RANK FORMULAS FOR CERTAIN PRODUCTS OF MATRICES

Rudolf Ahlswede and Ning Cai

Universität Bielefeld
Fakultät für Mathematik
Postfach 100131
4800 Bielefeld 1
Germany

Abstract

For two matrix operations, called *quasi–direct sum* and *quasi–outer product*, we determine their deviations from multiplicative behaviour of the rank. The second operation arises in the determination of the function table for so–called sum–type functions such as the Hamming distance.

A consequence of the corresponding rank formula is, that the frequently used log rank can be a very poor bound for two–way communication complexity.

Instead, as was shown in [9], a certain *exponential rank* gives often excellent or even optimal bounds.

1. Introduction

Before we enter our purely algebraic investigations we describe quickly how they originated with [9] in the study of the two–way communication complexity of sum–type functions (as for instance the Hamming distance function). Suppose that for a function $g : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ with finite domain a person (or processor) $P_{\mathcal{X}}$ observes output x and another person $P_{\mathcal{Y}}$ observes output y . They agree in advance on a protocol Q for transmitting alternatively strings of bits to each other. At the end of this exchange $P_{\mathcal{Y}}$ must be able to calculate $g(x,y)$. If $\ell_Q(x,y)$ is the number of bits exchanged for inputs x and y , then

$$L(Q) = \max_{x\in\mathcal{X},y\in\mathcal{Y}} \ell_Q(x,y)$$

is the (worst case) length of the protocol Q . Let $\mathcal{Q}_g$ denote the set of all protocols for g . Then we define the 2–way communication complexity with respect to an informed $P_{\mathcal{Y}}$ by

$$C(g; 1 \leftrightarrow 2^+) = \min_{Q\in\mathcal{Q}_g} L(Q).$$

It is known ([2]) that

$$C(g; 1 \leftrightarrow 2^+) \geq \log \operatorname{rank}_{\mathbb{F}}(M_g), \tag{1.1}$$

when $\mathcal{Z}$ carries a field structure $\mathbb{F}$ and matrix M_g corresponds to the function table of g .

Even though (1.1) is frequently used the bound can be very poor. Examples in [9] are sum–type functions. For sequences $(\mathcal{X}_t)_{t=1}^{\infty}$, $(\mathcal{Y}_t)_{t=1}^{\infty}$ of finite sets and a sequence $(f_t)_{t=1}^{\infty}$ of functions $f_t : \mathcal{X}_t \times \mathcal{Y}_t \to G$, where G is an abelian group, the associated sum–type function $S_n : \mathcal{X}^n \times \mathcal{Y}^n \to G$ is defined by

$$S_n(x^n, y^n) = \sum_{t=1}^{n} f_t(x_t, y_t) \tag{1.2}$$

for all $x^n = (x_1, x_2, \dots, x_n) \in \mathcal{X}^n = \prod_{t=1}^n \mathcal{X}_t$ and $y^n = (y_1, y_2, \dots, y_n) \in \mathcal{Y}^n = \prod_{t=1}^n \mathcal{Y}_t$. To analyse $\operatorname{rank}_{\mathbb{F}}\big(M_{S_n}\big)$, if $G = \mathbb{F}$ is a field, we have to see first how M_{S_n} relates to $M_{f_1}, \dots, M_{f_n}$. Thus we are naturally led to a notion of a product, which we call <u>quasi–outer product</u>:

For the matrices $M^{(t)} = \big(m^{(t)}_{i_t,j_t}\big)_{i_t=1,\dots,\ell_t; j_t=1,\dots,m_t} (t = 1,2)$ the product $M = M^{(1)} \circ_q M^{(2)}$ is an $\ell_1 \cdot \ell_2 \times m_1 \cdot m_2$ matrix whose $\big((i_1,i_2),(j_1,j_2)\big)$'s entry is $m^{(1)}_{i_1,j_1} + m^{(2)}_{i_2,j_2}$.

One readily verifies that

$$M_{S_n} = M_{f_1} \circ_q M_{f_2} \circ_q \cdots \circ_q M_{f_n}. \tag{1.3}$$

We define next the quasi–outer product in terms of outer products of vectors.

Let $\mathbb{F}^n = \{(h_1, \dots, h_n) \mid h_i \in \mathbb{F}\}$ be the n–dimensional vector space over $\mathbb{F}$. For $\vec{u} = (u_1, \dots, u_\ell) \in \mathbb{F}^\ell$ and $\vec{v} = (v_1, \dots, v_m) \in \mathbb{F}^m$ define the outer product

$$\vec{w} = \vec{u} \circ \vec{v} = (u_1 + v_1, u_1 + v_2, \dots, u_1 + v_m, u_2 + v_1, \dots, u_\ell + v_m), \tag{1.4}$$

and for $U = \begin{pmatrix} \vec{u}_1 \\ \vec{u}_2 \\ \vdots \\ \vec{u}_r \end{pmatrix}$ and $V = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_s \end{pmatrix}$ define the quasi–outer product

$$U \circ_q V = \begin{pmatrix} \vec{u}_1 \circ \vec{v}_1 \\ \vec{u}_1 \circ \vec{v}_2 \\ \vdots \\ \vec{u}_r \circ \vec{v}_s \end{pmatrix}.$$

This product can be called also "tensor sum", that is, a "tensor product", where the product operation is replaced by the sum operation. With the name "quasi–outer product" we view as in [5] the operation in the frame of the outer product of vectors.

This notation reminds us of another product. In [5] the outer product of two binary linear codes C and C' is defined as

$$C \circ C' = \{c \circ c' \mid c \in C, c' \in C'\}, \tag{1.5}$$

and it is shown there that

$$\dim(C \circ C') = \begin{cases} \dim C + \dim C' - 1, & \text{if } \vec{1} \in C \cap C' \\ \dim C + \dim C', & \text{if } \vec{1} \notin C \cap C', \end{cases} \tag{1.6}$$

where $\vec{1} = (1, 1, \dots, 1)$ is the vector with all components equal to 1. Actually this result can easily be generalized to subspaces $C \subset \mathbb{F}^{n_1}$, $C' \subset \mathbb{F}^{n_2}$ with an arbitrary field $\mathbb{F}$ (and $C \circ C'$ defined as in (1.5)).

If we denote by $S(M)$ the space spanned by the row vectors of the matrix M, then obviously $\dim S(M) = \mathrm{rank}(M)$. Moreover, by our definitions

$$S\big(M^{(1)} \circ_q M^{(2)}\big) \subseteq S\big(M^{(1)}\big) \circ S\big(M^{(2)}\big) \tag{1.7}$$

and if equality would hold here, then our problem of determining $\mathrm{rank}\big(M^{(1)} \circ_q M^{(2)}\big)$ would be solved by (the generalized form of) (1.6).

However, this equality often does not hold. Nevertheless, we solved our problem via the analysis of another pair of binary operations, namely the familiar direct sum and a relation, which we call quasi–direct sum.

For two linear spaces C and C' the direct sum is the linear space

$$C \oplus C' = \{c \oplus c' \mid c \in C \text{ and } c' \in C'\},$$

where $c \oplus c' = (c, c')$.

For two matrices U and V the quasi–direct sum is

$$U \oplus_q V = \begin{pmatrix} \vec{u}_1 \oplus \vec{v}_1 \\ \vec{u}_1 \oplus \vec{v}_2 \\ \vdots \\ \vec{u}_r \oplus \vec{v}_s \end{pmatrix} .$$

Analogously to (1.7) we have now

$$S\big(M^{(1)} \oplus_q M^{(2)}\big) \subseteq S\big(M^{(1)}\big) \oplus S\big(M^{(2)}\big). \tag{1.8}$$

and equality need not hold. This led us to introduce and investigate the notion of a "missing dimension", resulting in the desired rank formulas.

2. The type and the missing dimension of a set of vectors

Since the space $S(M)$, spanned by the row vectors of a matrix M does not depend on the labelling of the vectors as row vectors, we can study the rank problems described in the Introduction in a more general context by defining a quasi–direct sum for arbitrary sets of vectors as follows.

Suppose that $\phi \neq A \subset \mathbb{F}^m, \phi \neq B \subset \mathbb{F}^n$, then we set

$$A \oplus_q B = A \times B = \{(a,b) : a \in A, b \in B\}. \tag{2.1}$$

This is a subset of the vectorspace $\mathbb{F}^m \oplus \mathbb{F}^n$.

For the analysis of the dimension of its span it is convenient to use the subspace $D(A)$ (and $D(B)$), where

$$D(A) = S\big(\{a - a' : a, a' \in A\}\big), \tag{2.2}$$

and to introduce the type or the missing dimension of A as the number

$$\mu(A) = \dim S(A) - \dim D(A). \tag{2.3}$$

This number obviously equals 0 or 1 . Instead of $S(A)$ or $S\big(\{a, b, \dots\}\big)$ we also write sometimes $< A >$ or $< a, b, \cdots >$.

Lemma 1. *Equivalent are:*

(a) $\mu(A) = 1$

(b) A *contains a basis* C *of* $S(A)$ *with a coefficient matrix* $(\alpha_{ac})_{a\in A, c\in C}$ *(that is,* $a = \sum_c \alpha_{ac} \cdot c$ *for* $a \in A$ *), which satisfies the row–sum condition*

$$\sum_c \alpha_{ac} = 1 \quad \textit{for all} \quad a \in A.$$

(c) Every basis C *of* $S(A)$ *contained in* A *has the property described in (b).*

Proof.

$(a) \Rightarrow (c) \Rightarrow (b)$: The implication " $(c) \Rightarrow (b)$ " is obvious. For a basis $C = \{c_1, \dots, c_n\} \subset A$, we have $D(A) =< t_1 - t_n, \dots, t_{n-1} - t_n >$, because $\mu(A) = 1$. Thus, for all $a \in A$, $a - t_n = \sum_{i=1}^{n-1} \alpha_i (t_i - t_n)$ and hence $a = \sum_{i=1}^{n} \gamma_i t_i$ with $\sum_{i=1}^{n} \gamma_i = 1$.

$(b) \Rightarrow (a)$: Since $a - a' = \sum_c (\alpha_{ac} - \alpha_{a'c}) c \in \big\{\sum_c \gamma_c c : \sum_c \gamma_c = 0\big\}$,
$\dim D(A) = \dim S(A) - 1$.

Lemma 2. *For any* $A \subset \mathbb{F}^m$ *and* $B \subset \mathbb{F}^n$ *we have the properties*

(a) $D(A \times B) = D(A) \oplus D(B)$ *(law of inheritance), in particular* $\dim D(A \times B) = \dim D(A) + \dim D(B)$.

(b) *If* $\mu(A) = \mu(B) = 0$, *then* $S(A \times B) = S(A) \oplus S(B)$

(c) $\mu(A \times B) = \max\bigl(\mu(A), \mu(B)\bigr)$

(d) *If* $\max\bigl(\mu(A), \mu(B)\bigr) = 1$, *then* $D(A) \oplus D(B)$ *is a subspace of* $S(A \times B)$ *of codimension 1.*

(e) $\dim S(A \times B) = \dim S(A) + \dim S(B) - \min\bigl(\mu(A), \mu(B)\bigr)$.

Proof.

(a) Since for any $b^* \in B$ (resp. $a^* \in A$) we have

$$(a - a', 0) = (a, b^*) - (a', b^*) \in D(A \times B)$$

(resp. $(0, b - b') \in D(A \times B)$), we conclude that $(a - a', b - b') \in D(A \times B)$ and thus $D(A) \oplus D(B) \subset D(A \times B)$. Conversely, for any $(a, b) - (a', b') \in D(A \times B)$, we have

$$(a, b) - (a', b') = (a - a', 0) + (0, b - b') \in D(A) \oplus D(B).$$

(b) Since $D(A \times B) \subset S(A \times B) \subset S(A) \oplus S(B) = D(A) \oplus D(B)$, where the equation holds by the assumptions, we conclude with (a) that there are identities everywhere.

(c) The case $\max\bigl(\mu(A), \mu(B)\bigr) = 1$ remains to be considered, so let us assume that $\mu(A) = 1$. Choose any basis $\bigl\{(c_i, d_i) : i \in I\bigr\}$ for $S(A \times B)$ in $A \times B$ and denote its coefficient matrix by $\bigl(\gamma^i_{(a,b)}\bigr)^{i \in I}_{(a,b) \in A \times B}$. Since for $(a, b) \in A \times B$ we have

$$(a, b) = \sum_i \gamma^i_{(a,b)} (c_i, d_i),$$

it is also true that for any $b \in B$

$$a = \sum_i \gamma^i_{(a,b)} c_i \quad \text{for all} \quad a \in A.$$

Since $\mu(A) = 1$ Lemma 1 yields

$$\sum_i \gamma^i_{(a,b)} = 1 \quad \text{for all} \quad a \in A$$

and thus also for all $(a, b) \in A \times B$. Again by Lemma 1 this implies $\mu(A \times B) = 1$.

(d) By (c) and (a) $1 = \mu(A \times B) = \dim S(A \times B) - \dim D(A \times B) = \dim S(A \times B) - \dim D(A) - \dim D(B) = \dim S(A \times B) - \dim\bigl(D(A) + D(B)\bigr)$.

(e) This is an immediate consequence of (a), (b), and (d).

3. The rank under quasi direct sums

Recall that for a set A in a vectorspace V $\operatorname{rank}(A) = \dim S(A)$. We derive consequences of Lemmas 1, 2 for quasi direct sums with N terms. We use the convention $r^+ = \max(r, o)$ for any real number r .

Theorem 1.

Let $A^t (t = 1, \dots, N)$ be subsets of a vectorspace V and let the vectorspace sum $\sum_{t=1}^N S(A^t)$ be isomorphic to the direct sum $\Theta_{t=1}^N S(A^t)$. Furthermore, let $\{U_j^t : j = 1, \dots, d_j\} \subset A^t$ be a basis of $S(A^t)$ $(t = 1, 2, \dots, N)$ and set $T_i = \{t : A^t$ is of type $i\}$ for $i = 0, 1$.

Then we have

(a) $S(\oplus_q {}_{t=1}^N A^t) = \{\sum_{t,j} \beta_j^t U_j^t : \sum_j \beta_j^t = \sum_j \beta_j^{t'}$ *for all* $t, t' \in T_1\}$

(b) $\dim S(\oplus_q {}_{t=1}^N A^t) = \sum_{t=1}^N \dim S(A^t) - (|T_1| - 1)^+$.

Proof. (b) is an immediate consequence of (a). We abbreviate $S(\oplus_q {}_{t=1}^N A^t)$ as $\widetilde{S}$ and show first that any $w \in \widetilde{S}$ is contained in the right hand expression of (a).

We can write $w = \sum_i \alpha_i \sum_t w^t(i)$, where $w_i^t \in A^t$, $w^t(i) = \sum_j \beta_j^t(i) U_j^t$, and $\sum_j \beta_j^t(i) = 1$ for $t \in T_1$ (by Lemma 1).

Now set $\beta_j^t = \sum_i \alpha_i \beta_j^t(i)$ and calculate

$$w = \sum_t \sum_j \left[\sum_i \alpha_i \beta_j^t(i) \right] U_j^t = \sum_{t,j} \beta_j^t U_j^t.$$

Furthermore, for $t \in T_1$ we have

$$\sum_j \beta_j^t = \sum_i \alpha_i \sum_j \beta_j^t(i) = \sum_i \alpha_i.$$

Conversely, we notice first that for every $t \in T_0 \cup T_1$

$$U_j^t - U_1^t = \sum_{t' \neq t} U_1^{t'} + U_j^t - \sum_{t''} U_1^{t''},$$

that

$$\sum_{t' \neq t} U_1^{t'} + U_j^t, \sum_{t''} U_1^{t''} \in \underset{t=1}{\overset{N}{\Theta}}{}_q A_t, \tag{3.1}$$

and that therefore

$$U_j^t - U_1^t \in \widetilde{S} \quad \text{for} \quad t \in T_o \cup T_1. \tag{3.2}$$

Next, for $t \in T_0$, by Lemma 1 there is a $W^t \in A^t$ with

$$W^t = \sum_j \alpha_j^t U_j^t \quad \text{and} \quad \alpha = \sum_j \alpha_j^t \neq 1. \tag{3.3}$$

Now $(1-\alpha)W^t = \sum_j \alpha_j^t (U_j^t - U_1^t) + \alpha(U_1^t - W^t) = \sum_j \alpha_t^t (U_j^t - U_1^t) + \alpha \sum_{t''} U_1^{t''} - \alpha(\sum_{t' \neq t} U_1^{t'} + W^t)$ and since $U_j^t - U_1^t, \sum_{t''} U_1^t, \sum_{t' \neq t} U_1^t + W^t \in \widetilde{S}$, we have also $W^t \in \widetilde{S}$.

Furthermore, $W^t, U_2^t - U_1^t, U_3^t - U_1^t, \ldots, U_{d_t}^t$ are independent, because

$$\begin{aligned} 0 &= \sum_{j \geq 2} \Theta_j (U_t^t - U_1^t) + \theta W^t \\ &= \sum_{j \geq 2} [\Theta_j + \Theta \alpha_j^t] U_j^t + [\Theta \alpha_1^t - \sum_{j \geq 2} \Theta_j] U_1^t \end{aligned}$$

and hence $\Theta_j + \Theta \alpha_j^t = 0 (j \geq 2)$ and also $\Theta \alpha_1^t - \sum_{j \geq 2} \Theta_j = 0$.

We conclude that $\Theta_j = -\Theta \alpha_j^t$ and that $\Theta \alpha_1^t + \sum_{j \geq 2} \Theta \alpha_j^t = \Theta \alpha = 0$. We arrive at $\Theta = 0, \Theta_j = 0 (j \geq 2)$, which was to be shown.

Since every element of A^t is a linear combination of these vectors from $\widetilde{S}$, we obtain

$$A^t \subset \widetilde{S} \quad \text{for} \quad t \in T_0. \tag{3.4}$$

It remains to be seen that $\sum_{t \in T_1} \sum_j \beta_j^t U_j^t$ with $\sum_j \beta_j^t = \beta \quad (t \in T_1)$ is in $\widetilde{S}$.

Now

$$\sum_{t \in T_1} \sum_j \beta_j^t U_j^t = \sum_{t \in T_1} \sum_j \beta_j^t \left[\sum_{t' \in T_1 \setminus \{t\}} U_1^{t'} + U_j^t \right] - \sum_{t \in T_1} \sum_j \beta_j^t \sum_{t' \in T_1 - \{t\}} U_1^{t'}$$

and the first summand is in $\widetilde{S}$, because for any $a_t \in A_t$

$$\sum_{t \in T_1} a_t = \sum_t a_t - \sum_{t \in T_0} a_t \tag{3.5}$$

and $\sum_{t \in T_0} a_t \in \widetilde{S}$ by (3.4), obviously $\sum_t a_t \in \widetilde{S}$, and hence $\sum_{t \in T_1} a_t \in \widetilde{S}$.

We write the second summand in the form

$$\sum_{t\in T_1}\sum_j \beta_j^t \sum_{t'\in T_1-\{t\}} U_1^{t'} = \sum_{t'\in T_1}\left[\sum_{t\in T_1\setminus\{t'\}}\sum_j \beta_j^t\right] U_1^t = (|T_1|-1)\beta \sum_{t'\in T_1} U_1^{t'}.$$

By the reasoning above this is also an element of $\widetilde{S}$.

Corollary. *Suppose that* $\left\{M^{(t)}\right\}_{t=1}^{N}$ *is a sequence of matrices over* $\mathbb{F}$ *and that*

$$M = M^{(1)} \oplus_q M^{(2)} \oplus_q \cdots \oplus_q M^{(N)},$$

then

$$\text{(i) } S(M) = \left\{\sum_j \beta_j^1 U_j^1 \oplus \sum_j \beta_j^2 U_j^2 \oplus \cdots \oplus \sum_j \beta_j^N U_j^N;\ \sum_j \beta_j^t = \sum_j \beta_j^{t'} \text{ for all } t,t' \in T_1\right\},$$

where $\left\{U_j^t\right\}_{j=1}^{d_t}$ *is a maximal set of independent row vectors of* $M^{(t)}$ *and* $\beta_j^t \in \mathbb{F}$.

4. The rank under quasi outer products

We begin with an elementary result, which is a key tool in Proposition 1 of [5].

Lemma 3. *For positive integers* $m_1, \dots, m_L$ *with* $\sum_{t=1}^{L} m_t = n$ *write*

$$\mathbb{F}^n = \mathbb{F}^{m_1} \oplus \mathbb{F}^{m_2} \oplus \cdots \oplus \mathbb{F}^{m_L}$$

(Recall that for vector spaces the operations " $\oplus$ *" and "* $\oplus_q$ *" are the same.)*

The map $\varphi : \mathbb{F}^n \to \mathbb{F}^{\prod_{t=1}^{L} m_t}$ *, which sends* $f^{m_1} \oplus f^{m_2} \oplus \cdots \oplus f^{m_L} = (f^{m_1}, \dots, f^{m_L})$ *to* $f^{m_1} \circ f^{m_2} \circ \cdots \circ f^{m_L}$ *, is linear and has a null space*

$$N_\varphi = \big\{(x_1, \dots, x_1, x_2, \dots, x_2, \dots, x_L, \dots, x_L) \mid \sum_{t=1}^{L} x_t = 0\big\} \tag{4.1}$$

(Here x_t occurs m_t times.)

Proof. The linearity of φ is immediate from the definitions. Further, let $\varphi(z^n) = 0$.

We write $z^{(t)} \triangleq \big(z_1^{(t)}, \dots, z_{m_t}^{(t)}\big)$ and $z^n = \big(z^{(1)} \oplus z^{(2)} \oplus \cdots \oplus z^{(L)}\big) = \big(z^{(1)}, \dots, z^{(L)}\big)$.

Then the $(j_1, \dots, j_L)$–th component of $\varphi(z^n)$ is

$$\varphi\big(z^n;\ (j_1, \dots, j_L)\big) = \sum_{t=1}^{L} z_{j_t}^{(t)}. \tag{4.2}$$

Since $\varphi(z^n) = 0$ implies

$$\varphi\big(z^n;\ (i, j_2, \dots, j_L)\big) = \varphi\big(z^n;\ (i', j_2, \dots, j_L)\big) = 0$$

by (4.2), $z_i^{(1)} = z_{i'}^{(1)}$. Similarly, $z_i^{(t)} = z_{i'}^{(t)}$ for all t and thus (4.1).

For a sequence of matrices $\big(M^{(t)}\big)_{t=1}^{N}$ over $\mathbb{F}$ we are going to determine for

$$M^0 = M^{(1)} \circ_q M^{(2)} \circ_q \cdots \circ_q M^{(N)} \tag{4.3}$$

rank M^0 .

For this we need a partition of $\{1, 2, \dots, N\}$, which is a refinement of $\{T_1, T_0\}$ and defined as follows:

$$P_0 = \{t \mid t \in T_1, \nexists\ \xi_i\text{'s} \in \mathbb{F} \text{ with } \sum_i \xi_i U_i^{(t)} = \vec{1}\}$$

$$P_1 = \{t \mid t \in T_0, \nexists\ \xi_i\text{'s} \in \mathbb{F} \text{ with } \sum_i \xi_i U_i^{(t)} = \vec{1}\}$$

$$P_2 = \{t \mid t \in T_1, \exists\ \xi_i\text{'s} \in \mathbb{F} \text{ with } \sum_i \xi_i U_i^{(t)} = \vec{1}, \sum_i \xi_i = 0\}$$

$$P_3 = \{t \mid t \in T_0, \exists\ \xi_i\text{'s} \in \mathbb{F} \text{ with } \sum_i \xi_i U_i^{(t)} = \vec{1}\}$$

$$P_4 = \{t \mid t \in T_1, \exists\ \xi_i\text{'s} \in \mathbb{F} \text{ with } \sum_i \xi_i U_i^{(t)} = \vec{1}, \sum_i \xi_i \neq 0\} \tag{4.4}$$

It is clear from the definition of P_4 that for all $t \in P_4$ there are $\xi(t,i) \in \mathbb{F}$ with

$$\sum_i \xi(t,i) = 1, \ \sum_i \xi(t,i) U_i^{(t)} = \Theta^{(t)} \cdot \vec{1} \text{ and } \Theta^{(t)} \neq 0. \tag{4.5}$$

Theorem 2. *Let* M^0 , $\{P_i\}$ *and* $\Theta^{(t)}$ *be defined as above and let us use the abbreviation*

$$R = \sum_t \mathit{rank}\ M^{(t)} - (|T_1| - 1)^+, \tag{4.6}$$

$$R' = R - 1 - (|P_2| + |P_3| - 1)^+. \tag{4.7}$$

Then

$$\mathit{rank}\ M^0 = \begin{cases} R' \begin{cases} \textit{if } P_0 = P_2 = \varnothing, P_4 \neq \varnothing, P_3 \neq \varnothing & \textit{(i)} \\ \textit{or if } P_0 = P_2 = \varnothing, P_4 \neq \varnothing, P_3 = \varnothing & \textit{(ii)} \\ \quad \textit{and } \sum_{t \in P_4} \Theta^{(t)} = 0 & \end{cases} \\ R' + 1 \ \textit{otherwise.} \qquad\qquad\qquad\qquad\qquad\qquad \textit{(iii)} \end{cases}$$

Proof. Consider

$$M = M^{(1)} \oplus_q M^{(2)} \oplus_q \cdots \oplus_q M^{(N)} \tag{4.8}$$

and let φ_M be the restriction of φ (defined in Lemma 3) on the linear subspace $S(M)$. Then for any sequence $\left(A^{(t)}\right)_{t=1}^N$, where $A^{(t)}$ is any row vector of $M^{(t)}$, φ_M sends $A^{(1)} \oplus \cdots \oplus A^{(N)}$ to $A^{(1)} \circ \cdots \circ A^{(N)}$, i.e. the image space $\varphi_M(S(M))$ of $S(M)$ under φ_M equals $S(M^\circ)$. Therefore

$$\begin{aligned}
\text{rank } M^\circ &= \dim\bigl(S(M^\circ)\bigr)\\
&= \dim\bigl(S(M)\bigr) - \dim\ (\text{null space of } \varphi_M)\\
&= \dim\bigl(S(M)\bigr) - \dim\bigl(N_\varphi \cap S(M)\bigr)\\
&= \sum_t \text{rank } M^{(t)} - (|T_1| - 1)^+ - \dim\bigl(N_\varphi \cap S(M)\bigr). \qquad (4.9)
\end{aligned}$$

Here the third equality follows from Lemma 3 and the last equality follows from (ii) in Corollary 1.

Next by relabelling components we can assume w.l.o.g. that for all $t_i \in P_i \neq \varnothing \quad (i = 0, \dots, 4) \quad t_0 < t_1 < t_2 < \cdots < t_4$. Then every vector contained in $N_\varphi \cap S(M)$ has , by Lemma 3, the form

$$\Bigl(\varepsilon_1^0 \vec{1} \oplus \cdots \oplus \varepsilon_{|P_0|}^0 \vec{1}\Bigr) \oplus \Bigl(\varepsilon_1^1 \vec{1} \oplus \dots\Bigr) \oplus \cdots \oplus \Bigl(\varepsilon_1^4 \vec{1} \oplus \cdots \oplus \varepsilon_{|P_4|}^4 \vec{1}\Bigr) \qquad (4.10)$$

(where the first term in brackets corresponds to the P_0–part etc.) with

$$\sum_{x=0}^{4} \sum_{t \in P_x} \varepsilon_t^x = 0. \qquad (4.11)$$

Now, for a further analysis we use (i) of Corollary 1:

For all $t \in P_x$ there are $\eta(t,i)$'s in $\mathbb{F}$ with

$$\varepsilon_t^x \vec{1} = \sum_i \eta(t,i) U_i^{(t)} \qquad (4.12)$$

and for all $t, t' \in P_0 \cup P_2 \cup P_4$

$$\sum_i \eta(t,i) = \sum_{i'} \eta(t', i'). \qquad (4.13)$$

Also, by the definition of P_x ,

$$\varepsilon_t^x = 0 \ \text{ for all } \ t \in P_x \ (x = 0, 1). \qquad (4.14)$$

We discuss now the cases.

If $P_2 \neq \varnothing$ or $P_0 \neq \varnothing$, then by (4.13)

$$\varepsilon_t^4 = 0 \ \text{ for all } \ t \in P_4$$

and for $t \in P_x \quad (x = 2, 3) \quad \varepsilon_t^x$ can take any value obeying (4.11). Also, when $P_4 = \varnothing$, we have the same situation: $\operatorname{rank} M^0 = R' + 1$.

Henceforth we can assume therefore $P_0 = P_2 = \varnothing$ and $P_4 \neq \varnothing$.

Then for $\mu(t,i)$'s in (4.12) we can have by (4.13)

$$\sum_i \eta(t,i) = c \text{ (a constant) for all } t \in P_4 \tag{4.15}$$

However, by (4.5) and (4.12)

$$\begin{aligned} \sum_i \eta(t,i) U_i^{(t)} = \varepsilon_t^4 \vec{1} &= \left(\sum_i \xi(t,i) U_i^{(t)} \right) \frac{\varepsilon_t^4}{\Theta^{(t)}} \\ &= \sum_i \left(\xi(t,i) \frac{\varepsilon_t^4}{\Theta^{(t)}} \right) U_i^{(t)} \text{ for all } t \in P_4, \end{aligned}$$

where $\xi(t,i)$ and $\Theta^{(t)}$ are defined by (4.5).

By the uniqueness of representations

$$\eta(t,i) = \frac{\varepsilon_t^4}{\Theta^{(t)}} \xi(t,i) \text{ for all } t \in P_4.$$

Summation on both sides over i, (4.5), and (4.15) give $c = \frac{\varepsilon_t^4}{\Theta^{(t)}}$ or

$$\varepsilon_t^4 \vec{1} = c\, \Theta^{(t)} \vec{1} \text{ for all } t \in P_4. \tag{4.16}$$

When $P_3 \neq \varnothing$, then $\varepsilon_t^3, t \in P_3$, can take all values in $\mathbb{F}$ and by (4.16), (4.10), and (4.11) we obtain

$$\dim\big(N_\varphi \cap S(M)\big) = \big(|P_3| + 1\big) - 1 = |P_3|$$

and therefore (iii).

When $P_3 = \varnothing$ and $\sum_{t \in P_4} \Theta^{(t)} \neq 0$, then by (4.11), (4.14), and (4.16) $c = 0$, i.e. all ε_t^x equal 0. This means that $N_\varphi \cap S(M) = \{\vec{0}\}$, so (iii) holds.

Finally, when $\sum_{t \in P_4} \Theta^{(t)} = 0$, then (4.9) implies (4.11), i.e. c in (4.16) can take all values in $\mathbb{F}$. We have $\dim N_\varphi \cap S(M) = 1$ and thus (iii). The proof is complete.

References

[1] Yao, A.: Some Complexity Questions related to Distributive Computing. Proceedings 11th Ann. ACM Sympos. Theory of Computing, 209–213 (1979)

[2] Mehlhorn, K., Schmidt, E.M.: Las Vegas is Better than Determinism in VLSI and Distributed Computing. Proceedings 14th ACM STOC, 330–337 (1982)

[3] Papadimitriou, C.H., Sipser, M.: Communication Complexity. Proceedings 14th Ann. ACM Sympos. on Theory of Computing, 201–214 (1982)

[4] Ahlswede, R., Cai, N., Zhang, Z.: A General 4–Words Inequality with Consequences for 2–way Communication Complexity. Advances in Applied Mathematics **10**, 75–94 (1989)

[5] Brualdi, R., Cai, N., Pless, V.: Orphan Structure of the First Order Reed–Muller Codes. To appear in Discrete Math.

[6] Tamm, U.: Communication Complexity of Sum–Type Functions Invariant under Translation. Preprint 91–016 SFB 343 "Diskrete Strukturen in der Mathematik". To appear in Information and Computation.

[7] Ahlswede, R., Cai, N.: On Communication Complexity of Vector–Valued Functions. Preprint 91–041 SFB 343 "Diskrete Strukturen in der Mathematik", submitted to IEEE Trans. Information Theory.

[8] Ahlswede, R.: On Code Pairs with Specified Hamming Distances. Colloquia Mathematica Societatis János Bolyai 52. Combinatorics, Eger, 9–47 (1987)

[9] Ahlswede, R., Cai, N.: Two–Way Communication Complexity of Sum–Type Functions for One Processor to be Informed. Preprint 91–053 SFB 343 "Diskrete Strukturen in der Mathematik", submitted to IEEE Trans. Information Theory.

[10] Lovász, L.: Communication Complexity. A Survey in "Paths, Flows, and VLSI–Layout", Korte, B., Lovász, L., Prömel, H.J., Schrijver, A. (ed.): Springer, 235–266 (1990)