Des. Codes Cryptogr. (2018) 86:1095–1111
https://doi.org/10.1007/s10623-017-0381-1

Constructing permutation arrays from groups

Sergey Bereg[1] · **Avi Levy**[2] · **I. Hal Sudborough**[1]

Received: 27 January 2017 / Revised: 7 June 2017 / Accepted: 19 June 2017 /
Published online: 29 June 2017

Abstract Let $M(n, d)$ be the maximum size of a permutation array on n symbols with pairwise Hamming distance at least d. We use various combinatorial, algebraic, and computational methods to improve lower bounds for $M(n, d)$. We compute the Hamming distances of affine semilinear groups and projective semilinear groups, and unions of cosets of $AGL(1, q)$ and $PGL(2, q)$ with Frobenius maps to obtain new, improved lower bounds for $M(n, d)$. We give new randomized algorithms. We give better lower bounds for $M(n, d)$ also using new theorems concerning the contraction operation. For example, we prove a quadratic lower bound for $M(n, n-2)$ for all $n \equiv 2 \pmod 3$ such that $n+1$ is a prime power.

Keywords Permutation codes · Permutation arrays · Finite fields · Groups

Mathematics Subject Classification 05A05 · 94B25 · 05E18

1 Introduction

Two permutations π and σ on n symbols have *Hamming distance* $hd(\pi, \sigma) = d$ if, for exactly d distinct elements x, $\pi(x) \neq \sigma(x)$. The *Hamming distance* of a permutation array A (PA), denoted by $hd(A)$, is the minimum $hd(\pi, \sigma)$ for all permutations $\pi \neq \sigma$ in A. Arrays of permutations on n symbols and with Hamming distance at least d between any two permutations in the array have been used for error correcting codes in communication over very noisy power line channels [13,19]. For positive integers n and d, with $d \leq n$, denote by $M(n, d)$ the maximum size of such an array. Constructing maximum size permutation arrays

Communicated by C. J. Colbourn.

✉ Sergey Bereg
besp@utdallas.edu

[1] Department of Computer Science, Erik Jonsson School of Engineering and Computer Science, University of Texas at Dallas, Richardson, TX, USA

[2] Department of Mathematics, University of Washington, Seattle, WA, USA

is difficult and, except for special cases of n and d, work has generally been limited to finding good upper and lower bounds. It is known that sharply k-transitive groups G of permutations on n symbols form a maximum size permutation array for pairwise Hamming distance $d = n-k+1$ [10]. Except for the exceptional case, i.e. 4- and 5-transitive Mathieu groups [4,7,8], sharply k-transitive permutation groups on n symbols are only known for $k = 2$ and $k = 3$ and for n a power of a prime and one more than a power of a prime, respectively, [18]. Furthermore, it is known that sharply k-transitive groups do not exist otherwise. Combinatorial arguments [5,11,24] are known, which give upper and lower bounds for $M(n, d)$, for all n and d. There are also computational approaches that have been used to construct good permutation arrays for small values of n. Due to the growth rate of $n!$, computational approaches are limited to small values of n. The use of automorphism groups enables one to factor the set of all permutations into a smaller space and hence extend the range of computational processes [5,14,21]. It is also known that $M(n, n-1) \geq kn$, where k is the number of mutually orthogonal latin squares (MOLS) of order n [6], which means computing large collections of MOLS is related to searching for large permutation arrays. Other techniques that have been used include permutation polynomials [5], and special groups, such as the Mathieu groups M_{22}, M_{23} and M_{24} [4].

Let n be a positive integer and $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let S_n be the symmetric group on Z_n with composition defined by $(\pi\sigma)(i) = \sigma(\pi(i))$. If G is a group, then $G\sigma = \{g\sigma \mid g \in G\}$ and $\sigma G = \{\sigma g \mid g \in G\}$ are called a *right coset* of G and a *left coset* of G, respectively, with the *representative* σ [12].

Our results, giving infinitely many improved lower bounds are obtained by describing collections of cosets of groups. For example, we use the affine general linear groups $AGL(1, n)$ and the projective general groups $PGL(2, n)$ (for prime powers n) that are sharply t-transitive for $t = 2$ and $t = 3$, respectively. It is well known that, every sharply t-transitive permutation group in S_n has Hamming distance $n - t + 1$ [3,5,10]. We show that groups $A\Gamma L(1, n = p^k)$ and $P\Gamma L(2, n = p^k)$, where p is prime, obtained from $AGL(1, n)$ and $PGL(2, n)$ by adding k Frobenius endomorphisms, both have pairwise Hamming distance $n - p^{k^*}$, where k^* denotes the largest proper[1] factor of k. For example, $A\Gamma L(1, n = 2^k)$, when k is prime, consists of $kn(n-1)$ permutations on n symbols and has pairwise Hamming distance $2^k - 2$, so $M(n, n-2) \geq kn(n-1)$, $P\Gamma L(2, n = 2^k)$, when k is prime, consists of $k(n+1)n(n-1)$ permutations on $n+1$ symbols and has pairwise Hamming distance $2^k - 2$, so $M(n+1, n-2) \geq k(n+1)n(n-1)$. We also show that the groups $AGL(1, n)$ and $PGL(2, n)$, where $n = p^k$, together with the coset defined by the single Frobenius endomorphism $f(x) = x^p$, has pairwise Hamming distance $n - p$.

Using a coset technique and computations involving random choices, we give several improved lower bounds for $M(n, d)$, For example, we show that $M(13, 5) \geq 6,639,048$ and $M(14, 5) \geq 58,227,624$, which improve previous lower bounds.

2 New theoretical bounds

In this section we use group-theoretic techniques to obtain lower bounds on the sizes of permutation arrays with relatively large Hamming distance. First we consider permutation arrays obtained from semilinear groups over finite fields. Then we investigate a general procedure of modifying permutation arrays called contraction, and prove sharp Hamming distance bounds which involve the cycle structure of permutations in the permutation array.

[1] A factor of k is *proper* if it is smaller than k.

Let $\mathbb{F}_n$ be a field of order n. Then $n = p^k$, where p is a prime number throughout the remainder of the paper. A polynomial $f(x) \in \mathbb{F}_n[x]$ is called a *permutation polynomial* if it is injective. In this case, f permutes the elements of $\mathbb{F}_n$.

We consider the affine general semilinear group $A\Gamma L(1, n)$ and the projective general semilinear group $P\Gamma L(2, n)$. These groups are described in the appendix. It is well known that, for any permutations $\tau, \sigma, \rho \in S_n$, $hd(\sigma\tau, \sigma\rho) = hd(\tau, \rho)$.

The following lemma shows that computing the Hamming distance of a group G does not require computing the Hamming distance between all the pairs of element in G. It shows that the computation time is $O(|G|)$ rather than $O(|G|^2)$. For PA's A and B, $hd(A, B) = \min\{hd(\alpha, \beta) \mid \alpha \in A, \beta \in B\}$. If A consists of one permutation α we use $hd(\alpha, B) = hd(A, B)$.

Lemma 1 *Let G be a group of permutations $G \subseteq S_n$ with $|G| > 1$. The Hamming distance of G, i.e. $hd(G)$, equals $hd(e, G \setminus \{e\})$, where e is the identity permutation.*

Proof Pick any two distinct permutations $a, b \in G$. Then, $hd(a, b) = hd(e, a^{-1}b)$. Since $a^{-1}b$ is in G and is not the identity, the result follows. □

Lemma 2 *Let G and H be subgroups of S_n, such that $G = \cup_{0 \le i \le r} a_i H$, for some $r > 0$, where $a_0 = e$. Then,*

$$hd(G) = \min(\{hd(a_i, H) \mid 0 < i \le r\}, hd(e, H \setminus \{e\})).$$

Proof Observe that, since $G = \cup_{0 \le i \le r} a_i H$, then $G = \cup_{0 \le i \le r} H a_i^{-1}$. Indeed, if $g \in G$, then $g = a_i h$ for some $0 \le i \le r$ and $h \in H$. Then $g^{-1} \in G$ and $g^{-1} = h^{-1}a_i^{-1} \in Ha_i^{-1}$. So,

$$\begin{aligned} hd(G) &= \min(\{hd(e, a_i H) \mid 0 < i \le r\}, hd(e, H \setminus \{e\})) \\ &= \min(\{hd(e, Ha_i^{-1}) \mid 0 < i \le r\}, hd(e, H \setminus \{e\})) \\ &= \min(\{hd(a_i, H) \mid 0 < i \le r\}, hd(e, H \setminus \{e\})). \end{aligned}$$

□

Theorem 1 *The Hamming distance of $A\Gamma L(1, n)$ is $n - p^{k^*}$, where $n = p^k$ and k^* denotes the largest proper factor of k.*

Before we give a proof of Theorem 1, we show some of its applications. Since $A\Gamma L(1, n)$ contains $kn(n-1)$ elements, we conclude the following.

Corollary 1 *Let $n = p^k$ and let k^* be the largest proper factor of $k \ge 1$. Then $M(n, n - p^{k^*}) \ge kn(n-1)$. In particular,*

$$M(n, n-2) \ge kn(n-1), \qquad n = 2^k,$$

where k is prime. For example, $M(2048, 2046) \ge 11 \cdot 2048 \cdot 2047 = 46114816$.

Corollary 2 *Let $n = p^k$ for any $k \ge 1$. Let s be the smallest prime factor of k. Then $M(n, n-p) \ge s \cdot n(n-1)$. For example,*

$$\begin{aligned} M(16, 14) &\ge 2 \cdot 16 \cdot 15 = 480 \\ M(64, 62) &\ge 2 \cdot 64 \cdot 63 = 8064 \\ M(81, 78) &\ge 2 \cdot 81 \cdot 80 = 12960 \\ M(256, 254) &\ge 2 \cdot 256 \cdot 255 = 130560 \\ M(512, 510) &\ge 3 \cdot 512 \cdot 511 = 784896. \end{aligned}$$

Using the following lemma, one can compute the Hamming distance simply by counting roots of polynomials.

For any polynomial f with coefficients over a finite field $\mathbb{F}_n$, let $r(f)$ denote the number of roots of f in $\mathbb{F}_n$. If f and g are polynomials[2] that define permutations on $\mathbb{F}_n$, then the Hamming distance between the permutations f and g is equal to n minus the number of roots in the polynomial $f - g$, i.e. $hd(f, g) = n - r(f - g)$. This is easily seen by observing that $f(x) = g(x)$ is equivalent to $f(x) - g(x) = 0$; in other words, x is a root of the polynomial $f - g$.

Lemma 3 *For any distinct polynomials $f, g \in \mathbb{F}_n[x]$ we have*

$$hd(f, g) = n - r(f - g).$$

The number of roots of polynomials of $AGL(1, n)$ and Frobenius mappings is well known but we give a proof for completeness.

Proof of Theorem 1 Let $H = AGL(1, n)$. Since $A\Gamma L(1, n) = \cup_{0 \le i < k} x^{p^i} H$ and $hd(H) = n - 1$, by Lemma 2 it suffices to prove $hd(x^{p^i}, H) \ge n - p^{k^*}$ for all $1 \le i < k$. By Lemma 3, it suffices to prove $r(x^{p^i} + ax + b) \le p^{k^*}$ for any $1 \le i < k$, and $a \ne 0, b \in \mathbb{F}_n$. Fix $a \ne 0, b \in \mathbb{F}_n$. We show that

$$r(t_{a,b}(x)) \le r(t_a(x)) \le r(t(x)), \tag{1}$$

where $t_{a,b}(x) = x^{p^i} + ax + b$, $t_a(x) = x^{p^i} + ax$, and $t(x) = x^{p^i} - x$.

If $t_{a,b}(x)$ has no root in $\mathbb{F}_n$, then clearly $r(t_{a,b}(x)) \le r(t_a(x))$. Suppose that $t_{a,b}(x)$ has a root, say y_0. For any root y of $t_{a,b}(x)$, we have $t_a(y - y_0) = (y - y_0)^{p^i} + a(y - y_0) = y^{p^i} - y_0^{p^i} + ay - ay_0 = t_{a,b}(y) - t_{a,b}(y_0) = 0$, where the second equality follows from the property $(a + b)^p = a^p + b^p$ of Frobenius endomorphisms [4]. Thus, $y - y_0$ is a root of t_a. Since the mapping $y \to (y - y_0)$ is an injection, the first inequality of (1) follows.

We prove the second inequality of (1), by showing $r(s_a(x)) \le r(s(x))$, where $s_a(x) = t_a(x)/x = x^{p^i - 1} + a$, and $s(x) = t(x)/x = x^{p^i - 1} - 1$. Suppose that $a = 0$. Then 0 is the only root of $s_a(x)$. Since $s(x)$ also has the root 1, the inequality is trivially true. So, assume that $a \ne 0$. Then 0 is not a root of $s_a(x)$. We may also assume that $s_a(x)$ has at least one root; otherwise, the inequality is trivially true. Let z_0 be a root of $s_a(x)$. As z ranges over all roots of $s_a(x)$, map z to z/z_0. Observe that:

$$s\left(\frac{z}{z_0}\right) = \left(\frac{z}{z_0}\right)^{p^i - 1} - 1 = \frac{z^{p^i - 1}}{z_0^{p^i - 1}} - 1 = \frac{-a}{-a} - 1 = 0.$$

So, z/z_0 is a root of $s(x)$. Since the map is injective, it follows that $r(t_a(x)) \le r(t(x))$.

Let S be the set of all roots of $t(x) = x^{p^i} - x$. Observe that S forms a finite field, since the set of roots are closed under the operations of addition, multiplication, and division. Thus, S is a subfield of $\mathbb{F}_n$, and hence the cardinality of S divides the cardinality of $\mathbb{F}_n$, which is p^k. So, $|S| = p^j$, for some j, where $j \mid k$. Now consider the extension of $t(x) = x^{p^i} - x$ into its splitting field [9,16]. In this field, the expanded root set forms $\mathbb{F}_{p^i}$. So, S is a subfield of $\mathbb{F}_{p^i}$, and so $j \mid i$. Thus, j divides both i and k, i.e. $j = r(t(x)) \le p^{gcd(i,k)} \le p^{k^*}$. □

Theorem 2 *The Hamming distance of $P\Gamma L(2, n)$ is $n - p^{k^*}$, where k^* denotes the largest proper factor of k.*

[2] Since f and g are bijections, they correspond to permutations.

Proof From the definition of $P\Gamma L(2,n)$ we have

$$f(x)=\begin{cases}\frac{ax^{p^i}+b}{cx^{p^i}+d} & \text{if } x\in\mathbb{F}_n \text{ and } cx^{p^i}+d\neq 0,\\ \infty & \text{if } x\in\mathbb{F}_n, cx^{p^i}+d=0 \text{ and } ax^{p^i}+b\neq 0,\\ a/c & \text{if } x=\infty \text{ and } c\neq 0,\\ \infty & \text{if } x=\infty, c=0 \text{ and } a\neq 0.\end{cases}$$

It follows that $S=\text{STABILIZER}_{P\Gamma L(2,n)}(\infty)$ is isomorphic to $A\Gamma L(1,n)$.[3] So, $hd(S)=hd(A\Gamma L(1,n))=n-p^{k^*}$ by Theorem 1. Observe that $P\Gamma L(2,n)=\cup_{k=0}^{n-1}\pi_k S$, where π_k $(1\leq k<n)$ is a permutation in $P\Gamma L(2,n)$ that maps k to ∞, and π_0 is the identity permutation. (Such permutations are in $P\Gamma L(2,n)$, because it is sharply 3-transitive and hence 2-transitive.) By Lemma 2,

$$hd(P\Gamma L(2,n))=\min(\{hd(\pi_i,S)\mid 1\leq i<n\},\{hd(e,S-\{e\})).$$

As $hd(\pi_i,S)=hd(S)=hd(A\Gamma L(1,n))\geq n-p^{k^*}$, the result follows. □

Since $P\Gamma L(2,n)$ contains $k(n+1)n(n-1)$ elements, we conclude the following.

Corollary 3 *Let $n=p^k$ for any $k\geq 1$. Let k^* be the largest proper factor of k. Then $M(n+1,n-p^{k^*})\geq k(n+1)n(n-1)$. In particular when $n=2^p$, we have $M(n+1,n-2)\geq p(n+1)n(n-1)$ and therefore*

$$\begin{aligned}M(9,6)&\geq 3\cdot 9\cdot 8\cdot 7=1512\\ M(17,14)&\geq 2\cdot 17\cdot 16\cdot 15=8160\\ M(28,24)&\geq 3\cdot 28\cdot 27\cdot 26=58968\\ M(33,30)&\geq 5\cdot 33\cdot 32\cdot 31=163680.\end{aligned}$$

2.1 Contraction

In this section we describe a general method of modifying a permutation array called *contraction*. Contraction allows one to transfer a permutation array from S_n to S_{n-m} without affecting the Hamming distance by too much. First, we explain the idea of contraction for $m=1$.

The *contraction* of a permutation σ on S_n, denoted by σ^{CT}, is the permutation on S_{n-1} defined by the following, where $0\leq x\leq n-2$:

$$\sigma^{CT}(x)=\begin{cases}\sigma(x) & \text{if } \sigma(x)\neq n-1, \text{ and}\\ \sigma(n-1) & \text{if } \sigma(x)=n-1.\end{cases}\tag{2}$$

That is, the contraction σ^{CT} of σ is formed by substituting $\sigma(n-1)$ for $n-1$ and deleting the symbol $n-1$ altogether. For instance, if $\sigma(n-1)=n-1$, then σ^{CT} is formed by simply deleting the symbol $n-1$. For a PA A on S_n, let $A^{CT}=\{\sigma^{CT}\mid\sigma\in A\}$. In general, as the contraction operation leaves most of any permutations values untouched, the Hamming distance of A^{CT} (as we shall see) is at least as large as three less than the Hamming distance of A itself (see also [23]). Specifically, a decrease of three in the Hamming distance between two permutations ρ and σ occurs if and only if, for some integers $i,j<n-1$, and symbols $r,s<n-1$: (a) $\rho(i)=n-1$ and $\sigma(i)=r$, (b) $\rho(j)=s$ and $\sigma(j)=n-1$, and (c)

[3] Recall that, for a permutation group G on a set X, the *stabilizer* of an element $x\in X$ is the set of permutations $\{g\in G: g(x)=x\}$.

$\rho(n-1) = r$ and $\sigma(n-1) = s$. This is illustrated in Fig. 1. It follows that there is a decrease of three in the Hamming distance between ρ and σ if and only if the permutation $\rho^{-1}\sigma$ contains the cycle $(n-1\ r\ s)$ of length 3. If A is a group, since the order of a 3-cycle is three, the order of the group must be divisible by 3 (by Lagrange's theorem [4]). So, if A is a group whose order is not divisible by 3, there can be no 3-cycle and, therefore, the contraction operation decreases the Hamming distance by at most 2.

Of course the contraction operation can be applied iteratively. One can first contract to a permutation on S_{n-1}, then S_{n-2}, then S_{n-3}, ... We investigate conditions on the group A that is contracted in order to understand the number of times successive contractions decrease the Hamming distance by 2.

Lemma 4 *Let σ and τ be two permutations in S_n. If $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 2$ then* (i) *$n-1$ is in a cycle C of length at least two in the cycle decomposition of $\sigma^{-1}\tau$, and* (ii) *the cycle decomposition of $(\sigma^{CT})^{-1}\tau^{CT}$ is the same except that the length of C is decreased by two by removing $n-1$ and either the next or the previous element in C.*

Proof (i) follows from the fact that, if σ and τ have $n-1$ in the same position, then $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau)$.
(ii) Consider Fig. 2. If one of the permutations, say σ, has $n-1$ in position $n-1$, then $\sigma(i) = \tau(n-1)$ where i is the position of $n-1$ in τ (because $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 2$). Then $C = (\sigma(i)\ \ n-1)$ and it is deleted in the cycle decomposition of $(\sigma^{CT})^{-1}\tau^{CT}$.
Suppose that $\sigma(n-1) \neq n-1 \neq \tau(n-1)$ as shown in Fig. 3.
Since $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 2$, either $b = c$ or $a = d$. Then the cycle C containing $n-1$ is $(a\ n-1\ b\ d\ldots)$ or $(b\ a\ n-1\ c\ldots)$ respectively. The corresponding cycles in $(\sigma^{CT})^{-1}\tau^{CT}$ are $C - \{n-1, b\}$ and $C - \{a, n-1\}$. The lemma follows. □

Theorem 3 *Suppose a permutation array $P \subset S_n$ has Hamming distance d. Let $Q \subseteq S_{n-2}$ denote the permutation array obtained from P by applying the contraction operation two times.*

(a) *The Hamming distance of Q is at least $d-6$.*
(b) *Suppose, for any $\sigma, \tau \in P$, the cycle decomposition of $\sigma^{-1}\tau$ contains no 3-cycle and no 5-cycle. Then the Hamming distance of Q is at least $d-4$.*

Fig. 1 Illustration of contraction operation making two new agreements

positions	...	i	...	j	...	$n-1$
$\rho =$	...	$n-1$	...	s	...	r
$\sigma =$	...	r	...	$n-1$	...	s

Fig. 2 Two permutations where $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 2$ and $\sigma(n-1) = n-1$

positions	...	i	...	$n-1$
$\sigma =$	...	s	...	$n-1$
$\tau =$	...	$n-1$	...	s

Fig. 3 Two permutations where $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 2$ and $\sigma(n-1) \neq n-1 \neq \tau(n-1)$

positions	...	i	...	j	...	$n-1$
$\sigma =$	...	$n-1$	...	a	...	b
$\tau =$	...	c	...	$n-1$	...	d

Fig. 4 Two permutations where $(\sigma')^{-1}\tau'$ contains a 3-cycle

positions	$\ldots$	i	$\ldots$	j	$\ldots$	$n-2$
$\sigma' =$	$\ldots$	b	$\ldots$	$n-2$	$\ldots$	a
$\tau' =$	$\ldots$	$n-2$	$\ldots$	a	$\ldots$	b

Proof The part (a) follows form the fact that the Hamming distance decreases by at most three for each contraction operation.

We prove part (b). Suppose to the contrary that $hd(Q) \leq d-5$. Let σ and τ be two permutations of P such that $hd(\sigma'', \tau'') \leq d-5$ where $\sigma'' = (\sigma')^{CT}$, $\tau'' = (\tau')^{CT}$ and $\sigma' = \sigma^{CT}$, $\tau' = \tau^{CT}$. Since $\sigma^{-1}\tau$ contains no 3-cycle, $hd(\sigma', \tau') = d-2$. Then the contraction operation on σ' and τ' decreases the Hamming distance by exactly three. Therefore $(\sigma')^{-1}\tau'$ contains a 3-cycle as shown in Fig. 4.

Since $\sigma^{-1}\tau$ contains no 3-cycle and $hd(\sigma', \tau') = d-2$, by Lemma 4, $\sigma^{-1}\tau$ contains a 5-cycle. This is a contradiction. □

Corollary 4 (Contraction of $AGL(1, n)$)

(i) *For each prime power n such that* $3 \nmid (n-1)$,

$$M(n-1, n-3) \geq n(n-1).$$

(ii) *For each prime power n such that* $n \equiv 2 \pmod 3$ *and* $n \not\equiv 0, 1 \pmod 5$,

$$M(n-2, n-5) \geq n(n-1).$$

Proof The bounds can be obtained by applying the contraction operation on the affine general linear group $AGL(1, n)$. Let σ and τ be any two distinct permutations from $AGL(1, n)$. Suppose that $n \equiv 2 \pmod 3$. Since $\sigma^{-1}\tau \in AGL(1, n)$ and the order of $AGL(1, n)$ is not a multiple of 3, the bound of (i) follows. If $n \equiv 0 \pmod 3$, then suppose σ and τ are such that $hd(\sigma, \tau) = n$. If $hd(\sigma^{CT}, \tau^{CT}) = hd(\sigma, \tau) - 3$, then $hd(\sigma^{CT}, \tau^{CT}) \geq n-3$ and the Hamming distance bound for (i) is satisfied. Since $hd(AGL(1, n)) \geq n-1$, the other case is that σ and τ are such that $hd(\sigma, \tau) = n-1$. In this case σ and τ have one agreement, say at position i. Then $\sigma\tau^{-1} \in \text{STABILIZER}_i(AGL(1, n))$, which is a cyclic group C of order $n-1$. If $3 \nmid (n-1)$, then there can be no 3-cycle in C and, hence, $(\sigma\tau^{-1})^{-1} = \tau\sigma^{-1}$ has no 3-cycle. So, $hd(\sigma^{CT}, \tau^{CT}) = hd(\tau^{CT}, \sigma^{CT}) \geq hd(\sigma, \tau) - 2$. It follows that $hd(\sigma^{CT}, \tau^{CT}) \geq n-3$.

The bound of (ii) follows from Theorem 3(b) and the fact that the order of $AGL(1, n)$ is not a multiple of 3 and 5. □

Infinitely many new bounds can be obtained from Corollary 4. We show some examples.

$$M(31, 29) \geq 32 \cdot 31 = 992 \quad \text{for } n = 32,$$
$$M(40, 38) \geq 41 \cdot 40 = 1640 \quad \text{for } n = 41,$$
$$M(46, 44) \geq 47 \cdot 46 = 2162 \quad \text{for } n = 47.$$

Previously, the best lower bounds for these examples were

- $M(31, 29) \geq 930$, which was derived from $|AGL(1, 31)| \geq 930$ and $M(n, d-1) \geq M(n, d)$ [5],
- $M(40, 38) \geq 280$, since $M(40, 39) \geq 280$, as there are 7 MOLS for $n = 40$ [6],
- $M(46, 44) \geq 270$, since $M(46, 45) \geq 270$, as there are 6 MOLS for $n = 35$ [6],

Theorem 4 *For each prime power q such that* $3 \nmid (q-1)$,

$$M(q, q-3) \geq (q+1)q(q-1).$$

Proof Let $A_q = (PGL(2, q+1))^{CT}$. It suffices to show that $hd(A_q) \geq q-3$. Consider two permutations σ and τ from $PGL(2, q+1)$. If $hd(\sigma, \tau) = q+1$ then $hd(\sigma^{CT}, \tau^{CT}) \geq q-2$. Suppose that $hd(\sigma, \tau) \leq q$. Then $\sigma^{-1}\tau$ has a fixed point k. A point stabilizer of $PGL(2, n)$ is isomorphic to the affine general linear group $AGL(1, q)$. Since $3 \nmid (q-1)$, by Corollary 4, $hd(\sigma^{CT}, \tau^{CT}) \geq q-3$ and the claim follows. □

Examples

(1) $M(32, 29) \geq 32736$, since $M(33, 31) \geq 32736$, using $PGL(2, 2^5)$.
(2) $M(29, 26) \geq 24360$, since $M(30, 28) \geq 24360$, using $PGL(2, 29)$.
(3) $M(41, 38) \geq 68880$, since $M(42, 40) \geq 68880$, using $PGL(2, 41)$.

Previously, the best lower bounds for these examples were

(1) $M(32, 29) \geq 29760$, since $M(32, 30) \geq 29760$, using $PGL(2, 31)$.
(2) $M(29, 26) \geq 19656$, since $M(28, 26) \geq 19656$, using $PGL(2, 3^3)$.
(3) $M(41, 38) \geq 1640$, since $M(41, 40) \geq 1640$, using $AGL(1, 41)$.

The following is an improvement on Corollary 4.

Corollary 5 *For each prime power n such that* $3 \nmid (n-1)$,

$$M(n-1, n-3) \geq n^2 - 1.$$

Proof By Theorem 4, $M(n, n-3) \geq (n+1)n(n-1)$. By the combinatorial theorem [5] for all d, $M(n-1, d) \geq M(n, d)/n$. So, $M(n-1, n-3) \geq (n+1)n(n-1)/n = n^2 - 1$. □

Examples.

(1) $M(31, 29) \geq 1056$,
(2) $M(40, 28) \geq 1680$, and
(3) $M(46, 44) \geq 2208$.

3 Experimental results

Computer searches for arrays of permutations on Z_n with pairwise Hamming distance d are difficult. The number of all permutations, namely $n!$, is large, even for small values of n. Many previous search methods have used automorphism groups to factor the space of all permutations into collections of sets of permutations with considerably smaller cardinality [5, 14,21]. With this smaller cardinality, one constructs a graph $G(n, d)$, whose nodes correspond to sets of permutations, with an edge between two sets S_1 and S_2 if the Hamming distance between permutations in the sets is at least d [5,14,21]. One then uses a program to find a large clique in $G(n, d)$.

We give a different type of algorithm. We call it the *coset method*. We start with a group G that forms a good PA for $M(n, d')$, where $d' > d$. As exact values for $M(q, q-1)$ arise from sharply 2-transitive groups $AGL(1, q)$, and exact values of $M(q+1, q-1)$ arise from sharply 3-transitive groups $PGL(2, q)$, where q is a power of a prime, one easily finds a group with which to start. Also, the exact value of $M(n, n)$, for all n, arises from a cyclic group of order n. So, in fact, there is always a group with which to start. We search for a permutation, say π, at Hamming distance at least d from G. It follows that the entire coset πG is at distance at least d from G. That is,

$$\begin{aligned} hd(\pi G, G) &= \max\{hd(\pi g_1, g_2) \mid g_1, g_2 \in G\} \\ &= \max\{hd(\pi, g_2 g_1^{-1} \mid g_1, g_2 \in G\} \\ &= \max\{hd(\pi, g) \mid g \in G\}, \end{aligned}$$

since $g_2 g_1^{-1} \in G$ by properties of a group. So, one has a PA of cardinality $2 \cdot |G|$, by finding a single permutation π. Moreover, recording the coset representative π is sufficient, as all other permutations in the coset are obtained from the group G and π.

The process can be iterated. Suppose we have found k coset representatives π_0, $\pi_1, \ldots, \pi_{k-1}$, where π_0 is the identity permutation, so $\pi_0 G$ is the group G and the collection of all such cosets is a PA of cardinality $k \cdot |G|$. One can continue by finding a permutation π_k such that $hd(\pi_k, \pi_i G) \geq d$, for all $0 \leq i < k$. Such a permutation gives us a new coset, namely $\pi_k G$, and a PA of cardinality $(k+1) \cdot |G|$.

One implementation of this method guesses a new permutation π_k randomly and then checks (1) that $hd(\pi_k, \pi_i G) \geq d$, for all $0 \leq i < k$, and (2) $hd(\pi_k, \pi_i G) = d$, for some i $(0 \leq i < k)$. The second condition may need explanation. Recall the combinatorial Gilbert-Varshimov (GV) lower bound [10,17,20] for $M(n, d)$, namely $N_{GV}(n, d)$, where $N_{GV}(n, d)$ is given by:

$$N_{GV}(n, d) = \frac{n!}{V(n, d-1)}, \tag{3}$$

where $V(n, d-1)$, the number of permutations that are at distance less than d from a given permutation, e.g. the identity, is $V(n, d-1) = \sum_{k=0}^{d-1} \binom{n}{k} D_k$, where D_k is the number of *derangements* on k symbols. Note that the ratio given in (3) is a lower bound for the number of times one can select another permutation without choosing two with Hamming distance less than d. It is calculated with the assumption that all sets of permutations too close to different permutations are disjoint. (It should be noted that one can often get far more than $N_{GV}(n, d)$ permutations in a PA, because the assumption that the spheres are disjoint is not required. In fact, this combinatorial lower bound has recently been improved, see [11] and [24].) Of course, such sets need not be disjoint and one can choose a larger set of permutations by eliminating this condition. We do this by requiring each new permutation selected is at distance *exactly* d to one chosen before.

This simple technique makes it feasible to compute and verify large PA's. Previously, the implicit algorithm justifying the GV lower bound was not considered practical, due to large space requirements for keeping track of permutations already chosen and the large time needed for computing Hamming distances. As we have seen in Lemma 1, when the PA is a group and some of its cosets, one need not check the distance between every pair of permutations and one can store the set of coset representatives instead of the set of all permutations. It is worth noting that in [5], the authors computed a PA of size 58,322 for $M(16, 9)$ and stated that this lower bound is not as good as what is given by the GV lower bound.[4] They stated, "... However, the GV lower bound is not constructive." On the other hand, the coset method starting with the group $G = AGL(1, 16)$ found 5, 739 cosets of G for Hamming distance 9 and, hence, obtained a lower bound of 1, 377, 360 for $M(16, 9)$.

Also, in [21] the authors computed a PA of size 20, 908, 800 for $M(12, 4)$ and then stated "... it is too large to check fully, but has been extensively checked." In contrast, the coset method starting with the Mathieu group G of order 12 [4,7,8] found 638 cosets of G for Hamming distance 4 and, hence, obtained a lower bound of 60, 635, 520 for $M(12, 4)$. Furthermore, since testing of correctness of G and its cosets takes far less time using group-theoretic properties, verification was done in a few minutes using a computer.

[4] Note that $N_{GV}(16, 9) = 97, 579$.

Verifying the Hamming distance of a PA A on Z_n of size N generally involves computing $\binom{N}{2}$ pairs of permutations of n symbols, which is $O(N^2 n)$ time. When A is a group, using Lemma 1, one only need compute the distance between the identity and the other $N-1$ elements, so $O(Nn)$ time. In fact, if A is a group consisting of the identity permutation and its cyclic shifts or A consists of this cyclic group and, say, k of its cosets, the computation time is reduced to $O(N)$ and $O(kN)$, respectively. We discuss testing algorithms in Sect. 3.1.

The coset method has been used to obtain several new lower bounds. Many of the new lower bounds are given in Tables 1 and 2. The PA's that justify the lower bounds are available at our web site [22]. Sometimes finding a suitable coset representative takes considerable computation time and, hence, when found it should be recorded. For example, when started with the group $G = PGL(2, 19)$ the coset method with difficulty found one coset of G for Hamming distance 16. It can be described by one of its representatives, for example:

$$0, 1, 2, 3, 5, 7, 14, 4, 18, 17, 9, 6, 16, 15, 11, 19, 8, 10, 12, 13,$$

where 19 represents ∞. Thus, $M(20, 16) \geq 13,680$. Some other lower bounds obtained are:

$$\begin{aligned}
M(13, 5) &\geq 10,454,400\\
M(13, 6) &\geq 1,805,760\\
M(13, 7) &\geq 380,160\\
M(14, 5) &\geq 60,445,440\\
M(14, 6) &\geq 10,834,560\\
M(14, 7) &\geq 1,900,800\\
M(14, 8) &\geq 380,160\\
M(14, 9) &\geq 21,840\\
M(15, 6) &\geq 58,734,720\\
M(15, 7) &\geq 15,491,520\\
M(15, 8) &\geq 1,900,800\\
M(15, 9) &\geq 181,272\\
M(15, 10) &\geq 32,760\\
M(16, 7) &\geq 70,709,760\\
M(16, 8) &\geq 16,061,760\\
M(16, 9) &\geq 1,377,360\\
M(16, 10) &\geq 164,880.
\end{aligned}$$

Others can be found in Tables 1 and 2 and at the website.

3.1 Efficient testing of a new permutation

Suppose that we have a permutation array P consisting of k left cosets of a group G, i.e. $P = \cup_{i=1}^{k} P_i$. The critical step of our randomized construction is the computation of distance $hd(\pi, P)$ where π is a random permutation. The definition of Hamming distance suggests the computation $hd(\pi, P) = \min_{\sigma \in P} hd(\pi, \sigma)$. Then the running time is $O(n|P|) = O(nk|G|)$. We show that, if G is cyclic or has the cyclic subgroup, the algorithm for testing π can be improved. Let C_n denote the cyclic group, i.e.,

$$C_n = \{g_j \mid g_j = (j, j+1, \ldots, n-1, 0, 1, \ldots, j-1), j \in Z_n\}.$$

Table 1 Bounds for $M(n, d)$ for $9 \leq n \leq 17$

	d = 4	d = 5	d = 6	d = 7	d = 8	d = 9	d = 10	d = 11	d = 12	d = 13	d = 14	d = 15	d = 16
9	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	–	–	–	–	–	–	–	–	–	–
	$18{,}576_C$	3024_E	1512_E	504_g	72_g	9	–	–	–	–	–	–	–
10	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	**1504_u**	–	–	–	–	–	–	–	–	–
	$150{,}480_E$	$19{,}440_C$	8640_E	1484_C	720_g	49_D	10	–	–	–	–	–	–
11	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	–	–	–	–	–	–	–	–	–	–
	$1{,}742{,}400_E$	$205{,}920_E$	$95{,}040_E$	7920_a	7920_g	297_C	110_g	11	–	–	–	–	–
12	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	–	–	–	–	–	–	–	–	–	–
	$20{,}908{,}800_E$	$2{,}376{,}000_E$	$190{,}080_E$	$95{,}040_a$	$95{,}040_g$	1320_a	1320_g	112_C	12	–	–	–	–
13	638	110	20	4	–	–	–	–	–	–	–	–	–
	$60{,}635{,}520_r$	**$10{,}454{,}400_r$**	**$1{,}900{,}800_r$**	**$380{,}160_r$**	–	–	–	–	–	–	–	–	–
	$41{,}712{,}480_A$	$2{,}376{,}000_b$	$271{,}908_t$	$95{,}040_a$	$95{,}040_b$	6474_C	1320_b	276_C	156_g	13	–	–	–
14	–	636	115	21	4	10	–	–	–	–	–	–	–
	–	**$60{,}445{,}440_r$**	**$10{,}929{,}600_r$**	**$1{,}995{,}840_r$**	**$380{,}160_r$**	**$21{,}840_r$**	–	–	–	–	–	–	–
	$550{,}368{,}000_A$	$22{,}767{,}826_B$	$890{,}338_t$	$97{,}547_t$	$95{,}040_b$	6552_a	8736_C	2184_a	2184_g	59_C	14	–	–
15	–	–	618	163	20	83	15	–	–	–	–	–	–
	–	–	**$58{,}734{,}720_r$**	**$15{,}491{,}520_r$**	**$1{,}900{,}800_r$**	**$181{,}272_r$**	**$32{,}760_r$**	–	–	–	–	–	–
	4.01E9$_B$	$263{,}832{,}788_B$	$8{,}991{,}655_t$	$888{,}533_t$	$97{,}572_t$	$12{,}014_t$	6076_a	7540_C	2520_d	315_C	90_C	15	–

Table 1 continued

	d = 4	d = 5	d = 6	d = 7	d = 8	d = 9	d = 10	d = 11	d = 12	d = 13	d = 14	d = 15	d = 16
16	–	–	–	744	169	5739	687	–	–	–	–	–	–
	–	–	–	**70,709,760**$_r$	**16,061,760**$_r$	**1,377,360**$_r$	**164,880**$_r$	–	–	–	–	–	–
	1.268E11$_B$	3.317E9$_B$	–	8,972,298$_t$	888,755$_t$	97,579$_t$	40,320$_a$	40,320$_a$	40,320$_E$	1376$_C$	1376$_C$	240$_g$	16
17	–	–	–	–	791	2298	303	46	–	3	–	–	–
	–	–	–	–	**75,176,640**$_r$	**9,375,840**$_r$	**1,236,240**$_r$	**187,680**$_r$	–	**12,240**$_r$	**8160**	–	–
	7.93E11$_B$	–	–	–	8,974,885$_t$	888,727$_t$	97,569$_t$	12,014$_t$	83,504$_A$	4080$_a$	4080$_a$	4080$_g$	272$_g$

Bold values indicate improved bounds

Table 2 Bounds for $M(n, d)$ for $18 \leq n \leq 26$

	d = 11	d = 12	d = 13	d = 14	d = 15	d = 16	d = 17	d = 18	d = 19	d = 20	d = 21	d = 22	d = 23	d = 24
18	251	40	5	–	–	–	–	–	–	–	–	–	–	–
	1,228,896$_r$	**195,840**$_r$	**24,480**$_r$	**12,240**$_u$	**8160**$_u$	–	–	–	–	–	–	–	–	–
	97,569$_t$	83,504$_t$	4896$_a$	4896$_a$	4896$_a$	4896$_g$	90$_C$	18	–	–	–	–	–	–
19	–	3572	486	–	–	–	–	–	–	–	–	–	–	–
	–	**1,221,624**$_r$	**166,212**$_r$	–	**12,240**$_G$	–	–	–	–	–	–	–	–	–
	888,729$_t$	97,569$_t$	65,322$_a$	65,322$_F$	–	4896$_b$	342$_a$	342$_g$	19	–	–	–	–	–
20	–	1299	215	28	3	2	–	–	–	–	–	–	–	–
	–	**8,885,160**$_r$	**1,470,600**$_r$	**191,520**$_r$	**20,520**$_r$	**13,680**$_r$	–	–	–	–	–	–	–	–
	8,974,608$_t$	888,729$_t$	97,569$_t$	12,014	65,322	6840$_a$	6840$_a$	6840$_g$	120$_C$	20	–	–	–	–
21	–	–	–	174	23	5	2	–	–	–	–	–	–	–
	–	–	–	**1,190,160**$_r$	**157,320**$_r$	**34,200**$_r$	**13,680**$_u$	–	**333**$_G$	–	–	–	–	–
	–	–	888,729$_t$	97,569$_t$	65,322$_b$	6840$_a$	6840$_a$	6840$_b$	147$_a$	147$_C$	21	–	–	–
22	–	–	–	–	47,233	–	1250	–	–	–	–	–	–	–
	–	–	–	–	**1,039,126**$_r$	–	**27,500**$_r$	**13,680**$_u$	**1100**$_G$	**528**$_d$	**104**$_u$	–	–	–
	–	–	–	–	443,520$_a$	443,520$_g$	6840$_a$	6840$_b$	–	220$_A$	121$_C$	22	–	–
23	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	–	–	–	–	–	**12,144**$_a$	**12,144**$_c$	–	–	–	–
	–	–	–	–	10,200,960$_a$	10,200,960$_g$	291,456$_a$	291,456$_A$	–	–	506$_a$	506$_g$	23	–
24	–	–	–	–	–	–	89	–	2	–	–	–	–	–
	–	–	–	–	–	–	**1,080,816**$_r$	–	**24,288**$_r$	–	–	–	–	–
	–	–	–	–	–	2.44E8$_g$	97,569$_t$	291,456$_b$	23,782$_a$	23,782$_F$	12,144$_a$	12,144$_g$	168$_m$	24

Table 2 continued

	d = 11	d = 12	d = 13	d = 14	d = 15	d = 16	d = 17	d = 18	d = 19	d = 20	d = 21	d = 22	d = 23	d = 24
25	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	–	–	–	–	–	–	–	–	**61,200**$_d$	**15,600**$_a$	**15,600**$_c$	–	–	–
	–	–	–	–	–	–	–	–	–	–	–	12,144$_b$	600$_a$	600$_g$
26	–	–	–	–	–	–	–	–	102	10	2	–	–	–
	–	–	–	–	–	–	–	–	**1,591,200**$_r$	**156,000**$_r$	**31,200**$_r$	–	–	–
	–	–	–	–	–	–	–	–	–	–	12,144$_t$	–	–	15,600$_g$

Bold values indicate improved bounds

Lemma 5 *The Hamming distance from a permutation $\pi \in S_n$ to C_n can be computed in $O(n)$ time.*

Proof The Hamming distance $hd(\pi, C_n)$ can be computed as

$$hd(\pi, C_n) = \min_{0 \le j \le n-1} \{hd(\pi, g_j)\}.$$

The straightforward computation of $hd(\pi, g_j)$ takes $O(n)$ time. We show that it can be computed in $O(1)$ amortized time.

Let $D[0..n-1]$ be an array and we store a tentative distance of $hd(\pi, g_j)$ in $D[j]$. The algorithm has 2 steps.

1. We initialize $D[j] = n$ for all $j \in Z_n$.
2. For each $m \in Z_n$, subtract one from $D[j]$ where $j \equiv (\pi(m) - m) \bmod n$.

Clearly, the running time is $O(n)$. We show that the algorithm is correct. If $D[j]$ decreases for some m, then the m-th element of π is $j + m (\bmod n)$. Thus, π and g_j have matching elements in m-th position. In the end, $D[j]$ is equal to $n - n'$ where n' is the number of matching elements of π and g_j. The claim follows since $hd(\pi, g_j) = n - n'$. □

Lemma 6 *Suppose that $G = C_n$ and let π_i, $(i = 1, 2, \ldots, k)$ be a representative of the coset P_i, i.e. $P_i = \pi_i C_n$. Then, for any permutation $\pi \in S_n$, the Hamming distance $hd(\pi, P)$ can be computed in $O(kn)$ time.*

Proof The Hamming distance $hd(\pi, P)$ can be computed as

$$hd(\pi, P) = hd\left(\pi, \bigcup_{1 \le i \le k} P_i\right) = \min_{1 \le i \le k} \{hd(\pi, P_i\}.$$

It suffices to show that $d_i = hd(\pi, P_i)$ can be computed in $O(n)$ time, for any i. Since $P_i = \pi_i C_n$ and $d_i = hd(\pi_i^{-1}\pi, C_n)$, we first compute $\sigma = \pi_i^{-1}\pi$ and then $hd(\sigma, C_n)$ using the algorithm from Lemma 5. □

We generalize Lemma 6 as follows.

Theorem 5 *If C_n is a subgroup of G then the Hamming distance $hd(\pi, P)$ can be computed in $O(k|G|)$ time for any permutation $\pi \in S_n$.*

Proof Let $G/C_n = \{\sigma C_n \mid \sigma \in G\}$ be the set of left cosets of C_n in G. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be representatives of these cosets. The Hamming distance $hd(\pi, P)$ can be computed as

$$hd(\pi, P) = hd\left(\pi, \bigcup_{1 \le i \le k} \pi_i G\right) = hd\left(\pi, \bigcup_{\substack{1 \le i \le k \\ 1 \le t \le m}} \pi_i \sigma_t C_n\right)$$
$$= \min_{\substack{1 \le i \le k \\ 1 \le t \le m}} \{hd(\pi, \pi_i \sigma_t C_n)\}.$$

Since $hd(\pi, \pi_i \sigma_t C_n) = hd(\alpha, C_n)$ where $\alpha = (\pi_i \sigma_t)^{-1}\pi$. The Hamming distance $hd(\alpha, C_n)$ can be computed in $O(n)$ time using the algorithm from Lemma 5. The total time for computing $hd(\pi, P)$ is $O(kmn)$. It can be written as $O(k|G|)$ since $|G| = mn$. □

4 New tables and conclusions

We give in Tables 1 and 2 an updated partial list of lower bounds for $M(n, d)$, with $n \geq 9$ and $d \geq 4$. We also created a webpage [22] that allows one to obtain the PA's, or coded versions of them, for verification. Not all of our new results appear in the table, many are described by theorems in Sect. 2.

We use the following notation in the table to describe how the results are obtained:

- **a** - a bound derived from $M(n, d-1) \geq M(n, d)$.
- **b** - a bound derived from $M(n+1, d) \geq M(n, d)$.
- **d** - a bound derived from $M(n-1, d) \geq M(n, d)/n$. For example, we have $M(15, 12) \geq 2520$, because $M(16, 12) \geq 40320$.
- **t** - the Gilbert-Varshamov lower bound [10,17,20].
- **g** - a lower bound based on known permutation groups. This includes the Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ and groups $AGL(1, n)$ or $AGL(2, n)$, which are sharply 2-transitive and sharply 3-transitive, respectively.
- **m** - a bound derived from mutually orthogonal Latin squares [6].
- **u** - a result obtained by *partitioning and extending*, which is contained in [2].
- **r** - a result obtained by the coset method using random search. Our improved lower bounds are in bold. The previous lower bounds are given at the bottom of the cell. When a lower bound is obtained by the coset technique, the number of cosets is given at the top of the cell.
- **c** - a result obtained by *contraction*, which is an improvement of the $M(n-1, d-3) \geq M(n, d)$ result, described in [23]. For example, $M(23, 20) \geq 12144$ comes from $M(24, 22) \geq 12144$.

We use capital letters for the following references: A - [5], B - [11], C - [14], D - [15], E - [21], F - [23], G - [1].

We note that $M(9, 6) \geq 1512$ and $M(17, 14) \geq 8160$ follow from Corollaries 1 and 2.

Appendix

Finite Fields Let $n = p^k$ be a prime power. There is a field $\mathbb{F}_n$ with n elements, unique up to isomorphism. We consider groups over the field $\mathbb{F}_n$.

Groups The group $AGL(1, n)$ consists of the affine linear transformations

$$AGL(1, n) = \{ax + b | a, b \in \mathbb{F}_n, a \neq 0\},$$

where the group operation is function composition. This group is sharply 2−transitive and has $n(n-1)$ elements.

Denote the symbols of Z_{n+1} by $0, 1, 2, \ldots, n-1, \infty$. The permutations of $PGL(2, n)$ are $g : x \to \frac{ax+b}{cx+d}$ on Z_{n+1} such that $a, b, c, d \in GF(n), ad \neq bc, g(\infty) = a/c, g(-d/c) = \infty$ if $c \neq 0$ and $g(\infty) = \infty$ if $c = 0$. Then $|PGL(2, n)| = (n+1)n(n-1)$.

Recall that $n = p^k$. The group of affine semilinear polynomials $A\Gamma L(1, n)$ arises as a semidirect product of $AGL(1, n)$ with a cyclic group of order k. It is generated by iteratively composing the Frobenius automorphism x^p with the elements of $AGL(1, n)$. Equivalently,

$$A\Gamma L(1, n) = \{ax^{p^i} + b \mid a, b \in \mathbb{F}_n, a \neq 0, 0 \leq i < k\}$$

This group has $kn(n-1)$ elements.

The group of projective semilinear polynomials $P\Gamma L(2, n)$ arises as a semidirect product of $PGL(2, n)$ with a cyclic group of order k generated by the Frobenius automorphism. This group has $k(n + 1)n(n - 1)$ elements.

References

1. Bereg S., Morales L., Sudborough I.H.: Parallel and sequential partition and extension techniques. Manuscript, The University of Texas Dallas (2016).
2. Bereg S., Morales L., Sudborough I.H.: Extending permutation arrays: improving MOLS bounds. Des. Codes Cryptogr. **83**(3), 661–683 (2017).
3. Blake I.F., Cohen G.D., Deza M.: Coding with permutations. Inform. Control **43**(1), 1–19 (1979).
4. Cameron P.: Permutation Groups. London Mathematical Society Student TextsCambridge University Press, Cambridge (1999).
5. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**(1–3), 51–64 (2004).
6. Colbourn C.J., Kløve T., Ling A.C.H.: Permutation arrays for powerline communication and mutually orthogonal latin squares. IEEE Trans. Inform. Theory **50**(6), 1289–1291 (2004).
7. Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A.: Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups. Clarendon Press, Oxford (1985).
8. Dixon J., Mortimer B.: Permutation Groups. Springer, New York (1996).
9. Dummit D.S., Foote R.M.: Abstract Algebra, 2nd edn. Wiley, New York (1999).
10. Frankl P., Deza M.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory Ser. A **22**(3), 352–360 (1977).
11. Gao F., Yang Y., Ge G.: An improvement on the Gilbert-Varshamov bound for permutation codes. IEEE Trans. Inform. Theory **59**(5), 3059–3063 (2013).
12. Herstein I.N.: Topics in Algebra, 2nd edn. Wiley, New York (1975).
13. Huczynska S.: Powerline communication and the 36 officers problem. Philos. Trans. R. Soc. Lond. A **364**(1849), 3199–3214 (2006).
14. Janiszczak I., Lempken W., Östergård P.R.J., Staszewski R.: Permutation codes invariant under isometries. Des. Codes Cryptogr. **75**(3), 497–507 (2015).
15. Janiszczak I., Staszewski R.: An improved bound for permutation arrays of length 10. Technical Report 4, Institute for Experimental Mathematics, University Duisburg-Essen (2008).
16. Lidl R., Niederreiter H.: Finite Fields, 2nd edn. Cambridge University Press, Cambridge (1997).
17. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland/Elsevier, Amsterdam (1977).
18. Passman D.: Sharp transitivity. In: Permutation Groups. Benjamin, Inc., New York (1968).
19. Pavlidou N., Vinck A.H., Yazdani J., Honary B.: Power lines communications: state of the art and future trends. IEEE Commun. Mag. 34–40 (2003).
20. Pless V.S., H W.C. (eds.): Handbook of Coding Theory. North-Holland/Elsevier, Amsterdam (1998).
21. Smith D.H., Montemanni R.: A new table of permutation codes. Des. Codes Cryptogr. **63**(2), 241–253 (2012).
22. Table of cosets. http://www.utdallas.edu/~sxb027100/cosets.
23. Yang L., Chen K., Yuan L.: New constructions of permutation arrays. arXiv:abs/0801.3987 (2008).
24. Yang L., Chen K., Yuan L.: New lower bounds on sizes of permutation arrays. arXiv:abs/0801.3986 (2008).