COMMUNICATION COMPLEXITY OF FUNCTIONS ON DIRECT SUMS

Ulrich Tamm

Fakultät Mathematik, Universität Bielefeld, Postfach 100131, 33501 Bielefeld, Germany

tamm@mathematik.uni-bielefeld.de

Abstract: The paper surveys direct sum methods in communication complexity, mostly concentrating on the results obtained by several authors in the research group of Rudolf Ahlswede in Bielefeld. Lower bound techniques are investigated which behave multiplicatively for functions defined on direct sums of sets. Applications, as the exact or asymptotic determination of the communication complexity and the comparison of bounding techniques are discussed.

1 INTRODUCTION

We survey some results on the communication complexity of *sum-type functions* f_n and *vector-valued functions* f^n, which are defined on the powers $\mathcal{X}^n, \mathcal{Y}^n$ of the sets from the domain of some basic function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. Elements of $\mathcal{X}^n$ and $\mathcal{Y}^n$ are denoted as x^n and y^n, respectively. Hence, e. g., $x^n = (x_1, \dots, x_n)$ for some $x_1, \dots, x_n \in \mathcal{X}$. With this notation

$$f^n(x^n, y^n) = \big(f(x_1, y_1), \dots, f(x_n, y_n)\big), \qquad f_n(x^n, y^n) = \sum_{i=1}^{n} f(x_i, y_i),$$

where it is required that the range $\mathcal{Z}$ is a subset of an additive group G.

The investigations in Bielefeld in this direction trace back to a visit of the scientist celebrated in this volume to Stanford University, where he found his office full of computer printouts. Abbas El Gamal and King Pang told him that the printouts served to get insight into the structure of code pairs (A, B), $A, B \subset \{0, 1\}^n$, on which the Hamming distance h_n is constant, i. e. $h_n(a, b) = h_n(a', b')$ for all $a, a' \in A, b, b' \in B$. In order to get rid of all the paper, Ahlswede decided that the problem had to be solved. The result was the joint paper [0] and the following theorem, which he calls the “Four Continents Theorem” (the authors are from Europe, Africa, and Asia and the work was done in America).

Theorem ([0]) The size $|A \times B|$ of the largest code pair $(A, B), A, B \subset \{0,1\}^n$ on which the binary Hamming distance assumes a constant value is $2^{\lfloor n/2 \rfloor}$.

The theorem was settled by a combinatorial approach, giving the constant distance code pair (for the distance $\lfloor \frac{n}{2} \rfloor$) $A = \{00, 11\}^{\lfloor n/2 \rfloor}, B = \{01, 10\}^{\lfloor n/2 \rfloor}$ and an inductive optimality proof. Later Delsarte and Piret [0] and Hall and van Lint [0] derived the same result via algebraic methods. However, it turned out that the original proof from [0] was extendable to the case that the Hamming distance assumes a specified value δ (i. e. $h_n(a, b) = h_n(a', b') = \delta$ for all $a, a' \in A, b, b' \in B$) on $A \times B$ the size of which has to be maximized.
Such a constant distance code pair was called monochromatic rectangle by Yao [0], who used this concept in order to lower bound the communication complexity $C(f)$ of a function f. The bounds El Gamal and Pang [0] derived on the size of constant distance code pairs with specified value δ enabled them to determine the communication complexity of the binary Hamming distance up to one bit. Ahlswede [0] generalized this result to the Hamming distance over alphabets of size $q = 4, 5$ and also for $q = 3$ (unpublished manuscript).

Theorem ([0], [0]) For $q = 2, 3, 4, 5$ and all positive integers n

$$|C(h_n) - \lceil n \cdot \log q \rceil - \lceil \log(n + 1) \rceil| \leq 1 \tag{1.1}$$

Throughout this paper the logarithm is always taken to the base 2. Unfortunately the method of proof based on the exact determination of the size of largest constant distance code pairs (cf. also [0]) breaks down for alphabet size $q \geq 6$. It is strongly conjectured that (1) holds for all alphabet sizes q and all positive integers n.
The proofs in [0] and [0] are rather involved such that we shall not present them. Let us only mention that research motivated by the study of (1.1) followed several directions. Recently, Haemers [0] has bounded the size of constant distance code pairs by methods from algebraic graph theory. These bounds work quite well for large q. In my thesis [0] (see also [0]), using properties of the Hamming association scheme, (1) was shown to hold for special parameters n, e. g. when $n = p^s - 1$ with p a prime factor of q. Finally, the size of constant distance code pairs for further functions may be determined or at least closely bounded. Ahlswede in [0] also considered the parity of the Hamming distance. For $q = 2$ and $q = 4$ the size of largest constant distance code pairs was exactly determined. Recent progress on this was made in [0].

We shall concentrate, however, on a rather methodical direction of research - the search for possible induction proofs. The Hamming distance has a certain property, it is a sum-type function h_n, with basic function h indicating if $x_i = y_i$ or not. We are interested to conclude from the communication complexity of the basic function f to the communication complexity of the sum-type function f_n and to that of the vector-valued function f^n.
This is not in general possible if one studies lower bounds obtained via largest monochromatic rectangles. However, Ahlswede and Mörs [0] observed that the

situation changes if one does not require any more that the function is constant on the rectangle (or code pair) $A \times B$ but that instead the so-called $4 - word - property$ holds. In this case, we obtain a lower bound $C(f_n) \geq n \cdot C(f)$. This multiplicative behaviour is very useful in the study of the communication complexity of sum-type functions.
Furthermore, one can exploit the structure of the function matrix $M(f_n) = (f_n(x^n, y^n))_{x^n, y^n}$ which can be obtained from the function matrix $M(f)$ of the basic function f in terms of the *Kronecker product*. This is intensively discussed in [0], [0] and for vector-valued funtions in [0] (also for the case of nonidentical functions for each component). Parameters like the rank and the independence number which yield further lower bounds on the communication complexity are multiplicative under the Kronecker product.

A further line of research leading to direct sum methods in communication complexity goes back to Karchmer, Raz, and Wigderson [0], cf. also [0], pp. 42 - 48. Their question was if it is easier to solve communication problems simultaneously than separately. Recall the definition of a vector-valued function $f^n((x_1, \dots, x_n), (y_1, \dots, y_n)) = (f(x_1, y_1), \dots, f(x_n, y_n))$. An obvious upper bound on the communication complexity $C(f^n)$ is obtained by evaluating each component $f(x_i, y_i)$ separately and communicating the result for component i using the optimal protocol for f. Can we do better by considering all components simultaneously? We shall provide a simple example for a function where $C(f) = 2$ but $C(f^n) = \lceil n \cdot \log_2 3 \rceil$. The measure $\limsup_{n \to \infty} \frac{1}{n} C(f^n)$ is also called *amortized communication complexity* (see [0] or [0]).

Direct sum methods in communication complexity are useful tools in separating complexity classes. Further applications are the comparison of lower bound techniques and the study of their power (how large can be the gap between the lower bound and the communication complexity). The intuition is that small gaps for the basic function f become large for the vector-valued function f^n.

The paper is organized as follows. After presenting the basic notions on communication complexity and the functions to be studied, the lower bound techniques useful for sum-type and vector-valued functions are introduced in Section 3. The communication complexity of special functions is then studied in Section 4. Applications in Computer Science are discussed in the final section.

2 BASIC NOTIONS

The notion of communication complexity was introduced by Yao in 1979 [0]. Since then it found many applications in Computer Science, for which we refer to the books by Kushilevitz and Nisan [0] or by Hromkovic [0], see also the survey by Wegener [0] in this volume.
The communication complexity of a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ (where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite sets), denoted as $C(f)$, is the number of bits that two persons, P_1 and P_2, have to exchange in order to compute the function value $f(x, y)$, when initially P_1 only knows $x \in \mathcal{X}$ and P_2 only knows $y \in \mathcal{Y}$.

More specifically, let $\mathcal{Q}$ denote the set of protocols computing f and let $l_P(x,y)$ be the number of bits transmitted for the input (x,y), when the protocol $P \in \mathcal{Q}$ is used. Then the (worst-case) *communication complexity* is

$$C(f) := \min_{P\in\mathcal{Q}} \max_{(x,y)\in\mathcal{X}\times\mathcal{Y}} l_P(x,y).$$

A *protocol* P is a pair of mappings $\phi_1 : \mathcal{X}\times\{0,1\}^* \to \{0,1\}^*$, $\phi_2 : \mathcal{Y}\times\{0,1\}^* \to \{0,1\}^*$. So on input (x,y), the persons starting with P_1 alternatively send binary messages N_1, N_2, N_3, etc., until they both know the result.

There is also a slightly modified model in which communication already stops when one person knows the result. We denote by $C_1(f)$ the communication complexity in this case. Often, Boolean functions are considered, where the difference between the two models is at most the transmission of just one bit for the result. However, the functions we are going to study have a much larger range, such that the gap between $C(f)$ and $C_1(f)$ may be considerable.

Each message depends on the previous messages and on the inputs, hence $N_1 = \phi_1(x)$, $N_2 = \phi_2(y,\phi_1(x))$, $N_3 = \phi_1(x,\phi_1(x)\phi_2(y,\phi_1(x)))$, etc. It is required that the set of messages a person is allowed to send is *prefix-free*, i. e., no possible message is the beginning of another one. This property assures that the other person immediately recognizes the end of the message and can hence start the transmission without delay.

An upper bound on $C(f)$ for any function $f : \mathcal{X}\times\mathcal{Y} \to \mathcal{Z}$ (w. l. o. g. $|\mathcal{X}| \le |\mathcal{Y}|$) is always obtained from the following *trivial protocol*: P_1 transmits all the bits of his input $x \in \mathcal{X}$. P_2 now is able to compute the function value and returns the result $f(x,y) \in \mathcal{Z}$ (if P_1 must be informed). Hence

$$C_1(f) \le \lceil \log|\mathcal{X}|\rceil, \qquad C(f) \le \lceil \log|\mathcal{X}|\rceil + \lceil \log|\mathcal{Z}|\rceil.$$

As mentioned, we shall study the communication complexity of vector-valued and sum-type functions. Let us first present some examples.

i) Let $si : \{0,1\}\times\{0,1\} \to \{0,1\}$ be the logical "and" If we interpret the vectors $x^n, y^n \in \{0,1\}^n$ as representations of two subsets of an n–elementary set ($x_i = 1$ exactly if the i–th element is contained in the subset represented by $x^n = (x_1,\dots,x_n)$), then the vector–valued function $si^n(x^n,y^n)$ gives the intersection of these two sets, whereas the sum–type function $si_n : \{0,1\}^n \times \{0,1\}^n \to \{0,\dots,n\} \subset Z$ yields the cardinality of this intersection. The function si_n can be generalized to larger alphabets in two canonical ways: 1) the inner product of x^n and y^n, 2) the sum of the componentwise minima.

ii) The *Hamming distance*, which counts the number of components in which x^n and $y^n \in \{0,\dots,q-1\}$ differ, is the sum–type function h_n obtained via the basic function $h(x,y) = \begin{cases} 0, & \text{if } x = y \\ 1, & \text{if } x \neq y. \end{cases}$

For the binary Hamming distance the corresponding vector-valued function h^n yields the symmetric difference of the sets represented by x^n and y^n.

We shall also consider the parity of the Hamming distance (the Hamming distance modulo 2). Here we only have to replace the range Z by $Z_2 = Z/2Z$.

iii) A further measure for the distance of two vectors $x^n, y^n \in \{0, \dots, q-1\}^n$ in Coding Theory is the *Lee distance*. Here the basic function is defined by $\ell(x,y) = \min\bigl\{|x-y|, q-|x-y|\bigr\}$. It can be interpreted as the length of a shortest path on the cycle from x to y. Another distance function is the *taxi metric*, with basic function $t(x,y) = |x-y|$.

3 LOWER BOUND TECHNIQUES

The aim of this section is to present techniques which allow to conclude from the communication complexity $C(f)$ of the basic function f to the communication complexity of the sum-type function f_n or the vector–valued function f^n. All these bounds are expressed in terms of the *function matrix* $M(f) = \bigl(f(x,y)\bigr)_{x\in\mathcal{X}, y\in\mathcal{Y}}$. and the *function value matrices* $M_z(f) = (a_{xy})_{x\in\mathcal{X}, y\in\mathcal{Y}}$ for all $z \in \mathcal{Z}$ defined by $a_{xy} = \begin{cases} 1 & \text{if } f(x,y) = z \\ 0 & \text{if } f(x,y) \neq z. \end{cases}$
Yao [0] already showed that $C(f) \geq \log D(f)$, where the decomposition number $D(f)$ denotes the minimum size of a partition of $\mathcal{X} \times \mathcal{Y}$ into *monochromatic rectangles*, i. e., products $A \times B$ of pairs $A \subset \mathcal{X}, B \subset \mathcal{Y}$ on which the function is constant. The decomposition number usually is hard to determine, however, further lower bounds can be derived from it. Immediately, we have

$$C_1(f) \geq \left\lceil \log \frac{|\mathcal{X}| \cdot |\mathcal{Y}|}{Lmr\bigl(M(f)\bigr)} \right\rceil, \qquad C(f) \geq \left\lceil \log \sum_{z\in\mathcal{Z}} \frac{wt\bigl(M_z(f)\bigr)}{lmr\bigl(M_z(f)\bigr)} \right\rceil \tag{1.2}$$

where $Lmr\bigl(M(f)\bigr)$ denotes the size of the largest monochromatic rectangle in the function matrix $M(f)$, $lmr\bigl(M_z(f)\bigr)$ is the size of the largest monochromatic rectangle on which the function assumes the constant value z, and $wt\bigl(M_z(f)\bigr)$ denotes the number of pairs (x,y) with $f(x,y) = 1$.
Yao used this last bound in order to show that for almost all Boolean functions the trivial protocol is optimal up to two bits. Weakening the conditions on the rectangles, further lower bounds are obtained. For instance, it may be no longer required that the function is constant on the rectangle $A \times B$ but that the so called *4-word- property* has to be fulfilled, i. e., for all $a, a' \in A$, $b, b' \in B$

$$f(a,b) - f(a',b) - f(a,b') + f(a',b') = 0$$

Denoting by $Lfw(f)$ the size of the largest rectangle, on which the 4-word-property holds, we obtain

$$C_1(f) \geq \left\lceil \log \frac{|\mathcal{X}| \cdot |\mathcal{Y}|}{Lfw(f)} \right\rceil. \tag{1.3}$$

A *z–fooling set* $\bigl\{(x^{(1)}, y^{(1)}), \dots, (x^{(N)}, y^{(N)})\bigr\}$ for the function value z in $M(f)$ is a set of pairs with $f(x^{(i)}, y^{(i)}) = z$ for all $i = 1, \dots, N$ such that no two members of the set are in the same monochromatic rectangle. Denoting the size of a z–fooling set (or independent set as in [0]) by $ind(M_z(f))$ and $Ind(f) = \sum_{z\in\mathcal{Z}} ind(M_z(f))$ we obtain

$$C_1(f) \geq \lceil \log(\max_{z\in\mathcal{Z}} ind(M_z(f)))\rceil, \qquad C(f) \geq \lceil \log Ind(f)\rceil. \tag{1.4}$$

where the first bound was derived in [0] and the second one studied in [0]. Mehlhorn and Schmidt [0] observed that $C(f)$ can be lower bounded by the rank of the corresponding function matrices. We shall only use the rank over the reals.

$$C_1(f) \geq \lceil \log \mathrm{rank} M(f)\rceil, \qquad C(f) \geq \lceil \log r(f)\rceil, \text{ where } r(f) = \sum_{z\in\mathcal{Z}} \mathrm{rank} M_z(f) \tag{1.5}$$

It can be shown that the function f has the same communication complexity as the function g defined by $g(x,y) = c^{f(x,y)}$ for all x, y, when the number c is chosen appropriately ($c \neq 0, |c| \neq 1$). So it is also possible to lower bound $C(f)$ by the rank of $M(g) = \exp(M(f), c) = (c^{f(x,y)})_{x\in\mathcal{X}, y\in\mathcal{Y}}$, the *exponential transform* of the matrix $M(f)$. This yields

$$C_1(f) \geq \lceil \log \mathrm{rank} \exp(M(f), c)\rceil. \tag{1.6}$$

Central in the following arguments is the observation that the function matrices of the vector-valued and sum-type functions can be expressed in terms of the Kronecker product, defined for two matrices $A = (a_{ij})_{i,j}$ and $B = (b_{kl})_{k,l}$ as $A \otimes B = (a_{ij} \cdot b_{kl})_{i,j,k,l}$. The n-fold Kronecker product of a matrix is denoted as $A^{\otimes n}$. We have (cf. [0], [0], [0], [0])

$$M_{(z_1,\dots,z_n)}(f^n) = M_{z_1}(f) \otimes M_{z_2}(f) \otimes \dots \otimes M_{z_n}(f) \tag{1.7}$$

$$M_z(f_n) = \sum_{\substack{(z_1,\dots,z_n)\\ z_1+\dots+z_n=z}} M_{z_1}(f) \otimes \dots \otimes M_{z_n}(f) \tag{1.8}$$

$$\exp\big(M(f_n), c\big) = \big[\exp\big(M(f), c\big)\big]^{\otimes n} \tag{1.9}$$

It can be shown that the parameters in the bounds (3) - (6) behave multiplicatively. The properties are summarized in the following theorem. For the proofs we refer to the original research papers. Useful for sum-type functions are the 4-word-property, introduced by Ahlswede and Mörs [0] for the Hamming distance and thoroughly analyzed in [0], and the rank of the exponential transform [0]. The rank is multiplicative under the Kronecker product. For vector-valued functions, it is important that the same holds for $r(f) = \sum_{z\in Z} \mathrm{rank} M_z(f)$. This was derived by Ahlswede and Cai [0] who also found similar results for the independence number $Ind(f)$ and the parameter $\max(Ind(f), r(f))$.

Theorem 1:

$$Lfw(f_n) = n \cdot Lfw(f) \tag{1.10}$$
$$\text{rank}\exp\big(M(f_n), c\big) = (\text{rank}\big[\exp\big(M(f), c\big)\big])^n \tag{1.11}$$
$$r(f^n) = r(f)^n \tag{1.12}$$
$$Ind(f^n) \geq Ind(f)^n \tag{1.13}$$
$$\max(Ind(f^n), r(f^n)) \geq \big[\max(Ind(f), r(f))\big]^n \tag{1.14}$$

4 COMMUNICATION COMPLEXITY OF SPECIAL FUNCTIONS

4.1 Vector-valued functions

We shall study all vector-valued functions f^n with basic function $f : \{0,1\} \times \{0,1\} \to \{0,1\}$. They fall into four classes: constant functions, projections on one coordinate, the symmetric difference with function matrix $M(h) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and its complement, the logical "and" with $M(si) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and equivalent functions. In the first case no communication is necessary, projections require n bits of communication.

Theorem 2:

$$C(h^n) = 2n, \qquad C(si^n) = \lceil \log 3 \rceil \tag{1.15}$$

Proof: For the symmetric difference h^n, the trivial protocol requires $\lceil \log 2^n \rceil + \lceil \log 2^n \rceil = 2n$ bits of communication. With the rank lower bound (5) and (12) this can be shown to be optimal, since

$$C(h^n) \geq \log r(h^n) = n \cdot \log r(h) = n \cdot \log(\text{rank}M_0(h) + \text{rank}M_1(h))$$
$$= n \cdot \log(\text{rank}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \text{rank}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = n \cdot \log 4 = 2n$$

For set-intersection the rank lower bound yields

$$C(si^n) \geq \lceil \log r(si^n) \rceil = \lceil n \cdot \log r(si) \rceil = \lceil n \cdot \log(\text{rank}M_0(si) + \text{rank}M_1(si)) \rceil$$
$$= \lceil n \cdot \log(\text{rank}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + \text{rank}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}) \rceil = \lceil n \cdot \log 3 \rceil$$

In order to obtain the same upper bound, we shall modify the trivial protocol, which would require $2n$ bits of transmission. Again, in the first round person P_1 encodes his input $x^n \in \{0,1\}^n$. P_2 then knows both values and hence is able to compute the result $si^n(x^n, y^n)$, which is returned to P_1. However, in knowledge of x^n the set of possible function values is reduced to the set $S(x^n) = \{y^n : y^n \subset x^n\}$. Hence, only $\lceil \log S(x^n) \rceil$ bits have to be reserved for the transmission of $si^n(x^n, y^n)$ such that P_1 can assign longer messages to elements with few subsets. So, in contrast to the trivial protocol, the messages $\{\phi_1(x^n) : x^n \in \{0,1\}^n\}$ are now of variable length. Since the prefix property has to be guaranteed, Kraft's inequality for prefix codes yields a condition, from which the upper bound can be derived. Specifically, we require that to each x^n there corresponds a message $\phi_1(x^n)$ of (variable) length $l(x^n)$ such that for all $x^n \in \{0,1\}^n$ the sum $l(x^n) + \lceil \log S(x^n) \rceil$ takes a fixed value, L say. Kraft's inequality states that a prefix code exists, if $\sum_{x^n} 2^{-l(x^n)} \leq 1$. This is equivalent to $\sum_{x^n} 2^{\lceil \log S(x^n) \rceil} \leq 2^L$. With the choice $L = \lceil \log 3^n \rceil$ Kraft's inequality holds.

Remark: We used the fact that the subsets of an n-elementary set form a lattice. Functions defined on lattices were studied this way in [0], see also [0].

4.2 Sum-type functions

I) ONE PERSON HAS TO BE INFORMED ABOUT THE RESULT

As mentioned, the largest 4-word sets and the rank of the exponential transform are suitable lower bounds here. By (10) and (11), these parameters also behave multiplicatively and hence allow to conclude from the communication complexity $C_1(f)$ of the basic function to that of the sum-type function f_n.
The size of largest 4-word-sets have been determined for metrics of sum-type like the Lee distance (see also [0]) and the taxi metric in [0]. If the maximal 4-word set is one row in the function matrix, then the trivial protocol is optimal by bound (3), and by (4) it suffices to study the basic function f, from which the same result for the sum-type function f_n is immediate.
The exponential transform of the function matrix turned out to be very efficient for the analysis of the communication complexity when only one person has to be informed about the result. We summarize several results from [0]
Theorem 3: For the following sum-type functions $f_n\{0,\dots,q-1\} \times \{0,\dots,q-1\} \to Z$, where $q \geq 2$ is a positive integer, holds $C_1(f_n) = \lceil n \cdot \log q \rceil$
i) metrics of sum-type, ii) inner product, iii) sum of the componentwise minima.

Proof: The idea is to choose the parameter c appropriately in $\exp(M(f), c) = (c^{f(x,y)})_{x,y}$. This exponential transform for the basic function f then has full rank q. By (11), $\exp(M(f_n), c)$ has full rank q^n, from which by (16) the lower bound is immediate. The upper bound follows from the trivial protocol.
i) For metrics like Hamming distance, Lee distance, and taxi metric by definition $f(x,y) = 0$ exactly if $x = y$. Letting c tend to 0 the resulting matrix will be the identity matrix, which has full rank q, Now choose $c > 0$ small enough.
ii) The determinant of the exponential transform $\exp(M(f), c)$ of the basic function $f(x,y) = x \cdot y$ of the inner product is the Vandermonde determinant $\prod_{m=2}^{q} \prod_{l=1}^{m-1} (c^{m-1} - c^{m-1-l})$, which is different from 0 for $c \neq 0, -1, 1$.
iii) The determinant of $\exp(M(f), c)$ is $\prod_{m=1}^{q-1} (c-1) \cdot c^{m-1} \neq 0$ for $c \neq 0, 1$.

Remarks: 1) By choosing the parameter $c = e^{\frac{2\pi i}{p}}$ in the exponential transform it is also possible to study sum-type functions modulo the positive integer $p \geq 2$.

2) The inner product demonstrates the power of the approach via the rank of the exponential transform (which has full rank) compared to the rank of the function matrix (which has rank 1) itself.

3) The Kronecker product $M(f) \otimes M(g)$ of the function matrices (not their exponential transforms) of Boolean functions f, g has also been studied, since this is the function matrix of $f \wedge g$ as defined in [0], pp. 42-48.

II) Both persons have to be informed

Determining the communication complexity of sum-type functions when both persons have to be informed is a much harder problem, since the lower bounds are not multiplicative in general. However, we found several inductive rank calculations for the function value matrices $M_z(si_n)$ of the set-intersection function [0], [0], which allow to describe its communication complexity up to one bit.

Theorem 4: $n + \lceil \log(n+1) \rceil - 1 \leq C(si_n) \leq n + \lceil \log(n+1) \rceil$

The upper bound derived from the trivial protocol is assumed for $n = 2^s - 1$. The improvement of the trivial protocol via Kraft's inequality here occasionally allows to save one bit of communication, e. g., for $n = 2^s$ [0] or for $n = 2^s + 1$ and $n = 2^s + 3$ [0] ($s > 2$ is always a positive integer).

We saw in the introduction that also the communication complexity of the binary Hamming distance can be determined up to one bit and that the method of proof via largest monochromatic rectangles extends to small alphabet sizes q but does not yield a general approach. Also, the rank lower bound does not yield a satisfactory result up to now, although we have a lot of information. The function value matrices $M_z(h_n)$ form the Hamming association scheme, intensively studied in Coding Theory, and their eigenvalues are Krawchouk polynomials - as a set of orthogonal polynomials also an object of intensive research. The problem is to show that Krawchouk polynomials have only very few integral zeros. There is some hope to prove (1.1) for all q and n this way, since there seems to be some evidence that a Krawchouk polynomial for $q \geq 3$ can have at most three integral zeros (S. Litsyn, personal communication).

In [0] we determined the communication complexity of the parities of Hamming and Lee distance. Their function value matrices are simultaneously diagonalizable and hence $r(f)$ is multiplicative. This extends to translation-invariant functions modulo 2.

Theorem 5: Let $f_n : \{0, \ldots, q-1\} \times \{0, \ldots, q-1\} \to Z_2$ be a non-constant sum-type function invariant under translation and let q be an odd prime number. Then for all positive integers n we have $C(f_n) = \lceil n \cdot \log(q) \rceil + 1$.

5 APPLICATIONS IN COMPUTER SCIENCE

5.1 Comparison of Communication Complexity Classes

One reason for studying communication complexity is that here we have a framework that allows to compare different modes of communication. For instance, the equality function which compares two strings of length n ($eq(x^n, y^n) = 1$ if $x^n = y^n$ and 0 otherwise) has deterministic communication complexity n. However, there exist nondeterministic (for $\overline{\text{eq}}$) and randomized protocols which require only $O(\log n)$ bits of communication. So there is an exponential gap between deterministic complexity and nondeterministic or probabilistic complexity. For an intensive analysis of communication complexity classes see [0] and [0]. We point out here that sometimes functions defined on direct sums play an important role. The rank is determined exploiting the block structure of the function matrix, which shows that for these functions the trivial protocol is optimal and hence they have high deterministic communication complexity. One such function of sum-type is $\sum_{i=1}^{n} si_n(x_i, y_i)$ mod 2 the inner product (or set intersection) modulo 2. Replacing 0's by 1's and 1's by -1's in the function matrix (this yields the exponential transform with $c = -1$) we obtain a Hadamard matrix of full rank 2^n. So the rank lower bound coincides with the complexity of the trivial protocol. This function is very important in the study of probabilistic protocols, since randomization does not reduce the order of its communication complexity, as shown in [0] or [0]. The same holds for another function related to set intersection, the function indicating if $x^n \subset y^n$, cf. [0] and [0].

The second function we mention in this context is list disjointness defined for $x^n = (x_{(1)}, \ldots, x_{(n)}), y^n = (y_{(1)}, \ldots y_{(n)})$, where $x_{(i)}, y_{(i)} \in \{0,1\}^n$ for all i by

$$ld_n(x^n, y^n) = \begin{cases} 1, & \text{if there is an } i \text{ with } x_{(i)} = y_{(i)} \\ 0, & \text{else} \end{cases}$$

The function matrix $M(ld_n) = \sum_{\vec{j} \in \{0,1\}^n \setminus (1,\ldots,1)} (-1)^{n - \mathrm{wt}(\vec{j})} A_{j_1} \otimes \ldots \otimes A_{j_n}$ is built up of blocks of identity matrices $A_0 = I_n$ and all-one matrices $A_1 = J_n$ of size n. ($\mathrm{wt}(\vec{j})$ denotes the number of 1's in $\vec{j} = (j_1, \ldots, j_n)$). The Kronecker product allows to derive that all eigenvalues are odd, such that $M(ld_n)$ has full rank and ld_n high deterministic communication complexity. Mehlhorn and Schmidt [0] showed that nondeterministic and Las Vegas communication complexity are of smaller order for ld_n. An improved Las Vegas protocol [0] shows that list disjointness (asymptotically) attains the maximum possible quadratic gap between deterministic and Las Vegas complexity.

5.2 Amortized Communication Complexity

With Theorem 2 the function si^n can be evaluated much faster considering all n components simultaneously than by componentwise communication of the results for the basic function si, which would cost $2n$ bits. So the amortized communication complexity of the function si is $\frac{1}{n} \lim_{n\to\infty} C(si^n) = \log 3$.

Further with Theorem 2 it is also clear that this is the maximum compression for basic Boolean functions $f : \{0,1\} \times \{0,1\} \to \{0,1\}$. Karchmer, Raz, and Wigderson [0] asked how much better simultaneous computations are compared to the componentwise evaluation of the function f^n for basic functions $f : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$. They conjectured that the amortized communication complexity $\frac{1}{n} \limsup_{n\to\infty} C(f^n)$ cannot differ from $C(f)$ by more than $O(\log m)$ bits. This was further studied in [0] (cf. also [0]), where a partial function is presented with deterministic communication complexity $C(f) = \Theta(\log(m))$ but amortized complexity $O(1)$ and also randomized protocols are studied. Here simultaneous computations can save a lot of communication bits (cf. also [0], pp. 42-48). This contrasts to nondeterministic protocols [0]. The authors of [0] were rather interested in the amortized communication complexity of relations in the study of the circuit depth complexity for the composition of Boolean functions. Related questions had been studied before, e. g., by Paul [0].

5.3 *Comparison of Lower Bound Techniques*

In [0] was considered the function matrix

$$M(f) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \tag{1.16}$$

Since the first two rows and also the last two rows sum up to the all-one vector, the matrices $M_0(f)$ and $M_1(f)$ have rank 3, such that $r(f) = 6$. The largest fooling sets in $M_0(f)$ and $M_1(f)$ have size 4 such that $Ind(f) = 8$. Now the vector-valued function f^n has communication complexity $C(f(^n)) = \lceil 3n \rceil$, where the upper bound is obtained from the trivial protocol and the lower bound via the independence number: $C(f^n) \geq \lceil \log Ind(f^n) \rceil = \lceil \log Ind(f)^n \rceil = \lceil n \cdot \log Ind(f) \rceil = \lceil n \cdot 3 \rceil$. On the other hand the rank bound gives only $C(f^n) \geq \lceil n \log 6 \rceil$. So there is a gap of a factor $\frac{3}{\log 6}$ between communication complexity and bound (5). One might ask how large such gaps can be.
For Boolean functions the possible gaps between the communication complexity and the rank lower bound have intensively been studied, because of its relation to a problem in Graph Theory. It was asked by Lovasz and Saks [0] if for every Boolean function $C(f) = (\log \mathrm{rank} M(f))^{O(1)}$. It turns out that this problem is equivalent to to the problem if $\log \chi(\overline{G}) = (\log \mathrm{rank} G)^{O(1)}$, where G is a graph, $\overline{G}$ its complement, and the rank is taken of the adjacency matrix of G. Raz and Spieker [0] gave an example with a non-constant gap between $\log \mathrm{rank} M(f)$ and the communication complexity. A larger gap ($C(f) = \Omega(n)$, $\log \mathrm{rank} M(f) = O(n^{\log_3 2})$) was found for an explicit function by Nisan and Wigderson [0].

Furthermore, in the above example the lower bound obtained by the independence number $Ind(f)$ is better by a factor $\frac{3}{\log 6}$ than the bound obtained via the sum of ranks $r(f)$. Again, there has been more interest in comparing lower bound techniques for Boolean functions (e. g. [0]). Dietzfelbinger, Hromkovic, and Schnitger [0] constructed a sequence of functions via the Kronecker product from a matrix similar to (16) in order to show that the rank bound yields a result worse by a factor $\frac{\log 3}{2}$ than the bound obtained via largest fooling sets. It was further shown that the fooling set method can yield bounds better by at most a factor 2 than the bounds obtained from the rank of the function matrix and that there exist also functions for which the rank bound is better than the fooling set bound.

References

[1] R. Ahlswede, "On code pairs with specified Hamming distances", Combinatorics, Eger, 1987, *Colloquia Math. Soc. J. Bolyai* 52, 1988, 9 - 47.

[2] R. Ahlswede and M. Mörs, "Inequalities for code pairs", *European J. Combinatorics* 9, 1988, 175–188.

[3] R. Ahlswede and N. Cai, "On communication complexity of vector-valued functions", *IEEE Trans. Inform. Theory* 40, no. 6, 1994, 2062 - 2067, also Preprint 91-041, SFB 343, Bielefeld, 1991.

[4] R. Ahlswede and N. Cai, "2-way communication complexity of sum-type functions for one processor to be informed", *Probl. Inform. Transmission* 30, no. 1, 1994, 1 - 10, also Preprint 91-053, SFB 343, Bielefeld 1991.

[5] R. Ahlswede, N. Cai, and U. Tamm, "Communication complexity in Lattices", *Appl. Math. Letters* 6, no. 6, 1993, 53–58.

[6] R. Ahlswede, N. Cai, and Z. Zhang, "A general 4–word–inequality with consequences for 2–way communication complexity", *Advances in Applied Mathematics* 10, 1989, 75–94.

[7] R. Ahlswede and Z. Zhang, "Code pairs with specified parity of the Hamming distances", *Discr. Math.* 188, 1998, 1 - 11.

[8] R. Ahlswede, A. El Gamal, and K. F. Pang, "A two–family extremal problem in Hamming space", *Discr. Math.* 49, 1984, 1–5.

[9] A. V. Aho, J. D. Ullman, and M. Yannakakis, "On notions of information transfer in VLSI circuits", *Proc. ACM STOC*, 1983, 133-139.

[10] L. Babai, P. Frankl, and J. Simon, "Complexity classes in communication complexity theory", *Proc. IEEE FOCS*, 1986, 337-347.

[11] N. Cai, "A bound of sizes of code pairs satisfying the strong 4–words property for Lee distance", *J. System Sci. Math. Sci.* 6, 1986, 129–135.

[12] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM J. Comp.* 17, no. 2, 1988, 230–261.

[13] M. Dietzfelbinger, J. Hromkovic, and G. Schnitger, "A comparison of two lower bound methods for communication complexity", *Theoret. Comput. Sci.* 168, no. 1, 1996, 39 - 51.

[14] J. Diekmann, "Probabilistische Kommunikationskomplexität", Diploma thesis, Bielefeld, 1997.

[15] P. Delsarte and P. Piret, "An extension of an inequality by Ahlswede, El Gamal and Pang for pairs of binary codes", *Discr. Math.* 55, 1985, 313–315.

[16] A. El Gamal and K. F. Pang, "Communication complexity of computing the Hamming distance", *SIAM J. Comp.* 15, no 4, 1986, 932–947.

[17] T. Feder, E. Kushilevitz, M. Naor, and N. Nisan, "Amortized communication complexity", *SIAM J. Comp.* 24, no. 4, 1995, 736 - 750.

[18] M. Fürer, "The power of randomness for communication complexity", *Proc. ACM STOC*, 1987, 178-181.

[19] W. Haemers, "Disconnected vertex sets and equidistant code pairs", Electron. J. Combin. 4, no. 1, 1997, 10 pp.

[20] B. Halstenberg and R. Reischuk, "Relations between communication complexity classes ", *J. Comput. System Sci.* 41, 1990, 402-429.

[21] J. Hromkovic, *Communication complexity and parallel computing*, Springer, 1997.

[22] J. H. van Lint and J. I. Hall, "Constant distance code pairs", *Proc. Kon. Ned. Akad. v. Wet. (A)* 88, 1985, 41 - 45.

[23] B. Kalyanasundaram and G. Schnitger, "Probabilistic communication complexity of set intersection", *SIAM J. Discr. Math.* 5, 1992, 545-557.

[24] M. Karchmer, E. Kushilevitz, and N. Nisan, "Fractional covers and communication complexity", *SIAM J. Disc. Math.* 8, no. 1, 1995, 76-92.

[25] M. Karchmer, R. Raz, and A. Wigderson, "Super-logarithmic depth lower bounds via direct sum methods in communication complexity", *Proc. 6th IEEE Structure in Complexity Theory*, 1991, 299 - 304

[26] M. Krause, "Geometric arguments yield better bounds for threshold circuits and distributed computing", PhD thesis, Berlin , 1990, also: *Theoret. Comput. Sci.* 156, no. 1-2, 1996, 99 - 117.

[27] E. Kushilevitz and N. Nisan, *Communication complexity*, Cambridge University Press, 1997.

[28] L. Lovasz and M. Saks, "Communication complexity and combinatorial lattice theory", *J. Comput. System Sci.* 47, 1993, 330-337.

[29] K. Mehlhorn and E. M. Schmidt, "Las Vegas is better than determinism in VLSI and distributed computing", *Proc. ACM STOC*, 1982, 330 - 337.

[30] M. Naor, A. Orlitsky, and P. Shor, "Three results on interactive communication", *IEEE Trans. Inform. Theory* 39, no. 5, 1993, 1608 - 1615.

[31] N. Nisan and A. Wigderson, "On rank vs. communication complexity", *Combinatorica* 15, no. 4, 1995, 557-566.

[32] W. Paul, "Realizing Boolean functions on disjoint sets of variables", *Theoret. Comput. Sci.* 2, 1976, 383-396.

[33] R. Raz and B. Spieker, "On the log rank conjecture in communication complexity", *Combinatorica* 15, no. 4, 1995, 567 - 588.

[34] A. Razborov, "On the distributional complexity of disjointness", *Theoret. Comput. Sci.*, 106, 1992, 385-390

[35] U. Tamm, "Communication complexity of sum-type functions", PhD thesis, Bielefeld, 1991.

[36] U. Tamm, "Still another rank determination of set intersection matrices with an application in communication complexity", *Appl. Math. Letters* 7, 1994, 39 - 44.

[37] U. Tamm, “Communication complexity of sum - type functions invariant under translation”, *Inform. and Computation* 116, no. 2, 1995, 162 - 173.

[38] U. Tamm, “Deterministic communication complexity of set intersection”, *Discr. Appl. Math.*, 61, 1995, 271 - 283.

[39] J. H. van Lint, “Distance theorems for code pairs”, *Combinatorial Mathematics: Proceedings of the Third International Conference (New York, 1985), Ann. New York Acad. Sci.* 555, 1989, 421 - 424.

[40] I. Wegener, “Communication complexity and BDD lower bound techniques”, this volume, 1999.

[41] A. C. Yao, “Some complexity questions related to distributive computing”, *Proc. ACM STOC*, 1979, 209–213.