

# Groups, Difference Sets, and the Monster

Proceedings of a Special Research Quarter  
at The Ohio State University, Spring 1993

*Editors*

K. T. Arasu  
J. F. Dillon  
K. Harada  
S. Sehgal  
R. Solomon

*Offprint*



Walter de Gruyter · Berlin · New York 1996

---

## Contents

---

Preface .....	v
---------------	---

### Part 1 Groups and Geometry

<b>Barbara Baumeister</b> On flag-transitive $cc^*$ -geometries .....	3
<b>Michael F. Dowd</b> On the 1-cohomology of the groups $SL_4(2^n)$ , $SU_4(2^n)$ , and $Spin_7(2^n)$ .....	23
<b>Daniel Frohardt and Kay Magaard</b> About a conjecture of Guralnick and Thompson .....	43
<b>George Glauberman</b> On the Suzuki groups and the outer automorphisms of $S_6$ .....	55
<b>William M. Kantor</b> Note on Lie algebras, finite groups and finite geometries .....	73
<b>Ernest Shult</b> $m$ -systems and the BLT property .....	83
<b>Stephen D. Smith</b> A block complex collapsing to the Brauer tree .....	93
<b>Gernot Stroth</b> Some sporadic geometries .....	99
<b>Gernot Stroth</b> The uniqueness case .....	117

### Part 2 Difference Sets

<b>K. T. Arasu, James A. Davis, Jonathan Jedwab, Siu Lun Ma, Robert L. McFarland</b> Exponent bounds for a family of abelian difference sets .....	129
<b>James A. Davis and Jonathan Jedwab</b> A survey of Hadamard difference sets .....	145

Abs  
subj  
geom  
the  
grou

### Intro

Let  $G$   
in  $G$  is  
exactly  
Irr  
of  $\Delta$  a  
Sup  
 $p^b$ . Th  
among  
In s  
contair  
lists as  
 $\Delta \subset C$   
 $AG(G$   
An  
so as to  
Of  
by cas  
Sec  
(375, 1  
and th

### Theor

an  
1 Thi

# Difference sets in nilpotent groups with large Frattini quotient: geometric methods and (375, 34, 3)

Joel E. Iiams, Robert A. Liebler<sup>1</sup>, and Kenneth W. Smith

---

**Abstract.** We rule out a (375, 34, 3) difference sets in any group  $G$  with a normal subgroup  $K$  so that  $G/K \cong C_3 \times C_5 \times C_5$ . Algebraic number theory is combined with a geometric viewpoint to find a list of putative possible distributions of a difference set among the various homomorphic images of the group  $G$ . These methods work well in nilpotent groups with large Frattini quotient.

## Introduction — Philosophy

Let  $G$  be a finite group of order  $v$  written multiplicatively. A  $(v, k, \lambda)$ -difference set  $D$  in  $G$  is a subset of cardinality  $k$  so that every non-identity element of  $G$  can be written exactly  $\lambda$  ways as  $d_1 d_2^{-1}$ , where  $d_1, d_2 \in D$ .

Irreducible characters allow enumeration of a small list  $\Lambda_p$  of possible distributions of  $\Delta$  among the cosets of  $G/M$ ,  $M$  maximal, depending only on  $p = |G/M|$ .

Suppose  $G$  has a large elementary abelian homomorphic image  $G/B$ , of order say  $p^b$ . The problem is that we must enumerate the possibilities  $\Lambda_{p^b}$  for distributions of  $\Delta$  among the  $B$ -cosets in  $G$  that give rise to elements of the list  $\Lambda_p$ .

In simplest terms, our method is to work down through the lattice of subgroups of  $G$  containing  $B$ , constructing for each such subgroup  $L$ , a list  $\Lambda_{[G:L]}$  compatible with the lists associated with subgroups containing it and with the combinatorial condition that  $\Delta \subset G$ . These compatibility checks involve incidence matrices in the affine geometry  $AG(G/L)$ .

An important refinement is to work in a finite characteristic different from  $p$ , chosen so as to minimize the length of the list  $\Lambda_p$ .

Of course when they exist there seem to be lots, so this philosophy is often overwhelmed by cases. But not always.

Section 2 lays out the method in more detail and Section 3 addresses the specific case (375, 34, 3) where  $\Phi(G) = 1$ . The final section discusses the other groups of this order and the status of our knowledge of difference sets with these parameters. Thus

**Theorem 1.** *There is no (375, 34, 3)-difference set in  $G \cong C_3 \times C_5 \times C_5 \times C_5$ .*

and

---

<sup>1</sup> This research was partially supported by NSA grant 904-91-H-0048.

**Theorem 2.** *There is no  $(375, 34, 3)$ -difference set in any group  $G$  of order 375 with a normal subgroup  $K$  so that  $G/K \cong C_3 \times C_5 \times C_5$ .*

The authors wish to thank K.T. Arasu of Wright State University for his efforts in organizing this conference, and for his survey which led to this paper.

## Geometric methods

The *Fratini* subgroup  $\Phi(G)$  of a finite group  $G$  is defined to be the intersection of all maximal subgroups of  $G$ . If  $G$  is nilpotent (and finite), then  $G/\Phi(G)$  is the direct product of elementary abelian groups and is the largest homomorphic image with this property.

A *distribution* among the cosets of  $B \leq G$  is a function from the coset space  $G/B$  to the natural numbers  $\mathbb{N}$ . The distribution of  $\Delta \subset G$  is the function taking  $gB$  to  $|\Delta \cap gB|$ . In order to constructively study difference sets we are forced to work with lists of *putative possible distributions* (ppd)  $\Lambda_{|G/B|}$ . These are lists of distributions that might possibly be the distribution of a difference set  $\Delta$  among the  $B$ -cosets in  $G$ . As we work our way down through the subgroups of  $G$  containing  $\Phi(G)$ , one of three things happens. We come upon a subgroup  $B$  for which  $\Lambda_{|G/B|}$  is empty and thereby show nonexistence. Or we obtain a ppd list  $\Lambda_{|G/\Phi(G)|}$ . Or we are overwhelmed by a combinatorial explosion.

Suppose  $A \geq B \geq \Phi(G)$  and  $p$  divides  $|A/B|$  but does not divide  $[G:A]$ . Suppose a ppd list  $\Lambda_{p|[G:A]}$  is known (from other methods). We discuss obtaining a ppd list  $\Lambda_{[G:B]}$  in geometric language.

The group  $A/B$  is an elementary abelian  $p$ -group, of order say  $p^n$ , that is a homomorphic image of  $G$ . Regard  $A/B$  as an affine geometry  $AG(n, p)$ . Let  $A_{i,j}^n$ ,  $i, j = 0, \dots, n$  denote incidence matrices of affine  $i$ -spaces and affine  $j$ -spaces in  $AG(n, p)$  (with rows and columns all labelled in a fixed compatible manner), so that, eg. whenever  $0 \leq i \leq j \leq k \neq n$ ,

$$A_{i,j}^n A_{j,k}^n = \binom{k-i}{j-i}_p A_{i,k}^n,$$

where  $\binom{a}{b}_p$  denotes a Gaussian binomial coefficient and 0-spaces are points. Then each element  $\omega$  of the ppd list  $\Lambda_{p|[G:A]}$  has form  $\omega = A_{n-1,0} \delta$ , where  $\delta$  is (the characteristic function of) some element of the desired ppd list  $\Lambda_{[G:B]}$ . Because of the identities satisfied by these incidence matrices, we have

$$A_{0,n-1}^n \omega = A_{0,n-1}^n A_{n-1,0}^n \delta = \binom{n-2}{0}_p |\Delta| J + p^{n-2} \delta.$$

Because we argue recursively, we further assume a ppd list  $\Lambda_{[G:B]/p}$ . Each line  $\ell$  of  $AG(n, p)$  determines a parallel class of lines (a point of the hyperplane at infinity). Let  $\omega_\ell$  denote the truncation of  $\omega \in \Lambda_{p|[G:A]}$  consisting of only those coordinates labelled by affine hyperplanes of  $AG(n, p)$  that contain a line parallel to  $\ell$ . Then  $\epsilon \in \Lambda_{[G:B]/p}$

implies that for each line  $\ell$  of  $AG(n, p)$ , there is  $\omega \in \Lambda_{p[G:A]}$  such that

$$A_{0,n-2}^{n-1} \omega_\ell = \binom{n-3}{0}_p |\Delta| J + p^{n-3} \epsilon.$$

In practice, this process is reversed and the process of working our way downward toward the  $\Phi(G)$ , requires longer and longer lists  $\omega$ , each of which is pasted together from lists of the preceding level. The problem is that lots of possible  $\epsilon$ s must be considered.

Unfortunately, the combinatorial condition that  $\delta$  take integer values in the interval  $[0, |B|]$ , is really the only tool we have for narrowing the search while working downward. For this reason, we seek homomorphic images of the problem that simplify the complexity but still carry some information.

The above matrix equations involve only integer matrices and may be reduced modulo any natural number  $m$ . They can then be used to recover  $\delta$  (modulo  $m$ ) from  $\omega$  modulo  $m$  so long as  $p$  does not divide  $m$ . Our strategy is to choose  $m$  so as to minimize the length of the initial ppd list  $\Lambda_{p[G:A]}$  (modulo  $m$ ).

### Non-existence of a (375, 34, 3)-difference set

We illustrate the method in the previous section by showing non-existence of a (375, 34, 3)-difference set in  $G \cong C_5 \times C_5 \times C_5 \times C_3$ . This non-existence proof falls into several parts. Throughout this section  $G$  is any group of order 375 which also satisfies the hypothesis of the sub-section. This hypothesis usually takes the form that  $G$  has a normal subgroup  $K$ , of specified size, so that  $G/K$  is a specified group.

**The  $C_3$  Image.** Let  $\omega$  be a primitive cube root of unity and let  $\mathcal{R}$  be the ring of integers in the field  $\mathcal{Q}(\omega)$ . Let  $K$  be a normal subgroup of  $G$  of index 3. Consider the linear representation  $\chi$  which sends the generator of  $G/K$  to  $\omega$ . Then  $\chi(D)\overline{\chi(D)}^t = 31\chi(I) + 3\chi(J) = 31$ . Hence the ideal generated by  $\chi(D)$  in  $\mathcal{R}$  contains the ideal generated by 31.

Over  $\mathcal{R}$ , the ideal generated by 31 factors as

$$(31) = (5 - \omega)(5 - \omega^2).$$

Since  $\mathcal{R}$  is a UFD we have that, without loss of generality

$$\chi(D) = 5 - \omega = 15 + 9\omega + 10\omega^2.$$

That is, there is a unique distribution scheme for  $D$  among  $K$ -cosets, and the intersection numbers in that scheme are 9,10 and 15.

**The  $C_5$  Image.** Let now  $K$  be a normal subgroup of index 5 which is the kernel of a linear representation,  $\chi$ , sending a generator of  $G/K$  to  $\zeta$ , a primitive fifth root of unity. Here let  $\mathcal{R}$  be the ring of integers in the field  $\mathcal{Q}(\zeta)$ .

The difference set equation implies that the ideal generated by  $\chi(D)$  contains the ideal generated by 31.

In  $\mathcal{R}$ , up to associates,

$$31 = (-3 + \zeta + 3\zeta^3 + 3\zeta^4)(-3 + 3\zeta + 3\zeta^2 + \zeta^4).$$

Therefore we can assume that up to equivalence

$$\chi(D) = 3 + 7\zeta + 6\zeta^2 + 9\zeta^3 + 9\zeta^4.$$

Again there is a unique distribution scheme for  $D$  and the intersection numbers in this scheme are *in order* 7, 3, 9, 9 and 6. The term “in order” turns out to be important later. This means up to cyclic re-arrangement or the action of  $\text{Aut}_{\mathcal{Z}} \mathcal{Z}[\zeta]$  on  $\chi(D)$ .

**The  $C_{15}$  Image.** Now we assume that  $K$  is a normal subgroup of index 15 and that  $\zeta$  is a primitive 15th root of unity.  $\mathcal{R}$  is the corresponding ring of algebraic integers, and  $\chi$  the corresponding linear representation for  $G$ .

Again, the difference set equation implies that the ideal generated by  $\chi(D)$  over  $\mathcal{R}$  contains the ideal generated by 31.

In  $\mathcal{R}$ , (31) has the following prime ideal factorization,

$$(31) = \prod_{i=0}^7 P_i,$$

where each  $P_i$  takes the form  $P_i = (31, \zeta - x_i)$  and  $x_i$  is a primitive fifteenth root of unity in  $GF(31)$ .

To be explicit

$$\begin{aligned} P_0 &= (31, \zeta - 10) = (1 + \zeta + \zeta^7), \\ P_1 &= (31, \zeta - 14) = (1 + \zeta^2 + \zeta^{14}), \\ P_2 &= (31, \zeta - 18) = (1 + \zeta^4 + \zeta^{13}), \\ P_3 &= (31, \zeta - 7) = (1 + \zeta^8 + \zeta^{11}), \end{aligned}$$

and

$$\begin{aligned} P_4 &= (31, \zeta - 9) = (\overline{P_3}), \\ P_5 &= (31, \zeta - 19) = (\overline{P_2}), \\ P_6 &= (31, \zeta - 20) = (\overline{P_1}), \\ P_7 &= (31, \zeta - 28) = (\overline{P_0}). \end{aligned}$$

The group  $\text{Aut}_{\mathcal{Z}} \mathcal{Z}[\zeta]$  acts transitively on the prime factors of 31 in  $\mathcal{R}$ . Complex conjugation is induced by the automorphism which sends  $\zeta$  to  $\zeta^{-1}$  and decomposes the factors into orbits of size two. The ideal generated by  $\chi(D)$ , therefore, contains the same number of prime factors of (31) as its complex conjugate  $\overline{\chi(D)}$ .

Since the product  $\chi(D)\overline{\chi(D)}$  contains (31), each of  $\chi(D)$  and  $\overline{\chi(D)}$  contain four prime factors. Furthermore, each orbit of factors under complex conjugation is split between  $\chi(D)$  and  $\overline{\chi(D)}$ .

If  $\delta$  is a solution to  $\delta\overline{\delta} = 31$  in  $\mathcal{R}$ , then  $\delta$  must be the product of four of the eight factors  $P_i$ , none the complex conjugate of the other. There are  $2^4 = 16$  such products

but they break into four orbits under the action of  $\text{Aut}_Z \mathbb{Z}[\zeta]$ . Representatives of the orbits are

$$\begin{aligned} p_1(\zeta) &:= P_0 P_1 P_2 \overline{P_3} = (-1 - \zeta + 2\zeta^4 + 2\zeta^5 + 3\zeta^7 - \zeta^9 + 2\zeta^{11} - 2\zeta^{12} + \zeta^{13} + \zeta^{14}) \\ &= (-2\zeta + 2\zeta^4 + \zeta^5 + 4\zeta^7 - 2\zeta^8) \end{aligned}$$

$$p_2(\zeta) := (P_0 P_1 P_2 P_3) = (3 + 2(\zeta^7 + \zeta^{11} + \zeta^{13} + \zeta^{14}))$$

$$p_3(\zeta) := (P_0 P_1 \overline{P_2 P_3}) = (\zeta^3 - 3\zeta^6 + 3\zeta^9 + 3\zeta^{12}) = (-3 + 3\zeta^3 + 3\zeta^6 + \zeta^{12})$$

and

$$p_4(\zeta) := P_0 \overline{P_1 P_2 P_3} = (-1 + 5\zeta^5) = (5 - \zeta^{10}).$$

We turn these into images of a difference set by adding multiples of zero, that is multiples of

$$1 + \zeta^3 + \zeta^6 + \zeta^9 + \zeta^{12}$$

and multiples of

$$1 + \zeta^5 + \zeta^{10}$$

so that

$$\delta \equiv 15 + 9\zeta + 10\zeta^2 \pmod{\zeta^3 - 1},$$

and

$$\delta \equiv 3 + 7\zeta + 6\zeta^2 + 9\zeta^3 + 9\zeta^4 \pmod{\zeta^5 - 1}.$$

For example,

$$\begin{aligned} p_2(\zeta) &= (3 + 2(\zeta^7 + \zeta^{11} + \zeta^{13} + \zeta^{14})) \\ &= (3 + 2(\zeta^7 + \zeta^{11} + \zeta^{13} + \zeta^{14}) + (1 + 2\zeta^5 + \zeta^{10})(1 + \zeta^3 + \zeta^6 + \zeta^9 + \zeta^{12}) \\ &\quad + (\zeta^2 + \zeta^3 - \zeta^4)(1 + \zeta^5 + \zeta^{10})) \\ &= (4 + 2\zeta + 2\zeta^2 + 2\zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + 5\zeta^7 + 2\zeta^8 + 2\zeta^{10} \\ &\quad + 3\zeta^{11} + 2\zeta^{12} + 5\zeta^{13} + 2\zeta^{14}) \end{aligned}$$

which is the set of intersection numbers

$$4 \ 2 \ 2 \ 2 \ 1 \ 1 \ 1 \ 5 \ 2 \ 0 \ 2 \ 3 \ 2 \ 5 \ 2.$$

This set is equivalent to item C in the list below.

From the four possibilities for  $\delta$ , we find six solutions. The factoring  $\delta = p_1(\zeta)$  gives no solutions;  $\delta = p_2(\zeta)$  gives solutions B and C below;  $\delta = p_3(\zeta)$  gives solutions D and E;  $\delta = p_4(\zeta)$  gives solutions A and F. The intersection numbers are

- A) 1 1 2 3 3 1 6 2 3 3 1 0 2 3 3
- B) 3 1 1 3 4 0 2 1 2 3 0 4 4 4 2
- C) 1 1 1 5 2 0 2 3 2 5 2 4 2 2 2
- D) 1 2 3 4 4 2 3 1 2 5 0 2 2 3 0
- E) 1 2 3 5 3 2 3 1 0 4 0 2 2 4 2
- F) 2 5 2 4 2 1 2 1 3 4 0 0 3 2 3

(These solutions were originally found by computer search.)

It is sometimes convenient to box these according as  $C_{15} = C_3 \times C_5$ . Then it is more obvious how one uses these numbers to get back to one of the previous levels.

For example, A) becomes

$$\begin{array}{cccccc} 1 & 1 & 2 & 3 & 3 & \\ 1 & 6 & 2 & 3 & & 3 \\ 1 & 0 & 2 & 3 & 3 & \end{array}$$

The row sums yield the  $C_3$  distribution, and the column sums yield the  $C_5$  distribution.

**The  $C_5 \times C_5$  Image.** Now let  $K$  be a normal subgroup of  $G$  so that  $G/K \cong C_5 \times C_5$ . View  $C_5 \times C_5$  as  $AG(2, 5)$ . Assign to each point a weight which is equal to the size of the intersection of the  $k$ -coset labeled by that point and the difference set.

Let  $m_i$  be the number of points of weight  $i$ . By elementary counting, we have that

$$\begin{aligned} \sum m_i &= 25 \\ \sum im_i &= 34 = k \\ \sum i(i-1)m_i &= 42. \end{aligned}$$

Observe that  $m_i = 0$  for  $i \geq 8$ , since the  $m_i$ 's are non-negative integers. We get 27 solutions in non-negative integers  $\{m_i\}$  to this system of equations. Unfortunately, the list is quite long. This is a case of where the analysis produces an explosion of possibilities.

In this case we wish to find a way to narrow the field. To that end let  $A$  be the line-point incidence matrix for  $AG(2, 5)$ . Let  $\vec{d}$  be the vector of point weights. Set  $\vec{v} = A\vec{d}$ . The entries of  $\vec{v}$  are the sums of the weights of points on given lines. We call this a line sum.

When one takes the line sums for all lines in a parallel class, one is effectively mapping  $C_5 \times C_5$  onto  $C_5$ . Thus the set of line sums from a parallel class is the set of intersection numbers associated with the  $C_5$  image, in an appropriate order. Therefore, modulo 3,  $\vec{v}$  gives the position of 6 lines, one from each parallel class, where the line sum is 7.

Next, observe that since

$$A\vec{d} \equiv \vec{v} \pmod{3}$$

that

$$A^t A\vec{d} \equiv A^t \vec{v} \pmod{3}.$$

So

$$(5I + J)\vec{d} \equiv A^t \vec{v} \pmod{3}$$

$$\begin{aligned}
 (J - I)\vec{d} &\equiv A^t\vec{v} \pmod{3} \\
 34\vec{j} - \vec{d} &\equiv A^t\vec{v} \pmod{3} \\
 \vec{j} - \vec{d} &\equiv A^t\vec{v} \pmod{3}.
 \end{aligned}
 \tag{3.4.1}$$

Call the six lines with line sum 7 “special”. Then the right-hand side is counting the number of special lines each point is on.

Let  $a_i$  be the number of points of  $AG(2, 5)$  which lie on exactly  $i$  special lines. Then the  $a_i$  must satisfy the following system of linear equations.

$$\begin{aligned}
 \sum a_i &= 25 \\
 \sum ia_i &= 30 \\
 \sum i(i - 1)a_i &= 30.
 \end{aligned}$$

Since any point lies on at most 6 lines,  $a_i = 0$  for  $i \geq 7$ . The congruence  $\vec{j} - \vec{d} \equiv A^t\vec{v}$  implies that we may replace the first linear equation by

$$\begin{aligned}
 a_1 + a_4 &= m_0 + m_3 + m_6 := x \\
 a_0 + a_3 + a_6 &= m_1 + m_4 := y \\
 a_2 + a_5 &= m_2 + m_5 := z.
 \end{aligned}$$

We get the following set of solutions  $\{m_i\}, \{a_i\}$ .

$M_0$	$m_1$	$m_2$	$m_3$	$m_4$	$a_0$	$a_1$	$a_2$	$a_3$	$a_4$
$\frac{6}{6}$	$\frac{8}{8}$	$\frac{9}{9}$	$\frac{0}{0}$	$\frac{2}{2}$	$\frac{8}{8}$	$\frac{6}{6}$	$\frac{9}{9}$	$\frac{3}{2}$	$\frac{0}{0}$
6	9	6	3	1	7	9	6	3	0
7	6	9	2	1	7	8	9	0	1
6	10	3	6	0	6	12	3	4	0
7	7	6	5	0	6	11	6	1	1

Call these cases in order A, B, C, D and E. We can show that only case B survives. The arguments are repetitive and we offer the following example of the argument.

Suppose that case E occurs. Then there is a point which lies on four special lines. Use the translation subgroup of the affine general linear group of  $AG(2, 5)$  so that the origin is this point.

Choose bases so that two of the special lines through the origin are the lines  $x = 0$  and  $y = 0$ .

The remaining pairs of lines through  $(0, 0)$  are in two orbits under the action of the diagonal map sending  $x$  to itself and  $y$  to  $2y$ . Therefore, up to equivalence, we may assume that the four lines through the origin are;

$$\{x = 0, y = 0, x = y, x = -y\}$$

or

$$\{x = 0, y = 0, x = y, y = 2x\}.$$

We suppose the first case. To this configuration of four lines, we wish to add two more: One line with slope 2 and non-zero  $y$ -intercept, and one line with slope  $\frac{1}{2}$  and

non-zero  $y$ -intercept. The lines of slope 2 with non-zero  $y$ -intercept fall in an orbit under the action of the diagonal map  $2I$ . So we can assume that a fifth line is  $y = 2x + 1$ . We need now only add a line of slope  $\frac{1}{2}$ . We may index the four possibilities by the non-zero value of the  $y$ -intercept of the last line added.

When we take the  $y$ -intercept value of the line of slope  $\frac{1}{2}$  to be 2, we get the following array. Consider the array as  $AG(2, 5)$  where the numbers are the number of special lines the corresponding point lies on. We coordinatize the array with the origin at the upper left-hand corner,  $x$  increasing to the right, and  $y$  increasing downward.

$$\begin{array}{ccccc} 4 & 2 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 2 & 0 \\ 1 & 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 3 \end{array}$$

From this array we wish to use our congruence (3.4.1) to reconstruct a  $5 \times 5$  array of intersection numbers.

The congruence tells us that any point which lies on two special lines is a point of weight two. Also, any point which lies on zero or three special lines must be a point of weight one. Therefore we may partially fill in the array of intersection numbers as:

$$\begin{array}{ccccc} - & 2 & 2 & - & - \\ 2 & - & 1 & - & - \\ 2 & 1 & - & 2 & 1 \\ - & - & 2 & - & 1 \\ - & - & 1 & 1 & 1 \end{array}$$

The current line sums of the lines with slope 1 are

$$\left\{ \left\{ \sum_{y=x+c} \right\}_{c=0} \right\}^4 = \{1, 6, 3, 3, 6\}.$$

Since the order of the line sums makes a difference, we know that this set of line sums must eventually yield 7, 9, 3, 6, 9 or 7, 9, 6, 3, 9. Therefore we know that the weight of  $(0, 4)$  equals the weight of  $(4, 0)$  is 3. So an updated version of our partial array of intersection numbers is

$$\begin{array}{ccccc} - & 2 & 2 & - & 3 \\ 2 & - & 1 & - & - \\ 2 & 1 & - & 2 & 1 \\ - & - & 2 & - & 1 \\ 3 & - & 1 & 1 & 1 \end{array}$$

Now, the current line sums of the lines with slope  $-1$  are

$$\left\{ \left\{ \sum_{y=-x+c} \right\}_{c=0} \right\}^4 = \{4, 6, 6, 3, 6\}.$$

Again the order matters and the first one is a special line which should eventually have a line sum of 7. Therefore these line sums must become in order 7, 9, 6, 3, 9. Thus we can update our partial array of intersection numbers to

$$\begin{matrix} - & 2 & 2 & 0 & 3 \\ 2 & 0 & 1 & - & - \\ 2 & 1 & - & 2 & 1 \\ 0 & - & 2 & 3 & 1 \\ 3 & - & 1 & 1 & 1 \end{matrix}$$

Finally we consider the line sums for the lines with infinite slope. These are currently

$$\left\{ \left\{ \sum_{x=c} \right\} \right\}_{c=0}^4 = \{ \{7, 3, 6, 6, 6\} \}.$$

The only possibility is that these should be in order 7, 3, 9, 9, 6. Therefore the array of intersection numbers is

$$\begin{matrix} 0 & 2 & 2 & 0 & 3 \\ 2 & 0 & 1 & 3 & 0 \\ 2 & 1 & 3 & 2 & 1 \\ 0 & 0 & 2 & 3 & 1 \\ 3 & 0 & 1 & 1 & 1 \end{matrix}$$

But now

$$\sum_{y=1} = \sum_{y=3} = \sum_{y=4} = 6$$

a contradiction.

The remaining subcases here fall similarly, as do cases A, C and D. However, a similar argument in case B leads to the following array of intersection numbers which is unique up to automorphisms of  $AG(2, 5)$ :

$$\begin{matrix} 1 & 1 & 2 & 3 & 0 \\ 2 & 0 & 1 & 4 & 2 \\ 0 & 0 & 2 & 1 & 0 \\ 2 & 1 & 1 & 1 & 1 \\ 2 & 1 & 3 & 0 & 3 \end{matrix}$$

**There is no  $C_5 \times C_5 \times C_5$  image.** Suppose now that  $K$  is a normal subgroup of  $G$  of size 3 so that  $G/K \cong C_5 \times C_5 \times C_5$ . Consider the quotient as  $AG(3, 5)$  with weighted points. The weight of a point is equal to the size of the intersection of the  $K$ -coset labeled by that point and our putative difference set.

Let  $\vec{d}_1$  be the vector of point weights and let  $B$  be the plane-point incidence matrix for  $AG(3, 5)$ . Set  $\vec{v}_1 = B\vec{d}_1$ .

Each entry of  $B\vec{d}_1$  is the sum of the weights of all points on a given plane. When the rows of  $B$  are arranged so that the planes are partitioned into parallel classes, these sums represent the  $C_5$  image. Therefore  $\vec{v}_1$  is a vector of length 155 which may be partitioned into 31 parts of size 5. Each part of size 5 is 7, 3, 9, 9, 6 in an appropriate order. Thus

modulo 3,  $\vec{v}_1$  is a position vector of 31 planes no two parallel. These are the planes with plane sum 7.

Let  $b_i$  be the number of points of  $AG(3, 5)$  which lie on exactly  $i$  of these 31 “special” planes. The  $b_i$ ’s must satisfy the following system of equations:

$$\begin{aligned} \sum b_i &= 125 \\ \sum i b_i &= |\text{incident (point, plane)}| = (31)(25) \\ \sum i(i-1)b_i &= |\text{incident (point, plane, plane)}| = (31)(30)(5) \end{aligned}$$

and

$$\sum i(i-1)(i-2)b_i = |\text{incident (point, plane, plane, plane)}|.$$

The last entry on the right-hand side breaks into two cases.

First we must count the number of triples of planes which intersect in exactly one point. This is  $(31)(30)(25)$ .

Second, we want 5 times the number of triples of planes in our configuration which intersect in a line. There are precisely 31 homomorphic images  $AG(2, 5)$  of  $AG(3, 5)$ . Each of these planes contains 3 points which are the intersection of precisely 3 special lines. The preimage of this point-line-line-line configuration in  $AG(3, 5)$  is an incident point-plane-plane-plane configuration and all of these configurations are distinct. Thus the last entry on the right-hand side is

$$(31)(30)(25) + (5)(31)(3).$$

This cannot occur. Every coefficient on the left-hand side of the last equation is divisible by six. By integrality the right-hand side must be divisible by six. It is clearly not.

Theorem 1.1 now follows immediately.

### The $C_3 \times C_5 \times C_5$ image

In this section  $K$  is a normal subgroup of index 15 in  $G$  so that  $G/K \cong C_3 \times C_5 \times C_5$ . View the quotient as three copies of  $AG(2, 5)$  stacked on top of each other. Weight the points according to intesection number.

Let  $p_i$  be the number of points of weight  $i$ . The  $p_i$ ’s satisfy

$$\begin{aligned} \sum p_i &= 75 \\ \sum i p_i &= 34 \\ \sum i(i-1)p_i &= 42. \end{aligned}$$

The solutions in non-negative integers to this system of equations is

$\frac{p_0}{44}$	$\frac{p_1}{30}$	$\frac{p_2}{9}$	$\frac{p_3}{9}$	$\frac{p_4}{1}$
45	28	0	2	0
46	25	3	1	0
47	22	6	0	0

The sum of the weights of the points on one copy of  $AG(2, 5)$  here is an intersection number related to the  $C_3$  image. Without loss of generality we may assume that the sum of the weights of the points on our three planes are in order 15, 10 and 9.

The line sums for a parallel class of lines in the bottom plane must sum to 9 and are therefore one of

- 1) 0 2 3 3 1
- 2) 0 4 1 2 2
- 3) 0 2 2 2 3

where these come from section 3.3.

Let  $\vec{d}$  be the vector of weights for this plane, and let  $A$  be as in section 3.4. Then

$$A^t A \vec{d} = 5\vec{d} + 9\vec{j} := A^t \vec{v}.$$

With appropriate row labels the vector  $\vec{v}$  breaks into 6 vectors of length 5, each having total weight 9 and equivalent to one of 1), 2) or 3).

If a point on this plane had weight 4, then since it is forcibly collinear to another point of non-zero weight, there would be a line sum greater than 4. This contradiction shows that our lower plane contains no point of weight 4.

Suppose next that the bottom plane has a point of weight 3. The argument of the previous paragraph forces the plane to contain no other point of weight greater than 2. Therefore, the bottom plane contains 6 points of weight 1 and 18 points of weight zero. Moreover each line through the point of weight three has exactly one point of weight 1 on it. Therefore, for every parallel class the line sums are equivalent to 2) above. Since the line weights are 0, 1, 2 and 4 and since  $1 = \frac{(4+5*2-9)}{5}$  we are forced to conclude that each point of weight one lies on five lines of weight 2. Therefore no line of weight one has a point of weight one on it. This contradiction forces the weights in the bottom plane to be only 0, 1 or 2.

At this point a computer program was written to find all  $5 \times 5$  arrays with row sums and column sums of the forms in cases 1), 2) or 3). Each solution found had the property that there was one  $C_5$  image which was similar but not equivalent to one of 1), 2) or 3). Therefore there is no  $C_3 \times C_5 \times C_5$  image.

Theorem 1.2 now follows.

We remark that the aforementioned program only ran for 20 minutes on a Macintosh. It may well be that there are few enough cases to enumerate and eliminate by hand, ala the methods of Section 3.4.

## References

- [1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York 1990.
- [2] E.S. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, New York 1983.

Joel E. liams  
Robert A. Liebler  
Colorado State University  
Fort Collins, CO 80523

Kenneth W. Smith  
Central Michigan University  
Mount Pleasant, MI 48859

---

<b>Joel E. Iiams, Robert A. Liebler, and Kenneth W. Smith</b>	
Difference sets in nilpotent groups with large Frattini quotient: geometric methods and $(375, 34, 3)$ .....	157
<b>David B. Meisner</b>	
A difference set construction of Turyn adapted to semi-direct products .....	169
<b>Harriet Pollatsek</b>	
Difference sets in groups of order $4p^4$ .....	175
<b>Alexander Pott</b>	
A survey on relative difference sets .....	195
<b>Ming-yuan Xia</b>	
Williamson matrices and difference sets .....	233
<b>Qing Xiang</b>	
Note on Paley type partial difference sets .....	239

### Part 3 The Monster

<b>Shogo Aoyama</b>	
Anti-bracket formalism with the Kähler geometry .....	247
<b>Imin Chen and Noriko Yui</b>	
Singular values of Thompson series .....	255
<b>John H. Conway</b>	
Understanding groups like $\Gamma_0(N)$ .....	327
<b>John H. Conway</b>	
The $\sqrt{\text{Monster}}$ construction .....	345
<b>Chongying Dong, Zongzhu Lin, and Geoffrey Mason</b>	
On vertex operator algebras as $SL_2$ -modules .....	349
<b>Charles R. Ferenbaugh</b>	
Lattices and generalized Hecke operators .....	363
<b>Robert L. Griess, Jr.</b>	
Codes, loops and $p$ -locals .....	369
<b>Koichiro Harada, Masahiko Miyamoto, and Hiromichi Yamada</b>	
A generalization of Kac–Moody algebras .....	377
<b>John McKay</b>	
A note on the elliptic curves of Harada–Lang .....	409
<b>Paul S. Montague</b>	
Ternary codes and $\mathbb{Z}_3$ -orbifold constructions of conformal field theories .....	411
<b>Simon P. Norton</b>	
Non-monstrous moonshine .....	433
<b>Michael P. Tuite</b>	
Monstrous Moonshine and orbifolds .....	443