*Publ. Math. Debrecen*
**39 / 1–2** (1991), 135–141

# Infinite Latin Squares Containing Nested Sets of Mutually Orthogonal Finite Latin Squares

By J. V. BRAWLEY (Clemson, SC) and
GARY L. MULLEN[1] (University Park, PA)

## 1. Introduction

There is a large literature on Latin squares and sets of mutually orthogonal Latin squares. Such squares are of importance in statistics where they can be used to construct designs for the statistical analysis of experiments. The treatise [4] by DÉNES and KEEDWELL provides an excellent survey of Latin square theory and also discusses statistical as well as other applications of such squares. In their work, DÉNES and KEEDWELL introduce the concept of an infinite Latin square (also see [6],) they define what it means for a pair of such squares to be mutually orthogonal, and they define the notion of a complete set of mutually orthogonal infinite Latin squares. They do not however give any examples of these objects.

The purpose of this note is to give examples of some sets of mutually orthogonal Latin squares (abbreviated MOLS) of infinite order containing nested sets of MOLS of finite order. In particular, by ordering the elements of an infinite field which is obtained as the union of a tower of nested finite fields, we construct for each prime $p$ an infinite set of mutually orthogonal infinite Latin squares with the property that for all $n \geq 0$ the first $p^{p^n} - 1$ squares contain in their top left corners a set of $p^{p^n} - 1$ MOLS of order $p^{p^n}$.

A main feature of our construction is that it is explicit rather than implicit; i.e., the element in any row and any column of any of the squares can be calculated by a straightforward algorithm. This is accomplished by using an iterated presentation of an infinite algebraic extension of $GF(p)$ due to BRAWLEY and SCHNIBBEN [2], which itself, is a generalization of an infinite algebraic extension of $GF(2)$ used by CONWAY [3] in his analysis

[1] This author would like to thank the National Security Agency for partial support under grant agreement #MDA904-87-H-2023.

of certain games. A further feature of our construction is that it extends to the case of infinite Latin squares the usual construction of $q-1$ MOLS of order $q$ first given by MOORE [7] and later by BOSE [1] for $q$ a prime power.

While infinite Latin squares may have limited use statistically, our construction nevertheless provides a unified treatment of both the finite and infinite cases.

## 2. Orthogonal Latin Squares

A *Latin square* of order $m$ is an $m \times m$ array consisting of the numbers $1, 2, \ldots, m$ with the property that each row and each column contains each of the numbers exactly once. Two such squares of order $m$ are said to be *orthogonal* if, when superimposed, every ordered pair $(i, j)$ with $1 \leq i, j \leq m$ occurs exactly once. A set $\{L_1, L_2, \ldots, L_t\}$ of $t \geq 2$ Latin squares of the same order is said to be *mutually orthogonal* if $L_i$ is orthogonal to $L_j$ whenever $i \neq j$. It is well known (see [4, Thm. 5.1.5.]) that for any $m \geq 2$ not more than $m-1$ MOLS of order $m$ can exist. Such a set of MOLS is called *complete* if $t = m-1$.

For $m = q$, $q$ a prime power, a complete set of MOLS of order $q$ can be constructed by using the finite field $GF(q)$ of order $q$ (see [5, Thm. 7.27]). This consrtuction is essentially that of MOORE [7] and can be described as follows: Let $GF(q) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{q-1}\}$ denote the finite field of order $q$, and label the rows and columns of a $q \times q$ square by the elements $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ in this order. Then the $q-1$ polynomials $f_\alpha(x, y) = \alpha x + y$ with $0 \neq \alpha \in GF(q)$ yield a complete set of MOLS of order $q$ where we place the element $f_\alpha(x, y)$ in row $x$, column $y$, of the $\alpha$-th square (see MULLEN [8, Cor. 2]).

An *infinite Latin square* is a countably infinite array of rows and columns with the property that each positive integer occurs exactly once in each row and column. Following [4], we say that two infinite Latin squares $L_1$ and $L_2$ are *orthogonal* if every pair of cells (say cells $(i, j)$ and $(r, s)$) in different rows and columns ($i \neq r$ and $j \neq s$) are occupied by the same symbol in at most one of $L_1$ and $L_2$. Further, a set $\{L_i : i \in I\}$ of infinite Latin squares is called a set of MOLS if $L_i$ is orthogonal to $L_j$ whenever $i \neq j$, and the set is said to be *complete* if every pair of cells in different rows and columns are occupied by the same symbol in exactly one square of the set. (These definitions are of course generalizations of the corresponding finite case definitions.) Note if the set $\{L_i : i \in I\}$ is a complete set of MOLS of infinite order, then $I$ has cardinality equal to the cardinality of the set of positive integers.

## 3. A Tower of Finite Fields.

For each prime $p$ and integer $n \geq 1$ let $GF(p^n)$ denote the finite field of order $p^n$. Since $p^n$ divides $p^{n+1}$ for each $n$, it follows that $GF(p^{p^n})$ is a subfield of $GF(p^{p^{n+1}})$ and hence we have a tower of fields

$$(1) \qquad GF(p) \subseteq GF(p^p) \subseteq GF(p^{p^2}) \subseteq GF(p^{p^3}) \subseteq \cdots .$$

Let $GF(p^{p^\infty})$ denote the union of the above fields so that $GF(p^{p^\infty})$ is an infinite field of characteristic $p$.

Finite fields are discussed in detail by LIDL and NIEDERREITER in [5], while in [2], BRAWLEY and SCHNIBBEN discuss infinite algebraic extensions of finite fields. For our purposes we shall only need the following where we assume throughout that $GF(q)$ has characteristic $p$.

**Lemma 1.** *Let $b \in GF(q)$. Then the polynomial $x^p - x - b$ is irreducible over $GF(q)$ if and only if it has no root in $GF(q)$.*

PROOF. See [5, Thm. 3.78].

**Lemma 2.** *Let $x^p - x - b$ be irreducible over $GF(q)$ and let $\alpha$ be a root of $x^p - x - b$ in some extension field of $GF(q)$. Then the polynomial $x^p - x - b\alpha^{p-1}$ is irreducible over $GF(q^p)$.*

PROOF. This result may be found in [5, p.146] and a proof is given in [2].

Following BRAWLEY and SCHNIBBEN [2], we inductively define the polynomials $P_i(x)$, $i \geq 1$, by $P_1(x) = x^p - x - 1$ and $P_{i+1}(x) = x^p - x - \pi_i^{p-1}$ where $\pi_i = \alpha_1 \alpha_2 \ldots \alpha_i$ and $\alpha_j$ is a root of $P_j(x)$ for $j = 1, 2, \ldots, i$. If $a \in GF(p)$, then clearly $P_1(a) = -1 \neq 0$; hence by Lemma 1, $P_1(x)$ is irreducible over $GF(p)$. Moreover for $i \geq 2$ we may inductively apply Lemma 2 to see that $P_i(x)$ is irreducible over $GF(p^{p^i})$. It follows that the set

$$(2) \quad \mathbf{B}_i = \{{\alpha_1}^{k_1} {\alpha_2}^{k_2} \ldots {\alpha_i}^{k_i} : \ 0 \leq k_1 \leq p-1, \ldots, 0 \leq k_i \leq p-1\}$$

is basis for the finite field $GF(p^{p^i})$ over $GF(p)$; i.e., the elements of $GF(p^{p^i})$ are the $GF(p)$–linear combinations of elements of $B_i$ where all computations are done in the obvious manner using the reduction equations

$$(3) \qquad \alpha_j^p = \alpha_j + ({\alpha_1}^{p-1} {\alpha_2}^{p-1} \ldots {\alpha_{j-1}}^{p-1}), \ \ j = 1, 2, 3 \ldots .$$

From (1) and (2) we see that the union

$$(4) \qquad \mathbf{B} = \bigcup \{\mathbf{B}_i : i \geq 1\}$$

is a basis for $GF(p^{p^\infty})$ over $GF(p)$.

We now want to specify an ordering of $GF(p^{p^\infty})$. By means of (2) the members of $\mathbf{B}$ are naturally identified with the set of all sequences of the form $(k_1, k_2, k_3, \dots)$ where $0 \le k_j \le p-1$ and where all but a finite number of the $k_j$'s are 0. We define

(5) $(k_1, k_2, k_3, \dots) < (k_1', k_2', k_3', \dots)$ iff $k_i < k_i'$ and $k_j = k_j'$ for all $j > i$.

Then (5) is an ordering on the sequences of $k$'s which, in turn, induces a natural ordering on the members of $\mathbf{B}$. Let $\gamma_0, \gamma_1, \gamma_2, \dots$ denote the ordered basis of $GF(p^{p^\infty})$ obtained in this way so that $\gamma_0 = 1$, $\gamma_1 = \alpha_1$, $\gamma_2 = {\alpha_1}^2, \dots, \gamma_{p-1} = {\alpha_1}^{p-1}, \gamma_p = \alpha_2$, etc.. Note that the first $p^i$ members of $\gamma_0, \gamma_1, \gamma_2, \dots$ constitute the basis $\mathbf{B}_i$. Now each $\gamma \in GF(p^{p^\infty})$ is a unique finite linear combination of the ordered basis $\gamma_0, \gamma_1, \gamma_2, \dots$; i.e.,

$$\gamma = a_0\gamma_0 + a_1\gamma_1 + a_2\gamma_2 + \cdots + a_m\gamma_m\,, \tag{6}$$

where $0 \le a_i \le p-1$ with $a_m \ne 0$ for $\gamma \ne 0$. With each $\gamma \in GF(p^{p^\infty})$ we associate the positive integer $z(\gamma)$ whose base $p$ representation is $z(\gamma) = a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m$ and we order the elements of $GF(p^{p^\infty})$ by declaring

$$\gamma \le \gamma' \text{ if and only if } z(\gamma) \le z(\gamma')\,. \tag{7}$$

Note that with the ordering (7), the first $p^{p^i}$ elements of the ordered field $GF(p^{p^\infty})$ constitute the finite field $GF(p^{p^i})$.

As an illustration of this ordering, let $p = 2$ so that $P_1(x) = x^2 - x - 1$, $P_2(x) = x^2 - x - \alpha_1$ where $P_1(\alpha_1) = 0$, and in general $P_i(x) = x^2 - x - \alpha_1\alpha_2 \dots \alpha_{i-1}$ where $\alpha_j$ is a root of $P_j(x)$ for $j \ge 1$. Hence, the first 16 elements of $GF(2^{2^\infty})$ are the members of $GF(16)$ and are ordered as follows

$$\begin{gathered} 0,\, 1,\, \alpha_1,\, 1+\alpha_1,\, \alpha_2,\, 1+\alpha_2,\, \alpha_1+\alpha_2,\, 1+\alpha_1+\alpha_2,\, \alpha_1\alpha_2, \\ 1+\alpha_1\alpha_2,\, \alpha_1+\alpha_1\alpha_2,\, 1+\alpha_1+\alpha_1\alpha_2,\, \alpha_2+\alpha_1\alpha_2, \\ 1+\alpha_2+\alpha_1\alpha_2,\, \alpha_1+\alpha_2+\alpha_1\alpha_2,\, 1+\alpha_1+\alpha_2+\alpha_1\alpha_2\,. \end{gathered} \tag{8}$$

Note that the first 2 elements give $GF(2)$, and the first 4 elements give $GF(2^2)$.

*Remark.* The field $GF(2^{2^\infty})$ as described above is essentially the field $On_2$ used by Conway [3, p.50] in his analysis of certain games; indeed, by setting $\alpha_i = 2^{2^{i-1}}$ in each linear combination of basis elements and viewing the result as an integer, we obtain Conway's identification of the elements of $GF(2^{2^\infty})$ with the nonnegative integers. Note in this identification the ordered list (8) becomes the ordered list of integers from 0 to 15. Incidentally, WEIDEMANN [9] gives a different iterated presentation of $GF(2^{2^\infty})$ which apparently does not have a natural generalization to $GF(p^{p^\infty})$. These iterated presentations, as well as others, are described in detail in the forthcoming monograph [2].

## 4. Construction of Orthogonal Latin Squares

Consider now an infinite square whose rows and columns are indexed, starting from the top left corner, by the elements of the ordered field $GF(p^{p^\infty})$ where $p$ is a fixed prime. If $f(x,y)$ is a polynomial over $GF(p^{p^\infty})$, form an infinite square by placing the element $f(x,y)$ at the intersection of row $x$ and column $y$.

**Theorem 3.** *The collection of polynomials* $f_\alpha(x,y) = \alpha x + y$ *with* $\alpha \in GF(p^{p^\infty})$, $\alpha \neq 0$, *represents a complete set of* MOLS *of infinite order.*

PROOF. We first show that for a fixed $\alpha \neq 0$, the polynomial $f_\alpha(x,y)$ represents a Latin square of infinite order. Since the mappings on $GF(p^{p^\infty})$ defined by $w \to w$ and $w \to \alpha w$ are bijections of $GF(p^{p^\infty})$, we see that each element of $GF(p^{p^\infty})$ occurs exactly once in each row and column. Hence the square represented by $f_\alpha(x,y)$ is indeed a Latin square.

As there are clearly an infinite number of squares, it only remains to show that the collection $\{f_\alpha(x,y) : 0 \neq \alpha \in GF(p^{p^\infty})\}$ represents a complete set of MOLS of infinite order. To this end, let $(x_1, y_1)$ and $(x_2, y_2)$ be a pair of cells in different rows and columns so that $x_1 \neq x_2$ and $y_1 \neq y_2$. Further let $\alpha = (y_2 - y_1)/(x_1 - x_2)$ so that $\alpha x_1 + y_1 = \alpha x_2 + y_2$. It follows that the cells $(x_1, y_1)$ and $(x_2, y_2)$ are occupied by a common element in the square represented by the polynomial $f_\alpha(x,y) = \alpha x + y$. To show that no other square has a common element in cells $(x_1, y_1)$ and $(x_2, y_2)$, suppose in addition to $\alpha_1 x_1 + y_1 = \alpha_1 x_2 + y_2$ we also have $\alpha_2 x_1 + y_1 = \alpha_2 x_2 + y_2$ for some $0 \neq \alpha_1,\ \alpha_2 \in GF(p^{p^\infty})$. Then $\alpha_1(x_1 - x_2) = \alpha_2(x_1 - x_2)$ and since $x_1 \neq x_2$, we have $\alpha_1 = \alpha_2$. Hence the collection of squares represented by the polynomials $\{f_\alpha(x,y) : 0 \neq \alpha \in GF(p^{p^\infty})\}$ give a complete set of MOLS of infinite order. □

As a result of the ordering given above we may state

**Corollary 4.** *For each* $n \geq 0$ *the top left* $p^{p^n} \times p^{p^n}$ *subsquare of the first* $p^{p^n} - 1$ *squares represented by the polynomials given in Theorem 3 represent a complete set of* MOLS *of order* $p^{p^n}$.

**Corollary 5.** *The polynomials given in Theorem 3 represent a complete set of* MOLS *of infinite order containing nested complete sets of* MOLS *of order* $p^{p^n}$ *for* $n = 0, 1, 2, \ldots$.

One may view the construction given in Theorem 3 as a limiting case of the construction given in Corollary 2 of MULLEN [8]. The point here is that we have given an explicit construction in the sense that the element in any row and column of any of the squares may be directly calculated.

As an illustration consider the case $p = 2$. Let $(\beta_0, \beta_1, \beta_2, \dots)$ denote the ordered listing of the elements of the field $GF(2^{2^\infty})$ are previously specified so that the first 16 elements of $GF(2^{2^\infty})$ are given by (8). Then our construction yields the MOLS $(\beta_h\beta_i + \beta_j)$ for $h = 1, 2, \dots$ where $i = 0, 1, \dots$ and $j = 0, 1 \dots$. For example, the element in position $(\beta_6, \beta_3)$ of the square indexed by $\beta_4$ is

$$\begin{aligned} f_{\beta_4}(\beta_6, \beta_3) &= \beta_4\beta_6 + \beta_3 = \alpha_2(\alpha_1 + \alpha_2) + (1 + \alpha_1) = \alpha_1\alpha_2 + {\alpha_2}^2 + 1 + \alpha_1 \\ &= \alpha_1\alpha_2 + (\alpha_2 + \alpha_1\alpha_2) + 1 + \alpha_1 = 1 + \alpha_1 + \alpha_2 = \beta_7 . \end{aligned}$$

From these infinite squares we may construct the following nested complete sets of MOLS of finite order:

| | | |
|---|---|---|
| 3 | MOLS of order | 4 |
| 15 | · | 16 |
| 255 | · | 256 |
| 65,535 | · | 65,536 |

etc..

*Acknowledgement.* The authors would like to thank RON BAKER for pointing out that E. H. MOORE, and not R. C. BOSE, was the first to construct a complete set of MOLS in the prime power case.

## References

[1] R. C. BOSE, On the application of the properties of Galois fields to the construction of hyper–Graeco–Latin squares, *Sankhya* **3** (1938), 323–338.

[2] J. V. BRAWLEY and G. E. SCHNIBBEN, Infinite Algebraic Extensions of Finite Fields, *American Mathematical Society Series: Contemporary Mathematics*, Volume **95** Providence R.I. (1989).

[3] J. H. CONWAY, On Numbers and Games, *Academic Press, New York*, 1976.

[4] J. DÉNES and A. D. KEEDWELL, Latin Squares and their Applications, *Academic Press, New York*, 1974.

[5] R. LIDL and H. NIEDERREITER, Finite Fields, *Encyclo. Math. and Appls.*, V. **20**. Addison–Wesley, Reading, Mass. 1983. (Now distributed by Camb. Univ. Press.)

[6] K. MANO, On the reduced number of the latin squares of the $n$th order, *Sci. Rep. Fac. Lit. Sci. Hirosaki Univ.* **7** (1960), 1–2.

[7] E. H. MOORE, Tactical Memoranda I–III, *Amer. J. Math.* **18** (1896), 264–303.

[8] G. L. MULLEN, Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order, *Discrete Mathematics* **69** (1988), 79–84.

[9] D. WIEDEMANN, An Iterated Quadratic Extension of $GF(2)$, *Fibonacci Quart.* **26** (1988), 290–295.

J. V. BRAWLEY
DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY
CLEMSON, SOUTH CAROLINA 29634

GARY L. MULLEN
DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PENNSYLVANIA 16802

*(Received Oktober 21, 1988)*