Des. Codes Cryptogr.
DOI 10.1007/s10623-014-9930-z

Permutation codes invariant under isometries

Ingo Janiszczak · Wolfgang Lempken · Patric R. J. Östergård · Reiner Staszewski

Received: 16 September 2013 / Revised: 9 January 2014 / Accepted: 21 January 2014

Abstract The symmetric group S_n on n letters is a metric space with respect to the Hamming distance. The corresponding isometry group is well known to be isomorphic to the wreath product $S_n \wr S_2$. A subset of S_n is called a permutation code or a permutation array, and the largest possible size of a permutation code with minimum Hamming distance d is denoted by $M(n, d)$. Using exhaustive search by computer on sets of orbits of isometry subgroups U we are able to determine serveral new lower bounds for $M(n, d)$ for $n \leq 22$. The codes are given by the group U and representatives of the U-orbits.

Keywords Backtrack search · Bounds · Isometry · Permutation code

Mathematics Subject Classification 05A05 · 05E20 · 20B25 · 94B60 · 94B65

1 Introduction

The concept of permutation codes was introduced by Blake [3] in 1974, and the seminal study was soon followed by several early papers including [8–10]; more recent studies include

Communicated by K. Metsch.

I. Janiszczak (✉) · W. Lempken · R. Staszewski
Institute for Experimental Mathematics, University of Duisburg-Essen, 45326 Essen, Germany
e-mail: ingo@iem.uni-due.de

W. Lempken
e-mail: lempken@iem.uni-due.de

R. Staszewski
e-mail: reiner@iem.uni-due.de

P. R. J. Östergård
Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 13000, 00076 Aalto, Finland
e-mail: patric.ostergard@aalto.fi

Published online: 11 February 2014

[4,6,11,12,18]. It has turned out that permutation codes are not only of mathematical interest, but they can be used in powerline communications; see, for example, [6,14].

Let S_n denote the symmetric group acting on the set $\{1, 2, \ldots, n\}$ for a fixed natural number n. It is well known that the Hamming distance $d_H(\sigma, \tau)$ for $\sigma, \tau \in S_n$ equals n minus the number of fixed points of $\sigma^{-1}\tau$. Any subset C of S_n is called a *permutation code* or a *permutation array* (PA) of length n and of minimum distance

$$d(C) := min\,\{d_H(\sigma, \tau) \mid \sigma, \tau \in C, \sigma \neq \tau\}.$$

For conformity we say that C is an (n, d)-PA. Moreover, $M(n, d)$ denotes the size of the largest (n, d)-PA for any $1 \leq d \leq n$.

By [13] it is known that the complete isometry group $Iso(n)$ with respect to the Hamming distance is isomorphic to the wreath product $S_n \wr S_2$ and thus can be realized as a subgroup of the symmetric group S_{2n} in the following way. Let B_1 and B_2 be the naturally embedded subgroups isomorphic to S_n acting on the sets $\{1, 2, \ldots, n\}$ and $\{n+1, n+2, \ldots, 2n\}$, respectively, and set $t_n := (1, n + 1)(2, n + 2) \cdots (n, 2n) \in S_{2n}$. Then $Iso(n) = \langle B_1, B_2, t_n\rangle = (B_1 \times B_2) : \langle t_n\rangle$, and the codes C to be investigated are subsets of B_1. In this setting the action of an element $x \in Iso(n)$ on B_1 will be denoted by $b * x$ for $b \in B_1$ and is defined as follows:

$$b * x = \begin{cases} x^{-1} \cdot b & \text{if } \ x \in B_1 \\ b \cdot \varphi(x) & \text{if } \ x \in B_2 \\ b^{-1} & \text{if } \ x = t_n, \end{cases}$$

where φ denotes the natural isomorphism from B_2 to B_1. It is easy to see that $*$ is really an action of $Iso(n)$ on B_1. Moreover, $b * U$ denotes the U - orbit of $b \in B_1$ under the action of $U \leq Iso(n)$.

The aim of this study is to construct new permutation codes and thereby improve lower bounds on $M(n, d)$ for small lengths n. The strategy is to construct (n, d)-PAs invariant under a given subgroup U of $Iso(n)$. In order to achieve this we have to calculate the set

$$M_U^d := \{b * U \mid b \in B_1,\ d(b * U) \geq d\}$$

and then investigate the possibility of joining elements of M_U^d to obtain maximal U-invariant (n, d)-PAs. For this we employ backtrack searches by computer.

A recent table of bounds for $M(n, d)$ appears in [18]. Some of these bounds have been found without the use of any subgroups of $Iso(n)$, e.g. $M(7, 4) \geq 349$ in [6]. Whenever subgroups of $Iso(n)$ have been used in the determination of bounds so far, only special types of subgroups U have been considered. In [18] U is contained either in B_1 or in B_2 and in [16] U is of the form $\{x \cdot x^{t_n} \mid x \in U_0\}$ for some subgroup U_0 of B_1. In this paper no restrictions on the subgroups U are made as long as all necessary computations can be carried out in a reasonable time.

It is well known that $M(n, d) \leq \frac{n!}{(d-1)!}$ and that C is an (n, d)-PA of size $\frac{n!}{(d-1)!}$ if and only if C is a sharply $(n - d + 1)$-transitive subset of S_n. Since all sharply l-transitive groups have been classified (cf. [15,20]), one knows that $M(11, 8) = \frac{11!}{7!}$, $M(12, 8) = \frac{12!}{7!}$, $M(n, 2) = \frac{n!}{2}$, $M(n, 1) = n!$, $M(n, n) = n$, $M(n, n - 1) = n(n - 1)$ for n a prime power, and $M(n, n - 2) = n(n - 1)(n - 2)$ for $n - 1$ a prime power. Moreover, $M(6, 5) = 18$ by [10,17]. So these cases will not be discussed in the following.

2 Search strategies

Let U be a subgroup of $Iso(n)$ and let $X_U^d = \{x_1, x_2, \ldots, x_r\}$ be a full set of representatives of elements in M_U^d. A backtrack search on M_U^d can be used to find a subset R of $\{1, 2, \ldots, r\}$ such that $d(x_i * U \cup x_j * U) = d(\{x_i\} \cup x_j * U) \geq d$ for all $i, j \in R$ and $\sum_{i \in R} |x_i * U|$ is maximal, giving a largest possible U-invariant (n, d)-PA. Unfortunately the number r becomes very large for small orders of U.

Let $N := \mathbf{N}_{Iso(n)}(U)$ be the normalizer of U in $Iso(n)$ and let C be a U-invariant subset of B_1, i.e. $C * u = C$ for all $u \in U$. In particular, C is a union of U-orbits. For $x \in N$ we have

$$(C * x) * U = C * (x \cdot U) = C * (U \cdot x) = (C * U) * x = C * x.$$

Therefore N acts on the set of all U-invariant subsets of B_1 preserving the minimal distances, i.e. $d(C) = d(C * x)$. Two U-invariant subsets C_1, C_2 of B_1 are called N-equivalent if $C_1 = C_2 * y$ for some $y \in N$; in particular this defines an equivalence relation on M_U^d. Now we will calculate M_U^d and partition M_U^d into N-equivalence classes.

Let C_1 be a U-invariant (n, d)-PA and let $\mathcal{O}_1, \mathcal{O}_2 \in M_U^d$ be elements of a fixed N-equivalence class such that $\mathcal{O}_1$ is a subset of C_1. Then there exists an (n, d)-PA C_2 such that $\mathcal{O}_2$ is a subset of C_2 and C_1 and C_2 are N-equivalent. Using this we can reduce the computation time substantially in the following way. Let s be the number of N-equivalence classes on M_U^d, and let $K_l := \{\mathcal{O}_{l1}, \mathcal{O}_{l2}, \ldots, \mathcal{O}_{lr_l}\}$ be the l-th N-equivalence class for $1 \leq l \leq s$. For a fixed $l \in \{1, .., s\}$ we let

$$T_l := \{\mathcal{O} \in (\cup_{k=l}^{s} K_k) \backslash \{\mathcal{O}_{l1}\} \mid d(\mathcal{O}_{l1} \cup \mathcal{O}) \geq d\}$$

and order the elements of T_l say $T_l := \{\mathcal{O}_1^l, ..., \mathcal{O}_{m_l}^l\}$. In order to calculate a largest U-invariant (n, d)-PA it is sufficient to run a backtrack search on all sets T_l for $1 \leq l \leq s$. This is much more efficient than running a backtrack search on M_U^d.

For a fixed subgroup U of $Iso(n)$ the described approach works well for all $n < 12$ provided the chosen subgroup U is not too small. For $n \geq 12$ it takes long to calculate all the U-orbits and for $n \geq 14$ we are even not able to store all of them in memory.

So for $n \geq 12$ we take a different approach by calculating only the non-regular U-orbits, i.e. those of size less than the order of U. This implies there must be an element $x \in U$, $x \neq id$ which stabilizes an element of the orbit. For this it is sufficient to assume that x has prime order. To be more specific, let $\mathcal{V}(p)$ denote a set of U-class-representatives of subgroups V of order p in U, where p is a prime dividing $|U|$. Furthermore, let $\mathcal{V}$ be the union of all such $\mathcal{V}(p)$. For each $V \in \mathcal{V}$ we then calculate the set

$$Fix_{B_1}(V) := \{b \in B_1 \mid b * V = \{b\}\}$$

and the set of orbits $\{b * U \mid b \in Fix_{B_1}(V)\}$.

We claim that these are all non-regular U-orbits. For this suppose that $b*U$ is a non-regular orbit, i.e.

$$Stab_U(b) := \{u \in U \mid b * u = b\} > \{id_U\}.$$

In particular there exists a cyclic subgroup W of $\mathrm{Stab}_U(b)$ of prime order, and hence there exists $V \in \mathcal{V}, u \in U$ such that $W^u = V$. We have $b * W = \{b\}$ and thus

$$\begin{aligned}(b * u) * V &= (b * u) * W^u = (b * u) * (u^{-1} W u) \\ &= (b * u) * u^{-1} * W * u = b * W * u\end{aligned}$$

$$= \{b * u\},$$

i.e. $b * u \in Fix_{B_1}(V)$.

Having calculated all non-regular U-orbits with minimum distance at least d, we proceed as described above in order to find codes of minimum distance d.

All this has been implemented in MAGMA [5].

3 Improvements

In Theorem 1, we list the new lower bounds on $M(n, d)$ obtained in the current study. The old bounds are from [18], except for the one for $n = 14$ and $d = 13$ which is from [19].

Theorem 1 *We have the following lower bounds on* $M(n, d)$*:*

(n, d)	*new bound*	*old bound*
(7, 5)	78	77
(9, 4)	18576	18144
(10, 5)	19440	18720
(10, 7)	1484	720
(11, 9)	297	154
(12, 11)	112	60
(13, 8)	38688	27132
(13, 9)	6474	4810
(13, 11)	276	195
(14, 10)	8736	6552
(14, 13)	59	56
(15, 11)	7540	6076
(15, 13)	315	243
(15, 14)	90	56
(16, 13)	1376	1266
(16, 14)	1376	269
(18, 17)	90	70
(20, 19)	120	78
(21, 20)	147	–
(22, 21)	121	–

Proof We present codes attaining the new bounds. Specifically, for a given pair (n, d) we describe the group U by listing its generators, and the corresponding U-invariant (n, d)-PA C is given by a set R consisting of representatives for each U-orbit in C. Also the lengths of the U-orbits are given in the form of a tuple L.

$(n, d) = (7, 5)$:
$|U| = 36$,
$U = \langle\ (1, 8)(2, 9, 7, 14)(3, 10, 4, 11)(5, 12, 6, 13),$
$(2, 7)(3, 4)(5, 6)(9, 14)(10, 11)(12, 13),$
$(9, 11, 12)(10, 13, 14),$
$(2, 4, 5)(3, 6, 7)(9, 12, 11)(10, 14, 13)\rangle,$
$R = \{\ (1, 3)(2, 7, 4), (1, 5, 3, 7, 6), id\},$
$L =\ [\ 36, 36, 6\ ].$

$(n, d) = (9, 4)$:
$|U| = 62208$,
$U = \langle\ (1, 5, 2, 7)(4, 9, 8, 6),$
$(4, 9)(5, 7)(6, 8)(13, 16)(14, 17)(15, 18),$
$(1, 10)(2, 11, 4, 18, 9, 13)(3, 12, 7, 14, 5, 16)(6, 17)(8, 15)\rangle,$
$R = \{\ (1, 3, 2, 5, 7), (1, 7, 8, 2), (1, 2)(5, 9)(6, 7), (5, 7)(6, 9), (1, 2, 3)(4, 6, 5),$
$(1, 9)(3, 4)(6, 7), (1, 4)(2, 8)(6, 9)\},$
$L =\ [\ 10368, 3888, 1944, 1944, 216, 144, 72\ ].$

$(n, d) = (10, 5)$:
$|U| = 51840$,
$U = \langle\ (1, 10)(2, 3)(5, 8)(6, 9)(11, 15, 20, 18)(12, 16, 13, 19),$
$(1, 2, 7, 3)(4, 9, 10, 8)(11, 19, 16, 12)(13, 14, 20, 18),$
$(11, 16, 19, 18)(12, 15, 14, 20),$
$(11, 20, 19, 15)(12, 16, 14, 18)\rangle,$
$R = \{\ (1, 8, 6, 3)(2, 9, 7), (2, 8, 4, 9, 3)(5, 6), (1, 2, 5, 8)(3, 6, 10)\},$
$L =\ [\ 6480, 6480, 6480\ ].$

$(n, d) = (10, 7)$:
$|U| = 294$,
$U = \langle\ (12, 17)(13, 16)(14, 15)(18, 19),$
$(4, 8, 10)(5, 6, 9)(12, 15, 13)(14, 16, 17),$
$(2, 9, 6, 8, 5, 10, 4)(11, 12, 13, 14, 15, 16, 17),$
$(11, 12, 13, 14, 15, 16, 17)\rangle,$
$R = \{\ (1, 8, 6, 5, 10, 7)(2, 4), (2, 9)(3, 10, 4, 5), (1, 10, 2, 6, 8, 9, 5, 3), (1, 10, 2, 7, 8, 6),$
$(3, 10, 6, 4)(7, 8), (1, 10, 5, 3, 8, 2, 4, 9), (1, 6, 7, 10, 3, 8)(4, 5), (1, 8, 6, 7, 9, 2, 5),$
$(1, 8, 4, 3, 9, 10, 7), (1, 10, 4, 3, 8, 6, 7, 9)\},$
$L =\ [\ 294, 294, 294, 98, 98, 98, 98, 98, 98, 14\ ].$

$(n, d) = (11, 9)$:
$|U| = 2420$,
$U = \langle\ (1, 12)(2, 13)(3, 14)(4, 15)(5, 16)(6, 17)(7, 18)(8, 19)(9, 20)(10, 21)(11, 22),$
$(1, 10, 5, 9, 8, 11, 2, 7, 3, 4)(12, 20, 21, 17, 22, 13, 16, 15, 19, 14),$
$(1, 5, 8, 2, 3)(4, 10, 9, 11, 7)(12, 18, 15, 22, 13)(14, 17, 21, 19, 20),$
$(1, 3, 5, 7, 9, 11, 2, 4, 6, 8, 10)(12, 15, 18, 21, 13, 16, 19, 22, 14, 17, 20),$
$(12, 19, 15, 22, 18, 14, 21, 17, 13, 20, 16)\rangle,$
$R = \{\ (1, 8, 11, 9)(2, 7, 6, 10, 3), (1, 8, 6, 3)(2, 5, 10, 4, 7), id\},$
$L =\ [\ 121, 121, 55\ ].$

$(n, d) = (12, 11)$:

$|U| = 216,$

$U = \langle$ (2, 6, 10)(3, 7, 11)(4, 8, 12)(14, 18, 22)(15, 19, 23)(16, 20, 24),
(1, 5)(2, 10)(4, 8)(7, 11)(13, 17)(14, 22)(16, 20)(19, 23),
(2, 3, 4)(6, 7, 8)(10, 11, 12)(14, 15, 16)(18, 19, 20)(22, 23, 24),
(1, 7, 2)(3, 6, 9)(5, 11, 10)(13, 19, 14)(15, 18, 21)(17, 23, 22)$\rangle$,

$R = \{$ (1, 12, 11)(2, 5, 9, 6, 7, 3, 10, 4, 8), (1, 3)(2, 5, 6, 9)(4, 11, 12, 7)(8, 10),
(1, 7, 2)(3, 6, 9)(4, 8)(5, 11, 10), $id\}$,

$L = 72, 27, 12, 1.$

$(n, d) = (13, 8)$:

$|U| = 24336,$

$U = \langle$ (14, 15, 22, 19, 24, 20, 18, 17, 23, 26, 21, 25),
(14, 18)(15, 17)(19, 26)(20, 25)(21, 24)(22, 23),
(14, 24, 23)(15, 20, 26)(17, 25, 19)(18, 21, 22),
(1, 6, 5, 13)(2, 11, 4, 8)(7, 10, 12, 9)(14, 21, 25, 18)(15, 16, 24, 23)(17, 19, 22, 20),
(1, 5)(2, 4)(6, 13)(7, 12)(8, 11)(9, 10)(14, 17)(15, 16)(18, 26)(19, 25)(20, 24)(21, 23),
(1, 10, 11)(2, 13, 7)(4, 6, 12)(5, 9, 8)(14, 24, 23)(15, 20, 26)(17, 25, 19)(18, 21, 22),
(1, 5, 9, 13, 4, 8, 12, 3, 7, 11, 2, 6, 10)(14, 17, 20, 23, 26, 16, 19, 22, 25, 15, 18, 21, 24),
(14, 24, 21, 18, 15, 25, 22, 19, 16, 26, 23, 20, 17)$\rangle$,

$R = \{$ (1, 11, 3, 2, 12, 4, 6, 8, 10, 13), (1, 8, 12, 10, 3, 9, 5, 7)(6, 11),
(1, 5, 6, 13, 2, 3, 7, 4, 8, 11), (1, 9, 7, 2, 13, 11, 12, 8, 4, 5, 3),
(1, 8, 7, 9, 5, 13, 10, 3, 4, 2, 6, 11)$\}$,

$L = 12168, 12168, 12168, 2028, 156.$

$(n, d) = (13, 9)$:

$|U| = 4056,$

$U = \langle$ (1, 19, 9, 16, 2, 17, 13, 21, 5, 24, 12, 23)(3, 15, 4, 26, 8, 18, 11, 25, 10, 14, 6, 22)(7, 20),
(1, 11, 2)(3, 4, 7)(5, 10, 12)(6, 13, 8)(14, 16, 22)(15, 19, 18)(17, 25, 23)(20, 21, 24),
(1, 12, 2, 4)(3, 9, 13, 7)(5, 6, 11, 10)(14, 21, 25, 18)(15, 16, 24, 23)(17, 19, 22, 20),
(1, 7)(2, 6)(3, 5)(8, 13)(9, 12)(10, 11)(14, 25)(15, 24)(16, 23)(17, 22)(18, 21)(19, 20),
(1, 6, 11, 3, 8, 13, 5, 10, 2, 7, 12, 4, 9)(14, 17, 20, 23, 26, 16, 19, 22, 25, 15, 18, 21, 24),
(14, 20, 26, 19, 25, 18, 24, 17, 23, 16, 22, 15, 21)$\rangle$,

$R = \{$ (1, 7, 12, 3)(2, 13, 9, 5, 8, 4), (1, 6, 3, 7, 5, 12, 8, 13, 2)(4, 10),
(1, 3, 10, 12, 4, 2, 7, 13, 8), (2, 4, 12, 3, 10, 8, 13, 9)(5, 7),
(1, 8, 5, 10, 13, 7, 6, 4, 3)(9, 12), (1, 7)(2, 3, 13, 9, 5, 6, 4, 10, 8),
(1, 4, 6, 3)(2, 9, 5, 11)(7, 8, 13, 12), $id\}$,

$L = 2028, 1352, 1352, 1014, 338, 338, 26, 26.$

$(n, d) = (13, 11)$:

$|U| = 660,$

$U = \langle$ (1, 11)(2, 3)(4, 6)(5, 7)(8, 13)(9, 12)(14, 24)(15, 16)(17, 19)(18, 20)(21, 26)(22, 25),
(1, 8, 13)(2, 4, 12)(3, 11, 5)(6, 9, 7)(14, 21, 26)(15, 17, 25)(16, 24, 18)(19, 22, 20)$\rangle$,

$R = \{$ (1, 6, 8, 13, 12)(2, 11, 7, 3, 5)(4, 10, 9), (1, 9, 4, 12, 3)(2, 11, 5, 8, 7)(6, 10),
(1, 7)(2, 11)(3, 12)(4, 5)(6, 8)(9, 13), $id\}$,

$L = 132, 132, 11, 1.$

$(n, d) = (14, 10)$:

$|U| = 4368,$

$U = \langle\ (1, 8)(2, 9)(3, 10)(4, 11)(5, 12)(6, 13)(7, 14)(15, 17)(16, 26)(18, 25)(19, 21)(20, 24)$
$(22, 27)(23, 28),$
$(1, 2, 11, 13, 8, 9, 3, 10, 6, 12, 4, 14, 7)(15, 16)(17, 26)(18, 21)(19, 25)(20, 28)(22, 27)$
$(23, 24),$
$(15, 16)(17, 26)(18, 21)(19, 25)(20, 28)(22, 27)(23, 24)\rangle,$

$R = \{\ (1, 11, 5, 3)(2, 10, 8, 14)(6, 13),\ (1, 12, 5, 7, 9, 6, 8, 2, 10)(4, 11),$
$(1, 6, 9, 7, 5, 12, 10, 11, 8, 4, 3, 13),\ (2, 8, 3, 5, 10, 6, 9, 4, 13, 11, 14)\},$

$L = 2184, 2184, 2184, 2184.$

$(n, d) = (14, 13)$:

$|U| = 42,$

$U = \langle\ (1, 22)(2, 25, 3, 28, 5, 27)(4, 24, 7, 26, 6, 23)(8, 15)(9, 21, 10, 20, 12, 18)$
$(11, 19, 14, 16, 13, 17),$
$(2, 5, 3)(4, 6, 7)(9, 12, 10)(11, 13, 14)(16, 19, 17)(18, 20, 21)(23, 26, 24)(25, 27, 28),$
$(1, 4, 7, 3, 6, 2, 5)(8, 11, 14, 10, 13, 9, 12)(15, 21, 20, 19, 18, 17, 16)$
$(22, 25, 28, 24, 27, 23, 26)\rangle,$

$R = \{\ (2, 7, 12, 8, 10, 9, 5, 13, 4, 6, 14),\ (1, 10, 3, 7, 12, 6, 13, 8, 9, 2, 11, 14, 5),$
$(1, 3, 2, 10, 11)(4, 8, 12, 6)(5, 14, 9),\ (1, 3, 7)(2, 5, 4)(8, 14, 13, 12, 11, 10, 9),$
$(1, 14, 3, 9, 7, 13)(2, 8, 5, 11, 4, 10)(6, 12),\ (1, 8)(2, 9, 3, 10, 5, 12)(4, 11, 7, 14, 6, 13)\},$

$L = 21, 21, 7, 6, 3, 1.$

$(n, d) = (15, 11)$:

$|U| = 2400,$

$U = \langle\ (1, 8, 14)(2, 6, 13)(3, 9, 12)(4, 7, 11)(5, 10, 15)(16, 30, 23)(17, 29, 21)(18, 28, 24)$
$(19, 27, 22)(20, 26, 25),$
$(16, 17, 18, 19, 20)(21, 24, 22, 25, 23)(26, 30, 29, 28, 27),$
$(1, 18)(2, 19)(3, 20)(4, 16)(5, 17)(6, 22)(7, 23)(8, 24)(9, 25)(10, 21)(11, 30)(12, 26)$
$(13, 27)(14, 28)(15, 29),$
$(1, 3, 2, 5)(6, 10, 8, 9)(12, 13, 15, 14)(17, 19, 20, 18)(21, 22, 25, 24)(26, 28, 29, 27),$
$(17, 20)(18, 19)(21, 25)(22, 24)(26, 29)(27, 28),$
$(1, 3, 5, 2, 4)(6, 11, 8, 12, 10, 13, 7, 14, 9, 15)(16, 19, 18, 20)(21, 29)(22, 28, 25, 30)$
$(23, 27, 24, 26),$
$(1, 2)(3, 5)(6, 8)(9, 10)(12, 15)(13, 14)(17, 20)(18, 19)(21, 25)(22, 24)(26, 29)(27, 28),$
$(1, 5, 4, 3, 2)(6, 8, 10, 7, 9)(11, 12, 13, 14, 15)(16, 18, 20, 17, 19)(21, 22, 23, 24, 25)$
$(26, 29, 27, 30, 28)\rangle,$

$R = \{\ (1, 9, 8, 3, 10, 15, 2, 12, 7)(4, 6, 5),\ (2, 7, 8, 5, 15, 3, 10, 12, 11, 9, 4, 6),$
$(1, 15, 7, 11, 2, 5)(3, 6, 13, 8)(10, 12),\ (1, 9, 11, 7, 15, 4, 14, 12)(3, 13, 6, 10),$
$(1, 3, 6, 2, 12, 9, 15, 5, 7, 8)(4, 14),\ (1, 7, 5, 13, 3, 6, 8, 14, 9)(10, 15, 12),$
$(2, 14, 11, 13)(4, 5)(7, 8)(9, 10),\ (6, 14, 8, 15, 10, 11, 7, 12, 9, 13),$
$(1, 15, 5, 11, 4, 12, 3, 13, 2, 14)\},$

$L = 1200, 1200, 1200, 1200, 1200, 1200, 300, 20, 20.$

$(n, d) = (15, 13)$:

$|U| = 150,$

$U = \langle$ (16, 17, 20, 18, 19)(21, 22, 23, 25, 24)(26, 30, 29, 27, 28),
(1, 29, 2, 30, 3, 26, 4, 28, 5, 27)(6, 24, 8, 25, 9, 23, 7, 22, 10, 21)
(11, 19, 13, 18, 12, 20, 14, 17, 15, 16),
(1, 10, 13)(2, 6, 12)(3, 8, 14)(4, 9, 15)(5, 7, 11)(16, 23, 28)(17, 25, 26)(18, 21, 29)
(19, 22, 27)(20, 24, 30),
(1, 2, 3, 4, 5)(6, 8, 9, 7, 10)(11, 13, 12, 14, 15)$\rangle$,

$R = \{$ (1, 13, 2, 3, 10, 4, 9, 12, 15)(7, 11), (1, 6, 13, 4, 11, 9, 12, 5, 10)(2, 15, 7, 3, 8),
(1, 12, 5, 2, 4, 7, 11, 13, 6)(3, 14, 8), (1, 13, 8, 11, 3, 9, 5)(4, 6, 14),
(1, 2, 5)(6, 9, 7, 8)(11, 13)(12, 15), (1, 8, 15, 3, 9, 14, 5, 7, 12, 2, 10, 13)(4, 6, 11),
(1, 12, 8, 2, 13, 7, 3, 11, 6)(4, 15, 9, 5, 14, 10)$\}$,

$L =$ [75, 75, 75, 75, 5, 5, 5].

$(n, d) = (15, 14)$:

$|U| = 150,$

$U = \langle$ (1, 3)(4, 5)(6, 10)(7, 8)(12, 14)(13, 15)(16, 28, 25, 18, 26, 21)(17, 27, 24)
(19, 30, 23, 20, 29, 22),
(16, 25, 26)(17, 24, 27)(18, 21, 28)(19, 23, 29)(20, 22, 30),
(1, 2, 3, 5, 4)(11, 15, 12, 14, 13)(16, 18, 19, 17, 20)(21, 23, 24, 22, 25)
(26, 28, 29, 27, 30),
(1, 5, 2, 4, 3)(6, 7, 8, 10, 9)(11, 12, 13, 15, 14)$\rangle$,

$R = \{$ (1, 12, 6, 11, 2, 8, 15, 3, 13, 9, 10, 7, 4), (2, 4)(3, 5)(6, 9, 7, 8)$\}$,

$L =$ [75, 15].

$(n, d) = (16, 13)$: same as $(n, d) = (16, 14)$

$(n, d) = (16, 14)$:

$|U| = 960,$

$U = \langle$ (1, 14, 12, 8, 13, 16, 6, 7, 15, 4, 3, 10, 9, 5, 11)
(17, 30, 28, 24, 29, 32, 22, 23, 31, 20, 19, 26, 25, 21, 27),
(1, 8, 13, 16)(2, 14, 6, 10)(3, 7)(4, 5, 12, 9)(17, 24, 29, 32)(18, 30, 22, 26)(19, 23)
(20, 21, 28, 25)$\rangle$,

$R = \{$ (1, 3, 8, 14, 10, 5, 12)(2, 4, 16, 15, 6, 11, 9),
(1, 7, 9, 2, 14, 13, 4, 16, 6, 8, 3, 15, 12, 5)(10, 11),
(1, 8, 2, 4, 3, 12)(5, 11, 14)(6, 7, 15, 13, 9, 10),
(1, 12, 13, 4)(2, 14, 6, 10)(3, 7)(5, 8, 9, 16),
(1, 6, 11, 4, 13, 10, 7, 8)(2, 3, 16, 5, 14, 15, 12, 9),
(1, 4)(2, 7)(3, 6)(5, 16)(8, 13)(9, 12)(10, 15)(11, 14), $id\}$,

$L =$ [480, 480, 160, 120, 120, 15, 1].

$(n, d) = (18, 17)$:

$|U| = 54,$

$U = \langle$ (1, 7, 13)(2, 8, 14)(3, 9, 15)(4, 10, 16)(5, 11, 17)(6, 12, 18)(19, 25, 31)(20, 26, 32)
(21, 27, 33)(22, 28, 34)(23, 29, 35)(24, 30, 36),
(19, 21, 23)(20, 22, 24)(25, 27, 29)(26, 28, 30)(31, 33, 35)(32, 34, 36),
(1, 3, 5)(2, 4, 6)(7, 9, 11)(8, 10, 12)(13, 15, 17)(14, 16, 18)(19, 21, 23)(20, 22, 24)
(25, 27, 29)(26, 28, 30)(31, 33, 35)(32, 34, 36),
(7, 13)(8, 14)(9, 15)(10, 16)(11, 17)(12, 18)(25, 31)(26, 32)(27, 33)(28, 34)(29, 35)
(30, 36)$\rangle$,

$R = \{\ (1, 17, 13, 10, 15, 11, 5, 16, 12, 6, 9, 4, 8, 14, 3)(2, 18),$
$(1, 17, 18)(2, 13, 7, 3, 12, 15)(4, 14, 9, 16, 10, 6, 11, 8, 5),$
$(1, 18, 11)(2, 13, 9)(3, 17, 10)(4, 5, 8, 14, 15, 6, 12, 7, 16),$
$(1, 13, 6, 10, 18, 5, 8, 15, 11, 3, 9, 16, 14, 2, 4, 7, 17),$
$(1, 13)(2, 16, 6, 14, 4, 18)(3, 15)(5, 17)(7, 10, 11, 8, 9, 12),$
$(1, 8)(2, 7)(3, 10)(4, 9)(5, 12)(6, 11)(14, 18, 16)\},$
$L = [\ 18, 18, 18, 18, 9, 9\ ].$

$(n, d) = (20, 19)$:
$|U| = 200,$
$U = \langle\ (1, 4)(2, 3)(6, 8)(9, 10)(11, 13)(14, 15)(16, 19)(17, 18)(21, 24)(22, 23)(26, 27)(28, 30)$
$(31, 32)(33, 35)(37, 40)(38, 39),$
$(21, 24, 22, 25, 23)(26, 28, 30, 27, 29)(31, 33, 35, 32, 34)(36, 39, 37, 40, 38),$
$(1, 16)(2, 17)(3, 18)(4, 19)(5, 20)(6, 11)(7, 12)(8, 13)(9, 14)(10, 15)(21, 37)(22, 38)$
$(23, 39)(24, 40)(25, 36)(26, 31)(27, 32)(28, 33)(29, 34)(30, 35),$
$(1, 5, 4, 3, 2)(6, 7, 8, 9, 10)(11, 15, 14, 13, 12)(16, 17, 18, 19, 20)(21, 25, 24, 23, 22)$
$(26, 27, 28, 29, 30)(31, 35, 34, 33, 32)(36, 37, 38, 39, 40),$
$(1, 9, 2, 7)(3, 10, 5, 6)(4, 8)(11, 16)(12, 19, 15, 18)(13, 17, 14, 20)(21, 28)$
$(22, 26, 25, 30)(23, 29, 24, 27)(31, 39)(32, 37, 35, 36)(33, 40, 34, 38)\rangle,$
$R = \{\ (1, 9, 4, 20, 14, 6, 11, 12, 7, 17, 8)(3, 18, 13, 19, 5)(10, 16),$
$(1, 6, 20, 7, 13, 14)(2, 12, 19, 4)(3, 10, 8, 11, 17)(9, 16),$
$(1, 6, 17, 15, 5, 7, 18, 14, 4, 8, 19, 13, 3, 9, 20, 12, 2, 10, 16, 11),$
$(1, 17, 5, 18, 4, 19, 3, 20, 2, 16)\},$
$L = [\ 50, 50, 10, 10\ ].$

$(n, d) = (21, 20)$:
$|U| = 294,$
$U = \langle\ (1, 19, 8)(2, 21, 12)(3, 16, 9)(4, 18, 13)(5, 20, 10)(6, 15, 14)(7, 17, 11)(22, 40, 29)$
$(23, 42, 33)(24, 37, 30)(25, 39, 34)(26, 41, 31)(27, 36, 35)(28, 38, 32),$
$(22, 26, 23, 27, 24, 28, 25)(29, 33, 30, 34, 31, 35, 32)(36, 40, 37, 41, 38, 42, 39),$
$(1, 4, 7, 3, 6, 2, 5)(8, 11, 14, 10, 13, 9, 12)(15, 18, 21, 17, 20, 16, 19)$
$(22, 25, 28, 24, 27, 23, 26)(29, 32, 35, 31, 34, 30, 33)(36, 39, 42, 38, 41, 37, 40),$
$(1, 22)(2, 23)(3, 24)(4, 25)(5, 26)(6, 27)(7, 28)(8, 29)(9, 30)(10, 31)(11, 32)(12, 33)$
$(13, 34)(14, 35)(15, 36)(16, 37)(17, 38)(18, 39)(19, 40)(20, 41)(21, 42)\rangle,$
$R = \{\ (1, 9, 14, 5, 13, 6, 3, 10, 21, 15, 7, 19, 2, 17, 8, 11, 18, 20, 12, 16),$
$(1, 5)(2, 11)(3, 15)(6, 9)(7, 21)(8, 10)(12, 17)(14, 16)(19, 20)\},$
$L = [\ 98, 49\ ].$

$(n, d) = (22, 21)$:
$|U| = 1210,$
$U = \langle\ (2, 5, 6, 10, 4)(3, 9, 11, 8, 7)(12, 13, 17, 22, 20)(14, 21, 16, 18, 15)(24, 28, 26, 27, 32)$
$(25, 33, 29, 31, 30)(35, 39, 37, 38, 43)(36, 44, 40, 42, 41),$
$(1, 5, 9, 2, 6, 10, 3, 7, 11, 4, 8)(12, 16, 20, 13, 17, 21, 14, 18, 22, 15, 19),$
$(23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33)(34, 44, 43, 42, 41, 40, 39, 38, 37, 36, 35),$
$(1, 13, 11, 12, 10, 22, 9, 21, 8, 20, 7, 19, 6, 18, 5, 17, 4, 16, 3, 15, 2, 14)(23, 34)(24, 35)$
$(25, 36)(26, 37)(27, 38)(28, 39)(29, 40)(30, 41)(31, 42)(32, 43)(33, 44)\rangle,$
$R = \{\ (1, 7, 22, 18, 5, 11, 19, 21, 15, 6, 12, 14, 8, 20, 3)(2, 17, 10, 13, 9)\},$
$L = [\ 121\ ].$

□

By considering representatives of all conjugacy classes of subgroups in $Iso(10)$, we can generalize the result of [16].

Theorem 2 *a) There exists a* $(10, 9)-$*PA of size* 49 *which is invariant under a subgroup* U *in* $Iso(10)$ *of order* 8.

(b) There exists no $(10, 9)-$*PA of size bigger than* 49 *which is invariant under a subgroup* U *in* $Iso(10)$ *such that* $|U| \geq 5$.

Proof Part (a) has been proved already in [16]. For part (b) recall first that $|Iso(10)| = 2^{17} \cdot 3^8 \cdot 5^4 \cdot 7^2$. Therefore we take U to be a representative of the $Iso(10)$-conjugacy classes of subgroups isomorphic to one of the following groups: C_9, $C_3 \times C_3$, C_7, C_5, C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, Q_8, D_8. In all these cases it turns out that a maximal U-invariant $(10, 9)$-PA C has size at most 49. Consequently, by Sylow's theorem, we may assume that $|U|$ divides $2^2 \cdot 3$. Thus, in the next step we consider the cases where $|U| = 6$ with $U \cong C_6$ or $U \cong S_3$ or $|U| = 12$ with $U \cong A_4$. As before, by computational means we get $|C| \leq 49$. This leaves $|U| \in \{1, 2, 3, 4\}$ as claimed. □

4 Concluding remarks

We would like to point out that the lower bounds on $M(n, n-1)$ in Theorem 1, except $n = 10$, have been improved for all possible values of $n \leq 22$ where the exact value is not known.

By results in [2], the best known upper bound for $M(10, 9)$ is 87, that is, $49 \leq M(10, 9) \leq 87$. The upper bound is closely related to the fact that no projective plane of order 10 exists. The existence problem for projective planes of order 12 has not been settled yet. After the current work we know that $112 \leq M(12, 11) \leq 132$. It is rather interesting to see that interval for $M(12, 11)$ is much smaller than that for $M(10, 9)$. The previously known lower bound 60 for $M(12, 11)$ is due to the existence of five mutually orthogonal latin squares (MOLS) of order 12, cf. [7]. It is therefore worth investigating whether the new bound could lead to a new bound on the maximum number of MOLS of order 12.

The code C_{112} of size 112 given in Theorem 1 decomposes into orbits of sizes 72, 27, 12, and 1. The orbit of size 72 is a disjoint union of three equidistant codes of size 24 and distance 11. It then follows that C_{112} does not contain a subcode which is a disjoint union of five equidistant codes of size 12 and distance 12, that is, not even five MOLS of order 12 can be be obtained from the code.

We like to thank the referees for drawing our attention to a very recent paper [1] in which the existence of five MOLS of order 18 has been established, thereby also proving $M(18, 17) \geq 90$. We also thank one of the referees for an independant check of the minimum distances of the codes given in the proof of Theorem 1.

Acknowledgments The third author was supported in part by the Academy of Finland under Grant No. 132122.

References

1. Abel, R.J.R.: Existence of five MOLS of orders 18 and 60. J. Comb. Designs (2013). doi:10.1002/jcd.21384
2. Bierbrauer, J., Metsch K.: A bound on permutation codes. Electr. J. Comb. **20**(3), P6 (2013)
3. Blake, I.F.: Permutation codes for discrete channels. IEEE Trans. Inf. Theory **20**, 138–140 (1974)

4. Bogaerts, M.: Isometries and construction of permutation arrays. IEEE Trans. Inf. Theory **56**, 3177–3179 (2010)
5. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997). IEEE Trans. Inf. Theory **56**, 3177–3179 (2010)
6. Chu W, Colbourn C.J., Dukes P.J.: Permutation codes for powerline communication. Design Codes Cryptogr. **32**, 51–64 (2004)
7. Colbourn, C.J., Kløve, T., Ling, A.C.H.: Permutation arrays for powerline communication and mutually orthogonal latin squares. IEEE Trans. Inf. Theory **50**, 1289–1291 (2004)
8. Deza, M.: Matrices dont deux lignes quelconque coïncident dans un nombre donné de positions communes. J. Comb. Theory Ser. A **20**, 306–318 (1976)
9. Deza, M., Frankl, P.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory Ser. A **22**, 352–360 (1977)
10. Deza, M., Vanstone, S.A.: Bounds for permutation arrays. J. Stat. Plan. Infer. **2**, 197–209 (1978)
11. Dukes, P.J.: Permutation codes and arrays. In: Colbourn C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs, 2nd ed. Chapman & Hall/CRC, Boca Raton, pp. 568–571 (2007)
12. Dukes, P.J., Sawchuck, N.: Bounds on permutation codes of distance four. J. Algebraic Combin. **31**, 143–158 (2010)
13. Farahat, H.: The symmetric group as a metric space. J. Lond. Math. Soc. **35**, 215–220 (1960)
14. Ferreira, H.C., Vinck, A.J.H.: Inference cancellation with permutation trellis arrays. In: Proceedings of IEEE Vehtcular Technology Conference, pp. 2401–2407 (2000)
15. Jordan, C.: Recherches sur les substitutions. J. de Math. Pures et Appl. **17**, 345–361 (1872)
16. Janiszczak, I., Staszewski, R.: An Improved Bound for Permutation Arrays of Length 10. Preprint 4, Institute for Experimental Mathematics, University Duisburg-Essen (2008)
17. Kløve, T.: Classification of permutation codes of length 6 and minimum distance 5. In: Proceedings of International Symposium on Information Theory and Its Applications, Honolulu, pp. 465–468 (2000)
18. Smith, D.H., Montemanni, R.A.: A new table of permutation codes. Designs Codes Cryptogr. **63**, 241–253 (2012)
19. Todorov, D.T.: Four mutually orthogonal Latin squares of order 14. J. Comb. Designs **20**, 363–367 (2012)
20. Zassenhaus, H.J.: Kennzeichnung endlicher linearer Gruppen. Abh. Math. Sem. Hamburg **11**, 17–40 (1936)