stichting
mathematisch
centrum

AFDELING ZUIVERE WISKUNDE ZW 136/80 JANUARI
(DEPARTMENT OF PURE MATHEMATICS)

A.E. BROUWER

ON THE EXISTENCE OF 30 MUTUALLY ORTHOGONAL LATIN SQUARES

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).

1980 Mathematics subject classification: 05B15

On the existence of 30 mutually orthogonal Latin squares

by

A.E. Brouwer

ABSTRACT

We show the existence of 30 mutually orthogonal Latin squares of order n for n > 65278, so that $n_{30} \leq 65278$.

KEYWORDS & PHRASES: *transversal design, orthogonal Latin squares*

0. INTRODUCTION

Let $N(v)$ denote the maximum number of mutually orthogonal Latin squares of order v. According to CHOWLA, ERDÖS & STRAUSS [4] we have $\lim_{v\to\infty} N(v) = \infty$ so that we may define n_r as the least integer such that $N(v) \geq r$ if $v > n_r$. It is convenient to put $N(0) = N(1) = +\infty$.

For tables of lower bounds for $N(v)$ $(v<10000)$ and of upper bounds for n_r $(r<16)$ see BROUWER [1,2] and BROUWER & VAN REES [3].

HANANI proved in 1970 [5] that $n_{29} \leq 34115553$, and recently STINSON [6], using Wilson's theorem, improved this considerably, showing that $n_{30} \leq 121605$. (Of course $n_{29} \leq n_{30}$.) Here we shall prove $n_{30} \leq 65278$ using the theorem from Brouwer & van Rees as our main tool. Of course we make a strong use of the fact that 31 and 32 are consecutive prime powers.

1. SOME THEOREMS

THEOREM 1.

$N(0) = N(1) = +\infty$

$N(q) = q-1$ *if* q *is a prime power.*

THEOREM 2. [Bush]

$N(uv) \geq N(u).N(v)$.

THEOREM 3. [Wilson] *If* $0 \leq u \leq t$ *then*

$N(mt+u) \geq \min\{N(m), N(m+1), N(t)-1, N(u)\}$.

THEOREM 4. [Wojtas]

$N(mt+w) \geq \min\{N(m), N(m+1), N(m+w), N(t)-w\}$.

THEOREM 5. [Brouwer]

If $n = mt + u$ *and* $N(t) \geq k+1$, $N(u) \geq k$ *and* $t = \Sigma_{i=1}^{s} h_i$, $u = \Sigma_{i=1}^{s} h_i m_i$ *and (for* $i=1,\ldots,s$*) designs* $T[k+2;m+m_i] - T[k+2;m_i]$ *exist,*

then $N(n) \geq k$.

(For an explanation of the notation $T[k;v] - T[k;u]$: a transversal design with k groups of size v with a 'hole' of size u, see BROUWER [1] and BROUWER & VAN REES [3]. A T[k;v] - T[k;u] certainly exists whenever a T[k;v] with subdesign T[k;u] exists (simply remove the blocks of the subdesign), but we shall see many applications where the existence of T[k;v] itself is unknown.)

PROPOSITION 6. [*A very special case of the theorem of BROUWER & VAN REES*]
If $n = 991t + 32u_1 + u_2 + v$, *where*
$0 \le v \le t$, $u_1 + u_2 \le t$, $N(t) \ge 32$, $N(32u_1+u_2) \ge 30$,
$N(v) \ge 30$ *then* $N(n) \ge 30$.

PROOF. We have to show the existence of

$$T[32,991+a+b] - T[32,a] - T[32,b]$$

for $a \in \{0,1,32\}$ and $b \in \{0,1\}$.

(i) 991 is prime, so T[32,991] exists.

(ii) If we delete one point from PG(2,31) we obtain a pairwise balanced design on $992 = 31^2 + 31$ points with block sizes 31 and 32, where the blocks of size 31 form a parallel class. Hence T[32,992] and therefore also T[32,992]- T[32,1] exists.

(iii) If we delete one point from AG(2,32) we obtain a pairwise balanced design on $1023 = 32^2 - 1$ points with block sizes 31 and 32 where the blocks of size 31 form a parallel class. Hence T[32,1023] - T[32,32] exists.

(iv) Considering PG(2,31) with its $993 = 31^2 + 31 + 1$ points and blocks of size 32 we see that T[32,993] and therefore also T[32,993] - T[32,1] - T[32,1] exists.

(v) Likewise, considering AG(2,32) one sees that T[32,1024] - T[32,32] - T[32,1] exists. □

Of sporadic application is the following theorem (BROUWER [2]):

THEOREM 7. *Let* q *be a prime power,* $0 \le t \le q^2 - q+1$, $n = t(q^2+q+1) + x$.
Let $d_0 = N(x)$, $d_1 = N(t)$, $d_2 = N(t+1)$, $d_3 = N(t+q)$, $d_4 = N(t+q+1)$ (*where* $N(0) = N(1) = \infty$).

Let $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{0,1\}$, *and*

$\varepsilon_1 = 0$ *iff* $x = q^2 - q - t$,

$\varepsilon_2 = 0$ *iff* $x = 1$,

$\varepsilon_3 = 0$ *iff* $x = q^2$,

$\varepsilon_4 = 0$ *iff* $x = t + q + 1$.

Then

(i) *if* $x = 0$ *then* $N(n) \geq \min(d_1, d_3)$,

(ii) *if* $x = t+q$ *then* $N(n) \geq \min(d_1-\varepsilon_3,\ d_3,\ d_4-1)$,

(iii) *if* $x = q^2-q+1-t$ *then* $N(n) \geq \min\ (d_0,\ d_2-\varepsilon_2,\ d_3-1)$,

(iv) *if* $x = q^2+1$ *then* $N(n) \geq \min(d_0,\ d_2-\varepsilon_4,\ d_4-1)$,

(v) *if* $0 < x < q^2-q+1-t$ *then*

$N(n) \geq \min(d_0, d_1-\varepsilon_1,\ d_2-\varepsilon_2,\ d_3-1)$,

(vi) *if* $t+q < x < q^2+1$ *then*

$N(n) \geq \min(d_0,\ d_1-\varepsilon_3,\ d_2-\varepsilon_4,\ d_4-1)$.

Incomplete transversal designs can be found as follows.

THEOREM 8.

(i) *If* $T[k;u]$ *and* $T[k;v]$ *exist, then*

$T[k;uv] - T[k;u]$ *exists.*

(ii) *If* $T[k;m]$, $T[k;m+1]$, $T[k+1;t]$ *exist, then*

$T[k;mt+u] - T[k;u]$ *exists for* $0 \leq u \leq t$.

If moreover $T[k;u]$ *exists, then*

$T[k;mt+u] - T[k;t]$ *exists,*

$T[k;mt+u] - T[k;m]$ *exists if* $u<t$, *and*

$T[k;mt+u] - T[k;m+1]$ *exists if* $u>0$.

(iii) *If* $T[k;m]$, $T[k;m+1]$, $T[k+w;t]$ *exist, then*

$T[k;mt+w] - T[k;m+w]$ *exists.*

If moreover $T[k;m+w]$ exists, then

$T[k;mt+w] - T[k;t]$ *exists,*

$T[k;mt+w] - T[k;m]$ *exists if* $m+w < t+1$, *and*

$T[k;mt+w] - T[k;m+1]$ *exists if* $w>0$.

(iv) $T[k;v] - T[k;1]$ *exists iff* $v\geq 1$ *and* $T[k;v]$ *exists.*

(Parts (i), (ii), (iii) follow from the proofs of Theorems 2,3,4. The other Theorems give analogous results. For example, the design constructed in Theorem 7 has a subdesign of order x. One may put $d_0 = +\infty$ and obtain bounds on k for T[k+2;n] - T[k+2;x].)

2. STINSON'S EXCEPTIONS

Stinson showed N(v) ≥ 30 for v ≥ 100000 with possibly eighteen exceptions. In view of his method and the fibre he indicates, his 101878 should probably be 101828. Let us show how these orders may be treated using the above theorems.

From Theorem 3:

order	m	t	u
(138932	31	4397	2625)
109215	3412	32	31
107206	2614	41	32

From Theorem 4:

order	m	t	w
(185905	127	1459	612)
114766	2799	41	7
109246	31	3457	2079
106975	2609	41	6

From Theorem 5:

order	m	t	u	$\Sigma h_i \times m_i$
121605	3799	32	37	1 × 31 + 6 × 1 + 25 × 0
121515	3793	32	139	4 × 31 + 15 × 1 + 13 × 0
121076	2799	43	719	23 × 31 + 6 × 1 + 14 × 0
119317	3210	37	547	17 × 31 + 20 × 1
118318	3183	37	547	17 × 31 + 20 × 1
108823	3396	32	151	4 × 31 + 27 × 1 + 1 × 0
102927	3209	32	239	7 × 31 + 22 × 1 + 3 × 0
101878	2481	41	157	5 × 31 + 2 × 1 + 34 × 0
101828	2481	41	107	3 × 31 + 14 × 1 + 24 × 0
101625	3173	32	89	2 × 31 + 27 × 1 + 3 × 0
100827	1876	53	1399	45 × 31 + 4 × 1 + 4 × 0
100029	1876	53	601	19 × 31 + 12 × 1 + 22 × 0

From Proposition 6:

order	t	u_1	u_2	$32u_1+u_2$	v
100682	101	16	0	512	79
100515	101	11	31	383	41

(All required estimates can be found in the table [1]. All required transversal designs with holes exits by Theorem 8.)

Using Stinson's results this implies $n_{30} < 100\ 000$.

3. 30 SQUARES

We ran a program with knowledge of Theorems 1-4; of Theorem 5 with $m_1 = 0$, $m_2 = 1$, $m_3 \in \{31,32\}$ (where incomplete transversal designs were found from Theorem 8); of Proposition 6, and of the inequalities $N(2016) \geq 31$ (see [1]) and $N(2395) \geq 42$ (from Theorem 7, see [2]). In the interval $60\ 000 \leq n \leq 300\ 000$ it found 44 possible exceptions (i.e., cases where $N(n) \geq 30$ could not be proved). A much better educated program, with knowledge of most things I know about orthogonal Latin squares, then attacked these 44 cases and killed 34 of them, usually by appealing to Theorem 5 or some other specialization of Brouwer & van Rees' theorem. 67378 is done using a theorem of Van Rees; 60458 by a theorem of Wilson. Let us give these 34 constructions

order	m	t	u	$\Sigma h_i \times m_i$	comment
87435	2728	32	139	30 × 1 + 1 × 31 + 1 × 78	2728=31.88
80900	2458	32	2244	5 × 31 + 2 × 32 + 25 × 81	2539=31.81+28
77901	2042	37	2347	2 × 1 + 35 × 67	2109=31.67+32
77362	2063	37	1031	19 × 0 + 5 × 32 + 13 × 67	2130=31.67+53
76465	2016	37	1873	8 × 0 + 2 × 32 + 27 × 67	2083=31.67+6
72328	2200	32	1928	1 × 1 + 8 × 31 + 23 × 73	2273=31.73+10
70282	1897	37	93	3 * 31	use three levels
70198	1871	37	971	13 × 0 + 17 × 32 + 7 × 61	1932=31.61+41
69531	1307	53	260	8 * 32 + 4 * 1	use twelve levels
69351	1819	37	2048	5 × 32 + 32 × 59	1878=31.59+49
69201	1426	47	2179	30 × 46 + 17 × 47	1426=31.46
69153	1426	47	2131	31 × 45 + 16 × 46	
69148	1426	47	2126	36 × 45 + 11 × 46	

order	m	t	u	$\Sigma h_i \times m_i$
68308	1621	41	1847	$1 \times 0 + 13 \times 32 + 27 \times 53$
68252	1813	37	1171	$8 \times 0 + 20 \times 32 + 9 \times 59$
67378	From prop 11 in [1], with m=1566, r=43, b=37, s=3.			
67294	2038	32	2078	$1 \times 1 + 31 \times 67$
66076	1332	49	808.	$(2 \times 0 + 47 \times 1) + (27 \times 1 + 16 \times 32 + 6 \times 37)$
66045	2011	32	1693	$1 \times 1 + 11 \times 32 + 20 \times 67$
66014	1332	49	746.	$(12 \times 0 + 37 \times 1) + (29 \times 1 + 12 \times 32 + 8 \times 37)$
65762	1332	49	494.	$(12 \times 0 + 37 \times 1) + (36 \times 1 + 12 \times 32 + 1 \times 37)$
65708	1332	49	440.	$(18 \times 0 + 31 \times 1) + (39 \times 1 + 10 \times 37)$
65245	2016	32	733	$17 \times 0 + 2 \times 1 + 4 \times 32 + 9 \times 67$
63201	1951	32	769	$19 \times 0 + 1 \times 1 + 12 \times 64$
62786	1457	43	135.	$(11 \times 0 + 32 \times 1) + (30 \times 0 + 10 \times 1 + 3 \times 31)$
62455	1486	41	1529	$10 \times 1 + 31 \times 49$
60458	From prop 11 in [1], with m=991, r=61, t=7.			
60445	1872	32	541	$1 \times 0 + 14 \times 1 + 17 \times 31$
60434	1621	37	457	$26 \times 0 + 6 \times 32 + 5 \times 53$
60374	1846	32	1302	$6 \times 1 + 10 \times 32 + 16 \times 61$
60248	1457	41	511.	$(9 \times 0 + 32 \times 1) + (12 \times 0 + 14 \times 1 + 15 \times 31)$
60242	961	61	1621	$9 \times 0 + 43 \times 31 + 9 \times 32$
60188	1840	32	1308	$3 \times 1 + 16 \times 32 + 13 \times 61$
60182	1840	32	1302	$6 \times 1 + 10 \times 32 + 16 \times 61$

I cannot do the following ten cases above 60000:

65278, 64718, 61834, 61298, 61198,
60686, 60440, 60392, 60066, 60056.

(I tried the following specialisations of the BR-theorem:

(i) one level only - this is theorem 5.

(ii) two levels, but with weights 0 and 1 on the second level.

(iii) many levels, but on each level only one point of nonzero weight, these points all being contained in a single block:

THEOREM 9. *If* $n = mt + w$ *and* $N(t) \geq k + s$, $N(m) \geq k$, $N(m+w) \geq k$ *and*

$w = \Sigma_{i=1}^{s} w_i$ *where for* $i=1,\ldots,s$ *designs*

$$T[k+2;\ m+w_i] - T[k+2;\ w_i]$$

exist, then

$$N(n) \geq k.$$

[Note that with $w_i = 1 (\forall_i)$ this reduces to Theorem 4, just as Theorem 5 reduces to Theorem 3 if one takes $m_i \in \{0,1\}$ $(\forall_i)$.]

Consequently, in order to attack the above ten cases one should either find a completely new construction, or try more complicated specializations.)

Since 65278 is the largest of these cases we proved

THEOREM 10. $n_{30} \leq 65278$.

REFERENCES

[1] A.E. BROUWER, *The number of mutually orthogonal Latin squares - a table up to order* 10000, Report ZW 123, Math. Centr., Amsterdam, June 1979.

[2] A.E. BROUWER, *A series of separable designs with application to pairwise orthogonal Latin squares*. Report ZW77, Math. Centr., Amsterdam, Aug 1979 (to appear in European J. of Comb.)

[3] A.E. BROUWER & G.H.J. VAN REES, *More Latin squares*, preprint 1979.

[4] S. CHOWLA, P. ERDŐS, & E.G. STRAUS, *On the maximal number of pairwise orthogonal Latin squares of a given order*, Canad. J. Math. 12 (1960) 204-208.

[5] H. HANANI, *On the number of orthogonal Latin squares*, J. Combinatorial Theory 8 (1970) 247-271.

[6] D.R. STINSON, *On the existence of 30 mutually orthogonal Latin squares*, Ars Combinatoria 7 (1979) 153-170.

[7] R.M. WILSON, *Concerning the number of mutually orthogonal Latin squares*, Discrete Math. 9 (1974) 181-198.