NESTED STEINER n-CYCLE SYSTEMS AND PERPENDICULAR ARRAYS

A. Granville
Department of Mathematics
University of Toronto
Toronto, Ontario
A. Moisiadis
Department of Mathematics Queen's University
Kingston, Ontario
R. Rees
Department of Mathematics
Mount Allison University
Sackville, New Brunswick
Canada

Abstract. We prove that for any odd positive integer $n > 1$ and for any sufficiently large integer $v > v_0(n)$, there exists a Nested Steiner n-Cycle System of order v if and only if $v \equiv 1 \pmod{2n}$. This gives rise to many new classes of perpendicular arrays.

1. Introduction.

In this paper, we are interested in a certain generalization of a Nested Steiner Triple System. A *Steiner Triple System*, STS(v), is a partition of the edge set of K_v into triangles (3-cycles); and is said to be *nested* if one can add a point to each triangle, obtaining a partition of the edges of $2K_v$ into K_4s. An *n-Cycle System of order* v, CS(v,n), is a partition of the edge set of K_v into n-cycles; and is said to be *nested* if one can add a point to each n-cycle in the system, obtaining a partition of the edges of $2K_v$ into '*wheels with n spokes*'(the original cycle being the rim and the added vertex, the *hub*).

These designs have been investigated by Lindner, Rodger and Stinson [3] and Stinson [5], [7]; and have been shown to exist in almost every case in which the necessary condition $v \equiv 1 \pmod{2n}$ holds.

A *Steiner n-Cycle System of order* v, SCS(v,n), is a CS(v,n) with the additional property that for each k with $1 \leq k < n/2$, any given pair of points is at distance k from one another in exactly one of the cycles: In other words, if $\{C_1, C_2, \ldots, C_m\}$ are the cycles of the CS(v,n) and $C_j^{(k)}$ is the graph defined by the vertices of C_j with edges between vertices that are at distance k in C_j, then the edges of $C_1^{(k)}, C_2^{(k)}, \ldots, C_m^{(k)}$ form a partition of the edge set of K_v for each k, $1 \leq k < n/2$ (in fact, a CS(v,r) where $r = n/gcd(n,k)$). For example, a SCS(v, 3) is just a STS(v), and a SCS(v, 4) is a CS(v, 4). A Steiner 5-cycle system is called a *Steiner Pentagon System* and is known to exist if and only if $v \equiv 1$ or 5(mod 10) and $v \not\equiv 15$ (see

[2]). General Steiner n-cycle systems do appear in the literature as they are equivalent to cyclic perpendicular arrays: A *perpendicular array*, PA(v, n), is a $\binom{v}{2} \times n$ array, each cell containing an integer from the set $\{1, 2, \ldots, v\}$, such that any given pair of columns contain all $\binom{v}{2}$ unordered pairs from the set $\{1, 2, \ldots, v\}$. A *cyclic perpendicular array*, CPA(v, n), is a PA(v, n) with the extra property that $x_2, x_3, \ldots, x_n, x_1$ is a row of the array whenever $x_1, x_2, \ldots, x_n$ is. Thus, a CPA(v, n) has $\frac{1}{n}\binom{v}{2}$ *generator rows*, the entire array being formed by cyclically shifting each generator row n times.

Lemma 1.1. *For any odd integer $n > 1$, there exists a SCS(v, n) if and only if there exists a CPA(v, n).*

Proof: The $\frac{1}{n}\binom{v}{2}$ cycles of an SCS(v, n) can be viewed precisely as the $\frac{1}{n}\binom{v}{2}$ generator rows of a CPA(v, n); and vice-versa. ∎

Cyclic perpendicular arrays have what Stinson refers to as the *pair-column balanced* property, that is, among all the rows in the array containing a given pair x and y, each of x and y occurs $(n-1)/2$ times in each column. This is important in constructing certain optimal private-key cryptosystems (for a full discussion of the relationship between perpendicular arrays and theoretically secure codes, see Stinson [6]).

A SCS(v, n) is *nested* if we nest the underlying CS(v, n). Similarly, a CPA(v, n) is *nested* if we can adjoin a column to the array and so produce a PA$(v, n+1)$ with the property that $x_2, x_3, \ldots, x_n, x_1, y$ is a row of the array whenever $x_1, x_2, \ldots, x_n, y$ is (the resulting array is called *1-rotational*). We have the following analogue of Lemma 1.1.

Lemma 1.2. *For any odd integer $n > 1$, there exists a nested SCS(v, n) if and only if there exists a nested CPA(v, n).*

Example:

	1,2,4,0	
	2,4,1,0	
	4,1,2,0	5,6,1,4
1,2,4; 0	2,3,5,1	6,1,5,4
2,3,5; 1	3,5,2,1	1,5,6,4
3,4,6; 2	5,2,3,1	6,0,2,5
4,5,0; 3	3,4,6,2	0,2,6,5
5,6,1; 4	4,6,3,2	2,6,0,5
6,0,2; 5	6,3,4,2	0,1,3,6
0,1,3; 6	4,5,0,3	1,3,0,6
	5,0,4,3	3,0,1,6
	0,4,5,3	
A nested SCS(7, 3) (i.e., a nested STS(7))	Corresponding nested CPA(7, 3) (i.e., a 1-rotational PA(7, 4))	

In [7] it was shown that there exists a nested SCS(v, 3) if and only if $v \equiv 1 \pmod 6$; and recently Stinson [5] has constructed SCS(v, 4) for all $v \equiv 1 \pmod 8$ except $v = 57, 65, 97, 113, 185, 265$.

In this paper, we will construct a nested SCS(v, n) whenever n is an odd integer and v is a prime power congruent to 1 (mod $2n$). Since, for each n, the set $\{v$: there exists a nested SCS(v, n)$\}$ is PBD-closed, this will enable us to apply Wilson's theorem to obtain asymptotic results on the existence of these designs.

2. Direct constructions for nested SCS(v, n)s.

Theorem 2.1. *For any odd integer $n > 1$ and prime power v with $v \equiv 1$ (mod $2n$), there exists a nested SCS(v, n).*

Proof: Let g be a primitive element in the field F with v elements and let $t = g^{2m}$ where $m = (v-1)/2n$. Label the vertices of K_v with the elements of F. For each $a \in F$ and integer i, $0 \leq i \leq m-1$, let $C_{a,i}$ be the n-cycle with vertices $a + t^j g^i$, $0 \leq j \leq n-1$, where $a + t^j g^i$ is adjacent to $a + t^{j-1} g^i$ and $a + t^{j+1} g^i$; and let $B_{a,i}$ be the *star* in which vertex a is adjacent to the vertices of $C_{a,i}$.

We observe that if $d \neq 0$ and x and y are any two vertices of F then exactly one of $(x-y)/d$ and $(y-x)/d$ may be written in the form $t^j g^i$ where $0 \leq i \leq m-1$ (as $-1 = g^{nm} = t^{(n-1)/2} g^m$).

Fix d, and for any two vertices x_1 and x_2 let y, z be the permutation of x_1 and x_2 such that $y - z$ may be written in the form $dt^j g^i$ where $0 \leq i \leq m-1$.

For $d = 1$ we have $y = z + t^j g^i$ so that the edge (y, z) exists in $B_{z,i}$.

For each k, $1 \leq k < n/2$, let $C_{a,i}^{(k)}$ be defined from $C_{a,i}$ by joining the vertices at distance k, and let $d = t^k - 1$. Then $y = z + (t^k - 1)t^j g^i$, and if $a = z - t^j g^i$ then $y = a + t^{j+k} g^i$ and so the edge (y, z) exists in $C_{a,i}^{(k)}$.

Thus, for any pair of distinct vertices x_1, x_2 in K_v the edge (x_1, x_2) appears in each of the sets of graphs $\{B_{a,i}: a \in F, 0 \leq i \leq m-1\}$ and $\{C_{a,i}^{(k)}: a \in F, 0 \leq i \leq m-1\}$ for each k, $1 \leq k < n/2$. But each of these sets of graphs contain exactly $\binom{v}{2}$ edges, and so it is clear that no edge is counted twice and, therefore, they each partition the edge set of K_v. ∎

Remark 1: The nested SCS(v, n) constructed in the above theorem has the additive group of F as a point-transitive group of automorphisms.

Remark 2: We may replace the set $\{1, g, g^2, \ldots, g^{m-1}\}$ in the construction of the $C_{a,i}$s by any set of representatives of the cosets of the subgroup $\langle -t \rangle$ in F^* to get another, often non-isomorphic, construction.

Examples:

A nested SCS(11,5):	1, 4, 5, 9, 3; 0	(mod 11)
	1, 2, 4, 8, 16; 0	
A nested SCS(31,5):	3, 6, 12, 24, 17; 0	(mod 31)
	5, 10, 20, 9, 18; 0	

3. Asymptotic existence of nested SCS(v, n)s.

Lemma 3.1. *If there exists a nested CS(v, n) then $v \equiv 1$ (mod $2n$).*

Proof: As the cycles of a CS(v, n) form a decomposition of th edges of K_v, so every vertex appears in these cycles equally often; and so, as the edge set of the *wheels* forms a decomposition of $2K_v$, thus, every vertex appears as the *hub* of the wheel equally often, say t times. Therefore, vt = the number of wheels $= (1/n)\binom{v}{2}$ so that $t = (v-1)/2n$ and we see that $v \equiv 1 \pmod{2n}$. (This Lemma was stated, without proof, in [3]). ∎

We have already shown, in Section 2, that this condition is sufficient whenever v is a prime power. More examples of these designs can be obtained by applying MacNeish's Theorem [4]:

Theorem 3.2. *For any odd integer $n > 1$, and positive integer v, a product of prime powers, which are each congruent to 1 (mod $2n$), there exists a nested SCS(v, n).*

Proof: Let $v = q_1 q_2 \dots q_r$ be the prime power decomposition of v where $q_1 > q_2 > \dots > q_r$. By MacNeish's Theorem there is a transversal design with q_i groups of size $q_1 q_2 \dots q_{i-1}$ for each i, $2 \le i \le r$.

In this way we can construct a pairwise balanced design on v points with block sizes $q_1, q_2, \dots, q_r$. Constructing a nested SCS on each block yields a nested SCS(v, n), as desired. ∎

In the remainder of this section we will show that the necessary condition of Lemma 3.1 is sufficient, provided that v is large enough compared to n. We do this by applying Wilson's Theorem (see [1]):

Theorem 3.3. *[Wilson] Let K be any set of integers, and define $\alpha(K) = gcd\{k-1 : k \in K\}$ and $\beta(K) = gcd\{k(k-1) : k \in K\}$. There is an integer c_K such that if $v \ge c_K$, $v - 1 \equiv 0$ (mod $\alpha(K)$) and $v(v-1) \equiv 0$ (mod $\beta(K)$), then there exists a pairwise balanced design on v points having block sizes from the set K.*

Lemma 3.4. *Given any positive even integer m there exist primes p and q for which $p \equiv q \equiv 1 \pmod m$, and $gcd\{p(p-1), q(q-1)\} = m$.*

Proof: By using Dirichlet's Theorem on the existence of primes in arithmetic progressions choose p to be any prime with $p \equiv m+1 \pmod{m^2}$. Observe that $(p-1)/m \equiv p \equiv 1 \pmod m$ so that $gcd\{p(p-1)/m, m\} = 1$; therefore, by the Chinese Remainder Theorem, we may select an integer r with $r \equiv 1$ (mod m) and $r \equiv -1 \pmod{p(p-1)/m}$. By again applying Dirichlet's Theorem we choose q to be any prime satisfying $q \equiv r \pmod{p(p-1)}$ so that $q \equiv 1$ (mod m). It remains to be shown that $gcd\{p(p-1), q(q-1)\} = m$.

Now $q \equiv r \equiv -1 \pmod{p(p-1)/m}$ so that $q(q-1) \equiv 2$ (mod $p(p-1)/m$). But $p \equiv (p-1)/m \equiv 1 \pmod m$ so that $p(p-1)/m$ is odd and, therefore, $gcd\{q(q-1), p(p-1)/m\} = 1$. Recalling that $q \equiv 1 \bmod m$, we have $gcd(p(p-1), q(q-1)) = m$ as required. ∎

We can now prove

Theorem 3.5. *For any odd positive integer $n > 1$ there exists an integer c_n such that if $v \geq c_n$ then there exists a nested SCS(v, n) if and only if $v \equiv 1$ (mod $2n$).*

Proof: From Lemma 3.4 we can chose primes p and q such that $p \equiv q \equiv 1$ (mod $2n$) and $gcd\{p(p-1), q(q-1)\} = 2n$. Applying Wilson's Theorem (3.3) with $K = \{p, q\}$, (so that $\alpha(K) = \beta(K) = 2n$), there exists an integer c_n such that whenever $v \geq c_n$ and $v \equiv 1 \pmod{2n}$ then there is a pairwise balanced design on v points with block sizes p and q. Since $p \equiv q \equiv 1$ (mod $2n$) we can construct a nested SCS on each block (Theorem 2.1), to obtain a nested SCS(v, n) as desired. ∎

References

1. A.E. Brouwer, *Wilson's Theory*, Math. Centre Tracts **106** (1979), 75 - 88, in "Packing and Combinatorics," ed. A. Schrijver.
2. C.C. Lindner and D.R. Stinson, *Steiner pentagon systems*, Discrete Maths. 52 (1984), 64 - 74.
3. C.C. Lindner, C.A. Rodger and D.R. Stinson, *Nesting of cycle systems of odd length*, Annals of Discrete Math. (to appear).
4. H.F. MacNeish, *Euler squares*, Ann. of Math. 23 (1922), 221 - 227.
5. D.R. Stinson, *On the spectrum of nested 4-cycle systems*, Utilitas Math. (to appear).
6. D.R. Stinson, *A construction for authentication/secrecy codes from certain combinatorial designs*, J. of Cryptology (to appear).
7. D.R. Stinson, *The spectrum of nested Steiner triple systems*, Graphs and Combinatorics **1** (1985), 189 - 191.