# A new family of nested row-column designs

K.T. Arasu* and A.B. Evans
Department of Mathematics and Statistics
Wright State University
Dayton, Ohio 45435, U.S.A.

R. Balasubramanian
Institute of Mathematical Sciences
Madras-600113
India

ABSTRACT. Using the characterization of those prime powers $q$ for which $GF(q)$ admits a quadratic starter: i.e. a pairing $(x_i, y_i), i = 1, 2, \ldots, \frac{q-1}{2}$, of nonzero squares $x_i$ with nonsquares $y_i$ in $GF(q)$ such that the differences $\pm(x_i - y_i)$ are all distinct, we obtain a new infinite family of nested row-column designs.

## 1 Introduction

Let $G$ be an abelian group of order $2t+1$. A starter in $G$ is a partition of the nonzero elements of $G$ into pairs $(x_i, y_i), i = 1, \ldots, t$, such that $\{\pm(x_i - y_i) \mid i = 1, \ldots, t\} = G - \{0\}$. For more on starters, refer to Wallis, Wallis and Street [10]. If $G = GF(q)$ (additive group) and the starter pairs a nonzero square in $GF(q)$ with a nonsquare in $GF(q)$, we call it a "quadratic starter". Existence of quadratic starters in $GF(q)$ for $q \equiv 3 \pmod 4$ is easy to establish and well-known (see Mullin and Nemeth [7]). $\{(x, Ax) : x$ a nonzero square$\}$ is a quadratic starter whenever $q \equiv 3 \pmod 4$ and $A$ is a nonsquare. The case $q \equiv 1 \pmod 4$ is so far open. A few sporadic cases have been dealt with by Sreenath [8] and Aggarwal and Arasu [1]. Using the concept of orthomorphisms (for more on orthomorphisms, refer to Evans [4]), we prove: for $q \equiv 1 \pmod 4, q-1$ not a

*Research partially supported by AFOSR grant F49620-96-1-0328 and by NSA grant #MDA904-97-1-0012.

power of 2, $GF(q)$ admits a quadratic starter. An alternate proof of this is in [3].

As a consequence of these quadratic starters, along the lines of Aggarwal and Arasu [1], we obtain a new infinite family of nested row-column designs.

Recent work of Morgan and Uddin [6] contains several examples of nested row-column designs. But our examples contain such designs where $b = v$ and each block is a $2 \times \left(\frac{v-1}{2}\right)$ array. These do not follow from the results of [6].

## 2 Preliminaries

In this section we provide all the preliminary results we need to prove our results. First we introduce the concept of orthomorphisms.

Let $G$ be a finite group. A bijection $\theta : G \to G$ is said to be an orthomorphism if $\theta - I_G$ is also a bijection of $G$. (Here $(\theta - I_G)(x) = \theta(x) - x$). Cyclotomic orthomorphisms use cyclotomic classes in $GF(q)$: Let $q = ef + 1$ and $g$ a primitive element in $GF(q)$. For $i = 0, 1, \ldots, e-1$, define $C_i = \left\{g^{ej+i} \mid j = 0, 1, \ldots, f-1\right\}$. $C_i$ is called the $i^{th}$ cyclotomic class of index $e$.

For $A_0, \ldots, A_{e-1} \in GF(q)$, define $[A_0, \ldots, A_{e-1}] : GF(q) \to GF(q)$ by

$$0 \to 0$$

$$x \to A_i x \text{ if } x \in C_i$$

Then $[A_0, \ldots, A_{e-1}]$ is an orthomorphism of $GF(q)$ if and only if $(i)\, C_i \to A_i C_i$ permutes $C_0, \ldots, C_{e-1}$ and $(ii)\, C_i \to (A_i - 1) C_i$ permutes $C_0, \ldots, C_{e-1}$. These will be referred to as cyclotomic orthomorphisms of index $e$. Note: cyclotomic orthomorphisms of index 2 are usually called quadratic orthomorphisms, not to be confused with quadratic starters. For more on orthomorphisms and related topics, see Evans [4].

We also need the following number theory result.

**Result 2.1:** (Ljunggren[5]). The only (non-negative) integer solutions of

$$\frac{x^n - 1}{x - 1} = y^2, n > 2$$

are $(n, x, y) = (4, 7, 20)$ or $(5, 3, 11)$.

## 3 Quadratic starters in $GF(q)$ for $q \equiv 1 \pmod 4$.

Let $q = ef + 1$, $e$ a power of 2, $e \neq 2$, $f$ odd, $f > 1$. (Thus we assume that $q - 1$ is not a power of 2.) We assert that for some cyclotomic class $C_\alpha, \alpha$

odd, we can find $A, B \epsilon C_\alpha$ such that $(i)\, A-1$ is a square and $(ii)\, B-1$ is a nonsquare.

To prove this, we proceed by assuming the contrary. Then for each nonsquare $k$, and each $w \in C_0$, $(k-1)(wk-1)$ is a square and so $(wk-1)^{\frac{q-1}{2}} - \varepsilon = 0$, where $\varepsilon = \left(\frac{1}{k-1}\right)^{\frac{q-1}{2}}$. As the $f$ distinct roots of $x^f - 1 = 0$ are precisely the elements of $C_0$, $g(x) = (xk-1)^{\frac{q-1}{2}} - \varepsilon \equiv 0$ modulo $x^f - 1$ in $GF(q)[x]$. Thus the reduction of $g(x)$ modulo $x^f - 1$ is the zero polynomial and in particular the coefficient of $x$ in this reduction is zero, i.e.

$$\sum_{i \equiv 1 \mod f \left(0 \le i \le \frac{q-1}{2}\right)} \binom{\frac{q-1}{2}}{i} k^i (-1)^{\frac{q-1}{2}-i} = 0 \qquad (1)$$

(1) is a polynomial expression in $k$. It is not identically zero, since the coefficient of $k$ is $\left(\frac{q-1}{2}\right)(-1)^{\frac{q-3}{2}} \neq 0$. Since each nonsquare $k$ is a root of (1), the degree of this polynomial is at least $\frac{q-1}{2}$. But since the index $i$ was over the range $\left[0, \frac{q-1}{2}\right]$ with $i \equiv 1 (\mod f)$, its degree is at most $\frac{q-1}{2} + 1 - f$. Thus $\frac{q-1}{2} \le \frac{q-1}{2} + 1 - f$, which is impossible since $f > 1$; proving the assertion. Let $\alpha$ be odd such that $A, B \epsilon C_\alpha$, A-1 is a square, B-1 is a nonsquare. Then $A^{-1}, B^{-1} \epsilon C_{e-\alpha}$.

Now we claim that

$$\begin{array}{rll} & 0 \to & 0 \\ \theta: & x \to & Ax \text{ if } x \epsilon C_{e/2}, C_{e/2}+2, \ldots, C_{e-2} \\ & x \to & Bx \text{ if } x \epsilon C_0, C_2, \ldots, C_{e/2}-2 \\ & x \to & A^{-1}x \text{ if } x \epsilon C_{e/2+\alpha}, C_{\frac{e}{2}+2+\alpha}, \ldots, C_{e-2+\alpha} \\ & x \to & B^{-1}x \text{ if } x \epsilon C_\alpha, C_{2+\alpha}, \ldots, C_{\frac{e}{2}-2+\alpha} \end{array}$$

is a cyclotomic orthomorphism (that gives rise to a quadratic starter). To see this we observe$(i)\, \theta$ is a bijection of $GF(q)$ that maps squares to nonsquares and vice versa.

(Reason:

$$\begin{array}{ll} & \left\{C_{i+\alpha} \mid i = \frac{e}{2}, \frac{e}{2}+2, \ldots, e-2\right\} \\ \cup & \left\{C_{i+\alpha} \mid i = 0, 2, \ldots, \frac{e}{2}-2\right\} \\ \cup & \left\{C_{e-\alpha+i} \mid i = \frac{e}{2}+\alpha, \ldots, e-2+\alpha\right\} \\ \cup & \left\{C_{e-\alpha+i} \mid i = \alpha, 2+\alpha, \ldots, \frac{e}{2}-2+\alpha\right\} \\ = & \{C_i \mid i = 0, 1, \ldots, e-1\}.) \end{array}$$

$(ii) A - 1 \epsilon C_{2\beta}$ (say) $\Rightarrow \theta - I$ sends $C_i \to C_{2\beta+i}$ for $i = \frac{e}{2}, \frac{e}{2}+2, \ldots, e-2$

$B - 1 \epsilon C_{2\gamma+1}$ (say) $\Rightarrow \theta - I$ sends $C_i \to C_{2\gamma+1+i}$ for $i = 0, 2, \ldots, \frac{e}{2}-2$

$A^{-1} - 1 = -(A-1)\,A^{-1}\epsilon C_{\frac{e}{2}-\alpha+2\beta}$

(Note: $-1\epsilon C_{e/2}$)

$\Rightarrow \theta - I$ sends $C_i \to C_{\frac{e}{2}-\alpha+i+2\beta}$ for $i = \frac{e}{2}+\alpha, e/2+2+\alpha, \ldots, e-2+\alpha$

Finally $B^{-1} - 1 = -(B-1)\,B^{-1}\epsilon C_{e/2-\alpha+2\gamma+1} \Rightarrow \theta - I$ sends $C_i \to C_{e/2-\alpha+2\gamma+1+i}$ for $i = \alpha, 2+\alpha, \ldots, e\ /\ 2-2+\alpha$ thus $\theta - I$ permutes $C_i$ $(i = 0, \ldots, e-1)$. Thus, we've proved:

**Theorem 1.** *For $q \equiv 1 (\mod 4), q-1$ not a power of 2, $GF(q)$ admits an orthomorphism, that gives rise to a quadratic starter.*

## 4 The case $q-1 =$ a power of 2.

In this section, we examine the exceptional case of Section 3, where $q-1$ is a power of 2. Write $q = p^r$ and assume $p^r - 1 = 2^n$.

**Proposition (4.1).** *Let $p$ be a prime such that $p^r - 1 = 2^n$. Then either $p$ is a Fermatt prime, i.e. $p = 2^{2^s}+1$ for some non-negative integer $s$, or $n = 3$ and $p^r = 9 = 3^2$.*

**Proof Case (1):** $r = 1$. Then $p = 2^n + 1$. If $n$ is odd, $p = 3$, because $2^n + 1 \equiv 0 (\mod 3)$ for any odd $n$. So, suppose $n$ is even. Write $n = 2^s \cdot t$, where $t$ is odd. Now $p = 2^{2^s \cdot t} + 1 \equiv 0 \left(\mod 2^{2^s}+1\right)$ since $t$ is odd. But then $p = 2^{2^s}+1$, since $p$ is a prime.

**Proof Case (2):** $r = 2$. Then $p^2 = 2^n + 1$. It is an easy exercise in elementary number theory: $2^n + 1$ is a perfect square if, and only if, $n = 3$. Hence, $p^2 = 9$.

**Proof Case (3):** $r > 2$. We've $p^r - 1 = 2^n \equiv 0 (\mod p-1)$. Hence, $p-1$ is also a power of 2. If $n$ is odd, $2^n + 1 \equiv 0 (\mod 3)$ implies $p = 3$. Hence, if $n$ is odd, $\frac{3^r-1}{3-1} = 2^{n-1}$ is impossible by Result 2.1.

If $n$ is even, $p - 1 = 2^m$ for some even integer $m$.

Thus, $\frac{p^r-1}{p-1} = 2^{n-m}$, (note: $n-m$ even) is again impossible by Result 2.1

This complete the proof of Proposition 4.1

**Remarks:** For the cases $q = 5$ and $q = 9, GF(q)$ does not admit a quadratic starter. For other known Fermatt primes, $q = 17, q = 257$, and $q = 65,537$, $GF(q)$ admits a quadratic starter.

For $q = 17$, the following serves as a quadratic starter:

$$\begin{pmatrix} 1 & 2 & 4 & 8 & 9 & 13 & 15 & 16 \\ 3 & 5 & 12 & 7 & 14 & 6 & 11 & 10 \end{pmatrix}.$$

For $q = 257$ & $q = 65,537$, Dillon [2] obtained quadratic starters using a computer search.

## 5 Application

A balanced incomplete block design with nested row and columns is an arrangement of $v$ treatments in $b$ blocks satisfying:

(i) each block is a $p \times q$ array of $pq$ plots,

(ii) every treatment occurs at most once in each block,

(iii) every treatment occurs in exactly $r$ blocks,

(iv) for every pair of treatments $i \neq i', p\lambda^R_{i,i'} + q\lambda^C_{i,i'} - \lambda_{i,i'} = \lambda = \frac{r(p-1)(q-1)}{v-1}$.

Here $\lambda^R_{i,i'}$ and $\lambda^C_{i,i'}$ denote respectively the number of rows and columns of the blocks in which treatment pair $(i, i')$ occurs together and $\lambda_{i,i'}$ denotes the number of blocks in which $(i, i')$ occurs together. We let $BIBRC\,(v, b, r, p, q, \lambda)$ denote such a design and all of them simply nested row-column designs.

Aggarwal and Arasu [1] implicitly used the idea of quadratic starters in a finite field and obtained a new construction of $BIBRC$ in which each block has two rows and the number of treatments is $v^\alpha, v \equiv 5 \pmod 8, v > 5, v$ a prime power, $\alpha$ any positive integer.

Their construction produces a quadratic starter only when $GF\,(v)$ admits a special type of primitive element. Our results in this paper strengthen the results of [1] in two ways: (i) we do not require any special type of primitive elements in $GF\,(q)$ (ii) we establish such quadratic starters whenever $q-1$ is not a power of 2. (The case of [1], $v \equiv 5\,(mod 8), v > 5$ is hence covered here completely.) Along the lines of [1], we obtain

**Theorem (5.1).** *Suppose $GF(q)$ admits a quadratic starter: $\{x_i, y_i\}, i = 1, \ldots, \frac{q-1}{2}$, where $\{x_i\} = \left(GF\,(q)^*\right)^2$ and $y_i = GF(q) \setminus \left((GF\ (q^*))^2 \cup \{0\}\right)$.*

Then $\binom{x_1, x_2 \ldots x_{\frac{q-1}{2}}}{y_1, y_2 \ldots y_{\frac{q-1}{2}}}$ serves as the initial block of a nested row-column design with parameters $\left(v = q; b = q; r = q-1; \lambda = \frac{q-3}{2}\right)$, where each block is a $2 \times \left(\frac{q-1}{2}\right)$array.

Hence, these designs exist for all prime powers $q, q-1$ not a power of 2, including the Fermatt primes $q = 17, q = 257$ & $q$ =65,537.

Combining Theorem 5.1 with a result of Uddin [9], we obtain

**Theorem (5.2).** *Let $q$ be a prime power such that $q-1$ is not a power of 2 or $q = 17, q = 257, q = 65,537$. Then for each positive integer $\alpha$, there exists a nested row-column design with parameters*

$$\left(v = q^\alpha; b = \frac{q^\alpha\,(q^\alpha - 1)}{q-1}; r = q^\alpha - 1; \lambda = \frac{q-3}{2}\right)$$

*where each block is a $2 \times \left(\frac{q-1}{2}\right)$ array.*

## References


[1] M.L. Aggarwal and K.T. Arasu, A new family of balanced incomplete block designs with nested rows and columns, *Australasian J. Comb.*, **12** (1995), 295–299.

[2] J.F. Dillon, (Private communication).

[3] Ding-Zhu Du and F.K. Hwang, Existence of symmetric skew balanced starters for odd prime powers, *Proceedings of American Mathematical Society* **104** (1988), 660–667.

[4] A.B. Evans, Orthomorphism graphs of groups, *Lecture notes in Math.* **1535**, Springer, New York (1992).

[5] W. Ljunggren, Neon Setninger on Ubestemte Likninger A. J. Forman $\frac{x^*-1}{x-1} = y^q$, *Norsk. Matem. Tidskrift*, (1943), 17–20.

[6] J.P. Morgan and N. Uddin, Optimal blocked main effect plans with nested rows and columns and related designs, *The Annals of Statistics* **24**, No. 3 (1996), 1185–1208.

[7] R.C. Mullin and E. Nemeth, An existence theorem for room squares, *Canad. Mathematical Bull.* **12** No. 4 (1969), 493–497.

[8] P.R. Sreenath, Construction of some balanced incomplete designs with nested rows and columns, *Biometrika* **76** (1989), 359–402.

[9] N. Uddin, Constructions for some balanced incomplete designs with nested rows and columns, *J. Stat. Planning and Inf.* **31** (1992), 253–261.

[10] W.D. Wallis, J. Wallis and A.P. Street, Combinatorics: Room squares, sum-free sets, Hadamard Matrices, *Lecture notes in Math.* **292**, Springer, New York, (1972).