stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE
(DEPARTMENT OF PURE MATHEMATICS)

ZW 102/77 OKTOBER

A.E. BROUWER

SOME NON-ISOMORPHIC BIBDs B(4,1;v)

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 05B05

Some non-isomorphic BIBDs B(4,1;v)

by

A.E. Brouwer

ABSTRACT

Let $v \equiv 1$ or $4 \pmod{12}$. It is proved that at least two non-isomorphic Steiner quadruple systems $S(2,4,v)$ exist if (and only if) $v > 16$.

KEY WORDS & PHRASES: *non-isomorphic block designs.*

0. INTRODUCTION

In WOJTAS [1] I found the statement

> "It is known that there exist at least two non-isomorphic systems B(4,1;v) if $v \equiv 1$ or 4 (mod 12), $v \geq 61$, $v \neq 73$ and $v \neq 85$ or if $v = 40$."

In this note, we construct some non-isomorphic designs for the remaining values of v. Although the finding of these designs turned out to be quite easy, the proof of their non-isomorphism was not obvious.

The main aim of [1] was to prove that the number of non-isomorphic B(4,1;v) is at least something like v/360. Of course this is a terribly weak bound, the truth being perhaps something like $(cv)^{v^2/12}$. I shall not go into this matter now - it seems not unlikely that this asymptotics has already been considered by someone else.

1. <u>$v < 25$</u>

If $v \equiv 1$ or 4 (mod 12) and $v < 25$ then there is a unique B(4,1;v):

$v = 1$: no blocks (empty design)
$v = 4$: a single block (trivial design)
$v = 13$: PG(2,3)
$v = 16$: AG(2,4).

2. <u>$v = 25$</u>

A first example of a B(4,1;25) (and the only example with a transitive automorphism group) is found by taking X = AG(2,5) for pointset, and $B_0 \subset AG(2,5)$ some quadrangle, no two sides of which are parallel. Let B_1 be the image of B_0 under some homothetie with dilation factor 2. Now let $\mathcal{B}$ be the collection of 50 blocks obtained by translating B_0 and B_1. Then $(X,\mathcal{B})$ is a B(4,1;25) design and its automorphism group has order 150. [For: there are 25.20.4 ways to choose B_0 and since translates generate the same design $\mathcal{B}$ we find 80 different designs $\mathcal{B}$. But |Aut AG(2,5)| = 25.24.20, hence $|\mathrm{Aut}\ \mathcal{B}| = 25.6 = 150$. (A priori it is conceivable that Aut $\mathcal{B}$ contains elements not in Aut AG(2,5) but this turns out not to be the case.)]

A short computer search showed that there is no S(2,4,25) design invariant under $\mathbb{Z}_{25}$ and a unique one (the above one) invariant under $\mathbb{Z}_5 \times \mathbb{Z}_5$. One explicit representation is: let $X_1 = \mathbb{Z}_5 \times \mathbb{Z}_5$ and take the blocks

$\{(0,0),(0,1),(1,0),(4,3)\}$ and
$\{(0,0),(0,2),(2,0),(3,1)\}$ mod (5,5).

A second example is the following:

Let $X_2 = \mathbb{Z}_3 \times (\mathbb{Z}_7 \cup\{\infty\}) \cup\{\Omega\}$ and take the blocks

$\{(0,\infty),(1,\infty),(2,\infty),\quad \Omega\}$,
$\{(0,0),(1,0),(2,0),\quad \Omega\}$ mod (–,7),
$\{(0,\infty),(0,1),(1,2),(2,4)\}$ mod (3,7), and
$\{(1,0),(0,1),(0,2),(0,4)\}$ mod (3,7).

This is again an S(2,4,25) and besides the obvious automorphisms of order 3 and 7 it has the automorphism of order 3 leaving Ω and (i,∞) invariant and sending (i,j) to $(i+1,2j)$.

It cannot be isomorphic to the previous design since $7 \nmid 150$. Another way to distinguish these designs is to study the intersection pattern of two fans: given two points a and b, let $B_0,\ldots,B_7$ be the eight blocks incident with a, and $B_0',\ldots,B_7'$ be the eight blocks incident with b, where the indexing is such that $B_7 = B_7'$ is the unique block containing a and b. Now define a 7×7 matrix M_{ab} with entries $m_{ij} = |B_i \cap B_j'|$. Calling our two designs $\mathcal{D}_1$ and $\mathcal{D}_2$ we find for $\mathcal{D}_2$ with $a = \Omega$ and $b = (0,\infty)$ the incidence matrix of PG(2,2), the Fano plane, and for $a = \Omega$ and $b = (0,0)$ the matrix

1010010
0100110
0011100
1101000
1010001
0001101
0100011

so that $(\mathrm{Aut}\ \mathcal{D}_2)_\Omega$ has two orbits. Since Aut $\mathcal{D}_1$ is transitive, if $\mathcal{D}_1$ and $\mathcal{D}_2$ were isomorphic we would have M_{ab} isomorphic to one of these two matrices for any two points $a, b \in X_1$. But for $a = (0,0)$, $b = (0,1)$ we find

0110100
0100011
0010011
1000011
0111000
1001100
1001100.

3. v = 28

Let $X_1 = (\mathbb{Z}_3)^3 \cup \{\infty\}$ and take the blocks

{011,021,102,202},{211,121,222,112} mod (3,3,3), and
{∞ ,000,001,002} mod (3,3,-).

(Here ijk stands for (i,j,k).)
This is a resolvable S(2,4,28): one parallel class (replication) is obtained by taking the base blocks mod (-,-,3).

Let $X_2 = I_4 \times \mathbb{Z}_7$ and take the blocks

[{00,01,10,13},{02,04,21,22},{03,06,33,35},{14,15,20,24},
{11,16,30,34},{23,25,31,32},{05,12,26,36}] mod (-,7), and
[{00,11,22,33} mod (-,7)], and
[{00,15,23,35} mod (-,7)].

This yields again a resolvable S(2,4,28) (the parallel classes being indicated between square brackets).

In order to prove non-isomorphism we can again use the fan intersection matrices: If $\mathcal{D}_1$ and $\mathcal{D}_2$ were isomorphic then the automorphism group would be transitive on points and blocks, and since $(\mathrm{Aut}\ \mathcal{D}_1)_\infty$ is transitive on $X_1\backslash\{\infty\}$ the group Aut $\mathcal{D}$ would be 2-transitive, and all matrices M_{ab} would be isomorphic. But for $\mathcal{D}_1$ we find for $a = \infty$ and $b = 000$ and for $a = 000$, $b = 001$ the matrices M_{ab} (respectively):

00 10 10 01		00 00 01 11
00 01 01 10		00 00 10 11
01 00 10 10		11 00 00 01
10 00 01 01		11 00 00 10
10 10 00 10	and	10 11 00 00
01 01 00 01		01 11 00 00
10 01 10 00		00 10 11 00
01 10 01 00		00 01 11 00

which are non-isomorphic. (Hence Aut $\mathcal{D}_1$ is not 2-transitive, i.e. Aut $\mathcal{D}_1$ leaves ∞ fixed.)

4. <u>v = 37</u>

Let X_1 = GF(37) and take the orbit of $B_0 = \{0,1,3,24\}$ under the group generated by $x \to x+1$ and $x \to 2^{12}.x$ (2 is a primitive root mod 37; $2^{12} = 26 = -11$), that is,

$\{0,1,3,24\},\{0,4,26,32\},\{0,10,18,30\}$ mod 37.

Let $X_2 = \mathbb{Z}_3 \times (\mathbb{Z}_{11} \cup \{\infty\}) \cup \{\Omega\}$ and take the blocks

$\{\Omega\ ,0\infty,1\infty,2\infty\}$,

$\{\Omega\ ,00,10,20\}$ mod (-,11),

$\{0\infty,00,16,22\},\{00,01,12,15\},\{00,02,07,1\,10\}$ mod (3,11).

Just as in the case v = 25 we see that if $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic then each matrix M_{ab} must be one of the two obtained by taking a = Ω, b = 00 and a = Ω, b = 0∞ in X_2. These matrices are respectively

11100000000*		10000100010
00011000001		01000010001
10010001000		10100001000
00000100011		01010000100
00101000010		00101000010
01010000100	and	00010100001 .
10000010010		10001010000
01000011000		01000101000
00000010101*		00100010100
00100100100		00010001010
00001101000*		00001000101

(They are different since the first one has three disjoint rows - marked with stars- unlike the second one.)

But the matrix M_{ab} with a = 00 and b = 0∞ in X_2 has first few rows

10000100010
11010000000
10110000000
....

and in particular contains a repeated pair. Hence Aut $\mathcal{D}_2$ is not transitive.

5. v ≥ 49, large

If v = 3u+1 and $(Y,\mathcal{B})$ is a B({4,5},1;u} then a B(4,1;v) can be constructed by taking $X = (I_3 \times Y) \cup \{\infty\}$ and $\mathcal{D} = \bigcup_{B \in \mathcal{B}} \mathcal{D}_B$, where for each B $\mathcal{D}_B$ is a B(4,1;3.|B|+1) design on the pointset $(I_3 \times B) \cup \{\infty\}$ containing the blocks $(I_3 \times \{b\}) \cup \{\infty\}$ for $b \in B$.
This construction leaves us a lot of freedom: if |B| = 4 then we can choose $\mathcal{D}_B$ in 72 ways $\left(\frac{4!(3!)^4}{|\mathrm{Aut}\ PG(2,3)_\infty|} = \frac{24.6^4.13}{\frac{1}{2}(27-1)(27-3)(27-9)} = 72\right)$ while if |B| = 5 then $\mathcal{D}_B$ can be chosen in 2592 = $72^2/2$ ways

$$\left(\frac{5!(3!)^5}{|\mathrm{Aut}\ AG(2,4)_\infty|} = \frac{120.6^5.8}{(64-4)(64-16)} = 2^5.3^4 = 72^2/2\right).$$

If v is large then we see that not all these designs can be isomorphic by simple counting, e.g. if $(Y,\mathcal{B})$ is a B(4,1;u) we find $72^{\frac{u(u-1)}{12}}$ designs, and each design can be isomorphic to at most (3u+1)! designs, but $72^{\frac{u(u-1)}{12}} \gg (3u+1)!$ so we find many non-isomorphic designs.

For smaller v we need a somewhat refined counting argument: since $(X,\mathcal{D})$ determines $(Y,\mathcal{B})$ we get different designs each time we start with another design $(Y,\mathcal{B})$. This yields an extra factor of at least $u!/|\mathrm{Aut}(Y,\mathcal{B})|$.

Thus for v = 85 we find from 85 = 3*28+1 that if N = $|\mathrm{Aut}(Y,\mathcal{B})|$ for some S(2,4,28) design $(Y,\mathcal{B})$ then there are at least

$$\frac{28!}{N} \cdot \frac{72^{63}}{85!} > \frac{1}{N} \cdot \frac{72^{63}.\left(\frac{28}{e}\right)^{28}\sqrt{2\pi.28}}{\left(\frac{85}{e}\right)^{85} e\sqrt{2\pi.85}} > \frac{72.^{63}10^{28}.5}{N.32^{85}.27} = \frac{3^{123}.5^{29}}{N.2^{188}} >$$

$$> \frac{2^{12}.3^{36}}{N}$$

non-isomorphic designs S(2,4,85). Now for the examples of a S(2,4,28) given above we probably have $1 < N < 1000$ but I am too lazy to compute the automorphism groups. A very rough estimate for the first example however yields $N \le 27.24.2^6 = 3^4.2^9$ (as soon as 2 points of a block are fixed, all you can do with the other two points is interchange them; since ∞ is fixed we have a fixed partition of $X\backslash\{\infty\}$ into 9 triples; the index of the stabilizer of one point $\neq \infty$ is 27, of three points (in a block with ∞) at most 54, of six points (in two blocks with ∞) at most $27.24.2^2$ etc.) so that we have in any case at least $2^3.3^{32}$ non-isomorphic S(2,4,85) systems.

Likewise for v = 73 we find from 73 = 3*24+1 using the B({4,5},1;24) obtained by shortening the affine plane AG(2,5):

$N = |\mathrm{Aut}(Y,\mathcal{B})| = |\mathrm{Aut}\ AG(2,5)_\infty| = \frac{1}{25} \cdot (125 - 5) \cdot (125 - 25) = 480$

$\mathcal{B}$ contains 6 blocks of size 4 and 24 blocks of size 5 so that we find at least

$$\frac{24!}{480} \cdot \frac{72^6.72^{48}}{73!.2^{24}} > \frac{(\frac{12}{e})^{24}\sqrt{2\pi.24}.\ 72^{54}}{(\frac{73}{e})^{73}.e\sqrt{2\pi.73}.\ 480} > \frac{72^{54}.4^{24}.4}{27^{73}.9.480} =$$

$$= \frac{2^{207}}{5.3^{114}} > 10^7$$

non-isomorphic designs S(2,4,73).

Finally for the cases v = 49 = 3*16+1 and v = 52 = 3*17+1 we have to examine somewhat more carefully the structure of the design $(X,\mathcal{D})$ since these rough counting arguments do not work any longer.

6. <u>v = 49</u>

Construct $(X,\mathcal{D})$ as above, using 49 = 3*16+1 and $(Y,\mathcal{B})$ being the affine plane AG(2,4). If we want the $(X,\mathcal{D})$ to have a subdesign S(2,4,16) then we have to choose a function $f: Y \to I_3$ (the set $\{(y,f(y)) | y \in Y\}$ will be the subdesign) and next construct the $\mathcal{D}_B$ in such a way that they contain the block $\{(b,f(b)) | b \in B\}$. For each B this can be done in 8 different ways. Since a S(2,4,49) cannot contain two different S(2,4,16) subdesigns (because these would intersect in at least 7 points and have a subdesign in common, hence coincide) it follows that among the 72^{20} different designs exactly $3^{16}.8^{20}$ contain a subdesign S(2,4,16) so that there are at least two non-isomorphic S(2,4,49).

7. v = 52

Construct $(X,\mathcal{D})$ as above, using $52 = 3*17+1$ and $(Y,\mathcal{B})$ being the one-point partial completion of AG(2,4) (with 4 blocks of size 5 and 16 blocks of size 4). From the blocks of size 5 we find 4 subdesigns S(2,4,16) containing ∞. If $Y = AG(2,4) \cup \{\Omega\}$ and $B\cup\{\Omega\}$ is a block of size 5 in $\mathcal{B}$ then there are $\frac{3!(2!)^4 4!}{24} = 96$ ways to choose $\mathcal{D}_{B\cup\{\Omega\}}$ in such a way that it contains the block $\{(b,f(b)) \mid b \in B\}$. Hence for each function $f: Y\backslash\{\Omega\} \to I_3$ we find $8^{16}.96^4$ designs containing the 'horizontal' subdesign $\{(y,f(y)) \mid y \in Y\backslash\{\Omega\}\}$ and hence at most $3^{16}.8^{16}.96^4$ designs $(X,\mathcal{D})$ with (at least) 5 subdesigns S(2,4,16), while the remaining (at least $72^{20}.36^4 - 3^{16}.8^{16}.96^4$) designs have exactly 4 subdesigns S(2,4,16). Again we find at least two non-isomorphic S(2,4,52) designs.

8. CONCLUSION

The above constructions, together with the results of Pukanow referred to in [1] (or the above constructions together with the observation that brute force counting works also for v > 85 and v = 76 and counting of subdesigns also for v = 40, 61 and 64) prove our

THEOREM. *Let* $v \equiv 1$ *or* 4 (mod 12). *There exist at least two non-isomorphic* S(2,4,v) *if (and only if)* $v > 16$.

REFERENCE

[1] M. WOJTAS, *On non-isomorphic* BIBDs B(4,1;v), Colloq. Math. 35 (1976) 327-330.

Den Helder 77 08 30 -
Paris 77 09 17
Amsterdam 77 10 27