Discrete Mathematics 341 (2018) 1740–1748

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Semidefinite bounds for mixed binary/ternary codes☆

Bart Litjens

Korteweg–De Vries Institute for Mathematics, University of Amsterdam, Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 14 July 2017
Accepted 14 March 2018
Available online 1 April 2018

Keywords:
Code
Mixed binary/ternary code
Upper bounds
Semidefinite programming

ABSTRACT

For nonnegative integers n_2, n_3 and d, let $N(n_2, n_3, d)$ denote the maximum cardinality of a code of length $n_2 + n_3$, with n_2 binary coordinates and n_3 ternary coordinates (in this order) and with minimum distance at least d. For a nonnegative integer k, let $\mathcal{C}_k$ denote the collection of codes of cardinality at most k. For $D \in \mathcal{C}_k$, define $S(D) := \{C \in \mathcal{C}_k \mid D \subseteq C, |D| + 2|C \setminus D| \leq k\}$. Then $N(n_2, n_3, d)$ is upper bounded by the maximum value of $\sum_{v\in[2]^{n_2}[3]^{n_3}} x(\{v\})$, where x is a function $\mathcal{C}_k \to \mathbb{R}$ such that $x(\emptyset) = 1$ and $x(C) = 0$ if C has minimum distance less than d, and such that the $S(D) \times S(D)$ matrix $(x(C \cup C'))_{C,C'\in S(D)}$ is positive semidefinite for each $D \in \mathcal{C}_k$. By exploiting symmetry, the semidefinite programming problem for the case $k = 3$ is reduced using representation theory. It yields 135 new upper bounds that are provided in tables.

1. Introduction

Let $\mathbb{Z}_+$ be the set of nonnegative integers, and let $[n] = \{1, \ldots, n\}$, for any $n \in \mathbb{Z}_+$. Let $n_2, n_3 \in \mathbb{Z}_+$ be fixed. Then a *mixed binary/ternary code* is a subset of $[2]^{n_2}[3]^{n_3}$. Mixed codes are of interest because of their application to football pools, see for instance [6]. Whenever $[n]$ consists of the *letters* of an *alphabet* of a code, we take the letters mod n. Since all codes considered in this paper are mixed, i.e., both $n_2 > 0$ and $n_3 > 0$, we will speak of *codes* from now on. An element of a code is called a *codeword* or *word*.

Given two words $v, w \in [2]^{n_2}[3]^{n_3}$, the *Hamming distance* $d_H(v, w)$ between v and w is the number of positions $i \in [n_2 + n_3]$ for which $v_i \neq w_i$. The Hamming distance between a word v and the all-zero word is called the *weight* of v, denoted $w(v)$. For a code C, the *minimum distance* of C is equal to the minimum of $d_H(v, w)$, where we range over distinct $v, w \in C$. Note that with this definition, the empty code and codes of size one do not have a minimum distance. The maximum cardinality of a code with minimum distance at least d is denoted by $N(n_2, n_3, d)$. We will define a hierarchy of upper bounds on $N(n_2, n_3, d)$ that sharpens the linear programming bound defined in [2].

For $k \in \mathbb{Z}_+$, let $\mathcal{C}_k$ denote the collection of codes of cardinality at most k. For $D \in \mathcal{C}_k$, define $S(D) := \{C \in \mathcal{C}_k \mid D \subseteq C, |D| + 2|C \setminus D| \leq k\}$. Note that $|C \cup C'| \leq k$, for $C, C' \in S(D)$. For each function $x : \mathcal{C}_k \to \mathbb{R}$, and for each $D \in \mathcal{C}_k$, define the $S(D) \times S(D)$ matrix $M_D(x) = (x(C \cup C'))_{C,C'\in S(D)}$. Then we define

$$N_k(n_2, n_3, d) := \max_x \sum_{v\in[2]^{n_2}[3]^{n_3}} x(\{v\}), \text{ where } x : \mathcal{C}_k \to \mathbb{R} \text{ satisfies} \tag{1}$$

(i) $x(\emptyset) = 1$,

(ii) $x(C) = 0$ if the minimum distance of C is less than d,

(iii) $M_D(x)$ is positive semidefinite for each $D \in \mathcal{C}_k$.

☆ The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 339109.

E-mail address: b.m.litjens@uva.nl.

https://doi.org/10.1016/j.disc.2018.03.013
0012-365X/

Observe that for a code D of size k, positive semidefiniteness of $M_D(x)$ is equivalent to nonnegativity of $x(D)$. Hence, in (1), we could as well assume that $x : \mathcal{C}_k \to \mathbb{R}_+$.

Proposition 1.1. *For $n_2, n_3, d, k \in \mathbb{Z}_+$, it holds that $N(n_2, n_3, d) \leq N_k(n_2, n_3, d)$.*

Proof. Let $D \subseteq [2]^{n_2}[3]^{n_3}$ be of minimum distance at least d, such that $|D| = N(n_2, n_3, d)$. Define $x : \mathcal{C}_k \to \mathbb{R}$ by $x(C) = 1$ if $C \subseteq D$ and $x(C) = 0$ otherwise. This function clearly satisfies conditions (i) and (ii) of (1). Since $(M_D(x))_{C,C'} = x(C)x(C')$ for all $C, C' \in \mathcal{C}_k$, condition (iii) is also satisfied. Now $\sum_{v \in [2]^{n_2}[3]^{n_3}} x(\{v\}) = |D| = N(n_2, n_3, d)$, and the proposition follows. □

In this paper, we consider $k = 3$. The optimization problem (1) for triples of codewords is very large. However, the problem is highly symmetric and therefore representation theory of the symmetric group can be applied in order to reduce the dimensions to size bounded by a polynomial in n_2 and n_3. This enables us to solve (1) by semidefinite programming for many choices of triples $(n_2, n_3, d) \in \mathbb{N}^3$. We will now describe the ideas of the reduction. The precise details may be found in Section 3.

Let G be the isometry group of $[2]^{n_2}[3]^{n_3}$. That is, G is the group of Hamming distance-preserving bijections from $[2]^{n_2}[3]^{n_3}$ to itself. Then $G = H_2 \times H_3$, where H_2 is the wreath product $S_2^{n_2} \rtimes S_{n_2}$ and H_3 is the wreath product $S_3^{n_3} \rtimes S_{n_3}$. Here, S_m denotes the symmetric group on m letters. For $i = 2, 3$, an element $h \in H_i$ permutes the n_i coordinates and permutes the letters in $[i]$ in every of the n_i positions. The group G acts on $\mathcal{C}_k$ and hence on functions $x : \mathcal{C}_k \to \mathbb{R}$, via $x^\pi(C) := x(\pi^{-1}(C))$, for $\pi \in G$ and $C \in \mathcal{C}_k$. By definition of G, minimum distances of codes are preserved under this action. Let $x : \mathcal{C}_k \to \mathbb{R}$ be a function satisfying the conditions and maximizing the objective function of (1). For $\pi \in G$, the function x^π again satisfies conditions (i) and (ii) of (1). Condition (iii) is met as well, as the matrix $M_D(x^\pi)$ is obtained from $M_D(x)$ by simultaneously permuting rows and columns. Since π is a bijection of $[2]^{n_2}[3]^{n_3}$, the objective function does not change when replacing x by x^π. Averaging over the group G yields a G-invariant function y, for which the matrices $M_D(y)$ are positive semidefinite by convexity of the set of positive semidefinite matrices. This shows that the optimal function x can be taken to be G-invariant.

Let Ω be the set of orbits of $\mathcal{C}_k$ under the action of G. Since a G-invariant function y is constant on orbits, for each $D \in \mathcal{C}_k$ the matrix $M_D(y)$ can be written in terms of variables $y(w)$, with $w \in \Omega$. Let G_D be the subgroup of G that leaves D invariant. Then $M_D(y)$ is invariant under the induced action of G_D on its rows and columns. Therefore, it admits a block-diagonalization $M_D(y) \mapsto U^T M_D(y) U$, where U is a matrix independent of y (see Eq. (3)). The matrix $M_D(y)$ is positive semidefinite if and only if each of the blocks is. This accounts for a large reduction as the blocks have far less entries than the original matrix, and the same block occurs repeatedly.

For $D \in \mathcal{C}_k$ and $\pi \in G$, the matrix $M_D(y)$ differs from $M_{\pi(D)}(y)$ by a permutation matrix. Hence, positive semidefiniteness of $M_D(y)$ needs only be checked for one element D out of each G-orbit of $\mathcal{C}_k$. Throwing away equivalent blocks, we are left with blocks whose entries are linear functions in the variables $y(w)$. The number of variables is bounded by a polynomial in n_2 and n_3, see Section 4.1.

The blocks as well as some further reductions of the optimization problem will be described in Section 3. The entries of the matrices are computed in Section 4. Table 1 at the end of the article shows the improvements that were found using the multiple precision versions of the semidefinite programming algorithm SDPA, with thanks to SURFsara (www.surfsara.nl) for the support in using the LISA Compute Cluster.

Several previously best known upper bounds were obtained via linear programming and extra constraints in [2] by Brouwer, Hämäläinen, Östergård and Sloane. For $d = 3$ and $d = 4$, improvements were found by Östergård using backtrack search in [9] and [8] respectively. The tables in [1], maintained by Andries Brouwer, contain all known bounds on the size of binary/ternary error-correcting codes.

1.1. Comparison with earlier bounds

The above described method is an adaption of the one in [7] and builds upon the work of Gijswijt, Mittelmann, Schrijver and Tanaka in [4,5,11]. Proposition 1.1 generalizes Proposition 1 of [7] for the binary and ternary case. In fact, for fixed $t \in \mathbb{Z}_+$ and distinct $p_1, \ldots, p_t \in \mathbb{N}$, the statement in Proposition 1.1 can be generalized to the case of mixed codes of length $n_1 + \cdots + n_t$, with n_i coordinates chosen from an alphabet with p_i letters, for $i = 1, \ldots, t$.

The method described in the previous section (with $k = 3$) fits into the second level of the Lasserre hierarchy for stable sets. It can be proved that for $k = 2$, Proposition 1.1 reduces to the pure linear programming bound described in Section 2 of [2].

Theoretically, our method could be extended to $k \geq 4$. However, the number of variables involved in the semidefinite program grows rapidly when going from $k = 3$ to $k = 4$. In practice, for $k = 4$ only one case could be made tractable. Furthermore, the instances in the tables in [1] where the value $N(n_2, n_3, d)$ is yet unsettled, typically involve codes for which the length $n_2 + n_3$ is large compared to the distance d. This amounts to many and large constraint matrices.

2. Preliminaries on representation theory

In this section some background information on group actions and representation theory of finite groups is given. It mostly concerns representation theory of the symmetric group. Proofs and details of the statements given are omitted. For