Latin Squares

Michael Bailey

April 1, 2019

Abstract

The construction for 6-HMOLS(2^q) from Stinson and Dinitz [4] is used to give some new 6-HMOLS(2^q) for higher prime powers q. The construction is then extended to give 9-HMOLS(2^{617}) and 10-HMOLS(2^{1009}).

1 Orthogonal Latin Squares and N(n)

A *latin square* of *order* n is an $n \times n$ array whose entries belong to some n-set (typically $\{1, 2, \ldots, n\}$), such that each element occurs exactly once in each row and each column.

Two latin squares of order n, L and L', on symbol sets S and S', respectively, are said to be *orthogonal* if $\{(L_{i,j}, L'_{i,j}) : i, j \in \{1, 2, \ldots, n\}\} = S \times S'$. A set of mutually orthogonal latin squres, abbreviated as MOLS, is a set of pairwise orthogonal latin squares.

$N(n)$ denotes the maximum number of latin squares in a set of MOLS of order n. It is well known that for all $n \geq 2$ that $1 \leq N(n) \leq n - 1$. In fact, the upper bound is achieved if and only if n is a prime power, and $N(n) \geq 2$ for all $n \neq 2, 6$. The following shows $N(5) = 4$.

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

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

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

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

Additionally, in 1960, Chowla, Erdős and Straus [2] showed that $N(n) \to \infty$ as $n \to \infty$, and also gave the asymptotic result of $N(n) > \frac{1}{3}n^{\frac{1}{91}}$. This was improved by Wilson [6] in 1974 to $N(n) > n^{\frac{1}{17}}$, and due to Beth [1], was further improved to $N(n) > n^{\frac{1}{14.8}}$, which is the currently the strongest lower bound known.

2 Holey Latin Squares

A *holey* or *incomplete latin square* $HLS(n; h_1, h_2, \ldots, h_k)$ is an $n \times n$ array L along with sets $H_i \subseteq S$ (hole sets), for $1 \leq i \leq k$ where $|H_i| = h_i$ and $H_i \cap H_j = \emptyset$ for $1 \leq i < j \leq k$, with the following properties:

1) each cell of L is empty or contains an element of S
2) the subarrays indexed by $H_i \cap H_j$ are empty (*holes*)
3) if $x \epsilon H_i$ then the elements in row and column x are exactly those of $S \setminus H_i$.

L is said to have type $h_1^{n_1} h_2^{n_2} ... h_l^{n_l}$ if there are exactly n_i holes of size h_i. Typically, an incomplete latin square refers to a latin square with only one hole set, whereas when the term holey latin square is used, it is implied that the hole sets partition S.

If L and L' are both holey latin squares of order n containing the same hole sets, then they are orthogonal if $\{(L_{i,j}, L'_{i,j}) : i, j \in \{1, 2, \ldots, n\}\} = (S \times S') \setminus \cup_{i=1}^{k} (H_i \times H_i)$. The term k-HMOLS($h_1^{n_1} h_2^{n_2} \ldots h_l^{n_l}$) refers to a set of k holey mutually orthogonal latin squares which have type $h_1^{n_1} h_2^{n_2} \ldots h_l^{n_l}$. In this paper we are concerned with the case when the holes partition the symbol set, and they all have the same size, that is, sets of HMOLS with type h^n. $N(h^n)$ denotes the maximum number of holey latin squares with type h^n in a set of HMOLS (of order hn). The following is an example of 2-HMOLS(1^4).

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

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

Similar to $N(n)$, it is known that $N(h^n) \leq n - 2$ for all h, and in 1987 Stinson and Zhu [5] proved that, for any $h \geq 2$, $N(h^n) \geq 2$ if and only if $n \geq 4$. However, unlike $N(n)$, there is no known asymptotic growth rate for $N(h^n)$. Showing this is the end goal.

3 6-HMOLS(2^q)

We start by simply using the construction from Stinson and Dinitz [4, Section 4], which uses the method of differences [4, Lemma 2.1], and the order 8 boolean Hadamard matrix to construct 6-HMOLS(2^q).

Take $q \equiv 1 \pmod 4$ a prime power, and let ω be a primitive element of $\mathbb{F}_q$. Define $C_0 = \{\omega^0, \omega^4, \omega^8, \ldots, \omega^{(q-1)-4}\}$, a multiplicative subgroup, and define its cosets as $C_i = \omega^i C_0$, $1 \leq i \leq 3$. Let

$$V = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

and let v_i equal the ith row of V, $0 \leq i \leq 7$. We will use V to construct blocks defining a set of 6-HMOLS(2^q) on $\mathbb{F}_q \times \mathbb{Z}_2$. For an element $(a, b) \in \mathbb{F}_q \times \mathbb{Z}_2$, we write it as a_b. Define $x \circ y = ((x_i, y_i) : 0 \leq i \leq k)$ for length $k+1$ vectors a and b.

Build vectors $u = (u_i : 0 \leq i \leq 7)$ and $u' = (u'_i : 0 \leq i \leq 7)$ so that $B = \{xu \circ v_0,\ \omega xu \circ v_1,\ \omega^2 xu \circ v_2,\ \omega^3 xu \circ v_3,\ xu' \circ v_4,\ \omega xu' \circ v_5,\ \omega^2 xu' \circ v_6,\ \omega^3 xu' \circ v_7 : x \in C_0\}$ has distinct i, j differences, with no difference equal to 0_0 or 0_1. For each block, take the first six block coordinates to determine entries of six latin squares at a (latin square) coordinate determined by the final two block coordinates (i.e one block fills the same coordinate in all six squares).

To build u and u', we find restrictions on which cosets the quotient $(u_j - u_i)/(u'_j - u'_i)$ can land in, for each $0 \leq i < j \leq 7$. For example, when $j = 2$ and $i = 0$, we require that all of $x(u_2 - u_0)_0$, $x\omega(u_2 - u_0)_1$, $x\omega^2(u_2 - u_0)_0$, $x\omega^3(u_2 - u_0)_1$, $x(u'_2 - u'_0)_1$, $x\omega(u'_2 - u'_0)_0$, $x\omega^2(u'_2 - u'_0)_1$, $x\omega^3(u'_2 - u'_0)_0$ be distinct. This gives the requirement that $(u_2 - u_0)/(u'_2 - u'_0) \in C_0, C_2$. We repeat this for each i, j pair, and build a table of "allowed cosets" for $(u_j - u_i)/(u'_j - u'_i)$.

$i \backslash j$	1	2	3	4	5	6	7
0	0	0, 2	0	2	1, 3	2	0, 1, 2, 3
1		2	1, 3	0, 1, 2, 3	0	0, 2	2
2			2	0	0, 1, 2, 3	0	1, 3
3				0, 2	0	0, 1, 2, 3	2
4					2	1, 3	0
5						2	0, 2
6							0

Table 1: Allowed Cosets for Order 8 Hadamard Matrix

In order to actually find u and u', we simply use a computer to build them together, coordinate by coordinate, testing that the built coordinates comply with the above table. Note that as we build up u and u', they define a smaller set of HMOLS, since they are built to satisfy the constraints of the columns of the allowed table. For instance when u and u' have only four entries, they define a pair of HMOLS, since the i, j block differences are distinct for $0 \leq i < j \leq 3$. The following are some new sets of 6-HMOLS not covered by Stinson and Dinitz.

q	u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7
81	ω^0	ω^{33}	ω^{14}	ω^{74}	ω^{57}	ω^{78}	ω^{23}	0
101	1	87	86	31	24	64	58	0
109	1	3	10	103	23	42	101	0
113	1	52	53	6	86	101	3	0
121	ω^0	ω^{55}	ω^{40}	ω^{116}	ω^1	ω^{74}	ω^{77}	0
125	ω^0	ω^{108}	ω^{75}	ω^{41}	ω^{114}	ω^{43}	ω^{110}	0
137	1	30	110	51	74	107	25	0
149	1	56	91	108	104	141	81	0
157	1	121	37	51	4	137	31	0
169	ω^0	ω^5	ω^{165}	ω^{69}	ω^{73}	ω^{118}	ω^{42}	0

q	u'_0	u'_1	u'_2	u'_3	u'_4	u'_5	u'_6	u'_7
81	ω^0	ω^{19}	ω^{51}	ω^{76}	ω^{73}	ω^{58}	ω^{79}	0
101	1	45	22	77	88	25	83	0
109	1	31	74	101	85	13	23	0
113	1	53	27	75	70	39	89	0
121	ω^0	ω^5	ω^{89}	ω^{30}	ω^{49}	ω^{116}	ω^{33}	0
125	ω^0	ω^{70}	ω^{40}	ω^{11}	ω^{110}	ω^{81}	ω^2	0
137	1	34	74	66	99	122	128	0
149	1	3	39	38	31	66	145	0
157	1	58	123	126	110	45	57	0
169	ω^0	ω^{55}	ω^{156}	ω^{39}	ω^9	ω^{56}	ω^{138}	0

4 9- and 10-HMOLS(2^q)

We can now generalize this construction to attempt to yield more than 6-HMOLS. Note that the construction completely relies on the Hadamard matrix used, as it determines what the blocks look like and so it determines what the allowed cosets are.

We take an order k boolean Hadamard matrix, which will yield $k-2$ HMOLS, and let $m = \frac{k}{2}$. Take $q \equiv 1 \pmod{m}$ a prime power, and again let ω be a primitive element of $\mathbb{F}_q$, and make the subgroup $C_0 = \{\omega^0, \omega^m, \omega^{2m}, \dots, \omega^{(q-1)-m}\}$, with cosets $C_i = \omega^i C_0$, $1 \le i \le m-1$, so there are m of them. Then as before, build vectors $u = (u_i : 0 \le i \le k-1)$ and $u' = (u'_i : 0 \le i \le k-1)$ so that $B = \{xu \circ v_0,\ \omega xu \circ v_1, \dots,\ \omega^{m-1} xu \circ v_{m-1},\ xu' \circ v_m,\ \omega xu' \circ v_{m+1}, \dots,\ \omega^{m-1} xu' \circ v_{k-1} : x \in C_0\}$ has distinct i,j differences, with no difference equal to 0_0 or 0_1. Then make a table of allowed cosets, and build u and u'.

First, we looked at the order 12 Hadamard matrix. Unfortunately, for many i,j pairs, it gives bad cosets. That is, for specific i and j, the $j-i$ differences in B can not be distinct, regardless of the choice of u and u'. However, the order 16 matrix does admit good cosets, so it is not necessarily a problem that the order 12 matrix does not work with this construction. A few more Hadamard matrices were tested to see if they admitted allowed cosets, and the order 20, 24, and 28 matrices gave bad cosets, while the order 32 matrix admitted good cosets. It seems very likely that Hadamard matrices with power of 2 orders will have some row permutation that gives good cosets.

Using the the order 16 Hadamard matrix, we found 9-HMOLS(2^{617}), with
$u = (1, 506, 250, 28, 11, 375, 294, 380, 0, 393, 155)$ and
$u' = (1, 474, 298, 318, 112, 480, 139, 108, 0, 343, 127)$,
and 10-HMOLS(2^{1009}) with $u = (1, 510, 81, 865, 744, 652, 17, 765, 0, 237, 669, 91)$ and $u' = (1, 687, 337, 10, 963, 575, 472, 593, 0, 179, 794, 68)$. Note that the choice of q here is not special, 617 was simply still small enough to do an exhaustive search, and 1009 was chosen with the hope to yield more than 9-HMOLS with a faster, random search.

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0
\end{bmatrix}$$

Table 2: Order 12 Hadamard Matrix

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{bmatrix}$$

Table 3: Order 16 Hadamard Matrix

$i\backslash j$	1	2	3	4	5	6	7	8	9	10	11
0	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$0, 3$	3	2	$\emptyset$	4
1		$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	0	$\emptyset$	2	1	$1, 4$	$\emptyset$
2			$\emptyset$	$\emptyset$	$\emptyset$	2	4	$\emptyset$	0	$\emptyset$	$2, 5$
3				$\emptyset$	$\emptyset$	4	3	$0, 3$	$\emptyset$	2	$\emptyset$
4					$\emptyset$	$\emptyset$	2	$\emptyset$	$1, 4$	1	0
5						$2, 5$	$\emptyset$	4	$\emptyset$	0	5
6							$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
7								$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
8									$\emptyset$	$\emptyset$	$\emptyset$
9										$\emptyset$	$\emptyset$
10											$\emptyset$

Table 4: Allowed Cosets for Order 12 Hadamard Matrix

$i\backslash j$	1	2	3	4	5	6	7	8
0	4	4	4	$2, 6$	$1, 3, 5, 7$	$2, 6$	4	$0, \ldots, 7$
1		$2, 6$	$1, 3, 5, 7$	4	4	4	$2, 6$	0
2			$2, 6$	4	4	4	$1, 3, 5, 7$	0
3				4	4	4	$2, 6$	0
4					$2, 6$	$1, 3, 5, 7$	4	$0, 4$
5						$2, 6$	4	$0, 2, 4, 6$
6							4	$0, 4$
7								0

$i\backslash j$	9	10	11	12	13	14	15
0	0	0	0	$0, 4$	$0, 2, 4, 6$	$0, 4$	0
1	$0, \ldots, 7$	$0, 4$	$0, 2, 4, 6$	0	0	0	$0, 4$
2	$0, 4$	$0, \ldots, 7$	$0, 4$	0	0	0	$0, 2, 4, 6$
3	$0, 2, 4, 6$	$0, 4$	$0, \ldots, 7$	0	0	0	$0, 4$
4	0	0	0	$0, \ldots, 7$	$0, 4$	$0, 2, 4, 6$	0
5	0	0	0	$0, 4$	$0, \ldots, 7$	$0, 4$	0
6	0	0	0	$0, 2, 4, 6$	$0, 4$	$0, \ldots, 7$	0
7	$0, 4$	$0, 2, 4, 6$	$0, 4$	0	0	0	$0, \ldots, 7$
8	4	4	4	$2, 6$	$1, 3, 5, 7$	$2, 6$	4
9		$2, 6$	$1, 3, 5, 7$	4	4	4	$2, 6$
10			$2, 6$	4	4	4	$1, 3, 5, 7$
11				4	4	4	$2, 6$
12					$2, 6$	$1, 3, 5, 7$	4
13						$2, 6$	4
14							4

Table 5: Allowed Cosets for Order 16 Hadamard Matrix

5 Closing Words

As previously mentioned, finding an asymptotic growth rate of $N(h^n)$ is the end goal. With our work so far we naturally start by aiming for a growth rate of $N(2^n)$. If one could show that for any k, the order 2^k Hadamard matrix can admit good cosets, they would be in a good position to find a growth rate using Wilson's theorem [7, Theorem 3] on coset selection. Wilson's theorem gives a lower bound on q such that $\mathbb{F}_q$ is guaranteed to have an r-tuple, such that its $j - i$ coordinate differences fall into prescribed cosets. Taking the prescribed cosets to simply be the entries of the coset table generated by the Hadamard matrix will give a lower bound on q such that the construction yields a full $(k-2)$-HMOLS(2^q).

References

[1] T. Beth, Eine Bemerkung zur Abschtzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, Abh Math Sem Univ Hamburg 53 (1983), 284–288

[2] S. Chowla, P. Erdos, and E.G. Straus, On the maximal number of pairwise orthogonal latin squres of a given order. *Canad. J. Math.* 12 (1960), 204–208.

[3] C.J. Colbourn and J.H. Dinitz, eds., The CRC Handbook of Combinatorial Designs,2nd edition, CRC Press, Boca Raton, 2006.

[4] J. H Dinitz, D. R Stinson, MOLS with holes. *Discrete Math.* 44 (1983), no.2 145–154

[5] D. R. Stinson and L. Zhu, On the existence of MOLS with equal-sized holes, *Aequationes Math* 33 (1987), 96–105.

[6] R. M. Wilson, Concerning the number of mutually orthogonal Latin squares, Discrete Math. 9 (1974), 181–198.

[7] R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory 4 (1) (1972) 17–47.