in \mathbb{N}\}$ is nonregular.

On the other hand, we construct an example of a symmetric Boolean function having one-way communication complexity exponentially larger than its two-way communication complexity. Finally, we generalize the two-party model to the case of multiple parties and extend our results to such a setting.

Our proofs are based on the fact that the communication matrix of the integer function f associated with a symmetric Boolean function F is a Hankel matrix. In general, the entries of the communication matrix M_f of f are defined by $m_{i,j} = f(i,j)$. A Hankel matrix is a matrix in which the entries on each anti-diagonal are constant (equivalently, $m_{i,j}$ only depends on $i+j$). Hankel matrices are completely determined by the entries of their first rows and their last columns. Thus with any $(m+1)\times(n+1)$-Hankel matrix H we associate a function f_H such that $f_H(0), f_H(1), \ldots, f_H(n)$ compose the first row of H and $f_H(n), f_H(n+1), \ldots, f_H(m+n)$ make up its last column. One of the main technical contributions of this paper is a theorem saying that if $m \le n$ and H has less than $m+1$ different rows, then f_H is periodic on a certain large interval. We apply this property to the one-way communication size using a known relationship between this measure and the number of different rows in communication matrices.

As a byproduct, we obtain a word combinatorial property: let w be an arbitrary string over some alphabet Σ. Then, for $m \le \lceil |w|/2 \rceil$ and $n = |w| - m + 1$, the number of different substrings of w of length n is at most as large as the number of different substrings of w of length m. Moreover, if the former number is strictly less than m (note that it can be at most m in general), then the number of different substrings of length n and the number of different substrings of length m coincide.

The paper is organized as follows: in Section 2, we introduce basic definitions and notation. Section 3 deals with the examination of the number of different rows and columns in Hankel matrices involving certain periodicity properties. In Section 4, we state some applications of these properties. Then, in Section 5, we present a class of symmetric Boolean functions with both maximal one-way and two-way communication complexity, and then we construct a symmetric Boolean

function with an exponential gap between its one-way and its two-way communication complexity. Finally, in Section 6, we discuss natural extensions of our results to the case of multiple parties.

2. Preliminaries

For any integers $0 \leq k < k'$, let $[k..k']$ denote the set $\{k, k+1, \ldots, k'\}$, and denote $[0..k]$ by $[k]$ for short. By $\mathbb{N}$ we denote the set of nonnegative integers. We consider deterministic one-way communication protocols between Alice and Bob for functions $f : [m] \times [n] \to \Sigma$, where Σ is an arbitrary (finite or infinite) nonempty set. More specifically, we assume that Alice holds a value $x \in [m]$, and Bob holds a value $y \in [n]$ for some fixed positive integers m and n. Their aim is to compute the value $f(x, y)$.

Let $\mathcal{M}_\Sigma(m, n)$ denote the set of all $(m+1) \times (n+1)$ matrices $M = (m_{i,j})$ with $m_{i,j} \in \Sigma$. We will frequently omit the index Σ when it is understood from the context. It will be convenient for us to enumerate the rows from 0 to m and the columns from 0 to n. For a given function $f : [m] \times [n] \to \Sigma$, we denote by M_f the corresponding communication matrix in $\mathcal{M}(m, n)$.

Definition 1. For a matrix $M \in \mathcal{M}(m, n)$, define $\#\mathrm{row}(M)$ to be the number of different rows of M, and similarly let $\#\mathrm{col}(M)$ be the number of different columns of M. Furthermore, for any $i, j \in [m]$, let $i \sim_M j$ denote that the rows i and j of M are equal.

Since the sender has to specify the type of row (resp. column) his input belongs to, it is easy to characterize the one-way communication size by #row and #col.

Fact 1. *For all $m, n \in \mathbb{N}$ and for every function $f : [m] \times [n] \to \Sigma$, it holds that* $S^{A \to B}(f) = \#\mathrm{row}(M_f)$ *and* $S^{B \to A}(f) = \#\mathrm{col}(M_f)$.

In this paper we will restrict ourselves to functions f that only depend on the sum of the arguments. Note that for such functions f the communication matrix M_f is a Hankel matrix. The problem of finding protocols for such restricted f arises naturally when one considers symmetric Boolean functions.

Definition 2. Let $f : [s] \to \mathbb{N}$, $\lambda \geq 1$ and $s_1, s_2 \in [s]$ with $s_1 \leq s_2 - \lambda$. We call f *λ-periodic on* $[s_1..s_2]$, if for all $x \in [s_1..s_2 - \lambda]$, $f(x) = f(x + \lambda)$.

Obviously, f is λ-periodic on $[s_1..s_2]$ if and only if for all $x, x' \in [s_1..s_2]$ with $\lambda \mid (x - x')$, it holds that $f(x) = f(x')$.

3. Periodicity of rows and columns in Hankel matrices

This section is devoted to examine the relationship between the number of different rows and the number of different columns in a Hankel matrix. Lemmas 1 through 3 are technical preparations for Theorem 1 which gives an explicit characterization of a certain periodic behaviour of the function associated with a Hankel

matrix and of the Hankel matrix itself. Theorems 2 and 3 reveal all possible constellations of values for $\#\mathrm{row}(H)$ and $\#\mathrm{col}(H)$ for a Hankel matrix H. The results will be applied to the theory of one-way communication in Section 4.

Fact 2. *Let $f : [s] \to \mathbb{N}$ be λ-periodic on $[s_1..s_2] \subseteq [s]$ and on $[t_1..t_2] \subseteq [s]$ such that $s_1 \le t_1$ and $t_1 + \lambda \le s_2$. Then f is λ-periodic on $[s_1..t_2]$.*

Proof. Let $x \in [s_1..t_2 - \lambda]$. If $x \le t_1$, then $s_1 \le x \le x + \lambda \le t_1 + \lambda \le s_2$, so $f(x) = f(x + \lambda)$ because of the λ-periodicity on $[s_1..s_2]$. On the other hand, if $x > t_1$, then $f(x) = f(x + \lambda)$ because of the λ-periodicity on $[t_1..t_2]$. □

Lemma 1. *Let $H \in \mathcal{M}(m, n)$ be a Hankel matrix, $m_0, m_1 \in [m]$ with $m_0 < m_1$, and $\lambda \in [1..m_1 - m_0]$. Then the following two statements are equivalent:*

(a) *f_H is λ-periodic on $[m_0..m_1 + n]$.*
(b) *For all $x \in [m_0..m_1]$ and all $k \in \mathbb{N}$ such that $x + k\lambda \le m_1$, $x \sim_H x + k\lambda$.*

Proof. "(a)⇒(b)": Let $x \in [m_0..m_1]$ and $k \in \mathbb{N}$ such that $x + k\lambda \le m_1$. For all $y \in [n]$,

$$x + y \ge m_0 \quad \text{and} \quad x + y + k\lambda \le m_1 + n.$$

Since f_H is λ-periodic on $[m_0..m_1 + n]$, we have $f_H(x + y) = f_H(x + k\lambda + y)$. "(b)⇒(a)": Let $x \in [m_0..m_1 + n - \lambda]$. We consider two cases. If $x \le m_0 + n$, then $f_H(x) = f_H(m_0 + (x - m_0)) = f_H(m_0 + \lambda + (x - m_0)) = f_H(x + \lambda)$, because $m_0 \sim_H m_0 + \lambda$ by hypothesis. If on the other hand $x > m_0 + n$, then $x - n > m_0$ and $x - n + \lambda \le m_1$. By hypothesis, $x - n \sim_H x - n + \lambda$, and thus $f_H(x) = f_H(x - n + n) = f_H(x - n + \lambda + n) = f_H(x + \lambda)$. □

Corollary 1. *Let $H \in \mathcal{M}(m, n)$ be a Hankel matrix and $i, j \in [m]$ with $i < j$. Then $i \sim_H j$ if and only if f_H is $(j - i)$-periodic on $[i..j + n]$.*

Corollary 2. *Let $H \in \mathcal{M}(m, n)$ be a Hankel matrix. If f_H is λ-periodic on $[m_0..m_1 + n]$ for some $m_0, m_1 \in [m]$ with $m_0 < m_1$ and some $\lambda \in [1..m_1 - m_0]$, then $\#\mathrm{row}(H) \le m_0 + \lambda + m - m_1$, where equality holds if and only if all rows $0, \ldots, m_0 + \lambda - 1$ and $m_1 + 1, \ldots, m$ are pairwise different.*

Lemma 2. *Let $H \in \mathcal{M}(m, n)$ be a Hankel matrix and $m_0, m_0', i, j \in [m]$ such that $m_0 \le i < j$, $m_0' - m_0 \le n + 1$, $j - m_0 \le n + 1$, $i \sim_H j$, and $m_0 \sim_H m_0'$. Then f_H is $(j - i)$-periodic on $[m_0..j + n]$.*

Proof. Choose $\lambda = j - i$ and $\mu_0 = m_0' - m_0$. By Corollary 1, f_H is

(i) μ_0-periodic on $[m_0..m_0' + n]$ and
(ii) λ-periodic on $[i..j + n]$.

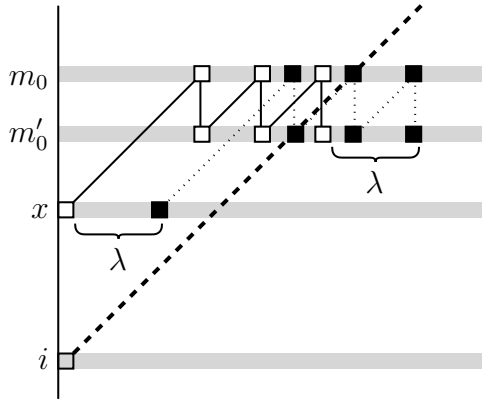

FIGURE 1. An illustration of Case 1.

Let $x \in [m_0..j+n-\lambda]$. In order to show that $f_H(x+\lambda) = f_H(x)$, we consider:

Case 1 ($m_0 \le x < i$)**.** Let $k \in \mathbb{N}$ such that $i \le x + k\mu_0 \le i + \mu_0 - 1$. We need to show that

$$x, x+k\mu_0, x+k\mu_0+\lambda, x+\lambda \in [m_0..m_0'+n] \quad \text{and} \tag{1}$$

$$x+k\mu_0, x+k\mu_0+\lambda \in [i..j+n] \tag{2}$$

in order to apply properties (i) and (ii) to the corresponding elements. Property (1) follows from $m_0 \le x$ and $x+k\mu_0+\lambda \le i+\mu_0+\lambda-1 = j+m_0'-m_0-1 \le m_0'+n$. Property (2) is due to $i \le x+k\mu_0$ and $x+k\mu_0+\lambda \le j-1+\mu_0 \le j+n$. Now (*cf.* Fig. 1) $f_H(x) = f_H(x+k\mu_0) = f_H(x+k\mu_0+\lambda) = f_H(x+\lambda)$, where the first and the last equality follow from properties (1) and (i), and the middle equality is due to properties (2) and (ii).

Case 2 ($i \le x \le j+n-\lambda$)**.** In this case, $f_H(x) = f_H(x+\lambda)$ by Corollary 1. □

The following lemma is symmetric to the previous one:

Lemma 3. *Let $H \in \mathcal{M}(m,n)$ be a Hankel matrix and $m_1, m_1', i, j \in [m]$ such that $i < j \le m_1$, $m_1 - m_1' \le n+1$, $m_1 - i \le n+1$, $i \sim_H j$, and $m_1 \sim_H m_1'$. Then f_H is $(j-i)$-periodic on $[i..m_1+n]$.*

Proof. Let $H = (h_{i,j})$. We define $\lambda = j - i$ and $H' = (h'_{\mu,\nu}) \in \mathcal{M}(m,n)$ by $h'_{\mu,\nu} = h_{m-\mu,n-\nu}$ for $(\mu,\nu) \in [m]\times[n]$, *i.e.* we rotate H by 180 degrees in the plane. Clearly, H' is again a Hankel matrix. Moreover, we have $f_H(z) = f_{H'}(m+n-z)$ for all $z \in [m+n]$. We set $m_0 = m-m_1$, $m_0' = m-m_1'$, $i' = m-j$, and $j' = m-i$. Now it is easy to check that $H', i', j', m_0,$ and m_0' fulfill the preconditions of Lemma 2 and $m+n-x-\lambda \in [m_0..j'+n-\lambda]$, thus yielding

$$f_H(x+\lambda) = f_{H'}(m+n-x-\lambda) = f_{H'}(m+n-x) = f_H(x). \qquad \square$$

Theorem 1. *Let $m \leq n+1$ and $H \in \mathcal{M}(m,n)$ be a Hankel matrix with $\#\mathrm{row}(H) < m+1$. Then there exist $\lambda \in [1..n]$ and $m_0, m_1 \in [m]$ with $m_1 - m_0 \geq \lambda$ such that the following two properties hold:*

(a) *The function f_H is λ-periodic on $[m_0..m_1+n]$.*

(b) *If $i,j \in [m]$ with $i<j$ and $i \sim_H j$, then $i,j \in [m_0..m_1]$ and $\lambda \mid (j-i)$.*

Moreover, m_0, m_1 and λ can be explicitly determined as follows:

$$\begin{aligned} m_0 &= \min\{k \in [m] \mid \exists k' \in [m] \text{ with } k' > k \text{ and } k \sim_H k'\},\\ m_1 &= \max\{k \in [m] \mid \exists k' \in [m] \text{ with } k' < k \text{ and } k \sim_H k'\}, \quad \text{and}\\ \lambda &= \min\{j-i \mid i,j \in [m] \text{ with } i \sim_H j \text{ and } i<j\}. \end{aligned}$$

Proof. Since $\#\mathrm{row}(H) < m+1$, there exist $i,j \in [m]$ with $i<j$ such that $i \sim_H j$. Thus, m_0, m_1 and λ are well-defined. Clearly, $m_1 - m_0 \geq \lambda$. Choose $i_0, j_0 \in [m]$ such that $i_0 \sim_H j_0$ and $j_0 - i_0 = \lambda$. Since $m \leq n$, all preconditions of Lemmas 2 and 3 are satisfied. Thus we conclude that f_H is λ-periodic on both discrete intervals $[m_0..j_0+n]$ and $[i_0..m_1+n]$. Fact 2 now yields property (a). Now let $i,j \in [m]$ with $i<j$ and $i \sim_H j$. Let $k \in \mathbb{N}$ such that $j-i = k\lambda + r$ with $0 \leq r < \lambda$. By property (a), f_H is λ-periodic on $[m_0..m_1+n]$, and so by Lemma 1 (note that $i+k\lambda = j-r \leq j \leq m_1$), we have $i+k\lambda \sim_H i \sim_H j$. As $r = j-i-k\lambda < \lambda$ and λ is the minimal difference between two equal rows of different indices, we have $r=0$, so $\lambda \mid (j-i)$. □

Using Corollary 2 we deduce two consequences of Theorem 1:

Corollary 3. *For H, m_0, m_1 and λ as in Theorem 1, $\#\mathrm{row}(H) = m_0 + \lambda + m - m_1$, i.e. H has exactly $m_0 + \lambda + m - m_1$ pairwise different rows.*

Corollary 4. *Let $m \leq n+1$ and $H \in \mathcal{M}(m,n)$ be a Hankel matrix with $\#\mathrm{row}(H) < m+1$. Then $\#\mathrm{col}(H) \leq \#\mathrm{row}(H)$.*

Proof. Let m_0, m_1 and λ be as in Theorem 1. From Theorem 1, we have that the function $f_H = f_{H^T}$ is λ-periodic on $[m_0..m_1+n] = [m_0..(m_1+n-m)+m]$. Now Corollary 2 implies that

$$\#\mathrm{row}(H^T) \leq m_0 + \lambda + n - (m_1 + n - m) = m_0 + \lambda + m - m_1 = \#\mathrm{row}(H),$$

where the last equality is due to Corollary 3. Hence the corollary follows since we have $\#\mathrm{col}(H) = \#\mathrm{row}(H^T)$. □

The next lemma states an "expansion property" of Hankel matrices with at least two equal rows.

Lemma 4. *For arbitrary $m,n \in \mathbb{N}$ let $H \in \mathcal{M}(m,n)$ be a Hankel matrix with $\#\mathrm{row}(H) < m+1$. Then there exist $m' \geq n$ and a Hankel matrix $\tilde{H} \in \mathcal{M}(m',n)$ such that $\#\mathrm{row}(\tilde{H}) = \#\mathrm{row}(H)$ and $\#\mathrm{col}(\tilde{H}) = \#\mathrm{col}(H)$.*

Proof. We duplicate the area between two equal rows until the total number of rows exceeds the total number of columns n. This process effects neither the number of different rows nor the number of different columns. To do this we

proceed as follows. Since $\#\mathrm{row}(H) < m+1$, there exist $m_0, m_1 \in [m]$ with $m_0 < m_1$ and $m_0 \sim_H m_1$. Set $\lambda = m_1 - m_0$, and let $c \in \mathbb{N}$ such that $m + c\lambda \geq n$. We set $m' = m + c\lambda$ and define $\tilde{H} = (\tilde{h}_{i,j}) \in \mathcal{M}(m', n)$, where for $j \in [n]$,

$$\tilde{h}_{i,j} = \begin{cases} h_{i,j} & \text{if } i < m_0, \\ h_{m_0+\ell,j} & \text{if } i = m_0 + k\lambda + \ell \text{ for some } k \in [c] \text{ and some } \ell \in [\lambda - 1], \\ h_{i-c\lambda,j}, & \text{if } i \geq m_1 + c\lambda. \end{cases}$$

Now, $\tilde{H}$ is again a Hankel matrix, and both properties $\#\mathrm{row}(\tilde{H}) = \#\mathrm{row}(H)$ and $\#\mathrm{col}(\tilde{H}) = \#\mathrm{col}(H)$ hold. □

Theorem 2. *Let $m \leq n+1$ and $H \in \mathcal{M}(m,n)$ be a Hankel matrix with $\#\mathrm{row}(H) < m+1$. Then $\#\mathrm{row}(H) = \#\mathrm{col}(H)$.*

Proof. From Corollary 4, we have $\#\mathrm{row}(H) \geq \#\mathrm{col}(H)$. By Lemma 4, there exist $m' \geq n$ and a Hankel matrix $\tilde{H} \in \mathcal{M}(m', n)$ such that $\#\mathrm{row}(\tilde{H}) = \#\mathrm{row}(H)$ and $\#\mathrm{col}(\tilde{H}) = \#\mathrm{col}(H)$. Thus, again by Corollary 4, we obtain $\#\mathrm{row}(H) = \#\mathrm{row}(\tilde{H}) = \#\mathrm{col}(\tilde{H}^T) \leq \#\mathrm{row}(\tilde{H}^T) = \#\mathrm{col}(\tilde{H}) = \#\mathrm{col}(H)$. Consequently, we have $\#\mathrm{row}(H) = \#\mathrm{col}(H)$. □

Theorem 3. *Let $m \leq n$ and $H \in \mathcal{M}(m,n)$ be a Hankel matrix with $\#\mathrm{row}(H) = m+1$. Then $\#\mathrm{col}(H) \geq m+1$.*

Proof. Induction on n: For $n = m$, we have $H = H^T$ and thus

$$\#\mathrm{col}(H) = \#\mathrm{row}(H^T) = \#\mathrm{row}(H) = m+1.$$

Now suppose that $n > m$. Let $H' \in \mathcal{M}(m, n-1)$ be the matrix H without its last column. We consider two cases:

Case 1. $n \sim_{H^T} n'$ for some $n' \in [n-1]$. Then $\#\mathrm{col}(H) = \#\mathrm{col}(H')$. In addition, $\#\mathrm{row}(H') = m+1$, because if $\#\mathrm{row}(H') \leq m$ was true, then we had $i \sim_{H'} j$ for some $0 \leq i < j \leq m$, and thus $i \sim_H j$, since $f_H(i+n) = f_H(i+n') = f_H(j+n') = f_H(j+n)$. Thus, we get $\#\mathrm{col}(H) = \#\mathrm{col}(H') \geq m+1$ by induction hypothesis.

Case 2. $n \not\sim_{H^T} n'$ for all $n' \in [n-1]$. Then $\#\mathrm{col}(H) = \#\mathrm{col}(H') + 1$. Once again, we have to consider two subcases:

Case 2a. $\#\mathrm{row}(H') = m+1$: Then $\#\mathrm{col}(H) = \#\mathrm{col}(H') + 1 = m+2 > m+1$ by induction hypothesis.

Case 2b. $\#\mathrm{row}(H') \leq m$: Assume that $\#\mathrm{row}(H') < m$, let

$$\begin{aligned} m_0 &= \min\{k \in [m] \mid \exists k' \in [m] \text{ with } k' > k \text{ and } k \sim_H k'\}, \\ m_1 &= \max\{k \in [m] \mid \exists k' \in [m] \text{ with } k' < k \text{ and } k \sim_H k'\}, \\ \lambda &= \min\{k' - k \mid k, k' \in [m] \text{ with } k < k' \text{ and } k \sim_H k'\}, \end{aligned}$$

and let m_0', m_1' and λ' be the corresponding numbers for H'. By Corollary 3, we have $\#\mathrm{row}(H') = m_0' + m - m_1' + \lambda'$, and by Theorem 1 f is λ'-periodic on $[m_0'..m_1' + n - 1]$. Since $\#\mathrm{row}(H') < m$ by assumption, $\lambda' < m_1' - m_0'$.

In particular, $m_0 \sim_H m_0 + \lambda'$, and thus $\lambda \mid \lambda'$ by Theorem 1. Consequently, $m_0 \le m_0'$, $m_1 \ge m_1' - 1$ and $\lambda \le \lambda'$. Hence again by Corollary 3,

$$\begin{aligned} \#\mathrm{row}(H) &= m_0 + m - m_1 + \lambda \le m_0' + m - (m_1' - 1) + \lambda' \\ &\le m_0' + m - m_1' + \lambda' + 1 = \#\mathrm{row}(H') + 1 < m + 1, \end{aligned}$$

contradicting $\#\mathrm{row}(H) = m+1$. Thus, $\#\mathrm{row}(H') = m$. By Theorem 2, $\#\mathrm{col}(H') = \#\mathrm{row}(H') = m$. Consequently, $\#\mathrm{col}(H) = \#\mathrm{col}(H') + 1 = m + 1$. □

We summarize Theorems 2 and 3 as follows.

Theorem 4. *Let $m \le n$ and $H \in \mathcal{M}(m,n)$ be a Hankel matrix. Then the following properties hold:*

(a) $\#\mathrm{row}(H) \le \#\mathrm{col}(H)$.
(b) *If* $\#\mathrm{row}(H) < m+1$, *then* $\#\mathrm{row}(H) = \#\mathrm{col}(H)$.

Note that for Hankel matrices over Σ with $|\Sigma| \ge m+n+1$ we can say even more. Namely, if $m \le n$, then for all $r \in [m+1..n+1]$, there exists a Hankel matrix $H \in \mathcal{M}(m,n)$ with $\#\mathrm{row}(H) = m+1$ and $\#\mathrm{col}(H) = r$. To see this, define $f : [m] \times [n] \to \Sigma = \{a_0, \ldots, a_{m+n}\}$ by $f(x,y) = a_{(x+y) \bmod r}$. Then $H = M_f$ is a Hankel matrix fulfilling the requested properties.

We conclude this section by providing a generalization of Theorem 4 which will show helpful when examining the multi-party case in Section 6. For a matrix $M \in \mathcal{M}_\Sigma(m,n)$ and $r \in \Sigma$, we denote by $\#\mathrm{row}(M,r)$ the number of different rows containing r and by $\#\mathrm{col}(M,r)$ the number of different columns containing r.

Lemma 5. *Let $m \le n$ and $H \in \mathcal{M}_\Sigma(m,n)$ be a Hankel matrix and $r \in \Sigma$. Then* $\#\mathrm{row}(H,r) \le \#\mathrm{col}(H,r)$.

Proof. For unary Σ, there is nothing to show, so we first consider the case that $\Sigma = \{0,1\}$ and $r = 1$. Denote by H' the matrix obtained from H by deleting all rows and all columns that consist only of 0's. Then H' is a Hankel matrix again, $\#\mathrm{row}(H',1) = \#\mathrm{row}(H,1)$, and $\#\mathrm{col}(H',1) = \#\mathrm{col}(H,1)$. Now all rows and columns of H' contain at least one 1, so

$$\#\mathrm{row}(H,1) = \#\mathrm{row}(H',1) = \#\mathrm{row}(H') \le \#\mathrm{col}(H') = \#\mathrm{col}(H',1) = \#\mathrm{col}(H,1),$$

the inequality following from Theorem 4.

Let us now turn to an arbitrary Σ and $r \in \Sigma$: Define $H' \in \mathcal{M}_{\{0,1\}}(m,n)$ by

$$h'_{ij} = \begin{cases} 1 & \text{if } h_{ij} = r \\ 0 & \text{otherwise.} \end{cases}$$

Then $\#\mathrm{row}(H',1) \le \#\mathrm{row}(H,r)$ and $\#\mathrm{col}(H',1) \le \#\mathrm{col}(H,r)$. If H' contains two equal rows with 1's in them, *i.e.* $i \sim_{H'} j$ for some $i < j$ and $h'_{i,k} = 1$ for some $k \in [n]$, then by Corollary 1, $f_{H'}$ is $(j-i)$-periodic on $[i..j+n]$. In particular, each column j_0 of H' contains a 1, namely one of the values

$$m_{i,j_0}, m_{i+1,j_0}, \ldots, m_{j,j_0}$$

must equal 1 (otherwise $f_{H'}$ would be constantly 0 on $[i..j+n]$ contradicting $f(i+k)=1$). But then also all columns of H contain at least one r, so again by Theorem 4,

$$\#\mathrm{row}(H,r) \le \#\mathrm{row}(H) \le \#\mathrm{col}(H) = \#\mathrm{col}(H,r).$$

On the other hand, if all rows in H' containing a 1 are pairwise different, then also all rows in H containing an r are pairwise different, so

$$\#\mathrm{row}(H,r) = \#\mathrm{row}(H',1) \le \#\mathrm{col}(H',1) \le \#\mathrm{col}(H,r),$$

where the first inequality follows from the $\{0,1\}$-case shown above. □

4. Applications

Theorem 4 can be restated in terms of one-way communication:

Theorem 5. *Let $m \le n$ and $f : [m] \times [n] \to \Sigma$ be a function for which the corresponding communication matrix M_f is a Hankel matrix. Then the following properties hold:*

(a) $S^{A\to B}(f) \le S^{B\to A}(f)$.
(b) *If $S^{A\to B}(f) < m+1$, then $S^{A\to B}(f) = S^{B\to A}(f)$.*

This result can immediately be applied to symmetric Boolean functions:

Corollary 5. *Let $m \le n$ and $F : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ be a symmetric Boolean function. Then the following properties hold:*

(a) $S^{A\to B}(F) \le S^{B\to A}(F)$.
(b) *If $S^{A\to B}(F) < m+1$, then $S^{A\to B}(F) = S^{B\to A}(F)$.*

Proof. The communication matrix M_f of the function $f : [m] \times [n] \to \{0,1\}$ defined by

$$f(x,y) = F((\underbrace{1,\dots,1}_{x},\underbrace{0,\dots,0}_{m-x}),(\underbrace{1,\dots,1}_{y},\underbrace{0,\dots,0}_{n-y}))$$

is a Hankel matrix. Thus the claim follows from Theorem 5. □

The results of the last paragraph can also be applied to word combinatorics:

Theorem 6. *Let w be an arbitrary string over some alphabet Σ, and let $N_w(i)$ denote the number of different subwords of w of length i. Then, for $m \le \lceil |w|/2 \rceil$ and $n = |w| - m + 1$, we have $N_w(n) \le N_w(m)$. Moreover, if $N_w(n) < m$ (note that $N_w(n) \le m$ in general), then $N_w(n) = N_w(m)$.*

Proof. Let $m \le \lceil |w|/2 \rceil$, $n = |w| - m + 1$, and $w = w_1 \dots w_{m+n-1}$ with $w_i \in \Sigma$ for $1 \le i \le m+n-1$. Define the Hankel matrix $H = (h_{i,j}) \in \mathcal{M}_\Sigma(m-1, n-1)$ by $h_{i,j} = w_{i+j+1}$. The rows of H make up the subwords of w of length n, while the columns of H compose the subwords of w of length m. Now Theorems 2 and 3 prove the claim. □

5. One-way *versus* two-way protocols

In this section we first present a class of families of functions for which one-way communication complexities are *almost* the same as two-way communication complexities. We denote the two-way complexity of F by $C(F)$. Let $F_1, F_2, F_3 \ldots$ with $F_m : \{0,1\}^{2m} \to \{0,1\}$ be a family of symmetric Boolean functions and let $f_m : [m] \times [m] \to \{0,1\}$ denote the integer function associated to F_m, *i.e.* $F(x_1, \ldots, x_{2m}) = 1$ if and only if $f(\sum_{i=1}^{m} x_i, \sum_{i=m+1}^{2m} x_i) = 1$.

Theorem 7. *Let $F_1, F_2, F_3 \ldots$ be a family of symmetric Boolean functions such that $f_m \subseteq f_{m+1}$ for all $m \in \mathbb{N}$. Then either*

(a) *for almost all $m \in \mathbb{N}$, $C^{A\to B}(F_m) = c$ for some constant c or*
(b) *for infinitely many $m \in \mathbb{N}$, $C(F_m) = \lceil \log(m+1) \rceil$.*

Moreover, (b) holds iff the language $L = \{0^{k+\ell} \mid f_{k+\ell}(k,\ell) = 1,\ k, \ell \in \mathbb{N}\}$ is nonregular.

Proof. First, Theorem 11.3 in [7] gives a nice characterization of (non)regular unary languages in terms of the rank of certain Hankel matrices. This characterization was first observed by Condon *et al.* [3]. It says that the unary language L is nonregular if and only if for infinitely many $m \in \mathbb{N}$, $\operatorname{rank}(M_{f_m}) = m+1$ (*i.e.* the communication matrix M_{f_m} has maximum rank). Second, Mehlhorn and Schmidt [11] showed that $C(f) \geq \log(\operatorname{rank}(M_f))$ for every f. Combining these facts we get that for nonregular L, $C(f_m) = \lceil \log(m+1) \rceil$ for infinitely many $m \in \mathbb{N}$.

On the other hand, if L is regular then by the Myhill-Nerode Theorem [5] the infinite matrix $M = (m_{i,j})_{i,j\in\mathbb{N}}$ defined by $m_{i,j} = 1$ iff $0^{i+j} \in L$, has constant number of different rows. Hence the theorem follows. □

Example 1. Let $F_m(x_1, x_2, \ldots, x_{2m}) = 1$ if and only if the number of 1's in the sequence $x_1, x_2, \ldots, x_{2m}$ is the square of some integer. By Theorem 7 either for all $m \in \mathbb{N}$, $C(F_m), C^{A\to B}(F_m) \leq c$ for some constant c or for infinitely many $m \in \mathbb{N}$, $C^{A\to B}(F_m) = C(F_m) = \lceil \log(m+1) \rceil$. Since the language $\{0^n \mid n$ is the square of some integer$\}$ is nonregular, the (one-way) communication complexity of F_m is maximal for infinitely many $m \in \mathbb{N}$.

Next, we construct a symmetric Boolean function with an exponential difference between its one-way and its two-way communication complexity. Let $p_0, p_1, \ldots$ with $p_i < p_{i+1}$ for all $i \in \mathbb{N}$ be the sequence of all prime numbers. According to the Prime Number Theorem, there are at least $\frac{\ell}{\log \ell}$ prime numbers in the interval $[\ell]$ for all $\ell \geq 5$. For $k = \lceil \log \log m \rceil$ and $n = 2^k \cdot (1 + \prod_{i=0}^{2^k-1} p_i)$, consider the function $f : [m] \times [n] \to \{0,1\}$ defined by $f(x,y) = 1$ iff $\lfloor \frac{z}{2^k} \rfloor \bmod p_{z \bmod 2^k} = 0$, where $z = x + y$. Using the following two-way protocol, one can see that the two-way communication complexity of f is at most $4 \log \log m$: In the first round, Bob sends $y_0 = y \bmod 2^k$ to Alice. In the second round, Alice sends $z_0 = (x + y_0) \bmod 2^k$ and $z' = \lfloor \frac{x+y_0}{2^k} \rfloor \bmod p_{z_0}$ to Bob. Finally, Bob computes $f(x,y)$ by checking whether $(\lfloor \frac{y}{2^k} \rfloor + z') \bmod p_{z_0} = 0$.

Note that $z_0 = z \bmod 2^k$. The correctness of the protocol can be seen by investigating the addition of integers using a remainder representation.

Lemma 6. $C(f) \leq 4 \log\log m$.

For the one-way communication complexity of f we obtain:

Lemma 7. $\#\mathrm{row}(M_f) = m + 1$, *i.e.* $C^{A\to B}(f) = \lceil \log(m+1) \rceil$.

The proofs of the lemmas are straightforward. We conclude the section with the following

Theorem 8. *For the symmetric Boolean function* $F : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}$ *associated with* f, *we have* $C(F) \in O(\log\log m)$ *and* $C^{A\to B}(F) \in \Theta(\log m)$.

6. Multi-party communication

So far we have analyzed the case that a fixed input partition for a function is given. However, sometimes it is also of interest to examine the communication complexity of a fixed function under *varying* the input partition. A typical question for this scenario is whether we can partition the input in such a way that the communication complexities for protocols of type $A \to B$ and $B \to A$ coincide. The main tool for these examinations is the *diversity* $\Delta(f)$ of f which we introduce below. For a function $f : [s] \to \Sigma$ and $m \in [s]$, define $f_m : [m] \times [s-m] \to \Sigma$ by $f_m(x,y) = f(x+y)$ for $x \in [m]$ and $y \in [s-m]$, and let $r_f(m) = \#\mathrm{row}(M_{f_m})$. We define $\Delta(f) = \max_{m\in[s]} r_f(m)$.

Lemma 8. *For every function* $f : [s] \to \Sigma$, *the following conditions hold:*

(a) $r_f(m) = m + 1$ *for all* $m \in [\Delta(f) - 1]$;
(b) *if* $\Delta(f) \leq \frac{s}{2}$, *then* $r_f(m) = \Delta(f)$ *for all* $m \in [\Delta(f) - 1 \,..\, s - \Delta(f) + 1]$;
(c) $r_f(m) \geq r_f(m+1)$ *for all* $m \in [\Delta(f) - 1 \,..\, s - 1]$.

Proof. Obviously, we have $r_f(m) \leq m + 1$. From the definition of f_m we can derive that the communication matrix of f_m is a Hankel matrix. The first and last part of the claim follow directly from the following observation:

> Assume that for some m we have $r_f(m) < m+1$. Then for every $i \geq m$ it holds $r_f(i) \geq r_f(i+1)$.

Below we show that the observation is true. Note first that if rows j and k in M_{f_i} are equal then in $M_{f_{i+1}}$ rows j and k are equal, too. Hence $r_f(m) < m+1$ implies that for every $i \geq m$ it holds $r_f(i) < i + 1$.

Let k be the maximum index of a row in M_{f_i} such that for some $j < k$ the rows j and k coincide. Such a pair exists because $r_f(i) < i + 1$. Since each row $\ell + 1$ of $M_{f_{i+1}}$ can be derived from row ℓ in M_{f_i} by deleting its first entry, it is true that in $M_{f_{i+1}}$ the rows $j + 1$ and $k + 1$ coincide. If $k = i$, then the number of different rows among the rows $0, \ldots, i$ in $M_{f_{i+1}}$ is at most $r_f(i)$, the number of different rows in M_{f_i}. Since the last row in $M_{f_{i+1}}$ coincides with row $j + 1$, we have $r_f(i+1) \leq r_f(i)$. If on the other hand $k < i$, then the rows $j + 1$ and

$k+1$ do not coincide in M_{f_i} (by maximality of k), so the number of different rows among rows $1,\ldots,i$ in $M_{f_{i+1}}$ is strictly smaller than in M_{f_i}. This implies $r_f(i+1) \leq (r_f(i)-1)+1 = r_f(i)$.

Let us now focus on the second part of the claim. Let $m = \Delta(f)-1$ and $n = s-\Delta(f)+1$. Then $m \leq n$ (since $\Delta(f) \leq \frac{s}{2}$) and $\#\mathrm{row}(M_{f_m}) = \Delta(f) = m+1$ by part (a). From Theorem 3 it follows that $\#\mathrm{col}(M_{f_m}) \geq m+1 = \Delta(f)$. Since $M_{f_{s-m}}$ (for arbitrary $m \in [s]$) is the transpose of M_{f_m}, we have $\#\mathrm{col}(M_{f_{s-m}}) = \#\mathrm{row}(M_{f_s})$. Consequently,

$$\begin{aligned} r_f(\Delta(f)-1) &= \Delta(f) \\ &\leq \#\mathrm{col}(M_{f_{\Delta(f)-1}}) \\ &= \#\mathrm{row}(M_{f_{s-\Delta(f)+1}}) \quad = \quad r_f(s-\Delta(f)+1). \end{aligned}$$

On the other hand, r_f is nonincreasing on $[\Delta(f)-1..s-1]$ by part (c), so $r_f(m) = \Delta(f)$ for all $m \in [\Delta(f)-1..s-\Delta(f)+1]$. □

It is an immediate consequence of Lemma 8 that $\Delta(f)$ equals the minimum m such that M_{f_m} has less than $m+1$ different rows, provided that such an m exists.

The diversity is helpful to analyze the case that more than two parties are involved. For such multi-party communication we assume that the input is distributed among d parties $P_1,\ldots,P_d$. Every party P_i knows a value $x_i \in [m_i]$. The goal is to compute a fixed function $f : [m_1] \times \ldots \times [m_d] \to \Sigma$. Analogously to communication matrices in the two-party case, we use multidimensional arrays to represent f.

Let $\mathcal{M}(m_1,\ldots,m_d)$ be the set of all d-dimensional $(m_1+1) \times \ldots \times (m_d+1)$ arrays M with entries $M(i_1,\ldots,i_d) \in \Sigma$ for $i_j \in [m_j]$, $j \in [1..d]$. M is called the *communication array* of a function f iff $M(i_1,\ldots,i_d) = f(i_1,\ldots,i_d)$. We denote the communication array of f by M_f.

Recall that in the two-party model the sender has to specify the type of row/column his input belongs to. In the multi-party case each party has to specify the type of subarray determined by his input value. Therefore, for each $k \in [1..d]$ and each $x \in [m_k]$, we define the subarray $M_x^{(k)} \in \mathcal{M}(m_1,\ldots,m_{k-1},m_{k+1},\ldots,m_d)$ of M by $M_x^{(k)}(i_1,\ldots,i_{k-1},i_{k+1},\ldots,i_d) = M(i_1,\ldots,i_{k-1},x,i_{k+1},\ldots,i_d)$ for all $0 \leq i_j \leq m_j$, $j \in [1..d] \setminus \{k\}$. Finally, for $k \in [1..d]$ we define $\#\mathrm{sub}_k(M)$ as the number of different subarrays with fixed k^{th} dimension:

$$\#\mathrm{sub}_k(M) \;=\; |\{\; M_x^{(k)} \mid x \in [m_k] \;\}| \;.$$

We call $M \in \mathcal{M}(m_1,\ldots,m_d)$ a *Hankel array*, if $M(i_1,\ldots,i_d) = M(j_1,\ldots,j_d)$ for every pair $(i_1,\ldots,i_d),(j_1,\ldots,j_d) \in [m_1]\times\ldots\times[m_d]$ with $i_1+\ldots+i_d = j_1+\ldots+j_d$. For a Hankel array $M \in \mathcal{M}(m_1,\ldots,m_d)$, let $f_M : [\sum_{i=1}^d m_i] \to \Sigma$ be defined by $f_M(x) = M(x_1,\ldots,x_d)$, if $x = x_1+\ldots+x_d$. Note that f_M is well-defined since M is a Hankel array.

Lemma 9. *For a function f such that the corresponding communication array M is a Hankel array, we have $r_{f_M}(m_k) = \#\mathrm{sub}_k(M)$ for every $k \in [1..d]$.*

Proof. Since the value of the function f depends only on the sum of its variables, it is sufficient to show the claim for $k = 1$.

Assume that for $x_1, x_1' \in [m_1]$ the corresponding subarrays $M^{(1)}_{x_1}$ and $M^{(1)}_{x_1'}$ are different. Then there exists $x_2 \in [m_2], \ldots, x_d \in [m_d]$ such that $M(x_1, x_2, \ldots, x_d) \neq M(x_1', x_2, \ldots, x_d)$ and therefore $f_M(x_1 + x_2 + \ldots + x_d) \neq f_M(x_1' + x_2 + \ldots + x_d)$ and $f_{m_1}(x_1, x_2 + \ldots + x_d) \neq f_{m_1}(x_1', x_2 + \ldots + x_d)$. Hence if two subarrays $M^{(1)}_{x_1}$ and $M^{(1)}_{x_1'}$ are different, then also the rows x_1 and x_1' in $M_{f_{m_1}}$ are different, too. This implies $r_{f_M}(m_1) \geq \#\mathrm{sub}_1(M)$.

Analogously, let us assume that for $x_1, x_1' \in [m_1]$ the rows in $M_{f_{m_1}}$ are different. Then there exists $y \in [\sum_{i \in [2..d]} m_i]$ such that $f_{m_1}(x_1, y) \neq f_{m_1}(x_1', y)$. Choosing $x_2 \in [m_2], \ldots, x_d \in [m_d]$ such that $y = x_2 + \ldots + x_d$ we get

$$\begin{aligned} & M(x_1, x_2, \ldots, x_d) = f_M(x_1 + x_2 + \ldots + x_d) = f_{m_1}(x_1, y) \\ \neq \quad & f_{m_1}(x_1', y) = f_M(x_1' + x_2 + \ldots + x_d) = M(x_1', x_2, \ldots, x_d) \ . \end{aligned}$$

Hence if rows x_1 and x_1' in $M_{f_{m_1}}$ are different then also the two subarrays $M^{(1)}_{x_1}$ and $M^{(1)}_{x_1'}$ are different. This implies $r_{f_M}(m_1) \leq \#\mathrm{sub}_1(M)$. □

To study communication complexity issues for multi-party computations, we consider the following natural extension of the one-way communication model to multiple parties. Let $P_1, \ldots, P_d$ be connected by a directed chain specified by a permutation $\pi : [1..d] \to [1..d]$, *i.e.* $P_{\pi(i)}$ can only send messages to $P_{\pi(i+1)}$ for $i \in [d-1]$. A protocol $\mathcal{P}$ that runs on such a chain is called *π-ordered*. For a π-ordered protocol $\mathcal{P}$, let the *size* $S(\mathcal{P})$ be the number of different communication sequences of $\mathcal{P}$, and let $S(\mathcal{P}, r)$ be the number of different communication sequences of $\mathcal{P}$ on inputs $z_1 \in [m_1], \ldots, z_d \in [m_d]$ with $f(z_1, \ldots, z_d) = r$. For a function f, we define $S^\pi(f)$ to be the minimum size of a π-ordered protocol for f, and for each value $r \in \Sigma$, let

$$S^\pi(f, r) \ = \min_{\mathcal{P} \text{ computes } f \text{ and is } \pi-\text{ordered}} S(\mathcal{P}, r).$$

We will now present a protocol of minimal size for a fixed chain network and functions f such that M_f is a Hankel array. During the computation the parties use the Hankel arrays M_i defined by

$$M_i(y_i, \ldots, y_d) \ = \ M_f(z_1, \ldots, z_d),$$

where $y_i = \sum_{j=1}^{i} z_{\pi(j)}$ and $y_j = z_{\pi(j)}$ for all $j \in [i+1..d]$. Furthermore, let $\Gamma_i(y_i)$ be the minimum value z such that $(M_i)^{(1)}_z = (M_i)^{(1)}_{y_i}$. The protocol works as follows:

1. $P_{\pi(1)}$ sends $\gamma_1 = \Gamma_1(x_{\pi(1)})$ to $P_{\pi(2)}$.
2. For $i \in [2..d-1]$, $P_{\pi(i)}$ receives γ_{i-1} from $P_{\pi(i-1)}$ and sends $\gamma_i = \Gamma_i(x_{\pi(i)} + \gamma_{i-1})$ to $P_{\pi(i+1)}$.
3. $P_{\pi(d)}$ receives γ_{d-1} from $P_{\pi(d-1)}$. Then $M_d(\gamma_{d-1} + x_{\pi(d)})$ is the result of the function.

Theorem 9. *For a function f such that $M_f \in \mathcal{M}(m_1, \ldots, m_d)$ is a Hankel array, the size of the protocol presented above is minimal.*

The theorem follows from the following lemma:

Lemma 10. *Let f be a function such that $M_f \in \mathcal{M}(m_1, \ldots, m_d)$ is a Hankel array. Then a π-ordered protocol $\mathcal{P}$ is optimal with respect to $S(\mathcal{P})$ and $S(\mathcal{P}, r)$ for every $r \in \Sigma$ iff for each $i \in [1..d-1]$ the message sent by the party $P_{\pi(i)}$ to $P_{\pi(i+1)}$ only depends on the subfunction of f obtained by fixing the inputs of $P_{\pi(1)}, \ldots, P_{\pi(i)}$ and on the message received by $P_{\pi(i)}$.*

Proof. Let us first assume that there exists a party $P_{\pi(i)}$ with $i \in [1..d-1]$ and two inputs $x_{\pi(1)}, \ldots, x_{\pi(i)}$ and $y_{\pi(1)}, \ldots, y_{\pi(i)}$ such that (1) they specify two different subfunctions f_x, f_y of f and (2) $P_{\pi(i)}$ sends the same message to $P_{\pi(i+1)}$ for both inputs. Since f_x, f_y are different functions, there exists an input $z_{\pi(i+1)}, \ldots, z_{\pi(d)}$ for the parties $P_{\pi(i+1)}, \ldots, P_{\pi(d)}$ such that f_x and f_y result in different values. Since the parties $P_{\pi(i+1)}, \ldots, P_{\pi(d)}$ cannot distinguish between both inputs, the protocol computes an incorrect value for at least one input. On the other hand, we do not increase $S(\mathcal{P})$ and $S(\mathcal{P}, r)$ if $P_{\pi(i)}$ adds some information about the received message to the message it is going to send.

Let us now assume that there exists $i \in [1..d-1]$ such that for two different partial inputs $x_{\pi(1)}, \ldots, x_{\pi(i)}$ and $y_{\pi(1)}, \ldots, y_{\pi(i)}$ that specify the same subfunction f' of f, the party $P_{\pi(i)}$ receives the same message but sends two different messages to $P_{\pi(i+1)}$. Let X be the set of all inputs where the values of $P_{\pi(1)}, \ldots, P_{\pi(i)}$ are given by $x_{\pi(1)}, \ldots, x_{\pi(i)}$. For $x \in X$ let Y_x denote the set of all inputs for which $P_{\pi(i)}$ receives the same message from its predecessor as for the input x, the input of $P_{\pi(i)}$ is given by $z_{\pi(i)}$ and the input of $P_{\pi(j)}$ is given by $x_{\pi(j)}$ for all $j \in [i+1..d]$.

Note that $f(x) = f(y)$ for every $x \in X$ and every $y \in Y_x$. Hence we do not increase the size of the protocol if $P_{\pi(i)}$ sends on both inputs the same messages to $P_{\pi(i+1)}$. Moreover, if every party only sends to its successor a unique message for each $y \in Y_x$ we reduce total size as well as the size of $S(\mathcal{P}, f(x))$. □

Note that the communication size S^π may depend on the order π of the parties on the chain. We call a permutation $\pi : [1..d] \to [1..d]$ with $m_{\pi(i)} \leq m_{\pi(i+1)}$ for all $i \in [1..d-1]$ a *sorting* of $m_1, \ldots, m_d$. Consequently, for a sorting π of $m_1, \ldots, m_d$, the ordering is optimal with respect to the communication size.

Theorem 10. *Let f be a function such that $M_f \in \mathcal{M}(m_1, \ldots, m_d)$ is a Hankel array, and let π be a sorting of $m_1, \ldots, m_d$. Then for every permutation $\pi' : [1..d] \to [1..d]$, $S^\pi(f) \leq S^{\pi'}(f)$.*

Proof. The proof of the theorem follows by induction. We start with the induction base $d = 2$. Without loss of generality, we can assume that $m_1 \leq m_2$, $\pi = \mathrm{id}$, $\pi'(1) = 2$, and $\pi'(2) = 1$. In terms of the two-party scenario considered earlier in this article, we have $S^\pi(f) = S^{A \to B}(f)$, $S^{\pi'}(f) = S^{B \to A}(f)$. Thus the claim follows directly from Theorem 4. If we apply Lemma 5, we can even say a little more. Namely, for any $r \in \Sigma$,

$$S^\pi(f, r) \leq S^{\pi'}(f, r). \tag{3}$$

This is because $S^{\pi}(f,r) = \#\mathrm{row}(M_f, r)$ and $S^{\pi'}(f,r) = \#\mathrm{col}(M_f, r)$, as can be easily verified.

Let us now investigate the case that $d > 2$. Let $\mathcal{P}$ be a π-ordered protocol for f that is optimal with respect to protocol size. We will show that for every permutation $\pi_s : [1..d] \to [1..d]$ and for every π_s-ordered protocol $\mathcal{P}_s$,

$$S(\mathcal{P}) \;\leq\; S(\mathcal{P}_s)\;. \tag{4}$$

Note that for two permutations π_1, π_2 which are equivalent in the sense that for every $i \in [1..d]$ $m_{\pi_1(i)} = m_{\pi_2(i)}$, we can simulate any π_1-ordered protocol on a chain that is given by the permutation π_2 without increasing the size of the protocol. Hence it is sufficient to show that (4) holds for *some* sorting π of $m_1, \ldots, m_d$.

For $i \in [1..d]$ and $x \in [m_i]$ let $f_x^{(i)}$ denote the integer function corresponding to $M_x^{(i)}$. Furthermore, let $\pi_x^{(i)}$ be a sorting of $m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_d$, and let $\mathcal{P}_x^{(i)}$ be an optimal $\pi_x^{(i)}$-ordered protocol for $f_x^{(i)}$, hence fulfilling $S(\mathcal{P}_x^{(i)}) \leq S^{\pi_x^{(i)}}(f_x^{(i)})$ by induction hypothesis.

Since for every input $x \in [m_{\pi_s(1)}]$ $M_x^{(\pi_s(1))}$ is a Hankel array, we can apply the induction hypothesis to prove the existence of an optimal $\pi_x^{(\pi_s(1))}$-ordered protocol $\mathcal{P}_x^{(\pi_s(1))}$ for $f_x^{(\pi_s(1))}$ such that for every permutation $\pi' : [1..d-1] \to [1..d-1]$

$$S(\mathcal{P}_x^{(\pi_s(1))}) \;\leq\; S^{\pi'}(f_x^{(\pi_s(1))})\;.$$

This implies that for every permutation $\pi'' : [1..d] \to [1..d]$ with $\pi''(1) = \pi_s(1)$ there exists a protocol $\mathcal{P}_h$ on the chain that starts with $P_{\pi_s(1)}$ and where the remaining parties are $\pi_x^{(\pi_s(1))}$-ordered such that

$$S(\mathcal{P}_h) \;=\; \sum_{M_x^{(\pi_s(1))}} S(\mathcal{P}_x^{(\pi_s(1))}) \;\leq\; \sum_{M_x^{(\pi_s(1))}} S^{\pi'''}(f_x^{(\pi_s(1))}) \;=\; S^{\pi''}(f)$$

where π''' denotes the permutation that corresponds to π'' without $\pi(1)$. The protocol $\mathcal{P}_h$ can be constructed as follows: The first party $P_{\pi_s(1)}$ computes the type of the subarray $M_x^{(\pi_s(1))}$ with $x \in [m_{\pi_s(1)}]$ that is given by its input $x_{\pi_s(1)}$. The remaining parties simulate the protocol $\mathcal{P}_x^{(\pi_s(1))}$. Note that if π_h is a sorting of $m_1, \ldots, m_d$ then the claim follows directly.

Let us focus now on the case that π_h is not a sorting of $m_1, \ldots, m_d$. Since $\pi_h(i)$ is a sorting of $m_{\pi_h(2)}, \ldots, m_{\pi_h(d)}$, the value $m_{\pi_h(2)}$ is minimal for all values $m_1, \ldots, m_d$.

We proceed in two steps:

1. In the first step, we will investigate permutations $\tilde{\pi}_h$ that are similar to π_h except for the first two values, *i.e.* $m_{\tilde{\pi}_h(1)} = m_{\pi_h(2)}$ and $m_{\tilde{\pi}_h(2)} = m_{\pi_h(1)}$.
2. In the second step, we will investigate permutations π'_h with $\pi'_h(1) = \tilde{\pi}_h(1)$.

For any $x_1 \in [m_{\pi_h(1)}]$ and $x_2 \in [m_{\pi_h(2)}]$ define f_{x_1,x_2} as the subfunction of f where we assign to the $\pi_h(1)$-th and $\pi_h(2)$-th variable of f the values x_1 and x_2,

respectively. Furthermore, let M_{x_1,x_2} denote the communication array of f_{x_1,x_2}. Note that M_{x_1,x_2} is a Hankel array, too.

Let us now divide $\mathcal{P}_h$ into two parts. The first part $\mathcal{P}_h^1$ consists of the strategies for the first two parties $P_{\pi_h(1)}$ and $P_{\pi_h(2)}$. If $\mathcal{P}_h$ is optimal with respect to its size $S(\mathcal{P}_h)$ and $S(\mathcal{P}_h, r)$ with respect to all π_h-ordered protocols, we can assume that $P_{\pi_h(2)}$ only sends the type of the subarray M_{x_1,x_2} to $P_{\pi_h(3)}$.

The second part $\mathcal{P}_h^2(M_{x_1,x_2})$ of $\mathcal{P}_h$ consists of the strategies for the remaining $d-2$ parties $P_{\pi_h(3)}$ to $P_{\pi_h(d)}$ where the input of the first two parties is given by x_1 and x_2, respectively. Let Σ_M be the set of all subarrays M_{x_1,x_2}, then we have

$$S(\mathcal{P}_h) \;=\; \sum_{M_{x_1,x_2}\in\Sigma_M} S(\mathcal{P}_h^1, M_{x_1,x_2}) \cdot S(\mathcal{P}_h^2(M_{x_1,x_2}))\ .$$

Let $g : [m_{\pi_h(1)}] \times [m_{\pi_h(2)}] \to \Sigma_M$ be the function that is computed by the first two parties in the chain. Note that the communication array M_g of g is a Hankel array again.

Let $\tilde{\pi}_h$ be a permutation with $\tilde{\pi}_h(1) = \pi_h(2)$, $\tilde{\pi}_h(2) = \pi_h(1)$, and $\tilde{\pi}_h(i) = \pi_h(i)$ for all $i \in [3..d]$. We will now investigate the $\tilde{\pi}_h$-ordered protocol $\tilde{\mathcal{P}}_h$ that is defined as follows: $\tilde{\mathcal{P}}_h$ runs an optimal strategy to compute g on the first two parties and simulates $\mathcal{P}_h$ on the remaining parties. Analogously to the partition of $\mathcal{P}_h$, we partition $\tilde{\mathcal{P}}_h$ into two parts $\tilde{\mathcal{P}}_h^1$ and $\tilde{\mathcal{P}}_h^2$. From equation (3) we can conclude that there exists such a subprotocol $\tilde{\mathcal{P}}_h^1$ with

$$\forall M_{x_1,x_2} \in \Sigma_M \;:\; S(\tilde{\mathcal{P}}_h^1, M_{x_1,x_2}) \;\le\; S(\mathcal{P}_h^1, M_{x_1,x_2}),$$

and therefore we have

$$\begin{aligned} S(\tilde{\mathcal{P}}_h) \;&=\; \sum_{M_{x_1,x_2}\in\Sigma_M} S(\tilde{\mathcal{P}}_h^1, M_{x_1,x_2}) \cdot S(\tilde{\mathcal{P}}_h^2(M_{x_1,x_2})) \\ &\le\; \sum_{M_{x_1,x_2}\in\Sigma_M} S(\mathcal{P}_h^1, M_{x_1,x_2}) \cdot S(\tilde{\mathcal{P}}_h^2(M_{x_1,x_2})) \;=\; S(\mathcal{P}_h). \end{aligned}$$

Analogously to the construction of $\mathcal{P}_h$ we can now apply a transformation on $\tilde{\mathcal{P}}_h$ to get a π'_h-ordered protocol $\mathcal{P}'_h$ for a permutation $\pi'_h(1) = \tilde{\pi}_h(1)$ and $m_{\pi'_h(i)} \le m_{\pi'_h(i+1)}$ for all $i \in [2..d-1]$ such that $\mathcal{P}'_h$ fulfills the following inequalities:

$$S(\mathcal{P}'_h) \;\le\; S(\tilde{\mathcal{P}}_h) \;\le\; S(\mathcal{P}_h) \;\le\; S^{\pi_s}(f) \;\le\; S(\mathcal{P}_s)$$

for every π_s-ordered protocol $\mathcal{P}_s$.

Since $m_{\tilde{\pi}_h(1)}$ is minimal for all values $m_1, \ldots, m_d$ and the values $m_{\pi'_h(i)}$ for $i \in [2..d]$ are ordered according to their size, we can conclude that $\pi'_h(i)$ is a sorting of $m_1, \ldots, m_d$. □

Note that Theorem 10 can easily be generalized to $S^{\pi}(f, r) \;\le\; S^{\pi'}(f, r)$. One application of such generalisation can be found in [2].

A second generalization of the two-party model is the simultaneous communication complexity (denoted by $C^{||}$), where all parties can simultaneously write in a single round on a blackboard. This means that the messages sent by each party do not depend on the messages sent by the other parties. After finishing the communication round, each party has to be able to compute the result of the function (see *e.g.* [10]). For two-party communication it is well-known that

$$C^{||}(f) \;=\; C^{A\to B}(f) + C^{B\to A}(f) \;=\; \lceil \log S^{A\to B}(f) \rceil + \lceil \log S^{B\to A}(f) \rceil \;.$$

Similarly, for the d-party case we have

$$C^{||}(f) \;=\; \textstyle\sum_{i\in[1..d]} \lceil \log \#\mathrm{sub}_i(M_f) \rceil \;.$$

Hence if M_f is a Hankel array and if for some $k \in [1..d]$ we have $\#\mathrm{sub}_k(M_f) \leq \min_{i\in[1..d]} m_i$, then by Lemmas 8 and 9

$$C^{||}(f) \;=\; d \cdot \lceil \log \Delta(f_{M_f}) \rceil \;.$$

As a third generalization, we consider the case that in each round some party can write a message on a blackboard. The message and its sender may depend on messages that have been published on the board in previous rounds. We restrict the communication such that each party (except for the last one) publishes exactly one message on the blackboard, and in each round exactly one message is published. After finishing the communication rounds, at least one party has to be able to compute the result of the function. Let $S^{\square}$ be the corresponding size of an optimal protocol. Note that this model generalizes both of the previous models.

Theorem 11. *Let f be a function such that $M_f \in \mathcal{M}(m_1,\ldots,m_d)$ is a Hankel array and let π be a sorting of $m_1,\ldots,m_d$. Then* $S^{\pi}(f) \;=\; S^{\square}(f)$.

Proof. The proof follows by complete induction on the number of parties d. For $d = 2$ the claim follows directly from the standard one-way two-party scenario.

For $d > 2$ let us first note that the first party that writes a message to the blackboard has to be determined by the protocol independently of the concrete input. Let P_k be the party that writes its message first. The second party that writes a message on the blackboard may depend on the type of $M^{(k)}_{x_k}$ where $z_k \in [m_k]$ is the input of P_k. Let $f^{(k)}_{x_k}$ describe the function with communication array $M^{(k)}_{x_k}$. Since $M^{(k)}_{x_k}$ is a Hankel array too, we can apply the induction hypothesis to the computation of $f^{(k)}_{x_k}$. Note that $M^{(k)}_{x_k} \in \mathcal{M}(m_1,\ldots,m_{k-1},m_{k+1},\ldots,m_d)$. Hence for a sorting $\pi_k : [1..d-1] \to [1..d-1]$ of $m_1,\ldots,m_{d-1}$ we have:

$$S^{\pi_k}(f^{(k)}_{x_k}) \;=\; S^{\square}(f^{(k)}_{x_k}).$$

Since the first party that writes a message on the blackboard is chosen independently of the concrete input, this equation implies

$$S^{\pi'}(f) \;=\; \sum_{M_{z_k}^{(k)}} S^{\pi_k}(f_{z_k}^{(k)}) \;=\; \sum_{M_{z_i}^{(i)}} S^{\square}(f_{z_i}^{(i)}) \;=\; S^{\square}(f)$$

where $\pi'(1) = k$ and for $i \in [1..d-1]$ $\pi'(i+1) = \pi_k(i)$. By Theorem 10 we get for a sorting $\pi : [1..d] \to [1..d]$ of $m_1, \ldots, m_d$:

$$S^{\pi}(f) \;\leq\; S^{\pi'}(f) \;=\; S^{\square}(f).$$

On the other hand, we can always simulate a protocol which works on a chain by a protocol that uses a blackboard without increasing the size of the protocol. Hence

$$S^{\square}(f) \;\leq\; S^{\pi}(f).$$

The claim follows directly. □

7. Conclusions and open problems

In this paper we have investigated one-way communication complexity of functions for which the corresponding communication matrices are Hankel matrices. We have established some structural properties of such matrices. As a direct application, we have obtained a complete solution to the problem of how the communication direction in *deterministic* one-way communication protocols affects the communication complexity of symmetric Boolean functions. One possible direction of future research is to study other kinds of one-way communication such as *nondeterministic* and *randomized* for the class of symmetric functions.

Another interesting extension of the topic is to drop the restriction to *one-way* protocols and consider the deterministic two-way communication complexity of symmetric Boolean functions for both a bounded and an unbounded number of communication rounds. This particularly involves results about the computation of the rank of Hankel matrices. In addition, consequences for word combinatorics and OBDD theory may be of interest.

Acknowledgements. We would like to thank Ingo Wegener for his useful comment on the connection between one-way communication and OBDD theory.

References

[1] F. Ablayev, Lower bounds for one-way probabilistic communication complexity and their application to space complexity. *Theoret. Comp. Sci.* **157** (1996) 139–159.

[2] M. Bläser, A. Jakoby, M. Liśkiewicz and B. Manthey, Privacy in Non-Private Environments, in *Proc. of the 10th Ann. Int. Conf. on the Theory and Application of Cryptology and Information Security ASIACRYPT*, Springer-Verlag. *Lect. Notes. Comput. Sci.* **3329** (2004) 137–151.

[3] A. Condon, L. Hellerstein, S. Pottle and A. Wigderson, On the power of finite automata with both nondeterministic and probabilistic states. *SIAM J. Comput.* **27** (1998) 739–762.
[4] P. Ďuriš, J. Hromkovič, J.D.P. Rolim and G. Schnitger, *On the power of Las Vegas for one-way communication complexity, finite automata, and polynomial-time computations*, in *Proc. of the 14th Int. Symp. on Theoretical Aspects of Computer Science (STACS)*, Springer-Verlag. *Lect. Notes. Comput. Sci.* **1200** (1997) 117–128.
[5] J.E. Hopcroft and J.D. Ullman, *Formal Languages and Their Relation to Automata*. Addison-Wesley, Reading, Massachusetts (1969).
[6] J. Hromkovič, *Communication Complexity and Parallel Computing*. Springer-Verlag (1997).
[7] I.S. Iohvidov, *Hankel and Toeplitz Matrices and Forms*. Birkhäuser, Boston (1982).
[8] H. Klauck, *On quantum and probabilistic communication: Las Vegas and one-way protocols*, in *Proc. of the 32nd Ann. ACM Symp. on Theory of Computing (STOC)* (2000) 644–651.
[9] I. Kremer, N. Nisan and D. Ron, On randomized one-round communication complexity, *Computational Complexity* **8** (1999) 21–49.
[10] E. Kushilevitz and N. Nisan, *Communication Complexity*. Camb. Univ. Press (1997).
[11] K. Mehlhorn and E.M. Schmidt, Las Vegas is better than determinism in VLSI and distributed computing, in *Proc. of the 14th Ann. ACM Symp. on Theory of Computing (STOC)* (1982) 330–337.
[12] I. Newman and M. Szegedy, *Public vs. private coin flips in one round communication games*, in *Proc. of the 28th Ann. ACM Symp. on Theory of Computing (STOC)* (1996) 561–570.
[13] C. Papadimitriou and M. Sipser, Communication complexity. *J. Comput. System Sci.* **28** (1984) 260–269.
[14] I. Wegener, Optimal decision trees and one-time-only branching programs for symmetric Boolean functions. *Inform. Control* **62** (1984) 129–143.
[15] I. Wegener, *The complexity of Boolean functions*. Wiley-Teubner (1987).
[16] I. Wegener, personal communication (April 2003).
[17] A.C. Yao, *Some complexity questions related to distributive computing*, in *Proc. of the 11th Ann. ACM Symp. on Theory of Computing (STOC)* (1979) 209–213.

Communicated by J. Hromkovič.
Received August 23, 2004. Accepted February 5, 2005.

To access this journal online:
www.edpsciences.org