Can. J. Math., Vol. XXXIII, No. 6, 1981, pp. 1365–1369

DIRECT PRODUCT OF DERIVED STEINER SYSTEMS USING INVERSIVE PLANES

K. T. PHELPS

1. Introduction. A Steiner system $S(t, k, v)$ is a pair (P, B) where P is a v-set and B is a collection of k-subsets of P (usually called blocks) such that every t-subset of P is contained in exactly one block of B. As is well known, associated with each point $x \in P$ is a $S(t - 1, k - 1, v - 1)$ defined on the set $\mathrm{P}_x = P\backslash\{x\}$ with blocks

$$B(x) = \{b\backslash\{x\} | x \in b \text{ and } b \in B\}.$$

The Steiner system $(P_x, B(x))$ is said to be *derived* from (P, B) and is called (obviously) a *derived Steiner* $(t - 1, k - 1)$-system. Very little is known about derived Steiner systems despite much effort (cf. [**11**]). It is not even known whether every Steiner triple system is derived.

Steiner systems are closely connected to equational classes of algebras (see [**7**]) for certain values of k. In particular one can define an equational class and hence a direct product for Steiner (t, k)-systems only when $t = 2$ and k is a prime power or $t = 3$ and $k = 4$ (see [**6**], [**7**]). Thus it makes sense to talk of the direct product of an $S(2, q, n)$ and an $S(2, q, m)$ as an $S(2, q, nm)$, at least when q is a prime power.

One of the first results on derived designs was actually a construction of a Steiner quadruple system $S(3, 4, 3n + 1)$ from an $S(3, 4, n + 1)$ [**8**]. This has been generalized so that the direct product of derived triple systems is a derived triple system ([**1**], [**14**], [**11**]). That is, if there exists an $S(3, 4, n + 1)$ and an $S(3, 4, m + 1)$ then there exists an $S(3, 4, nm + 1)$. The main purpose of this note is to extend these results to Steiner $(3, q + 1)$-systems. Since these results hinge on the existence of orthogonal arrays we will need to consider known results in this area first.

2. Orthogonal arrays. An n^t by k array with entries from an n-set N, with the property that for any choice of t columns, the n^t t-tuples formed from the rows are all different, is called an orthogonal array of order n, depth k and strength t (and index unity [**13**]). Let us denote such an orthogonal array by $OA(t, k, n)$. (Note that when $t = 2$ such an orthogonal array is equivalent to a set of $k - 2$ mutually orthogonal latin squares of order n.) The following results can be found in [**13**]:

Received May 30, 1980 and in revised form July 27, 1980.

https://doi.org/10.4153/CJM-1981-105-7 Published online by Cambridge University Press

THEOREM 2.1 [**3**]. *There exists an* $OA(t, q + 1, q)$ *whenever* q *is a prime power and* $t < q$. *If* $q = 2^r$ *then there exists an* $OA(t, q + 2, q)$.

LEMMA 2.2 [**4**]. *If there exists an* $OA(t, k, n)$ *and an* $OA(t, k, m)$ *then there exists an* $OA(t, k, nm)$.

From the construction of $OA(t, q + 1, q)$ when q is a prime power, one obtains Corollary 2.3 below. A sketch of the proof for $t = 3$ is provided as this is all that we require.

COROLLARY 2.3. *If* (a_{ij}) *is the* $q^3 \times (q + 1)$ $OA(3, q + 1, q)$ *where* $a_{ij} \in \{1, 2, \ldots, q\}$ *then one can assume that* $a_{ij} = i$ *for* $j = 0, 1, \ldots, q$ *and for* $i = 1, 2, \ldots, q$.

Proof. (cf. [**13**]). Let $GF(q) = \{b_1, b_2, \ldots, b_q\}$ and let $f_i(x)$, $i = 1, 2, \ldots, q^3$ be all polynomials of degree 2 or less with coefficients from $GF(q)$ Define $\bar{a}_{ij} = k$ if and only if $f_i(b_j) = b_k$ for $i = 1, 2, \ldots, q^3, j = 1, 2, \ldots q$. Define $\bar{a}_{i0} = k$ if and only if the leading coefficient of $f_i(x)$ is b_k. Let us assume that $f_j(x) = b_j x^2 + x + 1$ for $j = 1, 2, \ldots q$. Clearly then $\bar{a}_{ji} \neq \bar{a}_{ki}$ for any $j, k \in \{1, 2, \ldots, q\}, j \neq k$. Define a permutation α_i for $i = 0, 1, \ldots, q$, by $\alpha_i(\bar{a}_{ji}) = j$ for each $j = 1, 2, \ldots, q$. Finally let $a_{ij} = \alpha_j(\bar{a}_{ij})$ for $i = 1, 2, \ldots, q^3$ and $j = 0, 1, 2, \ldots q$. Then (a_{ij}) will be an $OA(3, q + 1, q)$ which will have the desired rows.

Finally the following observation was first made by A. E. Brouwer [**2**]:

LEMMA 2.4. *If there exists a* $S(3, q + 1, n + 1)$, *where* q *is a prime power, then there exists an* $OA(3, q + 1, n)$.

Proof. Let G be a sharply triply transitive permutation group acting on the set $X = \{0, 1, \ldots, q\}$ and define

$$D(X) = \{(0^g, 1^g, \ldots, x^g, \ldots, q^g) | g \in G\},$$

i.e., $D(X)$ is a collection of row vectors defined on the set X. Let Y be a q-set and $A(Y)$ be the $OA(3, q + 1, q)$ constructed in Corollary 2.3 above. If (P, B) is the $S(3, q + 1, n + 1)$, then for $\infty \in P$ the collection $B' = \{b \backslash \{\infty\} | b \in B\}$ is a 3-design on $P \backslash \{\infty\}$ with block sizes q and $q + 1$. Let $B' = B(\infty) \cup BB$ where $B(\infty)$ are the blocks of the derived $S(2, q, n)$ and BB is the collection of $(q + 1)$-subsets in B'. Define the following collection of distinct row vectors:

$$OA = \{D(b) | b \in BB\} \cup \{A(b) | b \in B(x)\}.$$

First OA contains n^3 distinct row vectors; for each $b \in BB$, $D(b)$ contains $q^3 - q$ row vectors; for each $b \in B(\infty)$, $A(b)$ has q^3 row vectors but q of these are of the form $(y, y, \ldots, y)$ for each $y \in b$ so ignoring these we have $q^3 - q$ as well. Since $|B'| = (n^3 - n)/(q^3 - q)$ this gives us $n^3 - n$ row vectors not counting the n row vectors $(y, y, \ldots, y)$, $y \in P \backslash \{\infty\}$. So

https://doi.org/10.4153/CJM-1981-105-7 Published online by Cambridge University Press

OA has n^3 row vectors and thus it is equivalent to an $n^3 \times (q + 1)$ array which is in fact an orthogonal array of strength 3.

Note that G does not have to be group and as Brouwer remarked there are sets of permutations which are sharply 3-transitive.

3. Product constructions. A Sterner system $S(3, q + 1, q^2 + 1)$ is known as an inversive plane; the derived design $S(2, q, q^2)$ is always an affine plane. It is well known that such inversive planes exist whenever q is a prime power (cf. [**5**]) and of course they may exist for other values of q as well.

Suppose that there exists an $S(3, q + 1, n + 1)$ on a set of $P \cup \{\infty\}$ with B as the collection of blocks. Let (P, B^*) denote the points and blocks of the derived $S(2, q, n)$. Let us assume there exists an $S(3, q + 1, q^2 + 1)$ as well as an $OA(3, q + 1, q)$ and an $OA(3, q + 1, n)$. Finally let $(Q \cup \{\infty\}, C)$ be the point set and block collection for an $S(3, q + 1, m + 1)$ and let (Q, C^*) denote the derived $S(2, q, m)$ as before. Then we have the following construction of an $S(3, q + 1, nm + 1)$ on $P \times Q \cup \{\infty\}$:

(1) For each $b \in B^*$ and $c \in C^*$ form an $S(3, q + 1, q^2 + 1)$ on the set $\{\infty\} \cup (b \times c)$ so that $\{\infty\} \cup (b \times \{i\})$ is a block for each $i \in c$ and $\{\infty\} \cup (\{j\} \times c)$ is a block for each $j \in b$. (Here we use the property that the derived design is an affine plane.) Let $X_{b,c}$ denote the collection of blocks for this $S(3, q + 1, q^2 + 1)$, then $X_{b,c} \subset D$.

(2) For each $b \in B$, where $\infty \notin b$ and for each $c \in C^*$ consider an $OA(3, q + 1, q)$ on the set c. Assuming that $b = \{x_0, x_1, \ldots, x_q\}$ then

$$\{(x_j, a_{ij}) | j = 0, 1, , , q\} \in D \quad \text{for } i = 1, 2, \ldots, q^3$$

where $a_{ij} \in C$ is the entry in row i, column j of the chosen $OA(3, q + 1, q)$. (Let us assume that (a_{ij}) is as in Corollary 2.3.)

(3) For each $c \in C$ where $\infty \notin c$ choose an $OA(3, q + 1, n)$, (r_{ij}); then assuming $c = \{y_0, y_1, \ldots, y_q\}$ we have

$$\{(r_{ij}, y_j) | j = 0, 1, \ldots, q\} \in D \quad \text{for each } i = 1, 2, \ldots, q^3.$$

THEOREM 3.1. *$(P \times Q \cup \{\infty\}, D)$ as defined above is an $S(3, q + 1, nm + 1)$.*

Proof. We must show that every triple of $P \times Q \cup \{\infty\}$ is contained in exactly one block of D.

(a) $\{\infty, (x, y), (x', y')\}$. Suppose $x \neq x'$ then there exists a unique block $b \in B^*$ containing $\{x, x'\}$. If $y = y'$ then this triple is in the unique block $\{\infty\} \cup (b \times \{y\})$ otherwise it must be in a unique block of the $S(3, q + 1, q^2 + 1)$ defined on $\{\infty\} \cup (b \times c)$ where $\{y, y'\} \subset c \in C^*$.

(b) $\{(x, i), (x, j), (y, j)\}$. There exists a unique $b \in B^*$ and $c \in C^*$ such that $\{x, y\} \subset b$ and $\{i, j\} \subset c$. This triple is contained in a unique block of the $S(3, q + 1, q^2 + 1)$ on $\{\infty\} \cup (b \times c)$.

https://doi.org/10.4153/CJM-1981-105-7 Published online by Cambridge University Press

(c) $\{(x, i), (y, i), (z, j)\}$. $\{x, y, z\}$ is contained in a unique block $b \in B$ and $\{i, j\}$ is contained in a unique block $c \in C^*$. If $b \backslash \{\infty\} \in B^*$ then, as before, this triple is contained in a unique block of type (1) otherwise it will be contained in a unique block of type (2).

(d) $\{(x, i), (x, j), (y, k)\}$. The argument is similar to case (c) above; there exists a unique $b \in B^*$ containing $\{x, y\}$ and a unique $c \in C$, $\{i, j, k\} \subset c$. If $\infty \in c$ (i.e., $c \backslash \{\infty\} \in C^*$) then this triple is contained in a unique block of type (1) otherwise it will be contained in a unique block of type (3).

(e) $\{(x, i), (y, i), (z, i)\}$ or $\{(x, i), (x, j), (x, k)\}$. There exists a unique block, $b \in B$, containing $\{x, y, z\}$. If $\infty \in b$ then this triple is contained in the unique block $\{\infty\} \cup (b \backslash \{\infty\}) \times \{i\}$; otherwise it is contained in a unique block of type (2) because the $OA(3, q + 1, q)$ used contains rows of the form $(a_{ij} = i | j = 0, 1, \ldots, q)$ for each $i = 1, 2, \ldots, q$. For the triple $\{(x, i), (x, j), (x, k)\}$ the argument is similar but much simpler because since it will be contained in a unique block of type (1) or type (3); no special assumptions about the $OA(3, q + 1, n)$ are necessary.

(f) $\{(x, i), (y, j), (z, k)\}$. $\{i, j, k\}$ is contained in a unique $c \in C$. If $\infty \notin c$ then this triple will be contained in a unique block of type (3); if $\infty \in c$ then $\{x, y, z\}$ will be contained in a unique block $b \in B$. If $\infty \notin b$ then this triple is contained in a unique block of type (2); otherwise it will be contained in a unique block of type (1).

Since most of the assumptions needed in this construction are valid whenever q is a prime power we have the following corollaries:

COROLLARY 3.2. *If there exists an $S(3, q + 1, n + 1)$ and an $S(3, q + 1, m + 1)$ where q is a prime power then there exists an $S(3, q + 1, nm + 1)$.*

Proof. This follows from Lemmas 2.1 and 2.4 and Theorem 3.1.

COROLLARY 3.3. *If there exists an $S(3, q + 1, m + 1)$ where q is a prime power, then there exists an $S(3, q + 1, qm + 1)$.*

In closing this section we remark that the construction presented allows for a significant amount of freedom; the consequence of this is that as m (or n) grows the number of nonisomorphic systems that can be constructed increases. To illustrate this point take Corollary 3.3 and consider only the blocks of type (3) in the construction of the $S(3, q + 1, qm + 1)$. Let c be the number of distinct $OA(3, q + 1, q)$ then $(q!)^{q-2}$ is a trivial lower bound for c. Let r be the number of blocks of an $S(3, q + 1, m + 1)$ which do not contain a fixed point ∞, then

$$r = \frac{(m + 1)m(m - 1)}{(q + 1)q(q - 1)} - \frac{m(m - 1)}{q(q - 1)}.$$

Now one can construct c^r distinct $S(3, q + 1, qm + 1)$ from the same $S(3, q + 1, m + 1)$ and as c^r grows faster then $(qm + 1)!$ we have that

https://doi.org/10.4153/CJM-1981-105-7 Published online by Cambridge University Press

the number of non-isomorphic $S(3, q + 1, qm + 1)$ increases with m. This argument is presented in more detail in [**11**] for the case $q = 3$.

4. Problems. Since Steiner quadruple systems, (i.e., $S(3, 4, n)$) are also co-extensive with a variety of algebras it is natural to ask whether similar results hold for $S(4, 5, n + 1)$. Unfortunately an analogous construction fails to work because one needs a 4-skein of order 4 such that $g(x, x, x, x) = x$ and every 2-generated sub-4-skein has order 2. (A 4-skein defined on an n-set N is a mapping $g: N^4 \rightarrow N$ such that the $n^4 \times 5$ array with row vectors $(x, y, z, w, g(x, y, z, w))$ is an $OA(4, 5, n)$.) So the question as to whether a direct product of derived Steiner quadruple systems is derived remains open.

Finally E. Mendelsohn [**9**] has shown that the direct product of "derived" Steiner loops is derived, cf. [**11**]. R. Quackenbush [**12**] has shown that a loop product (or idempotent reduct) theorem exists for $(2, k)$-Steiner systems for certain other values of k. Can E. Mendelsohn's results be generalized to these designs?

Acknowledgements. The author would like to thank Alex Rosa and Eric Mendelsohn for their support and assistance.

References

1. I. S. Ŏ. Aliev, *Simmetričeskije algebry i sistemy Štejenera*, Dok. Akad, Nauk. SSR *174* (1967), 511–513; English translation: *Symmetric algebras and Steiner systems*, Soviet Math. Kokl. *8* (1967), 651–653.

2. A. E. Brouwer, Private Communication, Montreal (1978).

3. K. A Bush, *Orthogonal arrays of index unity*, Ann. Math. Stat. *23* (1952), 426–434.

4. ——— *A generalization of a theorem due to MacNeish*, Ann. Math. Stat. *23* (1952), 293–295.

5. P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin, 1968).

6. B. Ganter and H. Werner, *Equational classes of Steiner systems*, Algebra Univ. *5* (1975), 125–140.

7. ——— *Co-ordinatizing Steiner systems*, Annals of Discrete Math. *7* (1980), (to appear).

8. H. Hanani, *On quadruple systems*, Can. J. Math. *12* (1960), 145–147.

9. E. Mendelsohn, *The smallest non-derived Steiner triple system is simple as loop*, Algebra Universalis *8* (1978), 256–259.

10. K. T. Phelps, *Rotational quadruple systems*, Ars Combinatoria *4* (1977), 177–185.

11. ——— *A survey of derived triple systems*, Annals of Discrete Math. *7* (1980).

12. R. Quackenbush, *Near vector spaces over $GF(q)$ and $(v, q + 1, 1)$-BIBD's*, Linear Alg. Appl. *10* (1975), 259–266.

13. D. Raghavarao, *Constructions and combinatorial problems in the design of experiments* (John Wiley & Sons, New York, 1971).

14. B. Rokowska, *Some new constructions of 4-triple systems*, Colloq. Math. *17* (1967), 111–121.

McMaster University,
Hamilton, Ontario

https://doi.org/10.4153/CJM-1981-105-7 Published online by Cambridge University Press