RM-259 AH-4 ES-14
August 1970

ON A METHOD OF SUM COMPOSITION OF ORTHOGONAL LATIN SQUARES III*

By

A. Hedayat[1] and E. Seiden
Michigan State University

* This research was supported by NIH GM-05900-11 grant at Cornell University and NSF Grant GP-20537 at Michigan State University.

1) On leave from Cornell University.

I. Introduction and Summary

In [2] we showed that under certain combinatorial regularities one can compose two Latin squares of order n_1 and n_2 to obtain a Latin square of order $n = n_1 + n_2$. Reasonably enough we called this method a sum composition method. We also showed that this method can be used to construct a pair of orthogonal Latin squares of order n, designated by $O(n,2)$, by the sum composition of an $O(n_1,2)$ and $O(n_2,2)$. Indeed, we exhibited a method of construction of a pair of orthogonal Latin squares by sum composition of (i) an $O(n_1,2)$ and an $O(n_2,2)$, where $7 \leq n_1 = p^\alpha$, p a prime and α a positive integer, $n_1 \neq 13$ and $n_2 = (n_1-1)/2$; (ii) an $O(n_1,2)$ and an $O(n_2,2)$ where, $8 \leq n_1 = 2^\alpha$ and $n_2 = n_1/2$; (iii) an $O(n_1,2)$ and an $O(3,2)$ where $n_1 = p^\alpha$, $p \geq 7$ for all those p's having any of the following forms: $3m + 1$, $8m + 1$, $8m + 3$, $24m + 11$, $60m + 23$ and $60m + 47$. Clearly cases (i) and (iii) capture an infinite collection of pairs of orthogonal Latin squares of order $4t+2$.

The technique of sum composition itself together with some other combinatorial impossibilities force us to limit ourselves to certain families of n_1 and n_2. Thus far we have considered only those n_1 which are either prime or powers of primes. This is because Galois fileds exist only for these orders. Also, we are forced to take n_2 to be in the range of $3 \leq n_2 \leq [\frac{n_1}{2}]$ except $n_2 = 6$, where $[x]$ denotes the integer part of x. The restriction on the upper bound is due to the method of sum composition. However, the restriction on the lower bound and the exclusion of 6 is due to the fact that there is no pair of orthogonal Latin squares of order 2 nor of order 6. Surely, there is a trivial pair of orthogonal Latin squares of order unity. But this has also been excluded from the lower bound only because our method fails. In the final part of this report we have shown that one can possibly modify the method of sum composition in order to take into account the lower bound of unity. To support this statement we have

exhibited an $O(10,2)$ which has been obtained by a composition of a trivial pair of orthogonal Latin squares of order unity and a special pair of non-orthogonal Latin squares of order 9.

If $n_1 = p^\alpha \geq 7$ then cases (i) and (ii) jointly show that n_2 hits the upper bound. However case (iii) shows that n_2 hits the lower bound for all p^α, where $7 \leq p$ of the form $3m + 1$ and only for those p's of the form $3m + 2$ which can also be written in any of the forms" $8m + 1$, $8m + 3$, $24m + 11$, $60m + 23$ and $60m + 47$. Before proceeding further we shall analyze the latter case more deeply. The totality of all primes can be divided into two subfamilies; those of the form $3\ell + 1$ and $3\ell + 2$. We already have a uniform solution for the composition of an $O(3,2)$ with $O(p^\alpha,2)$, where $7 \leq p$ of the from $3\ell + 1$. Now the family of primes of the form $3\ell + 2$, $\ell \neq 0$ can be divided into four mutually exclusive and exhaustive subfamilies with arithmetic progressions $3(8k + 1) + 2$, $3(8k + 3) + 2$, $3(8k + 5) + 2$ and $3(8k + 7) + 2$. Now for $m = 3k + 1$ all the primes of the form $8m + 3$ and for $m = k$ all the primes of the form $24m + 11$ will separately exhaust the subfamily of primes of the form $3(8k + 3) + 2$. For m odd the primes of the form $60m + 23$ and/or $60m + 47$ will also capture some of the primes of the form $3(8k + 3) + 2$. Clearly all the subfamily of primes of the from $3(8k + 5) + 2$ can be obtained from our family of primes of the form $8m + 1$ by letting $m = 3k + 2$. For $m = 0$ or m even our family of primes of the from $60m + 47$ will coincide with subfamilies of primes of the form $3(8k + 7) + 2$. Note also that for m even the family of primes of the form $60m + 23$ will capture a subset of primes of the form $3(8k + 7) + 2$. The preceeding analysis reveals the fact that we have already composition rules of $O(3,2)$ with $O(p^\alpha,2)$ for all $p \geq 7$ except those p's of the form $3(8k + 1) + 2$, such as 29, 53, 101, etc. However, note that the sum composition of $O(3,2)$ and $O(p^\alpha,2)$, p of the form $3(8k + 1) + 2$ will never capture any $O(n,2)$ for n of the form $4t + 2$. Thus we can

conclude that if $n = 4t + 2 \geq 10$ can be written as $p^{\alpha} + 3$ then one can construct an $O(n,2)$ by sum composition of an $O(3,2)$ and an $O(p^{\alpha},2)$.

The object of this paper is two-fold. In section 2, we shall explicitly study twenty four possible ways of composition of an $O(3,2)$ with an $O(p^{\alpha},2)$. By doing this we have been able to obtain some new results concerning the family of primes of the form $3(8k + 1) + 2$. Actually we have shown that if either $f(y) = 2y^4 + 4y^3 + 4y^2 + 2y + 1$ and/or $f(y) = 2y^4 + 3y^3 + 3y^2 + 2y + 1$ has a root in $GF(p)$, for all p of the form $3(8k+ 1) + 2$ then our problem of composition of an $O(3,2)$ and an $O(p^{\alpha},2)$ for all $7 \leq p$ of the form $3(8k + 1) + 2$ is totally solved. Then, as we mentioned before, this result together with those obtained in [2] will jointly solve the problem of composition of an $O(3,2)$ and an $O(p^{\alpha},2)$ for all $p \geq 7$.

Thus far, we have mainly considered those n_2 which hit either the lower or the upper bound. By exhibiting solutions for composition of an $O(4,2)$ with an $O(11,2)$ and an $O(13,2)$ and also composition of an $O(5,2)$ with an $O(13,2)$ and an $O(17,2)$ we showed in [2] that other values of n_2 also can be considered. However, we did not have any theory in this respect. Here in section 3, we shall present a theorem which gives a uniform method of composition of an $O(4,2)$ and an $O(p^{\alpha},2)$ for all $7 < p$ of the form $8m + 1$ or $8m + 3$. The composed orthogonal Latin squares, derived by the method of this theorem, has an interesting combinatorial property which can be utilized in a construction of a family of designs for two successive experiments. In the rest of this paper we shall adopt the notations and terminologies of [2].

II. In this section we enumerate 24 distinct patterns for construction of $O(n,2)$, $n = n_1 + 3$, $n_1 = p^{\alpha}$, $n_1 \geq 7$. Two patterns will be considered distinct if they cannot be obtained from each other by permuting the elements within the sets S and T interchanging the squares or transposing both squares.

The 24 patterns exhaust all the cases in which $k_1(s_i,t_j)$ assumes two values of the set S and one value of the set T or all three values of S. To enumerate all possible cases we should consider also the remaining possibilities i.e. the cases in which $k_1(s_i,t_j)$ ranges over the set T only or assumes two values belonging to T and one to S. The 24 cases yield patterns which enable us to construct $O(n,2)$ for $n = n_1 + 3$, $n_1 = p^\alpha$ for all p of the form $3m + 1$ and p's of the form $3m + 2$ except possibly not all p's of the form $3(8m + 1) + 2$. We hope that considering the remaining patterns we shall be able to eliminate this deficiency if any. Among the 24 cases considered there were few cases which did not yield a pair of $O(n,2)$. In these cases one reason for it was that the system of the six equations was consistent provided that y is equal to 1,-1 or 0 hence did not have a distinct inverse as required for our method of construction. In other cases the condition imposed on y for solvability of the system implied that the elements of $S \cup T$ could not be distinct, a condition which also violates our method of construction. In most of the cases we obtained a condition that y has to be a root of some quadratic equation. Clearly in such cases we could easily determine the progression of p to which the pattern could be applied. This lead to the conclusion stated above. Some of the cases resulted in a fourth degree equation of which y has to be a root. These cases seem to be difficult to analyze by existing algebraic number theory methods. However by computing the values of the fourth degree polynomials for some values of y we obtained that these patterns do enable us to construct a pair $O(n,2)$ for some of the missing values of p of the form $3(8m + 1) + 2$. It is quite possible that they yield all of them. Another possibility is to complete the enumeration of the remaining 24 cases hoping that some simple conditions on y will enable us to complete the construction of $O(n,2)$, $n = n_1 + 3$ for all $n_1 = p^\alpha$. We shall study both possibilities shortly. The reasons for considering both plans for research

is that considering higher order polynomials may give us methods useful in cases n_2 is not necessarily equal to 3. On the other hand examining the remaining 24 cases may help us to avoid special difficulties at least in the present case.

Presently we shall proceed to describe the result of the investigation of the 24 patterns which we already evaluated.

Notice first that we may assume that in the expression $k_1(s_i,t_j)$ i is equal to j since this amounts to a permutation of the elements of one set S or T. We shall first consider the 12 cases in which $k_1(s_i,t_i)$ $i = 1,2,3$ assumes two values from S and one from T. These cases will have three equations in common since we may assume without loss of generality that $k_1(s_1,t_1) = s_2$, $k_1(s_2,t_2) = s_3$, $k_1(s_3,t_3) = t_1$. To obtain all distinct patterns sharing these three equations it is easy to see that there are six distinct possibilities to recapture of s_1 through $k_2(s_i,t_j) = s_1$ since i can assume only the values 2 and 3 and j the values 1,2,3. Then for each of the six cases there again are two possibilities. This yields the 12 cases.

Analogous reasoning will enumerate the 12 possibilities in case $k_1(s_i,t_i)$ assumes the values from S only. Here again the 12 cases may be assumed to share common three equations.

The first three equations common to cases 1-12 are as follows:

$$k_1(s_1,t_1) = s_2 \qquad \text{(i)}$$

$$k_1(s_2,t_2) = s_3 \qquad \text{(ii)}$$

$$k_1(s_3,t_3) = t_1 \qquad \text{(iii)}$$

Case 1.

$$k_2(s_1,t_2) = t_3 \qquad \text{(iv)}$$

$$k_2(s_2,t_1) = s_1 \qquad \text{(v)}$$

$$k_2(s_3,t_3) = t_2 \qquad \text{(vi)} .$$

This system will be consistent provided that $y^2 + y + 1 = 0$ i.e. -3 is a quadratic residue mod p or p of the form $3m + 1$. Solving this system of equations in terms of s_3 and t_3 we obtain the following system of solutions.

$$s_1 = -s_3/(y+1) + (y+2)t_3/(y+1)$$
$$s_2 = (2y+1)s_3/(y+1) - yt_3/(y+1)$$
$$t_1 = s_3/(y+1) + yt_3/(y+1)$$
$$t_2 = ys_3(y+1) + t_3/(y+1).$$

Case 2. $k_2(s_1,t_3) = t_2$ (iv)

$k_2(s_2,t_1) = s_1$ (v)

$k_2(s_3,t_2) = t_3$ (vi)

Expressing s_1 in terms of s_2 and t_1 from equations (i) and (iv) we obtain that this system of equations will be consistent provided that $y^2 + y + 1 = 0$. However using equations (ii), (iii) and (v) to express t_1, t_2 and s_2 in terms of t_3 and s_3 we get

$$s_2 = (y^2 + y + 1)s_3 - y(y + 1)t_3.$$

This together with $y^2 + y + 1 = 0$ implies $s_2 = t_3$. Hence S and T cannot be disjoint.

Case 3. $k_2(s_1,t_3) = t_2$ (iv)

$k_2(s_2,t_2) = s_1$ (v)

$k_2(s_3,t_1) = t_3$ (vi)

This case is analogous to the previous one. Expressing t_1 from (iii) and (vi) as a function of s_3 and t_3 we obtain the condition consistency $y^2 + y + 1 = 0$. On the other hand if we express s_1, s_3 and t_1 as functions of s_2 and t_2 using (i), (ii) and (iv) we see that the $y^2 + y + 1 = 0$ implies $t_1 = t_2$.

Case 4. $k_2(s_1,t_1) = t_3$ (iv)

$k_2(s_2,t_2) = s_1$ (v)

$k_2(s_3,t_3) = t_2$ (vi)

This case was discussed in [2] p. 12 with the following substitution $(s_1,s_3,s_2)(t_1,t_2,t_3)$.

Case 5. $k_2(s_1,t_1) = t_2$ (iv)

$k_2(s_2,t_3) = s_1$ (v)

$k_2(s_3,t_2) = t_3$ (vi)

This system is consistent provided that

$$y^4 + 2y^3 + 3y^2 + y + 1 = 0.$$

The problem of determining the set of primes for which this fourth degree equation has roots is under investigation. Expressing four variables as linear functions of s_1 and t_1 we obtain the following system of solutions.

$$s_2 = s_1/(y+1) + yt_1/(y+1)$$
$$s_3 = (1+y^2)s_1/(y+1)^2 + 2yt_1/(y+1)^2$$
$$t_2 = ys_1/(y+1) + t_1/(y+1)$$
$$t_3 = (y^2 + y + 1)s_1/(y+1) - y^2t_1/(y+1).$$

Case 6. $k_2(s_1,t_2) = t_3$ (iv)

$k_2(s_2,t_3) = s_1$ (v)

$k_2(s_3,t_1) = t_2$ (vi)

The condition of consistency becomes now

$$2y^4 + 3y^3 + 3y^2 + 2y + 1 = 0$$

Again we don't know yet how to characterize the set of primes mod of which this equation has a root.

Lets express now four dependent variables in terms of s_3 and t_1

$$s_1(2y+1)s_3 - 2yt_1$$

$$s_2 = (2y+1)s_3/(y+1) - yt_1/(y+1)$$

$$t_2 = ys_3/(y+1) + t_1/(y+1)$$

$$t_3 = -s_3/y + (y+1)t_1/y$$

Case 7. $k_2(s_1,t_3) = t_2$ (iv)

$k_2(s_2,t_2) = t_3$ (v)

$k_2(s_3,t_1) = s_1$ (vi)

The condition for solvability becomes here:

$$3y^2 + 3y + 2 = 0.$$

This equation will have a root provided that -15 is a quadratic residue i.e. when -5 and 3 or -3 and 5 are quadratic residues. Alternatively the prime p has to be of the form $60m + 23$ or $60m + 47$.

Case 8. $k_2(s_1,t_2) = t_3$ (iv)

$k_2(s_2,t_3) = t_2$ (v)

$k_2(s_3,t_1) = s_1$ (vi)

The condition for consistency becomes here

$$y^4 + 3y^3 + 6y^2 + 5y + 2 = 0.$$

A system of solution is:

$$s_2 = s_1/(y+1)s_1 + yt_1/(y+1)$$

$$s_3 = (y+1)s_1/y - t_1/y$$

$$t_2 = -(y^3 + y^2 + 2y + 1)/y^2 + (y+1)(y^2 + y + 1)t_1/y^2$$

$$t_3 = -(y+1)s_1/y^2 + (y^2 + y + 1)t_1/y^2.$$

Case 9. $k_2(s_1,t_1) = t_3$ (iv)

$k_2(s_2,t_3) = t_2$ (v)

$k_2(s_3,t_2) = s_1$ (vi)

This system is solvable provided that

$$y^4 + 2y^3 + 3y^2 + y + 1 = 0.$$

A system of solutions has the form:

$$s_2 = s_1/(y+1) + yt_1/(y+1)$$
$$s_3 = -y^2 s_1/(y+1) + (y^2 + y + 1)t_1/(y+1)$$
$$t_2 = (y^3 + y^2 + 2y + 1)s_1/(y+1) - (y^3 + y^2 + y)t_1/(y+1)$$
$$t_3 = ys_1/(y+1) + t_1/(y+1)$$

Case 10.
$$k_2(s_1,t_3) = t_2 \quad \text{(iv)}$$
$$k_2(s_2,t_1) = t_3 \quad \text{(v)}$$
$$k_2(s_3,t_2) = s_1 \quad \text{(vi)}$$

This system will admit consistent solutions provided that

$$2y^4 + 4y^3 + 4y^2 + 2y + 1 = 0.$$

A system of solutions is:

$$s_1 = ys_3/(y+1) + t_2/(y+1)$$
$$s_2 = (y+1)s_3 - yt_2$$
$$t_1 = -(2y^2 + y)s_3 + (2y^2 + y + 1)t_2$$
$$t_3 = -y^2 s_3(y+1) + (y^2 + y + 1)t_2/(y+1)$$

Case 11.
$$k_2(s_1,t_2) = t_3 \quad \text{(iv)}$$
$$k_2(s_2,t_1) = t_2 \quad \text{(v)}$$
$$k_2(s_3,t_3) = s_1 \quad \text{(vi)}$$

The condition for solvability is here the same as in Case 5 i.e.

$y^4 + 2y^3 + 3y^2 + y + 1 = 0.$

A system of solutions is:

$$s_1 = s_3/(y+1) + yt_3/(y+1)$$
$$s_2 = (2y + 1)s_3/(y+1) - yt_3/(y+1)$$
$$t_1 = -y(2y+1)s_3/(y+1) + (2y^2 + 2y + 1)t_3/(y+1)$$
$$t_2 = ys_3/(y+1) + t_3/(y+1).$$

Case 12. $k_2(s_1,t_1) = t_2$ (iv)

$k_2(s_2,t_2) = t_3$ (v)

$k_2(s_3,t_3) = s_1$ (vi)

The condition for solvability becomes here $3y^2 + 1 = 0$. Hence this system has solutions if and only if -3 is a quadratic residue i.e. p is of the form $3m + 1$.

A system of solutinn is:

$$s_2 = (1+y^2)s_1/(y+1) + y(y-1)s_3/(y+1)$$

$$t_1 = ys_1 + (1-y)s_3$$

$$t_2 = 2ys_1/(y+1) + (1-y)s_3/(y+1)$$

$$t_3 = (y+1)s_1 - ys_3.$$

The next 12 systems of equations have again three equations in common. They are the following:

$k_1(s_1,t_1) = s_2$ (i)

$k_1(s_2,t_2) = s_3$ (ii)

$k_1(s_3,t_3) = s_1$ (iii)

Case 13. $k_2(s_1,t_2) = t_1$ (iv)

$k_2(s_2,t_1) = t_3$ (v)

$k_2(s_3,t_3) = t_2$ (vi)

This system is solvable provided that

$$2y^2 + 3y + 3 = 0.$$

Hence $y = \frac{-3 + \sqrt{-15}}{4}$ and the equation will have a root provided that -3 and 5 or -5 and 3 are quadratic residues i.e. p has the form $60m + 23$ or $60m + 47$.

This system of equations admits the following solutions:

$$s_1 = (y^2 + y + 1)s_2 - y(y+1)t_2$$
$$s_3 = s_2/(y+1) + yt_2/(y+1)$$
$$t_1 = -ys_2 + (y+1)t_2$$
$$t_3 = (y^3 + y^2 + y)s_2/(y+1) - (y^3 + y^2 - 1)t_2/(y+1).$$

Case 14. $k_2(s_1,t_2) = t_1$ (iv)

$k_2(s_3,t_1) = t_3$ (v)

$k_2(s_2,t_3) = t_2$ (vi)

The condition for consistency is here:

$$y^4 + 3y^3 + 6y^2 + 6y + 3 = 0.$$

A system of solutions is:

$$s_2 = s_1/(y+1) + yt_1/(y+1)$$
$$s_3 = (y^4 + 2y^3 + 3y^2 + 2y + 1)s_1/(y+1) - (y^4 + 2y^3 + 3y^2 + y)t_1/(y+1)$$
$$t_2 = (y+1)t_1 = ys_1$$
$$t_3 = -(y^3 + 2y^2 + 2y)s_1/(y+1) + (y^3 + 2y^2 + 3y + 1)t_1/(y+1).$$

Case 15. $k_2(s_1,t_1) = t_3$ (iv)

$k_2(s_2,t_2) = t_1$ (v)

$k_2(s_3,t_3) = t_2$ (vi)

The condition for solvability here is $y = 0$. Hence this case is not applicable for our purpose.

Case 16. $k_2(s_1,t_3) = t_2$ (iv)

$k_2(s_2,t_2) = t_1$ (v)

$k_2(s_3,t_1) = t_3$ (vi)

Here we have to have $2y^2 + 3y + 3 = 0$.

A system of solutions is given by:

$$s_1 (2y+1)s_2/(y+1) - yt_2/(y+1)$$

$$s_3 = s_2/(y+1) + yt_2/(y+1)$$

$$t_1 = ys_3/(y+1) + t_1/(y+1)$$

$$t_3 = 2ys_2/(y+1)^2 + (y^2+1)t_2/(y+1)^2.$$

Case 17. $k_2(s_1,t_3) = t_2$ (iv)

$k_2(s_2,t_1) = t_3$ (v)

$k_2(s_3,t_2) = t_1$ (vi)

The condition for solvability becomes the same as in case 14 i.e.

$y^4 + 3y^3 + 6y^2 + 6y + 3 = 0.$

A system of solutions can be chosen:

$$s_1 = (y^3 + 2y^2 + 3y + 1)s_3/(y+1) - (y^3 + 2y^2 + 2y)t_2/(y+1)$$

$$s_2 = (y+1)s_3 - yt_2$$

$$t_1 = ys_3/(y+1) + t_2/(y+1)$$

$$t_3 = (y^2 + 2y + 3)s_3 - (y^2 + 2y + 2)t_2.$$

Case 18. $k_2(s_1,t_1) = t_3$

$k_2(s_2,t_3) = t_2$

$k_2(s_3,t_2) = t_1$

The condition for solvability is here the same as in case 13 i.e.

$2y^2 + 3y + 3 = 0.$

We may choose a system of solutions as follows:

$$s_1 = (2y+1)s_2/(y+1) - yt_2/(y+1)$$

$$s_3 = s_2/(y+1) + yt_2/(y+1)$$

$$t_1 = ys_2/(y+1) + t_2/(y+1)$$

$$t_3 = 2ys_2/(y+1)^2 + (y^2+1)t_2/(y+1)^2.$$

Case 19. $k_2(s_1,t_3) = t_1$ (iv)

$k_2(s_2,t_1) = t_2$ (v)

$k_2(s_3,t_2) = t_3$ (vi)

Here the condition becomes $y^2 + 3y + 3 = 0$. We may choose a system of solutions:

$$s_2 = s_1/(y+1) + yt_1/(y+1)$$
$$s_3 = (y^2 + y + 1)s_1 - y(y+1)t_1$$
$$t_2 = ys_1/(y+1)^2 + (y^2 + y + 1)t_1/(y+1)^2$$
$$t_3 = -ys_1 + (y+1)t_1$$

Case 20. $k_2(s_1,t_3) = t_1$ (iv)

$k_2(s_2,t_2) = t_3$ (v)

$k_2(s_3,t_1) = t_2$ (vi)

This case was discussed in [2] p. 13.

Case 21. $k_2(s_1,t_1) = t_2$ (iv)

$k_2(s_2,t_3) = t_1$ (v)

$k_2(s_3,t_2) = t_3$ (vi)

The equation for y is the same as in case 16 and 18 i.e. $2y^2 + 3y + 3 = 0$.

Solutions:

$$s_2 = s_1/(y+1) + yt_1/(y+1)$$
$$s_3 = (y^2+1)s_1/(y+1)^2 + 2yt_1/(y+1)^2$$
$$t_2 = ys_1/(y+1) + t_1/(y+1)$$
$$y_3 = -ys_1/(y+1) + (2y+1)t_1/(y+1).$$

Case 22. $k_2(s_1,t_2) = t_3$ (iv)

$k_2(s_2,t_3) = t_1$ (v)

$k_2(s_3,t_1) = t_2$ (vi)

This case was discussed in [2] p. 12.

Case 23. $k_2(s_1,t_1) = t_2$ (iv)

$k_2(s_2,t_2) = t_3$ (v)

$k_2(s_3,t_3) = t_1$ (vi)

This case was discussed in [2] p. 11.

Case 24. $k_2(s_1,t_2) = t_3$ (iv)

$k_2(s_2,t_1) = t_2$ (v)

$k_2(s_3,t_3) = t_1$ (vi)

The condition for y is as in cases 16, 18, 20 and 21 i.e. $2y^2 + 3y + 3y = 0$.

The system of solutions is:

$$s_1 = (y^2 + y + 1)s_2 - y(y+1)t_2$$

$$s_3 = s_2/(y+1) + yt_2/(y+1)$$

$$t_3 = -(y^3 + 2y^2 + 2y)s_2/(y+1) + (y^3 + 2y^2 + 3y + 1)t_2/(y+1).$$

Remark 1. In conclusion we wish to point out that the 24 patterns examined previously can be classified into three main categories. There were three patterns which cannot be used since the conditions required for solvability of the corresponding system of equations were not compatible with our method of construction of $O(n,2)$. In the other cases y had to be a root of either a quadratic or a fourth degree polynomial. Clearly in the cases of second degree polynomials we could characterize the arithmetic progressions of primes for which the corresponding pattern would be applied. However $GF(p^2)$ can be generated by an irreducible polynomial mod p. Thus any of the quadratic equations will have a root in $GF(p^2)$ irrespective of the form of p. We could use the patterns corresponding to the quadratic polynomial to construct a pair $O(n,2)$, $n = p^\alpha + 3$ for any $p \geq 7$ and $\alpha \geq 2$.

In the cases in which it was required that a fourth degree polynomial vanishes we were not yet able to characterize the primes for which such a condition holds. However in these cases also we could use the corresponding patterns to construct a pair $O(n,2)$, $n = p^\alpha + 3$ irrespective of the form of p, provided that $\alpha \geq 4$.

Remark 2. As seen from the detailed discussion of the 24 patterns none of the quadratic polynomials had roots in $GF(p)$, for $p = 3(8m + 1) + 2$. This does not imply however that our method of sum composition fails for $n = p^\alpha + 3$,

$p = 3(8m + 1) + 2$, $\alpha < 4$. In fact it is quite possible that we do not have to resort even to the not yet examined patterns in order to apply it. To substantiate this claim we computed the values of the fourth degree polynomials for some y's and found that at least two of them do have roots in $GF(p)$ of the desired form. In fact the polynomail $f(y) = 2y^4 + 4y^3 + 4y^2 + 2y + 1$ has roots in $GF(p)$ for all p of the form $3(8m + 1) + 2$ less than or equal to 101. It vanishes for $y = -5$ and $y = 12$ in $GF(29)$, $y = -18$ in $GF(53)$ and $y = 12$ in $GF(101)$. The polynomial $f(y) = 2y^4 + 3y^3 + 3y^2 + 2y + 1$ vanishes for $y = 5$ in $GF(29)$.

III. In this section we shall exhibit a method of composition of an $O(4,2)$ with a family of $O(p^\alpha,2)$. The composed orthogonal Latin squares have an interesting combinatorial property which can be used for a construction of two families of designs for two successive experiments on the same experimental units (see [3] for more details).

Theorem 3.1. If p is a prime of the form $8m + 1$ or $8m + 3$, $m \neq 0$, then one can compose an $O(4,2)$ with an $O(p^\alpha,2)$ based on Galois field, to obtain an $O(p^\alpha + 4,2)$.

Method of Construction. In any $GF(p^\alpha)$, p of the form $8m + 1$ or $8m + 3$ there exists a z such that $z^2 = -2$, i.e. -2 is a quadratic residue. Now as in [2] we shall exhibit a set S and a set T together with a y such that the union of two functions $k_1(,)$ and $k_2(,)$ exhaust the set $S \cup T$. Let $y = (z-1)/3$ or $-(z+1)/3$. Then for arbitrary t_1 and t_2, $t_1 \neq t_2$ in $GF(p)$ the following sets S and T together with the given projection rules guarantees that all the requirements (see [2] for details) are satisfied.

Members of S:

$$s_1 = (y+1)t_1 - yt_2,$$
$$s_2 = (3y^2 + 3y + 1)t_1 - 3y(y+1)t_2$$
$$s_3 = (y+1)t_2 - yt_1,$$
$$s_4 = (y+2)t_2 - (y+1)t_1.$$

Members of T:

$$t_1,$$

$$t_2,$$

$$t_3 = (3y^2 + 4y + 2)t_2 - (y+1)(3y+1)t_1,$$

$$t_4 = 2(y+1)t_2 - (2y+1)t_1.$$

Projection rules:

We shall give here the arguments and the values of two functions $k_1(,)$ and $k_2(,)$. The arguments of $k_1(,)$ and $k_2(,)$ indicate the projection rules on rows and columns respectively. The values of $k_1(,)$ and $k_2(,)$ reveal the fact that the given y, the sets S and T together with the projection rules work, i.e. $k_1(,) \cup k_2(,) = S \cup T$.

$$k_1(s_1,t_2) = t_1 \qquad k_2(s_1,t_3) = t_4$$
$$k_1(s_2,t_4) = s_1 \qquad k_2(s_2,t_1) = t_3$$
$$k_1(s_3,t_1) = t_2 \qquad k_2(s_3,t_4) = s_4$$
$$k_1(s_4,t_3) = s_2 \qquad k_2(s_4,t_2) = s_3 .$$

Corollary 3.1. The composed $O(p^\alpha + 4,2)$ has at least 3 common parallel transversals.

Proof. The original $O(p^\alpha,2)$ has p^α common parallel transversals. Since $p^\alpha \geq 11$ therefore after removing 8 common parallel transversals we are left with at least 3 common parallel transversals in the corresponding portion of $O(p^\alpha,2)$ in the composed $O(p^\alpha + 4,2)$. Now it is known that any $O(4,2)$ has 4 common parallel transversals. Thus any three common parallel transversals of the corner $O(4,2)$ in the composed set with any three common parallel transversals in the portion corresponding to $O(p^\alpha,2)$ form three common parallel transversal for the entire set.

$O(n,2)$ with common parallel transversals have an application for the construction of a family of designs for two successive experiments (see [3]).

Thus we can conclude that all such designs exist for $n = p^{\alpha} + 4$, p of the form $8m + 1$ or $8m + 3$.

Example. Let $p = 11$, $\alpha = 1$. Then $-2 = 3^2$ in GF(11), thus $z = 3$. Let $y = -(z+1)/3 = 6$. Now set $t_1 = 0$, $t_2 = 1$. Then we have:

Members of S:	Members of T:
$s_1 = 5$	$t_1 = 0$
$s_2 = 6$	$t_2 = 1$
$s_3 = 7$	$t_3 = 2$
$s_4 = 8$	$t_4 = 3$.

Since $k_1(s,t) = (yt+s)(1+y)^{-1}$ and $k_2(s,t) = (ys+t)(1+y)^{-1}$ (see p. 7 of [2]), then for our projection rules given above we have

$$k_1(s_1,t_2) = k_1(5,1) = 0 \qquad k_2(s_1,t_3) = k_2(5,2) = 3$$
$$k_1(s_2,t_4) = k_1(6,3) = 5 \qquad k_2(s_2,t_1) = k_2(6,0) = 2$$
$$k_1(s_3,t_1) = k_1(7,0) = 1 \qquad k_2(s_3,t_4) = k_2(7,3) = 8$$
$$k_1(s_4,t_3) = k_1(8,2) = 6 \qquad k_2(s_4,t_2) = k_2(8,1) = 7$$

which checks i.e. $k_1(,) \cup k_2(,) = S \cup T$ with 8 distinct members.

IV. If $B(x)$ and $B(y)$, $x = y^{-1}$ based on Galois field GF(n) form an $O(n,2)$, then it is impossible to construct an $O(n+1,2)$ by sum composition of this $O(n,2)$ and a trivial pair of orthogonal Latin squares of order unity. This is so because it forces S to be equal to T and this can be seen by the fact that S and T each contain one element only, say s and t respectively. Now $k_1(s,t) = (yt+s)(1+y)^{-1}$ will be equal to s or t only if $t = s$, but we require $S \cap T = \phi$. However, we believe that with some modifications of the method of sum composition this can be done. Let us look at the following example.

0 1 2 3 4 5 6 7 8	0 1 2 3 4 5 6 7 8
1 3 6 8 7 2 0 5 4	2 5 7 6 1 8 4 3 0
2 6 7 5 1 4 8 3 0	5 6 4 0 3 7 2 8 1
3 8 5 4 0 6 2 1 7	7 4 3 8 5 1 0 6 2
4 7 1 0 2 3 5 8 6	6 0 8 1 2 4 7 5 3
5 2 4 6 3 8 7 0 1	1 3 5 2 7 6 8 0 4
6 0 8 2 5 7 1 4 3	8 7 1 4 6 0 3 2 5
7 5 3 1 8 0 4 6 2	4 2 0 7 8 3 5 1 6
8 4 0 7 6 1 3 2 5	3 8 6 5 0 2 1 4 7 .

This two Latin squares of order 9 are obviously not orthogonal. However, all the cells on the main diagonals or parallel to main diagonals form common parallel transversals. Now let us remove the underlined transversal in each square and project them on the tenth row and column and fill their corresponding cells with 9 and add a 1x1 Latin square in the lower right corner. Thus we obtain

9 1 2 3 4 5 6 7 8 | 0	0 1 2 3 4 5 6 7 9 | 8
1 9 6 8 7 2 0 5 4 | 3	9 5 7 6 1 8 4 3 0 | 2
2 6 9 5 1 4 8 3 0 | 7	5 9 4 0 3 7 2 8 1 | 6
3 8 5 9 0 6 2 1 7 | 4	7 4 9 8 5 1 0 6 2 | 3
4 7 1 0 9 3 5 8 6 | 2	6 0 8 9 2 4 7 5 3 | 1
5 2 4 6 3 9 7 0 1 | 8	1 3 5 2 9 6 8 0 4 | 7
6 0 8 2 5 7 9 4 3 | 1	8 7 1 4 6 9 3 2 5 | 0
7 5 3 1 8 0 4 9 2 | 6	4 2 0 7 8 3 9 1 6 | 5
8 4 0 7 6 1 3 2 9 | 5	3 8 6 5 0 2 1 9 7 | 4
0 3 7 4 2 8 1 6 5 | 9	2 6 3 1 7 0 5 4 8 | 9 .

The reader can check for himself that these Latin squares of order 10 are orthogonal. Note that these two orthogonal Latin squares have many common transversals all sharing the lower right corner cell. These common transversals can be located on the diagonals parallel to the main diagonal. It is easy to show that this $O(10,2)$ is not isomorphic with our previous $O(10,2)$ derived by composition of an $O(7,2)$ and $\theta(3,2)$.

The preceeding example indicates a possible modification of sum composition method, viz, starting with non-orthogonal Latin squares. But of course they should have certain combinatorial properties which we could not yet characterize. This matter is under investigation.

Before closing this section we should mention that sum composition with Latin squares of order unity has two important consequences. First, there is no bound on the number of mutually orthogonal Latin squares of order unity. Secondly, in the process of sum composition we only lose two common parallel transversals for each composition. These are very important if one hopes to construct a set consisting of more than two orthogonal Latin squares by sum composition method.

References

[1] Hedayat, A. and Seiden, E. (1969). On a method of sum composition of orthogonal Latin squares. RM-238, Department of Statistics and Probability, Michigan State University.

[2] Hedayat, A. and Seiden E. (1970). On a method of sum composition of orthogonal Latin squares II. RM-257, Department of Statistics and Probability, Michigan State University.

[3] Hedayat, A., Parker, E.T. and Federer, W.T. (1970). On an existence and construction of two families of designs for two successive experiments. To appear in August issue of Biometrica.