On permutation sum sets

Don Coppersmith
Department of Mathematical Sciences
IBM T.J. Watson Research Center
Yorktown Heights NY, USA
email: dcopper@us.ibm.com

Abraham D. Flaxman *
Department of Mathematical Sciences
Carnegie Mellon University
email: abie@cmu.edu

Clifford Smyth
Zeev Nehari Visiting Assistant Professor
Department of Mathematical Sciences
Carnegie Mellon University
email: csmyth@andrew.cmu.edu

June 6, 2005

Abstract

A permutation sum (resp. difference) set on a group G is a set $\mathcal{F}$ of bijections from G to G such that fg (resp. $f^{-1}g$) is again a bijection for all $f, g \in \mathcal{F}$ (resp. $f, g \in \mathcal{F}$ with $f \neq g \in S$), where $(fg)(x) := f(x)g(x)$ for all $x \in G$, etc. The maximum size $d(G)$ of a permutation difference set has been well studied, with many connections drawn between such sets and combinatorial objects such as families of pairwise orthogonal Latin squares. Here we primarily study its natural counterpart, $s(G)$, the maximum size of a permutation sum set.

The two quantities often differ widely. If p is a prime, we have $d(\mathbb{Z}_{p-1}) = p-1$ while $\max(p \times 2^{(p-1)/k}, \binom{p}{2}) \leq s(\mathbb{Z}_p) \leq p((p-1)/2)^{(p-3)/2}$ where k is the multiplicative order of -2 mod p. For example $d(\mathbb{Z}_{1613}) = 1612$ while $s(\mathbb{Z}_{1613}) \geq 1613 \times 2^{31} > 3 \times 10^{12}$.

1 Introduction

Let G be a (finite) group. We call a bijection from G to G, a permutation on G. We say a family $\mathcal{F}$ of functions from G to G is a permutation sum (resp. difference) set on G if and only $\mathcal{F}$ is a family of permutations and fg (resp. $f^{-1}g$) is a permutation for every $f, g \in \mathcal{F}$ (resp. $f, g \in \mathcal{F}$ with $f \neq g$). Here $(fg)(x) := f(x)g(x)$ and $g^{-1}(x) := (g(x))^{-1}$ for

*Supported in part by NSF VIGRE Grant DMS-9819950

$x \in G$. Let $s(G)$ (resp. $d(G)$) be the maximum cardinality of a permutation sum set (resp. difference set) on G if this maximum exists. See the concluding remarks section at the end of the paper for some of the connections between these parameters and families of pairwise orthogonal Latin squares on G and the orthomorphism graph of G [4]. A problem on Latin transversals of submatrices of the addition table of $\mathbb{Z}_n$ studied in [1] is somewhat related to our problem.

Some known results about $d(G)$ include: $d(G) = 1$ for $|G| \equiv 2 \pmod 4$, and $p-1 \le d(G) \le |G|-1$ where p is the smallest prime dividing $|G|$ [4].

Theorem 1. *If $|G|$ is even, then $s(G) = 0$. Suppose A is abelian and has canonical form $\mathbb{Z}_{m_1} \oplus \cdots \oplus Z_{m_t}$ where $m_1|m_2|\cdots|m_t$. If m_i is odd for $i < t$ and m_t is even then $d(A) = 1$.*

Let $\phi(n)$ be the Euler phi function, and $\exp(G)$, the exponent of the group G, the least common multiple of the orders of the elements of G.

Theorem 2. *If G is a group of odd order, then*

$$s(G) \ge \frac{\phi(\exp(G))}{2^{m(|G|)}}$$

where $m(n)$ is the number of distinct prime factors of n. If A is an abelian group of odd order then

$$s(A) \ge |A|\frac{\phi(\exp(A))}{2^{m(|A|)}}.$$

Theorem 3. *If $p \ge 3$ is a prime and k is the order of -2 in $\mathbb{Z}_p^\times$, then*

$$s(\mathbb{Z}_p) \ge p2^{(p-1)/k}.$$

As a concrete example, since the order of -2 in $\mathbb{Z}_{1613}^\times$ is 52, we have $s(1613) \ge 1613 \times 2^{31} > 3 \times 10^{12}$. Contrast this with the lower bound of $s(\mathbb{Z}_{1613}) \ge \binom{1613}{2} = 1300078$ from Theorem 2.

Let $Z(G) = \{z \in G : gz = zg, \forall g \in G\}$ be the center of G.

Theorem 4. *Let G be a group of odd order. If $H \le Z(G)$ and $F = G/H$ then*

$$s(G) \ge s(H)^{|F|}s(F).$$

Corollary 5. *If A is an abelian group of odd order and $|A|$ has prime factorization $|A| = p_1p_2\dots p_m$, then*

$$s(A) \ge \prod_{i=1}^{m} s(\mathbb{Z}_{p_i})^{p_{i+1}p_{i+2}\cdots p_m}.$$

Suppose N is a nilpotent group of odd order. Suppose N has ascending central series $1 = Z_0 \le Z_1 \le \dots \le Z_c = G$ where $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. If $|N|$ has prime factorization $|N| = p_1p_2\cdots p_m$ and we have $0 = j_0 < j_1 < \dots < j_c = m$ such that $|Z_i/Z_{i-1}| = p_{j_{i-1}+1}p_{j_{i-1}+2}\cdots p_{j_i}$, then

$$s(N) \ge \prod_{i=1}^{m} s(\mathbb{Z}_{p_i})^{p_{i+1}p_{i+2}\cdots p_m}.$$

To optimize the lower bound given by this theorem you may reorder the p_i's any way you like if G is abelian, and if G is nilpotent only the p_i's within each block $j_k < i \le j_{k+1}$.

Using linear algebraic techniques we also obtain

Theorem 6. *For all odd n, $n \ge 3$,*

$$s(\mathbb{Z}_n) \le n \left(\frac{n-1}{2}\right)^{\frac{n-3}{2}},$$

and if A is abelian of order $|A| = n$ then

$$s(A) \le n^{\frac{n-1}{2}}.$$

2 Proofs

Proof. (Theorem 1) If $|G|$ is even then by Cayley's theorem G has an element x of order 2. If f is a permutation, let $y, z \in G$ such that $f(y) = 1$ and $f(z) = x$. Then f^2 maps both y, z to 1, and hence fails to be a permutation. Thus $s(G) = 0$.

Suppose now that A is abelian of the form specified in the statement of the theorem. For $i < t$, the map $y \to -y$ on $\mathbb{Z}_{m_i}$ has no non-zero fixed point. Indeed, if $y_0 = -y_0$, $2y_0 = 0$ and thus $y_0 = \lceil m_i/2 \rceil (2y_0) = 0$. Thus $\sum_{a\in\mathbb{Z}_{m_i}} a = 0$ by pairing a with $-a$ for all $a \ne 0$. Since m_t is even $\mathbb{Z}_{m_t}$ has two fixed points under the negation map, 0 and $m_t/2$, thus $\sum_{a\in\mathbb{Z}_{m_t}} a = m_t/2 \ne 0$ has order 2 . Let $x = \sum_{a\in A} a$. We claim x is of order 2. Indeed the tth coordinate of x will be $x_t = (m_1 m_2 \cdots m_{t-1})(m_t/2) = m_t/2$ since $m_1 m_2 \cdots m_{t-1}$ is odd while the other coordinates will be 0.

Thus for any permutation f on G we have $\sum_{a\in A} f(a) = x \ne 0$ and for any two permutations f, g we have $\sum_{a\in A} (f - g)(a) = 0$. Thus $f - g$ cannot be a permutation, and $d(A) \le 1$. $\square$

Proof. (Theorem 2) For $r \in \mathbb{Z}$ we define the power map $f_r \colon G \to G$ by $f_r(x) = x^r$ for all $x \in G$. We form a permutation sum set of the form $\mathcal{F} = \{f_r : r \in R\}$ for some $R \subseteq \mathbb{Z}$. We claim that f_r is a permutation if and only if $(r, n) = 1$ [4]. Indeed if $(r, n) = 1$ then there exists r' such that $rr' \equiv 1 \pmod{n}$ and so $f_r(f_{r'}(x)) = x^{rr'} = x$ and f_r is a permutation. On the other hand, if p is a prime, such that $p|r$ and $p|n$, then by Cayley's theorem G has an element x_0 of order p, and $f_r(x_0) = 1 = f_r(1)$ and f_r fails to be a permutation. Since $\exp(G)|n$ where $n = |G|$, we need only consider $R \subseteq \{1, \ldots, n-1\}$. Note that if $\exp(G)|(r - r')$ then $x^{r-r'} = 1$ for all $x \in G$ and f_r and $f_{r'}$ are the same function on G.

Thus $\mathcal{F} = \{f_r : r \in R\}$ is a permutation sum set of size $|R|$ if and only if $R \subseteq \mathbb{Z}_n^\times$, $\exp(G) \not| (r - s)$ for all $r, s \in R$ with $r \ne s$, and $r + s \in \mathbb{Z}_n^\times$ for all $r, s \in R$. Note that $\mathbb{Z}_n \cong Z_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{e_m}}$ and $\mathbb{Z}_n^\times \cong Z_{p_1^{e_1}}^\times \times \cdots \times \mathbb{Z}_{p_m^{e_m}}^\times$ where $n = \prod p_i^{e_i}$ with $p_1 < \cdots < p_m$ primes, $e_i > 0$. In either case, the isomorphism is $r \to (r_1, \ldots, r_m)$ where $r_i = r \pmod{p_i^{e_i}}$ [5]. Let $\exp(G) = \prod p_i^{f_i}$ (note $f_i \le e_i$). For each $r = (r_1, \ldots, r_m) \in \mathbb{Z}_n$ define $0 \le k_i(r) < p_i^{e_i - 1}$ and $0 \le l_i(r) < p_i$ such that $r_i = k_i p_i + l_i$. Let $R = \{r : \forall i \quad 0 \le k_i(r) < p_i^{f_i - 1}, 1 \le l_i(r) \le (p_i - 1)/2\}$.

We claim $\mathcal{F} = \{f_r : r \in R\}$ is a permutation sum set. Indeed, $R \subseteq \mathbb{Z}_n^\times$ and $r + s \in \mathbb{Z}_n^\times$ for all $r, s \in R$. Suppose $r, s \in R$, and $\exp(G)|(r - s)$. Then $p_i^{f_i}|(r_i - s_i)$ for all i. Viewing r_i,s_i as integers we have $|r_i - s_i| < p^{f_i}$ and hence $r_i = s_i$ for all i and $r = s$. Finally, $|\mathcal{F}| = |R| = \prod_i (p_i^{f_i-1}(p_i - 1)/2)$ is the size claimed.

If A is abelian then let $f_{r,c}(x) = rx + c$ where $r \in \mathbb{Z}$ and $c \in A$. It is now easy to see that $\mathcal{F}' = \{f_{r,c} : r \in R, c \in A\}$ is a permutation sum set of the size claimed. $\square$

Proof. (Theorem 3) Let $c_0, \ldots, c_{l-1}$ be representative elements of the $l = (n - 1)/k$ multiplicative cosets of $\langle -2\rangle$ in $\mathbb{Z}_p^\times$. Consider the family $\mathcal{F} = \{f_s : s = (s_0, \ldots, s_{l-1}) \in \{0, 1\}^l\}$ where f_s is given by $f(0) = 0$, and

$$f_s(ki + j) = c_i(-2)^{j+s_i},$$

for $0 \le i \le l - 1$ and $0 \le j \le k - 1$. First we prove that f_s is a permutation. Note that for each i with $0 \le i \le l - 1$, the function $f_s^i(j) := f_s(ki + j)$ is a bijection from $\{0, \ldots, k - 1\}$ to $c_i\langle -2\rangle$. Since the cosets partition $\mathbb{Z}_p^\times$ and $f_s(0) = 0$, f_s is a bijection.

To check that $g = f_s + f_s'$ is a permutation, we will show that for each $0 \le i \le l - 1$, $g^i = f_s^i + f_{s'}^i$ is a bijection from $\{0, \ldots, k - 1\}$ to $2c_i\langle -2\rangle$. As p is odd, the cosets of $\langle -2\rangle$ are permuted by a multiplication by 2 and so g will be a bijection. There are two cases. If $s_i = s_{i'} = a$, clearly $g^i(j) = c_i(-2)^{j+a} + c_i(-2)^{j+a} = 2c_i(-2)^{j+a}$. On the other hand, if $\{s_i, s_i'\} = \{0, 1\}$, then $g^i(j) = c_i(-2)^j + c_i(-2)^{j+1} = 2c_i(-2)^{j-1}$.

Now consider the family of functions $\mathcal{F}' = \{f_{s,t} : s \in \{0, 1\}^l, t \in \mathbb{Z}_p\}$ where $f_{s,t}(x) = f_s(x)+t$. Clearly, they form a permutation sum set. Furthermore, they are all distinct. If one has the values of $f_{s,t}$ one can recover t from $f_{s,t}(0) = t$, and then the values of f_s, and from those the values of the s_i. $\square$

If $H \triangleleft G$ and $F = G/H$ then we call G an extension of H by F. We quote here some material from the theory of group extensions that we will need to use:

Theorem 7. *(Compare with Thm 2.7.6 in [7].) Suppose $H \triangleleft G$ and $F = G/H$. For all $\sigma, \tau \in F$ choose $t(\sigma)$ in the coset of H corresponding to σ (we require $t(1) = 1$), choose $c(\sigma, \tau)$ in H such that $t(\sigma)t(\tau) = t(\sigma\tau)c(\sigma, \tau)$, and define $T(\sigma)(h) = t(\sigma)^{-1}ht(\sigma)$ (note $T(\sigma) \in Aut(H)$). Then G is isomorphic to $H \times F$ with multiplication $(x, \sigma)(y, \tau) := (c(\sigma, \tau)T(\tau)(x)y, \sigma\tau)$*

As an example, consider $G = \mathbb{Z}_{100}$ with $H = \mathbb{Z}_{10}$, the "ten's digits", and $F = G/H \cong \mathbb{Z}_{10}$, the "one's digits". We have $(t, o) + (t', o') = (t + t' + c(o, o'), o + o')$ where $c(o, o') = 1$ if $o + o' \ge 10$ (as integers) and 0 otherwise. Note that Theorem 2.7.6 of [7] is more general than the result we need here and does not prove the isomorphism. However it is easily seen that the map taking $g = t(\sigma)x \in G$ (where $x \in H$) to $(x, \sigma) \in H \times F$ is an isomorphism.

Proof. (Theorem 4) Note if $H \le Z(G)$ then the automorphisms $T(\tau)$ of Theorem 7 act trivially on H. Since H is also abelian the multiplication in $H \times F$ looks like $(h, f)(h', f') = (h + h' + c(f, f'), ff')$. Let $\mathcal{A}, \mathcal{B}$ be permutation sum sets on H, F respectively. Define $\mathcal{C} := \{c_{A,b}|A : F \to \mathcal{A}, b \in \mathcal{B}\}$ where $c_{A,b} : G \to G$ is defined by $c_{A,b}(h, f) := (A_f(h), b(f))$.

We claim that $\mathcal{C}$ is a permutation sum set on C of size $|\mathcal{C}| = |\mathcal{A}|^{|F|}|\mathcal{B}|$. This suffices to prove the theorem.

We first show that each $c_{A,b}$ is an injection and hence a bijection. Suppose $c_{A,b}(h,f) = c_{A,b}(h',f')$. Then $b(f) = b(f')$ and $f = f'$ since b is a permutation. Since $A_f = A_{f'}$ is a permutation, $A_f(h) = A_{f'}(h')$ implies $h = h'$. Thus $c_{A,b}$ is an injection as claimed. Now we show that $c_{A,b} + c_{A',b'}$ is an injection. Suppose $(c_{A,b} + c_{A',b'})(h,f) = (c_{A,b} + c_{A',b'})(h',f')$. Then $(bb')(f) = (bb')(f')$ and $f = f'$ since bb' is a permutation. We also have $(A_f + A'_f)(h) + c(b(f), b'(f)) = (A_{f'} + A'_{f'})(h') + c(b(f'), b'(f'))$ or $(A_f + A'_f)(h) = (A_f + A'_f)(h')$ since $f = f'$. But this implies $h = h'$ as $A_f + A'_f$ is a permutation. It is not hard to recover A and f from the values of $c_{A,b}$ and thus the functions $c_{A,b}$ are all distinct. $\square$

Proof. (Corollary 5) Suppose A is abelian of odd order and the prime factorization of $|A|$ is $|A| = p_1 \cdots p_m$. We prove

$$s(A) \geq \prod_{i=1}^{m} s(\mathbb{Z}_{p_i})^{p_{i+1}\cdots p_m}. \tag{1}$$

by induction on m. If $m = 1$, clearly we have $s(A) = s(\mathbb{Z}_{p_1})$. Suppose $m > 1$. By Cayley's theorem there is an element x of order p_1 in A. Let $H = \langle x \rangle \cong \mathbb{Z}_{p_1}$. Since $Z(A) = A$ we apply Theorem 4 to get

$$s(A) \geq s(H)^{|A/H|} s(A/H).$$

But A/H is abelian of odd order with $|A/H| = p_2 \cdots p_m$ so by induction we have

$$s(A) \geq s(\mathbb{Z}_{p_1})^{p_2\cdots p_m} \prod_{i=2}^{m} s(\mathbb{Z}_{p_i})^{p_{i+1}\cdots p_m}$$

or (1), as desired.

Suppose N is nilpotent of odd order with ascending central series $1 = Z_0 \leq Z_1 \leq Z_c = G$ where $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. We first prove

$$s(G) \geq \prod_{i=1}^{c} s(Z_i/Z_{i-1})^{|G/Z_i|} \tag{2}$$

by induction on c. If $c = 1$ this is trivial. Suppose $c > 1$. Since $H = Z_1/Z_0 = Z(G)$ we can apply Theorem 4 to get

$$s(G) \geq s(Z_1)^{|G/Z_1|} s(G/Z_1).$$

Since G/Z_1 is nilpotent with ascending central series $1 = Z_1/Z_1 \leq Z_2/Z_1 \leq \cdots \leq Z_c/Z_1 = G/Z_1$ we apply induction and the fact that $(Z_i/Z_1)/(Z_j/Z_1) \cong Z_i/Z_j$ for $i > j$ to get

$$s(G) \geq s(Z_1)^{|G/Z_1|} \prod_{i=2}^{c} s(Z_i/Z_{i-1})^{|G/Z_i|}$$

or (2), as desired.

If each $|Z_i/Z_{i-1}|$ has prime factorization $|Z_i/Z_{i-1}| = p_{j_{i-1}+1} \cdots p_{j_i}$ then, since each Z_i/Z_{i-1} is abelian we have

$$s(Z_i/Z_{i-1}) \geq \prod_{k=j_{i-1}+1}^{j_i} s(\mathbb{Z}_{p_k})^{p_{k+1}\cdots p_{j_i}}$$

by (1). Plugging this in to (2) our earlier formula gives

$$s(N) \geq \prod_{i=1}^{m} s(\mathbb{Z}_{p_i})^{p_{i+1}\cdots p_m}.$$

$\square$

For the proof of Theorem 6 we need here some information on bilinear forms collected from [6]. Let V be a finite dimensional vector space over a field k with a symmetric bilinear form f (for each $v \in V$ the mappings $f(\cdot, v), f(v, \cdot) : V \to k$ are k-linear and $f(x, y) = f(y, x)$ for all $x, y \in V$). For $S \subset V$, $v \in V$ we write $v \perp S$ if and only if $f(v, s) = 0$ for all $s \in S$ and define $S^\perp := \{v \in S : v \perp S\}$. Note $S^\perp$ is always a subspace of V. We say f is non-degenerate or non-singular if $V^\perp = 0$. If f is non-degenerate and $W \leq V$ then $\dim W + \dim W^\perp = \dim V$ [6]. Following [2],[3] we call W isotropic if and only if $W \leq W^\perp$. In this case we have $\dim W \leq \lfloor \dim(V)/2 \rfloor$.

Proof. (Theorem 6) We use linear algebraic methods. Suppose $\mathcal{F} = \{f_1, \ldots, f_m\}$ is a permutation sum set on $\mathbb{Z}_n$. For $1 \leq q \leq m$ define the vector $v_q = (v_q(k)) \in \mathbb{C}^n$ by

$$v_q(k) := e^{2\pi i f_q(k)/n}, 0 \leq k \leq n-1,$$

where we identify the elements of $\mathbb{Z}_n$ and $\{0, \ldots, n-1\}$ in the obvious way. Let $W \subseteq \mathbb{C}^n$ be the subspace spanned by $\{v_1, \ldots, v_m\}$. We define a symmetric bilinear form on $V = \mathbb{C}^n$ by $f(v, w) = \sum_{k=0}^{n-1} v_k w_k$. Note that if $v \neq 0$ then $f(v, v^*) = \sum_k v_k \overline{v_k} = ||v||_2^2 > 0$ and so f is non-degenerate. W is isotropic. Indeed, for all $1 \leq q, r \leq m$, we have

$$f(v_q, v_r) = \sum_{k=0}^{n-1} e^{2\pi i (f_q(k) + f_r(k))/n} = 0,$$

since $f_q + f_r$ is a permutation. So $\dim W \leq \lfloor n/2 \rfloor = \frac{n-1}{2}$, since n is odd.

Let $m = \dim W$, and let $w_1, \ldots, w_m$ be a basis for W. Consider the matrix M whose columns are the w_i's. M has rank m, so let $I = \{i_1, \ldots, i_m\}$ be an index set of m independent rows of W. Then for any $v' = (v'(1), \ldots, v'(m)) \in \mathbb{C}^m$, there is a unique vector $v \in V$ so that $v(i_k) = v'(k)$ for $k \in \{1, \ldots, m\}$. In particular each permutation in $\mathcal{F}$ is determined by its value on a certain fixed set of m coordinates. There are at most $n((n-1)/2)^{m-1}$ such possible restrictions of permutations from $\mathcal{F}$. The first coordinate c can be chosen freely. The second coordinate cannot be c nor for any d can there be two restrictions $(c, d, \ldots)$ and $(c, 2c-d, \ldots)$. These restrictions would sum to $(2c, 2c, \ldots)$ which would not extend to a permutation, a contradiction. Thus there are at most $(n-1)/2$ choices for the second through mth coordinates of the restriction. Thus $|\mathcal{F}| \leq n((n-1)/2)^{(n-3)/2}$ as claimed.

We may assume $A = \bigoplus_{k=1}^{t} \mathbb{Z}_{m_k}$ (in not necessarily canonical form). Thus $n = |A| = m_1 m2 \cdots m_k$. Let $A = \{a_1, \dots, a_n\}$ and for $a \in A$, $1 \leq k \leq t$, let $c(a, k)$ be the coordinate of a in $\mathbb{Z}_{m_k}$. Suppose $\mathcal{F}$ is a permutation sum set on A. For each permutation f in $\mathcal{F}$ create the vector $v(f) \in \mathbb{C}^{nt}$

$$v(f)_{j,k} = \exp(2\pi i c(f(a_j)), k)$$

for $1 \leq j \leq n, 1 \leq k \leq t$.

For each $1 \leq k \leq t$ let $V_k = \{(v(f)_{j,k})_{j=1}^{n} : f \in \mathcal{F}\}$ and let W_k the subspace of $\mathbb{C}^n$ spanned by V_k. Since F is a permutation sum set, W_k is isotropic and hence there is a set of at most $(n-1)/2$ coordinates that determine its vectors. Thus there are at most $m_k^{(n-1)/2}$ vectors in V_k. Distinct f are not mapped to distinct vectors $(v(f)_{j,k})_{j=1}^{n}$ in V_k, however they are mapped distinct vectors $v(f)$ in $V = \{v(f) : f \in \mathcal{F}\}$. We have $|\mathcal{F}| \leq |V| \leq m_1^{(n-1)/2} m_2^{(n-1)/2} \cdots m_t^{(n-1)/2} = n^{(n-1)/2}$. □

3 Concluding Remarks

Although we believe the parameters $s(G)$ and $d(G)$ to be of considerable interest in themselves, there is much previous work on $d(G)$ especially in the connections between permutation difference sets to other combinatorial objects [4].

There is a connection between $d(G)$ and families of orthogonal Latin squares over G. Recall that a Latin square over a set of symbols S is an $|S| \times |S|$ matrix L over S such that each row and each column of L form a permutation of S. Two such Latin squares L, L' are orthogonal if the map $f(s, s') = (L_{ss'}, L'_{ss'})$ is a bijection on $S \times S$. If S is a set, let $\mathcal{L} = \mathcal{L}(S)$ be the graph whose vertices are the Latin squares on S and where two squares are adjacent if and only if they are orthogonal. Let $L(n)$ be the maximum size of a set of pairwise orthogonal Latin squares on a set of size n. If G is of order n we have $L(n) = \omega(\mathcal{L}(G))$, where $\omega(\mathcal{H})$ is the size of the largest clique in the graph $\mathcal{H}$. Given permutations f, g on G, the matrix L_f defined by $L_f(x, x') = xf(x')$ for $x, x' \in G$, is a Latin square on G. Also L_f and L_g are orthogonal if and only if $f^{-1}g$ is a permutation [4]. Let $\mathcal{S} = \mathcal{S}(G)$ be the graph whose vertices are the permutations on G and where permutations f, g are adjacent if and only if $f^{-1}g$ is a permutation. Then $d(G) = \omega(\mathcal{S}(G))$. Thus a permutation difference set $\mathcal{F}$ is a clique of $\mathcal{S}$ which in turn corresponds to a clique $\{L_f : f \in \mathcal{F}\}$ in $\mathcal{L}$. Thus we have $L(n) = \omega(\mathcal{L}) \geq \omega(\mathcal{S}) = d(G)$. Other results in this vein are $L(n) \leq n - 1$, $d(G) \leq |G| - 1$, $d(G) = 1$ if $|G| \equiv 2 \pmod 4$, etc. [4].

The neighbors in $\mathcal{S}$ of the identity permutation e (that is, $e(x) = x$ for all x in G) are called orthomorphisms of G and the restriction of $\mathcal{S}$ to the orthomorphisms is called the orthomorphism graph $\mathcal{O} = \mathcal{O}(G)$ of G [4]. A family $\{L_f : f \in \mathcal{F}\}$ of pairwise orthogonal Latin squares may be transformed by simultaneous column permutations until it contains L_e. So when looking for a family of this form, we may as well restrict our attention to $\mathcal{O}$. Every clique $\mathcal{F}'$ in $\mathcal{O}$ corresponds to a clique $\mathcal{F} = \mathcal{F}' \cup \{e\}$ in $\mathcal{S}$ and so $d(G) = \omega(\mathcal{S}) = \omega(\mathcal{O}) + 1$. Orthomorphisms are also of interest in the construction of nets, transversal designs, affine and projective planes, difference matrices, and generalized Hadamard matrices [4].

Our results on $s(G)$ say something further about the structure of $\mathcal{L}$ and $\mathcal{S}$. What is $bc(\mathcal{L})$, the maximum k such that the biclique $K_{k,k}$ is contained in $\mathcal{L}$? If $\mathcal{F}$ is a permutation sum set on G, every member of $X = \{L_{f^{-1}} : f \in \mathcal{F}\}$ is orthogonal with every member of $Y = \{L_g : g \in \mathcal{F}\}$, so we have $bc(\mathcal{L}) \geq bc(\mathcal{S}) \geq s(G)$. Contrast this with the rather smaller $\omega(\mathcal{S}) \leq \omega(\mathcal{L}) \leq |G| - 1$.

References

[1] N. Alon, Additive latin transversals, *Israel J. Math.* 117 (2000), 125-130.

[2] E. Artin, *Geometric Algebra*, (Interscience Publishers, New York, 1957)

[3] L. Babai and P. Frankl, *Linear Algebraic Methods in Combinatorics (Preliminary Version 2)* (1992)

[4] A. B. Edwards, *Orthomorphism graphs of groups*, Springer, New York (1992).

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, 2nd edition (corrected)*, (Springer, New York, 1990)

[6] S.Lang, *Algebra, 3rd ed.*, (Addison Wesley, New York, 1993)

[7] M. Suzuki, *Group Theory I*, (Springer, New York, 1982)