Des. Codes Cryptogr. (2017) 83:661–683
DOI 10.1007/s10623-016-0263-y

Extending permutation arrays: improving MOLS bounds

Sergey Bereg[1] · **Linda Morales**[1] · **I. Hal Sudborough**[1]

Received: 3 September 2015 / Revised: 17 May 2016 / Accepted: 22 July 2016 /
Published online: 3 August 2016

Abstract A permutation array (PA) A is a set of permutations on $Z_n = \{0, 1, \ldots, n-1\}$, for some n. A PA A has pairwise Hamming distance at least d, if for every pair of permutations σ and τ in A, there are at least d integers i in Z_n such that $\sigma(i) \neq \tau(i)$. Let $M(n, d)$ denote the maximum number of permutations in any PA with pairwise Hamming distance at least d. Recently considerable effort has been devoted to improving known lower bounds for $M(n, d)$ for all $n > d > 3$. We give a *partition and extension* operation that enables the production of a new PA A' for $M(n+1, d)$ from an existing PA A for $M(n, d-1)$. In particular, this operation allows for improvements for PA's for $M(q+1, q)$ for powers of prime numbers q, as well as for many other choices of n and d, where n is not a power of a prime. Finally, for prime numbers p, the partition and extension technique provides an asymptotically better lower bound for $M(p+1, p)$ than that given by current knowledge about mutually orthogonal Latin squares. We prove a new asymptotic lower bound for the set of primes p, namely, $M(p+1, p) \geq p^{1.5}/2 - O(p)$.

Keywords Permutation arrays · Hamming distance · Error correcting codes

Mathematics Subject Classification 05A05 · 05A18 · 68R05 · 94B60

1 Introduction

A *permutation array* (PA) A is a set of permutations on $Z_n = \{0, 1, \ldots, n-1\}$, for some n. Permutations σ and τ on Z_n have *Hamming distance* d, denoted by $hd(\sigma, \tau)$, if there are exactly d integers i in Z_n such that $\sigma(i) \neq \tau(i)$. When $\sigma(i) = \tau(i)$, we say that σ and τ *agree* at position i. The number of agreements between σ and τ is $n - hd(\sigma, \tau)$. The

Communicated by D. Jungnickel.

✉ I. Hal Sudborough
hal@utdallas.edu

[1] Department of Computer Science, University of Texas at Dallas, Richardson, TX 75080, USA

Hamming distance between two PA's A and B on Z_n, denoted by $hd(A, B)$, is the smallest Hamming distance between permutations $\sigma \in A$ and $\tau \in B$. The Hamming distance of a PA A on Z_n, denoted by $hd(A)$, is the smallest Hamming distance between two permutations $\sigma \neq \tau$ in A. If $hd(A) = d$, then A is an (n, d)-PA. Let $M(n, d)$ denote the maximum number of permutations on Z_n in any (n, d)-PA. Recently considerable effort has been devoted to improving known lower bounds for $M(n, d)$, for all $n > d > 3$ [4,6,7,9,10,12–14,20]. Large permutation arrays are valuable in creating better error correcting permutation codes, which have application in the transmission of information over very noisy channels, such as power lines [11,17]. It is known that, if q is either prime or a power of a prime, then $M(q, q-1) = q(q-1)$ and $M(q+1, q-1) = (q+1)q(q-1)$ [8,18]. More generally, if there is a sharply k-transitive group of order n consisting of N permutations, then $M(n, n-k+1) \geq N$ [8,16]. It is also known that, for any positive integer n, if there are k mutually orthogonal Latin squares of side n, then $M(n, n-1) \geq kn$ [6]. There are known combinatorial lower bounds and upper bounds for $M(n, d)$ [8,9]. Several papers give both computational and combinatorial techniques for improved lower bounds on $M(n, d)$ [4,6,13,20]. It is known [4], for any permutations σ, τ and ρ, that $hd(\sigma, \tau) = hd(\rho\sigma, \rho\tau)$, where multiplication denotes the composition of functions. So, for any group G of permutations on n symbols, $hd(G) = hd(\rho G)$, where ρ is any permutation on n symbols and ρG is the so-called left coset of G, which is obtained by function composition of the permutation ρ with every permutation in G.

We present a *partition and extension* operation that produces a new $(n+1, d)$-PA from an existing $(n, d-1)$-PA. In Sect. 2 we give a detailed description of the operation. In Sect. 3 we apply the partition and extension operation and create several PAs improving known lower bounds for $M(n+1, d)$. In Sect. 4, we prove a new asymptotic lower bound for the set of primes p, namely, $M(p+1, p) \geq p^{1.5}/2 - O(p)$.

2 The partition and extension technique

A rudimentary form of *extension* was described in [15]. Basically, the operation was specified for a group G of permutations on Z_n, for some n, and a left coset ρG, where ρ is a permutation not in G. For some integer d, let $hd(G) = d$ and $hd(G, \rho G) = d - 1$. One constructs by extension a set of permutations $G' = \{\sigma' \mid \sigma \in G\} \cup \{\tau'' \mid \tau \in \rho G\}$ on the symbols of $Z_{n+1} = \{0, 1 \ldots, n\}$, where:

(1) $\sigma'(i) = \sigma(i)$, for all $i < n$, and $\sigma'(n) = n$, and
(2) $\tau''(i) = \tau(i)$, for all i $(0 < i < n)$, $\tau''(0) = n$, and $\tau''(n) = \tau(0)$.

It was shown in [15] that G' is a PA on $n+1$ symbols with Hamming distance d. That is, from the PA $G \cup \rho G$ for $M(n, d-1)$, one extends to a PA G' for $M(n+1, d)$ which has $2|G|$ permutations.

We describe a new richer form of extension, which we call *partition and extension*, that enables the construction of PA's for $M(n+1, d)$ with considerably more than $2|G|$ permutations from PA's for $M(n, d-1)$. The necessary property to achieve the stated Hamming distance via partition and extension is to have sets of permutations, say $M_1, M_2, \ldots, M_k$, for some k, such that each set has (*intra*) Hamming distance say d, at least one greater than the (*inter*) Hamming distance between pairs of sets. When this is true, one can modify the sets by replacing different symbols in different positions in each permutation of $M_1, M_2, \ldots, M_k$ with the symbol n and moving the replaced symbol, in each case, to the end of the permutation. In addition, for one of the sets, one can simply put the symbol n at the end of

each permutation. Because the common new symbol may be positioned in the same location in each set, there will be one more position with identical symbols within them. Since the number of symbols also increases by one, the (*intra*) Hamming distance remains the same. On the other hand, since the positions of the replaced symbols and the replaced symbols themselves are different in different sets, the (*inter*) Hamming distance increases by one. So, the intra-distance of d remains d and the inter-distance of $d-1$ increases to d. In the case of rudimentary extension there are two sets, in one set the replacement always happens in the first position, but can involve any one of the original symbols, and in the second set the new symbol is placed at the end of each permutation. Clearly one can generalize, as we do now.

Let s be a positive integer, $M_1, M_2, \ldots, M_s$ be an ordered list of s pairwise disjoint sets of permutations on Z_n, and let $\mathcal{P} = (P_1, P_2, \ldots, P_s)$ and $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_s)$ be two ordered lists of subsets of Z_n such that the sets in $\mathcal{P}$ and $\mathcal{Q}$ are partitions of Z_n. Each set P_i is the set of locations for replacing symbols in the set M_i and each set Q_i is the set of symbols to be replaced. For each i, let $covered(M_i) = \{\sigma \in M_i \mid \exists p \in P_i(\sigma(p) \in Q_i)\}$. In order for a permutation to be included in the extended set of permutation on $n+1$ symbols it must be covered. In other words, it must have one of the named symbols in one of the named positions. In general, for integers i, when $\sigma \in covered(M_i)$, there may be more than one position $p \in P_i$ such that $\sigma(p) \in Q_i$. If so, arbitrarily designate one of these positions, denoted by p_*, to cover σ. If, on the other hand, there is exactly one position $p \in P_i$ such that $\sigma(p) \in Q_i$, then let the designated position p_* be p. In this case we say that σ is *uniquely covered*. If, for an integer i, there is a bijection mapping $P_i \times Q_i$ to $covered(M_i)$, so $|P_i \times Q_i| = |covered(M_i)|$, then we say M_i is *well covered* by (P_i, Q_i). Otherwise, we say that M_i is *covered*.

For our construction, we include an additional set of permutations M_{s+1}, for which there is no corresponding set of positions or symbols. None of the permutations in M_{s+1} are in any of the sets M_i. The partition and extension operation adds the new symbol n to the end of each permutation of M_{s+1}, as was done with the second set in the rudimentary form of extension. Every permutation in M_{s+1} is used in the construction of our new PA. By definition we say that M_{s+1} is *well covered*. Thus, we create the vector $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$, which includes this extra set. We define $\mathcal{M}$ to be *well covered* if every M_i, $0 \le i \le s+1$ is well covered.

We define a *distance-d partition system* for Z_n to be a triple $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ that satisfies the following properties:

(1) for all $M_i \in \mathcal{M}$, $hd(M_i) \ge d$, and
(2) for all $i, j (1 \le i < j \le s+1)$, $hd(M_i, M_j) \ge d-1$.

Observe that the set consisting of the union of the sets of $\mathcal{M}$ does not have Hamming distance d, because the distance between permutations in different sets may only be $d-1$.

In practice, the collection of pairwise disjoint sets of permutations $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$ will often consist of a group and some collection of its cosets. In such a case all sets have the same cardinality. The list $\mathcal{M}$, in general, will not correspond to all available cosets; in fact, we often choose the cosets and their order in a careful manner for optimality. As stated, the particular sets and partitions, and the order of the sets in the partitions $\mathcal{P}$ and $\mathcal{Q}$, will be chosen with some thought. Example 1 is a distance-7 partition system illustrating explicitly the covered permutations in each set M_i.

Example 1 Let $n = 7$ and $\mathcal{M} = (M_1, M_2, M_3, M_4)$ be an ordered list of permutation arrays on Z_7, where:

Table 1 Covered permutations of $\mathcal{M}$

M_1 covered by $P_1 =$ $\{0, 3\}$ and $Q_1 = \{0, 1, 2\}$	M_2 covered by $P_2 =$ $\{1, 4, 6\}$ and $Q_2 = \{3, 5\}$	M_3 covered by $P_3 =$ $\{2, 5\}$ and $Q_3 = \{4, 6\}$
0123456	0246135	0531642
1234560	2461350	3164205
2345601	4613502	1642053
4560123	1350246	2053164
5601234	3502461	
6012345	5024613	

Column 1 gives permutations in M_1 covered by $P_1 = \{0, 3\}$ and $Q_1 = \{0, 1, 2\}$, with the covered symbol in bold and underlined. Similarly, column 2 gives permutations in M_2 covered by $P_2 = \{1, 4, 6\}$ and $Q_2 = \{3, 5\}$, and column 3 gives permutations in M_3 covered by $P_3 = \{2, 5\}$ and $Q_3 = \{4, 6\}$

(1) $M_1 = \{0123456, 1234560, 2345601, 3456012, 4560123, 5601234, 6012345\}$,
(2) $M_2 = \{0246135, 2461350, 4613502, 6135024, 1350246, 3502461, 5024613\}$,
(3) $M_3 = \{0531642, 5316420, 3164205, 1642053, 6420531, 4205316, 2053164\}$, and
(4) $M_4 = \{0362514, 3625140, 6251403, 2514036, 5140362, 1403625, 4036251\}$.

Let $\mathcal{P} = (\{0, 3\}, \{1, 4, 6\}, \{2, 5\})$ and $\mathcal{Q} = (\{0, 1, 2\}, \{3, 5\}, \{4, 6\})$. The triple $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ is a distance-7 partition system.

All but one of the permutations in M_1 and M_2 are covered, and all but three of the permutations of M_3 are covered, as shown in Table 1. In this example $M_{s+1} = M_4$. All permutations in M_{s+1} are included in the construction. Each M_i is well covered so $\mathcal{M}$ is well covered. □

Let σ be a permutation on Z_n and let $k \in Z_n$. The *extension of* σ *by position* k, denoted by $ext_k(\sigma) = \sigma'$, is a permutation on Z_{n+1} defined by: $\sigma'(k) = n, \sigma'(n) = \sigma(k)$, and $\sigma'(j) = \sigma(j)$, for all j $(0 \le j < n, j \ne k)$. We will always extend σ at the designated position p_* and refer to this new permutation as $ext(\sigma)$ and σ' interchangeably.

Partition and extension uses sets P_i and Q_i in the two partitions $\mathcal{P}$ and $\mathcal{Q}$ to modify the covered permutations in M_i, for $1 \le i \le s$, for the purpose of creating a new PA on Z_{n+1} with Hamming distance d. Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ be a distance-d partition system, where $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$, for some s. We now show how the partition and extension operation creates a new permutation array $ext(\Pi)$ on Z_{n+1}. For all i $(1 \le i \le s)$, let $ext(M_i)$ be the set of permutations defined by

$$ext(M_i) = \{ext(\sigma) \mid \sigma \in covered(M_i)\}.$$

For M_{s+1}, let $ext(M_{s+1})$ be the set of permutations on Z_{n+1} defined by:

$$ext(M_{s+1}) = \{\tau' \mid \tau \in M_{s+1} \text{ and } \tau'(j) = \tau(j), \forall j\ (0 \le j < n), \text{ and } \tau'(n) = n\}.$$

Let $ext(\Pi)$ be defined by $ext(\Pi) = \cup_{i=1}^{s+1} ext(M_i)$. Note that $|ext(\Pi)| = \sum_{i=1}^{s+1} |ext(M_i)|$. A permutation $\sigma \in M_i$ is extended only by a position in its designated position set, P_i, which contains a symbol in its designated symbol set, Q_i. This will ensure that the permutations in $ext(\Pi)$ have Hamming distance d, as we shall prove in Theorem 1 below. Before we prove the theorem, we illustrate the creation of $ext(\Pi)$.

Example 2 Let us use the partition and extension operation to compute $ext(\Pi)$ for $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, the distance-7 partition system described in Example 1. Table 2 illustrates $ext(M_i)$ for all M_i in $\mathcal{M}$. □

Table 2 Permutations in $ext(\Pi)$

$ext(M_1)$	$ext(M_2)$	$ext(M_3)$	$ext(M_4) = ext(M_{s+1})$
71234560	02461375	05316724	03625147
72345601	24617503	31742056	36251407
73456012	46137025	16720534	62514037
45671230	17502463	20531746	25140367
56072341	37024615		51403627
60173452	50246173		14036257
			40362517

Column 1 gives permutations in $ext(M_1)$. Similarly, columns 2, 3, and 4 give permutations in $ext(M_2)$, $ext(M_3)$, and $ext(M_4)$, respectively. There are 23 permutations in $ext(\Pi)$ altogether

Of course, our goal is to use $ext(\Pi)$ to obtain improvements on $M(n+1, d)$. For this we need to compute $hd(ext(\Pi))$ and $|ext(\Pi)|$. Theorem 1 and Corollary 1 below show us how to compute these quantities.

Theorem 1 *Let d be a positive integer. Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ be a distance-d partition system for Z_n, with $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$ for some positive integer s. Let $ext(\Pi)$ be the PA on Z_{n+1} created by partition and extension. Then, $hd(ext(\Pi)) \geq d$.*

Proof First, suppose that both σ', τ' are in $ext(M_{s+1})$. Then $hd(\sigma', \tau') \geq d$, because σ and τ are in M_{s+1}, $hd(M_{s+1}) = d$, and by definition of $ext(M_{s+1})$, $\sigma'(j) = \sigma(j)$ and $\tau'(j) = \tau(j)$, for all j $(0 \leq j < n)$. That is, $hd(ext(M_{s+1})) \geq d$.

Next suppose τ' is in $ext(M_{s+1})$, and suppose that σ' is in $ext(M_i)$ for some i. This means that $\sigma' = ext_x(\sigma)$ for some covered permutation σ in M_i, where $0 \leq x < n$. Hence $\tau'(n) = n \neq \sigma'(n), \tau'(x) \neq n = \sigma'(x)$. In other words, the two positions that the partition and extension operation have altered in σ and τ, namely positions x and n, contain different symbols. That is, no additional agreement has been created. Furthermore since $hd(M_i, M_{s+1}) \geq d - 1$, there are at most $n - (d-1) = n - d + 1$ positions k such that $\sigma(k) = \tau(k)$, so, there are at least $(n+1) - (n-d+1) = d$ positions where σ' and τ' do not agree. Hence $hd(\sigma', \tau') \geq d$, and $hd(ext(M_{s+1}), ext(M_i)) \geq d$, for all i.

What remains is to show that $hd(ext(M_i), ext(M_j)) \geq d$, for all i, j $(1 \leq i, j \leq s)$. The rest of the proof is divided into two cases. The cases are based on whether two covered permutations, σ and τ, are in the same set M_i, for some i $(1 \leq i \leq s)$, or are in two different sets.

Case (1). For some i, σ and τ are covered permutations in the same set M_i.

Since $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ is a distance-d partition system, for all $M_i \in \mathcal{M}$, $hd(M_i) \geq d$. Thus, since $\sigma, \tau \in M_i, hd(\sigma, \tau) \geq d$. We show that $hd(\sigma', \tau') \geq d$, hence $hd(ext(M_i)) \geq d$, for all i.

Part (a): Let σ, τ both be covered by position r in P_i. Then $\sigma'(n) = \sigma(r)$ and $\tau'(n) = \tau(r)$. If $\sigma(r) = \tau(r)$, then since $hd(\sigma, \tau) \geq d$, there are at least d other positions m, such that $\sigma'(m) = \sigma(m) \neq \tau(m) = \tau'(m)$. So, $hd(\sigma', \tau') \geq d$. On the other hand, if $\sigma(r) \neq \tau(r)$, since $hd(\sigma, \tau) \geq d$, there are at least $d-1$ positions m, such that $\sigma'(m) = \sigma(m) \neq \tau(m) = \tau'(m)$. Hence, including position n, where $\sigma'(n) = \sigma(r) \neq \tau(r) = \tau'(n)$, there are at least d positions where σ' and τ' disagree, so $hd(\sigma', \tau') \geq d$.

Part (b): For some r, t $(0 \leq r, t < n, r \neq t)$, let σ be covered by position r in P_i and let τ be covered by position t in P_i. So $\sigma'(r) = n \neq \tau'(r)$ and $\tau'(t) = n \neq \sigma'(t)$. Moreover, since $hd(\sigma, \tau) \geq d$, there are at least $d-2$ other positions m, $(0 \leq m < n, m \notin \{r, t\})$ such that $\sigma'(m) = \sigma(m) \neq \tau(m) = \tau'(m)$. So, $hd(\sigma', \tau') \geq d$. Note that it is not necessary in

this argument to separate cases when $\sigma(r) = \tau(r)$ or $\sigma(t) = \tau(t)$, because regardless, as shown above by counting, there must be at least d positions in σ' and τ' with different values. Hence $hd(\sigma', \tau') \geq d$. Thus, for all i, $(1 \leq i \leq s)$, $hd(ext(M_i)) \geq d$.

Case (2). For some i, j $(1 \leq i < j \leq s)$, σ, τ are covered permutations in M_i and M_j, respectively.

Since $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ is a distance-d partition system, for all $M_i, M_j \in \mathcal{M}$, $hd(M_i, M_j) \geq d - 1$. Thus, $hd(\sigma, \tau) \geq d - 1$. We show that $hd(\sigma', \tau') \geq d$.

Let σ be covered at position r by the pair (P_i, Q_i), and let τ be covered at position t by the pair (P_j, Q_j). As P_i and P_j are disjoint, it follows that $r \neq t$. It follows that $\sigma'(r) = n \neq \tau'(r)$ and $\tau'(t) = n \neq \sigma'(t)$. Also, since $hd(\sigma, \tau) \geq d - 1$ there are at least $d - 3$ other positions m, $(0 \leq m < n, m \notin \{r, t\})$ such that $\sigma'(m) = \sigma(m) \neq \tau(m) = \tau'(m)$. Note that, since Q_i and Q_j are disjoint, $\sigma(r) \neq \tau(t)$. Hence $\sigma'(n) \neq \tau'(n)$. Hence, there are at least d positions where σ' and τ' disagree, so $hd(\sigma', \tau') \geq d$. Thus, for all i, j, $(1 \leq i < j \leq s)$, $hd(ext(M_i), ext(M_j)) \geq d$.

We have shown that for all i, j, $(1 \leq i, j \leq s + 1)$, $hd(ext(M_i), ext(M_j)) \geq d$. That is, $hd(ext(\Pi)) \geq d$. □

Corollary 1 *Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ be a distance-d partition system for Z_n, where $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$, and where $|M_{s+1}| = m$.*

(1) *If $\mathcal{M}$ is covered (but not well covered), then $|ext(\Pi)| = \sum_{i=1}^{s+1} |ext(M_i)|$.*
(2) *If $\mathcal{M}$ is well covered by $\mathcal{P} = (P_1, P_2, \ldots, P_s)$ and $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_s)$, then $|ext(\Pi)| = m + \sum_{i=1}^{s} |P_i| \cdot |Q_i|$. Hence,*

$$M(n + 1, d) \geq m + \sum_{i=1}^{s} |P_i| \cdot |Q_i|.$$

Proof For (1), for all M_i, $|ext(M_i)| = |covered(M_i)|$, by definition of $ext(M_i)$, and $|ext(M_{s+1})| = |M_{s+1}|$. Hence $|ext(\Pi)| = \sum_{i=1}^{s+1} |ext(M_i)|$.

For (2), clearly, $|ext(M_{s+1})| = |M_{s+1}| = m$. Because $\mathcal{M}$ is well covered, for any i, $(1 \leq i \leq s)$, $|ext(M_i)| = |covered(M_i)| = |P_i \times Q_i| = |P_i| \cdot |Q_i|$. Hence, $|ext(\Pi)| = |M_{s+1}| + \sum_{i=1}^{s} |M_i| = m + \sum_{i=1}^{s} |P_i| \cdot |Q_i|$. Since $ext(\Pi)$ consists of permutations of length $n + 1$, $M(n + 1, d) \geq m + \sum_{i=1}^{s} |P_i| \cdot |Q_i|$. □

3 New PAs obtained by partition and extension

Distance-d partition systems $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, as described, are useful for obtaining better lower bounds for $M(n+1, d)$ for many cases of n and d. There are generally three situations:

1. improving the lower bound for $M(q + 1, q)$, where q is a power of a prime,
2. improving the lower bound for $M(n + 1, n)$, where n is not a power of a prime, and the current bound for $M(n, n - 1)$ is given by mutually orthogonal Latin squares (MOLS), and
3. improving the lower bound for $M(n + 1, d)$, given a group $G = M_1$ of permutations over Z_n with $hd(G) = d$ and cosets $M_2, M_3, \ldots, M_k$ such that $hd(M_i, M_j) \geq d - 1$, $1 \leq i, j \leq k, i \neq j$.

We now illustrate the use of the partition and extension operation on certain distance-d partition systems Π to obtain new results.

Results 1 and 2 below illustrate the use of the partition and extension technique to obtain better lower bounds for $M(q, d)$ where q is a power of a prime. We create PAs from subsets of $AGL(1, q)$. $AGL(1, q)$ is the affine general linear group of permutations on Z_q, where $AGL(1, q) = \{ax + b \mid a, b, x \in GF(q), a \neq 0\}$ [19]. Note that, for any choice of $a, b \in GF(q), a \neq 0$, the function $f(x) = ax + b$ is a permutation, so $AGL(1, q)$ is a set of $q(q-1)$ permutations. $GF(q)$ denotes the Galois field on the elements of Z_q. If $q = p^1$, where p is a prime, then the operations are addition and multiplication $mod\ p$ [19]. When $q = p^\alpha, \alpha \neq 1$, (i.e. q is a power of a prime), elements of $GF(q)$ can be viewed as polynomials of degree at most $\alpha - 1$ with coefficients in Z_p. Addition of two polynomials is done with $mod\ p$ arithmetic of the coefficients. Multiplication in $GF(q)$ depends on a primitive polynomial $r(x)$ of degree α. That is, the elements of $GF(q)$ can be viewed as $1, x, x^2, \ldots, x^{q-1}$, where if $t > \alpha - 1$, then x^t is replaced by its remainder when divided by $r(x)$ [19].

$AGL(1, q)$ can be viewed as a collection of permutations given by a group $B_1 = \{x + b \mid b, x \in GF(q)\}$ together with $q - 2$ cosets of permutations denoted by $B_a = \{ax + b \mid a, b, x \in GF(q), a > 1\}$. For example, the coset B_2 is given by $\{2x + b \mid b, x \in GF(q)\}$; the coset B_3 is given by $\{3x + b \mid b, x \in GF(q)\}$, and so on. Note that, for any $a \in Z_q$, where $a > 1$, B_a is the left coset of B_1, given by $B_a = \pi_a B_1$, where π_a is the permutation by $\pi_a(x) = ax$ and the group operation is composition of permutations. When $q = p^1$ where p is prime, then $B_1 = C_p$, the cyclic group of permutations on Z_p, consisting of the identity permutation and its cyclic shifts.

It is known that $AGL(1, q)$ is sharply 2-transitive, hence, $hd(AGL(1, q)) = q - 2 + 1 = q - 1$. Consequently, for any subset X of $AGL(1, q)$, $hd(X) = q - 1$ as well.

Result 1: $M(26, 25) \geq 130$.

We begin with an example of type (1) for $q = 25$, a power of the prime $p = 5$, with $\alpha = 2$. We show that $M(26, 25) \geq 130$. The best previous lower bound, $M(26, 25) \geq 104$, was obtained by exhibiting 4 MOLS of side 26 [5].

Consider the Galois field $GF(5^2)$. We use the primitive polynomial $r(x) = x^2 + 2x + 3$ to obtain the cyclic group containing of the 24 non-zero elements: $\widehat{1} = x^0, \widehat{2} = x^1, \widehat{3} = x^2, \ldots, \widehat{24} = x^{23}$, of $GF(5^2)$, where we refer to the ith non-zero element x^{i-1} temporarily as $\widehat{i}$. We reduce each of these terms to polynomials of degree $\alpha - 1 = 1$ by computing the remainder when divided by the primitive polynomial ($mod\ 5$). Thus we have $\widehat{1} = x^0 = 1, \widehat{2} = x^1 = x, \widehat{3} = x^2 = 3x + 2, \widehat{4} = x^3 = 3x^2 + 2x = x + 1, \widehat{5} = x^4 = x^2 + x = 4x + 2$, and so on. The element $\widehat{0}$ is simply 0. Eliminating the hats on top of the names of the elements, we get the first two rows of the addition table of $GF(5^2)$, which are:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	19	4	10	18	6	16	13	24	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3

Here, the second row gives $1 + x$, for each x in $GF(5^2)$. For example, $\widehat{1} + \widehat{2} = \widehat{4}$, since $\widehat{4} = 1 + x$, as shown above. The remaining rows of the addition table for $GF(5^2)$ can be obtained using distributive laws of multiplication over addition. Specifically, if $x^i + x^j = x^k$, then $x^{i+1} + x^{j+1} = x(x^i + x^j) = x(x^k) = x^{k+1}$. So, if the entry in the ith row ($i \geq 2$) and jth column is x^k, then the entry in the $(i + 1)$st row and $(j + 1)$st column is $x^{k+1(\text{mod } 24)}$. Similarly, if the entry in the ith row ($i \geq 2$) and jth column is 0, then the entry in the $(i + 1)$st row and $(j + 1)$st column is also 0. Also, if $j = 24$, then the $(j + 1)$st column is column 1. This can be seen in Table 3, where the addition table of $GF(5^2)$, after a partition and extension operation, is shown in the first twenty four rows.

Create the distance-25 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where:

1. $\mathcal{M} = (M_1, M_2, M_3, M_4, M_5, M_6)$, where M_1 is the group B_1, M_2 is its coset B_2, $M_3 = B_3$, $M_4 = B_4$, $M_5 = B_5$ and the extra set is $M_6 = B_6$,
2. $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$, where $P_1 = \{0, 5, 11, 17, 23\}$, $P_2 = \{1, 7, 16, 21, 24\}$, $P_3 = \{2, 6, 9, 13, 19\}$, $P_4 = \{3, 10, 12, 15, 18\}$, $P_5 = \{4, 8, 14, 20, 22\}$, and
3. $\mathcal{Q} = \{Q_1, Q_2, Q_3, Q_4, Q_5\}$, where $Q_1 = \{0, 1, 2, 3, 10\}$, $Q_2 = \{4, 6, 8, 12, 23\}$, $Q_3 = \{9, 14, 15, 17, 24\}$, $Q_4 = \{11, 13, 16, 18, 19\}$, $Q_5 = \{5, 7, 20, 21, 22\}$.

Table 3 show the covered permutations from B_1, B_2, B_3, B_4, B_5, and B_6, after the partition and extension operation has replaced designated symbols in each covered permutation with the symbol 25 and put the original symbols at the end. The group B_1 is well covered by (P_1, Q_1), as can be seen in Table 3. That is, there are 5 positions in P_1 and 5 symbols in Q_1, and all $25 = 5 \cdot 5$ permutations in B_1 are covered. The cosets B_2, B_3, B_4, and B_5 are covered (but not well covered) by (P_2, Q_2), (P_3, Q_3), (P_4, Q_4), (P_5, Q_5), respectively, as can be seen also in Table 3. In fact, (P_2, Q_2) covers 21 permutations of B_2, (P_3, Q_3) covers 21 permutations of B_3, (P_4, Q_4) covers 19 permutations of B_4, and (P_5, Q_5) covers 19 permutations of B_5. The extra coset, B_6, is completely covered by putting the symbol 25 in the last position of each of its permutations. It follows from Theorem 1 that $hd(ext(\Pi)) \geq 25$. Furthermore, by Corollary 1, $|ext(\Pi)| = 25 + 21 + 21 + 19 + 19 + 25 = 130$. Hence $M(26, 25) \geq 130$. □

Result 2: $M(30, 29) \geq 170$.

Another example of type (1) is for the prime number $p = 29$. We show that $M(30, 29) \geq 170$. The best previous lower bound, $M(30, 29) \geq 120$, was obtained by exhibiting four mutually orthogonal Latin squares of side 30 [5]. Let $p = 29$ and consider the group $G = AGL(1, 29)$ of permutations on Z_{29}, where $hd(G) = 28$. G consists of the cyclic group C_{29} together with 27 cosets B_a defined by non-zero values a in $GF(29)$, $1 < a \leq 28$.

Create the distance-29 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where:

1. $\mathcal{M} = (M_1, M_2, M_3, M_4, M_5, M_6, M_7)$, where $M_1 = C_{29}$, and $M_2, \ldots M_7$ are its cosets: $M_2 = B_{28}$, $M_3 = B_2$, $M_4 = B_{27}$, $M_5 = B_4$, $M_6 = B_7$, $M_7 = B_3$,
2. $\mathcal{P} = (P_1, P_2, P_3, P_4, P_5, P_6)$, where $P_1 = \{0, 9, 14, 19, 24\}$, $P_2 = \{1, 6, 11, 16, 21\}$, $P_3 = \{2, 7, 12, 17, 22\}$, $P_4 = \{3, 8, 13, 18, 23\}$, $P_5 = \{5, 10, 15, 20, 25\}$, $P_6 = \{4, 26, 27, 28\}$, and
3. $\mathcal{Q} = (Q_1, Q_2, Q_3, Q_4, Q_5, Q_6)$, where $Q_1 = \{0, 1, 2, 3, 4\}$, $Q_2 = \{5, 6, 7, 8, 9\}$, $Q_3 = \{10, 14, 18, 22, 26\}$, $Q_4 = \{11, 15, 19, 23, 27\}$, $Q_5 = \{12, 16, 20, 24, 28\}$, $Q_6 = \{13, 17, 21, 25\}$.

Since $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ is a distance-29 partition system, it follows from Theorem 1 that $hd(ext(\Pi)) \geq 29$. Furthermore, $\mathcal{M}$ is well covered, so it follows from Corollary 1 that $|ext(\Pi)| = |M_7| + 5 \cdot 25 + 4 \cdot 4 = 170$. Hence, $M(30, 29) \geq 170$. □

Results 1 and 2 give new values $M(q + 1, q)$ for q a power of a prime. We now give two results of type (3). Results 3 and 4 below illustrate the partition and extension technique to obtain better lower bounds for $M(q + 2, d)$ where $q = p^\alpha$, $\alpha \neq 1$, is a power of a prime. We use the group $PGL(2, q)$, the projective general linear group of permutations on Z_{q+1}. Denote the symbols of Z_{q+1} by $0, 1, 2, \ldots, q - 1, \infty$. The permutations of $PGL(2, q)$ are defined for all $a, b, c, d \in GF(q)$ such that $ad \neq bc$:

- if $x \in GF(q)$, but $x \neq -d/c$, then $g(x) = \frac{ax+b}{cx+d}$,
- if $x = -d/c$, then $g(-d/c) = \infty$,
- if $c \neq 0$, then $g(\infty) = a/c$,
- if $c = 0$, then $g(\infty) = \infty$.

Table 3 Permutations in *ext*(Π) of Result 1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	0
25	19	4	10	18	6	16	13	24	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3	1
25	4	20	5	11	19	7	17	14	1	6	24	23	21	0	10	13	15	22	18	8	12	3	16	9	2
25	10	5	21	6	12	20	8	18	15	2	7	1	24	22	0	11	14	16	23	19	9	13	4	17	3
4	18	11	6	22	7	13	21	9	19	16	**25**	8	2	1	23	0	12	15	17	24	20	10	14	5	3
5	6	19	12	7	23	8	14	22	10	20	17	4	9	3	2	24	**25**	13	16	18	1	21	11	15	0
6	16	7	20	13	8	24	9	15	23	11	21	18	5	10	4	3	**25**	0	14	17	19	2	22	12	1
7	13	17	8	21	14	9	1	10	16	24	12	22	19	6	11	5	4	2	0	15	18	20	**25**	23	3
8	24	14	18	9	22	15	10	2	11	17	**25**	13	23	20	7	12	6	5	3	0	16	19	21	4	1
9	5	1	15	19	**25**	23	16	11	3	12	18	2	14	24	21	8	13	7	6	4	0	17	20	22	10
25	23	6	2	16	20	11	24	17	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	21	10
11	22	24	7	3	17	21	12	1	18	13	5	14	20	4	16	2	23	10	15	9	8	6	**25**	19	0
12	20	23	1	8	4	18	22	13	2	19	14	6	15	21	5	17	**25**	24	11	16	10	9	7	0	3
13	0	21	24	2	9	5	19	23	14	3	20	15	7	16	22	6	18	4	1	12	17	11	**25**	8	10
14	9	0	22	1	**25**	10	6	20	24	15	4	21	16	8	17	23	7	19	5	2	13	18	12	11	3
15	12	10	0	23	**25**	4	11	7	21	1	16	5	22	17	9	18	24	8	20	6	3	14	19	13	2
16	14	13	11	0	24	3	5	12	8	22	**25**	17	6	23	18	10	19	1	9	21	7	4	15	20	2
17	21	15	14	12	**25**	1	4	6	13	9	23	3	18	7	24	19	11	20	2	10	22	8	5	16	0
18	17	22	16	15	13	0	2	5	7	14	**25**	24	4	19	8	1	20	12	21	3	11	23	9	6	10
19	7	18	23	17	16	14	0	3	6	8	15	11	1	5	20	9	**25**	21	13	22	4	12	24	10	2
20	11	8	19	24	18	17	15	0	4	7	9	16	12	2	6	21	**25**	3	22	14	23	5	13	1	10
21	2	12	9	20	**25**	19	18	16	0	5	8	10	17	13	3	7	22	11	4	23	15	24	6	14	1

Table 3 continued

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
22	15	3	13	10	21	2	20	19	17	0	6	9	11	18	14	4	8	23	12	5	24	16	**25**	7	1
23	8	16	4	14	11	22	3	21	20	18	**25**	7	10	12	19	15	5	9	24	13	6	1	17	2	0
24	3	9	17	5	15	12	23	4	22	21	19	0	8	11	13	20	16	6	10	1	14	7	**25**	18	2
0	2	3	4	5	6	7	**25**	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	8
1	**25**	10	18	6	16	13	24	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3	19	4
2	20	5	11	19	7	17	14	1	6	24	23	21	0	10	13	15	22	18	8	12	3	16	9	**25**	4
4	11	6	22	7	13	21	9	19	16	3	8	2	1	23	0	**25**	15	17	24	20	10	14	5	18	12
5	19	12	7	23	8	14	22	10	20	17	4	9	3	2	24	0	13	16	18	1	21	11	15	**25**	6
7	17	8	21	14	9	1	10	16	24	12	22	19	6	11	5	**25**	2	0	15	18	20	3	23	13	4
8	14	18	9	22	15	10	2	11	17	1	13	23	20	7	12	**25**	5	3	0	16	19	21	4	24	6
10	6	2	16	20	11	24	17	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	21	**25**	23
11	24	7	3	17	21	12	1	18	13	5	14	20	4	16	2	**25**	10	15	9	8	6	0	19	22	23
12	**25**	1	8	4	18	22	13	2	19	14	6	15	21	5	17	3	24	11	16	10	9	7	0	20	23
13	21	24	2	9	5	19	**25**	14	3	20	15	7	16	22	6	18	4	1	12	17	11	10	8	0	23
15	10	0	23	2	4	11	7	21	1	16	5	22	17	9	18	24	8	20	6	3	14	19	13	**25**	12
16	13	11	0	24	3	5	**25**	8	22	2	17	6	23	18	10	19	1	9	21	7	4	15	20	14	12
17	15	14	12	0	1	4	**25**	13	9	23	3	18	7	24	19	11	20	2	10	22	8	5	16	21	6
18	22	16	15	13	0	2	5	7	14	10	24	4	19	8	1	20	12	21	3	11	**25**	9	6	17	23
19	18	23	17	16	14	0	3	6	8	15	11	1	5	20	9	2	21	13	22	4	**25**	24	10	7	12
20	**25**	19	24	18	17	15	0	4	7	9	16	12	2	6	21	10	3	22	14	23	5	13	1	11	8
21	**25**	9	20	1	19	18	16	0	5	8	10	17	13	3	7	22	11	4	23	15	24	6	14	2	12
22	3	13	10	21	2	20	19	17	0	6	9	11	18	14	4	**25**	23	12	5	24	16	1	7	15	8

Table 3 continued

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
23	16	4	14	11	22	3	21	20	18	0	7	10	12	19	15	5	9	24	13	6	1	17	2	**25**	8
24	9	17	5	15	12	23	**25**	22	21	19	0	8	11	13	20	16	6	10	1	14	7	2	18	3	4
0	3	4	5	6	7	8	9	10	11	12	13	14	**25**	16	17	18	19	20	21	22	23	24	1	2	15
1	10	18	6	16	13	**25**	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3	19	4	24
2	5	11	19	7	17	14	1	6	**25**	23	21	0	10	13	15	22	18	8	12	3	16	9	4	20	24
3	21	6	12	20	8	18	15	2	7	1	24	22	0	11	14	16	23	19	**25**	13	4	17	10	5	9
4	6	22	7	13	21	**25**	19	16	3	8	2	1	23	0	12	15	17	24	20	10	14	5	18	11	9
5	12	7	23	8	14	22	10	20	**25**	4	9	3	2	24	0	13	16	18	1	21	11	15	6	19	17
6	20	13	8	24	9	**25**	23	11	21	18	5	10	4	3	1	0	14	17	19	2	22	12	16	7	15
8	18	**25**	22	15	10	2	11	17	1	13	23	20	7	12	6	5	3	0	16	19	21	4	24	14	9
10	2	16	20	11	24	**25**	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	21	23	6	17
12	1	8	4	18	22	13	2	19	**25**	6	15	21	5	17	3	24	11	16	10	9	7	0	20	23	14
13	24	2	9	5	19	23	14	3	20	15	7	16	22	6	18	4	1	12	**25**	11	10	8	0	21	17
14	22	1	3	10	6	20	24	15	4	21	16	8	**25**	23	7	19	5	2	13	18	12	11	9	0	17
15	0	23	2	4	11	7	21	1	16	5	22	17	**25**	18	24	8	20	6	3	14	19	13	12	10	9
17	14	12	0	1	4	6	13	9	23	3	18	7	**25**	19	11	20	2	10	22	8	5	16	21	15	24
18	16	**25**	13	0	2	5	7	14	10	24	4	19	8	1	20	12	21	3	11	23	9	6	17	22	15
20	19	**25**	18	17	15	0	4	7	9	16	12	2	6	21	10	3	22	14	23	5	13	1	11	8	24
21	9	20	1	19	18	16	0	5	8	10	17	13	3	7	22	11	4	23	**25**	24	6	14	2	12	15
22	13	10	21	2	20	19	17	0	6	9	11	18	14	4	8	23	12	5	**25**	16	1	7	15	3	24
23	4	**25**	11	22	3	21	20	18	0	7	10	12	19	15	5	9	24	13	6	1	17	2	8	16	14

Table 3 continued

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
19	23	**25**	16	14	0	3	6	8	15	11	1	5	20	9	2	21	13	22	4	12	24	10	7	18	17
24	17	5	15	12	23	4	22	21	19	0	8	11	13	20	16	6	10	1	**25**	7	2	18	3	9	14
0	4	5	6	7	8	9	10	11	12	**25**	14	15	16	17	18	19	20	21	22	23	24	1	2	3	13
1	18	6	**25**	13	24	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3	19	4	10	16
3	6	12	20	8	18	15	2	7	1	24	22	0	11	14	**25**	23	19	9	13	4	17	10	5	21	16
4	22	7	**25**	21	9	19	16	3	8	2	1	23	0	12	15	17	24	20	10	14	5	18	11	6	13
5	7	23	8	14	22	10	20	17	4	9	3	2	24	0	**25**	16	18	1	21	11	15	6	19	12	13
6	13	8	24	9	15	23	11	21	18	5	10	4	3	1	0	14	17	**25**	2	22	12	16	7	20	19
7	21	14	9	1	10	16	24	12	22	**25**	6	11	5	4	2	0	15	18	20	3	23	13	17	8	19
8	9	22	15	10	2	11	17	1	13	23	20	7	12	6	5	3	0	**25**	19	21	4	24	14	18	16
10	16	20	**25**	24	17	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	21	23	6	2	11
11	3	17	21	12	1	18	13	5	14	20	4	**25**	2	23	10	15	9	8	6	0	19	22	24	7	16
12	8	4	**25**	22	13	2	19	14	6	15	21	5	17	3	24	11	16	10	9	7	0	20	23	1	18
14	1	3	10	6	20	24	15	4	21	16	8	17	23	7	**25**	5	2	13	18	12	11	9	0	22	19
16	0	24	3	5	12	8	22	2	17	6	23	**25**	10	19	1	9	21	7	4	15	20	14	13	11	18
17	12	0	1	4	6	13	9	23	3	**25**	7	24	19	11	20	2	10	22	8	5	16	21	15	14	18
18	15	13	0	2	5	7	14	10	24	4	19	8	1	20	12	21	3	**25**	23	9	6	17	22	16	11
21	20	1	**25**	18	16	0	5	8	10	17	13	3	7	22	11	4	23	15	24	6	14	2	12	9	19
22	10	21	2	20	19	17	0	6	9	**25**	18	14	4	8	23	12	5	24	16	1	7	15	3	13	11
23	14	11	22	3	21	20	18	0	7	10	12	**25**	15	5	9	24	13	6	1	17	2	8	16	4	19
24	5	15	12	23	4	22	21	19	0	8	11	**25**	20	16	6	10	1	14	7	2	18	3	9	17	13
1	6	16	13	24	5	23	22	**25**	0	9	12	14	21	17	7	11	2	15	8	3	19	4	10	18	20

Table 3 continued

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	19	7	17	14	1	6	24	23	21	0	10	13	15	22	18	8	12	3	16	9	4	**25**	5	11	20
3	12	20	8	18	15	2	7	1	24	22	0	11	14	16	23	19	9	13	4	17	10	**25**	21	6	5
4	7	13	21	9	19	16	3	8	2	1	23	0	12	15	17	24	20	10	14	**25**	18	11	6	22	5
5	23	8	14	**25**	10	20	17	4	9	3	2	24	0	13	16	18	1	21	11	15	6	19	12	7	22
6	8	24	9	15	23	11	21	18	5	10	4	3	1	0	14	17	19	2	22	12	16	**25**	20	13	7
7	14	9	1	10	16	24	12	**25**	19	6	11	5	4	2	0	15	18	20	3	23	13	17	8	21	22
8	22	15	10	2	11	17	1	13	23	20	7	12	6	**25**	3	0	16	19	21	4	24	14	18	9	5
9	10	23	16	11	3	12	18	2	14	24	21	8	13	7	6	4	0	17	20	**25**	5	1	15	19	22
10	20	11	24	17	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	**25**	23	6	2	16	21
13	9	5	19	23	14	3	20	15	7	16	22	6	18	4	1	12	17	11	10	8	0	**25**	24	2	21
14	3	10	6	20	24	15	4	**25**	16	8	17	23	7	19	5	2	13	18	12	11	9	0	22	1	21
15	2	4	11	7	21	1	16	**25**	22	17	9	18	24	8	20	6	3	14	19	13	12	10	0	23	5
16	24	3	5	12	8	22	2	17	6	23	18	10	19	1	9	21	7	4	15	**25**	14	13	11	0	20
17	0	1	4	6	13	9	23	3	18	7	24	19	11	**25**	2	10	22	8	5	16	21	15	14	12	20
18	13	0	2	**25**	7	14	10	24	4	19	8	1	20	12	21	3	11	23	9	6	17	22	16	15	5
19	16	14	0	3	6	8	15	11	1	5	20	9	2	**25**	13	22	4	12	24	10	7	18	23	17	21
22	21	2	20	19	17	0	6	9	11	18	14	4	8	23	12	5	24	16	1	**25**	15	3	13	10	7
23	11	22	3	**25**	20	18	0	7	10	12	19	15	5	9	24	13	6	1	17	2	8	16	4	14	21
0	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4	5	**25**
1	16	13	24	5	23	22	20	0	9	12	14	21	17	7	11	2	15	8	3	19	4	10	18	6	**25**

Table 3 continued

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	7	17	14	1	6	24	23	21	0	10	13	15	22	18	8	12	3	16	9	4	20	5	11	19	**25**
3	20	8	18	15	2	7	1	24	22	0	11	14	16	23	19	9	13	4	17	10	5	21	6	12	**25**
4	13	21	9	19	16	3	8	2	1	23	0	12	15	17	24	20	10	14	5	18	11	6	22	7	**25**
5	8	14	22	10	20	17	4	9	3	2	24	0	13	16	18	1	21	11	15	6	19	12	7	23	**25**
6	24	9	15	23	11	21	18	5	10	4	3	1	0	14	17	19	2	22	12	16	7	20	13	8	**25**
7	9	1	10	16	24	12	22	19	6	11	5	4	2	0	15	18	20	3	23	13	17	8	21	14	**25**
8	15	10	2	11	17	1	13	23	20	7	12	6	5	3	0	16	19	21	4	24	14	18	9	22	**25**
9	23	16	11	3	12	18	2	14	24	21	8	13	7	6	4	0	17	20	22	5	1	15	19	10	**25**
10	11	24	17	12	4	13	19	3	15	1	22	9	14	8	7	5	0	18	21	23	6	2	16	20	**25**
11	21	12	1	18	13	5	14	20	4	16	2	23	10	15	9	8	6	0	19	22	24	7	3	17	**25**
12	18	22	13	2	19	14	6	15	21	5	17	3	24	11	16	10	9	7	0	20	23	1	8	4	**25**
13	5	19	23	14	3	20	15	7	16	22	6	18	4	1	12	17	11	10	8	0	21	24	2	9	**25**
14	10	6	20	24	15	4	21	16	8	17	23	7	19	5	2	13	18	12	11	9	0	22	1	3	**25**
15	4	11	7	21	1	16	5	22	17	9	18	24	8	20	6	3	14	19	13	12	10	0	23	2	**25**
16	3	5	12	8	22	2	17	6	23	18	10	19	1	9	21	7	4	15	20	14	13	11	0	24	**25**
17	1	4	6	13	9	23	3	18	7	24	19	11	20	2	10	22	8	5	16	21	15	14	12	0	**25**
18	0	2	5	7	14	10	24	4	19	8	1	20	12	21	3	11	23	9	6	17	22	16	15	13	**25**
19	14	0	3	6	8	15	11	1	5	20	9	2	21	13	22	4	12	24	10	7	18	23	17	16	**25**
20	17	15	0	4	7	9	16	12	2	6	21	10	3	22	14	23	5	13	1	11	8	19	24	18	**25**
21	19	18	16	0	5	8	10	17	13	3	7	22	11	4	23	15	24	6	14	2	12	9	20	1	**25**
22	2	20	19	17	0	6	9	11	18	14	4	8	23	12	5	24	16	1	7	15	3	13	10	21	**25**
23	22	3	21	20	18	0	7	10	12	19	15	5	9	24	13	6	1	17	2	8	16	4	14	11	**25**
24	12	23	4	22	21	19	0	8	11	13	20	16	6	10	1	14	7	2	18	3	9	17	5	15	**25**

Then $|PGL(2,q)| = (q+1)q(q+1)$. It is known that $PGL(2,q)$ is sharply 3-transitive [16,19], hence

$$hd(PGL(2,q)) = (q+1) - 3 + 1 = q - 1. \quad (1)$$

Result 3: $M(10,7) \geq 1504$.

This is an example of type (3). We use the partition and extension technique to show that $M(10,7) \geq 1504$, which improves on the previous lower bound of $M(10,7) \geq 1484$ [13]. Consider $G = PGL(2,8)$ on Z_9, which is sharply 3-transitive, has $504 = 9 \cdot 8 \cdot 7$ elements and shows that $M(9,7) = 504$. We consider two cosets of G, say f_1G and f_2G, where f_1 and f_2 are the permutations defined by the Frobenius mappings $f_1(x) = x^2$ and $f_2(x) = x^4$ [19] and $hd(f_1G, G) = hd(f_2G, G) = hd(f_1G, f_2G) = 6$.

Create the distance-7 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where:

1. $\mathcal{M} = (M_1, M_2, M_3)$, where $M_1 = G$, $M_2 = f_1G$ and the extra set M_3 is f_2G,
2. $\mathcal{P} = (P_1, P_2)$, where $P_1 = \{0,1,2,3\}$, $P_2 = \{4,5,6,7,8\}$, and
3. $\mathcal{Q} = (Q_1, Q_2)$, where $Q_1 = \{0,1,2,3,4\}$, $Q_2 = \{5,6,7,8\}$.

It can be seen that (P_1, Q_1) covers all but four of the permutations in $M_1 = G$. This is because all but 4 of the permutations have one of the integers 0, 1, 2, 3 or 4 (i.e., one of the symbols in Q_1) in one of the first four positions (i.e., a position in P_1). Similarly, (P_2, Q_2) covers all but four of the 504 permutations in M_2. Lastly, the 504 permutations in M_3 are all included. Hence, by Theorem 1, $ext(\Pi)$ is a PA of $1504 = 504 \cdot 3 - 8$ permutations of length 10 with Hamming distance 7. So, by Corollary 1, $M(10,7) \geq 1504$. □

The PA of 1504 permutations for $M(10,7)$ is provided in [2].

Result 4: $M(18,14) \geq 12240$.

Another example of type (3) shows that $M(18,14) \geq 12240$, which improves the previous lower bound of $M(18,14) \geq 4896$ [20]. Consider the projective linear group $G = PGL(2,16)$, which is sharply 3-transitive, has $4080 = 17 \cdot 16 \cdot 15$ elements, and shows that $M(17,15) = 4080$. We use two left cosets of G, namely those with the representatives: $\sigma = (3,5,12,11,14,10,9,8,4,7,6,0,2,1,16,13,15)$, and $\tau = (1,7,3,16,5,15,0,10,9,2,6,8,4,11,13,14,12)$. It can be seen that $hd(\sigma G, G) \geq 13$, $hd(\tau G, G) \geq 13$, and $hd(\sigma G, \tau G) \geq 13$.

Create the distance-14 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where:

1. $\mathcal{M} = (M_1, M_2, M_3)$, where $M_1 = G$, $M_2 = \sigma G$ and the extra set M_3 is τG,
2. $\mathcal{P} = (P_1, P_2)$, where $P_1 = \{0,1,2,3,8,9,10,11\}$, $P_2 = \{4,5,6,7,12,13,14,15,16\}$, and
3. $\mathcal{Q} = (Q_1, Q_2)$, where $Q_1 = \{0,1,2,3,4,5,6,7\}$, $Q_2 = \{8,9,10,11,12,13,14,15,16\}$.

It can be seen that (P_1, Q_1) covers all of the permutations in $M_1 = G$, (P_2, Q_2), covers all of the permutations in M_2. Hence, all of the permutations in $\mathcal{M}$ are covered, and by Corollary 1, $ext(\Pi)$ is a PA of $4080 \cdot 3 = 12240$ permutations of length 18 with Hamming distance 14. So, $M(18,14) \geq 12240$. □

The PA of 12240 permutations for $M(18,14)$ is provided at [2].

Result 5: $M(33,32) \geq 183$.

An example of type (1) shows that $M(33,32) \geq 183$, whereas the previous lower bound, obtained by demonstrating five MOLS of side 33, was $M(33,32) \geq 165$ [21]. Define the group $AGL(1,32) = \{ax + b \mid a, b, x \in GF(32), a \neq 0\}$, which has 992 permutations.

Create the distance-32 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where:

1. $\mathcal{M} = (M_1, M_2, M_3, M_4, M_5, M_6, M_7)$, where $M_1 = B_1$, and M_2 through M_7 are the cosets B_2 through B_7, respectively.

Specifically, for the primitive polynomial $r(x) = x^5 + x^2 + 1$, the element named $\widehat{1}$ is x^0, the element named $\widehat{2}$ is x^1, the element named $\widehat{3}$ is x^2, the element named $\widehat{4}$ is x^3, the element named $\widehat{5}$ is x^4, the element named $\widehat{6}$ is x^5, which is equivalent to $x^2 + 1$ by dividing by the primitive polynomial, and so on. As the non-zero elements form a cyclic group under multiplication, they can be denoted by $x^0, x^1, x^2, \ldots, x^{30}$, and renamed as the remainders of division by the primitive polynomial given above. For example, the addition of $\widehat{1}$ and $\widehat{6}$ is $\widehat{3}$, because $1 + (x^2 + 1)$ is x^2. Note that $1 + 1 = 0$, as the coefficients of the polynomials are added via $GF(2)$. Also, as can be verified, $\widehat{19}$ is $x+1$, so $\widehat{1} + \widehat{2} = \widehat{19}$. Using this process we see that M_1 consists of the 32 permutations given by rows of an addition table for $GF(32)$, where rows 0, 1 and 2 (with hats on top of the names removed) are:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	19	6	30	11	3	28	23	21	17	5	20	24	15	14	25	10	31	2	12	9	26	8	13	16	22	29	7	27	4	18
2	19	0	20	7	31	12	4	29	24	22	18	6	21	25	16	15	26	11	1	3	13	10	27	9	14	17	23	30	8	28	5

where, when viewed as a matrix with entries $m_{i,j}$.
(a) for $i = 0$ and all j $(0 \le j \le 31)$, $m_{0,j} = j$. (This generates the 0th row of M_1 shown above, which consists of the integers 0 through 31 in increasing order).
(b) for $j = 0$ and all i $(1 \le i \le 31)$, $m_{i,0} = m_{0,i}$. (This generates the 0th column of M_1, which is the transpose of the 0th row).
When viewed as a matrix, the diagonal elements of M_1 are zero, and 0th row and 0th column consist of the integers 0 through 31 in increasing order. The sub-matrix starting at row 1 column 1 through row 31 column 31 (except for the main diagonal) is generated row by row, where row $i + 1$ is a right cyclic shift of row i, followed by adding 1 to each element, with the rule that $31 + 1 = 1$.
Furthermore, for all k $(1 < k \le 7)$, M_k is defined as the table with 32 permutations on Z_{32}, in which the 0th column is 0, 1, 2, 3, ..., 31, and each row, excluding the element in the 0th column, is the left cyclic shift of the corresponding row of M_{k-1} (excluding the element in the 0th column).
Note that addition and multiplication are abelian, so the jth row and the jth column of M_i are identical for all $M_i \in \mathcal{M}$.

2. $\mathcal{P} = (P_1, P_2, P_3, P_4, P_5, P_6)$, where $P_1 = \{1, 5, 8, 18, 24, 27\}$, $P_2 = \{2, 9, 13, 21, 30\}$, $P_3 = \{0, 4, 14, 15, 20, 23\}$, $P_4 = \{3, 7, 11, 16\}$, $P_5 = \{10, 12, 19, 25, 28, 29, 31\}$, $P_6 = \{6, 17, 22, 26\}$, and
3. $\mathcal{Q} = (Q_1, Q_2, Q_3, Q_4, Q_5, Q_6)$, where $Q_1 = \{6, 10, 11, 12, 13, 21\}$, $Q_2 = \{3, 8, 15, 16, 20, 24, 29\}$, $Q_3 = \{5, 9, 17, 26, 30\}$, $Q_4 = \{0, 1, 2, 7, 19, 27, 28\}$, $Q_5 = \{18, 23, 25, 31\}$, and $Q_6 = \{4, 14, 22\}$.

(P_1, Q_1) covers 28 permutations in M_1. (P_2, Q_2) covers 29 permutations in M_2. (P_3, Q_3) covers 28 permutations in M_3. (P_4, Q_4) covers 24 permutations in M_4. (P_5, Q_5) covers 27 permutations in M_5 and (P_6, Q_6) covers 12 permutations in M_6. So, by Theorem 1 $hd(ext(\Pi)) \ge 32$, and by Corollary 1, $|ext(\Pi)| = 28+29+26+28+28+12+32 = 183$. Thus, $M(33, 32) \ge 183$. □

Result 6: $M(118, 117) \ge 936$.

We give an example of type (2) for $n = 118$. The previous bound is $M(118, 117) \ge 708$, by demonstrating 6 MOLS of side 118 [5,21]. There are 8 MOLS of side 117 [5,21], hence $M(117, 116) \ge 8 \cdot 117 = 936$. It is known [5] that a set of k MOLS of side n, for integers k and n, can be transformed into a PA, A, of permutations on Z_n with kn elements such that $hd(A) = n - 1$. The transformation is such that the resulting PA A consists of k disjoint sets of permutations, say $M_1, M_2, \ldots, M_k$ such that $hd(M_i) = n$ and $hd(M_i, M_j) = n - 1$,

for all i, j $(1 \leq i < j \leq k)$. By the partition and extension technique we cover all 936 permutations in the PA A. Therefore, $M(118, 117) \geq 936$. The PA of 936 permutations for $M(118, 117)$ is provided in [2].

A natural question arises. Is it possible to use the partition and extension operation iteratively to obtain PA's on Z_{n+k}, for $k > 1$? The answer is a qualified "yes", but improved lower bounds may result only for large n. To see this consider the following: Given a distance-n partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ for Z_n, where $\mathcal{M} = (M_1, M_2, \ldots, M_s, M_{s+1})$, $\mathcal{P} = (P_1, P_2, \ldots, P_s)$, and $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_s)$, we can obtain an extended set of permutations, namely $ext(\Pi)$, which consists of permutations of Z_{n+1} with Hamming distance n. For all i, $ext(M_i)$ does not have Hamming distance $n+1$, because the new symbol n in Z_{n+1} (but not in Z_n) is often inserted in the same position by the extension operation. So, the ordered list of sets $M' = (ext(M_1), ext(M_2), \ldots, ext(M_s), ext(M_{s+1}))$, is not appropriate for a distance-$(n+1)$ partition system. Subsets of these PA's can be used for another extension. For each set $ext(M_i)$ we create a collection of subsets with Hamming distance $n+1$. For a pair of integers u, v, with u in $\mathcal{P}_i$ and v in Q_i, let $perm(u, v)$ be a permutation σ in M_i such that $\sigma(u) = v$. Note that there is at most one permutation in M_i with this property, because $hd(M_i) = n$. It follows that $ext_u(\sigma)$ has the symbol n in position u and the symbol v in position n. Let $r \neq u$ be a position, let $t \neq v$ be a symbol, and let $\tau = perm(r, t)$. Then the Hamming distance between σ and τ is $n+1$. That is, the new symbol n in Z_{n+1} in $ext_u(\sigma)$ is in position u and in $ext_r(\tau)$ is in position r, with $u \neq r$, and the symbols in position n in $ext_u(\sigma)$ and $ext_v(\tau)$, respectively, are v and t with $v \neq t$. It follows that, for any set of pairs $A = \{(u_1, v_1), (u_2, v_2), \ldots, (u_m, v_m)\}$ such that no two pairs agree in either coordinate, the subset $M_i(A) = \{perm(u_i, v_j) \mid (u_i, v_j) \in A, \forall j, (1 \leq j \leq m)\}$ has Hamming distance $n+1$. That is, the sets $ext(M_i)$ can be partitioned into subsets, each with Hamming distance $n+1$. This allows, for suitable partitions P' and Q', a distance-$(n+1)$ partition system $\Pi' = (\mathcal{M}', \mathcal{P}', \mathcal{Q}')$ for Z_{n+1}. It should be noted that the sets in $\mathcal{M}'$ are much smaller than the sets in $\mathcal{M}$ and, hence, the size of the PA produced by the partition and extension operation is also smaller.

For suitably large n, which is, say, 2 more than a power of a prime, iteration of the partition and extension operation could produce better bounds for $M(n, n-1)$ than can be achieved with MOLS. This is an area of continuing research.

Many other examples of improved values for $M(n, n-1)$ exist. For many small integers we did the partition and extension by hand. We also developed a simple program for computing partitions and extensions of PA's and used it on primes p, $61 \leq p \leq 309$ to construct PAs for $n = p+1$. For each such prime, the program uses partitions of $m = \lfloor \sqrt{p} \rfloor$ consecutive integers, that is, for all i, $(1 \leq i \leq \lfloor p/m \rfloor)$, it uses the set $P_i = Q_i = \{(i-1)m, (i-1)m+1, \ldots, (i-1)m+(m-1)\}$ and determines the number of permutations covered by (P_i, Q_i) in whichever coset (among those remaining) maximizes the number. Because of the arithmetic, since $\lfloor p/m \rfloor \cdot m$ is less than p, there are $t = p - \lfloor p/m \rfloor \cdot m$ of positions and symbols not used so far. The program chooses another coset and uses a partition consisting of these t symbols and positions to cover additional permutations in this coset. Finally, the program includes an additional coset (M_{s+1} in the definition of distance-d partition systems) from the remaining cosets. Recall that for M_{s+1}, no symbols are swapped, but the permutations are extended by putting the integer p in position p (at the end) of each permutation. This gives us a distance-p partition system Π. The size of the resulting $ext(\Pi)$ is our lower bound for $M(p+1, p)$. Our new results are summarized in Table 4 along with other known bounds $M(n, n-1)$ for $10 \leq n \leq 309$. PAs that exhibit some of our improved results are provided in [2]. In Table 4, improved lower bounds by our techniques, if known, are given in bold at the top of a cell. The second entry gives the

Table 4 Lower bounds for $M(n, n-1)$, for $n \in \{10, 11, \ldots, 309\}$

	0	1	2	3	4	5	6	7	8	9
10	49 [12]	–	112 [11]	–	59 [11]	90 [11]	–	–	–	–
	20	110	60	156	56	60	240	272	90	342
	2	10	5	12	4	4	15	16	5	18
20	120 [11]	147 [11]	121 [11]	–	–	–	**130**	–	–	–
	80	105	66	506	168	600	104	702	140	812
	4	5	3	22	7	24	4	26	5	28
30	**170**	–	–	**183**	–	–	–	–	**254**	–
	120	930	992	165	136	175	288	1332	152	195
	4	30	31	5	4	5	8	36	4	5
40	–	–	**282**	–	**296**	–	–	–	–	–
	280	1640	210	1806	220	270	184	2162	384	2352
	7	40	5	42	5	6	4	46	8	48
50	–	–	–	–	**408**	–	–	–	–	–
	300	255	260	2756	270	330	392	399	290	3422
	6	5	5	52	5	6	7	7	5	58
60	**481**	–	**478**	–	–	–	–	–	**568**	–
	300	3660	310	378	4032	455	330	4422	340	414
	5	60	5	6	63	7	5	66	5	6
70	–	–	**588**	–	**620**	–	–	–	–	–
	420	4970	504	5256	370	525	456	462	468	6162
	6	70	7	72	5	7	6	6	6	78
80	–	–	–	–	**776**	–	–	–	–	–
	720	6480	656	6806	504	510	516	522	616	7832
	9	80	8	82	6	6	6	6	7	88
90	**866**	–	–	–	–	–	–	–	**956**	–
	540	637	552	558	564	570	672	9312	588	792
	6	7	6	6	6	6	7	96	6	8
100	–	–	**1030**	–	**1070**	–	–	–	**1090**	–
	800	10100	612	10506	728	735	636	11342	648	11772
	8	100	6	102	7	7	6	106	6	108
110	**1130**	–	–	–	**1192**	–	–	–	**936**	–
	660	666	1456	12656	684	805	696	936	708	714
	6	6	13	112	6	7	6	8	6	6
120	–	–	–	–	–	–	–	–	–	–
	840	14520	732	738	744	15500	756	16002	16256	903
	7	120	6	6	6	124	6	126	127	7
130	–	–	**1508**	–	–	–	–	–	**1614**	–
	780	17030	792	931	804	945	952	18632	828	19182
	6	130	6	7	6	7	7	136	6	138

Table 4 continued

	0	1	2	3	4	5	6	7	8	9
140	**1640**	–	–	–	–	–	–	–	–	–
	840	987	852	1430	1440	1015	876	1029	888	22052
	6	7	6	10	10	7	6	7	6	148
150	**1818**	–	**1832**	–	–	–	–	–	**1922**	–
	900	22650	1064	1224	1232	1085	936	24492	1106	954
	6	150	7	8	8	7	6	156	7	6
160	–	–	–	–	**2042**	–	–	–	**2070**	–
	1440	1127	972	26406	984	1155	996	27722	1176	28392
	9	7	6	162	6	7	6	166	7	168
170	–	–	–	–	**2316**	–	–	–	–	–
	1020	1368	1032	29756	1044	1050	2464	1593	1068	31862
	6	8	6	172	6	6	14	9	6	178
180	**2404**	–	**2498**	–	–	–	–	–	–	–
	1080	32580	1092	1098	1288	1665	1116	1870	1128	1512
	6	180	6	6	7	9	6	10	6	8
190	–	–	**2638**	–	**2680**	–	–	–	**2786**	–
	1140	36290	1344	37056	1164	1365	1176	38612	1188	39402
	6	190	7	192	6	7	6	196	6	198
200	**2842**	–	–	–	–	–	–	–	–	–
	1400	1407	1212	1421	1224	1640	1236	1656	2912	2299
	7	7	6	7	6	8	6	8	14	11
210	–	–	**3026**	–	–	–	–	–	–	–
	2100	44310	1272	1491	1284	1505	1512	1736	1308	2190
	10	210	6	7	6	7	7	8	6	10
220	–	–	–	–	**3260**	–	–	–	**3380**	–
	1320	2652	1332	49506	2912	1800	1356	51302	1368	52212
	6	12	6	222	13	8	6	226	6	228
230	**3512**	–	–	–	**3602**	–	–	–	–	–
	1380	1617	1624	54056	1404	1645	1416	1659	1428	56882
	6	7	7	232	6	7	6	7	6	238
240	**3656**	–	**3716**	–	–	–	–	–	–	–
	1680	57840	1452	58806	1464	1715	1476	2964	1736	1743
	7	240	6	242	6	7	6	12	7	7
250	–	–	**3932**	–	–	–	–	–	**4066**	–
	1500	62750	1512	3036	2286	1785	65280	65792	1548	3108
	6	250	6	12	9	7	255	256	6	12
260	–	–	–	–	**4228**	–	–	–	–	–
	1560	2088	2096	68906	1848	2120	1862	2670	1876	72092
	6	8	8	262	7	8	7	10	7	268
270	**4318**	–	**4408**	–	–	–	–	–	**4574**	–
	1890	73170	4080	4368	1644	3575	2760	76452	1668	2511

Table 4 continued

	0	1	2	3	4	5	6	7	8	9
	7	270	15	16	6	13	10	276	6	9
280	–	–	**4684**	–	**4706**	–	–	–	–	–
	1960	78680	1692	79806	1704	3420	1716	2009	4320	83232
	7	280	6	282	6	12	6	7	15	288
290	–	–	–	–	**5068**	–	–	–	–	–
	1740	1746	1752	85556	1764	1770	2072	2970	2980	3588
	6	6	6	292	6	6	7	10	10	12
300	–	–	–	–	–	–	–	–	**5360**	–
	2100	2107	2114	2121	4560	4575	1836	93942	2156	2163
	7	7	7	7	15	15	6	306	7	7

For each entry, the first row, if present, contains bounds better than the bounds derived from MOLS, which are in the second row. The bounds in bold are obtained in this paper. The third row indicates the number of MOLS which can be found in [5,21]

previous lower bound. If the second entry comes from MOLS, the number of MOLS is given in the bottom entry of the cell.

4 A new lower bound for $M(p+1, p)$, for primes p

Previous lower bounds for $M(n, n-1)$ have been obtained by exhibiting sets of mutually orthogonal Latin squares (MOLS). Optimum results are known for powers of primes. When n is a power of a prime $M(n, n-1) = n(n-1)$; otherwise, finding a large set of MOLS is a combinatorial problem of considerable difficulty and ongoing interest [5,18]. Work has also been done on establishing an asymptotic lower bound on the number of MOLS. Let $N(n)$ denote the number of MOLS of side n. It is known that $N(n) \geq n^{1/14.8}$ for sufficiently large n [3]. As previously mentioned, for any positive integer n, if there are k mutually orthogonal Latin squares of side n, then $M(n, n-1) \geq kn$ [6]. From this we obtain $M(n, n-1) \geq n^{1+1/14.8}$ for sufficiently large n.

Using the partition and extension technique, we now show that for primes p, $M(p+1, p) \geq p^{1.5}/2 - O(p)$. So, for an infinite set of integers, the partition and extension technique provides an asymptotically better lower bound than that given by current knowledge about MOLS.

The proof considers, for each prime $p \geq 17$, partitions $\mathcal{P}$ and $\mathcal{Q}$, where $\mathcal{P} = \{P_1, P_2, P_3, \ldots, P_{t(p)}\}$, $\mathcal{Q} = \{Q_1, Q_2, Q_3, \ldots, Q_{t(p)}\}$, $P_i = Q_i = \{(i-1)s(p), (i-1)s(p)+1, (i-1)s(p)+2, \ldots, is(p)-1\}$, and where $s(p) = \lfloor \sqrt{p}/2 \rfloor$ and $t(p) \leq \lfloor p/(s(p)) \rfloor$ will be selected later. Note that the number of positions included in $\mathcal{P}$ is $s(p)t(p)$, which is less than or equal to p. The same is true for the number of symbols in $\mathcal{Q}$. In order to ensure that $\mathcal{P}$ and $\mathcal{Q}$ are partitions, we can add the missing elements to an arbitrary set P_k (resp. Q_k). This addition has no effect on the proof of Lemma 1. The important property is that the sets comprising $\mathcal{P}$ are pairwise disjoint (and likewise for $\mathcal{Q}$).

Lemma 1 *For any prime $p \geq 17$, and for any j, $s(p) \leq j \leq 3s(p)$ or $-3s(p) \leq j \leq -s(p)$, the permutations in the coset $B_j = \{jx + b \mid b \in GF(p)\}$ are uniquely covered by (P_i, Q_i), where $P_i = Q_i = \{(i-1)s(p), (i-1)s(p)+1, (i-1)s(p)+2, \ldots, is(p)-1\}$, for all i $(1 \leq i \leq t(p))$.*

Proof First, let $b = 0$. We show that, for any choice of j, with $s(p) \leq j \leq 3s(p)$, and for any position x in $P_1 = \{0, 1, \ldots, s(p) - 1\}$, the permutation $\pi_0(x) = jx \ (mod\ p)$ cannot have two values in $Q_1 = \{0, 1, \ldots, s(p) - 1\}$. In particular, the values in these specific positions are: $\pi_0(0) = 0, \pi_0(1) = j, \pi_0(2) = 2j, \ldots, \pi_0(s(p)-1) = (s(p)-1)j$. Since $j \geq s(p)$, all of the values except $\pi_0(0) = 0$ are larger than the elements in Q_1, at least when we do not compute remainders modulo p. Since $j \leq 3s(p)$, the largest such value, say L, when $j = 3s(p)$, namely $L = \pi_0(s(p) - 1) = (s(p) - 1)j$, is at most $(s(p) - 1)3s(p) = (\lfloor\sqrt{p}/2\rfloor - 1)3(\lfloor\sqrt{p}/2\rfloor) < 3p/4 < p$. For all values $v \neq 0$ in $V = \{0, j, 2j, \ldots, L = s(p)j\}$, $s(p) \leq v < p$ and the remainder of v divided by p is equal to v. Thus, only one value in V, namely, $\pi_0(0) = 0$, occurs in Q_1. Hence, π_0 is uniquely covered by (P_1, Q_1).

Observe that other permutations in the coset B_j, namely $\pi_b(x) = jx + b \ (mod\ p)$ for $0 < b < p$, which represent all cyclic shifts of π_0, have the same property. That is, if $\pi_b(0) = j \cdot 0 + b \ (mod\ p) = b$ is in Q_1, then $\pi_b(1) = j + b, \pi_b(2) = 2j + b, \ldots, \pi_b(s(p) - 1) = (s(p) - 1)j + b$ are all larger than the elements of Q_1, at least when we don't compute remainders modulo p. Again since $j \leq 3s(p)$, the largest such value, say L, when $j = 3s(p)$, namely $L = \pi_b(s(p) - 1) = (s(p) - 1)j + b$, is at most $(s(p) - 1)3s(p) + b = (\lfloor\sqrt{p}/2\rfloor - 1)3\lfloor\sqrt{p}/2\rfloor + \lfloor\sqrt{p}/2\rfloor - 1 < 3p/4 - \lfloor\sqrt{p}/2\rfloor - 1 < 4p/4 \leq p$. (Note that $b \leq \lfloor\sqrt{p}/2\rfloor - 1$, since b is in Q_1.) So, in fact, for each value v in $V = \{b, j + b, 2j + b, \ldots, L = (s(p) - 1)j + b\}$, the remainder of v divided by p is equal to v. Thus, only one value in V, namely, $\pi_b(0) = b$, occurs in Q_1. Hence, π_b is uniquely covered by (P_1, Q_1). That is, every covered permutation in the coset B_j is uniquely covered by (P_1, Q_1).

By a symmetric argument we can show that cosets B_j, with $-3s(p) \leq j \leq -s(p)$, are also uniquely covered by (P_1, Q_1). That is, in this case, one subtracts j instead of adding, but otherwise the argument is the same.

We may also generalize to the sets (P_i, Q_i), for $0 < i \leq t(p)$. In the first paragraph of this proof it was shown that for each j, with $s(p) \leq j \leq 3s(p)$, the permutation $\pi(j) = jx \ (mod\ p)$ cannot have two values in $Q_i = \{(i - 1)s(p), (i - 1)s(p) + 1, \ldots, i \cdot s(p) - 1\}$. Furthermore, as shown in the first paragraph of the proof, the maximum element in the sequence $j, 2j, 3j, \ldots, (s(p) - 1)j$ is less than p, so even when considering remainders modulo p it is not possible for two values to be in Q_i. Together with the generalization in the second paragraph to permutations of the form $\pi(j) = jx + b \ (mod\ p)$, we have shown that every covered permutation in the coset $B_j = \{jx + b \mid b \in GF(p)\}$ is uniquely covered by (P_i, Q_i), $P_i = Q_i = \{(i - 1)s(p), (i - 1)s(p) + 1, (i - 1)s(p) + 2, \ldots, is(p) - 1\}$, for all i $(1 \leq i \leq t(p))$. □

Theorem 2 *For primes p, $M(p + 1, p) \geq p^{1.5}/2 - O(p)$.*

Proof Create the distance-p partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ on Z_p, where:

1. $\mathcal{M} = (M_1, M_2, \ldots, M_{t(p)+1})$, where $M_j = B_j$ as described above, and $M_{t(p)+1}$ is an additional coset that is not part of the partition process,
2. $\mathcal{P} = (P_1, P_2, \ldots, P_{t(p)})$,
3. $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_{t(p)})$.

By Theorem 1, $hd(ext(\Pi)) \geq p$. By Lemma 1, for any prime $p \geq 17$, the covered permutations in the cosets B_j, for all j $(s(p) \leq j \leq 3s(p)$ or $-3s(p) \leq j \leq -s(p))$, are uniquely covered by (P_i, Q_i). All of these cosets are candidates for sets M_i. Recall that we can select at most $\lfloor p/\lfloor\sqrt{p}/2\rfloor\rfloor$ cosets. Hence the number of cosets to be partitioned and extended is

$$t(p) = \min\{4\lfloor\sqrt{p}/2\rfloor + 2, \lfloor p/\lfloor\sqrt{p}/2\rfloor\rfloor\}.$$

We show that

$$\min\{4\lfloor\sqrt{p}/2\rfloor + 2, \lfloor p/\lfloor\sqrt{p}/2\rfloor\rfloor\} \geq 2\sqrt{p} - 2,$$

by noting that

(i) $4\lfloor\sqrt{p}/2\rfloor + 2 \geq 2\sqrt{p} - 2$ or, equivalently, $\lfloor\sqrt{p}/2\rfloor \geq \sqrt{p}/2 - 1$, and
(ii) $p/\lfloor\sqrt{p}/2\rfloor \geq 2\sqrt{p}$ or, equivalently, $\lfloor\sqrt{p}/2\rfloor \leq \sqrt{p}/2$.

When we have sets M_i of permutations on Z_p such that $hd(M_i) = p$, if the permutations are uniquely covered, then M_i is well covered. That is, when M_i is viewed as a matrix with rows corresponding to permutations, each symbol v_k in Q_i appears once in each column u_j. So, for each column u_j there are $|Q_i|$ covered permutations. Since the permutations are uniquely covered, none of the permutations covered in column u_j are covered by another column u_r ($r \neq j$). So, altogether $|covered(M_i)| = |P_i| \cdot |Q_i|$ for all i. Hence $\mathcal{M}$ is well covered by $\mathcal{P} = (P_1, P_2, \ldots, P_{t(p)})$ and $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_{t(p)})$. So, by Corollary 1, $|ext(\Pi)| = |M_{t(p)+1}| + \sum_{i=1}^{t(p)} |P_i| \cdot |Q_i| = p + \sum_{i=1}^{t(p)} |P_i| \cdot |Q_i|$. There are $|P_i| \cdot |Q_i| = \lfloor\sqrt{p}/2\rfloor^2 \geq (\sqrt{p}/2 - 1)^2 = p/4 - \sqrt{p} + 1$ covered permutations in each covered coset. Hence, the total number of covered permutations is at least

$$p + (2\sqrt{p} - 2) \cdot (p/4 - \sqrt{p} + 1) = p^{1.5}/2 - 3p/2 + 4\sqrt{p} - 2. \tag{2}$$

The theorem follows. □

As an example, consider the prime $p = 10007$. By Eq. (2), $M(10008, 10007) \geq 10007^{1.5}/2 - 3 \cdot 10007/2 + 4 \cdot 10007^{0.5} - 2 \geq 485,912$. With more care in the choice of a partition system, we conjecture that one can show $M(10008, 10007)$ is at least one million.

5 Conclusions

Using a new partition and extension operation, we have given an algorithm for creating permutation arrays with a larger number of permutations than those generated by previous techniques. Hence, we improve results for $M(n, d)$ for various values of n and d. The size of the permutation arrays obtained by our techniques is related to the quality of the partitions, and it is quite likely that the results can be further improved by additional effort. Finding better values for $M(n, d)$ is an ongoing area of research.

The partition and extension operation has also allowed us to improve previous lower bounds on $M(n, n-1)$ which were obtained from MOLS. Our results are constructive. We use the partition and extension technique to build permutation arrays for primes p that exhibit $M(p+1, p) \geq p^{1.5}/2 - O(p)$. Explicitly, for any prime $p \geq 17$ the technique yields a permutation array of $p^{1.5}/2 - 1.5p + 4\sqrt{p} - 2$ permutations at Hamming distance p. Results for $M(n, d)$ can be obtained from our website [1]. Permutation arrays exhibiting some of our results can be found in [2].

Acknowledgements We would like to thank the referees for their many helpful suggestions and valuable comments.

References

1. Bereg S., Morales L., Sudborough I.: Table of lower bounds for $M(n, n-1)$. http://www.utdallas.edu/~sxb027100/soft/permutation-arrays/n-1/ (2016).
2. Bereg S., Morales L., Sudborough I.: PAs exhibiting results from partition and extension. http://www.utdallas.edu/~sxb027100/soft/permutation-arrays/n-1/data.zip (2016).
3. Beth T.: Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren. Abh. Math. Sem. Hamburg. **53**, 284–288 (1983).
4. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**, 51–64 (2004).
5. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs, 2nd edn. Chapman and Hall/CRC, New York (2006).
6. 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).
7. Deza M., Vanstone S.A.: Bounds for permutation arrays. J. Stat. Plan. Inference **2**, 197–209 (1978).
8. Frankl P., Deza M.: On the maximum number of permutations with given maximal or minimal distance. J. Comb. Theory A **22**, 352–360 (1977).
9. Gao F., Yang Y., Ge G.: An improvement on the Gilbert-Varshamov bound for permutation codes. IEEE Trans. Inf. Theory **59**, 3059–3063 (2013).
10. Huang Y.-Y., Tsai S.-C., Wu H.-L.: On the construction of permutation arrays via mappings from binary vectors to permutations. Des. Codes Cryptogr. **40**, 139–155 (2006).
11. Huczynska S.: Powerline communication and the 36 officers problem. Philos. Trans. R. Soc. Lond. A **364**, 3199–3214 (2006).
12. Janiszczak I., Staszewski R.: An Improved Bound for Permutation Arrays of Length 10. Technical Report 4. Institute for Experimental Mathematics, University Duisburg-Essen, Essen (2008).
13. Janiszczak I., Lempken W., Östergård P.R.J., Staszewski R.: Permutation codes invariant under isometries. Des. Codes Cryptogr. **75**, 497–507 (2015).
14. Lin T.-T., Tsai S.-C., Tzeng W.-G.: Efficient encoding and decoding with permutation arrays. In: IEEE International Symposium on Information Theory (ISIT'08), pp. 211–214 (2008).
15. Nguyen Q.T.: Transitivity and hamming distance of permutation arrays. PhD thesis, University of Texas at Dallas Richardson, TX (2013).
16. Passman D.: Permutation Groups. Benjamin Inc, New York (1968).
17. Pavlidou N., Vinck A.H., Yazdani J., Honary B.: Power line communications: state of the art and future trends. IEEE Commun. Mag. **41**, 34–40 (2003).
18. Quistorff J.: A new nonexistence result for sharply multiply transitive permutation sets. Discret. Math. **288**, 185–186 (2004).
19. Rotman J.J.: An Introduction to the Theory of Groups, 4th edn. Springer, New York (1995).
20. Smith D.H., Montemanni R.: A new table of permutation codes. Des. Codes Cryptogr. **63**, 241–253 (2012).
21. The Sage Developers: Mutually Orthogonal Latin Squares (MOLS). http://doc.sagemath.org/html/en/reference/combinat/sage/combinat/designs/latin_squares.html.