Decomposing the Complement of 3-Nets (Latin Squares) Into Triples (A natural generalization of GDD's)

E. Mendelsohn*
N. Shalaby

Department of Mathematics
University of Toronto
Toronto, Ontario M5A 1A7
CANADA

1. Introduction.

A geometric net is a set of objects called "points" together with a set of subsets called lines; the lines occur in parallel classes with the following properties:

1. each point belongs to one line of each parallel class;
2. if $L1$ and $L2$ are lines of different parallel classes, then $L1$ and $L2$ have exactly one point in common;
3. there are at least three parallel classes and at least two points on a line [6].

A net possessing π parallel classes is called a π-net.

An isotopy class of latin squares is the set of all latin squares that can be obtained from each other by rearranging rows, columns or renaming elements.

A set of latin squares which contains all squares isotopic to a given square and its conjugates is called a main class of latin squares.

A latin square is said to be in the standard form if the elements in the first row and column occur in the natural order $1, 2, 3, \ldots$.

It is known that every bordered latin square is associated with a geometric net of order n, having exactly 3 parallel classes [6].

Let $L = A_{ij}$ be a latin square of order n; define (the latin square graph of L) P to be a graph with n^2 vertices, each vertex being labeled by one of the n^2 ordered triples (a_{i1}, a_{1j}, a_{ij}) where $(i, j = 1, 2, \ldots, n)$. We will refer in this paper to the vertices as (i, j) when the latin square is understood. Two vertices of P are joined iff the two triples have a component in common [6].

The complement of the latin square graph P (3-net) is $K_{n^2} - P$. The same concept could be generalized if m orthogonal latin square graphs ($m + 2$-net) are removed from K_{n^2}.

A design (X, B), is a set X together with a family of subsets (blocks) B of X. A parallel class of disjoint (blocks or lines) $H \subset B$, the union of which equals X. A design (X, H, Y) where X is a set, H is a parallel class of subsets of X

*Supported in part by NSERC No. 7681.

called groups and Y is a family of subsets of X called proper blocks. The design (X, H, Y) is group divisible design (GDD) $GD[k, \lambda, m; v]$ if

i) $|X| = v$;
ii) $|h_i| = m$ for every h_i in H;
iii) $|y_j| = k$ for every y_j in Y;
iv) $|h_i \cap y_j| \leq 1$;
v) every pair $\{a, b\} \subset X$, such that a, b belong to distinct groups, is contained in exactly λ blocks of Y [9].

Hence decomposing the complement of a 1-net into blocks of size k is a GDD with $\lambda = 1$. Decomposition of the complement of a 2-net, for $k = 3$, was completely settled by A. Assaf, who called them "modified GDD's" [1].

We note that there is essentially one 1-net and one 2-net of size n for all n, but many 3-nets (e.g. for

$n = 4$ there are 2,

$n = 5$ there are 2,

$n = 6$ there are 12,

$n = 7$ there are 147,

$n = 8$ there are $\cong 25 \times 10^4$) [6].

The necessary conditions for decomposing the complement of a π-net into blocks of size k are

a) $(n^2 - 1) - \pi(n - 1) \equiv 0 \mod (k - 1)$.
b) $n^2(n^2 - 1) - \pi n^2(n - 1) \equiv 0 \mod k(k - 1)$.

This implies that for $k = 3$ if

$n \equiv 0, 4 \mod 6$, then $\pi \equiv 1 \mod 2$;

$n \equiv 1, 3 \mod 6$, then π unrestricted;

$n \equiv 2 \mod 6$, then $\pi \equiv 3 \mod 6$;

$n \equiv 5 \mod 6$, then $\pi \equiv 0 \mod 3$.

We note that for all k, π only $k = 3, \pi = 3 \mod 6$ give no condition on n.

We did the main latin square classes decomposition into triples for $n = 5$ and $n = 6$ (re. Appendix I). We know of no listing for the 147 main classes for the latin squares of order 7, though given the list we could easily do the decompositions. We have also decomposed the complement of the boolean latin square of order 8 and the complement of the 5 orthogonal latin squares of order 12 [7].

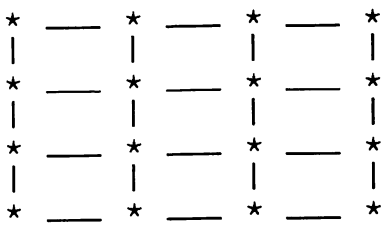
2. The conjecture.

In this paper we mainly study the decomposition of the complements of 3-nets into triples, and we prove that there exists a decomposition for all cyclic latin squares, and all latin squares which are extendable to an affine plane of prime power of $1, 3 \mod 6$, and elementary abelian groups for $n \equiv 5 \mod 6$. We also show that complements for all latin squares ($n \leq 6$) are decomposable, with the exception of the boolean latin square of order 4.

Hence we conjecture: The complement of a π-net is decomposable into triples $\Leftrightarrow$ (a) and (b) are satisfied, with the exception that for $\pi = m, m-1$ then an $(m, k, 1)$ design must also exist.

3. The exception.

The cyclic latin square of order 4 has the decomposition $\{(0,0), (1,3), (2,1)\}$ $\mathrm{mod}(4,4)$. The boolean 4 is a 3-net in a 5-net namely, $AG(4,2)$; hence the complement consists of two parallel classes on 16 points



The only way to find triples for the first point is to use 3 edges on the same line of the parallel class, which leaves the fourth point with one edge connected to the first, then we will have to use an edge from the other parallel (containing the first or the forth) class to form a triple containing the first point and the forth, which is impossible since we have no third edge. More generally the complement of an m-net on $m + 2$ points has a decomposition into k subsets $\Leftrightarrow$ there exist a BIBD$(m + 2, k, 1)$.

4. Geometric solutions.

A π-net with n points per line is completable to an affine geometry iff one can add $n+1-\pi$ new parallel classes of lines to the π-net to get an $(n+1)$-net. We note that, if $\pi = n+1, n, n-1$ or $n-2$, then the π-net is completable (for $n-2$ see [3]).

We wish to prove the following concerning completable π-nets.

Theorem 1. *Let N be a completable π-net with n points per line.*

a) *if a BIBD$(n, k, 1)$ exists then the complement of N can be decomposed into k subsets;*

b) $n+1-\pi \equiv 0(\bmod 3)$, *and n is odd and further N can be completed to a Desarguesian affine plane, the complement of N can be decomposed into triples;*

c) *if a BIBD$(n, k, 1)$ does not exist, then if $\pi = n-1$ or n, the complement of N cannot be decomposed into k subsets.*

Corollary 1. $(k = 3,\ \pi = 3)$

a) *if $p \equiv 1, 3(\bmod 6)$ then the complement of any latin square which can as a 3-net be completed to an affine plane, can be decomposed into triples;*

b) *if $p \equiv 5(\bmod 6)$ then the complement of a latin square, the elementary abelian groups $(Z_p)^r$, which as a 3-net be completed to an Desarguesian affine plane, can be decomposed into triples.*

This includes the elementary abelian groups, $(Z_p)^r$, p odd, as they are isotopic to the square obtained by the union of the lines of slopes $0, -1$ and ∞ in the Desarguesian plane over $GF(p^r)$.

c) *The complement of the latin square which is the elementary abelian group $(Z_2)^2$ cannot be decomposed into triples.*

Proof of Theorem 1:

a) We simply note that an edge in the complement determines a set of n points (a line not in N) and these can be further broken into k subsets using the existence of an $(n, k, 1)$-design.

b) In this case what we wish to do is decompose the union of three parallel classes into disjoint triples. We first note the complement of N has $3t$ parallel classes. Divide these arbitrarily into t groups of three classes each. Now given two points in the complement they determine uniquely three parallel classes in the complement and thus a latin square graph in the complement. Since the plane is Desarguesian, the latin square graph of any three parallel classes is the same as that of those of slope $0, -1$ and ∞, since there is enough transitivity. To decompose the latin square graph of the elementary abelian group Z_pr take $p = 1, 2, \ldots, \lfloor n/2 \rfloor$ and $x_1, x_2, \ldots, x_r$, as a basis and triples $\{(ix_t + u, u),\ (u, iu_t + u), (ix_t + u, ix_t)\}$; where $u \in Z_pr$, $1 \le t \le r$, $i \in P$.

c) For $\pi = n$ it is obvious since the complement is just nK_n. When $\pi = n+1$ then the complement of N is isomorphic to the graph $G(V, E)$ where $V = n \times n$ and $\{(x, y), (u, v)\} \in E$ iff $x = u$ or $y = v$ but not both. Since there is no (x, y) and (u, v) where $x = u$ and $y = v$, this is a contradiction. ∎

5. Two-dimensional Heffter like approach to the cyclic group.

Heffter [10] observed that the construction of a cyclic STS $S(2,3,v)$, where $v = 6n+1$, is equivalent to partitioning the set $1,\dots 3n$ into triples such that the sum of some pair of numbers equals the third or the sum of the three equals v; if $v = 6n+3$ is equivalent to partitioning $\{1,\dots,2n, 2n+2,\dots,3n+1\}$, i.e. every triple of differences or "distances" implies an orbit in Z_v and the decomposition of distances implies the existence of a cyclic STS.

A two-dimensional Heffter's approach would begin with the set of vertices $Z_n \times Z_n$. We choose residues in Z_n, to be $\{-\lfloor n/2 \rfloor \le 0, 0 \le \lfloor n/2 \rfloor : n \text{ is odd}\}$, and $\{-n/2 < 0, 0 \le n/2 : n \text{ is even}\}$. Define the distances

$$D = \left\{ \langle |x - x'|, (y - y') \rangle \,\middle|\, 0 \le x, x', y, y' \le \left\lfloor \frac{n}{2} \right\rfloor \quad n \text{ odd}; \right.$$
$$\left. \text{and} \quad 0 \le x, x', y, y' \le \frac{n}{2} \quad \text{if } n \text{ is even.} \right\}.$$

We use this approach to decompose the complement of the cyclic latin square given by $a_{ij} = i + j \pmod{n}$;

Define the distance D^p to be all the remaining distances after removing the distances $\{\langle x, 0\rangle, \langle 0, x\rangle, \langle x, x\rangle\}$.

$$D^P = \left\{ \langle |x - x'|, (y - y') \rangle \,\middle|\, \begin{array}{l} \text{(a) } |x - x'|,\ |y - y' \ne 0; \\ \text{(b) } (x - x') \ne |y - y'|; \\ \text{(c) } 0 \le x, x', y, y' \le \left\lfloor \frac{n}{2} \right\rfloor \quad n \text{ odd}; \\ \text{(d) } 0 \le x,\ x' \le \frac{n}{2},\ 0 \le y,\ y' < \frac{n}{2} \quad \text{if } n \text{ is even} \end{array} \right\}$$

Then the factorization of D^p into triples $(\langle a, b\rangle, \langle c, d\rangle, \langle e, f\rangle)$ such that $\langle a, b\rangle + \langle c, d\rangle = \langle e, f\rangle$, or $\langle a, b\rangle + \langle c + d\rangle + \langle e, f\rangle = \langle 0, 0\rangle \bmod (n, n)$, will yield a decomposition of the complement of P into disjoint orbits of triples mod (Z_n, Z_n) of n^2 edges, namely

$$\{(x, y), (x + a, y + b), (x + e, y + f) : (x, y) \in Z_n \times Z_n\}.$$

With the exclusion of the short orbits of length $n^2/9$ if $p \equiv 2 \bmod 3$ and $n = 2p + 1$ and $p \equiv 0 \bmod 3$, $n = 2p \bmod 3$,

$$\{(x, y), (x + n/3, y + n/3), (x + 2n/3, y + 2n/3) : 0 \le x, y < n/3\}.$$

For example, for $n = 5$,

$$D = \{\langle 1,2\rangle, \langle 1,-2\rangle, \langle 1,-1\rangle, \langle 2,-2\rangle, \langle 2,-1\rangle, \langle 2,1\rangle\}$$

where the factorization of distances is

$$\langle 1,-1\rangle + \langle 1,2\rangle = \langle 2,1\rangle$$
$$\langle 1,-2\rangle + \langle 2,-2\rangle + \langle 2,-1\rangle = \langle 5,-5\rangle.$$

This will give the following factorization to triples:

$$\{(0,0),(1,4),(2,1)\} \bmod (5,5)$$
$$\{(0,0),(1,3),(2,4)\} \bmod (5,5).$$

Theorem 1. *The complement of the cyclic latin square graph is decomposable into triples.*

Proof:
Case 1: If $n = 2p+1$, the total number of differences

$$\begin{aligned} |D| &= 2p(p-1) \quad \text{if } p = 0 \text{ or } 2 \bmod 3 \\ &= 2p(p-1) - 1 \quad \text{if } p = 1 \bmod 3. \end{aligned}$$

Take the distances

$$\langle s,-t\rangle + \langle t, t+s\rangle = \langle s+t, s\rangle$$

where $s = 1,2,\ldots, \left\lfloor \frac{p+1}{2} \right\rfloor$ $t = n-s, n-s-1, \ldots, s$. This gives

$$\begin{aligned} &(p-1) + (p-3) + \ldots + 3 + 1 \text{ distances if } p \text{ is even.} \\ &(p-1) + (p-3) + \ldots + 4 + 2 \text{ distances if } p \text{ is odd.} \end{aligned} \quad (1)$$

The distances

$$\langle s,t\rangle + \langle t,-s,-s\rangle = \langle t, t-s\rangle$$

where $s = 1,2 \ldots, \left\lfloor \frac{p-1}{2} \right\rfloor$ $t = p, p-1, \ldots, 2s$ give

$$\begin{aligned} &(p-2) + (p-4) + \ldots + 4 + 2 \text{ distances if } p \text{ is even.} \\ &(p-1) + (p-3) + \ldots + 3 + 1 \text{ distances if } p \text{ is odd.} \end{aligned} \quad (2)$$

By adding (1), (2) the number of distances used is

$$3((p-1) + (p-2) + \ldots + 1) = 3p(p-1)/2.$$

Hence the remaining distances are

$$(2p^2 - p) - \frac{3p(p-1)}{2} = 1/2p(p+1).$$

These distances could be rearranged in the triangle

$$\begin{array}{ccccc}
 & & & & \langle p,-1\rangle \\
 & & & \langle p-1,-2\rangle & \langle p,-2\rangle \\
 & & \cdot & \cdot & \cdot \\
 & \cdot & & \cdot & \cdot \\
\cdot & & & \cdot & \cdot \\
 & \langle 2-p,+1\rangle & & \cdots & \langle p,-p+1\rangle \\
\langle 1-p\rangle & \langle 2-p\rangle & & \cdots & \langle p,-p\rangle .
\end{array}$$

The distance triples

$$\langle u,-p+i-1\rangle + \langle p-u+i,-u\rangle + \langle p-i+1,-p+u-i\rangle = \langle 2p+1,-2p-1\rangle$$

where $i = 1,2,\dots,\lfloor (p-1)/2 \rfloor$. $u = 2i-1, 2i, \dots, p-i$. For every i the triples use all the distances along the circumference of the ith concentric triangle to the total of $\frac{p(p+1)}{2}$ distances. The last triangle contains either exactly three distances or exactly the distance of the short orbit.

Case 2: $n = 2p$.
The total number of distances = $(2p-1)(p-1)$ if $p \equiv 1$ or $2 \bmod 3$ or $(2p-1)(p-1) - 1$ if $p \equiv 0 \bmod 3$.
Steps 1, 2 are the same as Case 1 and for the triangle triples added are:

$$\langle u,-p+i\rangle + \langle p-u+i,-u\rangle + \langle p-i,-p+u-i\rangle = \langle 2p,-2p\rangle$$
$$i = 1,2,\dots,\lfloor p-1/2 \rfloor$$
$$u = 2i, 2i+1, \dots, p-i-1.$$

∎

As a corollary of Theorem 1 we have:

Corollary. *If n is odd then there is an STS(n^2) which admits an automorphism group $Z_n \times Z_n$.*

Proof: We have decomposed into $Z_n \times Z_n$ orbits all triples except those of distances $\langle x,0\rangle$, $\langle 0,x\rangle$ and $\langle x,x\rangle$; $x \le \lfloor n/2 \rfloor$; thus, adding the distance triple $\langle x,0\rangle + \langle 0,x\rangle = \langle x,x\rangle$ will yield an STS(n^2) with $Z_n \times Z_n$ as automorphism group. This result is also obtained in [3]. ∎

6. Computational results.

6.1.

We found decompositions of the complements of all main classes of latin squares of order $n \leq 6$ and the boolean latin square of order 8, and the Dulmage-Johnson-Mendelsohn set of 5 orthogonal latin squares of order 12 (these decompositions may be obtained from the authors).
In the appendix we give the results for $n = 5, 6$.

The method used for both in this section and in investigating the initial values for the previous section, is a hill-climbing technique similar to that of Stinson [11].

The algorithm for the bicyclic decomposition of the cyclic latin squares is

```
Begin
Solution: = ∅; List: = 0;
Make a list of all triples of distances that satisfy the equations for being an orbit.
        While (not end of the list) and i ≤ I
             Solution: = triple distance T_i.
                  If T_i ∩ T_j = ∅ then solution S: = T_i ∪ T_j
                  else if (T_j ∩ S) = ∅ and (T_j ∩ T_i) ≠ ∅, then
                  S = S(T_i ∪ T_j).
                  Next T_j.
        end;
end.
```

The algorithm resets $S = \emptyset$ after a number of iterations, and starts hill-climbing again.

This algorithm produced solutions for the cyclic cases, for every n attempted; with $I = 5$ (up to $n = 21$, i.e. 441 vertices).

6.2 All squares of side ≤ 6.

The algorithm for the general case was a combination of a greedy and a hill-climbing[2], [4] and [11].

```
Begin
        L: = List all edges of K_{n^2}; remove all three parallel classes.
             While (not end of list)
             edge: = first edge begin
                                 Make a block if possible containing edge,
                                  delete edges used from list.
                                 edge: = next edge.
                                 end
             If L ≠ ∅ then
                  while i < I
                  begin
                  Find any two edges that have a vertex in common,
```

if the required third edge is in an already formed triple.
then
form a new triple by adding the third edge
to the pair making a new triple,
and the two edges of the dismantled triple are added to the list.
else
next pair of edges with a vertex in common.
$i := i + 1;$

end;

end.

We found that for number of iterations $I < 500$, all cases that were attempted gave solutions. It was not the number of iterations but space and time constraints that interfered with the process.

References

1. A. Assaf, *Modified group divisible designs*, Ars Combinatoria **29** (1990), 13–20.
2. A.V. Aho, J.E. Hopcroft, and J.D. Ullman, "Data Structures and Algorithms", Addison-Wesley Publishing Co., 1983.
3. R.M. Bruk, *Finite nets II - uniqueness and imbedding*, Pacific J. Math. **13** (1963), 421–45.
4. M.J. Colbourn, *Algorithmic aspects of combinatorial designs: A survey*, Annals of Discrete Mathematics **26** (1985), 67–136.
5. M.J. Colbourn and R.A. Mathon, *On cyclic Steiner 2-designs*, Annals of Discrete Mathematics **7** (1980), 215–253.
6. J. Denes and A.D. Keedwell, "Latin Squares and their Applications", Academic Press, New York, 1967.
7. A.L. Dulmage, D.M. Johnson, and N.S. Mendelsohn, *Orthomorphisms of groups and orthogonal Latin squares I*, Can. J. Math. **13** (1961), 356–372.
8. M. Hall, Jr., "Combinatorial Theory", Blaisdell, Waltham-Toronto-London, 1967.
9. H. Hanani, *On balanced incomplete block designs and related designs*, Discrete Math. **11** (1975), 255–369.
10. L. Heffter, *Ueber Tripelsysteme*, Math. Ann. **49** (1897), 101–112.
11. D.R. Stinson, *Hill-climbing algorithms for the construction of combinatorial designs*, Annals of Discrete Mathematics **26** (1985), 321–334.