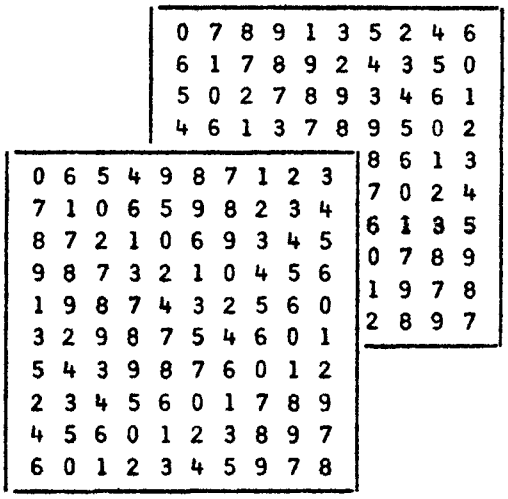
This research was done while the author was visiting the Department of Statistics, University of North Carolina at Chapel Hill, in May, 1970, and was partially supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and by the U. S. Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.



C O M B I N A T O R I A L
M A T H E M A T I C S
Y E A R

February 1969 - June 1970

ANTISYMMETRIC HADAMARD DIFFERENCE SETS

by

Paul Camion

University of Toulouse
Toulouse, FRance

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 600.30

June, 1970

ANTISYMMETRIC HADAMARD DIFFERENCE SETS

Paul Camion
University of Toulouse
Toulouse, France

1. INTRODUCTION.

In [1], we have studied binary relations (X, U) complete and antisymmetric, that is

$$\forall \quad i,j \in X: \quad (i,j) \in U \iff (j,i) \notin U$$

for which there exist a group of automorphisms verifying

1. For every pair of arcs, (i,j), $(i',j') \in U$, there exist a $g \in G$ with $(i)g = i$, $(j)g = j'$.
2. The identity alone fixes two points.
3. Let A be the set of elements of G moving all the points, there exists an $a \in A$ and two points i and j such that a is the unique element of A with $(i)a = j$.

We proved the following theorem.

The group of automorphisms of (X, U) verifies 1, 2, 3 iff X is the set of elements of a near-field K where there exists a subset $P \subset K$ verifying

---

This research was done while the author was visiting the Department of Statistics, University of North Carolina at Chapel Hill, in May, 1970, and was partially supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and by the U.S. Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.

$$P \cdot P \subset P$$

$$P \cap (-P) = \{0\} \quad \text{and} \quad P \cup (-P) = K,$$

and where $\forall\ m \in P\backslash\{0,1\}$, the mapping defined by $x \mapsto x-xm$ is an automorphism of the additive group K, and U is the set of couples (α,β) with $\beta-\alpha \in P$. Moreover, in the case where X is finite, condition 3 may be dropped, the near-field has an order congruent to 3 *mod* 4 and P is the set of its squares.

In the finite case, such a group of automorphisms may be defined as a sharply two homogeneous group(*), and a short proof of that special case may be found in [2], where the theorem of Feit and Thompson is used.

We consider here a generalization of the finite case. That is, the graph (X,U) has an abelian group of automorphism G, with the elements of which its vertices are labeled and the set

$$\{(0,x) \mid (0,x) \in U\}$$

is a difference set.

That condition is necessarily fulfilled when 1 and 2 are verified but the question of knowing if it is sufficient has not been cleared out in this paper except when G is cyclic.

However, we prove that G is a p-group, and our argument leads to a proof of the fact that condition 1 added to the difference set condition implies G is elementary abelian. The case where G is cyclic is thoroughly cleared out.

(*) We are indebted to Professor Michel Jean of the College Royal de Quebec who brought that fact to our attention.

2. Antisymmetric Hadamard Difference Sets.

2.1. Definition.

Let G be an abelian group and D be a *difference set* [3], that is a subset of G such that the integer

$$\lambda_a = |\{(x,y)|x,y \in D,\ x-y = a\}| \tag{1}$$

does not depend on $a \in G\backslash\{0\}$.

The common value of the λ_a is denoted λ and D is a *Hadamard difference set* whenever $k = (v-1)/2$, where $k \equiv |D|$ and $v \equiv |G|$

Now D will be called *antisymmetric* if

$$\forall\ x \in G\backslash\{0\},\ x \in D \Rightarrow -x \notin D. \tag{2}$$

A difference set D verifying all those conditions will be referred to as a A.H.D.S.

2.2. Statement of the result.

Theorem 2.1. *An abelian group which contains an antisymmetric Hadamard difference set is a p-group with order congruent to three modulo four. When it is cyclic, the difference set is the set of the quadratic residues or the set of the quadratic non-residues of a prime.*

2.3. General properties of A.H.D.S.

2.3.1. Properties of v, k and λ.

$|D| = (v-1)/2$ and as the mapping $x \mapsto -x$ of G into itself is injective, $|-D| = (v-1)/2$.

But by (2)

$$-D \cap D = \emptyset \tag{3}$$

and since $-D \cup D \subset G \setminus \{0\}$, $|-D \cup D| = v-1$ implies

$$-D \cup D = G \setminus \{0\}. \tag{4}$$

On the other hand, the identity

$$k(k-1) = \lambda(v-1) \tag{5}$$

is verified for any difference set which implies in the present case

$$\lambda = (k-1)/2 = (v-3)/4. \tag{6}$$

Hence the order of G is congruent to 3 *mod* 4.

2.3.2. Properties of the incidence matrix of a A.H. configuration.

Let A be the incidence matrix of G versus the subsets $\{y\}+D$, $y \in G$, that is $A = (a_{x,y})$, $a_{x,y} = 1 \iff x \in y+D$. (3) and (4) are equivalent to

$$A + A^T + I = J, \tag{7}$$

and since D is a difference set,

$$AA^T = nI + \lambda J, \tag{8}$$

where, as usually, $n = k-\lambda$.

We now have

PROPERTY 2.1. *Let A be a v by v matrix with entries 0 and 1. The following conditions are pairwise equivalent.*

I. $AA^T = nI + \lambda J$

II. $A + A^T + I = J$

III. $A^2 + A = n(J-I)$.

I implies

$$JA = kJ, \tag{9}$$

and

$$A^{-1} = \frac{1}{n}(A^{T} - \frac{\lambda}{k}J). \tag{10}$$

III follows immediately from I and II and II follows from I, III, (9) and (10), hence

$$(I \ \& \ II) \iff (I \ \& \ III). \tag{11}$$

On the other hand, I follows from II and III by simple calculation.

PROPERTY 2.2. *For any difference set D, condition III on its incidence matrix is equivalent to*

$$\begin{cases} \forall\ z\in D, \ |\{x|x\in D,\ z-x\in D\}| = n-1. \\ \forall\ z\notin D, \ z\neq 0 |\{x|x\in D,\ z-x\in D\}| = n \\ -D\cap D = \emptyset. \end{cases} \tag{12}$$

Actually if $A = (a_{x,y})$ and $A^2 = (b_{x,y})$, III is equivalent to

$$\forall\ z\in G: \ \sum_{x\in G} a_{z,x}a_{x,0} + a_{z,0} = n(1-\delta_{z,0}) = b_{z,0}. \tag{13}$$

COROLLARY 2.1. *Condition (12) implies, for any difference set D, $-D\cup D = G\setminus\{0\}$.*

Remark. If D verifies conditions (12) it is a A.H.D.S. and $n-1 = k-\lambda-1 = \lambda$. Also $k-1-(n-1) = \lambda$ and

$$\forall\ z\in D, \ |\{x|x\in D,\ z-x\notin D\}| = \lambda. \tag{14}$$

2.3.3. Equations in the convolution algebra $\mathbb{Z}G$ of the abelian group G over the ring $\mathbb{Z}$ of integers.

The matrix $A = (a_{x,y})$ is a sum of permutation matrices, i.e.

$$(15) \qquad a_{x,y} = \sum_{g\in D} \delta_{x-g,y},$$

and the transpose $A^T = (a^T_{y,x})$ is given by

$$(16) \qquad a^T_{y,x} = \sum_{g\in D} \delta_{y,x-g} = \sum_{g\in D} \delta_{y+g,x} = \sum_{g\in -D} \delta_{y-g,x}.$$

Consequently, conditions I, II, III may be considered as identities in the $\mathbb{Z}$-algebra generated by the set $\{(\delta_{x-g,y})\}_{g\in G}$.

Now let us represent as in [3] by a polynomial

$$(17) \qquad \sum_{g\in G} a_g X^g$$

an element of $\mathbb{Z}G$.

In the canonical basis $\{X^g\}_{g\in G}$ of the $\mathbb{Z}$-module $\mathbb{Z}G$, the matrix of the linear mapping $S_{g'}: \sum_{g\in G} a_g X^g \mapsto \sum_{g\in G} a_g X^{g+g'}$ corresponding to the multiplication by $X^{g'}$ is precisely

$$(18) \qquad (\delta_{x-g',y}).$$

We thus have the isomorphisms

$$(19) \qquad \mathbb{Z}G \approx \mathbb{Z}[\{S_g\}_{g\in G}] \approx \mathbb{Z}[\{\delta_{x-g,y}\}].$$

Now let us use the following notations.

$$(20) \qquad D(X) = \sum_{g\in D} X^g, \quad D(X^{-1}) = \sum_{g\in -D} X^g, \quad T(X) = \sum_{g\in G} X^g.$$

Then the conditions I, II, III become by (19)

I'. $D(X)D(X^{-1}) = n + \lambda T(X)$

II'. $D(X) + D(X^{-1}) + 1 = T(X)$

III'. $D^2(X) + D(X) = n(T(X)-1)$.

Here X^0 is denoted by 1, and as usual, $n = k-\lambda$.

2.4. Proof of the main lemma leading to Theorem 2.1.

The group G may be considered as a module over $\mathbb{Z}$ so that we shall use multiplication of elements of G by integers.

LEMMA 2.4. *If $D \subset G$ is a A.H.D.S., then for every integer t with $(t,v) = 1$*

$$tD = \left(\frac{t}{v}\right)D,$$

where $(-)$ is the Jacobi symbol [4]

By the quadratic reciprocity law, since $v \equiv 3 \bmod 4$, one has for $q \neq 2$, q a prime

$$\left(\frac{v}{q}\right)\left(\frac{q}{v}\right) = (-1)^{\frac{q-1}{2}}, \tag{22}$$

hence

$$\left(\frac{q}{v}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{v}{q}\right) \tag{23}$$

and if $q = 2$,

$$\left(\frac{2}{v}\right) = (-1)^{\frac{v^2-1}{8}}. \tag{24}$$

From (23), (24) and from the property

(25) $\left(\frac{t}{v}\right) = \prod_i \left(\frac{t_i}{v}\right)$, where $\prod_i t_i = t$, t_i a prime, $\forall$ i,

all we have to prove is

(26) $qD = (-1)^{\frac{q-1}{2}} \left(\frac{v}{q}\right) D$,

for q odd, and for q = 2

(27) $qD = (-1)^{\frac{v^2-1}{8}} D$.

For every prime q, we shall consider the group G* of characters of G into the group $[a] = F^*_{q^\nu}$, where F_{q^ν} is the splitting field of X^e-1 over F_q, e being the exponent of G. (i.e., ν is the smallest integer such that $q^\nu-1 \equiv 0$ *mod* e.)

We shall consider, as in [5], the isomorphism μ^{-1} of F_qG onto $F_{q^\nu}^{G^*}$. For brevity, we write D_χ for the image of D(X) under the character $\chi \in G^*$.

For every non principal character χ, one has

(28) $D_\chi^2 + D_\chi + n = 0, \quad \chi \in G^* \setminus \{0\}$.

So, for every non principal character χ, D_χ is one of the two roots of the first member of (28).

Let us first suppose that the polynomial Y^2+Y+n, (n is taken *mod* 9) does split over F_q, that is

(29) $1 - 4(\lambda+1) = -v$

is a quadratic residue *mod* 9, or in other words

(30) $(-1)^{\frac{q-1}{2}} \left(\frac{v}{q}\right) = 1$,

if q is odd, and if $q = 2$

(31) $\quad n = \lambda + 1 \equiv 0 \ mod\ 2, \quad or \quad v \equiv -1 \ mod\ 8.$

In that case, since $D_{\chi_0} = k \epsilon F_q$, every character sends $D(X)$ in F_q and we know that this is possible if and only if (see for example [5] for a proof)

(32) $\quad D(X) = D(X^q),$

since μ^{-1} is an isomorphism, which means that

(33) $\quad qD = D.$

Now, on the contrary, if for $q \neq 2$, $(-1)^{(q-1/2)}(\frac{v}{q}) = -1$, and, for $q = 2$, when $(-1)^{(v^2-1/8)} = 1$, Y^2+Y+n is irreducible over F_q.

In that case, Y^2+Y+n divides $X^{q^\nu-1}-1$, ν is even, and the Galois group of F_{q^ν} over F_{q^2} is given by all the even powers of q modulo $q^\nu-1$; every odd power of q defines an F_q automorphism of F_{q^ν} which permutes the roots of $Y^2+Y+n = (Y-b)(Y-c)$, and, in particular,

(34) $\quad b^q = c.$

But since $b+c = -1$, one has for every non principal character χ,

(35) $\quad D_\chi^q = -1 - D_\chi$

or, by II',

(36) $\quad D_\chi^q = (-D)_\chi.$

But also $D_{\chi_0} = (-D)_{\chi_0}$ for the principal character χ_0, hence, since the Fourier transform μ^{-1} is an isomorphism onto $F_{q^\nu}^{G^*}$,

(37) $\quad D(X^q) = D(X^{-1})$ C.Q.F.D.

2.5. Consequences of Lemma 2.4. for the group G.

PROPERTY 2.5.1. *If G' is a subset of G, symmetric with respect to the origin, one has for D' = D∩G'*

$$\begin{aligned} -D' \cup D' &= G'\backslash\{0\} \\ -D' \cap D' &= \emptyset. \end{aligned} \tag{38}$$

$$\begin{aligned} -D' \cup D' &= -(D\cap G') \cup (D\cap G') = (-D\cap G') \cup (D\cap G') \\ &= (-D\cup D) \cap G' = G'\backslash\{0\}. \\ -D' \cap D' &= (-D\cap G') \cap (D\cap G') = -D \cap D \cap G' = \emptyset. \end{aligned}$$

COROLLARY 2.5.1. *In the hypothesis of Lemma 2.4., v cannot have any prime factor congruent to one modulo four.*

We shall show that if v has a factor r congruent to one modulo four, there exists a non trivial subgroup G' of G such that D∩G' is empty, which is impossible for a A.H.D.S. D.

We split G into the canonical direct sum

$$G = G_1 \oplus \ldots \oplus G_\delta \tag{39}$$

where the order of G_1 is the exponent e of G. So r divides e, and a subgroup G" of G isomorphic with G_1 contains a subgroup G' of order r. Now, if (t,v) = 1, tG" = G" and

$$tG' = G'. \tag{40}$$

We write $v = v_1 r^c$, $(v_1, r) = 1$, and we choose, as it is possible, an integer t verifying

$$t \equiv 1 \ mod\ v_1, \quad t \equiv -1 \ mod\ r, \quad \text{and} \quad (t,v) = 1. \tag{41}$$

Now, let $D' = D \cap G'$. We have

$$tD' = -D', \tag{42}$$

by (41).

But also

$$tD' = t(D \cap G') = tD \cap G' \tag{43}$$

and by Lemma 2.4,

$$tD' = \left(\frac{t}{v}\right)D \cap G' = \left(\frac{t}{v}\right)(D \cap G') = \left(\frac{t}{v}\right)D'. \tag{44}$$

Now, let us compute $\left(\frac{t}{v}\right)$.

Since $t \equiv 1 \ mod \ v_1$, $\left(\frac{t}{v_1}\right) = 1$, and

$$\left(\frac{t}{v}\right) = \left(\frac{t}{v_1}\right)\left(\frac{t}{r^e}\right) = \left(\frac{t}{r^e}\right) = \left(\frac{t}{r}\right)^e = 1, \tag{45}$$

since -1 is a quadratic residue modulo r. But (42), (44) and (45) imply

$$-D' = D', \tag{46}$$

which is impossible by (38).

COROLLARY 2.5.2. *If G contains a A.H.D.S. D, let $p \equiv 3 \ mod \ 4$ be a prime factor of v and $q > v$ a prime number. Then*

$$\left(\frac{v}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}. \tag{42}$$

By (26), we have to prove that

$$\left(\frac{q}{p}\right)D = qD. \tag{48}$$

As in the lines following (39), we may find a subgroup G' of order p, contained in a cyclic subgroup G'' of order e, direct factor of G. Then

$$(49) \qquad qD' = q(D \cap G') = qD \cap G'.$$

Now, suppose (48) is not true.

Case 1: $(\frac{q}{p}) = 1$.

Then

$$(50) \qquad qD' = -D \cap G' = -(D \cap G') = -D'.$$

But q is a quadratic residue modulo p, $p \equiv 3 \ mod\ 4$, by assumption, and (50) implies that it generates in $\mathbb{Z}/(p)$ of multiplicative group of even order. This is impossible.

Case 2: $(\frac{q}{p}) = -1$.

Then

$$(51) \qquad qD' = D \cap G' = D'.$$

But this is impossible, since

$$(52) \qquad (\frac{q}{p}) = -1 \iff q^{\frac{p-1}{2}} \equiv -1 \ mod\ p$$

and the last identity means that

$$(53) \qquad q^{\frac{p-1}{2}} D' = -D'.$$

COROLLARY 2.5.3. *If G contains a A.H.D.S. D, v cannot contain two distinct prime factors congruent to three modulo four.*

Let $p \equiv r \equiv 3 \quad 4$ and pr/v. By Corollary 2, one has for every prime $q > v$,

$$(54) \qquad \left(\frac{q}{p}\right) = \left(\frac{q}{r}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{v}{q}\right).$$

Now, by the quadratic reciprocity law,

$$(55) \qquad 1 = \left(\frac{q}{p}\right)\left(\frac{q}{r}\right) = \left(\frac{p}{q}\right)\left(\frac{r}{q}\right) = \left(\frac{pr}{q}\right).$$

Hence pr is a quadratic residue modulo q, for every prime q greater than v. This implies that pr is a square. (A proof of that fact may be found in [4].)

2.6. Proof of Theorem 2.1.

2.6.1. General discussion.

Let $G = G_1 \oplus \ldots \oplus G_r$ where G_i has order $\ell_i \geq 1$.

Let L Be the subgroup of order p^r of G whose elements are of the type

$$(56) \qquad g = (g_1, \ldots, g_r), \quad g_i = 0 \text{ or } g_i = \alpha p^{\ell-1}, \quad 1 \leq \alpha \leq p-1.$$

Then the quotient group G/L has order $p^{\Sigma \ell_i - r}$. We may write an element of G

$$(57) \qquad \left(\sum_{1 \leq j \leq \ell_i} s_j^i \, p^{\ell_i - j} \right)_{1 \leq i \leq r},$$

so that a class in G/L is a set

$$(58) \qquad C_s = \left\{ \left(\alpha_i p^{\ell_i - 1} + \sum_{2 \leq j \leq \ell_i} s_j^i \, p^{\ell_i - j} \right)_{1 \leq i \leq r} \right\}_{\alpha_i \in F_p}$$

$$= \left\{ \left(\alpha_i p^{\ell_i - 1} + s_i \right)_{1 \leq i \leq r} \right\}_{\alpha_i \in F_p}.$$

Now, a set $B_s = C_s \cup C_{-s}$ is symmetric with respect to the origin and by Property 2.5.1, $|D \cap B_s| = |B_s|/2 = p^r$ for $s \neq 0$. Let

$$(59) \qquad |D \cap C_s| = p^r - x_s, \quad |D \cap C_{-s}| = x_s.$$

For counting the number of differences giving elements of $C_0 \setminus \{0\}$, we may count all the differences in the sets B_s and in C_0 and subtract

$$(60) \qquad 2 \cdot \sum_{1 \le s \le p^{\ell-r}} (p^r - x_s)\, x_s,$$

with $\sum_i \ell_i = \ell$.

We obtain

$$(61) \qquad p^r(p^r-1)\,\frac{p^{\ell-r}-1}{2} + \frac{p^r-1}{2}\,\frac{p^r-3}{2} - 2 \sum_{1 \le s \le p^{\ell-r}} (p^r - x_s)\, x_s$$

and this must equal

$$(62) \qquad (p^r-1)\lambda = \frac{(p^r-1)(p^\ell-3)}{4}.$$

The sum of the first two terms of (61) minus (62) gives

$$(63) \qquad \frac{p^r-1}{2} \cdot \frac{p^\ell - p^r}{2} = \frac{p^r-1}{2} \cdot \frac{p^{\ell-r}-1}{2}\, p^r.$$

This shows that the x_s cannot be all equal if G is not elementary abelian, since in this case we would have $x_s = p^r$, and $p^\ell - p^r = 0$, $\ell = r$, $\ell_i = 1$, $i = 1, \ldots, r$.

We arrive to the conclusion that a condition to be fullfilled by the order of G and the number r of its direct factors is, by (61), (62) and (63) that there exist integers x_s, $s = 1, \ldots p^{\ell-2}$, verifying

$$(64) \qquad x_s \le p^r \qquad \sum_{1 \le s \le p^{\ell-r}} x_s^2 \equiv 0 \ mod\ p^r.$$

One sees here the reason why if there exists a group of automorphism of G in which the stabilisor of $\{0\}$ leaves D invariant and operates transitively on it, then G is elementary abelian. Indeed, in that case, all the intersections of C_s and D must have the same cardinality.

2.6.2. The cyclic case.

In the case $r = 1$, C_s must be entirely contained in D or $-D$.

First, we have

$$tC_s = \left(\frac{t}{p}\right)^{\ell} C_s = \left(\frac{t}{p}\right) C_s, \tag{65}$$

by Lemma 2.4.

Now let $\alpha p^{\ell-1}+s$ and $\alpha' p^{\ell-1}+s$ be any two distinct elements of C_s. We write $s = s'p^j$, with $(s',p) = 1$. Let

$$x \equiv (\alpha'-\alpha)/s' \ mod\ p.$$

Multiplying $\alpha p^{\ell-1}+s$ by $xp^{\ell-j-1}+1$, we obtain, since $j < \ell-1$,

$$s'xp^{\ell-1} + \alpha p^{\ell-1} + s = \alpha' p^{\ell-1} + s. \tag{66}$$

Since $xp^{\ell-j-1}+1$ is a quadratic residue mod p, the thesis is proved and it follows from the preceding discussion that $\ell = 1$.

As a last remark, we observe that the present argument proves that $x_s \equiv 0 \ mod\ p$.

BIBLIOGRAPHY

[1] P. CAMION, "Groupes d'automorphisms de graphes complete antysymetriques et presque-corps" Université de Toulouse, Rapport de recherche 1967 (unpublished.)

[2] P. DEMBOWSKI, *Finite Geometries*, Springer-Verlag Berlin, Heidelberg, New York, 1968.

[3] HENRY B. MANN, *Addition Theorems*, Intersciences Publishers, 1965.

[4] LANDAU, *Elementary number theory*, Chelsea.

[5] P. CAMION, "Abelian Codes", MRC Technical Summary Report # 1059.