SURPRISING APPLICATIONS AND POSSIBLE EXTENSIONS OF DELSARTE'S METHOD

MÁTÉ MATOLCSI

Abstract. This is a short informal survey on some surprising applications of Delsarte's method, written for anyone being interested. I try to keep it as short and as informative as possible.

1. Introduction

Everything written here is **joint work with I. Ruzsa or M. Weiner** (or both of them, in some of the problems).

The aim of the project is twofold:

• **Identify problems** in different branches of mathematics where Delsarte's linear programming method could be applied. **Apply Delsarte's method** in these problems **to the best possible extent** (to achieve this is already far from obvious in some of the problems – as we shall see).

• More challengingly, identify **extensions** and **generalizations** of **Delsarte's method** (such as the application of **semi-definite programming** described in [1, 13]) in order to get sharper upper bounds. It is very well possible that the results of [1] can be applied, but i will need some time to digest them.

Achieving these goals could lead to the solution of prestigious conjectures – see below.

2. Difference sets and Delsarte's method

In this section we describe Delsarte's method in a form convenient to us (i was introduced to this form of the method by I.Ruzsa). It is not the most general form (as far as i know, the most general form is given by commutative association schemes), but it has two advantages:

– It is general enough to encompass many interesting applications.

– Delsarte's linear programming bound in this case reduces to Fourier analysis, so that the method is very simple (in principle) to apply.

Let us turn to the description of the scheme. Let G be a compact Abelian group, and let a symmetric subset $A = -A \subset G$, $0 \in A$ be given. We will call A the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \dots b_m\} \subset G$ such that all differences $b_j - b_k \in A^c \cup \{0\}$ (in other words, all differences avoid the forbidden set A). Some well-known examples of this general scheme are present in coding theory ([3]), sphere-packings ([2]), and sets avoiding square differences in number theory ([12]).

We now describe Delsarte's method in this scenario.

We are looking for a 'witness' function $h : G \to \mathbb{R}$ with the following properties.

• h is an even function, $h(x) = h(-x)$, such that the Fourier inversion formula holds for h (in particular, h can be any finite linear combination of characters on G).

• $h(x) \leq 0$ for all $x \in A^c$

• $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{G}$

• $\hat{h}(0) = 1$. (For this normalization we also need to agree how the measure is normalized on G. Of course, we normalize it so that the measure of the whole group G is 1.)

Lemma 2.1. *(Delsarte's method)*
Given a function $h : G \to \mathbb{R}$ with the properties above, we can conclude that for any $B = \{b_1, \dots b_m\} \subset G$ such that $b_j - b_k \in A^c \cup \{0\}$ the cardinality of B is bounded by $|B| \leq h(0)$.

Proof. For any $\gamma \in \hat{G}$ define $\hat{B}(\gamma) = \sum_{j=1}^{m} \gamma(b_j)$. Now, evaluate

$$S = \sum_{\gamma \in \hat{G}} |\hat{B}(\gamma)|^2 \hat{h}(\gamma). \tag{1}$$

All terms are nonnegative, and the term corresponding to $\gamma = 0$ (the trivial character, i.e. $\gamma(x) = 1$ for all $x \in G$) gives $|\hat{B}(0)|^2 \hat{h}(0) = |B|^2$. Therefore

$$S \geq |B|^2. \tag{2}$$

On the other hand, $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j - b_k)$, and therefore $S = \sum_{\gamma,j,k} \gamma(b_j - b_k)\hat{h}(\gamma)$. Summing up for fixed j, k we get $\sum_{\gamma} \gamma(b_j - b_k)\hat{h}(\gamma) = h(b_j - b_k)$ (the Fourier inversion formula), and therefore $S = \sum_{j,k} h(b_j - b_k)$. Notice that $j = k$ happens $|B|$-many

times, and all the other terms (when $j \neq k$) are non-positive because $b_j - b_k \in A^c$, and h is required to be non-positive there. Therefore

$$S \leq h(0)|B|. \tag{3}$$

Comparing the two estimates (2), (3) we obtain $|B| \leq h(0)$. □

Remark 2.2. One advantage here is that *any* witness function gives an upper bound. We may not be able to find the "best" witness function, but nevertheless we may still be able to prove strong upper bounds.

Remark 2.3. Notice that all conditions on h are *linear*. Therefore, on finite groups (of relatively small cardinality) one can find the best witness function by linear programming. This is very convenient.

Definition 2.1. Let us introduce the notation $\lambda^-(A)$ as the infimum of the possible values of $h(0)$ (i.e. the extremal value in our linear programming problem; this is the theoretical limit of Delsarte's method).

And here we come to the possibly **most important point of the project:**

Problem 2.4. *Beat this linear programming bound. Using semi-definite programming find a generalization of Delsarte's bound in this scenario. Preferably identify a "witness object" which testifies an upper bound as does the function h above. My feeling is that Delsarte's method should be "level 1" of some more general semi-definite programming scheme. At level k we should identify a witness object h_k which gives a better upper bound than h_{k-1}.*

3. Duality

The other huge advantage of the linear conditions on h is the following duality. Informally speaking: if a 'good' witness function h does not exist, it is because some 'generalized set' B of large cardinality exists. More precisely, note the following properties of the function $f(x) = \frac{1}{|B|^2}(1_B * 1_{-B})(x)$. (We think of G as being finite. If G is not finite, then f is a measure, rather than a function; in that case it is more convenient to remove the mass at zero, i.e. to consider the measure $f = \frac{1}{|B|^2}(1_B * 1_{-B}) - \frac{1}{|B|}\delta_0$. In that case the properties of f below change accordingly. I just mention this, because this is what we will do in describing the duality in Littlewood's conjecture.)

- $f(x)$ is a nonnegative, even function.
- $f(x)$ is supported on $A^c \cup \{0\}$.
- The Fourier transform $\hat{f}(\gamma)$ is nonnegative for each γ.

• Finally, $\hat{f}(0) = 1$ and $f(0) = \frac{1}{|B|}$.

In order to look for a 'generalized set' B (in fact, rather a generalized difference set $B - B$), we might as well look for a function f with the properties above, and minimize the value of $f(0)$ (because this corresponds to maximizing the size of $|B|$, as $f(0) = \frac{1}{|B|}$). This gives us another linear programming problem.

Definition 3.1. Let us introduce the notation $\lambda^+(A^c)$ for the infimum of the possible values of $f(0)$ above.

The two linear programming problems are connected by the following nice duality:

Proposition 3.1. $\lambda^-(A)\lambda^+(A^c) = 1$.

I skip the proof but it is not very hard. The main point is that this duality introduces a *dichotomy*: either Delsarte's method works well (i.e. we get a strong upper bound on $|B|$ by the linear program on h), or we can detect its failure (by the linear program on f). In principle, that is... In practice, the only problem that can occur is that possibly we cannot determine either of $\lambda^-(A), \lambda^+(A^c)$. The situation is particularly intriguing in the case of the Littlewood conjecture – see below.

4. Applications of Delsarte's method

In this section i describe some applications that we have in mind. Further applications are likely to emerge in the future.

4.1. **Well-known applications.** Let me start by some well-known applications.

1. Binary codes with prescribed Hamming distance. This is the original setting of Delsarte. The group is $G = \mathbb{Z}_2^n$ and the forbidden subset A is the set of words with weight less than d. We have not worked on this.

2. Sphere-packing in Euclidean spaces. It is quite surprising that it was only realized fairly recently that Delsarte's method can be used to good effect in this case, [2]. It should have been obvious immediately... The group $G = \mathbb{R}^n$ is not compact, but a simple limiting argument shows that one can consider the n-dimensional torus $G = \mathbb{T}^n = [-1/2, 1/2)^n$ instead, and the forbidden set $A = B(0, r)$ the ball of some small radius r around zero. Some of the best upper bounds on density of sphere-packings are obtained by Delsarte's method [2]. We have not worked on this.

3. Integer sets without prescribed differences. In number theory it is a famous problem to give bounds on the cardinality of a set $B \subset \{0, 1, \dots, N\}$ such that the differences $b_i - b_j$ avoid certain sets. For example, the differences $b_i - b_j$ are never square numbers (as described in [12]). It is clear that Delsarte's method can be applied, but it is not at all clear how to find the "best" witness function h, and what upper bound it gives. We are working on it [10].

If you follow Delsarte's method you conclude that the aim is to construct non-negative cosine polynomials with square frequencies only (in principle non-square frequencies are also allowed with negative coefficients, but we cannot make any use of them at the moment). An old argument of Imre Ruzsa (unpublished; not hard but rather clever), proves that if we use positive coefficients only then we cannot get any better bound than $\frac{N}{\log N}$ which is far inferior to the best currently known bound of [11]. However, some current calculations show that allowing negative weights will improve the upper bound considerably. We will need to write it up and work out all the details.

Update: The problem of avoiding the cubes seems to be a lot easier. The reason is that a direct product construction can be used in the modular case. We get a power gain in the modular case, and we hope to carry it over with a "black-box" theorem to the case of the integers. The black-box should work all the same for the squares, but we cannot get a power-gain in the modular case.

4.2. **New applications.** Here I will list three surprising applications.

4. Littlewood's conjecture. This is a rather surprising application. Also, it is a very prestigious open problem in number theory, and the solution of it is a great challenge. Let me describe the problem and its reformulation in terms of Delsarte's method:

Littlewood's conjecture states that for all real numbers α, β we have $\liminf n\|n\alpha\|\|n\beta\| = 0$, where $\|x\|$ denotes the distance of x from the closest integer. This conjecture has been open for some 80 years and the strongest result so far asserts that the set of possible exceptions α, β has Hausdorff dimension 0 in the plane [5].

One can see the relevance of Delsarte's method after reading a combinatorial reformulation of the problem on Tim Gowers' web-blog on this

topic: http://gowers.wordpress.com/2009/11/17/ problems-related-to-littlewoods-conjecture-2/ (Actually, i was introduced to the same reformulation by I. Ruzsa.) Following Gowers, let us assume by contradiction that there exists a counterexample α, β to Littlewood's conjecture. Then there exists a $\delta > 0$ such that $n\|n\alpha\|\|n\beta\| > \delta$, for all n. Now, consider a large even integer M, and take the points $P_j = (j/M, \{ja\}, \{jb\})$ in the 3-dimensional torus $\mathbb{T}^3 = [-1/2, 1/2)^3$, for $j = 1, \dots M/2$. (Here $\{x\}$ denotes the fractional part of x.) There are $M/2$ such points P_j and they have the property that the difference of any two of them lies outside the hyperboloid $H_\varepsilon = \{(x, y, z) : |xyz| < \varepsilon\}$, where $\varepsilon = \delta/M$. This leads to the fact that for every $\varepsilon > 0$ there must exist c/ε points in the 3-dimensional torus $\mathbb{T}^3$ such that the difference of any two of them falls outside the hyperboloid $H_\varepsilon = \{(x, y, z) : |xyz| < \varepsilon\}$. Therefore, in the language of Delsarte's scheme the underlying group is $G = \mathbb{T}^3$ and the forbidden set is $A = H_\varepsilon$. (The funny thing is that even after reading this reformulation not a single one of the many comments mentioned that Delsarte's method could be used here. Somehow mathematicians are not aware of it.)

What is the maximum number of points in $\mathbb{T}^3$ such that all the pairwise differences lie outside H_ε? In order to prove Littlewood's conjecture we must show that this quantity is $o(1/\varepsilon)$. To do so, it is sufficient to exhibit witness functions h_ε on the torus $\mathbb{T}^3$ such that $h_\varepsilon(x) = h_\varepsilon(-x)$, $h_\varepsilon|_{G\setminus H_\varepsilon} \leq 0$, $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{G} = \mathbb{Z}^3$, and $h(0)/\hat{h}(0) = o(1/\varepsilon)$. Of course, it is not at all obvious how to construct such functions, but neither is it obvious that such witness functions cannot exist.

In fact, using the duality principle described in the section above, we can also see what is needed to refute Delsarte's method in this setting (i.e. to prove that it cannot lead to the solution of Littlewood's conjecture; but be aware that such a refutation would only mean the failure of Delsarte's method and not the falsity of Littlewood's conjecture). We should find witness functions f_ε on the torus $\mathbb{T}^3$ such that $f_\varepsilon(x) = f_\varepsilon(-x)$, f_ε is supported on H_ε^c, $\hat{f}_\varepsilon(0) = 1$, and $\hat{f}(\gamma) \geq -c\varepsilon$ for all γ.

Starting from scratch it is not at all obvious whether the witnesses h_ε or f_ε will exist. We know by duality that either one or the other. Tim Gowers ventured to call it a "win-win" situation. The only way we can "lose" is if we cannot decide whether h_ε or f_ε exists. And this is exactly the situation right now, unfortunately. Nevertheless, this remains a promising approach to Littlewood's conjecture.

5. Mutually unbiased bases. This is another unexpected application. It is well-described in my preprint [9]. However, I will use slightly different and more convenient notations here to make things more transparent.

Recall that given an orthonormal basis $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ in $\mathbb{C}^d$, a unit vector $\mathbf{v}$ is called *unbiased* to $\mathcal{A}$ if $|\langle \mathbf{v}, \mathbf{e}_k \rangle| = \frac{1}{\sqrt{d}}$ for all $1 \leq k \leq d$. Two orthonormal bases in $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \dots, \mathbf{f}_d\}$ are called *unbiased* if for every $1 \leq j, k \leq d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \frac{1}{\sqrt{d}}$. A collection $\mathcal{B}_0, \dots \mathcal{B}_m$ of orthonormal bases is said to be *(pairwise) mutually unbiased* if every two of them are unbiased. What is the maximal number of pairwise mutually unbiased bases (MUBs) in $\mathbb{C}^d$? This question originates from quantum information theory and has been investigated thoroughly over the past decades (see [4] for a recent comprehensive survey on MUBs). The following result is well-known (see e.g. [4] and references therein for the original proofs; i will not try to give a comprehensive list of references here):

Theorem 4.1. *The number of mutually unbiased bases in $\mathbb{C}^d$ cannot exceed $d + 1$.*

The other important well-known result concerns prime-power dimensions (see e.g. [8] for a particularly simple construction).

Theorem 4.2. *A collection of $d + 1$ mutually unbiased bases (called a complete set of MUBs) can be constructed if the dimension d is a prime or a prime-power.*

However, if the dimension $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is composite then very little is known except for the fact that there are at least $p_j^{\alpha_j} + 1$ mutually unbiased bases in $\mathbb{C}^d$ where $p_j^{\alpha_j}$ is the smallest of the prime-power divisors. In some specific square dimensions there is also a construction based on orthogonal Latin squares which yields more MUBs than $p_j^{\alpha_j}+1$ (see [14]). The following basic problem, however, remains open for all non-primepower dimensions:

Problem 4.3. *Does a complete set of $d + 1$ mutually unbiased bases exist in $\mathbb{C}^d$ if d is not a prime-power?*

The answer is not known even for $d = 6$, despite considerable efforts over the past few years. The case $d = 6$ is particularly tempting because it seems to be the simplest to handle with algebraic and numerical methods. As of now, some *infinite families* of MUB-triplets in $\mathbb{C}^6$ have

been constructed ([15, 7]), but numerical evidence suggests that there exist no MUB-quartets.

To reformulate the problem in Delsarte's scheme, it will be important for us to recall that mutually unbiased bases are naturally related to *complex Hadamard matrices*. Indeed, if the bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ are mutually unbiased we may identify each $\mathcal{B}_l = \{\mathbf{e}_1^{(l)}, \dots, \mathbf{e}_d^{(l)}\}$ with the *unitary* matrix

$$[H_l]_{j,k} = \left[\left\langle \mathbf{e}_j^{(0)}, \mathbf{e}_k^{(l)} \right\rangle_{1\le k,j\le d}\right],$$

i.e. the k-th column of H_l consists of the coordinates of the k-th vector of $\mathcal{B}_l$ in the basis $\mathcal{B}_0$. (Throughout the paper the scalar product $\langle ., . \rangle$ of $\mathbb{C}^d$ is conjugate-linear in the first variable and linear in the second.) With this convention, $H_0 = I$ the identity matrix and all other matrices are unitary and have entries of modulus $1/\sqrt{d}$. Therefore, the matrices $H_l' = \sqrt{d}H_l$ have all entries of modulus 1 and complex orthogonal rows (and columns). Such matrices are called *complex Hadamard matrices*. It is thus clear that the existence of a family of mutually unbiased bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ is equivalent to the existence of a family of complex Hadamard matrices $H_1', \dots, H_m'$ such that for all $1 \le j \ne k \le m$, $\frac{1}{\sqrt{d}} H_j'^* H_k'$ is again a complex Hadamard matrix.

How do mutually unbiased bases fit into Delsarte's scheme? The answer is that they almost perfectly do, except for the fact that the underlying group is not Abelian. Indeed, let $G = U_{d\times d}$ the group of $d \times d$ unitary matrices, and let $H \subset U_{d\times d}$ denote the set of complex Hadamard matrices (rescaled by the factor $1/\sqrt{d}$)) in $U_{d\times d}$. Let the 'forbidden' set A be the complement of H. Of course, the group operations $+$ and $-$ in the Delsarte scheme are now replaced by matrix multiplication and inverse. Also, the role of zero element is taken by the identity matrix. Then, the maximal number of mutually unbiased bases in $\mathbb{C}^d$ is exactly the maximal cardinality of a set $\{U_0,\ U_1, \dots U_m\} \subset G$ such that all 'differences' $U_j^* U_k$ $(0 \le j, k \le m)$ lie in the prescribed subset $A^c \cup \{I\}$.

Unfortunately, we do not know how to generalize Delsarte's method to the case of non-commutative groups, in particular to $G = U_{d\times d}$. Nevertheless, we can still use Delsarte's scheme if we rephrase the problem appropriately, as follows.

Assume that a family $H_1, \dots H_m$ of m mutually unbiased complex Hadamard matrices exists. Then all entries of all matrices are of modulus 1, and the columns (and thus the rows) within each matrix are complex orthogonal, and we have the unbiasedness condition: for any

two columns $\mathbf{u}, \mathbf{v}$ coming from different matrices we have $|\langle \mathbf{u}, \mathbf{v} \rangle| = \sqrt{d}$. (Recall that we have re-normalized the matrices by a factor of $\sqrt{d}$.)

Each column vector $\mathbf{z}$ of each matrix H_j can be regarded as an element of the group $G = \mathbb{T}^d$. (In this case $\mathbb{T}$ is regarded as the complex unit circle, and the group-operation in $\mathbb{T}^d$ is coordinate-wise multiplication.) Also, note that each column can be multiplied by any complex number of modulus 1, without changing orthogonality or unbiased conditions. Therefore, each $\mathbf{z}$ can be regarded as an element of the factor group $G_0 = G/C$ where C denotes the subgroup of coordinate-wise constant vectors. The dual group is then $\hat{G}_0 = \mathbb{Z}_0^d$ the set of integer vectors of dimension d with coordinate sum equal to 0.

Let us introduce the orthogonality set ORT_d in G_0 as the set of vectors $\{\mathbf{z} = (z_1, \dots z_d) \ : \ z_1 + \cdots + z_d = 0\}$. Also, introduce the unbiased set $UB_d = \{\mathbf{z} = (z_1, \dots z_d) \ : \ |z_1 + \cdots + z_d| = \sqrt{d}\}$. We see that any two column-vectors $\mathbf{z_1}, \mathbf{z_2}$ appearing in the matrices H_j satisfy that $\mathbf{z_1}/\mathbf{z_2}$ belongs either to ORT_d or UB_d. Therefore, if we define the forbidden set $A_d \subset G_0$ as the complement $A_d = (ORT_d \cup UB_d)^c$, then we have arrived to Delsarte's scheme.

Actually, Delsarte's method with an appropriate witness function immediately gives a new proof of Theorem 4.1 (in a slightly more general form; see [9]). The witness function is:
$h(\mathbf{z}) = |z_1 + \cdots + z_d|^2(|z_1 + \cdots + z_d|^2 - d)$.

Remark 4.4. Clearly, this witness function is best possible if d is a prime power. There is some hope that better witnesses exist if $d = 6$, for example. But upon numerical evidence, I am inclined to doubt it. **Here again, any improvement on Delsarte's method by semi-definite programming would lead to the solution: a complete system of MUB's does not exist for $d = 6$.**

Remark 4.5. The forbidden set (or rather its complement) naturally breaks up as a union of ORT_d and UB_d. Somehow it looks like a waste to simply take the union, and handle them together. We are losing information: originally we know how many orthogonal and unbiased pairs of vectors should be, but we cannot handle them separately in Delsarte's method. However, we have made some good progress in this direction: we have introduced a "generalization" of Delsarte's scheme for the situation when A^c breaks up into two parts. And we have been able to prove all the results known in the literature up to dimension 5, but dimension 6 still eludes us. I will not describe this generalization here.

6. Mutually orthogonal Latin squares. Somehow MUBs and MOLs go hand-in-hand, so by now it may be less surprising that Delsarte's scheme applies also to the problem of MOLs.

The idea is to build up a complete analogy between MUBs and MOLs. Assume that a complete system $S_1, \dots S_{n-1}$ of MOLs of order n exist. (This is well-known to be equivalent to the existence of a finite affine (or projective) plane of order n. We will exploit this equivalence, without explicitly mentioning it.) For notational convenience we agree that the matrices S_j are filled with entries ranging from 0 to $n-1$ (instead of the usual 1 to n), and the indexing of the rows and columns also ranges from 0 to $n-1$. Now, add an additional $n \times n$ square S_0 to the system of MOLs, where all the coordinates of the jth column of S_0 are j ($j = 0, \dots, n-1$).

We will now associate to the system $S_0, S_1, \dots S_{n-1}$ a system of vectors in the group $G = \mathbb{Z}_n^n$ (where $\mathbb{Z}_n = \{0, 1, \dots n-1\}$ denotes the cyclic group of order n). As an analogy, we will think of each square S_j as the analogue of an orthonormal basis in the MUB problem, and two such squares S_i, S_j are thought to be "unbiased" to each other. Consider the square S_j ($j = 0, 1, \dots n-1$). We will associate n different vectors to S_j. Let $\mathbf{v_j^k} \in G$ ($k = 0, 1, \dots n-1$) be constructed in the following way: the square S_j contains exactly n entries equal to k – one in each row (this is also true for S_0). Let the mth coordinate ($m = 0, 1, \dots, n-1$) of $\mathbf{v_j^k}$ be the index of the column in which the number k appears in the row of index m of S_j. For example, if the entries k of S_j form the main diagonal of the matrix, then the associated vector is $\mathbf{v_j^k} = (0, 1, 2, \dots, n-1)$.

Applying the definition to S_0 we obtain $\mathbf{v_0^k} = (k, k, \dots, k)$. Also, it is easy to see from the fact that all other squares S_j are Latin squares, that each vector $\mathbf{v_j^k}$ ($j \neq 0$) will be a permutation of the numbers $0, 1, \dots n-1$.

Let us continue with our analogy to the MUB problem. Two vectors from the "same basis" are "orthogonal" to each other: that is, if you take $\mathbf{v_j^k}$ and $\mathbf{v_j^r}$ (coming from the same square S_j), then their difference (coordinate-wise modulo n) will not contain 0 as a coordinate. Indeed, if there was a 0 in $\mathbf{v_j^k} - \mathbf{v_j^r}$ at position m, it would mean that the mth row of S_j contains the numbers k and r in the same positions – clearly nonsense. So, in our analogy, the orthogonality set ORT_n will be given as the set of vectors with no 0 coordinates.

If we take two vectors $\mathbf{v_i^k}$ and $\mathbf{v_j^r}$ from different squares ($i \neq j$), then they must be "unbiased" to each other: that is, their difference will

contain exactly one 0 coordinate. (This is a consequence of the fact that the squares S_j form a complete system of MOLs.) Therefore, our unbiased set UB_n will consist of vectors with exactly one 0 coordinate.

Finally, in the scheme of Delsarte, we ask for the maximal number of vectors in $G = \mathbb{Z}_n^n$ such that each two have a difference either in ORT_n or in UB_n. We can also formulate this in terms of usual coding terminology. We are looking for $A_n(n, n-1)$, where $A_q(n, d)$ denotes the maximal number of codewords made up from a q-element alphabet such that each pair has Hamming distance at least d. Exactly this problem was dealt with in [6], and I wonder what bound we get for $A_6(6, 5)$ with the semi-definite programming method.

Remark 4.6. The Delsarte bound gives exactly the trivial bound n^2, so that at most n^2 vectors in G can exist such that each difference lies in $ORT_n \cup UB_n$ – this means exactly the trivial upper bound $n-1$ on the number of MOLs. (Exercise: find a witness function h.) But again, one can introduce some modification of Delsarte's method exploiting the fact that the prescribed set $ORT_n \cup UB_n$ naturally breaks up into two parts, and try to use this additional information. We have done steps in this direction, but we could not go beyond $n = 6$ due to computational complexity. **Again, it would be interesting to see what upper bounds the extensions of the Delsarte scheme by semi-definite programming give.** It would be quite a challenge to prove the non-existence of projective planes of order 12, for example.

References

[1] C. Bachoc, D. C. Gijswijt, A. Schrijver, F. Vallentin *Invariant semi-definite programs* http://arxiv.org/abs/1007.2905

[2] H. Cohn & N. Elkies, *New upper bounds on sphere packings I.* Ann. of Math. (2) **157** (2003), no. 2, 689–714.

[3] P. Delsarte, *Bounds for unrestricted codes, by linear programming.* Philips Res. Rep. 27 (1972), 272–289.

[4] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski, *On mutually unbiased bases.* International Journal of Quantum Information, Vol. **8**, No. 4 (2010) 535–640

[5] M. Einsiedler, A. Katok, E. Lindenstrauss, *Invariant measures and the set of exceptions to Littlewoods conjecture.* Ann. of Math. 164 (2), (2006), 513-560.

[6] D. C. Gijswijt, *Matrix Algebras and Semidefinite Programming Techniques for Codes.* PhD thesis, http://arxiv.org/abs/1007.0906

[7] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, M. Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6.* J. Physics A: Mathematical and Theoretical, Vol. 42, Number 24, 245305, 2009.

[8] A. Klappenecker & M. Rötteler, *Constructions of Mutually Unbiased Bases.* Finite fields and applications, 137–144, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, 2004.
[9] M. Matolcsi, *A Fourier analytic approach to the problem of mutually unbiased bases.* preprint, http://arxiv.org/abs/1009.2407
[10] M. Matolcsi, I. Ruzsa, *Sets without square differnces.* in preparation
[11] J. Pintz, W.L. Steiger, and E. Szemerdi, *On sets of natural numbers whose difference set contains no squares.* J. London Math. Soc. (2), 37: (1988) 219-231.
[12] I. Z. Ruzsa, *Difference sets without squares.* Period. Math. Hungar. 15 (1984), no. 3, 205–209.
[13] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming.* IEEE Trans. Inform. Theory. Vol. 51, 2859-2866.
[14] P. Wocjan & T. Beth, *New construction of mutually unbiased bases in square dimensions.* Quantum Inf. Comput. **5** (2005), 93-101.
[15] G. Zauner, *Quantendesigns Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, Universität Wien, 1999. (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf)

M. M.: Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary Tel: (+361) 483-8302, Fax: (+361) 483-8333

E-mail address: matomate@renyi.hu