Discrete Mathematics 67 (1987) 107–110
North-Holland

NOTE

A CONSTRUCTION OF CYCLIC STEINER TRIPLE SYSTEMS OF ORDER p^n

K.T. PHELPS
School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, U.S.A.

Received 4 March 1986
Revised 11 December 1986

1. Introduction

A Steiner triple system of order n is a pair (Z_n, B) where Z_n is the set of integers modulo n and B is a collection of triples of Z_n such that every pair of elements of Z_n is contained in exactly one triple of B. The triple system is said to be cyclic if the cyclic group $\langle Z_n, +\rangle$ is a subgroup of the automorphism group of (Z_n, B). Steiner triple systems of order n (briefly STS(n)) exist for all $n \equiv 1$ or 3 (mod 6) and cyclic STS(n) (briefly CSTS(n)) exist for all $n \equiv 1$ or 3 (mod 6) except $n = 9$ (Peltesohn [8]). A multiplier, $a \in Z_n$, is a unit in the ring of integers modulo n. A multiplier automorphism (isomorphism) of a CSTS(n) is an automorphism (isomorphism) of the form $f(x) \equiv ax \pmod n$.

In this note we present constructions for cyclic STS(p^n), for primes $p \equiv 1$ (mod 6), which have a number of interesting properties. The first and foremost of these is that they have isomorphic mates which are also CSTS(p^n) but for which there is no multiplier isomorphism. The existence of such systems was first proved by N. Brand [1], thereby disproving a long-standing conjecture of Bays–Lambossy (cf. [3]). Our construction and proof is simpler and more general than Brand's [1], although it is similar in a number of respects.

Similar constructions give CSTS(p^n) that have other interesting properties: they can be cyclically nested and they contain sub-CSTS(p^m) for $1 \leq m \leq n$.

Briefly a CSTS(n) can be cyclically nested if and only if $n \equiv 1$ (mod 6) and there exists a collection of base blocks (or orbit representatives) such that every non-zero difference modulo n occurs exactly once in some base blocks. All CSTS(n), $n \leq 31$, ($n \equiv 1$ (mod 6)) are known to have a cyclic nesting (Novak [7]). Also the standard finite field construction for triple systems will produce a cyclically nested CSTS(p) when p is a prime (but not when p is a prime power) (for reference see [5, 6, 4]).

2. Nested CSTS(p^n)

First, the group of units in the ring of integers modulo p^n is cyclic and has order $p^{n-1}(p-1)=6t$, for p a prime $p\equiv 1 \pmod 6$. Let α be the generator of this cyclic group of units; then α^{2t} satisfies

$$x^3-1=(x-1)(x^2+x+1)\equiv 0 \pmod{p^n},$$

and thus we can conclude that $\alpha^0+\alpha^{2t}+\alpha^{4t}\equiv 0 \pmod{p^n}$ since $\alpha^{2t}-1$ is not a zero divisor.

CSTS(n) can be represented by difference triples or orbit representatives (base blocks). The following construction works for either representation.

Construction 2.1. Let B_{n-1} be a collection of triples which represent a CSTS(p^{n-1}); let α be the generator of the cyclic group of units of the integers modulo p^n, where $p\equiv 1 \pmod 6$ is a prime and α has order $6t$. Define $pB_{n-1}=\{\{px,py,pz\}\mid\{x,y,z\}\in B_{n-1}\}$,

$$U=\{\{\alpha^i,\alpha^{i+2t},\alpha^{i+4t}\}\mid i=0,1,\ldots,t-1\},$$

then, $B_n=pB_{n-1}\cup U$, is a set of representatives for a CSTS(p^n).

Proof. By assumption on B_{n-1}, if $x-y\equiv 0 \pmod p$ then the pair x, y will occur exactly once in one orbit represented by pB_{n-1}. If $x-y\not\equiv 0 \pmod p$, then $x-y$ is a unit. U contains $3t$ of the $6t$ units; moreover, since $\alpha^{3t}\equiv -1 \pmod{p^n}$ we do not have both x and $-x$ occurring in a triple of U. Note if $x=\alpha^i$ and $i\in[0,t-1]\cup[2t,3t-1]\cup[4t,5t-1]$, then x is in some triple of U but $-x=\alpha^{i+3t}$ is not.

Since $\alpha^i(\alpha^0+\alpha^{2t}+\alpha^{4t})\equiv 0 \pmod{p^n}$, then U can be thought of as difference triples. Alternately since $\{\alpha^0,\alpha^{2t},\alpha^{4t}\}$ has differences $(\alpha^{2t}-1)$, $(\alpha^{2t}-1)\alpha^{2t}$, $(\alpha^{2t}-1)\alpha^{4t}$ and $\alpha^{2t}-1$ is a multiplier (unit mod p^n), then U can also be considered as a set of orbit representatives (base blocks).

Corollary 2.2. *There exists a cyclically nexted* CSTS(p^n) *for all* $n\geq 1$, *p a prime* $p\equiv 1 \pmod 6$.

Proof. When $n=1$, $B_{n-1}=\emptyset$. By induction on n, if B_{n-1} is a collection of orbit representatives for a cyclic nesting of a CSTS(p^{n-1}), then so is B_n by the previous arguments. □

Corollary 2.3. *For all primes* $p\equiv 1 \pmod 6$ *and* $n\geq 1$, *there exist* CSTS(p^n) *will cyclic sub*-CSTS(p^m).

3. Isomorphic CSTS(p^n)

A similar approach can be used to construct isomorphic CSTS(p^n), $n \geq 2$, for which there is no multiplier isomorphism. Brand [2] proves the isomorphism must have a particular form. For our purposes we choose a quadratic map $f(x) \equiv p^{n-1}x^2 + x \pmod{p^n}$. Clearly if $x - y \equiv 0 \pmod{p}$, then $f(x) - f(y) \equiv x - y \pmod{p^n}$ and thus such a map would fix the sub-CSTS(p^{n-1}), pB_{n-1}. Moreover, the inverse map is $f^{-1}(y) \equiv y - p^{n-1}y^2 \pmod{p^n}$. Finally, the map $f(x)$ will produce an isomorphic CSTS(p^n) if and only if $f^{-1}(f(x)+1) \equiv ((p-2)p^{n-1} + 1)x + 1 - p^{n-1} \pmod{p^n}$ is an automorphism of the CSTS(p^n). To ensure this we need to construct a CSTS(p^n) having multiplier automorphisms $\beta(x) \equiv mx \pmod{p^n}$ for all $m \equiv 1 \pmod{p^{n-1}}$. These multipliers clearly form a multiplicative subgroup. If we assume that $B_n = pB_{n-1} \cup U$ is our collection of orbit representatives of a CSTS(p^n) containing a sub-CSTS(p^{n-1}), then any multiplier automorphism $B(x) = mx \pmod{p^n}$ of the CSTS(p^n) must also be a multiplier automorphism of the sub-CSTS(p^{n-1}). Since $m \equiv 1 \pmod{p^{n-1}}$ and thus is a multiplier automorphism $(\bmod\, p^{n-1})$ of the sub-system we need to concentrate on the orbits represented by U.

For a prime $p \equiv 7 \pmod{12}$, choose

$$U = \{\{\alpha^{2i}, \alpha^{2i+2t}, \alpha^{2i+4t}\} \mid i = 0, 1, \ldots, t-1\}.$$

Since the even powers of α form a multiplicative subgroup which includes all $m \equiv 1 \pmod{p}$, any such multiplier will be a multiplier automorphism of U. Moreover, if a unit x is an even power of α, then $-x$ will be an odd power and thus $B_n = pB_{n-1} \cup U$ will again be a set of orbit representatives for a CSTS(p^n), where B_{n-1} is a set of orbit representatives for a CSTS(p^{n-1}). For $p \equiv 1 \pmod{12}$ one must be more careful in choosing U.

Suppose $6t = p^{n-1}(p-1) = 6kp^{n-1}$ and, again, α is the generator for the multiplicative group of units $(\bmod\, p^n)$. Note α^{p-1} is the generator for the subgroup of units $\{m \mid m \equiv 1 \pmod{p}\}$. Let $\beta = \alpha^{p-1}$. Choose

$$U = \{\{\beta^i\alpha^j, \beta^i\alpha^{j+2t}, \beta^i\alpha^{j+4t}\} \mid i = 0, \ldots, p^{n-1}-1, j = 0, 1, \ldots, k\} \quad (3.1)$$

All we need to do is prove that the triples $\{\alpha^j, \alpha^{j+2t}, \alpha^{j+4t}\}$ evaluated modulo p will be representative orbits of a CSTS(p). But $\alpha \pmod{p}$ must be a generator for the multiplicative group of units in Z_p and our claim then follows from the proof of Construction 2.1.

Theorem 3.2 (Brand [1]). *There exists* CSTS(p^n) *that are isomorphic but not multiplier isomorphic.*

Assume $6t = p^{n-1}(p-1)$ and α is the generator of the group of units in Z_{p^n}. We first choose B_{n-1}, a set of representatives for CSTS (p^{n-1}) for which $\{\alpha^0, \alpha^{2t}, \alpha^{4t}\}$ are the only multiplier automorphisms $(\bmod\, p^{n-1})$. Construction

2.1 will produce such a collection for each $n-1 \geq 1$. Choose U as in (3.1) above, then $B_n = pB_{n-1} \cup U$ is a set of representatives for a CSTS(p^n). Since every multiplier $m \equiv 1 \pmod{p^{n-1}}$ is an automorphism of this system $f(x) = p^{n-1}x^2 + x$ will be an isomorphism from B_n to another CSTS(p^n), B_n'. Since $f(x)$ fixes the orbits in pB_{n-1}, pB_{n-1} will be a form sub-CSTS(p^{n-1}) in B_n' and thus any multiplier isomorphism from B_n to B_n' must first be a multiplier automorphism $(\bmod\, p^{n-1})$ of B_{n-1}. By choice of B_{n-1}, the multiplier m must be congruent to 1, α^{2t}, or α^{4t} $(\bmod\, p^{n-1})$ but then the multiplier will be a multiplier automorphism for B_n.

References

[1] N. Brand, On the Bays-Lambossy theorem, preprint.

[2] N. Brand, Some combinatorial isomorphism theorems, preprint.

[3] M.J. Colbourn and R.A. Mathon, On cyclic Steiner 2-designs, Ann. Discrete Math. 7 (1980) 215–251.

[4] M.J. Colbourn, Algorithmic aspects of combinatorial designs: a survey, Ann. Discrete Math. 26 (1985) 67–136.

[5] C.J. Colbourn and M.J. Colbourn, Nested triple systems, Ars Combin. 16 (1983) 27–34.

[6] C.C. Lindner and D. Stinson, The spectrum for conjugate invariant subgroups of perpendicular arrays, Ars Combin. 18 (1984) 51–60.

[7] J. Novak, A Note on Disjoint Cyclic Steiner Triple Systems, Recent Advances in Graph Theory, Proc. Symp. Prague 1974 (Academia, Praha, 1975) 439–440.

[8] R. Peltesohn, Eine Losüng der beiden heffterschen differenzen Probleme, Compositio Math. 6 (1939) 251–257.