Applications of Semidefinite Programming to Coding Theory

Christine Bachoc
Institut de Mathématiques de Bordeaux
Université Bordeaux 1
351, cours de la Libération, 33405 Talence, France
Email: {christine.bachoc}@math.u-bordeaux1.fr

***Abstract*—We survey recent generalizations and improvements of the linear programming method that involve semidefinite programming. A general framework using group representations and tools from graph theory is provided.**

I. Introduction

The celebrated linear programming method was until recently the most powerful method to obtain estimates for extremal problems in coding theory. Initially developed by Philippe Delsarte in the early seventies in the framework of association schemes [12], it was proved equally suitable for two-point homogeneous spaces [10, Chapter 9]. We recall that a metric space X with distance $d_X(x, y)$ is said to be *two-point homogeneous* if the group of transformations of X preserving d_X, which will be called the automorphism group of X and denoted $\mathrm{Aut}(X)$, acts distance transitively on X^2. The binary Hamming space $H_n = \{0, 1\}^n$ is a core example of these spaces, and the fundamental number $A(n, d)$, the maximal number of elements of a binary code of length n with minimal Hamming distance at least equal to d, can be efficiently upper bounded with Delsarte's method. It has lead not only to numerical bounds, but also to explicit bounds [19], and to the best known asymptotic bounds [22]. Moreover this method has been equally successful for the other two-point homogeneous spaces including real spaces such as the unit sphere of Euclidean space [14], [17].

Despite of these great results, the search for improvements and for generalizations of this method have been fundamental issues in coding theory. In recent years, results in these directions have been obtained using *semidefinite programming* instead of linear programming. Semidefinite programming (SDP for short) is a subfield of convex optimization concerned with the optimization of a linear functional over the intersection of the cone of positive semidefinite matrices with an affine subspace. It contains linear programming (LP) as a special case. It is a field of recent and growing interest because on one hand it goes with efficient algorithms, and on the other hand it is capable of modeling or approximating many optimization problems, in particular in the area of combinatorial optimization.

The first step was taken by A. Schrijver in [26] who, using SDP, was able to improve the known upper bounds for $A(n, d)$ for some parameters (n, d). In [15] these results where extended to the q-Hamming space, and in [16] they are further improved. The idea underlying these results is to exploit constraints involving triples [26], [15], or even quadruples of codewords [16].

Generalizing the linear programming method to other metric spaces (X, d_X) is of special interest in view of the variety of spaces that play a role in recent areas of coding theory, such as codes over rings, network coding, and space time coding. The LP method was successfully generalized to some of these spaces (e.g. the non binary Johnson space [27], permutation codes [28], the Grassmann spaces [1], [24], the ordered codes [21], [7], the unitary codes [11]), essentially because the underlying spaces are *symmetric spaces*. Here we mean that the group of automorphisms exchanges any two elements of the space. However, other spaces do not fit into this framework, such as the projective space over a finite field or a ball in the Hamming space.

One can go from H_n to another metric space (X, d_X) and ask for estimates for the analogous number $A(X, d)$. One can also stick to the Hamming space but consider other types of constraints, such as constraints involving k-tuples of elements instead of pairs. To be more precise, we want to consider on the Hamming space H_n, some functions $f(x_1, \ldots, x_k)$ taking non negative values, defined on k-tuples, that generalize the Hamming distance. Such a function is called a *pseudo-distance* if it satisfies two properties: is is invariant by a permutation of the x_i and it is invariant by the diagonal action of $\mathrm{Aut}(H_n)$. Several such pseudo-distances have been studied in coding theory, for example the *generalized Hamming distance* introduced in [9]. Then, one can ask for $A_{k-1}(n, f, m)$, the maximal number of elements of a binary code C such that $f(x_1, \ldots, x_k)$ is at least equal to some value m when $(x_1, \ldots, x_k)$ runs over the set of k-tuples of pairwise distinct elements of C. It can be noticed that $A_1(n, d, m) = A(n, m)$. We show in [4] that Schrijver's method [26] can be used to derive upper bounds for $A_2(n, f, m)$ and in [5] that it can be generalized to $k \geq 3$.

Our aim in this paper is to give a general framework for the problems discussed above, based on a combination of tools from graph theory, and from the theory of group representations. Indeed, these situations can be interpreted in terms of the *independence number* of specific graphs (or hypergraphs); on the other hand, an upper bound for the

independence number of a graph, which is the optimal value of a SDP, was discovered by L. Lovász [20] who called it the *theta number* of the graph. In order to exploit this upper bound in coding theory, it is necessary to exploit the action of the automorphism group of the underlying space, and this step requires tools from group representations. We shall illustrate these ideas with the cases of projective space, Hamming balls and generalized Hamming distance. In this paper we restrict ourselves to finite spaces, although the ideas and results extend almost straightforwardly to the case of compact spaces (see [6], [3]).

The paper is organized as follows: Section II reviews Delsarte's LP method for binary codes. Section III discusses Lovász theta number of a graph. Section IV introduces semidefinite programs and their symmetrization. Section V links the theta number and the LP bound in the case of binary codes, and introduces the notions relative to a general space X. Section VI gives the necessary results from group representations. Section VII develops applications to codes in Hamming balls and to codes in the projective spaces. Section VIII discusses the applications to pseudo-distances.

II. Delsarte's LP method for binary codes

We take the following notations: for x an element of the binary Hamming space $H_n := \{0,1\}^n$, the *Hamming weight* $\mathrm{wt}(x)$ is the number of its non zero coordinates and the *Hamming distance* of a pair $(x,y) \in H_n^2$ equals $d_H(x,y) = wt(x-y)$. A certain family of orthogonal polynomials, the *Krawtchouk polynomials* $K_k^n(t)$, are naturally attached to the Hamming space, and satisfy the so-called *positivity property*:

$$\text{For all } C \subset H_n, \sum_{(x,y)\in H_n^2} K_k^n(d_H(x,y)) \geq 0. \qquad (1)$$

This property lies at the root of Delsarte LP method. Let us introduce the *distance distribution* $(x_i)_{0\leq i\leq n}$ of a code C:

$$x_i := \frac{1}{|C|}|\{(x,y) \in C^2 \ : \ d_H(x,y) = i\}|.$$

Then, these numbers satisfy the following inequalities:

1) For all $0 \leq k \leq n$, $\sum_{i=0}^n K_k^n(i)x_i \geq 0$.
2) $x_i \geq 0$
3) $x_0 = 1$
4) $\sum_{i=0}^n x_i = |C|$

where 1) rephrases (1). Moreover, if $d_H(C) \geq d$, then $x_i = 0$ for $i = 1, \ldots, d-1$. From these inequalities, one obtains a linear program in real variables y_i, the optimal value of which upper bounds the number $A(n,d)$ [12]:

$$\max\Big\{ \sum_{i=0}^n y_i : \begin{array}{l} y_i \geq 0, \\ y_0 = 1, \\ y_i = 0 \ \text{ if } i = 1, \ldots, d-1 \\ \sum_{i=0}^n K_k^n(i) y_i \geq 0 \quad 0 \leq k \leq n \end{array} \Big\} \qquad (2)$$

In view of generalizations of this method, the role of the Krawtchouk polynomials should be clarified. In fact, these polynomials come into play because they are closely related to the irreducible decomposition of the space $\mathcal{C}(H_n)$ of complex valued functions on H_n:

$$\mathcal{C}(H_n) := \{f : H_n \to \mathbf{C}\}$$

under the action of the group $\mathrm{Aut}(H_n)$ of transformations of H_n preserving the Hamming distance. This group, of order $2^n n!$, combines swaps of 0 and 1 with permutations of the coordinates.

More precisely, if $\chi_z(x) := (-1)^{x\cdot z}$ denote the characters of $(\mathbf{F}_2^n, +)$, we have:

$$\mathcal{C}(H_n) = \oplus_{z\in H_n} \mathbf{C}\chi_z = \oplus_{k=0}^n P_k$$

where $P_k := \oplus_{\mathrm{wt}(z)=k}\mathbf{C}\chi_z$ are $\mathrm{Aut}(H_n)$-irreducible subspaces, and the Krawtchouk polynomials can be defined by

$$K_k^n(d_H(x,y)) := \sum_{\mathrm{wt}(z)=k} \chi_z(x)\chi_z(y)$$

which in turn lead to the explicit expression:

$$K_k^n(t) = \sum_{j=0}^k (-1)^j \binom{t}{j}\binom{n-t}{k-j}.$$

III. Lovász's theta number

Let $\Gamma = (V,E)$ be a finite graph. An *independent set* S of Γ is a subset of V such that no pair of vertices in S is connected by an edge, in other words $S^2 \cap E = \emptyset$. The *independence number* $\alpha(\Gamma)$ is then the maximal number of elements of an independent set.

The number $A(n,d)$ studied in coding theory can be interpreted as the independence number of a particular graph, i.e. the graph $\Gamma(n,d)$ with vertex set $V = H_n$ and edge set $E = \{(x,y) \in H_n^2 : 0 < d_H(x,y) < d\}$. So the methods developed in graph theory in order to estimate the independence number can be applied. It turns out that the exact determination of this graph invariant is a hard problem, but that a relaxation was defined by L. Lovász [20] under the name of the *theta number*, which is computable with polynomial complexity in the size of the graph. More precisely, Lovász theta number $\vartheta(\Gamma)$ is the optimal value of a *semidefinite program*:

$$\vartheta(\Gamma) = \max\big\{ \textstyle\sum_{i,j} B_{i,j} : \begin{array}{l} B = (B_{i,j})_{1\leq i,j\leq v}, \ B \succeq 0 \\ \sum_i B_{i,i} = 1, \\ B_{i,j} = 0 \quad (i,j) \in E \end{array} \big\}$$

where the matrix B is indexed by the vertex set $V = \{1, \ldots, v\}$ and where $B \succeq 0$ stands for: B is a symmetric, positive semidefinite matrix. The celebrated *Sandwich theorem* is proved in [20]:

Theorem 1: If $\chi(\overline{\Gamma})$ denotes the chromatic number of the complementary graph $\overline{\Gamma}$, then

$$\alpha(\Gamma) \leq \vartheta(\Gamma) \leq \chi(\overline{\Gamma}).$$

Proof: We only prove the first inequality. Let S be an independent set and let $\mathbf{1}_S$ denote its characteristic function. The matrix

$$B_{i,j} := \frac{1}{|S|}\mathbf{1}_S(i)\,\mathbf{1}_S(j)$$

is feasible for the program $\vartheta(\Gamma)$ and moreover its optimal value $\sum_{i,j} B_{i,j}$ is equal to $|S|$. So $|S| \leq \vartheta(\Gamma)$. ∎

However, a straightforward application of the inequality $\alpha(\Gamma) \leq \vartheta(\Gamma)$ in the case of binary codes would not be satisfactory because the graph $\Gamma(n,d)$ has 2^n vertices, thus its size grows exponentially with the dimension n. The key to reduce the complexity of the computation of $\vartheta(\Gamma(n,d))$ is to exploit the action of $\mathrm{Aut}(H_n)$ on this graph. In this process, up to a minor modification (i.e. one should consider $\vartheta'(\Gamma(n,d))$, in which the constraint that B takes non negative values is added), $\vartheta'(\Gamma(n,d))$ turn to be equal to Delsarte linear programming bound (see Section V and [25]).

The situation described above is in fact very general. In coding theory, the spaces of interest are always huge spaces, but also have a huge group of automorphisms. Thus symmetry reduction will play a crucial role in the design of upper bounds of ϑ type for extremal problems.

IV. Semidefinite programs

A semidefinite program (SDP for short) is an optimization problem of the form:

$$\gamma := \min\big\{ \quad c_1x_1 + \cdots + c_mx_m : \\ -A_0 + x_1A_1 + \cdots + x_mA_m \succeq 0\big\}$$

where $(c_1,\ldots,c_m) \in \mathbf{R}^m$, $A_0,\ldots,A_m$ are real symmetric matrices, and the minimum is taken over $(x_1,\ldots,x_m) \in \mathbf{R}^m$. Linear programs correspond to the special case of A_i being diagonal matrices. The above *primal program* has an associated *dual program*, defined below, where $\langle A,B\rangle = \mathrm{Trace}(AB^*)$ is the standard inner product of matrices:

$$\gamma^* := \max\big\{\ \langle A_0,Z\rangle : \quad Z \succeq 0, \\ \langle A_i,Z\rangle = c_i, \quad i=1,\ldots,m\big\}.$$

Weak duality, i.e. $\gamma^* \leq \gamma$, always holds. Under some mild conditions, one has also *strong duality*, i.e. $\gamma = \gamma^*$. In this case, *interior point methods* lead to algorithms that allow to approximate γ to an arbitrary precision in polynomial time. Moreover free solvers are available, e.g. on the web site NEOS [23].

Let G be a group of permutations of $\{1,\ldots,r\}$. It acts on matrices of size r by: $(\sigma A)_{i,j} = A_{\sigma^{-1}(i),\sigma^{-1}(j)}$, $\sigma \in G$. The SDP γ^* is said to be *G-invariant* if the matrices A_i are of size r, if the set $\{Z : Z \succeq 0, \langle A_i,Z\rangle = c_i\}$ of feasible solutions is globally invariant by G, and if $\sigma A_0 = A_0$ for all $\sigma \in G$. In this case, if Z is a feasible solution, then another feasible solution Z' with the same optimal value and which is moreover invariant by G is obtained by an average of Z on G, i.e. setting

$$Z' := \frac{1}{|G|}\sum_{\sigma\in G} \sigma Z.$$

This reasoning shows that, if γ^* is G-invariant, one can restrict the feasible solutions to be G-invariant. In other words,

$$\gamma^* = \big(\gamma^*\big)^G := \max\big\{\ \langle A_0,Z\rangle : \quad Z \succeq 0, \\ \sigma Z = Z \text{ for } \sigma \in G, \\ \langle A_i,Z\rangle = c_i\ \big\}.$$

Going from γ^* to $\big(\gamma^*\big)^G$ is referred to as *symmetry reduction* or *symmetrization* of the SDP γ^*.

V. Back to the roots

We come back to $\vartheta'(n,d)$, which is $\mathrm{Aut}(H_n)$-invariant. Its symmetrization involves thus the matrices B indexed by H_n, which are positive semidefinite, and $\mathrm{Aut}(H_n)$-invariant. It turns out that there is a beautiful description of these matrices with help of the Krawtchouk polynomials. We now adopt a functional notation for matrices, i.e. we write $B(x,y)$ instead of $B_{x,y}$.

Theorem 2: $B \in \mathcal{C}(H_n^2)$ is positive semidefinite and G-invariant if and only if

$$B(x,y) = \sum_{k=0}^{d} a_k K_k^n(d_H(x,y)) \quad \text{with } a_k \geq 0,\ 0 \leq k \leq d.$$

This result shows that the condition $B \succeq 0$ can be replaced by the non negativity of the variables a_k. Replacing in ϑ', one obtains a *linear program in the variables* $(a_0,\ldots,a_n)$. With a little bit of transformations, one can show that it is equal to Delsarte linear program.

Now we consider following the same line for a metric space (X,d_X) with group of automorphisms G. With the obvious graph $\Gamma(X,d)$, we have similarly

$$A(X,d) \leq \vartheta'(\Gamma(X,d))^G. \tag{3}$$

Then we need a description of the G-invariant *positive definite functions* $F \in \mathcal{C}(X^2)$, i.e such that the matrix $(F(x,y))_{(x,y)\in X^2}$ is (Hermitian) positive semidefinite. This description can be obtained using *harmonic analysis* of G, and is explained in next section.

VI. Tools from harmonic analysis

We shall be rather sketchy here and refer to [6] for details. In [6], the more general case of compact groups is considered. The space $\mathcal{C}(X)$ is a G-module for the action $(gf)(x) := f(g^{-1}x)$ thus can be decomposed in irreducible submodules. So we have

$$\mathcal{C}(X) = R_0^{m_0} \perp R_1^{m_1} \perp \cdots \perp R_s^{m_s}$$

where the subspaces R_k are pairwise non isomorphic and G-irreducible. Then, for all $k = 0,\ldots,s$, one can define a G-invariant matrix $E_k(x,y)$, of size m_k, associated to the isotypic subspace $R_k^{m_k}$, such that we have:

Theorem 3: $F \in \mathcal{C}(X^2)$ is positive definite and G-invariant, if and only if

$$F(x,y) = \sum_{k=0}^{s} \langle F_k, E_k(x,y)\rangle \quad \text{with } F_k \succeq 0. \tag{4}$$

Moreover, since $E_k(x,y)$ is G-invariant, its coefficients only depend on the orbits $O_G(x,y)$ of pairs $(x,y) \in X^2$ under the action of G, i.e. we have

$$E_k(x,y) = Y_k(O_G(x,y))$$

for some matrix Y_k. It remains to explicitly compute this matrix, which is a non trivial task in general. Special cases will be worked out in the next section. Replacing $F \succeq 0$ by the expression (4) in $\vartheta'(\Gamma(X,d))$ then leads to a semidefinite program in the "variables" $F_k \succeq 0$. Here we can see exactly when this SDP turns to be an LP: since the matrices F_k have size m_k, it corresponds to the cases when $m_k = 1$ for all $0 \leq k \leq s$. One can show that it is so if X is a *symmetric space* as defined in the Introduction.

VII. Bounds for codes in Hamming balls and in Projective geometry

The projective space $X = \mathcal{P}_{q,n}$ over $\mathbf{F}_q$, the set of all linear subspaces of $\mathbf{F}_q^n$, is a metric space for the distance $d_X(x,y) := \dim(x) + \dim(y) - 2\dim(x \cap y)$. Its automorphism group is the group $G = \mathrm{Gl}_n(\mathbf{F}_q)$ of invertible linear transformations. The codes of this space have found recent applications in network coding [18]. Its action on X is not transitive; there are $n+1$ orbits, the subsets X_k of subspaces of fixed dimension k, $0 \leq k \leq n$. The sets X_k themselves are two-point homogeneous, and Delsarte in [13], who calls them *q-Johnson spaces*, has shown that they can be seen as q-analogs of the Johnson spaces, i.e. the sets of binary words with fixed weight. This analogy in fact extends to the pairs (X,G) when X is the full projective space over $\mathbf{F}_q$ and G is the linear group $\mathrm{Gl}_n(\mathbf{F}_q)$, respectively the Hamming space and the symmetric group S_n. We discuss these situations in a uniform way, with the notations of (5).

X	$\mathcal{P}_{q,n}$	H_n
q	p^t	1
G	$\mathrm{Gl}_n(\mathbf{F}_q)$	S_n
$\lvert x\rvert$	$\dim(x)$	$\mathrm{wt}(x)$

(5)

G splits X into the orbits X_k:

$$X_k := \{x \in X : |x| = k\}$$

while the orbits of X^2 are:

$$X_{a,b,c} := \{(x,y) \in X^2 : |x| = a, |y| = b, |x \cap y| = c\}.$$

The distance on these spaces also has a common expression:

$$d_X(x,y) = |x| + |y| - 2|x \cap y|.$$

In [13], the G-decomposition of the spaces $\mathcal{C}(X_k)$ and the associated polynomials are determined (since the spaces are two-point homogeneous, the multiplicities m_k are equal to 1). They belong to the family of *q-Hahn polynomials*. From these results one can go one step further and infer the computation of the matrices Y_k for the space X ([2]):

Theorem 4: The space $\mathcal{C}(X)$ contains $1 + \lfloor n/2 \rfloor$ isotypic subspaces indexed by $0 \leq k \leq \lfloor n/2 \rfloor$, with multiplicities $m_k = n - 2k + 1$, corresponding to irreducible spaces R_k of dimension h_k. The coefficients of the associated matrices $E_k(x,y)$ are explicitly given by the formulas:

$$E_{k,i,j}(x,y) = |X| h_k \frac{\begin{bmatrix} j-k \\ i-k \end{bmatrix} \begin{bmatrix} n-2k \\ j-k \end{bmatrix}}{\begin{bmatrix} n \\ j \end{bmatrix} \begin{bmatrix} j \\ i \end{bmatrix}} q^{k(j-k)} Q_k(n,i,j; i - |x \cap y|)$$

where $k \leq i \leq j \leq n-k$, $|x| = i$, $|y| = j$, $E_{k,i,j}(x,y) = 0$ if $|x| \neq i$ or $|y| \neq j$, and $Q_k(n,i,j;t)$ are q-Hahn polynomials with parameters n, i, j.

As an application, it is possible to derive from (3) upper bounds for $A(J_{q,n}, d)$ and for $A(B_n(w), d)$ where $B_n(w)$ is the Hamming ball of radius w centered at 0:

$$B_n(w) := \{x \in H_n : \mathrm{wt}(x) \leq w\}.$$

Some numerical results are displayed in Table I. The stars indicate optimal bounds, attained by the intersection of the Golay code with $B_n(w)$.

$n \backslash w$	8	9	10	11	12	13	14	15	16
18	67								
19	100	123	137						
20	154	222	253						
21	245	359	465						
22	349	598	759	870	967	990	1023		
23	507	831	1112	1541	1800	1843	1936	2047	
24	760^*	1161	1641	2419	3336^*	3439	3711	3933	4095^*

TABLE I
SDP bounds for $A(B_n(w), 8)$

VIII. Bounds for binary codes related to pseudo-distances

We begin with the introduction of three pseudo-distances that have been studied in coding theory. For $(x_1, \ldots, x_k) \in H_n^k$, the *generalized Hamming distance* $d(x_1, \ldots, x_k)$ is defined by:

$$d(x_1, \ldots, x_k) = |\{j,\ 1 \leq j \leq n :\ x^j \notin \{0^k, 1^k\}\}|.$$

where $x^j := ((x_1)_j, \ldots, (x_k)_j)$ denotes the j-th column of the array:

$$\begin{aligned} x_1 &= 0 \ldots 01 \ldots 1100 \ldots 0 \\ x_2 &= 0 \ldots 01 \ldots 1011 \ldots 0 \\ &\vdots \\ x_k &= 0 \ldots 01 \ldots 1 \underbrace{001 \ldots 1}_{d(x_1,\ldots,x_k)} \end{aligned}$$

This notion was introduced in [9], and takes its origin in the work of Ozarow and Wyner, and of Wei, who studied the generalized Hamming weight of linear codes in view of cryptographic applications. When $k = 2$, $d(x_1, x_2)$ is nothing else than the usual Hamming distance.

The *radial distance* has connections with the notion of list decoding ([8]). The radial distance $r(x_1, \ldots, x_k)$ is by definition the smallest radius of a Hamming ball containing the points $x_1, \ldots, x_k$:

$$r(x_1, \ldots, x_k) = \min_{y \in H_n} \big\{ \max_{1 \leq i \leq k} d(y, x_i) \big\}.$$

Because this parameter is difficult to analyse, it is sometimes studied jointly with the *average radial distance* ([8])

$$\overline{r}(x_1, \ldots, x_k) := \min_y \big\{ \frac{1}{k} \sum_{1 \leq i \leq k} d(y, x_i) \big\}.$$

We want to define an upper bound for the number $A_{k-1}(n, f, m)$ relative to a pseudo-distance f, that resembles Lovász's theta number. In view of the proof of the inequality $\alpha(\Gamma) \leq \vartheta(\Gamma)$ of Theorem 1, it is natural to consider the function

$$\chi_C(z_1, \ldots, z_k) := \frac{1}{|C|} \mathbf{1}_C(z_1) \ldots \mathbf{1}_C(z_k) \qquad (6)$$

associated to a binary code C, and to work out a semidefinite program from its properties. With this line of thought, we obtain in the simplest form:

Theorem 5: [5] The optimal value of the following SDP is an upper bound of $A_{k-1}(n, f, m)$:

$$\max \Big\{ \sum_{(x,y)\in H_n^2} F(x, y) : \quad F : H_n^k \to \mathbf{R}, \\ F \text{ satisfies } (1) - (4) \Big\}$$

where:

(1) $F(z_1, \ldots, z_k) = F(\{z_1, \ldots, z_k\})$
(2) $(x, y) \mapsto F(x, y, z_3, \ldots, z_k) \succeq 0$ and ≥ 0
(3) $F(z_1, \ldots, z_k) = 0$ if $f(z_1, \ldots, z_k) \leq m-1$ and $z_i \neq z_j$
(4) $\sum_{x\in H_n} F(x) = 1$

A slightly stronger condition is used in [5] instead of (2). In order to compute effectively with this program, it is again necessary to reduce it with $\mathrm{Aut}(H_n)$, which amounts to express the $\mathrm{Aut}(H_n)$-invariant functions F satisfying condition (2). This step can be completed with an analysis of the positive definite functions on H_n which are invariant under the stabilizer of $k-2$ elements $(z_3, \ldots, z_k)$. The case $k = 3$ corresponds to the stabilizer of one element, which can be chosen to be the zero word, thus to the group S_n, so this case is contained in Theorem 4. The resulting symmetrized program for $k = 3$ coincides with the program used in [26] (with of course a change in condition (3)). In [4], numerical bounds for $k = 2$ and for the three pseudo-distances defined above are computed and compared to the previous known bounds. It turns out that in almost every case the SDP bound is better. In [5], numerical results are obtained for $k = 4$, i.e. for quadruple functions. However, it seems difficult to consider larger values of k, because the size of the resulting SDP is of order of magnitude $n^{2^{k-1}-1}$.

Remark 6: There is also a graphic view point on Theorem 5. Indeed, the semidefinite program that we have defined, upper bounds the independence number of an hypergraph if H_n is replaced by its vertex set and if condition (3) is replaced by: $F(z_1, \ldots, z_k) = 0$ if $\{z_1, \ldots, z_k\}$ is an hyperedge of the hypergraph.

Remark 7: The semidefinite bound presented in [16], involves functions F defined on the set $\mathcal{S}_k(H_n)$ of subsets of H_n of cardinality at most k. The semidefinite constraints on F are as follows: for all $S \subset \mathcal{S}_k(H_n)$,

$$(X, Y) \mapsto F(X \cup Y) \succeq 0$$

where X, Y run over the elements of $\mathcal{S}_k(H_n)$, containing S, and of size at most $(k + |S|)/2$ (so that $|X \cup Y| \leq k$). The case $|S| = k - 2$ corresponds to condition (2).

The authors obtain with $k = 4$ new upper bounds for $A(n, d)$ for sixteen values of (n, d) in the range $18 \leq n \leq 26$ and $6 \leq d \leq 12$. Remarkably, the new bound in the case $(n, d) = (20, 8)$ reaches the lower bound provided by successive shortening of the Golay code, thus proves $A(20, 8) = 256$.

REFERENCES

[1] C. Bachoc, "Linear programming bounds for codes in Grassmannian spaces", *IEEE Trans. Inf. Theory* vol. 52, no. 5 (2006), pp. 2111–2125.
[2] C. Bachoc and F. Vallentin, "More semidefinite programming bounds", in *Proceeding of DMHF 2007*, Fukuoka, 2007.
[3] C. Bachoc and F. Vallentin, "New upper bounds for kissing numbers from semidefinite programming", *J. Amer. Math. Soc*, vol. 21 (2008), pp. 909–924.
[4] C. Bachoc and G. Zémor, "Bounds for binary codes relative to pseudo-distances of k points", to appear in Adv. Math. Com.
[5] C. Bachoc and C. Riener, in preparation.
[6] C. Bachoc, D. Gijswijt, A. Schrijver and F. Vallentin, "Invariant semidefinite programs", in preparation.
[7] A. Barg and P. Purkayastha, "Bounds on ordered codes and orthogonal arrays", *Moscow Math. Journal* vol. 2 (2009).
[8] V. M. Blinovskii, "Bounds for codes in the case of list decoding of finite volume", *Problems of Information Transmission*, vol. 22, no. 1 (1986), pp. 7–19.
[9] G. Cohen, S. Litsyn and G. Zémor, "Upper bounds on generalized Hamming distances", *IEEE Trans. Inf. Theory*, vol. 40 (1994), 2090-2092.
[10] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*. Springer-Verlag, 1988.
[11] J. Creignou and H. Diet, "Linear programming bounds for unitary codes", em Advances in Math. Com., to appear in Adv. Math. Com.
[12] P. Delsarte, "An algebraic approach to the association schemes of coding theory", *Philips Res. Rep. Suppl.* (1973), vi+97.
[13] P. Delsarte, "Hahn polynomials, discrete harmonics and t-designs", *SIAM J. Appl. Math.*, vol. 34, no. 1 (1978).
[14] P. Delsarte, J.M. Goethals and J.J. Seidel, "Spherical codes and designs", *Geom. Dedicata*, vol. 6 (1977), pp. 363–388.
[15] D.C. Gijswijt, A. Schrijver and H. Tanaka, "New upper bounds for nonbinary codes", *J. Combin. Th. Ser. A*, vol. 13 (2006), pp. 1717–1731.
[16] D.C. Gijswijt, H. Mittelmann and A. Schrijver, "Semidefinite code bounds based on quadruple distances", arXiv:1005.4959
[17] G.A. Kabatiansky and V.I. Levenshtein, "Bounds for packings on a sphere and in space", *Problems of Information Transmission*, vol. 14 (1978), pp. 1–17.
[18] R. Koetter, "Coding for errors and erasures in random network coding", in *Proc. IEEE Int. Symp. Information Theory*, 2007.
[19] V. I. Levenshtein, "Universal bounds for codes and designs", in *Handbook of Coding Theory*, eds V. Pless and W. C. Huffmann, Amsterdam: Elsevier, 1998, pp. 499–648.
[20] L. Lovász, "On the Shannon capacity of a graph", *IEEE Trans. Inform. Theory* vol. 25 (1979), pp. 1-5.
[21] W.J. Martin and D.R. Stinson, "Association schemes for ordered orthogonal arrays and (T, M, S)-nets", *Canad. J. Math.* vol. 51, no. 2 (1999), pp. 326–346.
[22] R. J. McEliece, E. R. Rodemich, H. Rumsey, L. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities", *IEEE Trans. Inf. Theory* vol. 23 (1977), pp. 157–166.
[23] http://www-neos.mcs.anl.gov/
[24] A. Roy, "Bounds for codes and designs in complex subspaces", preprint, arXiv:0806.2317
[25] A. Schrijver, "A comparaison of the Delsarte and Lovász bound", *IEEE Trans. Inform. Theory* vol. 25 (1979), pp. 425–429.
[26] A. Schrijver, "New code upper bounds from the Terwilliger algebra and semidefinite programming", *IEEE Trans. Inf. Theory* vol. 51 (2005), pp. 2859–2866.
[27] H. Tarnanen, M. Aaltonen and J.-M. Goethals, "On the nonbinary Johnson scheme", *Europ. J. Comb.*, vol. 6, no. 3 (1985), pp. 279–285.
[28] H. Tarnanen, "Upper bounds on permutation codes via linear programming", *Europ. J. Comb.*, vol. 20, (1999), pp. 101–114.