New Results on Permutation Arrays

Ivan Hal Sudborough

University of Texas at Dallas

(joint work with Sergey Bereg, Zachary Hancock, Linda Morales, and Alexander Wong)

Overview`

- Definitions
- Affine General Linear Groups: AGL(1,q)
- Partition and Extension Techniques
- Theorems
- Conclusions and Open Questions

Definitions and Examples

- A *permutation* of Z_n={0,1, … ,n-1} is an unsorted list of elements in Z_n. For example, σ = 4 0 2 3 1 is a permutation of Z_5.
- Also, a one-to-one function $\sigma: Z_n \rightarrow Z_n$, where, for example, σ(0)=4, σ(1)=0, σ(2)=2, σ(3)=3, σ(4)=1.
- Two permutations σ and τ on Z_n have *Hamming distance* d, if $\sigma(x) \neq \tau(x)$, for exactly d different symbols x in Z_n. (This is denoted by *hd(σ,τ)=d*.)

Definitions and Examples

- For example, $\sigma = 4\ 0\ 2\ 3\ 1$ and

  $\tau = 0\ 2\ 3\ 1\ 4$

  have Hamming distance 5. (That is, $hd(\sigma,\tau)=5$.)
- An *array* (set) of permutations S of Z_n has Hamming distance d, if, for every two distinct permutations σ and τ in S, $hd(\sigma,\tau) \geq d$. (*Denoted by $hd(S) \geq d$.*)
- Let M(n,d) denote the largest number of permutations of Z_n with Hamming distance d.

Affine General Linear Group: AGL(1,q)

- Let q be a power of a prime.

- AGL(1,q) is the sharply 2-transitive group consisting of all permutations in { p(x) = ax+b | a,b in GF(q), a≠0 }, where GF(q) denotes the Galois field of order q.

Affine General Linear Group: AGL(1,q)

- C = { x+b | b in GF(q) }. The permutations in C form the addition table of GF(q).
- C_2 = { 2x+b | b in GF(q) } and, in algebraic terms, the *coset* of C obtained by composing the permutation p(x)=2x with everything in C.
- Both consists of q permutations with Hamming distance q, *i.e.* no agreements anywhere.

Affine General Linear Group: AGL(1,q)

- Similarly, we have cosets C_3, C_4, C_5, … , C_{q-1}, for a = 3, 4, 5, … , q-1.
- Altogether, AGL(1,q) consists of q(q-1) permutations and has Hamming distance q-1.
- So, whenever q is a power of a prime, M(q,q-1) = q(q-1).

A technique to generate new PA's

- We consider a technique called *Partition and Extension* (P&E)
- It enables one often to convert a PA A on n symbols with Hamming distance d to a new PA A' on n+1 symbols with Hamming distance d+1.

Partition and Extension (P&E)

- We illustrate P&E for the group AGL(1,q)
- We define sets of positions P_i and symbols S_i for each chosen coset C_i. For different cosets, both the position sets and the symbol sets must be disjoint.
- For each chosen coset C_i, we put the new symbol in one of the defined positions in P_i if symbol in S_i occurs there, and we move that symbol in S_i to the end of the permutation.

P&E

- For all i, a permutation π in block B_i is *covered* if a symbol s in the set S_i occurs in a position p in the set P_i, *i.e.* $\pi(p)=s$.

P&E (Example)

Coset 1 for AGL(1,9), *i.e.* the addition table for GF(3^2):

Positions = {1,2,4} Symbols = {0,2,6}

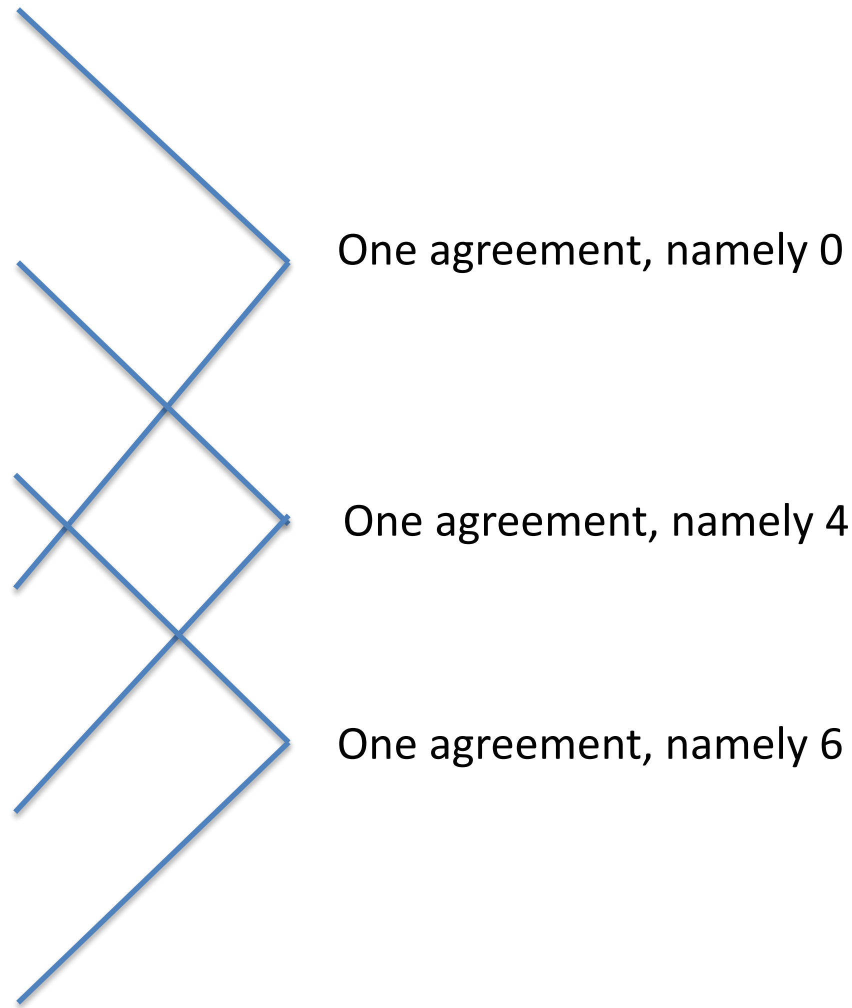
0	1	**2**	3	4	5	6	7	8
1	5	8	4	**6**	0	3	2	7
2	8	**6**	1	5	7	0	4	3
3	4	1	7	**2**	6	8	0	5
4	**6**	5	2	8	3	7	1	0
5	**0**	7	6	3	1	4	8	2
6	3	**0**	8	7	4	2	5	1
7	**2**	4	0	1	8	5	3	6
8	7	3	5	**0**	2	1	6	4

we will:
substitute symbol 9 for each chosen symbol and then put the chosen symbol at the end

Hamming distance: cosets 1 and 2

0	1	**2**	3	4	5	6	7	8
1	5	8	4	**6**	0	3	2	7
2	8	**6**	1	5	7	0	4	3
3	4	1	7	**2**	6	8	0	5
4	**6**	5	2	8	3	7	1	0
5	**0**	7	6	3	1	4	8	2
6	3	**0**	8	7	4	2	5	1
7	**2**	4	0	1	8	5	3	6
8	7	3	5	**0**	2	1	6	4

0	2	3	4	5	6	7	8	**1**
1	8	4	6	0	**3**	2	7	5
2	6	1	5	7	0	4	3	**8**
3	1	7	2	6	**8**	0	5	4
4	5	2	8	3	7	**1**	0	6
5	7	6	3	1	4	**8**	2	0
6	0	8	7	4	2	5	1	**3**
7	4	0	1	8	5	**3**	6	2
8	3	5	0	2	**1**	6	4	7



"Freebie"

0	4	5	6	7	8	1	2	3	9
1	6	0	3	2	7	5	8	4	9
2	5	7	0	4	3	8	6	1	9
3	2	6	8	0	5	4	1	7	9
4	8	3	7	1	0	6	5	2	9
5	3	1	4	8	2	0	7	6	9
6	7	4	2	5	1	3	0	8	9
7	1	8	5	3	6	2	4	0	9
8	0	2	1	6	4	7	3	5	9

Partition and Extension for n=p^{2k} for integer k≥1 and prime p (even powers of a prime)

Using P&E on AGL(1, p^{2k}), which has $p^{4k} - p^{2k}$ elements: (So, M(n,n-1) $\geq p^{4k} - p^{2k}$)

Theorem. M(n+1,n) $\geq p^{3k} + p^{2k}$

Proof (sketched):

Proof (sketch)

The elements of GF(p^{2k}) are 2k-tuples of elements in Z_p, say (a_1, a_2, … , a_{2k}), each of which corresponds to an integer in $Z_{p^{2k}}$

For P&E of AGL(1, p^{2k}) we need to:

(1) Define blocks C_1, C_2, … , C_{p^k}

(2) Define sets of symbols S_i for each block

(3) Define sets of positions P_i for each block

Proof (sketch)

Consider the subgroup C of AGL(1, p^{2k})

The permutations in C $\subseteq$ AGL(1, p^{2k}) are the rows of the addition table for GF(p^{2k}), which form a subgroup of p^{2k} permutations.

That is, C = { p(x) = x+b | b$\in$ GF(p^{2k}) }

For P&E the blocks are C=C_1, C_2, … , C_{p^k} (cosets of C)

Proof (sketch)

GF(p^{2k}) can be partitioned into sets A_1, A_2, … , A_{p^k} based on the last k coordinates in the 2k-tuple, *i.e.* (a_{k+1}, a_{k+2}, … , a_{2k}). That is, A_i consists of all values in GF(p^{2k}), whose last k coordinates (its suffix) is the i^{th} choice of (a_{k+1}, a_{k+2}, … , a_{2k}).

Each A_i is called a suffix set.

The set of symbols for C_i is A_i.

Proof (sketch)

Consider a coset C_i of C ($1 \leq i \leq p^k$), where C_1=C.

For P&E, choose a set of ***positions*** P_i which includes one integer from each suffix set

(*P_i must be disjoint from P_j. We compute the actual position sets by max. matching in a bipartite graph*)

(Again, we choose the ***symbol set*** S_i to be **all** of the suffix set A_i.)

Proof (sketch)

It follows, for any permutation σ(x) = mx+b in C_m, where b∈ GF(p^{2k}), there is a position j such that σ(j) is in A_m.

That is, C_m is a column shifted addition table of GF(p^{2k}), so $\exists j$[(b + j)∈A_m].

Note: The values of j give all possible suffixes, and b is fixed, so the sum b+j gives all possible suffixes.

So, one position must yield a sum in suffix set A_m .

Proof (sketch)

For example, $n=9 = 3^2$

The elements of $GF(3^2)$ are (a_1, a_2), where $a_i \in Z_3$,

and the suffix classes are:

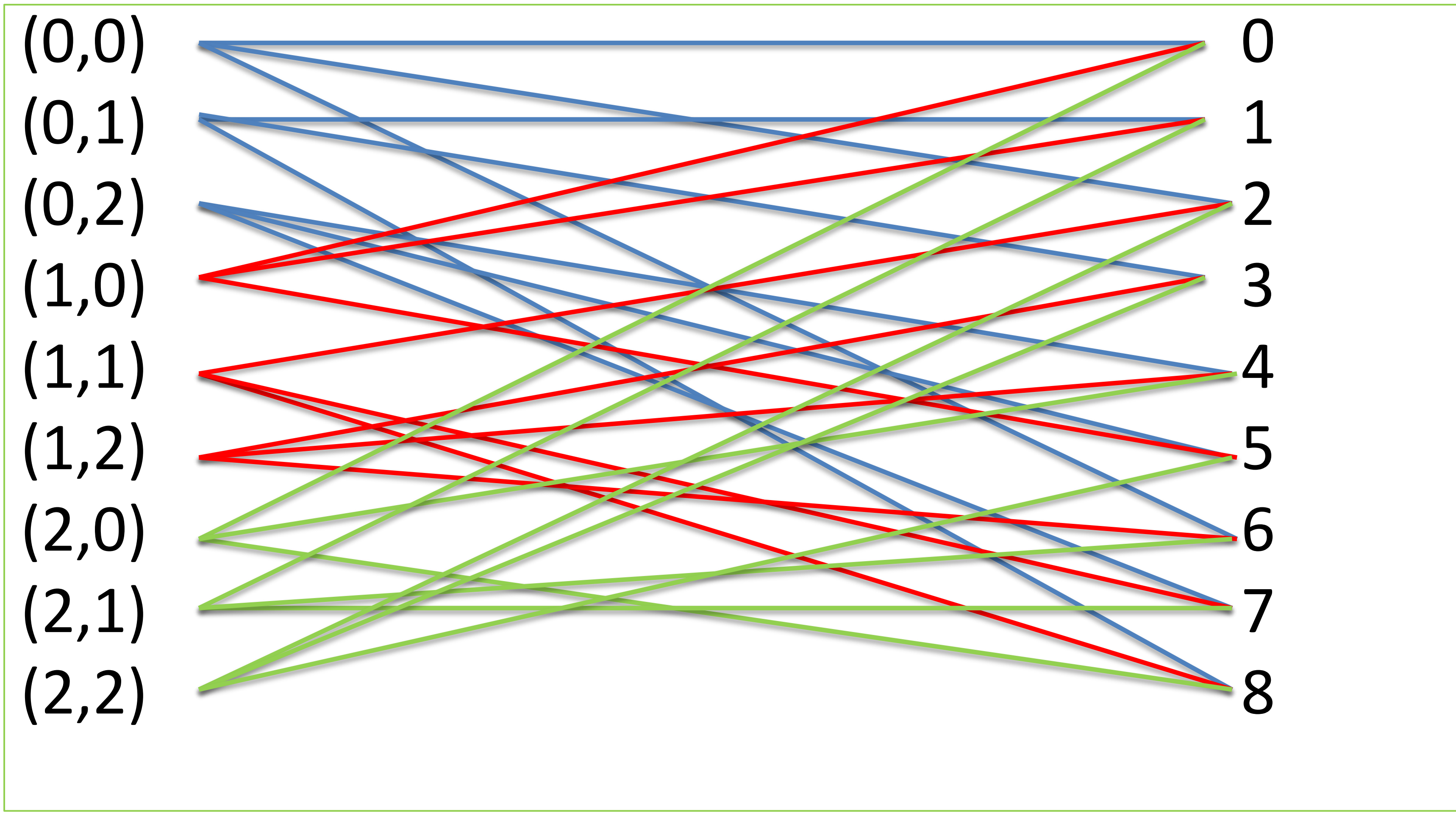
A_1	A_2	A_3
0 = (0,0)	1 = (0,1)	4 = (2,2)
2 = (1,0)	3 = (2,1)	5 = (0,2)
6 = (2,0)	8 = (1,1)	7 = (1,2)

Proof (sketch): Cyclic shift of columns

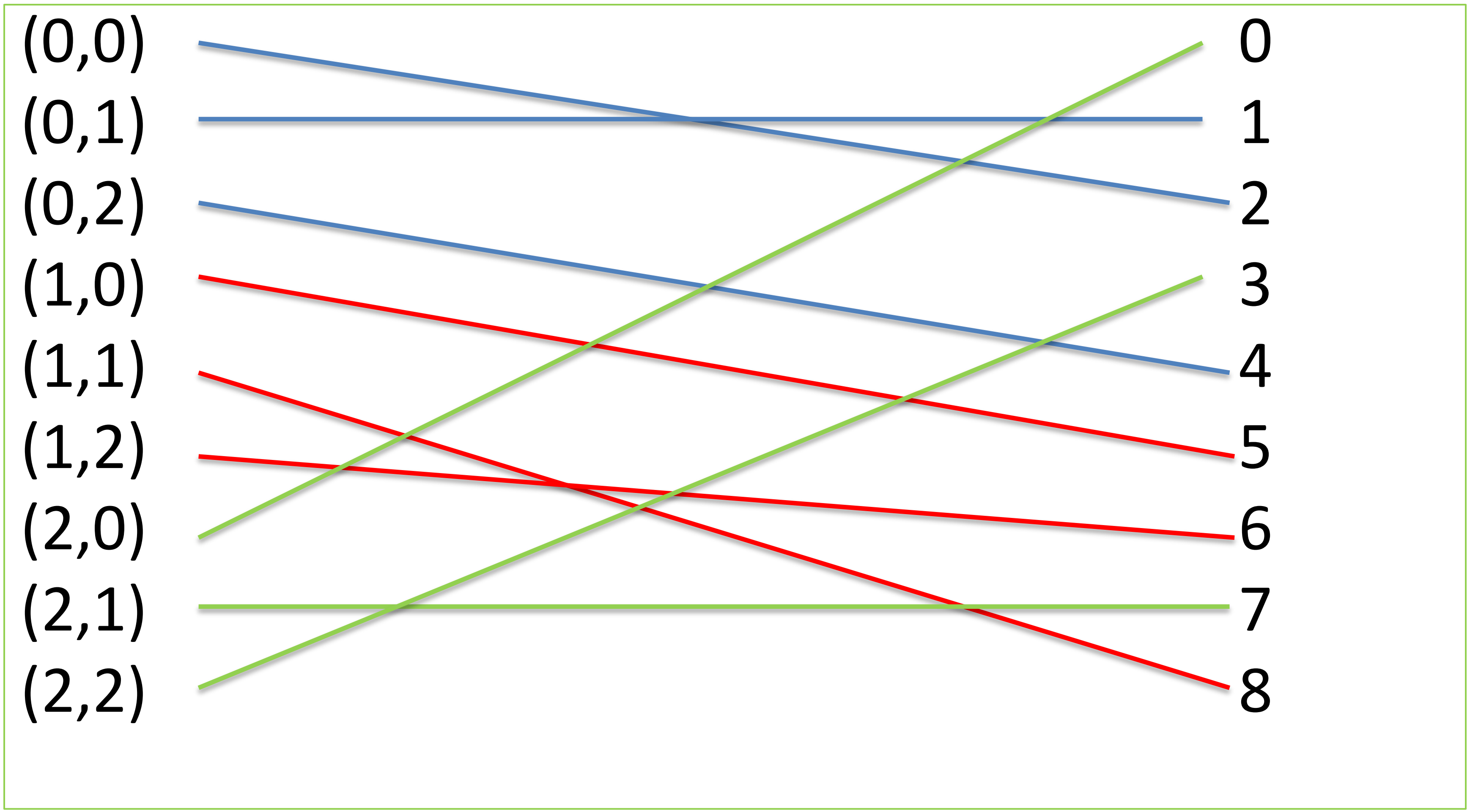
$$C = \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 8 & 4 & 6 & 0 & 3 & 2 & 7 \\ 2 & 8 & 6 & 1 & 5 & 7 & 0 & 4 & 3 \\ 3 & 4 & 1 & 7 & 2 & 6 & 8 & 0 & 5 \\ 4 & 6 & 5 & 2 & 8 & 3 & 7 & 1 & 0 \\ 5 & 0 & 7 & 6 & 3 & 1 & 4 & 8 & 2 \\ 6 & 3 & 0 & 8 & 7 & 4 & 2 & 5 & 1 \\ 7 & 2 & 4 & 0 & 1 & 8 & 5 & 3 & 6 \\ 8 & 7 & 3 & 5 & 0 & 2 & 1 & 6 & 4 \end{matrix} \qquad C_2 = \begin{matrix} 0 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \\ 1 & 8 & 4 & 6 & 0 & 3 & 2 & 7 & 5 \\ 2 & 6 & 1 & 5 & 7 & 0 & 4 & 3 & 8 \\ 3 & 1 & 7 & 2 & 6 & 8 & 0 & 5 & 4 \\ 4 & 5 & 2 & 8 & 3 & 7 & 1 & 0 & 6 \\ 5 & 7 & 6 & 3 & 1 & 4 & 8 & 2 & 0 \\ 6 & 0 & 8 & 7 & 4 & 2 & 5 & 1 & 3 \\ 7 & 4 & 0 & 1 & 8 & 5 & 3 & 6 & 2 \\ 8 & 3 & 5 & 0 & 2 & 1 & 6 & 4 & 7 \end{matrix}$$

Shift(0) = 0, Shift(2)=1, ... , Shift(1)=8

Proof (sketch)



Proof (sketch)



Proof (sketch)

- By Hall's Theorem there is always a perfect matching in such a bipartite graph.
- So, we can always completely cover the cosets $C_1, C_2, \ldots, C_{p^k}$

Proof (sketch)

So, altogether we get full coverage of p^k+1 cosets, including the "freebie".

As each coset has p^{2k} permutations, the constructed PA has $p^{3k} + p^{2k}$ permutations.

So, M(p^{2k} +1, p^{2k}) $\geq p^{3k} + p^{2k}$, for all primes p and all positive integers k.

Odd powers (> 1) of primes

Similarly, we have theorems for odd powers of a prime.

Conclusions and Open Questions

We have several methods to produce better permutation arrays for Hamming distances and, hence, better lower bounds for M(n,d):

- Partition and extension
- Contraction
- Sequential partition and extension
- Searching for coset representatives
- Kronecker product and other product operations
- Using Frobenius maps to extend AGL(1,q) and PGL(2,q), and considering the semi-linear groups AΓL(1,q) and PΓL(2,q).
- Reed-Solomon codes (restricted to permutations)

What other techniques can be used?

Thank you!

(Spring break on “Starfish Island”, Honda Bay, Palawan, the Philippines)

Application to Power-line Communication (PLC)

- Example: Consider code words given by permutations

0 1 2 3 4

1 2 3 4 0

2 3 4 0 1

3 4 0 1 2

4 0 1 2 3

which is a set of permutations at Hamming distance 5.

- Let the signal sent be: f_1, f_2, f_3, f_4, f_0, corresponding to the code word 1 2 3 4 0, and suppose there is noise occurring at frequencies f_1 and f_4.

Application to Power-line Communication (PLC)

- If the signal sent is f_1, f_2, f_3, f_4, f_0, the signal received by *demodulation*, with noise at frequencies f_1, f_4 would be:

  at time t_0: $\{f_1, f_4\}$

  at time t_1: $\{f_1, f_2, f_4\}$

  at time t_2: $\{f_1, f_3, f_4\}$

  at time t_3: $\{f_1, f_4\}$

  at time t_4: $\{f_0, f_1, f_4\}$
- There are two code words consistent with the frequencies seen at time t_0, namely 1 2 3 4 0 and 4 0 1 2 3,
- There are three code words consistent with frequencies seen at time t_1, namely 0 1 2 3 4, 1 2 3 4 0, and 3 4 0 1 2.

So, in this case, the signal sent corresponds to 1 2 3 4 0.

Creating Permutation Arrays: Mutually Orthogonal Latin Squares (MOLS)

- Current lower bound table for N(k), k<60:

	0	1	2	3	4	5	6	7	8	9
0			1	2	3	4	1	6	7	8
10	2	10	5	12	4	4	15	16	5	18
20	4	5	3	22	7	24	4	26	5	28
30	4	30	31	5	4	5	8	36	4	5
40	7	40	5	42	5	6	4	46	8	48
50	6	5	5	52	5	6	7	7	5	58

- Example: Since $N(38) \geq 4$, $M(38,37) \geq 4 \times 38 = 152$.

Converting k MOLS with side n to PA's with kn permutations and Hamming Distance n-1

- A Latin square *A* can be viewed as a collection of triples in $Z_n \times Z_n \times Z_n$, namely $A = \{ (i,j,k) \mid A_{i,j} = k \}$.
- Define the permutation array A' = *S*(A) on Z_n by:

  A' = { (k,j,i) | (i,j,k) is in *A*}, which means that row k, column j, contains the symbol i (in A')
- If $A_1, A_2, \ldots, A_k$ is a set of k MOLS of size n, then the union of $S(A_1), S(A_2), \ldots, S(A_k)$ is a permutation array of $k \times n$ permutations on Z_n with Hamming distance n-1.

For P&E choose a set of ***positions*** which includes one integer from each set A_1, A_2, … , A_{p^k},

And choose a set of ***symbols*** to be **all** of the integers in set A_i, for some i.

M(n,n-2)

	0	1	2	3	4	5	6	7	8	9
0					24	60	120		336	504
10	720		1320		2184			4080	4896	
20	6840				12144		15600		19656	
30	24360	992	29760	32736					50616	
40	1640		68880		79464		2162		103776	
50	11760 0		2756		148824				3422	

Sequential Partition and Extension

Because the partition and extension operation uses a set Π_1 of roughly $n^{1/2}$ of the n-1 cosets of AGL(1,n), we can use the operation again on a set Π_2 of cosets disjoint from Π_1. We can do this several times. For sets of cosets, say extend(Π_1), extend(Π_2), … , extend(Π_k), we partition and extend again. The result is we get most of the permutations in:

$$\cup_{i\geq 1} \text{extend}(\Pi_i)$$

in a PA for M(n+2,n). This is called *sequential partition and extension*.

2^{nd} Way to Construct PA's for M(n,n-1): Mutually Orthogonal Latin Squares (MOLS)

- A *Latin square* of size n is an n×n table of symbols in Z_n with no symbol repeated in any row or column.
- Example: (of size 3)

0	1	2
2	0	1
1	2	0

- *Sudoku* is an example of completing a special Latin square of size 9

Mutually Orthogonal Latin Squares (MOLS)

- Two Latin squares A and B of size n are *orthogonal* if $\{ (a_{i,j}, b_{i,j}) \mid 0 \le i,j < n \} = Z_n \times Z_n$.

- Example: A=

0	1	2
2	0	1
1	2	0

B=

2	0	1
0	1	2
1	2	0

<u>A and B combined</u>:

0,2	1,0	2,1
2,0	0,1	1,2
1,1	2,2	0,0

Mutually Orthogonal Latin Squares (MOLS)

A set of Latin squares is called *mutually orthogonal* if each Latin square in the set is pairwise orthogonal to all other Latin squares of the set.

Mutually Orthogonal Latin Squares (MOLS)

- Let N(k) denote the largest number of MOLS of size k.
- Computing N(k) is a difficult problem of considerable interest worldwide
- MOLS have applications in experimental design and statistics
- Euler conjectured that there are no MOLS of size k, when k = 2 (mod 4). (It is true for k=2 and k=6 and false for all k>6.)

Creating Permutation Arrays: Mutually Orthogonal Latin Squares (MOLS)

- Current lower bound table for N(k), k<60:

	0	1	2	3	4	5	6	7	8	9
0			1	2	3	4	1	6	7	8
10	2	10	5	12	4	4	15	16	5	18
20	4	5	3	22	7	24	4	26	5	28
30	4	30	31	5	4	5	8	36	4	5
40	7	40	5	42	5	6	4	46	8	48
50	6	5	5	52	5	6	7	7	5	58

Example of conversion:

A =

0	1	2
2	0	1
1	2	0

B =

2	0	1
0	1	2
1	2	0

S(A) =

0	1	2
2	0	1
1	2	0

S(B) =

1	0	2
2	1	0
0	2	1

The permutation array with Hamming distance 2:

0 1 2, 2 0 1, 1 2 0, 1 0 2, 2 1 0, and 0 2 1

M(n,n-2)

	0	1	2	3	4	5	6	7	8	9
0					24	60	120		336	504
10	720		1320		2184			4080	4896	
20	6840	336			12144		15600		19656	
30	24360	992	29760	32736	899				50616	1258
40	1640		68880		79464	1722	2162		103776	
50	117600	2338	2756		148824	2461			3422	

Kronecker Product

Let A and B be blocks in some PA's on Z_n, such that hd(A,B)=n-1 and hd(A)=hd(B)=n. Then, AxA and BxB are PA's on Z_{2n} with hd=2n-1, *e.g. A*

0	1	2
2	0	1
1	2	0

,

B =

1	0	2
2	1	0
0	2	1

A × A =

0	1	2	3	4	5
2	0	1	5	3	4
1	2	0	4	5	3
3	**4**	**5**	**0**	**1**	**2**
5	3	4	2	0	1
4	5	3	1	2	0

B x B =

1	0	2	4	3	5
2	1	0	5	4	3
0	2	1	3	5	4
4	**3**	**5**	**1**	**0**	**2**
5	4	3	2	1	0
3	5	4	0	2	1

Kronecker Product

Partition and extension always works on the results of Kronecker product and covers all permutations:

A × A =

0	1	2	3	4	5
2	0	1	5	3	4
1	2	0	4	5	3
3	4	5	0	1	2
5	3	4	2	0	1
4	5	3	1	2	0

B x B =

1	0	2	4	3	5
2	1	0	5	4	3
0	2	1	3	5	4
4	3	5	1	0	2
5	4	3	2	1	0
3	5	4	0	2	1

Kronecker Product

Example:

(1) G_1 = AGL(1,7) is a group of 42 permutations and consists of 6 cosets A_1, A_2, A_3, A_4, A_5, A_6, each with 7 permutations, where hd(A_i)=7, for all i, and hd(G_1)=6.

(2) G_2 = AGL(1,5) is a group of 20 permutations and consists of 4 cosets B_1, B_2, B_3, B_4, each with 5 permutations, where hd(B_i)=5, for all i, and hd(G_2)=4.

(3) The union of A_1 X B_1, A_2 X B_2, A_3 X B_3, A_4 X B_4 is a PA K of 1420 permutations on Z_{35} with hd(K)=34

	4	5	6	7	8	9	10	11	12	13	14	15
4	4											
5	20	5										
6	120	18	6									
7	349	78	42	7								
8	2688	616	336	56	8							
9	18576	3024	1512	504	72	9						
10	150480	19490	8640	1504	720	49	10					
11	1742400	205920	95040	7920	7920	297	110	11 *				
12	20908800	2376000	190080	95040	95040	1320	1320	112	12			
13	60635520	10454400	1900800	380160	95040	6474	1320	276	156	13		
14	550368000	60445440	10834560	1900800	380160	26208	8736	2184	2184	59	14 *	
15	7925299200	98313989	58734720	15491520	1900800	181272	32760	7540	2520	315	90	15

Sharply Transitive Groups

- A <u>*group*</u> consists of a set S together with a binary operation (called multiplication), say ×, such that:

  (1) S is closed under ×,

  (2) x is *associative*,

  (3) there is an *identity* element, say e, such that, for all s in S, s × e = e × s = s.

  (4) for every s in S, there is an *inverse*, say s^{-1}, such that $s \times s^{-1} = s^{-1} \times s = e$.

Sharply Transitive Groups

- The set of all permutations on Z_n with the binary operation of *composition* (of functions) forms a group, called the symmetric group: S_n.
- A group G of permutations is *sharply k-transitive* if for any pair of k-tuples of elements in Z_n, say $v=(a_0,a_1,a_2, \ldots ,a_{k-1})$ and $w=(b_0,b_1,b_2, \ldots ,b_{k-1})$, there is a unique permutation in G that maps v to w.

Sharply Transitive Groups

- Consider the sharply 2-transitive group on Z_3, consisting of the following six permutations:

  0 1 2, 1 2 0, 2 0 1, 0 2 1, 2 1 0, 1 0 2

---

e.g. if one takes the pairs (0,1) and (2,1), the permutation 2 1 0 uniquely maps 0 to 2 and 1 to 1

Sharply Transitive Groups

- If G is a sharply 2-transitive group on Z_n, then G is a PA of n(n-1) permutations on Z_n with Hamming distance n-1.
- If G is a sharply 3-transitive group on Z_{n+1}, then G is a PA of (n+1)n(n-1) permutations on Z_{n+1} with Hamming distance n-1.
- There are sharply 2-transitive groups on Z_n iff n is a power of a prime number.
- There are sharply 3-transitive groups on Z_{n+1} iff n is a power of a prime number.

Sharply Transitive Groups

- The *sharply 2-transitive group* for $q = p^k$ is denoted as AGL(1,q) and consists of all permutations of the form $p(x) = ax+b$, with $a \neq 0$, where a,b are elements of GF(q),
- The *sharply 3-transitive group* for q+1, where $q = p^k$, is denoted as PGL(2,q) and consists of all permutations of the form $p(x) = (ax+b)/(cx+d)$, where a,b,c,d are elements of GF(q) U {∞}, with $ad \neq bc$.

Note: GF(q) is the Galois field on q elements.

Sharply Transitive Groups

- The group AGL(1,q) consists of a subgroup, namely the cyclic group C_1 ={ x+b | b in GF(q) }, and q-1 cosets of C_1, namely C_a = { ax+b | b in GF(q) }, for each a in GF(q). (For ease of notation, we call C_1 a coset, too.)
- The Hamming distance of each coset is q, but the Hamming distance between each pair of cosets is q-1.

Examples of cosets

$C_1 =$

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

$C_2 =$

0	2	4	1	3
2	4	1	3	0
4	1	3	0	2
1	3	0	2	4
3	0	2	4	1

$C_3 =$

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

$C_4 =$

0	4	3	2	1
4	3	2	1	0
3	2	1	0	4
2	1	0	4	3
1	0	4	3	2

M(n,n-1)

	0	1	2	3	4	5	6	7	8	9
0			2 1	6 2	12 3	20 4	6 1	42 6	56 7	72 8
10	20 2	110 10	60 5	156 12	56 4	60 4	240 15	272 16	140 5	342 18
20	80 4	105 5	66 3	506 22	168 7	600 24	104 4	702 26	140 5	812 28
30	120 4	930 30	992 31	165 5	136 4	175 5	288 8	1332 36	152 4	195 5
40	280 7	1640 40	210 5	1806 42	220 5	270 6	184 4	2162 46	384 8	2352 48
50	300 6	255 5	260 5	2756 52	270 5	330 6	392 7	399 7	290 5	3422 58

M(n,n-1)

	0	1	2	3	4	5	6	7	8	9
0				6 2	12 3	20 4		42 6	56 7	72 8
1 0		110 10		156 12			240 15	272 16		342 18
2 0				506 22		600 24		702 26		812 28
3 0		930 30	992 31					1332 36		
4 0		1640 40		1806 42				2162 46		2352 48
5 0				2756 52						3422 58

Contraction

- Let $\pi = a_0\ a_1\ a_2\ \ldots\ a_{n-1}$ be a permutation on Z_n, the *contraction* of π, denoted by π^{CT}, is defined by:

$$\pi^{CT}(j) = \left\{ \begin{array}{ll} \pi(j), & \text{if } j \neq n \text{ and } \pi(j) \neq n, \text{ and} \\ \pi(n), & \text{if } \pi(j) = n. \end{array} \right\}$$

Note: π^{CT} is a permutation on Z_{n-1}.

<u>Example</u>: $\pi = 3\ 0\ 4\ 1\ 2$,

$\pi^{CT} = 3\ 0\ 2\ 1$

Contraction

- If A is a PA, then $A^{CT} = \{ \pi^{CT} \mid \pi \text{ in } A \}$.
- $|A^{CT}| = |A|$
- $hd(A^{CT}) \geq hd(A)-3$
- Theorem.

  Let G = AGL(1,q), where q is a power of a prime. (We know hd(G)=q-1 and |G|=q(q-1).) If |G|is not divisible by 3, then G^{CT} is a PA on Z_{q-1} with Hamming distance = q-3.

Example: M(41,40) ≥ 1640 → M(40,38) ≥ 1640.

Contraction (Proof of Theorem)

- Consider two permutations σ and τ such that $hd(\sigma,\tau)=d$ and $hd(\sigma^{CT},\tau^{CT})=d-3$, where σ and τ are members of a group G. Since the Hamming distance decreases by 3, the contraction operation must make two new agreements:

	i	j	n	(positions)
σ:	… n	… b	… a	
τ:	… a	… n	… b	

So, the permutation $\sigma^{-1}\tau$ has the 3-cycle (n a b).

This means that the order of the group G is divisible by 3 (by *Cauchy's Theorem*)

Contraction (cont.)

- <u>Bereg's Theorem</u>. Let G = AGL(1,q), where q is a power of a prime. (We know hd(G)=q-1 and |G|=q(q-1).) If |G| *<u>is</u>* divisible by 3, then there is a subset A of G^{CT} with $(q^2-1)/2$ permutations and Hamming distance q-3.
- Example: Let G = AGL(1,79), which has 79×78 = 6162 permutations and Hamming distance 78. Then, there is a subset A of G^{CT} with 3120 permutations with Hamming distance 76, *i.e.* M(79,78) ≥ 6162 → M(78,76) ≥ 3120.

Projective General Linear Group: PGL(2,q), where q is a prime power

- PGL(2,q) is the group consisting of all permutations in:

  { (ax+b)/(cx+d) | a,b,c,d in GF(q) such that ad ≠ bc, and x is in GF(q) U { ∞ } },

  where p(x) = (ax+b)/(cx+d) is defined by:

- If x ε GF(q), then
  - If x ≠ -c/d, then p(x) = (ax+b)/(cx+d)
  - If x = -c/d, then p(x) = ∞

  If x = ∞, then
  - If c=0, then p(x) = ∞
  - If c≠0, then p(x) = a/c

Projective General Linear Group: PGL(2,q)

- PGL(2,q) is a group of (q+1)q(q-1) permutations on Z_{q+1} with Hamming distance q-1.

- Examples: $M(10,8) \geq 720$

  $M(12,10) \geq 1320$

  $M(33,31) \geq 32736$

  $M(48,46) \geq 103776$

Contraction on PGL(2,q)

- Theorem. If 3 is not a divisor of q(q-1), and G=PGL(2,q), then G^{CT} is a PA on Z_q with (q+1)q(q-1) permutations and Hamming distance q-3.
- Proof. If σ and τ are in G and hd(σ,τ) < q+1, then, for some i and a, σ(i) = τ(i) = a. It follows that $\sigma^{-1}\tau(a) = a$. That is, $\sigma^{-1}\tau$ is in the subgroup called the STABILIZER(a). It is known that the STABILIZER(a) is isomorphic to AGL(1,q).

- We have seen that, if 3 does not divide the order of AGL(1,q), then there are no 3-cycles and, hence, no pair of permutations σ and τ such that contraction reduces the Hamming distance by 3.
- So, if σ and τ are such that contraction reduces their Hamming distance by 3, they must have no agreements. That is, hd(σ,τ)=q+1.
- This means, after contraction, their Hamming distance is at least q-2.
- Other pairs of permutations, whose Hamming distance is q-1, are such that contraction reduces their Hamming distance by at most 2, hence their contractions have Hamming distance ≥ q-3.

P&E

- Example: The group AGL(1,37) consists of 36 cosets of the cyclic group C_1. Each coset has Hamming distance 37, and the Hamming distance between cosets is 36.
- We use cosets C_1, C_{36}, C_2, C_{35}, C_4, C_{33}, and C_3, and cover a total of 255 permutations. Thus, we get $M(38,37) \geq 255$.
- We use 7 of the 36 cosets.

Partition & Extension, for n=37

Coset	Set of Positions	Set of Symbols
1	0,6,12,18,24,30	0,1,2,3,4,5
36	1,7,13,19,25,31	6,7,8,9,10,11,36
2	2,9,14,21,26,33	12,16,20,24,28,32
35	3,8,15,20,27,32	13,17,21,25,29,33
4	4,10,16,22,28,34	14,18,22,26,30,34
33	5,11,17,23,29,36	15,19,23,27,31,35
5	37	37

Asymptotic Lower Bounds

- Theorem. For every prime p,

  $$M(p+1,p) \geq \tfrac{1}{2}p^{3/2} - O(p).$$

- It is known that $N(n) \geq n^{1/14.8}$ for sufficiently large n. So, by MOLS, $M(n,n-1) \geq n^{1.06}$.

For a=2, $\{p_{2,0}(x) = 0\ 2\ 4\ 6\ \ldots\ q\text{-}1\ 1\ 3\ \ldots\ q\text{-}2,$

$p_{2,2}(x) = 2\ 4\ 6\ \ldots\ q\text{-}1\ 1\ 3\ \ldots\ q\text{-}2\ 0,$

$p_{2,4}(x) = 4\ 6\ \ldots\ q\text{-}1\ 1\ 3\ \ldots\ q\text{-}2\ 0\ 2,$

…

$p_{2,q-2}(x) = q\text{-}2\ 0\ 2\ 4\ 6\ \ldots\ q\text{-}1\ 1\ 3\ \ldots\ \},$

For example, when **q is a prime** and a=1, we have:

$\{p_{1,0}(x)= 0\ 1\ 2\ 3\ 4\ \ldots\ q\text{-}2\ q\text{-}1,$

$p_{1,1}(x)= 1\ 2\ 3\ 4\ \ldots\ q\text{-}2\ q\text{-}1\ 0,$

$p_{1,2}(x)= 2\ 3\ 4\ \ldots\ q\text{-}2\ q\text{-}1\ 0\ 1,$

… ,

$p_{1,q-1}(x)=q\text{-}1\ 0\ 1\ 2\ 3\ 4\ \ldots q\text{-}2\ \},$

This forms a cyclic subgroup of AGL(1,q), denoted by C, with q permutations and with Hamming distance q, *i.e.* no agreements anywhere.

Extension

- Let A be permutation array on Z_n with Hamming distance d. A *trivial extension* yields a permutation array A’ on Z_{n+1} which has Hamming distance d.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

➔

0	1	2	3	4	5
1	2	3	4	0	5
2	3	4	0	1	5
3	4	0	1	2	5
4	0	1	2	3	5

- We want to extend to a PA A’, with Hamming distance d+1.

Illustration of P&E

Position Sets: {{0,2},{1,3,4}} / Symbol Sets:{{0,1,,2},{3,4}}

C_1=

0	1	2	3	4	5
1	2	3	4	0	5
2	3	4	0	1	5
3	4	0	1	2	5
4	0	1	2	3	5

C_2 =

0	2	4	1	3	5
2	4	1	3	0	5
4	1	3	0	2	5 ←
1	3	0	2	4	5
3	0	2	4	1	5

C_3' =

0	3	1	4	2	5
3	1	4	2	0	5
1	4	2	0	3	5
4	2	0	3	1	5
2	0	3	1	4	5

C_1' =

5	1	2	3	4	0
5	2	3	4	0	1
5	3	4	0	1	2
3	4	5	1	2	0
4	0	5	2	3	1

C_2'=

0	2	4	1	5	3
2	5	1	3	0	4
1	5	0	2	4	3
3	0	2	5	1	4

The ← indicated permutation in C_2 is not covered.

P&E (Example)

- Consider AGL(1,9), where GF(3^2) is given by:

(Using the Primitive Polynomial: $x^2 + x + 2$)

[0] $0 = 0$	[1] $x^0 = 1$	[2] $x^1 = x$
[3] $x^2=2x+1$	[4] $x^3 = 2x+2$	5] $x^4 = 2$
[6] $x^5 = 2x$	[7] $x^6 = x+2$	[8] $x^7 = x+1$