Designs, Codes and Cryptography (2020) 88:311–339
https://doi.org/10.1007/s10623-019-00684-z

Constructing permutation arrays using partition and extension

Sergey Bereg[1] · Luis Gerardo Mojica[1] · Linda Morales[1] · Hal Sudborough[1]

Received: 22 February 2019 / Revised: 24 July 2019 / Accepted: 23 September 2019 /
Published online: 13 October 2019

Abstract
We give new lower bounds for $M(n, d)$, for various positive integers n and d with $n > d$, where $M(n, d)$ is the largest number of permutations on n symbols with pairwise Hamming distance at least d. Large sets of permutations on n symbols with pairwise Hamming distance d are needed for constructing error correcting permutation codes, which have been proposed for power-line communications. Our technique, *partition and extension*, is universally applicable to constructing such sets for all n and all d, $d < n$. We describe three new techniques, *sequential partition and extension*, *parallel partition and extension*, and a *modified Kronecker product operation*, which extend the applicability of partition and extension in different ways. We describe how partition and extension gives improved lower bounds for $M(n, n-1)$ using mutually orthogonal Latin squares (MOLS). We present efficient algorithms for computing new partitions: an iterative greedy algorithm and an algorithm based on integer linear programming. These algorithms yield partitions of positions (or symbols) used as input to our partition and extension techniques. We report many new lower bounds for $M(n, d)$ found using these techniques for n up to 600.

Keywords Permutation arrays · Partition and extension · Kronecker product · Coset method

Mathematics Subject Classification 05A05 · 94B25 · 05E20 · 05A18

1 Introduction

The use of permutation codes for error correction of communications transmitted over power-lines has been suggested [17,22]. Due to the extreme noise in such channels, codewords are sent by frequency modulation rather than by amplitude modulation. Let's say we use

Communicated by C. J. Colbourn.

Sergey Bereg was supported in part by NSF award CCF-1718994.

✉ Sergey Bereg
besp@utdallas.edu

[1] Department of Computer Science, University of Texas at Dallas, Box 830688, Richardson, TX 75083, USA

frequencies $f_0, f_1, f_2, \ldots, f_{n-1}$, which we view by the index set $Z_n = \{0, 1, 2, \cdots, n-1\}$. A permutation on Z_n, corresponding to a codeword, specifies in which order frequencies are to be sent.

The Hamming distance between two permutations, σ and τ on Z_n, denoted by $hd(\sigma, \tau)$, is the number of positions x in Z_n such that $\sigma(x) \neq \tau(x)$. For example, the permutations on Z_5, $\sigma = 0\ 4\ 1\ 3\ 2$ and $\tau = 2\ 4\ 3\ 1\ 2$ have $hd(\sigma, \tau) = 3$, as they differ in positions 0, 2, and 3. A set A of permutations on Z_n (called a *permutation array* or *PA* for short) has Hamming distance d, denoted by $hd(A) \geq d$, if, for all $\sigma, \tau \in A$, $hd(\sigma, \tau) \geq d$. The maximum size of a PA A on Z_n with $hd(A) \geq d$ is denoted by $M(n, d)$. Two PAs A and B have Hamming distance d, denoted by $hd(A, B) \geq d$, if, for all $\sigma \in A$ and $\tau \in B$, $hd(\sigma, \tau) \geq d$.

There are known combinatorial upper and lower bounds on $M(n, d)$, specifically the Gilbert–Varshamov (*GV*) bounds, together with some recent improvements to the *GV* bounds [11,13,25]. Generally, these bounds are theoretical and are often improved by empirical techniques. Some exact values are known: (1) for all n, $M(n, n) = n$, and, (2) for q, a power of a prime, $M(q, q-1) = q(q-1)$ and $M(q+1, q-1) = (q+1)q(q-1)$. These exact values come from sharply k-transitive groups, for $k = 2$ and $k = 3$, namely the affine general linear group, denoted by *AGL*, and the projective general linear group, denoted by *PGL* [10,11]. The Mathieu sharply 4-transitive and 5-transitive groups, give exact values for $M(11, 8) = 7920$ and $M(12, 8) = 95{,}040$ [6,10,12]. It is not feasible to do an exhaustive search for good permutation arrays when n becomes large. There are $n!$ permutations on Z_n, so the search space becomes computationally impractical. Some researchers have attempted to mitigate the problem by considering automorphisms groups and replacing permutations by sets of permutations. For example, in [19], Janiszczak et al. considered sets of permutations invariant under isometries to improve several lower bounds for $M(n, d)$, for various choices of n and d, $n \leq 22$. Chu et al. [7] and Smith and Montemanni [23] also provide lower bounds obtained by the use of automorphism groups, and are also generally limited to small values of n.

There is also a connection between mutually orthogonal Latin squares (MOLS) and permutation arrays [9]. Specifically, if there are k mutually orthogonal Latin squares of side n, then $M(n, n-1) \geq kn$. Let $N(n)$ denote the number of mutually orthogonal Latin squares of side n. Finding better lower bounds for $N(n)$ is an on-going combinatorial problem of considerable interest world-wide [8,24].

Recently, we described a new technique, called *partition and extension* [3,4] and we illustrated how to use this technique to improve several lower bounds for $M(n, n-1)$ over those given by MOLS. Partition and extension operates on permutation arrays that can be decomposed into subsets with certain properties. (A description follows in Sect. 2.) In its simplest form, partition and extension converts a PA A on n symbols with $hd(A) = d - 1$, into a PA A' on $n+1$ symbols with $hd(A') = d$. That is, when a PA A exhibiting $M(n, d-1)$ meets the necessary conditions for simple partition and extension, the technique obtains a lower bound for $M(n+1, d)$.

The purpose of this paper is to illustrate many new ways to use the partition and extension technique, and ways to generate appropriate partitions. We describe a method called *sequential partition and extension*, an improvement which uses iteration to extend permutation arrays by two or more symbols. When certain conditions are met, sequential partition and extension obtains new PAs on $n+2$ symbols with Hamming distance d from PAs on n symbols with Hamming distance $d-1$. Another new technique, which we call *parallel partition and extension*, introduces several new symbols simultaneously. In some cases, parallel partition and extension on PAs on n symbols with Hamming distance $d-r$ gives new lower bounds for $M(n+r, d)$. We illustrate how to use partition and extension on blocks defined by cosets of the cyclic subgroup of the group $AGL(1, q)$, and on PAs created by a modified Kronecker product operation. We give new results derived from partition and extension on blocks defined by mutually orthogonal Latin squares (MOLS). We describe experimental algorithms and heuristics for creating partitions, including a greedy algorithm and an optimization approach based on integer linear programming. These new techniques improve on previously reported results [4].

2 Previous results on partition and extension

We briefly describe the technique called *partition and extension*, which transforms a PA on Z_n with Hamming distance $d-1$ into a PA on Z_{n+1} with Hamming distance d. A detailed description and several examples appear in [4]. Throughout this paper we will use the phrase *simple partition and extension* to refer to this version of partition and extension.

Let s be a positive integer. Let $M_1, M_2, \ldots, M_s$ be an ordered list of s pairwise disjoint permutation arrays on Z_n. 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. For each set M_i, P_i is the set of locations and Q_i is the set of symbols to be replaced by the new symbol n. When a permutation σ in M_i has a symbol q in Q_i appearing in a position p in P_i, σ is extended (i.e., converted to a permutation σ' on $n+1$ symbols) by moving q to the end of the permutation and placing the symbol n in position p. That is, 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 for all j $(0 \leq j < n, j \neq k)$, $\sigma'(j) = \sigma(j)$. We refer to this new permutation as $ext(\sigma)$ and σ' interchangeably.

For each i, let $covered(M_i)$ be the subset of M_i, defined by $covered(M_i) = \{\sigma \in M_i \mid \exists p \in P_i,\ \sigma(p) \in Q_i\}$. We say that a permutation σ is *covered* if $\sigma \in covered(M_i)$ for some i. In order for a permutation σ' to be included in the extended set of permutations on Z_{n+1}, σ must be covered. That is, σ must have one of the named symbols in one of the named positions. In general, 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 to cover σ.

For our construction, we include an additional PA 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 PAs M_i. The partition and extension operation adds the new symbol n to the end of each permutation in M_{s+1}. Every permutation in M_{s+1} is used in the construction of our new PA. Thus, we create the list $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$, which includes this extra set.

A triple $\Pi = (\mathcal{M}, P, Q)$ is a *distance-d partition system* for Z_n if it satisfies the following properties:

(I) $\forall M_i \in \mathcal{M},\ hd(M_i) \geq d$, and
(II) $\forall i, j\ (1 \leq i < j \leq s+1),\ hd(M_i, M_j) \geq d-1$.

Simple 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 $1 \leq i \leq s$, 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 simple partition and extension operation creates a new permutation array $ext(\Pi)$ on Z_{n+1}. For all i $(1 \leq i \leq s)$, let $ext(M_i)$ be the set of permutations defined by

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

Table 1 An example of simple partition and extension on the distance-4 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where $\mathcal{M} = (M_1, M_2, M_3)$, $\mathcal{P} = \{\{0, 2\}, \{1, 3\}\}$ and $\mathcal{Q} = \{\{0, 1\}, \{2, 3\}\}$

Initial permutations in Π	Modified permutations in $ext(\Pi)$
$M_1 = \begin{bmatrix} \mathbf{0} & 1 & 2 & 3 \\ \mathbf{1} & 0 & 3 & 2 \\ 2 & 3 & \mathbf{0} & 1 \\ 3 & 2 & \mathbf{1} & 0 \end{bmatrix}$	$ext(M_1) = \begin{bmatrix} \mathbf{4} & 1 & 2 & 3 & \mathbf{0} \\ \mathbf{4} & 0 & 3 & 2 & \mathbf{1} \\ 2 & 3 & \mathbf{4} & 1 & \mathbf{0} \\ 3 & 2 & \mathbf{4} & 0 & \mathbf{1} \end{bmatrix}$
$M_2 = \begin{bmatrix} 0 & \mathbf{2} & 3 & 1 \\ 1 & \mathbf{3} & 2 & 0 \\ 2 & 0 & 1 & \mathbf{3} \\ 3 & 1 & 0 & \mathbf{2} \end{bmatrix}$	$ext(M_2) = \begin{bmatrix} 0 & \mathbf{4} & 3 & 1 & \mathbf{2} \\ 1 & \mathbf{4} & 2 & 0 & \mathbf{3} \\ 2 & 0 & 1 & \mathbf{4} & \mathbf{3} \\ 3 & 1 & 0 & \mathbf{4} & \mathbf{2} \end{bmatrix}$
$M_3 = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \end{bmatrix}$	$ext(M_3) = \begin{bmatrix} 0 & 3 & 1 & 2 & \mathbf{4} \\ 1 & 2 & 0 & 3 & \mathbf{4} \\ 2 & 1 & 3 & 0 & \mathbf{4} \\ 3 & 0 & 2 & 1 & \mathbf{4} \end{bmatrix}$

The column on the left shows the ordered list of PAs $\mathcal{M}$ consisting three PAs, M_1, M_2 and M_3 on Z_4 with $hd(M_i) \geq 4$, for $i \in \{1, 2, 3\}$, and $hd(\mathcal{M}) \geq 3$. The column on the right shows the new PAs, $ext(M_1)$, $ext(M_2)$ and $ext(M_3)$, obtained by simple partition and extension. By Theorem 1, $hd(ext(\Pi)) \geq 4$

For M_{s+1}, let $ext(M_{s+1})$ be the set of permutations on Z_{n+1} defined by adding the symbol n to the end of every permutation of M_{s+1}.

Let $ext(\Pi)$ be the set of permutations on Z_{n+1} defined by

$$ext(\Pi) = \bigcup_{i=1}^{s+1} ext(M_i).$$

Note that

$$|ext(\Pi)| = \sum_{i=1}^{s+1} |ext(M_i)|. \quad (1)$$

Theorem 1 ([4]) *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 simple partition and extension. Then, $hd(ext(\Pi)) \geq d$.*

The example in Table 1 illustrates the application of Theorem 1 to $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, where $\mathcal{M} = (M_1, M_2, M_3)$, $\mathcal{P} = \{\{0, 2\}, \{1, 3\}\}$ and $\mathcal{Q} = \{\{0, 1\}, \{2, 3\}\}$. The column on the left shows the PAs M_1, M_2 and M_2. M_1 is the cyclic subgroup of $AGL(1, 4)$, and M_2 and M_3 are two of its cosets. The blue symbols are the symbols of Q_i that occupy positions in P_i, for $i \in 1, 2$. The column on the right shows the new PAs obtained by simple partition and extension on Π. To create $ext(M_1)$ and $ext(M_2)$, the blue symbols are moved to the end of the permutations and a new symbol, 4, in red, occupies the positions vacated by the blue symbols. To create $ext(M_3)$, the symbol 4 is simply appended to the end of each permutation. Note that $hd(M_1) \geq 4$, $hd(M_2) \geq 4$ and $hd(M_1, M_2) \geq 3$, so Π is a distance-4 partition system. By Theorem 1, $hd(ext(\Pi)) \geq 4$.

3 Sequential partition and extension

Let $\mathfrak{M} = \{M_1, M_2, \ldots M_t\}$, for some t, be a collection of PAs on Z_n that satisfy Properties I and II for a distance-d partition system. The basic idea of sequential partition and extension is that we first create several disjoint PA's by simple partition and extension, each consisting of permutations on $n+1$ symbols with internal Hamming distance d. Then, we use partition and extension again on these PA's to get a larger PA on $n+2$ symbols and Hamming distance d. Such an iterative application of partition and extension can produce interesting new results.

Let $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_m)$ be an ordered set of subsets of $\mathfrak{M}$ such that each $\mathcal{M}_i$ contains some number of PAs, such as $M_k, \ldots, M_l$, from $\mathfrak{M}$, and for all $i, j,\ (1 \le i < j \le m)$, $\mathcal{M}_i$ and $\mathcal{M}_j$ are pairwise disjoint. Let $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$, be a collection of distance-d partition systems on Z_n, where for all $i,\ (1 \le i \le m),\ \Pi_i = (\mathcal{M}_i, \mathcal{P}_i, \mathcal{Q}_i)$, and $\mathcal{M}_i \subseteq \mathfrak{M}$. We say that $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$ is *pairwise disjoint* if for all $i, j,\ (1 \le i < j \le m)$, $\mathcal{M}_i$ and $\mathcal{M}_j$ are pairwise disjoint.

For each iteration i, we employ a different distance-d partition system, $\Pi_i = (\mathcal{M}_i, \mathcal{P}_i, \mathcal{Q}_i)$, that uses a previously unused set of PAs, $\mathcal{M}_i \subseteq \mathfrak{M}$, to create a new PA, ext(Π_i), on Z_{n+1}, with Hamming distance d. Hence, by repeated simple partition and extension, we create a collection of new PAs, $ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)$, for some $m > 1$. As long as the distance-d partition systems $\Pi_1, \Pi_2, \ldots, \Pi_m$ are pairwise disjoint, the sets $\{ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)\}$ are pairwise disjoint as well.

In the following, we assume that the distance-d partition systems under consideration are pairwise disjoint. The partitions $\mathcal{P}_i$ and $\mathcal{Q}_i$ need not be distinct from partitions $\mathcal{P}_j$ and $\mathcal{Q}_j$.

Consider the case of applying simple partition and extension twice in succession using two distance-d partition systems, $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1)$ and $\Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2)$. We present Theorem 2 and Corollary 3, which give results on the Hamming distance and the size of the resulting PA. Corollary 4 extends these results by induction. These results will be useful later for describing a new method for creating PAs which we call *sequential partition and extension*.

Theorem 2 *Let $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1)$ and $\Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2)$ be pairwise disjoint distance-d partition systems for Z_n, with $hd(\mathcal{M}_1, \mathcal{M}_2) \ge d-1$. Then $hd(ext(\Pi_1)) \ge d$, $hd(ext(\Pi_2)) \ge d$, and $hd(ext(\Pi_1), ext(\Pi_2)) \ge d-1$.*

Proof By Theorem 1, $hd(ext(\Pi_1)) \ge d$, $hd(ext(\Pi_2)) \ge d$. We show that $hd(ext(\Pi_1), ext(\Pi_2)) \ge d-1$. Pick two arbitrary permutations $\sigma' \in ext(\Pi_1)$ and $\tau' \in ext(\Pi_2)$, where for some k and j, $\sigma' = ext_k(\sigma)$ for some $\sigma \in \Pi_1$, and $\tau' = ext_j(\tau)$ for some $\tau \in \Pi_2$. We consider two cases to determine the number of new agreements between σ' and τ' created by the extension operation:

Case 1: $k = j$

The extension operation creates a new agreement in position $k = j$ because $\sigma'(k) = \tau'(k) = n$. Note that since $\sigma'(n) = \sigma(k)$ and $\tau'(n) = \tau(k)$, the relationship between $\sigma'(n)$ and $\tau'(n)$ is the same as the relationship between $\sigma(k)$ and $\tau(k)$. Hence, there is at most one new agreement between σ' and τ'.

Case 2: $k \ne j$

In this case, $\sigma'(k) = n$ and $\tau'(j) = n$, so the new symbol n is in different positions in σ' and τ'. That is, inserting the symbol n does not, in itself, increase the number of agreements. Now consider the symbols $\sigma(k)$ and $\tau(j)$. If $\sigma(k) = \tau(j)$, then $\sigma'(n) = \tau'(n)$. In this situation, extension creates a new agreement in position n. On the other hand, if $\sigma(k) \ne \tau(j)$, then $\sigma'(n) \ne \tau'(n)$, so no new agreement is created by extension. In either situation, extension creates at most one new agreement between σ' and τ'.

By assumption, $hd(\mathcal{M}_1, \mathcal{M}_2) \geq d-1$, hence $hd(\sigma, \tau) \geq d-1$ as well. That is the number of disagreements between σ and τ is at least $d-1$, or equivalently, the number of agreements between σ and τ is at most $n-(d-1)$. So, the number of agreements between σ' and τ' is at most $1+n-(d-1)$. Since $\sigma' = ext_k(\sigma)$ and $\tau' = ext_m(\tau)$, both σ' and τ' are permutations on $n+1$ (not n) symbols. Hence, $hd(\sigma', \tau') \geq (n+1) - (1+n-(d-1)) \geq d-1$, so $hd(ext(\Pi_1), ext(\Pi_2)) \geq d-1$. □

Corollary 3 *Let $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1)$ and $\Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2)$ be pairwise disjoint distance-d partition systems for Z_n, with $hd(\mathcal{M}_1, \mathcal{M}_2) \geq d-1$. Let $\mathcal{A} = ext(\Pi_1) \cup ext(\Pi_2)$. Then $\mathcal{A}$ is a PA on Z_{n+1} such that $|\mathcal{A}| = |ext(\Pi_1)| + |ext(\Pi_2)|$ and $hd(\mathcal{A}) \geq d-1$.*

Proof Since both $ext(\Pi_1)$ and $ext(\Pi_2)$ are created by simple partition and extension of PAs on Z_n, $\mathcal{A}$ is a PA on Z_{n+1}. Given that $\mathcal{M}_1$ is disjoint from $\mathcal{M}_2$, Equation 1 tells us that $|\mathcal{A}| = |ext(\Pi_1)| + |ext(\Pi_2)|$. Lastly, by Theorem 2, $hd(\mathcal{A}) \geq d-1$. □

Simple partition and extension can be used in a similar way on several more distance-d partition systems on Z_n to create large PAs on Z_{n+1}. This is formalized by Corollary 4.

Corollary 4 *Let $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1)$, $\Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2)$, ..., $\Pi_m = (\mathcal{M}_m, \mathcal{P}_m, \mathcal{Q}_m)$ be a collection of pairwise disjoint distance-d partition systems, for some $m > 1$, where $hd(\mathcal{M}_i, \mathcal{M}_j) \geq d-1$, for all i, j $(1 \leq i < j \leq m)$. Let $\mathcal{A} = ext(\Pi_1) \cup ext(\Pi_2) \cup \ldots \cup ext(\Pi_m)$. Then*

(1) $\forall i, j\ (1 \leq i < j \leq m),\ hd(ext(\Pi_i), ext(\Pi_j)) \geq d-1$,
(2) $\mathcal{A}$ is a PA on Z_{n+1},
(3) $|\mathcal{A}| = \sum_{i=1}^{m} |ext(\Pi_i)|$, and
(4) $hd(\mathcal{A}) \geq d-1$.

Proof The results follow from Theorem 2 and Corollary 3 by induction on m. □

A new technique, which we call *sequential partition and extension*, can be used to improve bounds for $M(n+2, d)$. It has two steps. First, simple partition and extension is used to create the extended PAs $ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)$, for some $m > 1$. Let $\mathbb{M} = \{\mathbb{M}_1, \mathbb{M}_2, \ldots, \mathbb{M}_m\}$, where for all i, $\mathbb{M}_i = ext(\Pi_i)$. Note that $\mathbb{M}$ is a collection of PAs on Z_{n+1}. Let $\mathbb{P}$ and $\mathbb{Q}$ be partitions of Z_{n+1} such that $\Psi = (\mathbb{M}, \mathbb{P}, \mathbb{Q})$ is a distance-d partition system on Z_{n+1}. Next, simple partition and extension is again used to create a new PA, $ext(\Psi)$, on Z_{n+2}.

We show that $ext(\Psi)$ is a PA on $n+2$ symbols with Hamming distance d.

Theorem 5 *Sequential partition and extension on a collection $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$, of pairwise disjoint distance-d partition systems on Z_n, results in a new PA on Z_{n+2} with Hamming distance d.*

Proof Let $ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)$ be the PAs on Z_{n+1} created the first phase of sequential partition and extension. By Theorem 1, $hd(ext(\Pi_i)) \geq d$. By Corollary 4, $\forall i, j\ (1 \leq i < j \leq m),\ hd(ext(\Pi_i), ext(\Pi_j)) \geq d-1$.

Let $\mathbb{M} = (ext(\Pi_1),\ ext(\Pi_2), \ldots, ext(\Pi_m))$, and let $\mathbb{P}$ and $\mathbb{Q}$ be suitable partitions of Z_{n+1}, such that $\Psi = (\mathbb{M}, \mathbb{P}, \mathbb{Q})$ forms a distance-d partition system on Z_{n+1}. Let $ext(\Psi)$ be the PA created by simple partition and extension on $\Psi = (\mathbb{M}, \mathbb{P}, \mathbb{Q})$. Since, Ψ is a distance-d partition system on Z_{n+1}, $ext(\Psi)$ is a PA on Z_{n+2}. By Theorem 1, $hd(ext(\Psi)) \geq d$. □

We now illustrate sequential partition and extension by means of an example.

Example 1 Consider the group $AGL(1, 37)$ on 37 symbols with Hamming distance 36, containing 1332 permutations. This gives $M(37, 36) \geq 1332$. Using sequential partition and extension we show that $M(39, 37) \geq 1301$.

$AGL(1, 37)$ can be decomposed into 36 Latin squares, where one of the Latin squares is a cyclic subgroup of $AGL(1, 37)$ consisting of the identity permutation and all cyclic shifts. This is the set of permutations $C_1 = \{x + b \mid b \in Z_{37}\}$. The other 35 Latin squares can be defined as the left cosets of C_1, namely, $C_i = \{ix + b \mid b \in Z_{37}\}$, for each i $(2 \leq i \leq 36)$.

First, we give six distance-37 partition systems for $AGL(1, 37)$, namely, $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1), \Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2), \Pi_3 = (\mathcal{M}_3, \mathcal{P}_3, \mathcal{Q}_3), \Pi_4 = (\mathcal{M}_4, \mathcal{P}_4, \mathcal{Q}_4), \Pi_5 = (\mathcal{M}_5, \mathcal{P}_5, \mathcal{Q}_5)$, $\Pi_6 = (\mathcal{M}_6, \mathcal{P}_6, \mathcal{Q}_6)$, where $\mathcal{M}_1 = \{C_1, C_2, \ldots, C_7\}$, $\mathcal{M}_2 = \{C_8, C_9, \ldots, C_{14}\}$, $\mathcal{M}_3 = \{C_{15}, C_{16}, \ldots, C_{21}\}$, $\mathcal{M}_4 = \{C_{22}, C_{23}, \ldots, C_{28}\}$, $\mathcal{M}_5 = \{C_{29}, C_{30}, \ldots, C_{35}\}$, $\mathcal{M}_6 = \{C_{36}\}$ with the partitions $\mathcal{P}_i$, $\mathcal{Q}_i$ $(1 \leq i \leq 6)$ described in Table 2. Note that in each Π_i, the last coset is covered by adding the new symbol '37' in the 37^{th} position.

Simple partition and extension yields six PAs on Z_{38}, where for all i, $(1 \leq i \leq 6)$, $hd(ext(\Pi_i)) \geq 37$, and for all i, j $(1 \leq i < j \leq 6)$, $hd(ext(\Pi_i), ext(\Pi_j)) \geq 36$. Moreover, $|ext(\Pi_1)| = 253$, $|ext(\Pi_2)| = 253$, $|ext(\Pi_3)| = 253$, $|ext(\Pi_4)| = 253$, $|ext(\Pi_5)| = 252$, and $|ext(\Pi_6)| = 37$.

Finally, we form a distance-37 partition system $\Psi = (\mathbb{M}, \mathbb{P}, \mathbb{Q})$, where $\mathbb{M} = (ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_6))$ with suitable partitions $\mathbb{P}$ and $\mathbb{Q}$ as shown in Table 3. The result is a PA, $ext(\Psi)$, on 39 symbols with Hamming distance 37, which has 1301 permutations. The previous lower bound for $M(39, 37)$, given by the five known MOLS on 39 symbols, was 195.

Sequential partition and extension also results in the lower bounds $M(34, 32) \geq 945$ and $M(66, 64) \geq 4029$. Table 4 shows additional improved lower bounds on $M(n, n-2)$ obtained by sequential partition and extension.

In fact, sequential partition and extension can be applied an arbitrary number of times, provided that suitable distance-d partitions systems can be found at each stage. That is, sequential partition and extension on a sequence of r distance-d partitions systems could result in new lower bounds for $M(n + r, d)$, for arbitrary r.

4 Parallel partition and extension

In Sect. 3, we described a new technique, based on simple partition and extension, called sequential partition and extension. We now present another new technique, called *parallel partition and extension* which introduces multiple new symbols simultaneously. As previously described, simple partition and extension extends a permutation array by replacing *one* existing symbol in a carefully selected position in each permutation with the symbol n, and appending the displaced symbol to the end of the permutation. Sequential partition and extension allows additional symbols to be introduced one at a time by applying simple partition and extension sequentially. In contrast, *parallel partition and extension* on a PA A on Z_n creates a PA A' on Z_{n+r} by introducing, to each permutation in A, r new symbols *simultaneously*. Table 6 shows new bounds obtained using Theorems 6 and 7 for parallel partition and extension. These theorems are proved in Sects. 4.1 and 4.2.

Table 2 Step 1 of sequential partition and extension on $AGL(1, 37)$, which gives $M(38, 36) \geq 1301$

Π_i	Set of cosets, $\mathcal{M}_i$	$\mathcal{P}_i$	$\mathcal{Q}_i$	$\lvert ext(\Pi_i)\rvert$
Π_1	$\{x + b \mid b \in Z_{37}\}$	{4, 11, 18, 25, 31, 34}	{0, 1, 2, 3, 4, 5, 6}	253
	$\{2x + b \mid b \in Z_{37}\}$	{5, 8, 10, 13, 16, 19, 21}	{7, 8, 9, 10, 11, 12}	
	$\{3x + b \mid b \in Z_{37}\}$	{14, 20, 22, 24, 28, 30}	{13, 14, 15, 16, 17, 18}	
	$\{4x + b \mid b \in Z_{37}\}$	{9, 12, 15, 26, 29, 32}	{19, 20, 21, 22, 23, 24}	
	$\{5x + b \mid b \in Z_{37}\}$	{6, 7, 17, 23, 27, 33}	{25, 26, 27, 28, 29, 30}	
	$\{6x + b \mid b \in Z_{37}\}$	{0, 1, 2, 3, 35, 36}	{31, 32, 33, 34, 35, 36}	
	$\{7x + b \mid b \in Z_{37}\}$	{37}	{37}	
Π_2	$\{8x + b \mid b \in Z_{37}\}$	{1, 12, 23, 25, 36}	{0, 1, 2, 3, 4, 5, 6}	253
	$\{9x + b \mid b \in Z_{37}\}$	{0, 11, 13, 22, 24, 35}	{7, 8, 9, 10, 11, 12}	
	$\{10x + b \mid b \in Z_{37}\}$	{8, 9, 10, 17, 18, 26, 27}	{13, 14, 15, 16, 17, 18}	
	$\{11x + b \mid b \in Z_{37}\}$	{4, 5, 6, 7, 19, 20, 28}	{19, 20, 21, 22, 23, 24}	
	$\{12x + b \mid b \in Z_{37}\}$	{14, 15, 16, 32, 33, 34}	{25, 26, 27, 28, 29, 30}	
	$\{13x + b \mid b \in Z_{37}\}$	{2, 3, 21, 29, 30, 31}	{31, 32, 33, 34, 35, 36}	
	$\{14x + b \mid b \in Z_{37}\}$	{37}	{37}	
Π_3	$\{15x + b \mid b \in Z_{37}\}$	{2, 3, 4, 6, 15, 27}	{0, 1, 2, 3, 4, 5, 6}	253
	$\{16x + b \mid b \in Z_{37}\}$	{12, 13, 14, 16, 17, 18, 22}	{7, 8, 9, 10, 11, 12}	
	$\{17x + b \mid b \in Z_{37}\}$	{0, 21, 25, 28, 29, 33}	{13, 14, 15, 16, 17, 18}	
	$\{18x + b \mid b \in Z_{37}\}$	{7, 8, 19, 20, 31, 32}	{19, 20, 21, 22, 23, 24}	
	$\{19x + b \mid b \in Z_{37}\}$	{10, 11, 23, 24, 35, 36}	{25, 26, 27, 28, 29, 30}	
	$\{20x + b \mid b \in Z_{37}\}$	{1, 5, 9, 26, 30, 34}	{31, 32, 33, 34, 35, 36}	
	$\{21x + b \mid b \in Z_{37}\}$	{37}	{37}	
Π_4	$\{22x + b \mid b \in Z_{37}\}$	{2, 3, 5, 9, 21, 33}	{0, 1, 2, 3, 4, 5, 6}	253
	$\{23x + b \mid b \in Z_{37}\}$	{4, 8, 11, 22, 23, 34}	{7, 8, 9, 10, 11, 12}	
	$\{24x + b \mid b \in Z_{37}\}$	{7, 16, 17, 25, 26, 35}	{13, 14, 15, 16, 17, 18}	
	$\{25x + b \mid b \in Z_{37}\}$	{12, 13, 14, 30, 31, 32}	{19, 20, 21, 22, 23, 24}	
	$\{26x + b \mid b \in Z_{37}\}$	{1, 6, 10, 15, 24, 29}	{25, 26, 27, 28, 29, 30}	
	$\{27x + b \mid b \in Z_{37}\}$	{0, 18, 19, 20, 27, 28, 36}	{31, 32, 33, 34, 35, 36}	
	$\{28x + b \mid b \in Z_{37}\}$	{37}	{37}	
Π_5	$\{29x + b \mid b \in Z_{37}\}$	{2, 5, 13, 18, 26, 29}	{0, 1, 2, 3, 4, 5, 6}	252
	$\{30x + b \mid b \in Z_{37}\}$	{12, 19, 21, 27, 34, 36}	{7, 8, 9, 10, 11, 12}	
	$\{31x + b \mid b \in Z_{37}\}$	{6, 7, 8, 9, 10, 11}	{13, 14, 15, 16, 17, 18}	
	$\{32x + b \mid b \in Z_{37}\}$	{4, 14, 15, 25, 31, 35}	{19, 20, 21, 22, 23, 24}	
	$\{33x + b \mid b \in Z_{37}\}$	{0, 3, 16, 17, 20, 23, 33}	{25, 26, 27, 28, 29, 30}	
	$\{34x + b \mid b \in Z_{37}\}$	{1, 22, 24, 28, 30, 32}	{31, 32, 33, 34, 35, 36}	
	$\{35x + b \mid b \in Z_{37}\}$	{37}	{37}	
Π_6	$\{36x + b \mid b \in Z_{37}\}$	{37}	{37}	37

4.1 Rudimentary parallel partition and extension

In its rudimentary form, parallel partition and extension operates on $2r$ *blocks* (*i.e.,* sets) of permutations, for some integer r. Specifically, suppose a PA A, on Z_n, is partitioned into $k = 2r$ blocks of permutations $B_0, B_1, \ldots, B_{k-1}$, where, for all i, $(0 \leq i < k)$,

Table 3 Step 2 of sequential partition and extension on $AGL(1, 37)$ for $M(39, 37) \geq 1301$

$\mathbb{M}$	$\mathbb{P}_i \in \mathbb{P}$	$\mathbb{Q}_i \in \mathbb{Q}$	$\lvert ext(\mathbb{M}_i)\rvert$
$\mathbb{M}_1$=ext(Π_1)	{4, 11, 18, 25, 31, 34}	{0, 1, 2, 3, 4, 5, 6}	253
$\mathbb{M}_2$=ext(Π_2)	{5, 8, 10, 13, 16, 19, 21}	{7, 8, 9, 10, 11, 12}	253
$\mathbb{M}_3$=ext(Π_3)	{14, 20, 22, 24, 28, 30}	{13, 14, 15, 16, 17, 18}	253
$\mathbb{M}_4$=ext(Π_4)	{9, 12, 15, 26, 29, 32}	{19, 20, 21, 22, 23, 24}	253
$\mathbb{M}_5$=ext(Π_5)	{38}	{38}	252
$\mathbb{M}_6$=ext(Π_6)	{0, 1, 2, 3, 6, 7, 17, 23, 27, 33, 35, 36, 37}	{25, 26, 27, 28, 29, 30, 31 32, 33, 34, 35, 36, 37}	37
Total			1301

Table 4 $M(n, n-2)$ lower bounds

n	PREV	NEW	n	PREV	NEW	n	PREV	NEW
34	192	945	159	2051	16,666	291	5202	80,385
39	255	1301	165	2185	17,632	295	5088	54,572
45	270	1726	171	2354	27,330	309	5539	60,715
51	392	2308	175	2354	19,792	315	5634	60,952
55	423	2461	183	2533	21,994	319	5793	67,379
63	1,514	3306	195	2758	25,022	333	6091	70,696
66	576	4029	201	2867	25,427	339	6280	69,485
69	594	3965	213	3170	30,288	345	5205	89,272
75	667	4747	225	3421	32,728	351	6642	76,195
85	812	6116	231	3548	33,779	355	6746	77,215
91	902	6709	235	3625	35,001	363	7220	125,709
99	1,017	8206	245	3475	43,717	369	7108	83,418
105	1,119	9239	253	4075	40,094	375	7298	87,434
111	1,187	9990	259	4222	43,268	385	7428	90,213
115	1,277	11,142	265	4342	44,733	391	7690	90,991
123	1,452	13,996	273	4548	46,268	411	8240	104,098
133	1,554	11,604	279	4701	49,243	514	11,264	197,859
141	1,723	13,522	285	4868	51,571	531	12,696	271,043
153	1,923	16,118						

PREV denotes the previous bound and *NEW* denotes the new bound obtained using sequential partition and extension

$hd(B_i) \geq d$, for some d, and for all i, j $(0 \leq i \neq j < k)$, $hd(B_i, B_j) \geq d - r$. In particular, $hd(A) \geq d - r$. We create a new PA A' on Z_{n+r}, such that $hd(A') \geq d$, by inserting a sequence of new symbols from the set $\{n, n+1, \ldots, n+r-1\}$ into the permutations in each block. Each block uses a different sequence.

Define SHIFT(γ, 0) to be the sequence $(n, n+1, n+2, \ldots, n+r-1)$, and for each integer t, denote by SHIFT(γ, t) the left cyclic shift of the sequence by t (mod r) positions. For example, SHIFT(γ, 1) is the sequence $(n+1, n+2, \ldots, n+r-1, n)$, and SHIFT($\gamma$, 2) is the sequence $(n+2, \ldots, n+r-1, n, n+1)$, and so on.

The creation of the new PA A' takes place in two steps. The first step modifies the blocks $B_0, B_1, \ldots, B_{r-1}$. For all l, $(0 \le l < r)$, a new block B'_l of permutations on Z_{n+r} is created from the block B_l as follows: the first r symbols in each permutation of B_l, are replaced by SHIFT(γ, l), and the r replaced symbols are put in their original order at the end of the permutation in positions $n, n+1, \ldots, n+r-1$.

In the second step, a new block of permutations B'_m is created from each block B_m, for all m, $(r \le m < 2r)$, by appending the sequence, SHIFT(γ, m) to each permutation in positions $n, n+1, \ldots, n+r-1$. The blocks B'_l, $(0 \le l < r)$ together with the blocks B'_m, $(r \le m < 2r)$ comprise the new PA A' on Z_{n+r}.

It is known that the Hamming distance between two permutations does not change when the order of the symbols in both permutations is altered in a fixed manner. Consequently, the Hamming distance between permutations in the same block, or between permutations in different blocks is not altered by the movement of the first r symbols in each permutation to positions $n, n+1, \ldots, n+r-1$. Since the ordering of the new symbols $n, n+1, \ldots, n+r-1$ in any block is a cyclic shift of sequence of new symbols in any other block, rudimentary parallel partition and extension does not create any new agreements between permutations in different blocks. For the original permutation array A, $hd(A) \ge d - r$. For the new permutation array A', the permutations in each block have been extended by r symbols in a way that ensures that the inter-block Hamming distance is at least d. That is, for all i, j $(0 \le i \ne j < k)$, $hd(B'_i, B'_j) \ge d$, and the length of the permutations has increased by r. Within each new block, the r new symbols are put in a fixed order into fixed positions, creating r new agreements in addition to the $(n-d)$ agreements that existed in the unaltered blocks. For the new blocks B'_l for all l $(0 \le l < r)$, the displaced symbols are moved to the end of each permutation. For the new blocks B'_m, for all m $(r \le m < 2r)$, no symbols are displaced because the r new symbols are appended at the end of the permutations. Thus the intra-block Hamming distance for the new permutations is $(n + r - (r + (n - d))) = d$. That is, for all i, $(0 \le i < k)$, $hd(B'_i) \ge d$. Hence, $hd(A') \ge d$. The size of the PA A' is given by Theorem 6. The proof is described in [21].

Theorem 6 ([21]) *Let A be a PA on Z_n comprising $2r$ blocks for some r. Denote the blocks by $B_0, B_1, \ldots, B_{2r-1}$, so that $A = \cup_{i=0}^{2r-1} B_i$. If each block B_i has Hamming distance at least d and the Hamming distance of the entire set A is at least $d - r$, then rudimentary parallel partition and extension on A results in a new PA A' on Z_{n+r} that exhibits $M(n+r, d) \ge \sum_{i=0}^{2r-1} |B_i|$.*

Table 5 illustrates rudimentary parallel partition and extension for $n = 9, d = 9$ and $r = 3$ using a PA A on Z_9. We provide $k = 2r = 6$ blocks such that for each block B_i, $(0 \le i \le 5)$, $hd(B_i) \ge d = 9$ and for all i, j $(0 \le i \ne j \le 5)$, $hd(B_i, B_j) \ge d - r = 6$. These blocks comprise the PA A and are shown in the column on the left of Table 5. The symbols to be relocated by rudimentary parallel partition and extension are shown in blue. Note that $hd(A) \ge 6$. Rudimentary parallel partition and extension on A results in the PA A' on Z_{12} with $hd(A') \ge 6$. The permutations comprising A' are shown in the column on the right of Table 5, with the displaced symbols shown in blue and the new symbols shown in red.

More results based on Theorem 6 are shown in Table 6. For example, for $n = 42, d = 39, r = 4$, take $PGL(2, 41)$, which contains $40 \cdot 41 \cdot 42 = 68880$ permutations on 42 symbols, with hamming distance at least 39. We found $2r = 8$ cosets of $PGL(2, 41)$ with $d = 35$. Then by Theorem 6, $M(46, 39) \ge 8 \cdot 68{,}880 = 551{,}040$ using 8 cosets.

Table 5 An example of rudimentary parallel partition and extension, with $n = 9, d = 9, r = 3$

Initial permutations in the PA A	Modified permutations in the PA A'
0 1 2 3 4 5 6 7 8	**9 10 11** 3 4 5 6 7 8 **0 1 2**
1 5 8 4 6 0 3 2 7	**9 10 11** 4 6 0 3 2 7 **1 5 8**
2 8 6 1 5 7 0 4 3	**9 10 11** 1 5 7 0 4 3 **2 8 6**
3 4 1 7 2 6 8 0 5	**9 10 11** 7 2 6 8 0 5 **3 4 1**
4 6 5 2 8 3 7 1 0	**9 10 11** 2 8 3 7 1 0 **4 6 5**
5 0 7 6 3 1 4 8 2	**9 10 11** 6 3 1 4 8 2 **5 0 7**
6 3 0 8 7 4 2 5 1	**9 10 11** 8 7 4 2 5 1 **6 3 0**
7 2 4 0 1 8 5 3 6	**9 10 11** 0 1 8 5 3 6 **7 2 4**
8 7 3 5 0 2 1 6 4	**9 10 11** 5 0 2 1 6 4 **8 7 3**
1 3 6 7 5 8 2 4 0	**10 11 9** 7 5 8 2 4 0 **1 3 6**
5 4 3 2 0 7 8 6 1	**10 11 9** 2 0 7 8 6 1 **5 4 3**
8 1 0 4 7 3 6 5 2	**10 11 9** 4 7 3 6 5 2 **8 1 0**
4 7 8 0 6 5 1 2 3	**10 11 9** 0 6 5 1 2 3 **4 7 8**
6 2 7 1 3 0 5 8 4	**10 11 9** 1 3 0 5 8 4 **6 2 7**
0 6 4 8 1 2 7 3 5	**10 11 9** 8 1 2 7 3 5 **0 6 4**
3 8 2 5 4 1 0 7 6	**10 11 9** 5 4 1 0 7 6 **3 8 2**
2 0 5 3 8 6 4 1 7	**10 11 9** 3 8 6 4 1 7 **2 0 5**
7 5 1 6 2 4 3 0 8	**10 11 9** 6 2 4 3 0 8 **7 5 1**
3 5 7 2 6 0 8 4 1	**11 9 10** 2 6 0 8 4 1 **3 5 7**
4 0 2 8 3 1 7 6 5	**11 9 10** 8 3 1 7 6 5 **4 0 2**
1 7 4 6 0 2 3 5 8	**11 9 10** 6 0 2 3 5 8 **1 7 4**
7 6 0 1 8 3 5 2 4	**11 9 10** 1 8 3 5 2 4 **7 6 0**
2 3 1 5 7 4 0 8 6	**11 9 10** 5 7 4 0 8 6 **2 3 1**
6 1 8 7 4 5 2 3 0	**11 9 10** 7 4 5 2 3 0 **6 1 8**
8 4 5 0 2 6 1 7 3	**11 9 10** 0 2 6 1 7 3 **8 4 5**
0 8 3 4 5 7 6 1 2	**11 9 10** 4 5 7 6 1 2 **0 8 3**
5 2 6 3 1 8 4 0 7	**11 9 10** 3 1 8 4 0 7 **5 2 6**
4 2 7 8 0 1 3 5 6	4 2 7 8 0 1 3 5 6 **9 10 11**
6 8 2 7 1 5 4 0 3	6 8 2 7 1 5 4 0 3 **9 10 11**
5 6 4 3 2 8 1 7 0	5 6 4 3 2 8 1 7 0 **9 10 11**
2 1 0 5 3 4 7 6 8	2 1 0 5 3 4 7 6 8 **9 10 11**
8 5 1 0 4 6 2 3 7	8 5 1 0 4 6 2 3 7 **9 10 11**
3 7 8 2 5 0 6 1 4	3 7 8 2 5 0 6 1 4 **9 10 11**
7 0 5 1 6 3 8 4 2	7 0 5 1 6 3 8 4 2 **9 10 11**
1 4 3 6 7 2 0 8 5	1 4 3 6 7 2 0 8 5 **9 10 11**
0 3 6 4 8 7 5 2 1	0 3 6 4 8 7 5 2 1 **9 10 11**
3 5 7 8 4 6 0 1 2	3 5 7 8 4 6 0 1 2 **10 11 9**
4 0 2 7 6 3 1 5 8	4 0 2 7 6 3 1 5 8 **10 11 9**
1 7 4 3 5 0 2 8 6	1 7 4 3 5 0 2 8 6 **10 11 9**
7 6 0 5 2 8 3 4 1	7 6 0 5 2 8 3 4 1 **10 11 9**
2 3 1 0 8 7 4 6 5	2 3 1 0 8 7 4 6 5 **10 11 9**
6 1 8 2 3 4 5 0 7	6 1 8 2 3 4 5 0 7 **10 11 9**
8 4 5 1 7 2 6 3 0	8 4 5 1 7 2 6 3 0 **10 11 9**
0 8 3 6 1 5 7 2 4	0 8 3 6 1 5 7 2 4 **10 11 9**
5 2 6 4 0 1 8 7 3	5 2 6 4 0 1 8 7 3 **10 11 9**

Table 5 continued

Initial permutations in the PA A	Modified permutations in the PA A'
$\begin{bmatrix} 0&4&2&5&6&1&7&3&8\\ 1&6&8&0&3&5&2&4&7\\ 2&5&6&7&0&8&4&1&3\\ 3&2&1&6&8&4&0&7&5\\ 4&8&5&3&7&6&1&2&0\\ 5&3&7&1&4&0&8&6&2\\ 6&7&0&4&2&3&5&8&1\\ 7&1&4&8&5&2&3&0&6\\ 8&0&3&2&1&7&6&5&4 \end{bmatrix}$	$\begin{bmatrix} 0&4&2&5&6&1&7&3&8&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 1&6&8&0&3&5&2&4&7&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 2&5&6&7&0&8&4&1&3&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 3&2&1&6&8&4&0&7&5&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 4&8&5&3&7&6&1&2&0&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 5&3&7&1&4&0&8&6&2&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 6&7&0&4&2&3&5&8&1&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 7&1&4&8&5&2&3&0&6&\mathbf{11}&\mathbf{9}&\mathbf{10}\\ 8&0&3&2&1&7&6&5&4&\mathbf{11}&\mathbf{9}&\mathbf{10} \end{bmatrix}$

The column on the left shows a PA A consisting of six blocks of permutations on Z_9 with $hd(A) \geq 6$. The column on the right shows the new PA A' on Z_{12} with $hd(A') \geq 6$

Table 6 $M(n, d)$ lower bounds obtained using *parallel partition and extension* (Theorem 6 and 7)

n	d	r	NEW	Origin of blocks (see Table 8)
30	26	2	$58{,}968_R$	$P\Gamma L$(2,27) and 2 cosets
40	34	2	$287{,}437_P$	PGL(2,37) and 2 cosets (see M(38,32))
44	38	2	$397{,}198_P$	PGL(2,41) and 2 cosets (see M(42,36))
45	39	3	$413{,}280_R$	PGL(2,41) and 3 cosets (see M(42,36))
46	39	4	$551{,}040_R$	PGL(2,41) and 4 cosets (see M(42,35))
52	46	2	$470{,}397_R$	PGL(2,49) and 2 cosets (see M(50,44))
53	47	3	$470{,}400_R$	PGL(2,49) and 3 cosets (see M(50,44))
56	50	2	$446{,}472_R$	PGL(2,53) and 2 cosets (see M(54,48))
70	63	2	$1{,}503{,}462_P$	PGL(2,67) and 2 cosets (see M(68,61))

The blocks used by these theorems were obtained by the coset method [5] (see Table 8). Columns: r denotes the number of new symbols, *NEW* denotes the new new bound. New bounds computed using rudimentary parallel partition and extension (Theorem 6) and general parallel partition and extension (Theorem 7) are denoted with a subscript R and P, respectively

4.2 General parallel partition with *r* symbols

As described in Sect. 4.1, rudimentary parallel partition and extension with $r = 2$ allows extension of at most $2r = 4$ blocks. We describe a new technique, called *general parallel partition and extension with r symbols*, that allows a larger number of blocks to be extended.

We start with the simplest form of general parallel partition and extension, for $r = 2$ symbols. It expands on the simple partition and extension technique described in Sect. 2 by introducing an additional pair of partitions of Z_n, denoted by $\mathcal{R}$ and $\mathcal{S}$ in the description that follows.

Let s be a positive integer, and let $M_1, M_2, \ldots, M_s$ be an ordered list of s pairwise disjoint PAs on Z_n. Let $\mathcal{P} = (P_1, P_2, \ldots, P_s)$, $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_s)$, $\mathcal{R} = (R_1, R_2, \ldots, R_s)$, and $\mathcal{S} = (S_1, S_2, \ldots, S_s)$, be four partitions of Z_n such that, for all i, $P_i \cap R_i = \emptyset$ and $Q_i \cap S_i = \emptyset$. The sets P_i and R_i are sets of locations for replacing symbols in the PA M_i, and the sets Q_i and S_i are sets of symbols to be replaced. For each i, let 2-$covered(M_i)$ be defined by

$$2 - covered(M_i) = \{\sigma \in M_i \mid \exists p \in P_i,\ \exists r \neq p \in R_i\ (\sigma(p) \in Q_i,\ \sigma(r) \in S_i)\}.$$

We say that a permutation σ is 2-*covered* if $\sigma \in 2\text{-}covered(M_i)$ for some i. In general, when σ is 2-*covered*, there may be multiple pairs $(p, r) \in P_i \times R_i$ such that $\sigma(p) \in Q_i$ and $\sigma(r) \in S_i$. If so, arbitrarily designate one of these pairs to cover σ. We use the notation (p, r) to refer to the designated pair.

The *parallel extension of* σ *by the pair* (p, r), denoted by $2\text{-}ext(\sigma) = \sigma'$, is a permutation on Z_{n+2} defined by

$$2\text{-}ext(\sigma(x)) = \sigma'(x) = \begin{cases} n & \text{if } x = p \\ \sigma(p) & \text{if } x = n \\ n+1 & \text{if } x = r \\ \sigma(r) & \text{if } x = n+1 \\ \sigma(j) & \forall j,\ (0 \le j < n \ \wedge \ j \notin \{p, r\}). \end{cases} \tag{2}$$

We will always extend σ at the designated pair of positions (p, r) and refer to this new permutation as $2\text{-}ext(\sigma)$ or σ' interchangeably. Note that in order for a permutation σ' to be included in the extended set of permutations on $n + 2$ symbols, σ must be 2-covered. In other words, σ must have two of the named symbols in two of the named positions.

For our construction, we include two additional PAs, M_{s+1}, M_{s+2}, for which there are no corresponding sets of positions or symbols. None of the permutations in M_{s+1} or M_{s+2} are in any of the sets M_i $(1 \le i \le s)$. In a manner similar to rudimentary parallel partition and extension, parallel partition and extension extends M_{s+1} and M_{s+2} by appending the two new symbols n and $n+1$, to the end of each permutation. For M_{s+1}, the sequence $(n, n+1)$ is appended to the end of each permutation. Similarly, for M_{s+2}, the sequence $(n+1, n)$ is appended to the end of each permutation. Every permutation in M_{s+1} and M_{s+2} is used in the construction of our new PA. We create the list $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1}, M_{s+2})$, which includes the extra sets M_{s+1} and M_{s+2}.

A partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{S})$ is a $(d, 2)$-*partition system* for Z_n if it satisfies the following properties:

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

Parallel partition and extension uses sets P_i, Q_i, R_i, and S_i from the partitions $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$, and $\mathcal{S}$, respectively, to modify the 2-covered permutations in M_i, for $1 \le i \le s$, for the purpose of creating a new PA on Z_{n+2} with Hamming distance d. Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q}, \mathcal{R}, S)$ be a $(d, 2)$-partition system, where $\mathcal{M} = (M_1, M_2, \ldots, M_{s+2})$, for some s. We now show how parallel partition and extension operation creates a new permutation array $2\text{-}ext(\Pi)$ on Z_{n+2}. For all i $(1 \le i \le s)$, let $2\text{-}ext(M_i)$ be the set of permutations defined by

$$2\text{-}ext(M_i) = \{2\text{-}ext(\sigma) \mid \sigma \in 2\text{-}covered(M_i)\}.$$

For M_{s+1}, let $2\text{-}ext(M_{s+1})$ be the set of permutations on Z_{n+2} defined by adding the symbols n and $n+1$, in that order, to the end of every permutation of M_{s+1}. For M_{s+2}, let $2\text{-}ext(M_{s+2})$ be the set of permutations on Z_{n+2} defined by adding the symbols $n+1$ and n, in that order, to the end of every permutation of M_{s+2}.

Let $2\text{-}ext(\Pi)$ be defined by

$$2\text{-}ext(\Pi) = \bigcup_{i=1}^{s+2} 2\text{-}ext(M_i).$$

Note that

$$|2\text{-}ext(\Pi)| = \sum_{i=1}^{s+2} |2\text{-}ext(M_i)|.$$

Theorem 7 *Let d be a positive integer, let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{S})$ be a $(d, 2)$-partition system for Z_n, with $\mathcal{M} = (M_1, M_2, \ldots, M_{s+2})$ for some positive integer s. Let 2-$ext(\Pi)$ be the PA on Z_{n+2} created by parallel partition and extension. Then, $hd(2\text{-}ext(\Pi)) \geq d$.*

Proof Our proof has three steps. We first use simple partition and extension to create a PA $ext(\Pi')$, on Z_{n+1}, that exhibits $hd(ext(\Pi')) \geq d - 1$. Next, using simple partition and extension again, we create a PA $ext(\Pi'')$, on Z_{n+2}, that exhibits $hd(ext(\Pi'')) \geq d$. Finally, we show that the PA $2\text{-}ext(\Pi) = ext(\Pi'') \cup 2\text{-}ext(M_{s+1}) \cup 2\text{-}ext(M_{s+2})$ exhibits $hd(2\text{-}ext(\Pi)) \geq d$.

Consider $\mathcal{M}' = (M_1, M_2, \ldots, M_s)$. First, observe that $\Pi' = (\mathcal{M}', \mathcal{P}, \mathcal{R})$ can be viewed as a distance-$(d-1)$ partition system for Z_n since $hd(M_i) \geq d \geq d-1$ for all i, $(1 \leq i \leq s)$ and $hd(M_i, M_j) \geq d - 2$ for all i, j, $(1 \leq i < j \leq s)$. Simple partition and extension on Π' results in the PA $ext(\Pi')$ on Z_{n+1}. By Theorem 1, $hd(ext(\Pi')) \geq d - 1$. In particular, for all i, j $(1 \leq i, j \leq s,\ i \neq j)$, $hd(ext(M_i), ext(M_j)) \geq d - 1$.

Notice that, for all i $(1 \leq i \leq s)$, $hd(ext(M_i)) \geq d$ since $hd(M_i) \geq d$. (As shown in [4], this follows from case 1 in the proof of Theorem 1. For two permutations σ and τ from the same set M_i, at most one new agreement appears between $ext(\sigma)$ and $ext(\tau)$. Since $ext(\sigma)$ and $ext(\tau)$ are in Z_{n+1}, $hd(ext(\sigma), ext(\tau)) = hd(\sigma, \tau) \geq d$. See [4] for the full proof of Theorem 1.)

Let $\mathcal{M}'' = (ext(M_1), ext(M_2), \ldots, ext(M_s))$. Then $\Pi'' = (\mathcal{M}'', \mathcal{R}, \mathcal{S})$ is a distance-d partition system for Z_{n+1}. Simple partition and extension on Π'' results in the PA $ext(\Pi'')$ on Z_{n+2}. By Theorem 1, $hd(ext(\Pi'')) \geq d$.

By assumption, Π is a $(d, 2)$-partition system, so, by property I of $(d, 2)$ partition systems, $hd(M_{s+1}) \geq d$ and $hd(M_{s+2}) \geq d$. By definition, every permutation τ' in $2\text{-}ext(M_{s+1})$ is built from a permutation τ in M_{s+1} by appending the sequence $(n, n+1)$ to the end. This increases the length of each permutation by 2, and number of agreements between every pair of permutations in $2\text{-}ext(M_{s+1})$ by 2. So $hd(2\text{-}ext(M_{s+1})) = n + 2 - ((n - d) + 2) \geq d$. Similar reasoning applies to every permutation in $2\text{-}ext(M_{s+2})$ using the appended sequence $(n+1, n)$, so $hd(2\text{-}ext(M_{s+2})) \geq d$. Let $\tau' \in 2\text{-}ext(M_{s+1})$ and $\rho' \in 2\text{-}ext(M_{s+2})$ be arbitrary permutations. The appended sequences $(n, n+1)$ and $(n+1, n)$ create no new agreements between τ' and ρ'. By property II of $(d, 2)$ partition systems, $\forall i, j$ $(1 \leq i < j \leq s+2)$, $hd(M_i, M_j) \geq d - 2$. In particular, $hd(M_{s+1}, M_{s+2}) \geq d - 2$. So it follows that $hd(2\text{-}ext(M_{s+1}), 2\text{-}ext(M_{s+2})) \geq n + 2 - (n - (d-2)) = d$.

To see that $hd(ext(\Pi''), 2\text{-}ext(M_{s+1})) \geq d$, let $\sigma'' \in ext(\Pi'')$. Extending the original permutation σ to create σ'' merely replaces designated symbols in designated positions with the symbols n and $n+1$, and moves the displaced symbols to positions n and $n+1$, respectively. On the other hand, for any permutation $\tau' \in 2\text{-}ext(M_{s+1})$, the symbols n and $n+1$ are in positions n and $n+1$. In both cases, no other symbols are moved. So the symbols n and $n+1$ in σ'' are not in the same locations as they are in τ' and neither are the displaced symbols. That is, no new agreements are created. Hence, $hd(ext(\Pi''), 2\text{-}ext(M_{s+1})) \geq n+2-(n-(d-2)) = d$. Similarly, $hd(ext(\Pi''), 2\text{-}ext(M_{s+2})) \geq n + 2 - (n - (d-2)) = d$.

Finally, observe that $2\text{-}ext(\Pi) = ext(\Pi'') \cup 2\text{-}ext(M_{s+1}) \cup 2\text{-}ext(M_{s+2})$. We showed above that the pairwise Hamming distance between all PAs in $2\text{-}ext(\Pi)$ is at least d, so it follows that $hd(2\text{-}ext(\Pi)) \geq d$. □

Example 2 This example illustrates the use of Theorem 7 to construct a PA for $n = 40$ and $d = 34$. We start with $PGL(2, 37)$ is a PA on Z_{38}. It contains $38 \cdot 37 \cdot 36 = 50,616$ permutations with Hamming distance at least 36, giving $M(38, 36) \geq 50,616$. Using the coset method [5], we found five cosets of $PGL(2, 37)$ in S_{38}, with Hamming distance 34 from $PGL(2, 37)$ (see Table 8). The cosets are defined by the coset representatives $\alpha, \beta, \gamma, \delta$ and θ:

$\alpha =$ 27 12 30 25 15 37 35 22 29 36 10 1 13 33 24 3 28 16 26 8 19 17 23 0
11 34 20 5 31 6 21 14 18 32 7 9 2 4
$\beta =$ 16 22 35 6 4 30 37 26 23 11 0 20 18 24 8 7 15 13 1 29 36 27 17 33 3
9 10 14 32 25 12 19 28 21 2 31 5 34
$\gamma =$ 12 26 21 32 37 24 2 9 23 27 0 30 18 16 20 11 6 34 33 29 15 22 5 10 17 4
35 13 28 1 14 25 7 36 19 3 31 8
$\delta =$ 17 28 22 37 26 9 8 12 18 4 32 33 31 5 2 1 34 29 0 3 21 6 10 16 23 36
20 15 14 35 11 30 19 24 25 7 13 27
$\theta =$ 9 30 12 6 36 13 31 11 1 17 27 26 5 24 14 35 25 10 23 7 34 18 20 2 16 0
8 19 29 15 37 33 4 21 22 32 28 3

Let $\mathcal{M} = \{M_1, M_2, M_3, M_4, M_5, M_6\}$ where

$$M_1 = PGL(2, 37) \quad M_2 = \alpha M_1 \quad M_3 = \beta M_1 \quad M_4 = \gamma M_1 \quad M_5 = \delta M_1 \quad M_6 = \theta M_1.$$

Note that for all i, j, $(1 \leq i < j \leq 6)$, $hd(M_i) = 36$ and $hd(M_i, M_j) \geq 34$.
Let $X = \{X_1, X_2, X_3, X_4\}$ be the partition of Z_{38} given by

$$X_1 = \{0, 4, 8, 13, 19, 22, 26, 30, 35\} \qquad X_3 = \{2, 6, 10, 12, 16, 21, 24, 28, 33, 37\}$$
$$X_2 = \{1, 5, 9, 15, 18, 23, 27, 31, 34\} \qquad X_4 = \{3, 7, 11, 14, 17, 20, 25, 29, 32, 36\}.$$

The two partitions of positions, $\mathcal{P}$ and $\mathcal{R}$, are based on X. That is, $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$, where $P_1 = X_1, P_2 = X_2, P_3 = X_3$, and $P_4 = X_4$ and $\mathcal{R} = \{R_1, R_2, R_3, R_4\}$, where $R_1 = X_2, R_2 = X_3, R_3 = X_4$, and $R_4 = X_1$.
Let $Y = \{Y_1, Y_2, Y_3, Y_4\}$ be the partition of Z_{38} given by

$$Y_1 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \qquad Y_3 = \{20, 21, 22, 23, 24, 25, 26, 27, 28\}$$
$$Y_2 = \{10, 11, 12, 13, 14, 15, 16, 17, 18, 19\} \qquad Y_4 = \{29, 30, 31, 32, 33, 34, 35, 36, 37\}.$$

The two partitions of symbols, $\mathcal{Q}$ and $\mathcal{S}$, are based on Y. That is, $\mathcal{Q} = \{Q_1, Q_2, Q_3, Q_4\}$ where $Q_1 = Y_1, Q_2 = Y_2, Q_3 = Y_3, Q_4 = Y_4$ and $\mathcal{S} = \{S_1, S_2, S_3, S_4\}$ where $S_1 = Y_2, S_2 = Y_3, S_3 = Y_4, S_4 = Y_1$.
Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{S})$. It can be verified that Π is a $(d, 2)$-partition system for Z_{38} where $d = 34$. Parallel partition and extension on Π results in $2\text{-}ext(\Pi)$, where $|2\text{-}ext(\Pi)| = 287,437$. Theorem 7 for $n = 38$ and $d = 34$ implies $M(40, 34) \geq 287,437$ which is a new lower bound. See Table 6.

Theorem 7 applies to general parallel partition and extension using $r = 2$ symbols. This result can be generalized to arbitrary r provided that a sufficient number of blocks with appropriate Hamming distance properties can be found, along with a corresponding number of partitions of positions and symbols. Table 6 shows new bounds obtained using parallel partition and extension (Theorems 6 and 7).

The general parallel partition and extension technique does not put restrictions on the partitions of positions $\mathcal{P}, \mathcal{R}, \ldots$, and partitions of symbols $\mathcal{Q}, \mathcal{S}, \ldots$, making the search space for good partitions very large. Because of this, we have experimented with several ways of creating partitions. For example, given a partition of positions $\mathcal{P} = \{P_0, P_1, \ldots P_{k-1}\}$, a family of partitions $\{\mathcal{P}_i\}$ can be derived from $\mathcal{P}$ as follows. For all i, $(i \leq 0 < k)$, define $\mathcal{P}_i$, the i^{th} partition of positions, to be $\mathcal{P}_i = \{P_{(i+j) \pmod k}, \forall (0 \leq j < k)\}$. Using this notation, the partitions $\mathcal{P}$ and $\mathcal{R}$ of Example 2 are correspond to $\mathcal{P}_0$ and $\mathcal{P}_1$. In other words, $\mathcal{P}_1$ is obtained by a cyclic shift of the sets in $\mathcal{P}_0$. In this way, each partition $\mathcal{P}_i$ comprises a different partition of the set of positions. Define a similar family of partitions of symbols $\{\mathcal{Q}_i\}$ using a partition of symbols $\mathcal{Q} = \{Q_0, Q_1, \ldots Q_{k-1}\}$ as a starting point. Clearly, each pair of partitions $(\mathcal{P}_i, \mathcal{Q}_i)$ satisfies the conditions of the parallel partition and extension technique. To create the initial partitions $\mathcal{P}$ and $\mathcal{Q}$, we have used several techniques, including a greedy technique and a technique based on integer linear programming. These are described in Sects. 6.1 and 6.2.

Results obtained by parallel partition and extension can be compared with results from the *coset method* [5] and the *contraction method* [5]. The coset method starts with a group X exhibiting $M(n, d')$, for some $d' > d$ and searches for cosets of X at Hamming distance d. The PA A, formed from X together with its cosets, exhibits Hamming distance d. If X is a good PA for $M(n, d')$, the PA A could represent a new lower bound for $M(n, d)$. The operation of contraction on a PA Y on Z_{n+1} with Hamming distance $d + 1$ results in new PA Y' on Z_n. As with the coset method, if Y is a good PA for $M(n + 1, d)$, Y' could exhibit a new lower bound for either $M(n, d - 2)$ or $M(n, d - 3)$, depending on conditions described in [5].

To be competitive, the groups that serve as the starting point for any of these methods must be large. We have used $AGL(1, q)$ and $PGL(2, r)$ for various powers of primes q and r. The coset method and the contraction method are quite fruitful, but there are instances where parallel partition and extension gives better results for $M(n, d)$.

We have also experimented with several methods for generating blocks of permutations with a desired Hamming distance. For example, to search for new PAs that exhibit improved lower bounds for $M(n, d)$, one technique looks for cosets at Hamming distance d from a group G on Z_{n-r} that exhibits $M(n - r, d')$, where $d' > d$. Let $\mathcal{M}$ consist of G and the cosets. Using parallel partition and extension, the permutations in $\mathcal{M}$ are extended by r symbols to create a new PA on Z_n exhibiting $M(n, d)$. Our coset search techniques are discussed in Sect. 6.3.

5 Partition and extension of modified Kronecker product

Kronecker product is a well known operation in linear algebra, combinatorics, and other areas of mathematics [15,16]. A modification of the Kronecker product operation on PAs can be used to create larger PAs suitable for simple partition and extension.

Let X and Y be PAs defined by $X = \{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ where each α_i is a permutation on l symbols, and $Y = \{\beta_1, \beta_2, \ldots, \beta_m\}$ where each β_i is a permutation on m symbols. The notation $\alpha_i(j)$ denotes the symbol in permutation α_i at position j. Let $(\alpha_i(j), Y)$ denote a modified copy of the PA Y such that each symbol in each permutation of Y has an offset $m \cdot \alpha_i(j)$ added to it. Clearly $|(\alpha_i(j), Y)| = |Y|$. Moreover, like Y, $(\alpha_i(j), Y)$ is a PA on m symbols, however, the symbol set of $(\alpha_i(j), Y)$ is offset by the value $m \cdot \alpha_i(j)$. Hence the PAs Y and $(\alpha_i(j), Y)$ have no symbols in common.

Let $(X \otimes Y)_i$ be the PA defined by $(X \otimes Y)_i = [(\alpha_i(0), Y), (\alpha_i(1), Y), \ldots, (\alpha_i(l-1), Y)]$. That is, if β_r is the permutation in Y, there is a corresponding permutation γ on lm symbols in $(X \otimes Y)_i$ of the form $\gamma = (m \cdot \alpha_i(0) + \beta_r(0)), \ldots, (m \cdot \alpha_i(0) + \beta_r(m - 1)), (m \cdot \alpha_i(1) +$

Fig. 1 The PA $(X \otimes Y)$, the modified Kronecker product of PA's X and Y

$(\alpha_1(1), Y)$	$(\alpha_1(2), Y)$	$\dots$	$(\alpha_1(l), Y)$
$(\alpha_2(1), Y)$	$(\alpha_2(2), Y)$	$\dots$	$(\alpha_2(l), Y)$
$\dots$			
$(\alpha_l(1), Y)$	$(\alpha_l(2), Y)$	$\dots$	$(\alpha_l(l), Y)$

$\beta_r(0)), \dots, (m\cdot\alpha_i(1)+\beta_r(m-1)), \dots, (m\cdot\alpha_i(l-1)+\beta_r(0)), \dots, (m\cdot\alpha_i(l-1)+\beta_r(m-1))$. In other words, γ can be viewed as the concatenation of l copies of β_r with an appropriate offset added to the symbols in each copy. The offsets ensure that each of the $|Y|$ rows in the sub-array $(X \otimes Y)_i$ is a permutation on the lm symbols $\{0, 1, 2 \dots lm - 1\}$.

Define the modified Kronecker product [2] of PAs X and Y, denoted by $(X \otimes Y)$, to be the PA on lm symbols defined by $(X \otimes Y) = \bigcup_{i=1}^{l} (X \otimes Y)_i$. This is illustrated in Fig. 1.

Define the *block decomposition* of a PA A on n symbols as a collection of sub-arrays (*i.e., blocks*), say $A^{(1)}, A^{(2)}, \dots, A^{(m)}$, such that for all i $(1 \le i \le m)$, $hd(A^{(i)}) = n$. A detailed discussion of block decomposition appears in [2], along with several examples using $AGL(1, q)$ and $PGL(2, q)$, where q is a prime or a prime power. We use block decompositions of PAs and the modified Kronecker product to produce new PAs, which in some cases give new lower bounds for $M(n + 1, n)$. Corollaries 10 and 11 below describe our results. Our block decompositions have a property that the blocks are *full, i.e.,* $|A^{(i)}| = n$. We need two lemmas describing properties of PAs produced by modified Kronecker product to establish Corollaries 10 and 11.

Lemma 8 ([2]) *Let $A^{(1)}, A^{(2)}, \dots, A^{(k)}$ be a block decomposition of a PA A on l symbols with $hd(A) = l - a$ Let $B^{(1)}, B^{(2)}, \dots B^{(k)}$ be a block decomposition of PA B on m symbols with $hd(B) = m - b$. Let $M_i = A^{(i)} \otimes B^{(i)}$ Then*

$$hd\left(\bigcup_{i=1}^{k} M_i\right) = lm - ab.$$

Lemma 9 *Let $A^{(1)}, A^{(2)}, \dots, A^{(k)}$ be a block decomposition of a PA A on l symbols with $hd(A) = l - 1$. Let $B^{(1)}, B^{(2)}, \dots B^{(k)}$ be a block decomposition of PA B on m symbols with $hd(B) = m - 1$. Then $M(n + 1, n) \ge kn$, where $n = lm$.*

Proof First, we set $\mathcal{M} = \{M_1, M_2, \dots, M_k\}$ where for all i, $(i = 1, 2, \dots, k)$, $M_i = A^{(i)} \otimes B^{(i)}$. That is, M_i is the modified Kronecker product of the blocks $A^{(i)}$ and $B^{(i)}$. The PA M_i can be viewed as an $l \times l$ table of blocks. In particular, the columns of this table are columns of blocks, and the rows of the table are rows of blocks. We will refer to the rows and columns as *block rows* and *block columns*, respectively. Let $C_1, C_2, \dots, C_l$ be the block columns of the table. For each block column C_j, $(j = 1, 2, \dots, l)$ we select the $(i - 1)^{st}$ position in C_j, keeping in mind that positions are numbered starting at 0. Let P_i be the set of selected positions. That is, $P_i = \{i - 1, (i - 1) + l, (i - 1) + 2l, \dots, (i - 1) + kl\}$. We choose the symbols for Q_i as $0, 1, \dots, m - 1$ with added offset $(i - 1)m$. That is, $Q_i = \{0 + (i - 1)m, 1 + (i - 1)m, \dots, (m - 1) + (i - 1)m\}$. Note that each block row of the table contains a block column such that all symbols in it have offset $(i - 1)m$. Therefore all permutations in this block row are covered. The lemma follows since all klm permutations of the modified Kronecker product are covered. □

Corollary 10 *Let p and q be prime powers. Let $n = pq$ and $k = \min\{p-1, q-1\}$. Then $M(n+1, n) \geq kn$.*

Proof It follows from Lemma 9 if we take the affine general linear groups $A = AGL(1, p)$ and $B = AGL(1, q)$. □

Corollary 11 *Let $n \geq 2$ and $m \geq 2$ be integers. Let N_n be the maximum number of MOLS of order n. Let $k = \min\{N_n, N_m\}$. Then $M(nm+1, nm) \geq knm$.*

Proof Colbourn et al. [9] proved that a set of k MOLS of order n can be transformed into a permutation array A of size kn on Z_n. Each Latin square C_s is transformed into a block D_s of n permutations with pairwise Hamming distance n. The transformation changes triples $(i, j, k) \in C_s$ to triples $(k, j, i) \in D_s$. In other words, for all $i, j, k \in Z_n$ the symbol k in row i and column j in the Latin square C_s becomes the symbol i in row k and column j in the block D_s.

Suppose there are k MOLS of order n. Denote the Latin squares by $A_1, A_2, \ldots, A_k$. The transformation creates k blocks, say $B_1, B_2, \ldots, B_k$ of permutations on n symbols. Moreover, the pairwise Hamming distance between blocks B_i, B_j for all i, j, $(1 \leq i, j, \leq k,\ i \neq j)$ is $n-1$. We repeat this transformation for k MOLS of order m to create the block decomposition $E_1, E_2, \ldots, E_k$ of permutations on Z_m, with pairwise Hamming distance $m-1$. By Lemma 9, $M(nm+1, nm) \geq knm$. □

Example 3 shows several new bounds obtained by Corollary 10. Additional new results obtained by Corollaries 10 and 11 are listed in Tables 10 and 11.

Example 3 A sample of results from Corollary 10 with $A = AGL(1, p)$ and $B = AGL(1, q)$.

(a) $M(117{,}116) \geq 8 \cdot 117 = 936$ by using $p = 9$ and $q = 13$. So $M(118{,}117) \geq 936$.
(b) $M(171{,}170) \geq 8 \cdot 171 = 1368$ by using $p = 9$ and $q = 19$. So $M(172{,}171) \geq 1{,}368$.
(c) $M(187{,}186) \geq 10 \cdot 187 = 1870$ by using $p = 11$ and $q = 17$. So $M(188{,}187) \geq 1870$.
(d) $M(299{,}298) \geq 12 \cdot 299 = 3588$ by using $p = 13$ and $q = 23$. So $M(300{,}299) \geq 3588$.
(e) $M(575{,}574) \geq 22 \cdot 575 = 12{,}650$ by using $p = 23$ and $q = 25$. So $M(576{,}575) \geq 12{,}650$.

6 Algorithms for selecting partitions

In Sects. 3, 4 and 5, we described three new enhancements of the partition and extension operation which are used for transforming a distance-d partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ on Z_n, for some positive integer d, into a new PA on Z_{n+r} for positive integers r, such that the Hamming distance of the new PA is at least d' for some $d' \geq d$. The size of a PA resulting from the application of any of these techniques to a particular distance-d partition system, $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$, is of course entirely dependent on the choice of $\mathcal{M}$, $\mathcal{P}$, and $\mathcal{Q}$. Exhaustive search for high yield partitions $\mathcal{P}$ and $\mathcal{Q}$ amounts to trying all possible partitions of Z_n. Similarly, selecting a productive set of PAs to include in $\mathcal{M}$ involves selecting sets from partitions of S_n, the symmetric group of permutations on n symbols. Clearly, any sort of exhaustive search is infeasible.

This leads to a natural question: how to select the sets $\mathcal{M}$, $\mathcal{P}$, and $\mathcal{Q}$. We now describe several techniques we have found useful for selecting partitions for the set $\mathcal{P}$ (or, equivalently, $\mathcal{Q}$), and finding PAs for the set $\mathcal{M}$.

In Sects. 6.1 and 6.2, we turn our attention to methods for finding partitions of Z_n. Such partitions can be fruitful candidates for either for $\mathcal{P}$ or $\mathcal{Q}$. We describe two approaches. Both approaches start with a given partition of symbols $\mathcal{Q}$ and a given collection of PAs $\mathcal{M} = (M_1, M_2, \ldots, M_{k+1})$ on Z_n, for some positive integer k, that satisfies Property I of the definition of a distance-d partition system. Section 6.1 describes a greedy algorithm that uses a fixed partition of symbols $\mathcal{Q}$ and greedily creates a partition of positions, $\mathcal{P}$. Section 6.2 describes an optimization approach that uses integer linear programming to find a fruitful partition of positions, $\mathcal{P}$. To describe the techniques, we focus on creating a partition of positions $\mathcal{P}$, however, the same techniques can be used for creating a partition of symbols $\mathcal{Q}$ instead. We have experimented with both methods and have obtained new lower bounds for $M(n, d)$ which are included in Section 7.

Section 6.3 describes methods we have used for searching for fruitful PAs to include in $\mathcal{M}$. New lower bounds obtained by this method are included in Sect. 7.

6.1 A greedy approach to partition selection

We have developed a greedy algorithm for finding a partition of positions $\mathcal{P}$, which approaches an intractable search problem by fixing both the partition of symbols, $\mathcal{Q}$, and the collection of PAs, $\mathcal{M}$, then greedily creating $\mathcal{P}$, a partition of positions. In this way, the search space is restricted, at the cost of possibly missing an optimum solution.

Our algorithm creates a partition positions $\mathcal{P}$, of Z_n, that maximizes $covered(M_i)$ for all i. The input for the algorithm is a fixed partition of symbols $\mathcal{Q}$ of Z_n, and a collection of PAs on Z_n, $\mathcal{M} = (M_1, M_2, \ldots, M_k)$, that satisfies properties I and II of a distance-d partition system for some $d < n$. We fix $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_k)$ for some $k \leq \sqrt{n}$ where $Q_1 = \{0, 1, \ldots, k-1\}$, $Q_2 = \{k, \ldots, 2k-1\}, \ldots$ $Q_k = \{k^2 - k, \ldots, k^2 - 1\}$.

The algorithm starts with a set of subsets of positions $\{P_1, P_2, \ldots, P_k\}$ where $P_i = \emptyset$ for all i $(0 \leq i \leq k-1)$. The algorithm then iterates to find a partition of positions $\mathcal{P}$ that represents a local maximum for the number of covered permutations. At each iteration, an unused position, r, is selected. Let $M_i' = M_i \setminus covered(M_i)$. That is, M_i' is the set of permutations $\{\sigma\}$ in M_i for which there is no position $p \in P_i$ such that $\sigma(p) = q$ for some $q \in Q_i$. For each i $(1 \leq i \leq k)$, we count the number of covered permutations for $(M_i', P_i \cup \{r\}, Q_i)$. If the number of covered permutations is maximized for some $i = i^*$, then we add r to P_{i^*}. The algorithm stops when there are no more unused positions.

The resulting partition $\mathcal{P}$, together with $\mathcal{Q}$ and $\mathcal{M}$ form a distance-d partition system for Z_n, $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$. So, by Theorem 1, $hd(ext(\Pi)) \geq d$. There are several instances for which our greedy approach results in a partition system Π that provides full coverage, that is, for all i $(1 \leq i \leq k)$, $covered(M_i) = M_i$. When Π is derived from large PAs such as $AGL(1, q)$, for q, a power of a prime, improved lower bounds can be achieved for $M(q+1, d)$. A list of results is included in Tables 9, 10 and 11.

6.2 An optimization approach to partition selection

We describe another approach for finding a partition of positions $\mathcal{P}$, which casts the search for $\mathcal{P}$ as an optimization problem. Like the greedy method, our optimization approach starts with a given partition $\mathcal{Q}$ of symbols, and a collection $\mathcal{M}$ of PAs that satisfies properties I and II of a distance-d partition system for some $d < n$. We encode the search for $\mathcal{P}$ as an integer linear program (ILP) and use an off-the-shelf *solver* to explore the entire search space of partitions for $\mathcal{P}$. There are several commercial solvers [14,18] capable of solving large ILP problems efficiently. We have chosen the Gurobi optimizer [14] for our computations.

We now describe our ILP encoding. The input is a partition of symbols $\mathcal{Q}$ and a collection $\mathcal{M}$ of blocks (PAs) on n symbols. Let k be the number of blocks. Let $c_{i,j}$ be a binary variable indicating that permutation j of block i is covered. Let $u(i)$ be a function that maps the block index i to the number of permutations in it. Let $b_{i,p}$ be a binary variable indicating that position p is assigned to block i.

An integer linear program for selecting partitions

$$\underset{c_{i,j}}{\text{maximize}} \sum_{i=0}^{k-1} \sum_{j=0}^{u(i)-1} c_{i,j} \tag{3}$$

subject to

$$\sum_{i=0}^{k-1} b_{i,p} = 1;\ \ \forall p; \tag{4}$$

$$\sum_{y \in Q_i} \mathbb{1}_{\sigma\, p,y} \cdot b_{i,p} \geq c_{i,j};\ \ \forall i, j, p; \text{ and} \tag{5}$$

$$\sum_{i=0}^{k-1} \sum_{p=0}^{n-1} b_{i,p} = n; \tag{6}$$

$$\text{where} \quad \mathbb{1}_{\sigma_{p,y}} = \begin{cases} 1 & \text{if } \sigma[p] = y \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

Equation (3) is the objective function to be maximized, that is, the total number of covered permutations in all blocks in $\mathcal{M}$. The optimization is subject to three constraints:

- Constraint (4) assures that the resulting partition $\mathcal{P}$ assigns a position to exactly one block.
- Constraint (5) establishes that permutation j in block i is covered when at least one of its symbols listed in Q_i appears in position p, and p is assigned to this block i.
- Constraint (6) assures that every position has been assigned to some block.

Constraints (4) and (6) effectively ensure that the solution is a partition. Equation (7) defines an indicator function that states whether or not a permutation σ is covered by checking if symbol y appears at position p.

Our integer linear program has provided many new lower bounds for $M(n, d)$, and has has outperformed our greedy approach in several instances. See Tables 9, 10 and 11.

6.3 Methods for coset search

We have used several methods for coset search, including the *coset method* [5] and Integer Linear Programming.

Given a group G on Z_n for some n, the coset method creates a collection of PAs $\mathcal{M}$ to be used for partition and extension by randomly searching for cosets of G at a specified pairwise Hamming distance d. The group $G = M_1$, with its cosets, $M_2, M_3, \ldots,$ comprise $\mathcal{M} = (M_1, M_2, M_3, \ldots,)$ in a distance-d partition system Π. When the starting group G is large, the coset method often produces a productive collection of PAs for $\mathcal{M}$.

Table 7 New $M(n, d)$ lower bounds obtained by applying Theorem 1 to PAs generated by the coset method [5]

n	d	PREV	NEW
43	37	176,988	369,948
49	43	207,552	415,062
51	44	235,200	687,903
51	45	235,200	470,347
61	54	410,640	1,181,794
69	62	601,392	1,500,426

Column *PREV* shows previously known bounds (obtained from rudimentary parallel partition and extension, by applying Theorem 6). Column *NEW* shows new bounds obtained through Theorem 1

Table 7 shows the lower bounds obtained by applying Theorem 1 to new permutation arrays computed using the coset method. For example, for our new lower bound for $M(43, 37)$, we start with the projective general linear group $G = PGL(2, 41)$, which has 68,880 permutations on Z_{42}, and looked for cosets of G at Hamming distance 36. We were able to find five cosets, M_2, M_3, M_4, M_5, M_6, which together with the group $G = M_1$ gives a collection of 6 blocks with 68,800 permutations each, giving a total of 413,280 permutations at Hamming distance 36. This gives $\mathcal{M} = (M_1, M_2, \ldots, M_6)$. We were also able to find a partition of positions $\mathcal{P}$ and a partition of symbols $\mathcal{Q}$, which, together with $\mathcal{M}$ forms a distance-37 partition system $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ for Z_{42}. Using simple partition and extension on Π, we obtained 369,948 permutations on 43 symbols with Hamming distance 37. That is, we show that $M(43, 37) \geq 369,948$, which is an improvement over the previous lower bound of 176,988.

We have also searched for fruitful PAs by formulating the coset search problem as a constraint satisfaction problem, implemented as an integer linear program. Given a group G on Z_n, where $hd(G) \geq d$, let d' be the target Hamming distance between a coset representative $\pi \in S_n$ and the group G. Let $X = Z_n \times Z_n = \{(0, 0), (0, 1), \ldots, (i, j), \ldots, (n-1, n-1)\}$. The set X represents all possible pairs of positions and symbols assignable to the coset representative π.

Create a binary variable $x_{i,j}$ for each element in the set X indicating that if the variable $x_{i,j}$ is true, then $\pi(i) = j$. The integer linear program is:

$$\underset{x_{i,j}}{\text{maximize}} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} x_{i,j} \tag{8}$$

subject to

$$\sum_{j=0}^{n-1} x_{i,j} = 1; \ \forall i \in Z_n, \tag{9}$$

$$\sum_{i=0}^{n-1} x_{i,j} = 1; \ \forall j \in Z_n, \text{ and} \tag{10}$$

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \mathbb{1}_{\sigma_{i,j}} \cdot x_{i,j} \leq n - d; \ \forall \sigma \in G, \tag{11}$$

$$\text{where} \quad \mathbb{1}_{\sigma_{i,j}} = \begin{cases} 1 & \text{if } \sigma(i) = j \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Table 8 New lower bounds for $M(n, d)$ using PAs generated by the coset method [5] and by ILP approximation described in Sect. 6.3

n	d	Group	Num cosets	PREV	NEW
18	13	$PGL(2,17)$	6	24,480	$29{,}376_j$
24	19	$PGL(2,23)$	3	24,288	$36{,}432_j$
26	20	$PGL(2,25)$	15	202,800	$234{,}000_j$
26	21	$PGL(2,25)$	3	31,200	$46{,}800_j$
28	22	$PGL(2,27)$	14	235,872	$275{,}184_j$
30	24	$PGL(2,29)$	12	170,520	$292{,}320_j$
32	25	$PGL(2,31)$	44	372,992	$1{,}309{,}440_j$
33	27	$P\Gamma L(2,32)$	2	97,440	$327{,}360_j$
34	27	$P\Gamma L(2,32)$	15	2,127,840	$2{,}455{,}200_c$
38	32	$PGL(2,37)$	6	202,464	$303{,}696_j$
38	30	$PGL(2,37)$	129	1,265,400	$6{,}529{,}464_c$
42	34	$PGL(2,41)$	73	888,729	$5{,}028{,}240_c$
42	35	$PGL(2,41)$	28	206,640	$1{,}928{,}640_j$
42	36	$PGL(2,41)$	6	206,640	$413{,}280_j$
44	37	$PGL(2,43)$	25	413,280	$1{,}986{,}600_j$
48	42	$PGL(2,47)$	4	207,552	$415{,}104_j$
49	42	$PGL(2,47)$	14	207,552	$1{,}452{,}864_c$
50	42	$PGL(2,49)$	43	207,552	$5{,}056{,}800_c$
50	43	$PGL(2,49)$	18	207,552	$2{,}116{,}800_j$
50	44	$PGL(2,49)$	4	103,776	$470{,}400_j$
54	47	$PGL(2,53)$	16	1,339,416	$2{,}381{,}184_j$
54	48	$PGL(2,53)$	3	297,648	$446{,}472_j$
55	48	$PGL(2,53)$	10	297,648	$1{,}488{,}240_c$
55	49	$PGL(2,53)$	3	297,648	$446{,}472_j$
62	54	$PGL(2,61)$	38	821,280	$8{,}622{,}960_c$
62	55	$PGL(2,61)$	6	821,280	$1{,}361{,}520_c$
68	60	$PGL(2,67)$	29	821,280	$8{,}720{,}184_c$
68	61	$PGL(2,67)$	5	524,160	$1{,}503{,}480_c$
68	62	$PGL(2,67)$	2	524,160	$601{,}392_j$
72	64	$PGL(2,71)$	17	888,729	$6{,}083{,}280_c$
72	65	$PGL(2,71)$	4	357,840	$1{,}431{,}360_c$

Columns: *Group* denotes starting group, *Num Cosets* denotes the number of cosets, *PREV* denotes the previously known bound, and *NEW* denotes the new bound. c coset method (random coset search) [5]; j ILP coset search (see Sect. 6.3)

The objective function (8) is designed to make the ILP solver assign as many binary variables $x_{i,j}$ true as possible. This objective function alone would produce a solution that is not a permutation. For this reason constraints (9) and (10) ensure that exactly one symbol j is assigned to every position i and that every symbol j is assigned to exactly one position i, respectively, so the solution is indeed a permutation on Z_n. Constraint (11) requires the solution to be at Hamming distance at least d' from every permutation in G. This is encoded by limiting the number of agreements, $n - d'$, between a candidate solution and each of the permutations in G.

Table 9 An aggregated table showing our new lower bounds for $M(n, d)$, for $n < 550$ and $d < n - 1$. The subscripts give the tables containing more details about the new results

n	d	PREV	NEW	n	d	PREV	NEW	n	d	PREV	NEW
18	13	24,480	29,376$_8$	53	47	148,824	470,400$_6$	171	169	2354	27,330$_4$
24	19	24,288	36,432$_8$	54	46	8,036,496	8,334,144$_8$	175	173	2354	19,792$_4$
26	20	202,800	234,000$_8$	54	47	1,339,416	2,381,184$_8$	183	181	2533	21,994$_4$
26	21	31,200	46,800$_8$	54	48	297,648	446,472$_8$	195	193	2758	25,022$_4$
28	22	235,872	275,184$_8$	55	48	297,648	1,488,240$_8$	201	199	2867	25,427$_4$
30	24	170,520	292,320$_8$	55	49	297,648	446,472$_8$	213	211	3170	30,288$_4$
30	26	24,360	58,968$_6$	55	53	423	2461$_4$	225	223	3421	32,728$_4$
32	25	372,992	1,309,440$_8$	56	50	205,320	446,472$_6$	231	229	3548	33,779$_4$
33	27	97,440	327,360$_8$	61	54	410,640	1,181,794$_7$	235	233	3625	35,001$_4$
34	27	2,127,840	2,455,200$_8$	62	54	821,280	8,622,960$_8$	245	243	3475	43,717$_4$
34	32	192	945$_4$	62	55	821,280	1,361,520$_8$	253	251	4075	40,094$_4$
38	30	1,265,400	6,529,464$_8$	63	61	1514	3306$_4$	259	257	4222	43,268$_4$
38	32	202,464	303,696$_8$	66	64	576	4029$_4$	265	263	4342	44,733$_4$
39	37	255	1301$_4$	68	60	821,280	8,720,184$_8$	273	271	4548	46,268$_4$
40	34	68,880	287,437$_6$	68	61	524,160	1,503,480$_8$	279	277	4701	49,243$_4$
42	34	888,729	5,028,240$_8$	68	62	524,160	601,392$_8$	285	283	4868	51,571$_4$
42	35	206,640	1,928,640$_8$	69	62	601,392	1,500,426$_7$	291	289	5202	80,385$_4$
42	36	206,640	413,280$_8$	69	67	594	3965$_4$	295	293	5088	54,572$_4$
43	37	176,988	369,948$_7$	70	63	524,160	1,503,462$_6$	309	307	5539	60,715$_4$
44	37	413,280	1,986,600$_8$	72	64	888,729	6,083,280$_8$	315	313	5634	60,952$_4$

Table 9 continued

n	*d*	PREV	NEW	*n*	*d*	PREV	NEW	*n*	*d*	PREV	NEW
44	38	68,880	397,198$_6$	72	65	357,840	1,431,360$_8$	319	317	5793	67,379$_4$
45	39	103,776	413,280$_6$	75	73	667	4747$_4$	333	331	6091	70,696$_4$
45	43	270	1726$_4$	85	83	812	6116$_4$	339	337	6280	69,485$_4$
46	39	103,776	551,040$_6$	91	89	902	6709$_4$	345	343	5205	89,272$_4$
48	42	207,552	415,104$_8$	99	97	1017	8206$_4$	351	349	6642	76,195$_4$
49	42	207,552	1,452,864$_8$	105	103	1119	9239$_4$	355	353	6746	77,215$_4$
49	43	207,552	415,062$_7$	111	109	1187	9990$_4$	363	361	7220	125,709$_4$
50	42	207,552	5,056,800$_8$	115	113	1277	11,142$_4$	369	367	7108	83,418$_4$
50	43	207,552	2,116,800$_8$	123	121	1452	13,996$_4$	375	373	7298	87,434$_4$
50	44	103,776	470,400$_8$	133	131	1554	11,604$_4$	385	383	7428	90,213$_4$
51	44	235,200	687,903$_7$	141	139	1723	13,522$_4$	391	389	7690	90,991$_4$
51	45	235,200	470,347$_7$	153	151	1923	16,118$_4$	411	409	8240	104,098$_4$
51	49	392	2308$_4$	159	157	2,051	16,666$_4$	514	512	11,264	197,859$_4$
52	46	148,824	470,397$_6$	165	163	2185	17,632$_4$	531	529	12,696	271,043$_4$

Table 10 New lower bounds for $M(n, n-1), n < 300$

n	Prev	New	n	Prev	New	n	Prev	New
26	133_P	150_a	132	1508_P	1572_g	212	3026_P	3172_i
28	140_M	144_i	134	804_M	931_g	214	1284_M	1491_g
30	170_P	173_g	138	1614_P	1696_g	218	1308_M	1736_g
33	183_P	192_a	140	1640_P	1726_i	220	1320_M	2190_g
34	136_M	165_g	142	852_M	987_g	222	1332_M	2652_g
38	254_P	255_g	145	1015_M	1429_i	224	3260_P	3475_i
42	282_P	286_g	146	876_M	1015_g	225	1800_M	2902_i
44	296_P	307_g	148	888_M	1029_g	226	1356_M	1800_k
46	184_M	270_g	150	1818_P	1905_g	228	3380_P	3482_i
50	300_M	392_a	152	1832_P	1946_g	230	3512_P	3567_g
51	255_M	300_g	155	1085_M	1232_g	234	3602_P	3673_i
54	408_P	423_g	156	936_M	1085_g	236	1416_M	1645_g
58	361_P	399_i	158	1922_P	2052_g	238	1428_M	1659_g
60	481_P	493_g	159	954_M	1106_g	240	3656_P	3803_i
62	478_P	519_g	161	1377_P	1440_i	242	3716_P	3864_g
65	455_M	576_a	162	972_M	1127_g	244	1464_M	3483_a
66	380_P	455_g	164	2042_P	2185_g	246	1476_M	1715_g
68	568_P	594_g	166	1153_P	1155_g	248	1736_M	2964_g
72	588_P	637_g	168	2070_P	2267_g	250	1500_M	1743_g
74	620_P	667_g	170	1020_M	2366_a	252	3932_P	4075_g
76	456_M	525_g	172	1032_M	1368_k	254	2286_M	3027_i
80	720_M	755_g	174	2316_P	2358_i	255	1785_M	2286_g
82	656_M	810_a	177	1593_M	2214_i	258	4066_M	4222_g
84	776_P	812_g	178	1068_P	1593_g	260	1560_M	3108_g
90	866_P	902_g	180	2404_P	2500_g	264	4228_P	4351_i
92	552_M	637_g	182	1092_P	2533_g	266	1862_M	2120_g
98	956_P	1017_g	186	1619_P	1665_g	268	1876_M	2670_g
102	1030_P	1101_g	188	1128_M	1870_k	270	4318_M	4521_i
104	1070_P	1119_g	190	1140_M	1512_g	272	4408_M	4575_i
106	636_M	735_g	192	2638_P	2767_i	274	1644_M	3873_i
108	1090_P	1175_g	194	2680_P	2803_i	276	2760_M	3575_g
110	1130_P	1199_g	196	1176_M	1365_g	278	4574_M	4767_i
114	1192_P	1277_g	198	2786_P	2870_g	280	1960_M	2511_g
116	696_M	805_g	200	2842_P	2867_g	282	4684_M	4863_i
118	708_M	936_k	202	1212_M	1407_i	284	4706_P	4916_i
122	732_M	1452_a	204	1224_M	1421_i	286	1716_M	3420_g
126	756_M	1221_a	206	1236_M	1640_g	290	1740_M	5202_a
129	903_M	1472_a	209	2299_M	2912_g	294	5068_M	5088_g
130	780_M	903_g	210	2100_M	2299_g			

M—previous result from MOLS; *P*—previous result from simple partition and extension [4]; *a*—methods described in [1]; *g*—partition of positions $\mathcal{P}$ from greedy partition selection algorithm (see Sect. 6.1); *i*—partition of positions $\mathcal{P}$ from ILP partition selection algorithm (see Section 6.2); *k*—PA $\mathcal{M}$ from modified Kronecker product (see Sect. 5)

Table 11 New lower bounds for $M(n, n-1)$, $(300 \le n \le 600)$

n	Prev	New	n	Prev	New	n	Prev	New
300	2100_M	3588_k	406	2842_M	3240_k	494	2964_M	7888_k
306	1836_M	4575_i	408	4070_M	6105_i	498	2988_M	7455_k
308	5360_M	5524_i	410	2870_M	8389_i	500	3500_M	11373_i
312	5436_M	5660_i	412	3296_M	5343_g	504	3527_M	11416_i
314	2198_M	5723_i	414	4140_M	4956_g	506	3036_M	7575_i
316	2212_M	3150_g	415	3735_M	4140_g	508	3556_M	7605_i
318	2226_M	5793_g	417	6255_M	7481_i	510	3060_M	11661_i
322	1932_M	4815_g	418	2926_M	6255_i	513	9234_M	11264_a
324	2592_M	5168_k	420	2940_M	8744_i	516	4128_M	7725_g
326	1956_M	3900_k	422	2954_M	8822_i	518	5170_M	6204_g
330	1980_M	2961_g	424	3384_M	6345_i	520	4160_M	7785_g
332	2324_M	6105_i	426	2556_M	6800_k	522	5220_M	11983_i
334	2338_M	2664_k	430	2580_M	3003_g	524	6288_M	12029_i
335	2010_M	2338_g	432	6480_M	9051_i	526	4208_M	7875_g
338	2028_M	6349_i	434	2608_M	9093_i	528	7920_M	8432_k
340	2040_M	2373_g	436	2616_M	6525_i	530	3710_M	12696_a
344	2408_M	6076_a	438	3066_M	7866_k	532	4256_M	7965_i
346	2076_M	2415_g	440	3159_M	9219_i	534	3738_M	6396_k
348	2088_M	6658_i	442	3528_M	6615_i	536	4288_M	8025_i
350	2800_M	6714_i	444	3108_M	9069_g	538	5380_M	8055_i
354	2124_M	6746_g	446	3122_M	5785_i	540	6480_M	8085_k
356	2492_M	3195_g	450	3220_M	9429_g	542	3794_M	12443_i
358	2148_M	3213_g	452	4510_M	6765_i	545	8704_M	9792_k
360	2520_M	6965_i	456	3192_M	6825_i	548	3836_M	12581_i
362	2172_M	7220_a	458	3206_M	9644_g	550	3850_M	4392_k
366	2196_M	2555_g	460	3220_M	7334_k	552	5220_M	9918_k
368	5520_M	7108_g	462	3234_M	$10{,}061_i$	558	3906_M	$13{,}329_i$
370	2952_M	5535_i	464	6960_M	$10{,}162_i$	561	3927_M	8400_i
372	2604_M	5565_i	466	3262_M	6975_i	564	3948_M	$13{,}500_i$
374	2618_M	7381_i	468	3744_M	$10{,}253_i$	566	3396_M	3955_g
376	2632_M	5625_i	470	3290_M	3752_g	570	3420_M	$13{,}654_i$
378	4524_M	4901_i	472	3304_M	7065_i	572	4004_M	$13{,}699_i$
380	2660_M	7556_i	474	4740_M	7095_k	576	4608_M	$12{,}650_k$
382	2674_M	4572_i	476	3332_M	8550_k	578	4046_M	$13{,}848_i$
384	5760_M	7692_i	478	3816_M	7155_i	582	4074_M	4648_g
386	2702_M	5775_i	480	7200_M	$10{,}538_i$	584	4088_M	5830_i
388	3096_M	5805_i	482	5772_M	7215_i	586	4102_M	4680_g
390	2730_M	7897_i	484	3872_M	7245_i	588	4116_M	$14{,}088_i$
392	2744_M	6256_k	485	3395_M	3872_g	590	$10{,}030_M$	$10{,}602_k$
398	2786_M	7940_i	486	2916_M	3395_g	591	4137_M	$10{,}030_i$

Table 11 continued

n	Prev	New	n	Prev	New	n	Prev	New
402	2814_M	8020_i	488	3416_M	$10{,}714_i$	594	4752_M	$14{,}232_i$
404	4836_M	6045_k	490	2940_M	7335_g	596	4172_M	8925_i
405	3240_M	4444_g	492	2952_M	$10{,}802_i$	600	8400_M	14828_i

Refer to Table 10 for an explanation of the subscripts

Table 8 gives a detailed view of new lower bounds for $M(n, d)$, resulting from our coset search techniques. For each new result, the group, G and the number of cosets is shown. The subscript j in the column labeled *NEW* indicates that the cosets were found by the integer linear program described in Sect. 6.3 [20]. The subscript c indicates that the cosets were found by the coset method [5].

7 Summary of new results

We have computed many new lower bounds for $M(n, d)$ for various n and d using our new techniques for partition and extension, namely: sequential partition and extension (Corollary 4 and Theorem 5), parallel partition and extension (Theorem 6, 7), and modified Kronecker product (Corollaries 10, and 11). These techniques are described in Sects. 3, 4, and 5. We have also used our earlier technique of simple partition and extension (see Theorem 1 [4]) to generate new lower bounds. The use of partition and extension requires, as input, a partition of positions and a separate partition of symbols. We have used our greedy and ILP algorithms, (described in Sect. 6.1 and 6.2), to obtain fruitful partitions of positions for many n. We have described methods for generating good collections of PAs for our partition and extension techniques (see Sect. 6.3).

We summarize all of our new lower bounds for $M(n, d)$, for $d < n - 1$, in Table 9 for the sake of easy referencing. We also report experimental results and provide new tables of lower bounds for $M(n, n-1)$, for many integers $n < 600$. Due to the large number of results, we show these separately from our results for $M(n, d)$, for $d < n-1$. Tables 10 and 11 show new lower bounds for $M(n, n-1)$ computed by our partition and extension techniques. Columns *PREV* and *NEW* in Tables 10 and 11 denote the previous and the new bound, respectively. The previous lower bounds are either from an earlier use of simple partition and extension [4], and are denoted with a subscript P, or are derived from known numbers of mutually orthogonal squares (MOLS) [8], and are denoted with a subscript M. It should be noted that there are other known lower bounds for $M(n, n-1)$, for integers n not listed in Tables 10 and 11. They have been previously reported in [4,8], and [19]. The subscripts in the *NEW* column indicate the method for generating either the partition of positions $\mathcal{P}$ or the collection of PAs $\mathcal{M}$. Subscript g indicates that $\mathcal{P}$ was computed using the greedy partition selection algorithm (see Sect. 6.1). Subscript i indicates that $\mathcal{P}$ was computed using the integer linear program for partition selection (see Sect. 6.2). Subscript a indicates new bounds described in [1]. Subscript k indicates the collection of PAs $\mathcal{M}$ is obtained by modified Kronecker product (see Sect. 5).

In conclusion, we offer the following conjecture about the relationship between $N(n)$, the known lower bound on the number of MOLS of side n and $M(n, n-1)$:

$$\textit{Conjecture: } M(n, n-1) \geq (n-1) \cdot \min(\lfloor\sqrt{n-1}\rfloor, N(n-1)). \tag{13}$$

Table 12 A comparison of experimentally computed $M(n, n-1)$ lower bounds to conjectured lower bounds for four cases that (so far) do not agree with the conjecture. Column *Computed* shows known bounds obtained from techniques described in this paper. Column *Conjectured* shows conjectured bounds from Equation 13

n	d	Computed	Conjectured
145	144	1429	1440
177	176	2214	2288
225	224	2902	2912
254	253	3027	3036

This conjecture is based on our computational results. We verified that the conjecture is true for all $n \leq 600$, except the four cases listed in Table 12. Although these may seem to be counterexamples for the conjecture, we believe the computed values can be improved, and therefore, the conjecture validated for all $n \leq 600$.

8 Conclusion

We have presented new computational methods for the partition and extension technique that produce several competitive new lower bounds on $M(n, d)$ for various integers n and d. We described sequential partition and extension, which is very useful for improving lower bounds. The techniques of rudimentary and general parallel partition and extension introduce several new symbols simultaneously. They are different extension strategies that provide many improved lower bounds for $M(n, d)$. We have given several new techniques and experimental results that provide new lower bounds for $M(n, n-1)$, for many integers $n < 600$.

Acknowledgements We would like to thank Zachary Hancock and Alexander Wong, who separately wrote programs to compute some of our improved lower bounds.

References

1. Bereg S., Hancock Z., Mojica L.G., Morales L., Sudborough H., Wong A.: Permutation arrays for p^k+1, where p is prime. Manuscript (2017).
2. Bereg S., Mojica L.G., Morales L., Sudborough H.: Kronecker product and tiling of permutation arrays for hamming distances. In: the 2017 IEEE International Symposium on Information Theory (ISIT), pp. 2198–2202 (2017).
3. Bereg S., Mojica L.G., Morales L., Sudborough I.H.: Parallel partition and extension. In: 51st Annual Conference on Information Sciences and Systems (CISS 2017), pp. 1–6 (2017).
4. Bereg S., Morales L., Sudborough I.H.: Extending permutation arrays: improving MOLS bounds. Des. Codes Cryptogr. **83**(3), 661–683 (2017).
5. Bereg S., Levy A., Sudborough I.H.: Constructing permutation arrays from groups. Des. Codes Cryptogr. **86**(5), 1095–1111 (2018).
6. Cameron P.J.: Permutation Groups, vol. 45. Cambridge University Press, New York: (1999).
7. Chu W., Colbourn C.J., Dukes P.: Constructions for permutation codes in powerline communications. Des. Codes Cryptogr. **32**, 51–64 (2004).
8. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs. CRC Press, Boca Raton (2006).
9. Colbourn C., Kløve T., Ling A.C.: Permutation arrays for powerline communication and mutually orthogonal latin squares. IEEE Trans. Inf. Theory **50**(6), 1289–1291 (2004).
10. Conway J.H., Curtis R.T., Norton S.P., Parker R.A.: Atlas of Finite Groups. Oxford University Press, Oxford (1985).
11. Deza M., Vanstone S.A.: Bounds for permutation arrays. J. Stat. Plan. Inference **2**, 197–209 (1978).

12. Dixon J.D., Mortimer B.: Permutation Groups, vol. 163. Springer, New York (1996).
13. Gao F., Yang Y., Ge G.: An improvement on the Gilbert–Varshamov bound for permutation codes. IEEE Trans. Inf. Theory **59**(5), 3059–3063 (2013).
14. Gurobi I.: Optimization. Gurobi Optimizer Reference Manual (2016).
15. Henderson H.V., Pukelsheim F., Searle S.R.: On the history of the Kronecker product. Linear Multilinear Algebra **14**(2), 113–120 (1983).
16. Holmquist B.: The direct product permuting matrices. Linear Multilinear Algebra **17**(2), 117–141 (1985).
17. Huczynska S.: Powerline communication and the 36 officers problem. Philos. Trans. R. Soc. Lond. A Math. Phys. Eng. Sci. **364**(1849), 3199–3214 (2006).
18. IBM ILOG: CPLEX. V12. 1: User's manual for CPLEX. Int. Bus. Mach. Corp. **46**(53), 157 (2009).
19. Janiszczak I., Lempken W., Östergård P.R.J., Staszewski R.: Permutation codes invariant under isometries. Des. Codes Cryptogr. **75**(3), 497–507 (2015).
20. Mojica L.G.: Permutation arrays with large Hamming distance. PhD Thesis, University of Texas at Dallas, Richardson (2017).
21. Nguyen Q.T.: Transitivity and hamming distance of permutation arrays. PhD thesis, University of Texas at Dallas, Richardson (2013)
22. Pavlidou N., Vinck A.H., Yazdani J., Honary B.: Power line communications: state of the art and future trends. IEEE Commun. Mag. **41**(4), 34–40 (2003).
23. Smith D.H., Montemanni R.: A new table of permutation codes. Des. Codes Cryptogr. **63**(2), 241–253 (2012).
24. Von Beth T.: Eine bemerkung zur abschätzung der anzahl orthogonaler lateinischer quadrate mittels siebverfahren. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **53**(1), 284–288 (1983).
25. Wang X., Zhang Y., Yang Y., Ge G.: New bounds of permutation codes under hamming metric and Kendall's τ-metric. Des. Codes Cryptogr. **85**(3), 533–545 (2017).