BULL. AUSTRAL. MATH. SOC. 20N05, 05B05
VOL. 18 (1978), 221-236.

Stein quasigroups I: Combinatorial aspects

M.J. Pelling and D.G. Rogers

This paper, in conjunction with its algebraic sequel, aims to provide a foundation, long outstanding, to the theory of quasigroups obeying the law $x(xy) = yx$, otherwise known as Stein quasigroups.

1. Introduction

Quasigroups satisfying the law $x(xy) = yx$ seem first to have been considered by Stein [13], in which paper he raised the problem of determining their spectrum. Standard constructions using Galois fields yield possible orders $4^k m$, where the square-free part of m does not contain any prime $p \equiv 2, 3 \pmod 5$ ([10], [13]). Later, in [14], Stein used certain block designs to construct the orders $12k + 1$, $12k + 4$, $20k + 1$, $20k + 5$ for all $k \geq 0$, and in [9] Lindner used the singular direct product of Sade [12] to obtain further orders, including 17. By construction of more elaborate block designs we show (Section 4) that systems exist for all orders greater than 1042. We also apply block design methods to consideration of isomorphisms and automorphisms (Section 5) and to subsystems (Section 6), and in Section 7 we consider further constructions involving a generalisation of the singular direct product and a block design analogue.

It is known [2] that there are Latin squares orthogonal to their transpose of all orders $n \neq 2, 3, 6$. Since any Stein system is orthogonal to its transpose ([13], Section IV) our results provide an

Received 5 January 1978.

additional proof for $n > 1042$.

For further discussion and references see also [3], [4], [5].

2. The method of block designs

In this paper a block design, as originally introduced by Bose and Shrikhande [1], will mean a triple (S, D, K) where S is a set, D a non-empty collection of subsets of S called blocks, and K a set of integers greater than or equal to 2 satisfying:

(i) for any $x \neq y$ in S there is a unique block $B \in D$ containing x and y ;

(ii) if $B \in D$ then $|B| \in K$.

If $|S| = v$ we write $v \in B(K)$ and shall also use $B(K)$ to denote the whole class of block designs with block sizes all in K . The following theorem (Stein [14], Section 4) is the basis of this paper.

THEOREM 1. *Let V be a variety of idempotent quasigroups in which all the defining laws involve at most two variables. Suppose that for every k in a set K of integers greater than or equal to 2 there is a member S_k of V of order k . Then if $v \in B(K)$, there is a member of V of order v .*

Proof. Let (S, D, K) be a block design with $|S| = v$. Then S becomes a member of V if each block of size k is regarded as a system S_k and the binary operation $x.y$ of S is defined (when $x \neq y$) by restriction to the unique block system S_k containing x and y ; $x \cdot x$ is defined to be x . //

For brevity we say that n is an R-number or $R(n)$ if there is a Stein system of order n . The following methods can now be used to construct new R-numbers from previously known ones. For completeness we include the known results.

MO. *$R(p)$ if p is a prime $p \equiv 0, 1, 4 \pmod 5$ and $R(p^2)$ if p is a prime $p \equiv 2, 3 \pmod 5$.*

Proof. In the first case the equation $c^2 + c = 1$ is soluble in the Galois field $GF(p)$, and defining $x \cdot y = c^2x + cy$ turns $GF(p)$ into a

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

Stein system. The same construction works in the second case with the field $GF(p^2)$. //

M1. *If* $R(m)$ *and* $R(n)$ *then* $R(mn)$. //

M2. *Suppose* $v \in B(K)$ *where* $R(k), R(k-1)$ *for each* $k \in K$ *, and let* (S, D, K) *be a block design with* $|S| = v$ *. Suppose that* $S^* \subseteq S$ *forms a subdesign (that is to say, any block containing two elements of* S^* *is a subset of* S^* *) and let* $|S^*| = v^* \geq 0$ *. Then if* $0 \leq m \leq v^*$ *and* $R(m)$ *, then also* $R(v-v^*+m)$ *. If* $S^* = \emptyset$ *, we only need* $R(k)$ *for* $k \in K$ *.*

Proof. Delete $v^* - m$ of the points of S^* leaving a set W of m points. Define a block design on $(S \backslash S^*) \cup W$ by taking as blocks

(i) the blocks in D which do not meet S^* ,

(ii) the blocks of D which meet S^* in one point only, that point being deleted if not in W ,

(iii) W itself.

$R(v-v^*+m)$ follows on applying Theorem 1 to this design. //

M3. *Suppose* $v \in B(K)$ *where* $R(k), R(k+1)$ *for each* $k \in K$ *, and that the design* (S, D, K) *admits* $m \geq 1$ *disjoint resolutions into parallel blocks, that is there are distinct blocks* B_{ij} *,* $1 \leq i \leq m$ *,* $1 \leq j \leq t_i$ *, such that* $S = \bigcup_{j=1}^{t_i} B_{ij}$ *and, for any* i *,* $B_{ij}, B_{ij'}$ *are disjoint when* $j \neq j'$ *. Then if* $R(m)$ *, then also* $R(v+m)$ *.*

Proof. Add new points $a_1, a_2, \ldots, a_m$ and apply Theorem 1 to the design on $S \cup \{a_1, a_2, \ldots, a_m\}$ with blocks:

(i) any block B different from any B_{ij} in D ;

(ii) any set $B_{ij} \cup \{a_i\}$;

(iii) $\{a_1, a_2, \ldots, a_m\}$. //

M4. *Suppose* P *is a subsystem of a* Stein *system* Q *and let* $p = |P|$ *,* $q = |Q|$ *. Then if* $R(q-p)$ *and* $R(v)$ *, then also* $R(v(q-p)+p)$ *. In particular, if* $q = k + 1$ *,* $R(vk+1)$ *is implied by* $R(k), R(k+1), R(v)$ *.*

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

Proof. This is obtained by Lindner's construction [9], using the singular direct product. //

The final three methods (see also [6]) use block designs constructed from T-systems. For an account of T-systems see Hanani [6], whose notation we adopt here.

M5. *If* $t \in T_0(m)$ *and* $R(t+1)$, $R(m)$, *then* $R(mt+1)$.

Proof. Given a T-system with $t \in T_0(m)$, add a new point a^* and define blocks

(i) the t^2 m-tuples of the T-system,

(ii) the sets $\tau_i \cup \{a^*\}$, $1 \le i \le m$, where the τ_i are the t-element sets of the T-system.

A block design with $K = \{m, t+1\}$ results, and Theorem 1 can be applied.//

M6. *If* $t \in T_e(m)$, $R(t)$, $R(m)$, $R(m+1)$, *and* $R(k)$ *for* $k \le e$, *then* $R(mt+k)$.

Proof. Select k parallel sets $D_1, D_2, \ldots, D_k$ of m-tuples in the T-system and let new points $a_1, a_2, \ldots, a_k$ be added. Apply Theorem 1 with blocks:

(i) all m-tuples not in any D_i ;

(ii) the t-element sets τ_i of the T-system;

(iii) all sets $L_i \cup \{a_i\}$ for $L_i \in D_i$, $1 \le i \le k$;

(iv) $\{a_1, a_2, \ldots, a_k\}$. //

M7. *If* $t \in T_e(m)$, $R(t+1)$, $R(m)$, $R(m+1)$, *and* $R(k+1)$ *for* $k \le e$, *then* $R(mt+k+1)$.

Proof. Select k parallel sets $D_1, D_2, \ldots, D_k$ of m-tuples in the T-system and let new points $a, a_1, a_2, \ldots, a_k$ be adjoined. Apply Theorem 1 with blocks:

(i) all m-tuples not in any D_i ;

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

(ii) the $(t+1)$-element sets $\tau_i \cup \{a\}$, $1 \le i \le m$;

(iii) all sets $L_i \cup \{a_i\}$ for $L_i \in D_i$, $1 \le i \le k$;

(iv) $\{a, a_1, a_2, \ldots, a_k\}$. //

3. Known orders up to 116

We now list all known R-numbers up to 116 , briefly justifying each number as listed. For example $92 = 4 \cdot 19 + 16$ (M6) will mean that 92 is an R-number on the basis of M6 with $m = 4$, $t = 19$, $k = 16$. As for the existence of the relevant T-systems we only use the fact [6] that $t \in T_t(m)$ (which implies $t \in T_e(m)$ for $e \le t$) if t is a product of prime powers $p_i^{s_i} \ge m$.

(i) From M0 and M1 we obtain: 1, 4, 5, 9, 11, 16, 19, 20, 25, 29, 31, 36, 41, 44, 45, 49, 55, 59, 61, 64, 71, 76, 79, 80, 81, 89, 95, 99, 100, 101, 109, 116 .

(ii) $17 = 4 \cdot 4 + 1$ (M4 or M5) and then 68, 85 by M1. Also $96 = 5 \cdot 19 + 1$ (M4) .

(iii) $12k + 1$, $12k + 4$, $20k + 1$, $20k + 5$ for $k \ge 0$ by Theorem 1 and known block designs in $B(4)$, $B(5)$ (see [6], [7], [14]) giving with M1: 13, 52, 65, 21, 84, 105, 28, 112, 37, 40, 73, 88, 97 .

(iv) There are resolvable $B(4)$ designs for $v = 12k + 4$ (see [8]); so $R(12k+5)$ by M3, giving 53, 77, 113 .

(v) Applying M2 to the 3-dimensional projective space over GF(4) , the blocks being the lines, by deleting points in a hyperplane we deduce the R-numbers $69 = 64 + 5$, $75 = 64 + 11$, $83 = 64 + 19$.

(vi) Applying M2 to a block design in $B(5)$ with $v = 20k + 1$ or $v = 20k + 5$ and deleting 1, 4 , or 5 points from one of its blocks, we deduce $20k - 4$, $20k - 3$, $20k$, $20k + 4$, giving 24, 56, 57, 60, 104 .

(vii) By [6] there is a design in $B(4)$ with $v = 28$ in which the 63 blocks fall into 9 parallel sets of 7 each. By M3 therefore we obtain $32 = 28 + 4$ and $33 = 28 + 5$; or $33 = 4 \cdot 8 + 1$ (M5) .

(viii) $48 = 4 \cdot 11 + 4$ (M6) , $63 = 4 \cdot 13 + 11$ (M6) , $72 = 4 \cdot 17 + 4$

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

(M6) , $87 = 4\cdot19 + 11$ (M6) , $91 = 4\cdot20 + 11$ (M6) , $92 = 4\cdot19 + 16$ (M6) , $93 = 4\cdot19 + 17$ (M6) , $103 = 4\cdot23 + 11$ (M7) , $108 = 4\cdot23 + 16$ (M7) , $111 = 4\cdot25 + 11$ (M6) .

These results may be collected in a theorem.

THEOREM 2. *The numbers in the following list are possible orders of* Stein *systems*: 1, 4, 5, 9, 11, 13, 16, 17, 19, 20, 21, 24, 25, 28, 29, 31, 32, 33, 36, 37, 40, 41, 44, 45, 48, 49, 52, 53, 55, 56, 57, 59, 60, 61, 63, 64, 65, 68, 69, 71, 72, 73, 75, 76, 77, 79, 80, 81, 83, 84, 85, 87, 88, 89, 91, 92, 93, 95, 96, 97, 99, 100, 101, 103, 104, 105, 108, 109, 111, 112, 113, 116 . //

It should be noted that there are no numbers $4k + 2$ in this list.

4. Possible orders in general

THEOREM 3. *There are* Stein *systems of the following orders:*

(i) *all numbers of the form* $4k + 1$;

(ii) *all numbers of the form* $4k$ *excepting* 8 *and* 12 ;

(iii) *all numbers of the form* $4k + 3$ *excepting* 3 *and* 7 , *and possibly excepting* 15, 23, 27, 35, 39, 43, 47, 51, 67, 107, 115 ;

(iv) 210, 214 , *and all numbers of the form* $4k + 2 > 1042$.

Orders 2, 6, 10, 14 *are not possible.*

Proof. *(i)* If $t = 12k + 1$, $12k + 4$, or $12k + 5$, then $t \in T_t(4)$ and $R(t)$; so, by M6, if $R(v)$, then $R(48k+4+v)$ for $v \le 12k + 1$, $R(48k+16+v)$ for $v \le 12k + 4$, and $R(48k+20+v)$ for $v \le 12k + 5$. With appropriate values of v the following R-numbers are obtained:

$v = 1$	$48k + 5$, 17, 21	$k \ge 0$,
$v = 5$	$48k + 9$, 25	$k \ge 1$,
$v = 9$	$48k + 13$, 29	$k \ge 1$,
$v = 13$	$48k + 33$	$k \ge 1$,
$v = 17$	$48k + 37$	$k \ge 1$,
$v = 21$	$48k + 41$	$k \ge 2$,
$v = 25$	$48k + 45$	$k \ge 2$,

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

$$v = 29 \qquad 48k + 1 \qquad k \geq 3 ;$$

and in conjunction with Theorem 2 this proves part *(i)*.

(ii) Repeat the preceding with values of v as follows:

$v = 0$	gives	$48k + 4,\ 16,\ 20$	$k \geq 0$,
$v = 4$		$48k + 8,\ 24$	$k \geq 1$,
$v = 16$		$48k + 32,\ 36$	$k \geq 1$,
$v = 20$		$48k + 40$	$k \geq 2$,
$v = 24$		$48k + 28,\ 44$	$k \geq 2$,
$v = 28$		$48k$	$k \geq 3$,
$v = 40$		$48k + 12$	$k \geq 4$.

In conjunction with Theorem 2 and the value $156 = 4 \cdot 32 + 28$ (M6) this proves part *(ii)* - that there are no systems of order 8 or 12 is shown in [11].

(iii) That there are no systems of order 3 or 7 is shown in [11]. Applying the preceding method, but including now the case $t = 12k + 8$ for $k \geq 1$ which gives $R(48k+32+v)$ when $R(v)$ and $v \leq 12k + 8$, the following R-numbers are obtained:

$v = 11$	$48k + 15,\ 27,\ 31,\ 43$	$k \geq 1$,
$v = 19$	$48k + 23,\ 35,\ 39$	$k \geq 2$,
$v = 19$	$48k + 3$	$k \geq 2$,
$v = 31$	$48k + 47$	$k \geq 3$,
$v = 55$	$48k + 11$	$k \geq 6$,
$v = 63$	$48k + 19$	$k \geq 7$,
$v = 71$	$48k + 7$	$k \geq 8$.

The following cases must be verified separately.

(a) $48k + 47$ for $k = 2$. Then $143 = 11 \cdot 13$ (M1) .

(b) $48k + 11$ for $k = 3, 4, 5$. Then $155 = 5 \cdot 31$ (M1) , $203 = 4 \cdot 43 + 31$ (M7) , 251 (M0) .

(c) $48k + 19$ for $k = 3, 4, 5, 6$. Then $163 = 4 \cdot 36 + 19$ (M6) , 211 (M0) , $259 = 4 \cdot 60 + 19$ (M6) , $307 = 4 \cdot 72 + 19$ (M6) .

(d) $48k + 7$ for $k = 3, 4, 5, 6, 7$. Then 151 (M0) , 199 (M0) , $247 = 4 \cdot 59 + 11$ (M6) , $295 = 5 \cdot 59$ (M1) , $343 = 4 \cdot 81 + 19$ (M6) .

In conjunction with Theorem 2 this completes the proof of part *(iii)*.

(iv) The impossibility of orders 2, 6, 10, 14 is shown in [11]. We have $210 = 11\cdot19 + 1$ (M4 or M5) and $214 = 11\cdot19 + 5$ (M4). Since $t \in T_t(4)$ for all $t > 51$ (see [8]), parts *(i)-(iii)* and M6 give $R(210+4m)$ for all $m > 210$ and $m \equiv 0, 1, 3 \pmod 4$. So $16k + 1054$, $16k + 1058$, $16k + 1062$ are R-numbers for $k \geq 0$. Similarly $R(214+4m)$ for $m > 214$ and $m \equiv 1 \pmod 4$, giving $16k + 1082$ for $k \geq 0$.

Finally, $1066 = 5\cdot213 + 1$ (M5), $1050 = 5\cdot210$ (M1), $1046 = 5\cdot209 + 1$ (M5). //

COROLLARY. *There are* Stein *systems, and Latin squares orthogonal to their transpose for all orders greater than* 1042. //

In view of the comparative incompleteness of part *(iv)* it is of interest to know whether there are any orders $4k + 2 < 210$.

5. Isomorphism and automorphism

In this section we show how block designs methods can yield interesting results about isomorphisms and automorphisms of Stein systems.

THEOREM 4. *There are at least* 1821 *non-isomorphic* Stein *systems of order* 16 *all of whose* 2 *element generated subsystems are of order* 4.

Proof. The affine plane T over GF(4), regarded as a $B(4)$ block design, can be converted as in Theorem 1 into a Stein system of order 16 by imposing a binary operation on each line to make it an order 4 subsystem. The automorphism group of the unique Stein system of order 4 is the alternating group A_4, and there are 20 lines, so this can be done in 2^{20} different ways. Any isomorphism of two of these systems must map lines to lines and so is also an automorphism of the affine plane T. There are 5760 such automorphisms so the number of non-isomorphic systems is at least $2^{20}/5760$, which exceeds 1820. //

THEOREM 5. *There is a* Stein *system of order* 75 *which admits only the identity automorphism.*

Proof. Let S be the 3-dimensional projective space V over GF(4) with 10 points deleted in a hyperplane H. S is converted into a Stein system by taking blocks as in M2 - the set W of 11 points remaining in

H and the lines not in H of 5 points (if they meet W) or 4 points (if they do not). Any automorphism of S induces an automorphism f of the projective space V, and it suffices to show that W and the binary operations in the blocks can be chosen to force f to be the identity.

Certainly $f(H\backslash W) = H\backslash W$, since W is the unique subsystem of S of order 11. Let l, m be distinct lines in H and $P_1, \ldots, P_5$ be the points of l with $P_5 = l \cap m$. Let additional points P_6, P_7, P_8 be chosen on m in such a way that P_1P_6, P_2P_7, P_3P_8 are collinear in P_9 and P_2P_6, P_3P_7, P_4P_8 are collinear in P_{10}. Taking $H\backslash W = \{P_1, P_2, \ldots, P_{10}\}$, it is easy to see that any projective automorphism of H which leaves $H\backslash W$ invariant must be the identity. It follows that with this choice of W, f must be a translation on the affine space $V\backslash H$.

Now there are 21 directions d_k, $0 \le k \le 20$, in $V\backslash H$ and, apart from the identity, 3 translations in each direction. Let l_k be a line (of 4 or 5 points appropriately) in the direction d_k. The 3 translations in direction d_{k-1} map l_k into 3 new lines l_k^i, $i = 1, 2, 3$, and if in each case the binary operation on l_k^i is chosen different from the translated operation on l_k, then f cannot be a translation in direction d_{k-1}. This can be done for every value of k (mod 21), so that f is forced to be the identity. //

6. Subsystems

In this section we show how block designs can be used to construct Stein systems whose 2 element generated subsystems are of prescribed type; we also give constructions for systems with large subsystems.

LEMMA. *Let K be a set of integers $4k$ $(k \ge 1)$ and K' a set of integers $4k+1$ $(k \ge 1)$. Then $v \in B(K \cup K')$ implies that $v \equiv 0, 1$ (mod 4).*

Proof. It suffices to deal with the finite case $K = \{k_1, \ldots, k_n\}$,

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

$K' = \{k_1', \ldots, k_m'\}$. Let P_j , $1 \le j \le v$, be the points of a $B(K \cup K')$ design and suppose b_{ij} k_i-blocks and b'_{ij} k'_i-blocks contain P_j . Then

$$v - 1 = \sum_{i=1}^{n} b_{ij}(k_i-1) + \sum_{i=1}^{m} b'_{ij}(k'_i-1) \equiv 3\left(\sum_{i=1}^{n} b_{ij}\right) \pmod 4 ,$$

whence

$$v(v-1) \equiv 3 \sum_{i=1}^{n} \left(\sum_{j=1}^{v} b_{ij}\right) \pmod 4 .$$

But $\sum_{j=1}^{v} b_{ij} = N_i k_i \equiv 0 \pmod 4$, where N_i is the total number of k_i-blocks, so that $v(v-1) \equiv 0 \pmod 4$; which proves the lemma. //

THEOREM 6. *$v \in B(4, 5)$ if and only if $v \equiv 0, 1 \pmod 4$, excepting 8, 9, 12 , and possibly excepting 48 . Excluding these exceptions there is a* Stein *system of all such orders v with the property that every 2 element generated subsystem is the system of order 4 or 5 .*

Proof. We have $12k + 1$ and resolvable $12k + 4$ in $B(4)$, $k \ge 0$, so that by M3 also $12k + 5 \in B(4, 5)$. Since $t \in T_t(4)$ for $t = 12k + 1 \ge 4$, it follows by M6 that $48k + 4 + 12j + 4 \in B(4, 5)$ for $0 \le j \le k$, $1 \le k$, and $48k + 4 + 12j + 5 \in B(4, 5)$ for $0 \le j \le k-1$.

So $12i + 8 \in B(4, 5)$ for $i \ge 12$ and $12i + 9 \in B(4, 5)$ for $i \ge 16$, and the remaining cases congruent to $8, 9 \pmod{12}$ are, apart from 8 and 9 , covered by Section 3 (vi) and (vii) or are amongst the following: $68 = 4 \cdot 16 + 4$ (M6) , $69 = 4 \cdot 16 + 5$ (M6) , $92 = 4 \cdot 19 + 16$ (M7) , $93 = 4 \cdot 23 + 1$ (M5) , $128 = 4 \cdot 32$ using $32 \in T_0(4)$, $129 = 4 \cdot 32 + 1$ (M6) , $153 = 4 \cdot 32 + 25$ (M6) , $189 = 4 \cdot 40 + 29$ (M6) .

Hence $12k + 8$ and $12k + 9$ are in $B(4, 5)$ for $k \ge 1$.

Finally $48k + 4 + 12j + 8 \in B(4, 5)$ by M6 for $1 \le j \le k-1$, and the remaining cases congruent to $0 \pmod{12}$ not covered by Section 3 (vi) are, apart from 12 and 48 : $72 = 4 \cdot 17 + 4$ (M6) , $108 = 4 \cdot 23 + 16$ (M7) , $132 = 4 \cdot 28 + 20$ (M6) , $192 = 4 \cdot 44 + 16$ (M6) , $252 = 4 \cdot 56 + 28$ (M6) .

Hence $12k \in B(4, 5)$ for $k \ne 1, 4$. We have not been able to settle

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

the case 48 , but 8 and 12 are impossible since there are no Stein systems of these orders and 9 is impossible because there is no Stein system of order 9 with a subsystem of order 4 or 5 . //

For a similar theorem with $v \equiv 2, 3 \pmod 4$ it is necessary to bring in a block size not of the forms $4k$, $4k + 1$. Adding 11 we have:

THEOREM 7. *$v \in B(4, 5, 11)$ for $v \equiv 3 \pmod 4$, $v \geq 247$, and for $v \equiv 2 \pmod 4$, $v \geq 1198$. For any such v there is a* Stein *system of order v such that any 2 element generated subsystem is of order 4 or 5 or 11 . In particular (by Theorem 6) this is true for* all *$v \geq 1198$.*

Proof. We have $55 \in B(4, 5, 11)$ by $55 = 5 \cdot 11$ and $11 \in T_0(5)$, and $63 \in B(4, 5, 11)$ by $63 = 4 \cdot 13 + 11$ (M6) . Since $t \in T_t(4)$ for $t > 51$, it follows by M6 that $4 \cdot 4k + 55$, $4 \cdot 4k + 63$, $4 \cdot (4k+1) + 55$, $4 \cdot (4k+1) + 63 \in B(4, 5, 11)$ for $k \geq 16$, that is $16i + 7$, $16i + 11$, $16i + 15$ for $i \geq 19$, and $16i + 3$ for $i \geq 20$. This deals with $v \equiv 3 \pmod 4$ for $v \geq 311$, and the remaining cases down to 247 can be proved individually - we omit the details.

Also $210, 214 \in B(4, 5, 11)$ by a T-system modification of M4 (see Section 7), since $210 = 11 \cdot 19 + 1$, $214 = 11 \cdot 19 + 5$, $19 \in T_0(11)$, $20 \in B(4, 5)$, and $24 \in B(4, 5)$ with a subsystem of order 5 . It follows by M6 that $4 \cdot 4k + 210$, $4 \cdot (4k+1) + 214$, $4 \cdot 4k + 214 \in B(4, 5, 11)$ for $4k+1 \geq 214$ and, using the first part, also $4 \cdot (4k+3) + 210 \in B(4, 5, 11)$ for $4k+3 \geq 247$, which completes the proof. //

Almost certainly the lower bounds 247, 1198 which occur in this theorem can be improved.

If a Stein system S has a proper subsystem T then $|S| \geq 3|T| + 1$ (see [*11*]) and equality does sometimes hold. For example if S_n is the n-dimensional projective space over GF(3) considered as a design in $B(4)$, then we may apply Theorem 1 to obtain an ascending chain $S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$ of Stein systems with $|S_n| = \frac{1}{2}(3^{n+1}-1) = 3|S_{n-1}| + 1$. Write $Q(n)$ if there is a Stein system of order n which is a subsystem of one of order $3n + 1$.

THEOREM 8. *If* $n \in T_0(4)$ *and* $Q(n)$ *then* $Q(4n)$.

Proof. We make use of a construction of Hanani ([6], p. 363). Given a T-system for $n \in T_0(4)$, we may in the cartesian $x - y$ plane regard the four n-tuples as four sets of points $A_i = \{(i, y) \mid 0 \le y \le n-1\}$, $i = 0, 1, 2, 3$, and the traversing 4-tuples as graphs $y = y_h(x)$, $0 \le x \le 3$, for $h = 1, 2, \ldots, n^2$.

Similarly $3 \in T_0(4)$ in the $x - z$ plane with traversing 4-tuples $z = z_j(x)$, $1 \le j \le 9$, and we may suppose that $z_1(x) = 0$, $0 \le x \le 3$.

Then $3n \in T_0(4)$ with traversing 4-tuples $(y_h(x), z_j(x))$ if we take the four $3n$-tuples as the sets

$$B_i = \{(i, y, z) \mid 0 \le y \le n-1, 0 \le z \le 2\}$$

for $i = 0, 1, 2, 3$. If the set A_i is identified with $\{(i, y, 0) \mid 0 \le y \le n-1\}$ and $y_h(x)$ with $(y_h(x), z_1(x))$, then $A_i \subseteq B_i$, and the original T-system for $n \in T_0(4)$ is contained in the T-system for $3n \in T_0(4)$.

Adding a new point a^* , the quasigroup multiplication can be defined, since $Q(n)$, to make A_i a subsystem of $B_i \cup \{a^*\}$, and can be defined in the rest of $S = B_0 \cup B_1 \cup B_2 \cup B_3 \cup \{a^*\}$ by separate definition in the 4-tuples of the T-system. Then $A = A_0 \cup A_1 \cup A_2 \cup A_3$ is a subsystem of S , and $|S| = 3|A| + 1$, $|A| = 4n$. //

COROLLARY. $Q(n)$ *holds for* $n = 4^m(3^{k+1}-1)/2$ *and* $m, k \ge 0$. //

7. Other constructions

In this section the singular direct product ([9], [12]) is generalised to a product of n factors, and since the law $x(xy) = yx$ is preserved, it provides another construction of Stein systems. A block design analogue is also considered.

THEOREM 9. *Suppose that* P_i *is a subquasigroup of a quasigroup* Q_i

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

with binary operation g_i , $1 \le i \le n$, *where the* Q_i *are idempotent for* $i > 1$. $P_i = \emptyset$ *is allowed, but not* $P_i = Q_i$, *and the* Q_i *are assumed disjoint as sets. Suppose there is a binary operation* g *on* $W = P_1 \cup P_2 \cup \ldots \cup P_n$ *which makes* W *into a quasigroup with each* $(P_i, g_i|_{P_i})$ *a subquasigroup. Let* $P'_i = Q_i \backslash P_i$ *and suppose that* (P'_i, g'_i) *are idempotent quasigroups for* $1 \le i \le n$. *Then* $(V, *)$ *is a quasigroup, where* $V = \prod_{i=1}^{n} P'_i \cup W$ *and* $*$ *is defined by:*

(i) *if* $x, y \in W$, *then* $x*y = g(x, y)$;

(ii) *if* $x \in P_j$ *and* $y = (y_1, \ldots, y_n) \in \prod P'_i$, *then*

$$x*y = (y_1, \ldots, y_{j-1}, g_j(x, y_j), y_{j+1}, \ldots, y_n)$$

and

$$y*x = (y_1, \ldots, y_{j-1}, g_j(y_j, x), y_{j+1}, \ldots, y_n) ;$$

(iii) *if* $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \prod P'_i$ *and* $x_i \ne y_i$ *for at least two values of* i , *then*

$$x*y = (g'_1(x_1, y_1), \ldots, g'_n(x_n, y_n)) ;$$

(iv) *if* $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \prod P'_i$ *and* $x_i = y_i$ *for* $i \ne j$ *but* $x_j \ne y_j$, *then*

$$x*y = (x_1, \ldots, x_{j-1}, g_j(x_j, y_j), x_{j+1}, \ldots, x_n)$$

if $g_j(x_j, y_j) \in P_j$ *and* $x*y = g_j(x_j, y_j)$ *if* $g_j(x_j, y_j) \in P'_j$;

(v) *if* $x = (x_1, \ldots, x_n) \in \prod P'_i$, *then*

$$x*x = (g_1(x_1, x_1), x_2, \ldots, x_n) \quad \text{if } g_1(x_1, x_1) \in P'$$
$$= g_1(x_1, x_1) \quad \text{if } g_1(x_1, x_1) \in P_1 .$$

The proof is a straightforward verification and is omitted. The Sade singular direct product is the case $n = 2$, $P_2 = \emptyset$, in which case the idempotence condition on (P_1', g_1') can be relaxed.

The following is the block design analogue. Suppose (S, D, K) is a block design such that S admits n partitions $B_{i1}, B_{i2}, \ldots, B_{ik_i}$, $1 \le i \le n$, into disjoint blocks. Let the remaining blocks be B_l, $l = 1, 2, \ldots$, and suppose that the operation g_l on B_l converts it into a Stein system. Suppose also that there are disjoint sets P_i (disjoint from S) and binary operations g_{ij} on $Q_{ij} = P_i \cup B_{ij}$, $1 \le i \le n$, $1 \le j \le k_i$, and g on $W = P_1 \cup P_2 \cup \ldots \cup P_n$ which convert these sets into Stein systems with P_i being the common subsystem of W and Q_{ij}. Then $(S \cup W, *)$ is a Stein system, if $*$ is defined by:

(i) $x*y = g(x, y)$ if $x, y \in W$;

(ii) $x*y = g_{ij}(x, y)$ if $x, y \in B_{ij}$ or $x \in B_{ij}$, $y \in P_i$ or $x \in P_i$, $y \in B_{ij}$;

(iii) $x*y = g_1(x, y)$ if $x, y \in B_1$.

The methods M5, M6, M7 are instances of this construction. Also M4 can be replaced by it provided that a suitable block design exists to replace the singular direct product. For example $214 = 11 \cdot 19 + 5$ and $19 \in T_0(11)$ so that we may take (S, D, K) as the T-system with the 11-tuples and 19-tuples as the blocks and $n = 1$, the B_{1j} as the 19-tuples, and P_1 as the Stein system of order 5 (which is a subsystem of a suitable Stein system of order 24).

The block design analogue also works for other idempotent quasigroups whose defining laws only involve two variables.

References

[1] R.C. Bose and S.S. Shrikhande, "On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler", *Trans. Amer. Math. Soc.* 95 (1960), 191-209.

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

[2] R.K. Brayton, Donald Coppersmith and A.J. Hoffman, "Self-orthogonal Latin squares of all orders $n \neq 2, 3, 6$ ", *Bull. Amer. Math. Soc.* 80 (1974), 116-118.

[3] J. Dénes, A.D. Keedwell, *Latin squares and their applications* (Akadémiai Kiadó, Budapest; English Universities Press, London, 1974).

[4]* Roger Guérin, "Existence et propriétés des carrés latins orthogonaux. I", *Publ. Inst. Statist. Univ. Paris* 15 (1966), 113-213.

[5]* Roger Guérin, "Existence et propriétés des carrés latins orthogonaux. II", *Publ. Inst. Statist. Univ. Paris* 15 (1966), 215-293.

[6] Haim Hanani, "The existence and construction of balanced incomplete block designs", *Ann. Math. Statist.* 32 (1961), 361-386.

[7] Haim Hanani, "A balanced incomplete block design", *Ann. Math. Statist.* 36 (1965), 711.

[8] Haim Hanani, D.K. Ray-Chaudhuri and Richard M. Wilson, "On resolvable designs", *Discrete Math.* 3 (1972), 343-357.

[9] Charles C. Lindner, "Construction of quasigroups satisfying the identity $X(XY) = YX$ ", *Canad. Math. Bull.* 14 (1971), 57-59.

[10] N.S. Mendelsohn, "Combinatorial designs as models of universal algebras", *Recent progress in combinatorics*, 123-132 (Proc. Third Waterloo Conf. Combinatorics, 1968. Academic Press, New York and London, 1969).

[11] M.J. Pelling and D.G. Rogers, "Stein quasigroups (II): algebraic aspects", submitted.

[12] A. Sade, "Produit direct singulier de quasigroupes orthogonaux et anti-abéliens", *Ann. Soc. Sci. Bruxelles Sér. I* 74 (1960), 91-99.

[13] Sherman K. Stein, "On the foundations of quasigroups", *Trans. Amer. Math. Soc.* 85 (1957), 228-256.

* [Unverified references. Editor]

https://doi.org/10.1017/S0004972700008030 Published online by Cambridge University Press

[14] Sherman K. Stein, "Homogeneous quasigroups", *Pacific J. Math.* 14 (1964), 1091-1102.

Balliol College,
Oxford,
England;

Department of Mathematics,
University of Western Australia,
Nedlands,
Western Australia.