Finally, someone interested in the problems considered in this paper, could do no better than consulting Selmer's research monograph [12].

References

[1] R. Alter and J. A. Barnett, *A postage stamp problem*, Amer. Math. Monthly 87 (1980), 206–210.

[2] A. Brauer and J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), 215–220.

[3] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York 1981.

[4] G. Hofmeister, *Asymptotische Abschätzungen für dreielementige Extremalbasen in natürlichen Zahlen*, J. Reine Angew. Math. 232 (1968), 77–101.

[5] — *Die dreielementigen Extremalbasen*, ibid. 339 (1983), 207–214.

[6] W. Klotz, *Extremalbasen mit fester Elementeanzahl*, ibid. 237 (1969), 194–220.

[7] S. Mossige, *Algorithms for computing the h-range of the postage stamp problem*, Math. Comp. 36 (1981), 575–582.

[8] — *On extremal h-bases A_4*, Math. Scand. 61 (1987), 5–16.

[9] Ö. J. Rödseth, *On a linear Diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.

[10] — *On h-bases for n*, Math. Scand. 48 (1981), 165–183.

[11] H. Rohrbach, *Ein Beitrag zur additiven Zahlentheorie*, Math. Z. 42 (1937), 1–30.

[12] E. S. Selmer, *The local postage stamp problem, I, II*, Research monograph (available on request), Dept. of Math., University of Bergen 1986.

[13] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I*, J. Reine Angew. Math. 194 (1955), 40–65.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN
Allégt. 55
N-5007 Bergen
Norway

Received on 18.4.1988 (1814)

ACTA ARITHMETICA
LIV (1990)

Subfield permutation polynomials and orthogonal subfield systems in finite fields

by

STEPHAN J. SUCHOWER* (University Park, Pa.)

1. Introduction. In [5] Niederreiter developed the concepts of permutation polynomials in several variables over a finite field and orthogonal systems of polynomials over a finite field. In this paper we generalize these notions by allowing the image spaces of the polynomials to be arbitrary subfields of the finite field. Several properties of permutation polynomials and orthogonal systems are preserved and new ralationships are exhibited. For a development of the basic properties of permutation polynomials and orthogonal systems, see [1], Ch. 7, Sec. 5.

In [3] Mullen demonstrated an application of the theory of permutation polynomials and orthogonal systems to the construction of complete sets of mutually orthogonal frequency squares of prime power order. Although Mullen's construction generated previously known designs, his algebraic approach was completely different than previous methods which were based upon statistical design theory. In a similar manner, we will show in a follow-up article how to use the theory developed in this paper to construct additional complete sets of frequency squares, rectangles and hyper-rectangles, as well as build orthogonal arrays of various strengths.

Let F_{q^n} denote the finite field of order q^n where q is a power of a prime p and n is a positive integer. Let $F_{q^n}^*$ denote the multiplicative group of nonzero elements and let $F_{q^n}^k$ denote the product of k copies of F_{q^n}, $k \geq 1$. The ring of polynomials in k variables over F_{q^n} will be denoted by $F_{q^n}[x_1,\ldots,x_k]$. Unless otherwise specified, two polynomials $f, g \in F_{q^n}[x_1,\ldots,x_k]$ are equal if they are equal as functions. Recall that every function $f\colon F_{q^n}^k \to F_{q^n}$ can be uniquely realized as a polynomial in $F_{q^n}[x_1,\ldots,x_k]$ of degree at most q^n-1 in each variable.

Following Niederreiter in [5], a polynomial $f \in F_{q^n}[x_1,\ldots,x_k]$ is called a *permutation polynomial over* F_{q^n} if the equation $f(x_1,\ldots,x_k) = a$ has exactly $q^{n(k-1)}$ solutions in $F_{q^n}^k$ for each $a \in F_{q^n}$. In addition, a system of polynomials

* This work is part of the author's Ph. D. dissertation at PSU under the direction of Professor G. L. Mullen.

$f_1,\dots,f_r \in F_{q^n}[x_1,\dots,x_k]$ is an orthogonal system in F_{q^n} if the system of equations $f_1(x_1,\dots,x_k)=a_1,\dots,f_r(x_1,\dots,x_k)=a_r$ has exactly $q^{n(k-r)}$ solutions in $F_{q^n}^k$ for each $(a_1,\dots,a_r)\in F_{q^n}^r$.

For any $t|n$ we know F_{q^t} is a subfield of F_{q^n}. Since q is fixed, the trace function of F_{q^n} over F_{q^t} will be denoted by $\mathrm{TR}_{n/t}$ and is defined by the polynomial

$$\mathrm{TR}_{n/t}(x) = x + x^{q^t} + \dots + x^{q^{n-t}}.$$

Let TR_t denote the trace function of F_{q^t} over F_p. Throughout this paper, let $K_{n/t} = \ker \mathrm{TR}_{n/t}$. Define an additive character ψ_1 of F_{q^t} via

$$\psi_1(x;t) = \exp(2\pi i \cdot \mathrm{TR}_t(x)/p).$$

As indicated in Theorem 5.7 of [1], all nontrivial additive characters of F_{q^t} have the form $\psi_a(x;t)=\psi_1(ax;t)$ for some $a\in F_{q^t}^*$. Also note that

$$\psi_1(x;n) = \psi_1(\mathrm{TR}_{n/t}(x);t). \tag{1.1}$$

By equation (5.9) of [1], we also have for every $a\in F_{q^t}^*$,

$$\sum_{b\in F_{q^t}} \psi_a(b;t) = 0. \tag{1.2}$$

Finally, $\bar{\psi}_a$ will denote the character defined by $\bar{\psi}_a(x;t)=\overline{\psi_a(x;t)}$.

2. Field permutation functions. Throughout this section, assume n, t, u, v, and k are positive integers. We begin with the following concept:

DEFINITION 1. A function $f\colon F_{q^t}^k \to F_{q^u}$ is called a *field permutation function* (FPF) from F_{q^t} to F_{q^u} in k variables (denoted as $(k;t;u)$ FPF) if the equation $f(x_1,\dots,x_k)=a$ has exactly q^{tk-u} solutions in $F_{q^t}^k$ for each $a\in F_{q^u}$.

We see that the existence of a $(k;t;u)$ FPF is guaranteed whenever $tk \geqslant u$. Moreover, the number of different $(k;t;u)$ FPFs is given by $(q^{tk}!)/(q^{tk-u}!)q^u$. It is often necessary, particularly in various applications, to view a $(k;t;u)$ FPF f as a polynomial in the ring $F_{q^n}[x_1,\dots,x_k]$ with $f\colon F_{q^n}^k \to F_{q^u}$, where n is a common multiple of t and u. The FPF f is determined by restricting the domain of the polynomial to $F_{q^t}^k$, and the values of the polynomial off of $F_{q^t}^k$ are generally ignored. In this setting, we call the FPF a $(k;t;u)$ *subfield permutation polynomial* (SPP) since we consider F_{q^t} and F_{q^u} as subfields of F_{q^n}. It is easy to see that for any common multiple n of t and u there are $q^{u(q^{nk}-q^{tk})}$ distinct polynomials in $F_{q^n}[x_1,\dots,x_k]$ which give rise to the same $(k;t;u)$ FPF.

When $t=u=n$ we have Niederreiter's notion of a permutation polynomial of F_{q^n} in k variables, denoted here as a $(k;n)$ PP, and a $(1;n)$ PP is a one-to-one map of F_{q^n} onto itself.

In the following result we present a useful necessary and sufficient condition in terms of character sums:

THEOREM 1. *Let $f\colon F_{q^t}^k \to F_{q^u}$. Then f is a $(k;t;u)$ FPF if and only if*

$$\sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_c(f(b_1,\dots,b_k);u) = 0$$

for all $c\in F_{q^u}^*$.

Proof. Suppose that f is a field permutation function. Then for $c\neq 0$ we have

$$\sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_c(f(b_1,\dots,b_k);u) = q^{tk-u} \sum_{a\in F_{q^u}} \psi_c(a;u) = 0$$

by (1.2).

Conversely, for $a\in F_{q^u}$ let $N(a)$ be the number of solutions in $F_{q^t}^k$ of $f(x_1,\dots,x_k)=a$. Then we have

$$\begin{aligned} N(a) &= \frac{1}{q^u} \sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \sum_{c\in F_{q^u}} \psi_c(f(b_1,\dots,b_k);u)\bar{\psi}_c(a;u) \\ &= \frac{q^{tk}}{q^u} + \frac{1}{q^u} \sum_{c\in F_{q^u}^*} \bar{\psi}_c(a;u) \sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_c(f(b_1,\dots,b_k);u) \\ &= q^{tk-u} + 0 \end{aligned}$$

as desired.

When $t=u=n$, Theorem 1 reduces to Niederreiter's result (Theorem 1 of [4] or Theorem 7.7 of [1]) concerning permutation polynomials. We can use Theorem 1 to generate a key example of a subfield permutation polynomial in one variable. To do this, of course, we must assume that $t\geqslant u$, and n is any common multiple of t and u. First observe that

$$F_{q^n} \neq K_{n/t}\cdot F_{q^u} = \{ab\colon a\in K_{n/t},\ b\in F_{q^u}\}.$$

This is easy to see from the following calculation: for any $n\geqslant 1$ and $t\geqslant u$,

$$\begin{aligned} |K_{n/t}\cdot F_{q^u}| &\leqslant (q^{n-t}-1)(q^u-1)+1 \\ &\leqslant (q^{n-t}-1)(q^t-1)+1 \leqslant q^n - 2q^{n/2}+2 < q^n. \end{aligned}$$

We now know there exists some nonzero $\gamma\in F_{q^n}\backslash K_{n/t}\cdot F_{q^u}$. We claim that the polynomial $\mathrm{TR}_{n/u}(\gamma x)$ is a $(1;t;u)$ SPP in $F_{q^n}[x]$. Applying Theorem 1, we have for any $c\in F_{q^u}^*$,

$$\begin{aligned} \sum_{b\in F_{q^t}} \psi_c(\mathrm{TR}_{n/u}(\gamma b);u) &= \sum_{b\in F_{q^t}} \psi_c(\gamma b;n) \\ &= \sum_{b\in F_{q^t}} \psi_1(\mathrm{TR}_{n/t}(c\gamma b);t) = \sum_{b\in F_{q^t}} \psi_d(b;t) = 0 \end{aligned}$$

by (1.2) since $d=\mathrm{TR}_{n/t}(c\gamma)\neq 0$ (otherwise, $c\gamma\in K_{n/t}$ which implies $\gamma\in K_{n/t}\cdot F_{q^u}$). Note the use of (1.1) in the first two steps.

Incidentally, note that if $t < u$ and n is any common multiple of t and u, then $F_{q^n} = K_{n/t} \cdot F_{q^u}$. Otherwise, we could use the construction above to exhibit a $(1;t;u)$ FPF, an impossibility since $q^{t-u} < 1$.

Assuming only that $tk \geqslant u$ and n is a common multiple of tk and u, we can now easily see that $\mathrm{TR}_{n/u}(\gamma(x_1\omega_1 + \ldots + x_k\omega_k))$ is an example of a $(k;t;u)$ SPP, where $\omega_1, \ldots, \omega_k$ is any basis of $F_{q^{tk}}$ over F_{q^t}, and $\gamma \in F_{q^n} \backslash K_{n/tk} \cdot F_{q^u}$.

This naturally leads us to the following relationship among field permutation functions.

THEOREM 2. *Let $tk \geqslant u \geqslant v$, and n be a common multiple of u and v. Given $\gamma \in F_{q^n} \backslash K_{n/u} \cdot F_{q^v}$, then f is a $(k;t;v)$ FPF if and only if there exists a $(k;t;u)$ FPF g such that $f = \mathrm{TR}_{n/v} \circ \gamma g$.*

Proof. Suppose f is a $(k;t;v)$ FPF. We shall construct a suitable $(k;t;u)$ FPF g. For $a \in F_{q^v}$, define

$$X(a) = \{(b_1, \ldots, b_k) \in F_{q^t}^k : f(b_1, \ldots, b_k) = a\},$$

and

$$Y(a) = \{c \in F_{q^u} : \mathrm{TR}_{n/v}(\gamma c) = a\}.$$

We know that for any $a \in F_{q^v}$,

$$|X(a)| = q^{tk-v}, \quad |Y(a)| = q^{u-v}, \quad \text{and} \quad \bigcup_{a \in F_{q^v}} X(a) = F_{q^t}^k, \quad \bigcup_{a \in F_{q^v}} Y(a) = F_{q^u}.$$

For each $a \in F_{q^v}$, arbitrarily partition $X(a)$ into q^{u-v} disjoint subsets of size q^{tk-u} and label them $W(c)$, one for each $c \in Y(a)$. We can now define a function $g: F_{q^t}^k \to F_{q^u}$ by $g(b_1, \ldots, b_k) = c$ if $(b_1, \ldots, b_k) \in W(c)$ for some $c \in F_{q^u}$. By construction we have $f = \mathrm{TR}_{n/v} \circ \gamma g$.

To show the converse, first recall that $\mathrm{TR}_{n/v}(\gamma x)$ is a $(1;u;v)$ SPP in $F_{q^n}[x]$, so each $a \in F_{q^v}$ has exactly q^{u-v} preimages in F_{q^u}. If g is a $(k;t;u)$ FPF, then each $b \in F_{q^u}$ has exactly q^{tk-u} preimages in $F_{q^t}^k$. Thus, the function $\mathrm{TR}_{n/v} \circ \gamma g$ has the property that each $a \in F_{q^v}$ has exactly $q^{u-v} \cdot q^{tk-u} = q^{tk-v}$ preimages in $F_{q^t}^k$. We conclude that $\mathrm{TR}_{n/v} \circ \gamma g$ is a $(k;t;v)$ FPF.

The choice of the function g is, in general, not unique. The proof above indicates that there are $\dfrac{(q^{tk-v}!)^{q^v}}{(q^{tk-u}!)^{q^u}}$ $(k;t;u)$ FPFs for each $(k;t;v)$ FPF.

Two immediate corollaries of Theorem 2 may be worth noting.

COROLLARY 3. *Let $tk \geqslant u$. If $t < u$, set $m = k$; otherwise, we can set $m = 1$ or $m = k$. Let n be a common multiple of tm and u. Put $\Omega_k(x_1, \ldots, x_k) = \omega_1 x_1 + \ldots + \omega_k x_k$ where $\omega_1, \ldots, \omega_k$ is any basis of $F_{q^{tk}}$ over F_{q^t}, and $\Omega_1(x_1, \ldots, x_k) = (x_1, \ldots, x_k)$, the identity function. Given $\gamma \in F_{q^n} \backslash K_{n/tm} \cdot F_{q^u}$, then f is a $(k;t;u)$ FPF if and only if there exists a $(k-m+1;tm)$ PP g such that $f = \mathrm{TR}_{n/u}(\gamma g \circ \Omega_m)$.*

Proof. If $t \geqslant u$ and $m = 1$, we simply replace u by t and v by u in Theorem 2 to get the desired result. If $m = k$, we first define a $(1;tk;u)$ FPF f_1 from f via $f_1(x_1\omega_1 + \ldots + x_k\omega_k) = f(x_1, \ldots, x_k)$. Apply Theorem 2 to f_1 by replacing u by tk and v by u to obtain a $(1;tk)$ PP g such that

$$f(x_1, \ldots, x_k) = f_1(x_1\omega_1 + \ldots + x_k\omega_k) = \mathrm{TR}_{n/u}(\gamma g(x_1\omega_1 + \ldots + x_k\omega_k)).$$

This result gives, via the trace function, a nice relationship between permutation polynomials of $F_{q^{tm}}$ and field permutation functions from $F_{q^{tm}}$ to F_{q^u}. In effect, if all permutation polynomials of $F_{q^{tm}}$ in $k-m+1$ variables are known, then all field permutation functions in k variables are known.

In Theorem 2, if $v|u$ then we may take $n = u$ so that $K_{n/u} = \{0\}$. By choosing $\gamma = 1$, we have the following special case that is independent of the parameter n.

COROLLARY 4. *Suppose $v|u$. Then f is a $(k;t;v)$ FPF if and only if there exists a $(k;t;u)$ FPF $\cdot\, g$ such that $f = \mathrm{TR}_{u/v} \circ g$.*

An incidental fact derived from this series of results is that when $t \geqslant u$, n is a common multiple of t and u, and $\gamma \in F_{q^n} \backslash K_{n/t} \cdot F_{q^u}$, then the function $h(x) = \gamma x$ maps F_{q^t} uniformly onto $F_{q^n}/K_{n/u}$. That is, each coset of $F_{q^n}/K_{n/u}$ has exactly q^{t-u} preimages in F_{q^t}.

3. Orthogonal field systems. Throughout this section, let n, t, v, k, r, and $u_1, \ldots, u_r$, $v_1, \ldots, v_r$ all be positive integers. Set $s = u_1 + \ldots + u_r$. We now introduce a new concept:

DEFINITION 2. For each i, $1 \leqslant i \leqslant r$, let $f_i: F_{q^t}^k \to F_{q^{u_i}}$. The system of functions $f_1, \ldots, f_r$ is an *orthogonal field system* (OFS) from F_{q^t} to $F_{q^{u_1}}, \ldots, F_{q^{u_r}}$ in k variables (denoted as $(k;t;u_1, \ldots, u_r)$ OFS) if the system of equations $f_1(x_1, \ldots, x_k) = a_1, \ldots, f_r(x_1, \ldots, x_k) = a_r$, has exactly q^{tk-s} solutions in $F_{q^t}^k$ for each $(a_1, \ldots, a_r) \in F_{q^{u_1}} \times \ldots \times F_{q^{u_r}}$.

Once again, we can represent each function above as a polynomial in the ring $F_{q^n}[x_1, \ldots, x_k]$ where n is a common multiple of $t, u_1, \ldots, u_r$. In this case we call the system a $(k;t;u_1, \ldots, u_r)$ *orthogonal subfield system* (OSS). When $t = u_1 = \ldots = u_r = n$, we obtain the notion of an orthogonal system of permutation polynomials of F_{q^n} in k variables as defined in the introduction. We will see many similarities with this concept.

One can easily show that if $f_1, \ldots, f_r$ form a $(k;t;u_1, \ldots, u_r)$ OFS, then for each i, $1 \leqslant i \leqslant r$, the function f_i is a $(k;t;u_i)$ FPF. This indicates that an orthogonal field system is a natural extension of the concept of field permutation function discussed earlier. In fact, the number of different orthogonal field systems of the form $(k;t;u_1, \ldots, u_r)$ is given by $(q^{tk}!)/(q^{tk-s}!)^{q^s}$. We note that this reduces in the case $t = u_1 = \ldots = u_r = n$ to Niederreiter's calculation in [5] (p. 422).

The following result provides us with an implicit bound on the possible number of functions in an orthogonal field system. This result extends Theorem 1 of [5] (or Theorem 7.36 of [1]) by taking $t = u_1 = \ldots = u_r = n$ (in this case, note that the condition $tk \geqslant s$ becomes $k \geqslant r$).

THEOREM 5. *Let $f_1,\dots,f_r$ form a $(k;t;u_1,\dots,u_r)$ OFS. Then we can always form a $(k;t;u_1,\dots,u_r,v)$ OFS $f_1,\dots,f_r,g$ provided $tk \geqslant s+v$.*

Proof. We shall construct a suitable function g. For

$$(a_1,\dots,a_r)\in \Pi = F_{q^{u_1}}\times\dots\times F_{q^{u_r}},$$

put

$$X(a_1,\dots,a_r) = \{(b_1,\dots,b_k)\in F_{q^t}^k\colon f_i(b_1,\dots,b_k) = a_i \text{ for } 1\leqslant i\leqslant r\}.$$

Since $|X(a_1,\dots,a_r)| = q^{tk-s}$ for any $(a_1,\dots,a_r)\in\Pi$, we can then arbitrarily partition $X(a_1,\dots,a_r)$ into q^v disjoint subsets each of size q^{tk-s-v}, and label these subsets $Y(a_1,\dots,a_r,a)$, one for each $a\in F_{q^v}$. We define a function g in the following way: $g(b_1,\dots,b_k)=a$ if $(b_1,\dots,b_k)\in Y(a_1,\dots,a_r,a)$ for some $(a_1,\dots,a_r)\in\Pi$ and $a\in F_{q^v}$. Clearly by design we have that $f_1,\dots,f_r,g$ form a $(k;t;u_1,\dots,u_r,v)$ OFS.

The result above shows that not only is it necessary that $tk\geqslant s$, but that every orthogonal field system with $tk>s$ can be extended to the limit $tk=s$. If $tk=s$, then the OFS gives a bijection between $F_{q^t}^k$ and $F_{q^{u_1}}\times\dots\times F_{q^{u_r}}$, where $s=u_1+\dots+u_r$.

We now present some necessary and sufficient conditions.

THEOREM 6. *Let $v|\gcd(u_1,\dots,u_r)$. Suppose for each i, $1\leqslant i\leqslant r$, $f_i\colon F_{q^t}^k\to F_{q^{u_i}}$. Then the following are equivalent:*

(a) *$f_1,\dots,f_r$ form a $(k;t;u_1,\dots,u_r)$ OFS;*

(b) $\sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_{c_1}(f_1(b_1,\dots,b_k);u_1)\dots\psi_{c_r}(f_r(b_1,\dots,b_k);u_r) = 0$ *for all* $(c_1,\dots,c_r)\in F_{q^{u_1}}\times\dots\times F_{q^{u_r}}\backslash\{(0,\dots,0)\}$;

(c) $h(x_1,\dots,x_k) = \sum_{i=1}^{r} \mathrm{TR}_{u_i/v}(c_i f_i(x_1,\dots,x_k))$ *is a $(k;t;v)$ FPF for every* $(c_1,\dots,c_r)\in F_{q^{u_1}}\times\dots\times F_{q^{u_r}}\backslash\{(0,\dots,0)\}$.

Proof. Set $\Pi = F_{q^{u_1}}\times\dots\times F_{q^{u_r}}$ and $\Pi^* = \Pi\backslash\{(0,\dots,0)\}$. The equivalence between (a) and (b) is essentially the same argument found in the proof of Theorem 1, and so is omitted. The equivalence between (b) and (c) follows from the simple calculation: for $d\in F_{q^v}^*$,

$$\begin{aligned}
&\sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_{dc_1}(f_1(b_1,\dots,b_k);u_1)\dots\psi_{dc_r}(f_r(b_1,\dots,b_k);u_r)\\
&= \sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_d(\mathrm{TR}_{u_1/v}(c_1f_1(b_1,\dots,b_k));v)\dots\psi_d(\mathrm{TR}_{u_r/v}(c_rf_r(b_1,\dots,b_k));v)\\
&= \sum_{(b_1,\dots,b_k)\in F_{q^t}^k} \psi_d(h(b_1,\dots,b_k);v).
\end{aligned}$$

We need only note that for any $d\in F_{q^v}^*$, $d\Pi^*=\Pi^*$, so the first sum above is the same sum found in (b). This completes the proof.

Once again observe that when $t=u_1=\dots=u_r=n$, the equivalence between (a) and (b) reduces to Niederreiter's Theorem 2 in [5] (or Theorem 7.37 in [1]), and the equivalence between (a) and (c) reduces to the Corollary of Theorem 2 in [5] (or Corollary 7.39 in [1]) since the trace functions $\mathrm{TR}_{u_i/v}$, $1\leqslant i\leqslant r$, become the identity function.

The following theorem determines a relationship between the orthogonal field systems $(k;t;u_1,\dots,u_r)$ and $(k;t;v_1,\dots,v_r)$ where $u_i\geqslant v_i$, $1\leqslant i\leqslant r$, and $tk\geqslant s$. Except for technical adjustments, the proof is similar to the proof of Theorem 2.

THEOREM 7. *Let n be a common multiple of $u_1,\dots,u_r,v_1,\dots,v_r$, and for each i, $1\leqslant i\leqslant r$, fix some $\gamma_i\in F_{q^n}\backslash K_{n/u_i}\cdot F_{q^{v_i}}$.*

Then $f_1,\dots,f_r$ form a $(k;t;v_1,\dots,v_r)$ OFS if and only if there exists a $(k;t;u_1,\dots,u_r)$ OFS $g_1,\dots,g_r$ such that for each i, $1\leqslant i\leqslant r$, $f_i = \mathrm{TR}_{n/v_i}\circ\gamma_i g_i$.

As implied above, Theorem 7 is a generalization of Theorem 2 to OFSs. Following the notation used in the statement of Theorem 7, we see that there are $\frac{(q^{tk-s'}!)^{q^{s'}}}{(q^{tk-s}!)^{q^s}}$ $(k;t;u_1,\dots,u_r)$ OFSs for each $(k;t;v_1,\dots,v_r)$ OFS, where $s=u_1+\dots+u_r$, $s'=v_1+\dots+v_r$.

4. Additional properties. Many of the results in this section are extensions of properties of permutation polynomials and orthogonal systems. We shall adopt the notation of the previous two sections where appropriate.

Recall that every $(1;t)$ PP has degree at most q^t-2 (Corollary 7.5 in [1]). We use this fact in the following:

THEOREM 8. *For $t\geqslant u$, let f be a $(1;t;u)$ SPP in $F_{q^n}[x]$, where n is a common multiple of t and u. Then there exists a $(1;t;u)$ SPP $h\in F_{q^n}[x]$ such that $f=h$ on F_{q^t} and $q^{t-u}\leqslant\deg h\leqslant q^n-2$.*

Proof. First examine $(x^m)^{q^{iu}} \bmod (x^{q^n}-x)$ where $0\leqslant m\leqslant q^t-2$ and $0\leqslant i\leqslant n/u$. We can write $m=aq^{n-iu}+b$ where $0\leqslant b<q^{n-iu}$. Note that $0\leqslant a\leqslant q^{iu}-1$. Observe also that if $a=q^{iu}-1$, then $b\leqslant q^{n-iu}-2$; if $b=q^{n-iu}-1$, then $a\leqslant q^{iu}-2$. This happens because $m\leqslant q^t-2\leqslant q^n-2$. We now have $\bmod (x^{q^n}-x)$,

$$(x^m)^{q^{iu}} = (x^{aq^{n-iu}+b})^{q^{iu}} = x^{aq^n}x^{bq^{iu}} = x^{bq^{iu}+a}$$

and

$$bq^{iu}+a < (q^{n-iu}-1)q^{iu}+(q^{iu}-1) = q^n-1.$$

That is, $(x^m)^{q^{iu}} \bmod (x^{q^n}-x)$ has degree at most q^n-2. By Corollary 3 we know there exists a $(1;t)$ PP $g\in F_{q^t}[x]$ and $\gamma\in F_{q^n}\backslash K_{n/t}\cdot F_{q^u}$ such that $f=\mathrm{TR}_{n/u}\circ\gamma g$ on F_{q^t}. Since g has degree at most q^t-2 and $\mathrm{TR}_{n/u}(x)=x+x^{q^u}+\dots+x^{q^{n-u}}$, then the calculations above imply that $h(x)=\mathrm{TR}_{n/u}(\gamma g(x)) \bmod (x^{q^n}-x)$ agrees with f on F_{q^t} and has degree at most q^n-2. Moreover, since h is a $(1;t;u)$ SPP, then h has at least q^{t-u} distinct roots in F_{q^t}. Thus, $\deg h\geqslant q^{t-u}$.

When $u|t$, so that we may take $n=t$, the bounds found above are sharp.

However, when $u \nmid t$ we can still exhibit a $(1;t;u)$ SPP in $F_{q^n}[x]$ which realizes the upper bound, namely

$$h(x) = \mathrm{TR}_{n/u}(\gamma x^{q^n-2}) \bmod (x^{q^n}-x) = \sum_{i=1}^{n/u} \gamma^{q^{(i-1)u}} x^{q^n - q^{(i-1)u}-1}$$

has degree q^n-2.

The following result extends Theorems 5 and 6 of [2] (or Theorems 7.42 and 7.43 of [1]) to FPFs. The proofs are similar and so are omitted.

THEOREM 9. *Let $1 \leqslant j < k$, and f: $F_{q^t}^k \to F_{q^u}$. Suppose we can write*

$$f(x_1,\ldots,x_k) = g(x_1,\ldots,x_j) + h(x_{j+1},\ldots,x_k).$$

If either g is a $(j;t;u)$ FPF or h is a $(k-j;t;u)$ FPF, then f is a $(k;t;u)$ FPF. The converse is true only when q is prime, $u=1$, and g: $F_{q^t}^j \to F_{q^u}$, h: $F_{q^t}^{k-j} \to F_{q^u}$.

We now turn our attention once again to orthogonal field systems. We generalize Theorem 7 of [5] (or Theorem 7.44 of [1]).

THEOREM 10. *If $k = rl$, then there is a one-to-one correspondence between orthogonal field systems of the form $(k;t;u_1,\ldots,u_r)$ and field permutation functions of the form $(l;tr;s)$, where $s = u_1 + \ldots + u_r$.*

Proof. Since the number of such orthogonal field systems and field permutation functions agree, then many correspondences exist. We will construct a particular bijection. Choose n so that $t|n$ and for each i, $1 \leqslant i \leqslant r$, $u_i|n$. Fix a basis $\omega_1,\ldots,\omega_r$ of $F_{q^{tr}}$ over F_{q^t}, and a basis $\delta_1,\ldots,\delta_r$ of $F_{q^{nr}}$ over F_{q^n}. Set $X = \sum_{i=1}^{r} \delta_i F_{q^{u_i}}$. Note that X is a subspace of $F_{q^{nr}}$ of cardinality q^s. Thus there exists a vector space isomorphism φ: $X \to F_{q^s}$.

Suppose $f_1,\ldots,f_r$ form a $(k;t;u_1,\ldots,u_r)$ OFS. For $(a_1,\ldots,a_l) \in F_{q^{tr}}^l$, write for each i, $1 \leqslant i \leqslant l$, $a_i = \sum_{j=1}^{r} b_{r(i-1)+j}\omega_j$ where for each j, $1 \leqslant j \leqslant k$, $b_j \in F_{q^t}$. Define a function g: $F_{q^{tr}}^l \to F_{q^s}$ by

$$g(a_1,\ldots,a_l) = \varphi\left(\sum_{i=1}^{r} \delta_i f_i(b_1,\ldots,b_k)\right).$$

It is easy to see that g is a $(l;tr;s)$ FPF. Moreover, the process can be reversed to define $f_1,\ldots,f_r$ given the function g.

Note that when $t = u_1 = \ldots = u_r$, we may take $\omega_i = \delta_i$, $1 \leqslant i \leqslant r$, and φ the identity map to obtain the same proof found in [5].

We finish with the following straightforward result for generating orthogonal fields systems. This theorem is useful for constructing complete sets of mutually orthogonal frequency squares, as mentioned in the introduction. This result is also a partial generalization of the Corollary of Theorem 2 in [5].

THEOREM 11. *Let n be a common multiple of $t, u_1,\ldots,u_r$. For each i, $1 \leqslant i \leqslant r$, fix $\gamma_i \in F_{q^n} \setminus K_{n/t} \cdot F_{q^{u_i}}$, and define*

$$L_i = \{\mathrm{TR}_{n/t}(c\gamma_i) : c \in F_{q^{u_i}}\}.$$

Let $g_1,\ldots,g_r$ be $(k;t)$ PPs. If

$$p(x_1,\ldots,x_k) = \sum_{i=1}^{r} d_i g_i(x_1,\ldots,x_k)$$

is a $(k;t)$ PP for every $(d_1,\ldots,d_r) \in L_1 \times \ldots \times L_r \setminus \{(0,\ldots,0)\}$, then the functions

$$\mathrm{TR}_{n/u_1} \circ \gamma_1 g_1, \ldots, \mathrm{TR}_{n/u_r} \circ \gamma_r g_r$$

form a $(k;t;u_1,\ldots,u_r)$ OFS.

Proof. For any $(c_1,\ldots,c_r) \in F_{q^{u_1}} \times \ldots \times F_{q^{u_r}} \setminus \{(0,\ldots,0)\}$, we have by Theorem 1,

$$\begin{aligned} 0 &= \sum_{(b_1,\ldots,b_k)\in F_{q^t}^k} \psi_1(\mathrm{TR}_{n/t}(c_1\gamma_1)g_1(b_1,\ldots,b_k) + \ldots + \mathrm{TR}_{n/t}(c_r\gamma_r)g_r(b_1,\ldots,b_k);\ t) \\ &= \sum_{(b_1,\ldots,b_k)\in F_{q^t}^k} \psi_1(\mathrm{TR}_{n/t}(c_1\gamma_1)g_1(b_1,\ldots,b_k);\ t)\ldots\psi_1(\mathrm{TR}_{n/t}(c_r\gamma_r)g_r(b_1,\ldots,b_k);\ t) \\ &= \sum_{(b_1,\ldots,b_k)\in F_{q^t}^k} \psi_{c_1}(\mathrm{TR}_{n/u_1}(\gamma_1 g_1(b_1,\ldots,b_k));\ u_1)\ldots\psi_{c_r}(\mathrm{TR}_{n/u_r}(\gamma_r g_r(b_1,\ldots,b_k));\ u_r) \end{aligned}$$

which completes the proof by Theorem 6.

Acknowledgements. The author is grateful to Professor Gary L. Mullen for his suggestions and comments. Thanks are also due to the referee for several useful comments. This work was supported by the NSA under grant agreement # MDA 904-87-H-2023.

References

[1] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley Pub. Co., Reading, Mass., 1983 (Now distributed by Cambridge University Press).

[2] — — *On orthogonal systems and permutation polynomials in several variables*, Acta Arith. 22(1973), 257–265.

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

[4] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), 1001–1005.

[5] — *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. 28 (1971), 415–422.

DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
University Park, PA 16802
U.S.A.

Received on 3.5.1988
and in revised form on 21.9.1988 (1821)