New Upper Bounds for the Size of Permutation Codes via Linear Programming

Mathieu Bogaerts

Université Libre de Bruxelles
Service de Mathématiques, Faculté des Sciences Appliquées
CP 165/11 avenue Roosevelt 50
B-1050 Brussels, Belgium

mbogaert@ulb.ac.be

Submitted: Jan 2, 2010; Accepted: Sep 30, 2010; Published: Oct 15, 2010
Mathematics Subject Classification: 05B15

Abstract

An (n, d)-permutation code of size s is a subset C of S_n with s elements such that the Hamming distance d_H between any two distinct elements of C is at least equal to d. In this paper, we give new upper bounds for the maximal size $\mu(n, d)$ of an (n, d)-permutation code of degree n with $11 \leqslant n \leqslant 14$. In order to obtain these bounds, we use the structure of association scheme of the permutation group S_n and the irreducible characters of S_n. The upper bounds for $\mu(n, d)$ are determined solving an optimization problem with linear inequalities.

1 Permutation arrays and permutation codes

An (n, d)-*permutation code* of distance d, size s and degree n is a non-empty subset C of the symmetric group S_n acting on the set $\{1, \ldots, n\}$ such that the Hamming distance between any two distinct elements of C is at least equal to d. The *Hamming distance* between two permutations $\phi, \psi \in S_n$ is defined as $d_H(\phi, \psi) = |\{i \in \{1, \ldots, n\} : \phi(i) \neq \psi(i)\}|$.
The *weight* of a permutation $\phi \in S_n$ if the number of non fixed points of ϕ.
The $s \times n$ array A associated to a (n, d)-permutation code $C = \{\phi_1, \ldots, \phi_s\}$ of size s by $A_{ij} = \phi_i(j)$ has the following properties: every symbol 1 to n occurs exactly in one cell of any row and any two rows disagree in at least d columns. Such an array is called a *permutation array* (PA) of distance d, size s and degree n.
Permutation codes have first been proposed by Ian Blake in 1974 as error-correcting codes for powerline communications [3]. This application motivates the study of the largest possible size that a permutation code can have. Upper bounds for the maximal size $\mu(n, d)$ of a permutation code with fixed parameters n and d have been studied by

many authors, see e.g. Deza and Frankl [10], Cameron [6], and more intensively since Chu, Colbourn and Dukes [8], Tarnanen [15], and Han Vinck [2, 16]. An $(n,d)-$ *permutation code* C *of weight* w is an $(n,d)-$ permutation code such that all permutations have weight w. The maximal size of such a permutation code is denoted by $\mu(n,d,w)$.
An (n,d)-permutation code C of size s is *maximal* if C is not contained in an (n,d)-permutation code of larger size $s' > s$. Note that an (n,d)-permutation code reaching the maximal size $\mu(n,d)$ is necessarily maximal while the converse is not true. The most basic upper bounds on $\mu(n,d)$ appears in Deza and Frankl [10]:

Theorem 1. *For* $n \geqslant 3$ *and* $d \leqslant n$,

$$\mu(n,d) \leqslant n\ \mu(n-1,d)$$

and therefore

$$\mu(n,d) \leqslant \frac{n!}{(d-1)!}$$

In this paper, we will establish new bounds for $\mu(n,d)$ for small values of the parameters n and d. In [15], H. Tarnanen uses the conjugacy scheme of the group S_n in order to obtain new upper bounds for the size of a permutation code. We use this method to obtain new upper bounds for $\mu(n,d)$.

2 Isometries

A distance D on S_n is called *left-invariant* (resp. *right-invariant*) if $D(\phi,\psi) = D(\alpha\phi,\alpha\psi)$ (resp. $D(\phi,\psi) = D(\phi\alpha,\psi\alpha)$) for all $\alpha,\phi,\psi \in S_n$. A distance that is both left- and right-invariant is said to be *bi-invariant*. For any bi-invariant distance, the left multiplications $l_\alpha : \phi \mapsto \alpha\phi$ and the right multiplications $r_\alpha : \phi \mapsto \phi\alpha^{-1}$ are isometries. As noticed by Deza and Huang [11], any bi-invariant distance is invertible: $D(\phi,\psi) = D(\phi^{-1},\psi^{-1})$, or equivalently, the inversion i, mapping each permutation onto its inverse, is an isometry. Let $\mathcal{R}$ (resp. $\mathcal{L}$) denote the group of all right (resp. left-) multiplications and $\mathcal{I}$ denote the group generated by the inversion i. We will say that the distance D *distinguishes the transpositions* if there exists a constant c such that $D(\phi,\psi) = c \Leftrightarrow \phi\psi^{-1}$ is a transposition. In 1960, Farahat characterized the *isometry group* $Iso(n)$ of the metric space (S_n, d_H) [12]. Since the Hamming distance is bi-invariant and distinguishes the transpositions, the following result appears in [4] and generalizes the characterisation given by Farahat:

Theorem 2. *Let* D *be a bi-invariant distance distinguishing the transpositions on* S_n $(n \geqslant 3)$*, then the group* Iso_D *of isometries of* (S_n, D) *is* $(\mathcal{L}\times\mathcal{R}) \rtimes \mathcal{I}$*, isomorphic to* $S_n \wr 2$.

Every isometry $t \in Iso(n)$ can be uniquely written as $l_\alpha r_\beta i^k$ with $k = 0$ or 1, $\alpha,\beta \in S_n$. The action of a left multiplication l_α on a given code corresponds to the permutation under α of the symbols appearing in the PA associated to the code, and the action of a right-multiplication r_β is equivalent to the permutation under β of the columns of the PA. In other words, classifying permutation codes up to isometry is equivalent to classifying PA's up to permutation of their rows, their columns, their symbols and up to the inversion. It immediately follows from this theorem that the autormorphism group of the conjugacy scheme of S_n is precisely the isometry group of the metric space (S_n, d_H).

3 Linear programming bound

A *symmetric association scheme with m classes* is a finite set X with $m+1$ relations $R_0, R_1, \dots R_m$ on X such that:

- $\{R_0, R_1, \dots R_m\}$ is a partition of $X \times X$
- $R_0 = \{(x,x) | x \in X\}$
- If $(x,y) \in R_i$, then $(y,x) \in R_i$ for all $x, y \in X$ and for all $i = 0, \dots, m$
- For each pair $(x,y) \in R_k$, the number p_{ij}^k of elements $z \in X$ such that $(x,z) \in R_i$ and $(y,z) \in R_j$ only depends on i, j and k

The numbers p_{ij}^k are called *intersection numbers* of the association scheme. Let n denote the size of the set X and $n_i := p_{ii}^0 \quad i = 0, \dots, m$. The intersection matrices $L_0, \dots, L_m$ are defined by: $(L_i)_{jk} = p_{ij}^k$. The relations R_i can be described by their adjacency matrix A_i: The *adjacency matrix* A_i of the relation R_i is the $n \times n$-matrix such that:

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } (x,y) \in R_i \\ 0 & \text{otherwise} \end{cases}$$

In terms of adjacency matrices the conditions defining the association scheme become:

- $\displaystyle\sum_{i=0}^{m} A_i = J$ where J is the full one matrix, i.e. $J_{ij} = 1$ for all i, j.
- $A_0 = I$ where I is the identity matrix,
- $A_i = A_i^T$ for all $i \in \{0, \dots, m\}$
- $A_i A_j = \displaystyle\sum_{k=0}^{m} p_{ij}^k A_k$ for all $i, j \in \{0, \dots, m\}$

The adjacency matrices commute and generate the commutative Bose Mesner algebra $\mathcal{A}$ of dimension $m+1$. The algebra $\mathcal{A}$ has a basis $E_0, \dots, E_m$ such that:

1. $E_i E_j = \delta_{ij} E_i$
2. $\displaystyle\sum_{i=0}^{m} E_i = I$

The matrix E_0 can be taken as to be $\frac{J}{n}$ where J is the full one matrix, i.e. $J_{ij} = 1$ for all i, j. Let P and $\frac{1}{n}Q$ be the basis transition matrices in $\mathcal{A}$:

$$A_j = \sum_{i=0}^{m} P_{ij} E_j$$

$$E_j = \frac{1}{n} \sum_{i=0}^{m} Q_{ij} A_j$$

We then obtain $PQ = QP = nI$ and $A_j E_i = P_{ij} E_i$ The numbers P_{ij} are the eigenvalues of A_j with the columns of E_i as corresponding eigenvectors.
Let Y be a subset of X and denote by χ the characteristic vector of Y: $\chi_i = 1$ if $i \in Y$ and $\chi_i = 0$ if $i \notin Y$. The inner distribution of a subset Y of an association scheme is the vector

$$\bar{a} = (a_0, \dots a_m)$$

where $a_i = \frac{1}{|Y|} \chi^T A_i \chi$. It is obvious that $a_0 = 1$ (because $A_0 = I$) and $\sum_{i=0}^{m} a_i = |Y|$. For all $i = 0, \dots, m$, a_i corresponds to the number of ordered pairs $(x, y) \in Y \times$ such that $(x, y) \in R_i$, divided by $|Y|$.

Theorem 3 (Delsarte [9],Th. 3.3, p. 26)**.** *The inner distribution $\bar{a}$ of a non empty set Y of an association scheme satisfies $\bar{a}Q \geqslant 0$.*

Let Y be a subset of an association scheme such that $\forall x, y \in Y, (x, y) \notin R_i$ for all $i \in \{1, \dots \delta - 1\}$, or equivalently $(x, y) \in R_i \Rightarrow i = 0$ or $\delta \leqslant i \leqslant m$. The inner distribution vector $\bar{a}$ of Y satisfies:

$$\begin{cases} a_0 = 1 \\ \\ a_k = 0 \text{ if } 1 \leqslant k \leqslant \delta - 1 \\ a_k \geqslant 0 \text{ if } \delta \leqslant k \leqslant m \\ \bar{a}Q \geqslant 0 \\ a_0 + \sum_{i=\delta}^{m} a_i = |Y| \end{cases}$$

Theorem 4 (Delsarte [9], Th. 3.8,p.31)**.**

Consider $a_\delta, \dots, a_m$ as real variables and define $a^* = 1 + \sum_{i=\delta}^{m} a_i$ as the maximal value of this sum such that

$$\begin{cases} Q_{1j} + \sum_{i=\delta}^{m} a_i Q_{ij} \geqslant 0 \quad j = 0, \dots, m \\ a_i \geqslant 0, \quad i = \delta, \dots, m \end{cases}$$

Then $|Y| \leqslant a^*$.

4 Conjugacy scheme

Any group G defines a symmetric association scheme on its elements with relations defined by the conjugacy classes C_i of G for $\phi, \psi \in G$, $(\phi, \psi) \in R_i \Leftrightarrow \phi\psi^{-1} \in C_i$. For $G = S_n$, denote by $p(n)$ the number of conjugacy classes of G.
Let $\chi_0, \dots, \chi_m$ be the irreducible characters of S_n , indexed in such a manner that $\chi_0(\alpha) = 1 \quad \forall \alpha \in S_n$. There are $p(n) = m+1$ irreducible characters, where $p(n)$ is the number of conjugacy classes of S_n. Recall that the values of χ_k are integers, that the functions χ_k are constant on each conjugacy class and that $\displaystyle\sum_{k=0}^{m} \chi_k^2(Id) = n!$. The irreducible characters form an orthonormal basis of the set $Cf(S_n)$ of class functions of S_n, for the product $< \cdot, \cdot >_n$: $Cf^2(S_n) \to \mathbb{R}$ defined by

$$< f, g >_n = \sum_{\alpha \in S_n} \frac{f(\alpha)g(\alpha)}{n!}$$

Theorem 5 (Tarnanen, [15])**.** *For the conjugacy scheme $(S_n, R_0, \dots, R_m)$, the transition coefficents Q_{ij} are given by:*

$$Q_{ij} = \chi_j(Id).\chi_j(C_i)$$

Every $(n, d)-$permutation code C is a subset of the conjugacy scheme. Suppose that the permutations of S_n are indexed $\phi_1, \dots, \phi_{n!}$. To avoid confusion, we will denote by ξ_C the caracteristic vector of the code C, defined as $(\xi_C)_i = 1$ if $\phi_i \in C$ and $(\xi_C)_i = 0$ otherwise. For any (n, d)-permutation code C, the numbers $a_i = \xi_C A_i \xi_C^T$ are invariant under the action of $Iso(n)$ (see [4] for more information on invariants).

Theorem 6 (LP bound for permutation codes (Tarnanen,[15]))**.** *Let D be a subset of $\{1, \dots, m\}$ and E any subset of S_n such that for any distinct permutations ϕ, ψ, $(\phi, \psi) \in R_i$ with $i \in D$*

Considering $a_k, \quad k \in D$ as real variables and denoting by a^* the number $1 + \sum_{i \in D} a_i$, the maximal value of this sum with

$$\begin{cases} \chi_j(C_0) + \displaystyle\sum_{i \in D} a_i \chi_j(C_k) \geqslant 0 & \forall j \in \{0, \dots, m\} \\ a_i \geqslant 0, \quad i \in D \end{cases}$$

Then $|E| \leqslant a^*$.

If D is a subset of indices of conjugacy classes whose elements have less than $n - d$ fixed points, this bound provides an upper bound for the size of a permutation code of distance d. The permutation characters of S_n are available on programs as Magma [5] or GAP [13]. Using the "linprog" routine of Matlab [14], we obtain the bounds in Table 1. Note that the linear programming provides the values of the coefficients a_i, considered as real variables. On the other hand, if there exists an $(n, d)-$ permutation code C whose size reaches the upper bound a^* then the the numbers $b_i = a_i a^* = \xi_C^T A_i \xi_C$ are integers.

The linear inequalities in theorem 6 lead to the following check routine of the feasability of the upper bound a^*. Let $d \leqslant n$ be fixed, and suppose that a^* is the value obtained by linear programming bound of Theorem 6. Then consider $b_k, \quad k \in D$ as integer variables and denote by b^* the maximal value $1 + max \sum_{i \in D} b_i$, with

$$\begin{cases} a^* \chi_j(C_0) + \sum_{i \in D} b_i \chi_j(C_i) \geqslant 0 & \forall j \in \{0, \dots, m\} \\ b_i \geqslant 0, \quad i \in D \end{cases}$$

Then the bound a^* is feasable if $b^* = a^{*2}$. The integer linear programming problem above can be solved using appropriate matlab routine [14].

	LP bound	Previous known bound
$\mu(13,4)$	367270674	479001600
$\mu(11,5)$	362880	712800
$\mu(12,5)$	6141046	7149277
$\mu(13,5)$	75789398	78823048
$\mu(11,6)$	138600	273402
$\mu(12,6)$	1766160	3926242
$\mu(13,6)$	21621600	29511947
$\mu(11,7)$	32874	55440
$\mu(12,7)$	361396	665280
$\mu(13,7)$	4163390	8648640
$\mu(13,8)$	879493	1235520

Table 1: LP bound for $11 \leqslant n \leqslant 13$

Applying theorem 1 to the results of Table 1, we obtain recursive consequences. This leads to the upper bounds appearing in Table 2. The previous known bounds are due to Deza and Frankl [10].

As noticed by H. Tarnanen [15], many of the upper bounds obtained by linear programming coincide with the bound $\mu(n,d) \leqslant \frac{n!}{(d-1)!}$ of theorem 1. For $14 \leqslant n \leqslant 16$, computations of the LP bound give $\frac{n!}{(d-1)!} \leqslant a^*$ for all $d \leqslant n$. In order to obtain sharper upper bounds, other linear constraints on the coefficents a_i must be considered. The following theorem motivates the study of permutation arrays of given weight.

Theorem 7. *Let C be an $(n,d)-$ permutation code and $a_i = \frac{1}{|C|} \xi_C^T A_i \xi_C$. Let $D = \{i_1, \dots, i_k\}$ be the set of indices of the conjugacy classes whose elements have $n - w$ fixed points. Then*

$$\sum_{i \in D} a_i \leqslant \mu(n,d,w)$$

$\mu(n,d)$	$n\mu(n-1,d)$	Previous known bound
$\mu(11,4)$	3326400	3628800
$\mu(12,4)$	39916800	39916800
$\mu(12,5)$	4354560	7149277
$\mu(13,5)$	56609280	78823048
$\mu(14,5)$	792529920	947590121
$\mu(12,6)$	1663200	3926242
$\mu(13,6)$	21621600	29511947
$\mu(14,6)$	302702400	351525367
$\mu(14,7)$	58287460	106314989
$\mu(14,8)$	12312902	17297280

Table 2: Upper bounds for $\mu(n,d)$ obtained by $\mu(n,d) \leqslant n\mu(n-1,d)$

Proof. For each i, $a_i|C|$ counts the number of pairs of permutations (ϕ,ψ) with $\phi,\psi \in C$ and $\phi\psi^{-1} \in C_i$, or, equivalently, the sum for $\phi \in C$ of the number of permutations $\psi \in C$ such that $\phi\psi^{-1} \in C_i$. The conjugacy classes are disjoint so we can write $|C|\sum_{i\in D} a_i = \sum_{\phi\in C} |\{\psi \in C : \phi\psi^{-1} \in \cup_{i\in D} C_i\}|$. For each $\phi \in C$, the set $r_\phi(\{\psi \in C : \phi\psi^{-1} \in \cup_{i\in D} C_i\})$ is composed of permutations of weight w, so $|C|\sum_{i\in D} a_i = \sum_{\phi\in C} \mu(n,d,w)$, and this concludes the proof. □

Denote by $A(n,d,w)$ the maximum possible size of a constant weight w binary code of length n and distance d. Properties and known values of $A(n,d,w)$ for small values of the parameters can be found in [1]. In [17], Yang, Dong and Chen stated properties of $\mu(n,d,w)$ for $w \leqslant d$.

Theorem 8. *Yang, Dong and Chen[17]*

(i) $\mu(n,d,w) \leqslant A(n,2d-2w,w)$ *for* $w < d$

(ii) $\mu(n,d,w) = 1$ *for* $2w < d$, $w \neq 1$

(iii) $\mu(n,2k,k) = \lfloor \frac{n}{k} \rfloor$ *for* $2 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$

(iv) $\mu(n,2k+1,k+1) = A(n,2k,k+1)$ *for* $1 \leqslant k \leqslant \lfloor \frac{n-1}{2} \rfloor$

(v) $\mu(n,4,3) \leqslant \dfrac{n(n-1)}{3}$ *for* $n \geqslant 4$

The following theorem provides upper bounds for $\mu(n,d,w)$ even if $w > d$.

Theorem 9. *For all* $n \geqslant 3$, *(i)* $\mu(n, n, n) = n - 1$

(ii) $\mu(n, n, n - 1) = n$

(iii) $\mu(n, d, w) \leqslant \binom{n}{k}\mu(k, d, w)$ *for* $w \leqslant k < n$

(iv) $\mu(n, d, w) \leqslant \mu(n - 1, d, w) + (n - 1)(\mu(n - 1, d, w - 1) + \mu(n - 2, d, w - 2))$ *for* $w < n$

(v) $\mu(n, d, n) \leqslant (n - 1)(\mu(n - 1, d, n - 1) + \mu(n - 2, d, n - 2)$ *for* $2 \leqslant d < n$

(vi) $\mu(n, n - 2, n) \leqslant (n - 1)(\mu(n - 1, n - 2) - 1)$

Proof. The set consisting of the identity and all permutations of a (n, n)-code of weight n is a (n, n)-code. Equality (i) immediately follows from $\mu(n, n) = n$. In [7], G. Chang proved that a diagonal partial latin square whose entries are 1,2,...,n can always be completed in a latin square, such a latin square corresponds to a $(n, n)-$code of weight $n - 1$, and so (ii) holds.
If C is a $(n, d)-$code of weight w, then for each $k-$subset K of $\{1, \dots, n\}$, the permutations $\phi \in C$ with $supp(\phi) \subset K$ form a set isometric to a $(k, d)-$code of weight w. This leads to inequality (iii).
Denote by C^i the subset of permutations ϕ in a $(n, d)-$code C of weight w such that $\phi(1) = i$. If $w < n$, the subset C^1 is a $(n - 1, d)-$code of weight w. For $i = 2, \dots, n$, $l_{(1,i)}(C^i)$ consists of permutations whose support is of cardinality $w-1$ and of permutations fixing 1 and i, with support of cardinality $w - 2$, and so $|l_{(1,i)}(C^i)| \leqslant \mu(n - 1, d, w - 1) + \mu(n - 2, d, w - 2)$. Any $(n, d)-$code of weight w can be written as a disjoint union $C = \cup_{i=1}^{n} C^i$, proving inequality (iv). If $w = n$ then C^1 is empty, and the corresponding inequality is (v). For $w = n$ and $d = n - 2$, and for $i = 2, \dots, n$ each of subset $l_{(1,i)}(C^i)$ is isometric to a $(n - 1, n - 2)-$code whose all elements have support at least $n - 2$. Such a code can be completed with the identity permutation and therefore has size less than $\mu(n - 1, n - 2) - 1$, hence equality (vi). □

The upper bounds given in Theorem 9 are not sharp. For example, a clique search inspired by the method developped in [8] gives $\mu(6, 5, 5) = 15$, while the upper bound obtained by application of Theorem is 9 $\mu(6, 5, 5) \leqslant 34$. For this reason, the upper bounds do not contribute to any improvement of the results given by Theorem 7 for the range of values considered in Tables 1 and 2.

References

[1] Erik Agrell, Alexander Vardy, and Kenneth Zeger. Upper bounds for constant-weight codes. *IEEE Transactions on Information Theory*, 46(7):2373–2395, 2000.

[2] V. B. Balakirsky and A. J. Han Vinck. On the performance of permutation codes for multi-user communication. *Probl. Inf. Transm.*, 39(3):239–254, 2003.

[3] Ian Blake. Permutation codes for discrete channels. *IEEE Tansactions on Information Theory*, pages 138–140, 1974.

[4] Mathieu Bogaerts. *Codes et tableaux de permutations: construction , énumération et automorphismes*. PhD thesis, Université Libre de Bruxelles, June 2009.

[5] Wieb Bosma, John J. Cannon, and Catherine Playoust. The Magma algebra system. I. The user language, 1997. http://magma.maths.usyd.edu.au/magma/.

[6] P. J. Cameron. Metric and geometric properties of sets of permutations. In Deza, Frankl, and Rosenberg, editors, *Algebraic, Extremal and Metric Combinatorics 1986*, pages 39–53. Cambridge University Press, 1988.

[7] Gerard J. Chang. Complete diagonals of latin square. *Canadian Bulletin of Mathematics*, 22(4):477–481, 1979.

[8] Wensong Chu, Charles J. Colbourn, and Peter Dukes. Construction for permutation codes in powerline communications. *Des. Codes Cryptography*, 32:51–64, 2004.

[9] P. Delsarte. An algebraic approach to the association schemes of coding theory. Technical report, Philips Research Reports, 1973.

[10] M. Deza and P. Frankl. On the maximum number of permutations with given maximal or minimal distance. *Journal of Combinatorial Theory (A)*, 22:352–360, 1977.

[11] Michael Deza and Tayuan Huang. Metrics on permutations, a survey. *J. Combinatorics, Information and System Sciences*, 23:173–185, 1998.

[12] H. Farahat. The symmetric group as a metric space. *Journal of London Mathematical Society*, 35:215–220, 1960.

[13] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008. http://www.gap-system.org.

[14] MATLAB 7, 2004. http://www.mathworks.com/.

[15] Hannu Tarnanen. Upper bounds on permutation codes via linear programming. *European J. Combinatorics*, 20:101–114, 1999.

[16] A.J. Han Vinck. Coded modulation for power-line communications. *AE Int. J. Electron. and Commun.*, 54(1):45–49, 2000.

[17] Lizhen Yang, Ling Dong, and Kefei Chen. New upper bounds on sizes of permutation arrays. *CoRR*, abs/0801.3983, 2008. http://arxiv.org/abs/0801.3983.