Discrete Mathematics 311 (2011) 2283–2294

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

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

The triple distribution of codes and ordered codes

Horst Trinker *

Department of Mathematics, University of Salzburg, Hellbrunnerstr. 34, 5020 Salzburg, Austria

ARTICLE INFO

Article history:
Received 26 April 2010
Received in revised form 13 April 2011
Accepted 23 June 2011
Available online 5 August 2011

Keywords:
Codes
Linear codes
Triple distribution
Semidefinite programming bound
MacWilliams identity for the triple distribution
Linear programming bound

ABSTRACT

We study the distribution of triples of codewords of codes and ordered codes. Schrijver [A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (8) (2005) 2859–2866] used the triple distribution of a code to establish a bound on the number of codewords based on semidefinite programming. In the first part of this work, we generalize this approach for ordered codes. In the second part, we consider linear codes and linear ordered codes and present a MacWilliams-type identity for the triple distribution of their dual code. Based on the non-negativity of this linear transform, we establish a linear programming bound and conclude with a table of parameters for which this bound yields better results than the standard linear programming bound.

1. Introduction

We consider error-correcting block codes in Hamming space (we refer to [10] for an introduction) and a generalization, ordered codes, which were introduced by Rosenbloom and Tsfasman as "codes for the m-metric" in [14]. Let the set A be an alphabet with $|A| = q \geq 2$ elements. Typically we will use $A = \mathbb{Z}_q$, the set of integers modulo $q \geq 2$, or $A = \mathbb{F}_q$, the Galois field of order q. An ordered code C of length s and depth l over the alphabet A is a subset of $(A^l)^s$.

For "blocks" $u = (u_1, \ldots, u_l)$, $v = (v_1, \ldots, v_l) \in A^l$, we define their ordered distance to be $h(u, v) := \max\{1 \leq i \leq l : u_i \neq v_i\}$, where $\max \emptyset := 0$. Based thereupon, the type distance $d(x, y) := e$ of $x = (x_1, \ldots, x_s), y = (y_1, \ldots, y_s) \in (A^l)^s$ is defined to be the tuple $e = (e_0, e_1, \ldots, e_l) \in \mathbb{N}_0^{\{0,\ldots,l\}}$, where $e_\nu := |\{1 \leq i \leq s : h(x_i, y_i) = \nu\}|$ counts the number of blocks at ordered distance ν. Clearly, for depth $l = 1$, the type distance is equivalent to the Hamming distance and we have the case of codes in Hamming space.

The set of all possible types, i.e. all elements of $\mathbb{N}_0^{\{0,\ldots,l\}}$ that sum up to s, will be denoted by $T^{s,l}$, and the type distribution of C is meant to be the tuple $(\alpha_e) \in \mathbb{Q}^{T^{s,l}}$, where $\alpha_e := \frac{1}{|C|}\left|\left\{(x, y) \in C^2 : d(x, y) = e\right\}\right|$. By $\mathrm{si}(e) = \sum_{i=1}^{l} ie_i$ and $\mathrm{br}(e) = \sum_{i=1}^{l} e_i$, we will refer to the size and breadth of a type e, respectively. The largest $d \in \{1, \ldots, sl + 1\}$ such that $\alpha_e = 0$ for all types with $1 \leq \mathrm{si}(e) \leq d - 1$ is called the minimum distance of the code. A fundamental problem of coding theory is to determine the maximum number $|C|$ of possible codewords given a minimum distance d. Considering the Bose–Mesner algebra of the Hamming association scheme and the type distribution of a code (for $l = 1$), Delsarte [4] establishes one of the strongest general bounds on the number of codewords using linear programming (LP). Martin and Stinson [11] use Delsarte's approach to extend this bound for ordered codes. These generalized codes are of interest especially in the context of quasi-Monte Carlo methods, as the duality of codes and orthogonal arrays (cf. [9]) extends to a duality of ordered codes and (t, m, s)-nets, which are low discrepancy point sets in the s-dimensional unit cube [12,13].

* Tel.: +43 662 8044 5329; fax: +43 662 8044 137.
E-mail address: horst.trinker@sbg.ac.at.

0012-365X
doi:10.1016/j.disc.2011.06.028

Schrijver [15] focuses his attention to the distribution of triples of codewords of a binary code and uses it to establish a bound based on semidefinite programming (SDP) which strengthens the LP bound.

In order to establish the general framework of a triple distribution for ordered codes, we start by defining the ordered distance of the blocks $u, v, w \in A^l$ to be the triple $h(u, v, w) := (h(u, v), h(u, w), h(v, w)) \in R_{q,l}$, where obviously

$$R_{q,l} := \left\{(r_1, r_2, r_3) \in \{0, 1, \ldots, l\}^3 : |\{1 \le i \le 3 : \max\{r_1, r_2, r_3\} = r_i\}| \ge 2\right\}$$

for $q \ge 3$ and $R_{2,l} := R_{3,l} \setminus \bigcup_{t=1}^{l}\{(t, t, t)\}$. The "triple distance" $d(x, y, z) := \delta$ of $x, y, z \in (A^l)^s$ is the tuple $\delta \in \mathbb{N}_0^{R_{q,l}}$ with

$$\delta_{(r_1,r_2,r_3)} := |\{1 \le i \le s : h(x_i, y_i, z_i) = (r_1, r_2, r_3)\}|$$

for all $(r_1, r_2, r_3) \in R_{q,l}$. Clearly, $\sum_{(r_1,r_2,r_3)\in R_{q,l}} \delta_{(r_1,r_2,r_3)} = s$. We denote the set of all tuples in $\mathbb{N}_0^{R_{q,l}}$ that sum up to s by $I(q, s, l)$ and define the "triple distribution" of C to be the tuple $(\beta_\delta) \in \mathbb{Q}^{I(q,s,l)}$, where $\beta_\delta := \frac{1}{|C|}\left|\left\{(x, y, z) \in C^3 : d(x, y, z) = \delta\right\}\right|$. As

$$|R_{q,l}| = \begin{cases} \dfrac{l}{2}(3l+5)+1 & \text{for } q \ge 3, \\ \dfrac{3}{2}l(l+1)+1 & \text{for } q = 2, \end{cases} \tag{1}$$

and $|I(q, s, l)| = \left|\left\{(n_1, \ldots, n_{|R_{q,l}|-1}) \in \mathbb{N}_0^{|R_{q,l}|-1} : n_1 + \cdots + n_{|R_{q,l}|-1} \le s\right\}\right|$, we have

$$|I(q, s, l)| = \begin{cases} \binom{s + \frac{l}{2}(3l+5)}{\frac{l}{2}(3l+5)} & \text{for } q \ge 3, \\ \binom{s + \frac{3}{2}l(l+1)}{\frac{3}{2}l(l+1)} & \text{for } q = 2. \end{cases}$$

Before considering the triple distribution of a code more closely which leads to the desired generalization of the SDP bound for ordered codes (Section 3) as well as a new LP bound (Section 6), we study the symmetry groups of the above defined distances in the next section.

2. The symmetry group of the type distance

Let the alphabet $A = \mathbb{Z}_q$ be given. We define $\mathrm{Aut}((\mathbb{Z}_q^l)^s)$ to be the symmetry group of the type distance, i.e. the set of all permutations φ of $(\mathbb{Z}_q^l)^s$ with $d(\varphi(x), \varphi(y)) = d(x, y)$ for all $x, y \in (\mathbb{Z}_q^l)^s$. By $\mathrm{Aut}_{\mathbf{0}}((\mathbb{Z}_q^l)^s) := \{\sigma \in \mathrm{Aut}((\mathbb{Z}_q^l)^s) : \sigma(\mathbf{0}) = \mathbf{0}\}$ we refer to its subgroup fixing $\mathbf{0} := ((0, \ldots, 0), \ldots, (0, \ldots, 0)) \in (\mathbb{Z}_q^l)^s$.

We start by considering $\mathrm{Aut}((\mathbb{Z}_q^l)^1) = \mathrm{Aut}(\mathbb{Z}_q^l)$, canonically identifying $(\mathbb{Z}_q^l)^1$ with $\mathbb{Z}_q^l$. We define

$$F_{u_1,\ldots,u_t} := \{v = (v_1, \ldots, v_l) \in \mathbb{Z}_q^l : v_{l+1-k} = u_k \text{ for all } 1 \le k \le t\}.$$

If $\rho \in \mathrm{Aut}(\mathbb{Z}_q^l)$, then ρ permutes the $(F_{u_1})_{u_1\in\mathbb{Z}_q}$, so there is a permutation α of $\mathbb{Z}_q$ such that $\rho(F_{u_1}) = F_{\alpha(u_1)}$ for all $u_1 \in \mathbb{Z}_q$. Next the $(F_{u_1,u_2})_{u_2\in\mathbb{Z}_q}$ must be mapped bijectively onto the $(F_{\alpha(u_1),u_2})_{u_2\in\mathbb{Z}_q}$ for every $u_1 \in \mathbb{Z}_q$. So there are permutations $(\alpha_{u_1})_{u_1\in\mathbb{Z}_q}$ of $\mathbb{Z}_q$ such that $\rho(F_{u_1,u_2}) = F_{\alpha(u_1),\alpha_{u_1}(u_2)}$. Continuing in his fashion we finally arrive at

$$\rho(F_{u_1,u_2,\ldots,u_l}) = F_{\alpha(u_1),\alpha_{u_1}(u_2),\ldots,\alpha_{u_1,\ldots,u_{l-1}}(u_l)}.$$

On the other hand, if $\alpha, (\alpha_{u_1})_{u_1\in\mathbb{Z}_q}, \ldots, (\alpha_{u_1,\ldots,u_{l-1}})_{u_1,\ldots,u_{l-1}\in\mathbb{Z}_q}$ are given permutations of $\mathbb{Z}_q$, then the mapping ρ defined by

$$\rho(u_l, \ldots, u_2, u_1) := (\alpha_{u_1,\ldots,u_{l-1}}(u_l), \ldots, \alpha_{u_1}(u_2), \alpha(u_1))$$

clearly is in $\mathrm{Aut}(\mathbb{Z}_q^l)$. We have seen the following

Proposition 2.1. *In terms of the wreath product,*

$$\mathrm{Aut}(\mathbb{Z}_q^l) = S_q^1 \wr \cdots \wr S_q^l,$$

where $S_q^1 = \cdots = S_q^l$ denotes the symmetric group on $\mathbb{Z}_q$. In particular,

$$|\mathrm{Aut}(\mathbb{Z}_q^l)| = (q!)^{\frac{q^l-1}{q-1}}.$$