# Maximizing Hamming Distance in Contraction of Permutation Arrays

Sergey Bereg * Zevi Miller † Luis Mojica * Linda Morales * I.H. Sudborough*

**Abstract**

Two important examples of permutation arrays for the study of $M(n,d)$ are the Affine General Linear Group $AGL(1,q)$ acting on the finite field $GF(q)$ of size $q$, and the Projective Linear Group $PGL(2,q)$ acting on the set $GF(q) \cup \{\infty\}$ of size $q+1$. Lower bounds for $M(q-1,q-3)$ and $M(q,q-3)$ have been shown when $q \not\equiv 1 (\text{mod } 3)$. Here we consider the case when $q \equiv 1 (\text{mod } 3)$ We give lower bounds for $M(q-1,q-3)$ if $q \geq 7$, and when $q$ is odd for $M(q,q-3)$ if $q \geq 13$.

## 1 Introduction

We consider permutations on a set $\Omega$ of size $n$. Given two such permutations $\pi$ and $\sigma$, we let $hd(\pi,\sigma) = |\{x \in \Omega : \pi(x) \neq \sigma(x)\}|$, so $hd(\pi,\sigma)$ is the number of elements of $\Omega$ at which $\pi$ and $\sigma$ disagree. When $hd(\pi,\sigma) = d$, we say that $\pi$ and $\sigma$ and are at *Hamming distance d*. A *permutation array* A is a set of permutations on $\Omega$. We say that $hd(A) = d$ if $d = min\{hd(\pi,\sigma) : \pi,\sigma \in A\}$. For positive integers $n$ and $d$ with $d \leq n$ we let $M(n,d)$ be the maximum number of permutations in any array $A$ satisfying $hd(A) \geq d$.

The study of permutation arrays began (to our knowledge) with the papers [6] and [9]. In recent years there has been renewed interest in permutation arrays, motivated by applications in power line transmission [8], [14], [17], and [10], block ciphers [16], and in multilevel flash memories [12] and [13]. Some elementary exact values and bounds on $M(n,d)$ are shown in [5]). More sophisticated bounds were proved in [6] and [9], with a recent improvement in [18]. The smallest interesting case for $d$ is $d = 4$, where non-elementary bounds for $M(n,4)$ were developed in [7].

There are various construction methods for permutation arrays. If there are $m$ mutually orthogonal Latin squares (MOLS) of order $n$, then $M(n,n-1) \geq mn$ [4]. Computational approaches for bounding $M(n,d)$ include clique search, and the use of automorphisms, for small $n$ and $d$, are described in [5], [11], [15], permutation polynomials [5], coset search [2], and partition and extension [3].

In this paper we obtain new lower bounds on $M(n,d)$ for $n$ and $d$ near a prime power. Previous results of this kind are given in [5] where it is shown that for $n = 2^k$ with $n \not\equiv 1 (\text{mod } 3)$ we have $M(n,n-3) \geq (n+2)n(n-1)$ and $M(n,n-4) \geq \frac{1}{3}n(n-1)(n^2+3n+8)$.

Our method is to apply a *contraction* operation to the groups $AGL(1,q)$ and $PGL(2,q)$. We obtain the following lower bounds, assuming that $q$ is prime power satisfying $q \equiv 1 \text{ (mod } 3)$;

**1.** for $q \geq 7$, $M(q-1,q-3) \geq (q^2-1)/2$ for $q$ odd and $M(q-1,q-3) \geq (q-1)(q+2)/3$ for $q$ even, and

**2.** for $q \geq 13$, $M(q,q-3) \geq Kq^2 log(q)$ for some constant $K$ if $q$ is odd, and

**3.** bounds for $M(n,d)$ for a finite number of exceptional pairs $n,d$ using the Mathieu groups.

Consider a permutation array $A$ acting on a set $\Omega = \{x_1, x_2, \cdots, x_n\}$ of size $n$, where the elements of $\Omega$ are ordered by their subscripts. We distinguish some element, say $x_n$, by renaming it $F$. Thus the image string of any element $\sigma \in A$ will be $\sigma(x_1)\sigma(x_2)\cdots\sigma(F)$, and we say that $\sigma(x_i)$ occurs in *position* or *coordinate* $x_i$ of the string. Now for any $\pi \in A$, define the permutation $\pi^{\triangle}$ on $\Omega$ by

*Computer Science Dept., University of Texas at Dallas, Richardson, TX 75083, USA
†Dept. of Mathematics, Miami University, Oxford, OH 45056, USA

$$\pi^{\triangle}(x) = \begin{cases} \pi(F) & \text{if } \pi(x) = F, \\ F & \text{if } x = F, \\ \pi(x) & \text{otherwise.} \end{cases}$$

Thus the image string of $\pi^{\triangle}$ is obtained from the image string of $\pi$ by interchanging the symbols $F$ and $\pi(F)$ if $\pi(F) \neq F$, while $\pi^{\triangle} = \pi$ if and only if $\pi(F) = F$. In either case, $\pi^{\triangle}$ has $F$ as its final symbol. We let $\pi^{\triangle}_{-}$ be the permutation on $n-1$ symbols obtained from $\pi^{\triangle}$ by dropping the last symbol $F$ from $\pi^{\triangle}$. As an example, if $\pi = aFbcd$, then $\pi^{\triangle} = adbcF$, and $\pi^{\triangle}_{-} = adbc$. Further, for any subset $R \subset A$, let $R^{\triangle} = \{\pi^{\triangle} : \pi \in R\}$, and $R^{\triangle}_{-} = \{\pi^{\triangle}_{-} : \pi \in R\}$. So $R^{\triangle}_{-}$ is a permutation array on the $n-1$ symbols acting on the set $\Omega - \{F\}$, and is called the *contraction* of $R$.

**Lemma 1** *Let $G$ be a permutation group acting on the set $\Omega$ of size $n$, and $\pi, \sigma \in G$. (a) $hd(\pi^{\triangle}, \sigma^{\triangle}) \geq hd(\pi, \sigma) - 3$. **b)** Assume $hd(\pi^{\triangle}, \sigma^{\triangle}) = hd(\pi, \sigma) - 3$. Then $\pi\sigma^{-1}$ contains a 3-cycle in its disjoint cycle factorization, and $|G|$ is divisible by 3. **c)** Let $S \subseteq G$. Then $|S^{\triangle}| = |S^{\triangle}_{-}|$ and $hd(S^{\triangle}) = hd(S^{\triangle}_{-})$. If also $hd(S) > 3$, then $|S| = |S^{\triangle}|$.*

## 2 The contraction graph for $AGL(1, q)$

Recall the Affine General Linear Group $AGL(1, q)$ acting as permutation group on the finite field $GF(q)$ of size $q$, as the set of transformations $\{x \to ax + b : x, a \neq 0, b \in GF(q)\}$ under the binary operation of composition. Clearly $|AGL(1, q)| = q(q-1)$. It is straightforward to show that $hd(AGL(1, q)) = q - 1$.

For brevity set $H = AGL(1, q)$. We have previously proved that if $q \not\equiv 1 (\text{mod } 3)$, then $hd(H^{\triangle}) \geq q - 3$. Here we investigate the case where $q \equiv 1 (\text{mod } 3)$. The key idea is to find a subset $I \subset AGL(1, q)$ such that $hd(I^{\triangle}) \geq q - 3$. Once we have such an $I$, then $I^{\triangle}_{-}$ is a permutation array on $q - 1$ symbols, and by Lemma 1c satisfies $hd(I^{\triangle}_{-}) \geq q - 3$. This implies the lower bound $M(q-1, q-3) \geq |I^{\triangle}_{-}| = |I|$, since $q \geq 7$ implies $hd(I) \geq q - 1 > 3$. The actual size of $I$ will then yield our precise lower bound.

Consider the *contraction graph* $C_A(q)$ defined by $V(C_A(q)) = AGL(1, q)$, and $E(C_A(q)) = \{\pi\sigma : hd(\pi^{\triangle}, \sigma^{\triangle}) = q-4\}$. Now recall that $hd(AGL(1, q)) = q-1$, so that by Lemma 1 we have $hd(\pi^{\triangle}, \sigma^{\triangle}) \geq q - 4$ for all $\pi, \sigma \in AGL(1, q)$. So if $I$ is an independent set in $C_A(q)$, then $hd(I^{\triangle}) \geq q - 3$. We are thus reduced to finding a large independent set $I$ in $C_A(q)$.

**Lemma 2** *Let $\pi$ and $\sigma$ be vertices of the graph $C_A(q)$, $q \equiv 1 (mod\ 3)$, say with $\sigma(x) = ax + r$ and $\pi(x) = bx + s$. Then, (a) if $a \neq b$, $hd(\pi, \sigma) = q - 1$, (b) if $\pi(F) = F$, then $\pi$ is an isolated point in $C_A(q)$, (c) if $\pi$ and $\sigma$ are neighbors in $C_A(q)$, then (1) $hd(\pi, \sigma) = q-1$, and $hd(\pi^{\triangle}, \sigma^{\triangle}) = hd(\pi, \sigma)-3$, and (2) $\frac{a}{b}$ and $\frac{b}{a}$ are the distinct roots of the quadratic $t^2 + t + 1 = 0$ over $GF(q)$.*

We now define a graph $H(q)$ on the same vertex set as that of $C_A(q)$ which contains $C_A(q)$ as a subgraph. Then any independent set in $H(q)$ is also independent in $C_A(q)$, and thus it suffices to find a suitably large independent set in $H(q)$. The equation $t^2 + t + 1 = 0$ has two distinct roots in $GF(q)$ for $q \equiv 1 \pmod 3$. Also direct substitution shows that if $t$ is a root of this equation, then so is $\frac{1}{t}$. So with Lemma 2 as motivation, let us call two permutations $\pi, \sigma \in AGL(1, q)$, say with $\sigma(x) = ax + r$ and $\pi(x) = bx + s$, *associates* if $\frac{a}{b}$ and $\frac{b}{a}$ are the distinct roots of the quadratic $t^2 + t + 1 = 0$ over $GF(q)$. We then let $V(H(q)) = AGL(1, q)$ and $E(H(q)) = \{\pi\sigma : \pi$ and $\sigma$ are associates$\}$.

**Theorem 3** *Let $q$ be a prime power with $q \equiv 1 \pmod 3$. Then, (a) $H(q)$ is regular of degree 2, (b) Every connected component of $H(q)$ is a cycle of length a multiple of 3, (c) Each connected component $D$ of $H(q)$ contains an independent set of vertices in $C_A(q)$ of size at least: if $q$ is odd, $\lceil \frac{|V(D)|}{2} \rceil$, and if $q$ is even, $\frac{|V(D)|}{3}$.*

**Corollary 4** *Let $q$ be a prime power with $q \equiv 1 \pmod 3$. Then $M(q-1, q-3) \geq (q^2-1)/2$ if $q$ is odd, and $M(q-1, q-3) \geq (q-1)(q+2)/3$ if $q$ is even.*

## 3 The contraction graph for $PGL(2,q)$

Let $q$ be power of a prime. The permutation group $PGL(2,q)$ is defined as the set of one to one functions $\sigma : GF(q) \cup \{\infty\} \to GF(q) \cup \{\infty\}$, under the binary operation of composition, given by

$$\{\ \sigma(x) = \frac{ax+b}{cx+d} \mid a,b,c,d \in GF(q), ad \neq bc, x \in GF(q) \cup \{\infty\}\ \}. \quad (1)$$

Here $\sigma(x)$ is computed by the rules: (1) if $x \in GF(q)$ and $x \neq -(d/c)$, then $\sigma(x) = \frac{ax+b}{cx+d}$, (2) if $x \in GF(q)$ and $x = -(d/c)$, then $\sigma(x) = \infty$, (3) if $x = \infty$, and $c \neq 0$, then $\sigma(x) = a/c$, and (4) if $x = \infty$, and $c = 0$, then $\sigma(x) = \infty$. It is known that $|PGL(2,q)| = (q+1)q(q-1)$.

If $q \not\equiv 1 (\mathrm{mod}\ 3)$, then $hd(PGL(2,q)^{\triangle}) \geq q-3$. Thus, we restrict ourselves to the case $q \equiv 1 (\mathrm{mod}\ 3)$, $q$ an odd prime power. The plan will be similar to the one we used in the previous section. That is, for a certain set $I \subset PGL(2,q)$ we will find a permutation array $I_-^{\triangle} \subset PGL(2,q)_-^{\triangle}$ on $q$ symbols with $hd(I_-^{\triangle}) \geq q-3$, thus obtaining the lower bound on $M(q,q-3) \geq |I_-^{\triangle}|$.

Define the *contraction graph* $C_P(q)$ by $V(C_P(q)) = PGL(2,q)$, and $E(C_P(q)) = \{\pi\sigma : hd(\pi^{\triangle}, \sigma^{\triangle}) = q-4\}$. So edges of $C_P(q)$ correspond to pairs $\pi, \sigma$ for which $hd(\pi^{\triangle}, \sigma^{\triangle})$ achieves its least possible value of $q-4$, occurring when $\pi^{\triangle}$ and $\sigma^{\triangle}$ agree in 5 postions. Thus any independent set $I$ in $C_P(q)$ satisfies $hd(I^{\triangle}) \geq q-3$. By Lemma 1c, we get $hd(I_-^{\triangle}) \geq q-3$, while $|I_-^{\triangle}| = |I^{\triangle}| = |I|$.

Consider $\pi \in PGL(2,q)$, say with $\pi(x) = \frac{ax+b}{cx+d}$, where $x \in GF(q) \cup \{\infty\}$. If $c = 0$, then $\pi(\infty) = \infty$. Thus $\pi$ is an isolated point in $C_P(q)$. Suppose then that $c \neq 0$. Then some manipulation shows that $\pi(x) = \frac{ax+b}{cx+d} = K + \frac{r}{x-i}$, for suitable elements $K, r, i \in GF(q)$, $r \neq 0$, which depend on $\pi$.

**Lemma 5** *Let $q = p^m$, where $p$ is an odd prime, with $q \equiv 1 (mod\ 3)$, $q \geq 13$. Let $\pi, \sigma \in PGL(2,q)$, say with $\pi(x) = a + \frac{r}{x-i}$, $\sigma(x) = b + \frac{s}{x-j}$, $r, s \neq 0$. Then $\pi\sigma \in E(C_P(q)) \Longleftrightarrow r = s$ and $(b-a)(j-i) = r$.*

For any $S \subset CG(q)$, we let $[S]$ be the subgraph of $C_P(q)$ induced by $S$; that is, $V([S]) = S$ and $E([S]) = \{\pi\sigma : \pi, \sigma \in S, \pi\sigma \in E(C_P(q))\}$. When $r$ is fixed by context, we denote a vertex $v = a + \frac{r}{x-i}$ by the abbreviation $(i,a)$.

Consider the partition of $PGL(2,q)$ given by $PGL(2,q) = \cup_{r \neq 0} P_r$, where for $r \in GF(q)$ with $r \neq 0$, $P_r = \{a + \frac{r}{x-i} : a, i \in GF(q)\}$, so $|P_r| = q^2$. Further consider the partition of $P_r$ given by $P_r = \cup_{i \in GF(q)} B_i(r)$, where, $B_i(r) = \{a + \frac{r}{x-i} : a \in GF(q)\}$.

**Theorem 6** *Let $q = p^m$, where $p$ is an odd prime, with $q \equiv 1 (mod\ 3)$. Then the following hold in the graph $C_P(q)$. (a) For any $r \neq s$, $r, s \neq 0$, we have $[P_r] \cong [P_s]$. (b) For any $r \neq 0$ and $i \neq j$, $[B_i(r) \cup B_j(r)]$ is a perfect matching, which matches $B_i(r)$ to $B_j(r]$. (c) $C_P(q)$ is regular of degree $q-1$. (d) For any nonisolated vertex $v \in C_P(q)$, $[N(v)]$ is a disjoint union of cycles, where $N(v)$ is the set of neighbors of $v$ in $C_P(q)$.*

**Theorem 7** *Let $q = p^m$, where $p$ is an odd prime, $q \geq 13$. Then the connected components of $C_P(q)$ are: (1) the isolated points - these are of the form $\pi = ax + b$, $a \neq 0$, and there are $q(q-1)$ of them, and (2) the graphs $[P_r]$ induced by the sets $P_r$.*

We can now obtain our independent set by a theorem of Alon [1].

**Theorem 8** *[1] Let G = (V,E) be a graph on $N$ vertices with average degree $t \geq 1$ in which for every vertex $v \in V$ the induced subgraph on the set of all neighbors of $v$ is $r$-colorable. Then the maximum size $\alpha(G)$ of an independent set in $G$ satisfies $\alpha(G) \geq \frac{c}{log(r+1)} \frac{N}{t} log(t)$, for some absolute constant $c$.*

**Corollary 9** *Let $q$ be a power of an odd prime $p$, with $q \equiv 1 (mod\ 3)$, **a)** $\alpha(C_P(q)) \geq Kq^2 log(q)$ for some constant $K$. **b)** $M(q,q-3) \geq Kq^2 log(q)$ for some constant $K$.*

Note: A more complete version of this research is available at
`http://www.utdallas.edu/~besp/contraction.pdf`

## References


[1] N. Alon: Independence numbers of locally sparse graphs and a Ramsey type result, *Random Structures and Algorithms* **9(3)** (1996), 271-278.

[2] S. Bereg, A. Levy, and I.H. Sudborough: Constructing Permutation Arrays from Groups, to appear in *Designs, Codes, and Cryptography.*

[3] S. Bereg, L. Morales, and I.H. Sudborough: Extending permutation arrays: improving MOLS bounds, *Designs, Codes, and Cryptography* **83(3)** (2017), 661-883.

[4] C.J. Colbourn, T. Klove, Alan C.H. Ling: Permutation arrays for powerline communication and mutually orthogonal latin triangles, *IEEE Transactions on Information Theory* **50(6)**, 1289-1291.

[5] W. Chu, C.J. Colbourn, and P. Dukes: Constructions for permutation codes in powerline communications, *Designs, Codes, and Cryptography* **32** (2004), 51-64.

[6] M. Deza and S.A. Vanstone: Bounds for permutation arrays, *J. of Statistical Planning and Inference* **2(2)** (1978), 197-209.

[7] P. Dukes and N. Sawchuk: Bounds on permutation codes of distance four, *J. of Algebr. Comb.* **31** (2010), 143-158.

[8] H.C. Ferreira and A.J.H. Vinck: Interference cancellation with permutation trellis arrays, *Proc. IEEE Vehicular Technology Conf.*, Boston, MA, USA (Sept. 2000), 2401-2407.

[9] P. Frankl and M. Deza: On the maximum number of permutations with given maximal or minimal distance, *J. of Combinatorial Theory, Series A* **22(3)** (1977), 352-360.

[10] S. Huczynska: Powerline communications and the 36 officers problem, *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **364(1849)** (2003), 34-40.

[11] I. Janiszczak, W. Lempkin, P.R. Ostergard, and R. Staszewski: Permutation codes invariant under isometries, *Designs, Codes, and Cryptography* **75(3)** 2015, 497-507.

[12] A. Jiang, R. Mateescu, M. Schwartz, and J. Bruck: Rank modulation for flash memories, *Proc. IEEE Symp. Inf. Theory* (2008), 1731-1735.

[13] A. Jiang, M. Schwartz, and J. Bruck: Error-correcting codes for rank modulation, *Proc. IEEE Symp. Inf. Theory* (2008), 1736-1740.

[14] N. Pavlidou, A.J.H. Vinck, J. Yazdani, and B. Honary: Powerline communications: state of the art and future trends, *IEEE Commun. Mag.* **41(4)** (2003), 34-40.

[15] D.H. Smith and R. Montemanni: A new table of permutation codes, *Designs, Codes, and Cryptography* **63(2)** (2012), 241-253.

[16] D.R. de la Torre, C.J. Colbourn, and A.C.H. Ling: An application of permutation arrays to block ciphers, *Proc. 31st Southeastern Int. Conf. on Combinatorics, Graph Theory, and Computing*, Boca Raton, Fl., USA **145** (2000), 5-7.

[17] A.J.H. Vinck: Coded modulation for powerline commumnications, *A.E.U. Int. J. Electronic Commun.* **54** (2000), 45-49.

[18] X. Wang, Y. Zhang, Y. Yang, and G. Ge: New bounds of permutation codes under Hamming metric and Kendall's $\tau$-metric, *Designs, Codes, and Cryptography* **85(3)** (2017), 533-545.