ORDERINGS OF FINITE FIELDS AND BALANCED TOURNAMENTS

MARK B. BEINTEMA, JEFFREY T. BONN
ROBERT W. FITZGERALD AND JOSEPH L. YUCAS

Department of Mathematics
Southern Illinois University
Carbondale, IL 62901-4408

INTRODUCTION

A round robin tournament for the n teams $0, 1, \ldots, n-1$ is a collection of $n-1$ rounds in which each team plays once in every round and each team plays every other team in some round. For example,

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

is a round robin tournament for the 8 teams $0, 1, \ldots, 7$. Constructions of round robin tournaments with a variety of features have appeared throughout the literature. Russell [3] introduced the notion of balancing carry-over effects in round robin tournaments. Note that in the previous example Teams $2, 3, 4, 5$ and 7 each play Team 6 immediately before they play Team 1. If Team 6 is a particularly strong team then Teams $2, 3, 4, 5$ and 7 may enter their succeeding round against Team 1 demoralized, providing an advantage for Team 1. Russell's concept of balance is to eliminate such advantages. More specifically, let $O_r(j)$ denote the opponent of Team j in round r.

ARS COMBINATORIA 49(1998), pp. 41-48

Say Team i *affects* Team j if $i = O_{r-1}(O_r(j))$ for some $r \in \{1, 2, \ldots, n-1\}$. Here arithmetic is done mod $n-1$ on the set $\{1, 2, \ldots, n-1\}$ so when the subscript $r-1$ equals 0 we mean round $n-1$. The tournament is said to be *balanced with respect to carry-over effects* if each team is affected by every other team.

Russell showed that such a tournament can be constructed if n is a 2-power and conjectured that this condition is necessary. Briefly, his construction is as follows: Let $n = 2^m$ and $GF(2^m) = \{0 = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be ordered in such a way that the partial sums $S_t = \sum_{i=1}^{t} \alpha_i$ are distinct for $t = 1, \ldots, n-1$. Note that $S_{n-1} = 0$ and that $n-1$ field elements are accounted for. Let α_N be the remaining element. Then we set

$$i = O_r(j) \quad \text{if and only if} \quad \alpha_i = \alpha_j + \alpha_N + S_{r-1}.$$

In the first section of this paper we will show that the orderings of $GF(q^m)$ studied in [1] and [2] have distinct partial sums, thus satisfying Russell's condition. For orderings of this type we will also explicitly describe the "missing element" α_N.

In the second section of this paper we introduce the concept of completely balanced tournaments, strengthening Russell's concept of balance, and show that Russell's construction produces completely balanced tournaments when applied to the orderings of [1] and [2]. We will then show that the existence of a tournament balanced in this stronger sense implies the existence of a complete set of mutually orthogonal Latin squares.

1. Orderings from Primitive Polynomials.

By an ordering of a finite field, we simply mean a listing of the nonzero elements.

Proposition 1. *Let $p(x) = x^m - \sum_{i=0}^{m-1} c_i x^i$ be any primitive polynomial over $GF(q)$, and let $\{\alpha_1, \ldots, \alpha_m\}$ be any basis for $GF(q^m)$. For each $k > m$, set*

$$\alpha_k = \sum_{i=0}^{m-1} c_i \alpha_{k-m+i}.$$

Then with this ordering, the partial sums $S_t = \sum_{i=1}^{t} \alpha_i$ are distinct for $t = 1, \ldots, n-1$.

Proof. Let β be a primitive root of $p(x)$. Define a linear operator T on $GF(q^m)$ by setting $T(\alpha_{j+1}) = \beta^j$ for $j = 0, \ldots, m-1$ and extending linearly.

We show inductively that $T(\alpha_{j+1}) = \beta^j$ for $j = 0, \ldots, n-2$. First note that

$$\beta^m = \sum_{j=0}^{m-1} c_j \beta^j = \sum_{j=0}^{m-1} c_j T(\alpha_{j+1})$$
$$= T(\sum_{j=0}^{m-1} c_j \alpha_j) = T(\alpha_{m+1})$$

Now assume that $T(\alpha_{j+1}) = \beta^j$ for all $j < m+k$; then

$$T(\alpha_{m+k}) = T(\sum_{j=0}^{m-1} c_j \alpha_{j+k}) = \sum_{j=0}^{m-1} c_j T(\alpha_{j+k})$$
$$= \sum_{j=0}^{m-1} c_j \beta^{j+k-1} = \beta^{m+k-1}$$

Now note that the sums $\sum_{i=0}^{t-1} \beta^i$ are distinct, and that the operator T is invertible. Thus the sums

$$S_t = \sum_{i=1}^{t} \alpha_i = \sum_{i=0}^{t-1} T^{-1}(\beta^{i-1}) = T^{-1}(\sum_{i=0}^{t-1} \beta^{i-1})$$

are distinct as well. □

Proposition 2. *Let $p(x) = x^m - \sum_{i=0}^{m-1} c_i x^i$ be any primitive polynomial over $GF(q)$, and let $\{\alpha_1, \ldots, \alpha_m\}$ be any basis for $GF(q^m)$. For each $k > m$, set $\alpha_k = \sum_{i=0}^{m-1} c_i \alpha_{k-m+i}$. Then the only element of $GF(q^m)$ that does not arise as some S_k is*

$$\alpha = \sum_{i=0}^{m-1} \varepsilon_i \alpha_{i+1}$$

where

$$\varepsilon_i = 1 + \frac{\gamma_i}{1 - \gamma_{m-1}} \quad \text{for } i = 0, \ldots, m-1, \quad \text{and} \quad \gamma_i = \sum_{j=0}^{i} c_j.$$

Proof. Applying the map T used in the proof of Proposition 1, we see that an element $\alpha = \sum_{i=0}^{m-1} \varepsilon_i \alpha_{i+1} \in GF(q^m)$ ($\varepsilon_i \in GF(q)$) appears as a partial sum S_k if and only if

$$\sum_{i=0}^{k} \beta^i = \sum_{i=0}^{m-1} \varepsilon_i \beta^i \tag{1}$$

Multiplying the expression (1) by β yields

$$\begin{aligned}\sum_{i=1}^{k+1}\beta^i &= \sum_{i=0}^{m-1}\varepsilon_{i-1}\beta^i + \varepsilon_{m-1}\beta^m \\ &= \sum_{i=0}^{m-1}\varepsilon_{i-1}\beta^i + \varepsilon_{m-1}\sum_{i=0}^{m-1}c_i\beta^i \\ &= \sum_{i=0}^{m-1}(\varepsilon_{i-1}+\varepsilon_{m-1}c_i)\beta^i \qquad (\text{with } \varepsilon_{-1}=0) \qquad (2)\end{aligned}$$

Subtracting expression (2) from (1) we have

$$1-\beta^{k+1} = \sum_{i=0}^{m-1}(\varepsilon_i - \varepsilon_{i-1} - \varepsilon_{m-1}c_i)\beta^i \qquad (3)$$

Now α is equal to some S_k if and only if (3) holds. Since the powers of β generate the nonzero elements of $GF(q^m)$, the left hand side of (3) can be any element except 1. Thus the only element which does not arise as an S_k is $\alpha = \sum_{i=0}^{m-1}\varepsilon_i\beta^i$ satisfying

$$\sum_{i=0}^{m-1}(\varepsilon_i - \varepsilon_{i-1} - \varepsilon_{m-1}c_i)\beta^i = 1$$

Equating the coefficients ε_i, we have

$$\begin{aligned}\varepsilon_0 - \varepsilon_{m-1}c_0 &= 1 \\ \varepsilon_1 - \varepsilon_0 - \varepsilon_{m-1}c_1 &= 0 \\ \varepsilon_2 - \varepsilon_1 - \varepsilon_{m-1}c_2 &= 0 \\ &\vdots \\ \varepsilon_{m-1} - \varepsilon_{m-2} - \varepsilon_{m-1}c_{m-1} &= 0\end{aligned}$$

Thus we want $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1}$ such that

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & -c_0 \\ -1 & 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & -1 & 1 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & -1 & 1 & \cdots & 0 & -c_3 \\ & \vdots & & \vdots & & \vdots & \\ & \vdots & & \vdots & & \vdots & \\ & \vdots & & \vdots & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1-c_{m-1} \end{bmatrix} \begin{bmatrix} \varepsilon_0 \\ \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \vdots \\ \vdots \\ \vdots \\ \varepsilon_{m-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}.$$

This is readily solved by adding the first row to the second, then adding the second row to the third, and so on. Setting $\gamma_i = \sum_{j=0}^{i} c_j$, this yields

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & -\gamma_0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & -\gamma_1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & -\gamma_2 \\ 0 & 0 & 0 & 1 & \cdots & 0 & -\gamma_3 \\ & \cdot & & \cdot & & \cdot & \\ & \cdot & & \cdot & & \cdot & \\ & \cdot & & \cdot & & \cdot & \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1-\gamma_{m-1} \end{bmatrix} \begin{bmatrix} \varepsilon_0 \\ \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \cdot \\ \cdot \\ \cdot \\ \varepsilon_{m-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix}.$$

Now $p(x)$ is primitive, hence irreducible. In particular, $p(1) \neq 0$, and so $\gamma_{m-1} \neq 1$. It follows that the matrix above has full rank. Consequently, $\varepsilon_{m-1} = \dfrac{1}{1-\gamma_{m-1}} = 1 + \dfrac{\gamma_{m-1}}{1-\gamma_{m-1}}$, and for $0 \leq i \leq m-2$, we have $\varepsilon_i = 1 + \dfrac{\gamma_i}{1-\gamma_{m-1}}$, as desired. □

We end this section with an example of an ordering of $GF(16)$ which does not arise from a primitive polynomial, but for which the partial sums are distinct.

Example. We assume that some fixed basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is given, and write the nonzero elements in terms of their coordinates relative to this basis.

(1,0,0,0)	(1,1,1,1)
(0,1,0,0)	(1,1,0,1)
(0,0,1,0)	(0,0,1,1)
(0,0,0,1)	(1,0,1,0)
(1,1,0,0)	(0,1,1,0)
(1,0,0,1)	(1,1,1,0)
(1,0,1,1)	(0,1,0,1)
(0,1,1,1)	

The reader can easily verify that the only vector which does not appear as a partial sum is $(0,0,1,0)$. Moreover, $\alpha_5 = \alpha_1 + \alpha_2$, but $\alpha_6 \neq \alpha_2 + \alpha_3$, so the ordering cannot have been obtained from a primitive polynomial. □

2. Completely Balanced Round Robin Tournaments

Say that Team i affects Team j at level ℓ if $i = O_{r-\ell}(O_r(j))$ for some $r \in \{1,2,\ldots,n-1\}$. Here again arithmetic is done mod $n-1$ on the set $\{1,2,\ldots,n-1\}$ so $0 = n-1$, $-1 = n-2$ etc. The tournament will be called

balanced at level ℓ if each team is affected by every other team at level ℓ and we say that the tournament is *completely balanced* if it is balanced at level ℓ for each $\ell \in \{1, 2, \ldots, n-2\}$. Notice that balance at level 1 is just Russell's concept of balance.

Proposition 4. *Let $p(x) = x^m - \sum_{i=0}^{m-1} c_i x^i$ be any primitive polynomial over $GF(2)$, and let $\{\alpha_1, \ldots, \alpha_m\}$ be any basis for $GF(2^m)$. For each $k > m$, set $\alpha_k = \sum_{i=0}^{m-1} c_i \alpha_{k-m+i}$. If Russell's construction is applied with this ordering, the resulting tournament is completely balanced.*

Proof. Suppose that for some r, r', we have $i = O_{r-\ell}(O_r(j)) = O_{r'-\ell}(O_{r'}(j))$. Thus there exist k, k' such that

$$\alpha_i = \alpha_k + \alpha_N + S_{r-\ell-1} = \alpha_{k'} + \alpha_N + S_{r'-\ell-1}$$
$$\alpha_j = \alpha_k + \alpha_N + S_{r-1} = \alpha_{k'} + \alpha_N + S_{r'-1}$$

That is, $\alpha_j - \alpha_i = S_{r-1} - S_{r-\ell-1} = S_{r'-1} - S_{r'-\ell-1}$. This implies that

$$\sum_{i=r-\ell}^{r-1} \alpha_i = \sum_{i=r'-\ell}^{r'-1} \alpha_i \tag{4}$$

To show that Russell's constuction gives a completely balanced tournament it suffices to show that (4) holds if and only if $r = r'$. Applying the map T from Proposition 1 yields

$$\sum_{i=r-l}^{r-1} \beta^{i-1} = \sum_{i=r'-l}^{r'-1} \beta^{i-1} \quad \Longrightarrow \quad \beta^{r-l-1} \sum_{i=0}^{l-1} \beta^i = \beta^{r'-l-1} \sum_{i=0}^{l-1} \beta^i$$

and consequently $r = r'$. □

REMARK: If Russell's construction is applied to the example at the end of Section 1, the resulting tournament is not completely balanced. In fact, it is easily verified that $\alpha_1 + \alpha_2 = \alpha_7 + \alpha_8$, so the tournament is not even balanced at level 2.

Lemma 5. *In a round robin tournament balanced at level ℓ*

$$O_{r-\ell}(j) = O_{r'-\ell}(j') \text{ implies } O_r(j) \neq O_{r'}(j') \text{ for } r \neq r'.$$

Proof. If $O_r(j) = O_{r'}(j')$ then

$$\begin{aligned} O_{r-\ell}O_r(O_r(j)) = O_{r-\ell}(j) &= O_{r'-\ell}(j') \\ &= O_{r'-\ell}O_{r'}(O_{r'}(j')) = O_{r'-\ell}O_{r'}(O_r(j)). \end{aligned}$$

Now if $r \neq r'$ then this says that $O_r(j)$ is being affected at level ℓ twice by the same team. This contradicts balance at level ℓ. □

For $i = 0, 1, \ldots, n-1$ and $j = 1, 2, \ldots, n$ define $A_0 = [a_{ij}]$ by $a_{0j} = j$, $a_{ij} = O_i(j)$ for $i \neq 0$. For $\ell = 1, 2, \ldots, n-2$ define $A_\ell = [a_{ij}]$ by $a_{0j} = j$, $a_{ij} = O_{i-\ell}O_i(j)$ for $i \neq 0$.

Theorem 6. *For a completely balanced round robin tournament, A_ℓ, $\ell = 0, 1, \ldots, n-2$ form a complete set of mutually orthogonal Latin squares.*

Proof. The fact that A_ℓ is a Latin square just follows from the fact that we have a round robin tournament. Each team occurs exactly once in each row of A_ℓ, $\ell \neq O$, since O_r is an injective mapping. Each team occurs exactly once in each row of A_ℓ, $\ell \neq 0$, since we have balance at level ℓ. Hence A_ℓ, $\ell = 0, 1, \ldots, n-2$ are Latin squares. To show A_0 and A_ℓ, $\ell \neq 0$, are orthogonal notice that if $O_i(j_1) = O_{i'}(j_2)$ then $O_{i-\ell}O_i(j_1) \neq O_{i'-\ell}O_{i'}(j_2)$ if $i \neq i'$ since the tournament is round robin. Finally to show A_{ℓ_1} and A_{ℓ_2} are orthogonal for $\ell_1 \neq 0$, $\ell_2 \neq 0$ we must show $O_{i-\ell_1}O_i(j_1) = O_{i'-\ell_1}O_{i'}(j_2) \Rightarrow O_{i-\ell_2}O_i(j_1) \neq O_{i'-\ell_2}O_{i'}(j_2)$ for $i \neq i'$. This follows from Lemma 5 by taking $j = O_i(j_1)$, $j' = O_{i'}(j_2)$, $r = i - \ell_2$, $r' = i' - \ell_2$ and $\ell = \ell_1 - \ell_2$. □

REMARK: In view of Theorem 6, the existence of a completely balanced tournament of order n implies the existence of a projective plane of order n. Thus the prime power conjecture for projective planes implies Russell's conjecture for the completely balanced case.

As an example we show Russell's tournament for $n = 8$, constructed using the ordering obtained from listing the powers of β, a primitive root of $x^3 + x^2 + 1$ over $GF(2)$.

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

Now we compute 3 of the 7 Latin squares for this tournament, coming from Theorem 6.

$$A_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\ 4 & 3 & 5 & 1 & 0 & 2 & 7 & 6 \\ 5 & 7 & 4 & 6 & 2 & 0 & 3 & 1 \\ 6 & 2 & 1 & 5 & 7 & 3 & 0 & 4 \\ 7 & 5 & 3 & 2 & 6 & 1 & 4 & 0 \\ 1 & 0 & 6 & 4 & 3 & 7 & 2 & 5 \\ 2 & 6 & 0 & 7 & 5 & 4 & 1 & 3 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 6 & 1 & 4 & 0 \\ 1 & 0 & 6 & 4 & 3 & 7 & 2 & 5 \\ 2 & 6 & 0 & 7 & 5 & 4 & 1 & 3 \\ 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \\ 4 & 3 & 5 & 1 & 0 & 2 & 7 & 6 \\ 5 & 7 & 4 & 6 & 2 & 0 & 3 & 1 \\ 6 & 2 & 1 & 5 & 7 & 3 & 0 & 4 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 5 & 1 & 0 & 2 & 7 & 6 \\ 5 & 7 & 4 & 6 & 2 & 0 & 3 & 1 \\ 6 & 2 & 1 & 5 & 7 & 3 & 0 & 4 \\ 7 & 5 & 3 & 2 & 6 & 1 & 4 & 0 \\ 1 & 0 & 6 & 4 & 3 & 7 & 2 & 5 \\ 2 & 6 & 0 & 7 & 5 & 4 & 1 & 3 \\ 3 & 4 & 7 & 0 & 1 & 6 & 5 & 2 \end{bmatrix}$$

REFERENCES

1. R.W. Fitzgerald and J.L. Yucas, *On generating linear spans over $GF(p)$*, Congressus Numerantium **69** (1989), 55–60.
2. G.L. Mullen and W.S. Chou, *Generating linear spans over finite fields*, Acta Arith. **61** (1992), 183–191.
3. K.G. Russell, *Balancing carry-over effects in round robin tournaments*, Biometrika **67** (1980), 127–131.