CONTRIBUTIONS TO GENERAL ALGEBRA 5
Proceedings of the Salzburg Conference, Mai 29 - June 1, 1986
Verlag Hölder-Pichler-Tempsky, Wien 1987 - Verlag B. G. Teubner, Stuttgart

M. Fried - R. Lidl

ON DICKSON POLYNOMIALS AND RÉDEI FUNCTIONS

The main result of this paper is to give a generalisation of Rédei functions to functions of several indeterminates and to establish a connection between these functions and the generalized Dickson polynomials. In the last section we determine the fixed points of Dickson polynomials of the second kind in one variable.

1. Introduction

In recent years considerable attention has been given to properties of Dickson polynomials and Rédei functions and their applications in cryptology, see for example [7], [8], [11], [12], [13]. In this paper we describe some properties of Dickson polynomials of the first and second kind in one variable, and of Rédei functions. Our aim is to consider extensions to several variables. By now the literature on these polynomials and functions is quite extensive and ranges over a period of some eighty years, see [7], p. 382 and p. 387 for some references.

Let $\mathbb{F}_q$ denote the finite field with q elements. The *Dickson polynomials* $g_k(x,b)$ *of the first kind* can be defined as the polynomials of degree k over $\mathbb{F}_q$ given by

$$g_k(x,b) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-b)^i \; x^{k-2i}$$

Here the parameter b is an element in $\mathbb{F}_q$.
If u is an element of an extension field of $\mathbb{F}_q$ such that

$$u + \frac{b}{u} = x \quad \text{or} \quad u^2 - xu + b = 0$$

then the polynomials $g_k(x,b)$ can be defined by the equation

$$g_k(u + \frac{b}{u}, b) = u^k + (b/u)^k$$

by using Waring's formula [7] p. 355.
In the case $b=1$ the polynomials $g_k(x,1)$ are a linear transformation of the classical Chebyshev polynomial $t_k(x)$ of the first kind, since $g_k(x,1) = 2t_k(x/2)$. Therefore the Dickson polynomials are sometimes also referred to as Chebyshev polynomials.

The *Dickson polynomials of the second kind* over $\mathbb{F}_q$ are denoted by $f_k(x,b)$ and, are

† Partially supported by NSF grant # DMS-8508962.

‡ Research of the second author received support from Australian Research Grants Scheme grant # F 84151831.

defined by

$$f_k(x,b) = \sum_{i=0}^{\lfloor k/2 \rfloor} \begin{bmatrix} k-i \\ i \end{bmatrix} (-b)^i \; x^{k-2i}$$

or, for $b \neq 1$ and with $x = u + \frac{b}{u}$, by the equation

$$f_k(x,b) = \frac{u^{k+1} - (b/u)^{k+1}}{u - b/u} \quad .$$

If $b = 1$ and char $\mathbb{F}_q = p$, then

$$f_k(x,1) = \frac{u^{k+1} - \frac{1}{u^{k+1}}}{u - \frac{1}{u}} \quad \text{for } u \neq \pm 1$$

$$f_k(2,1) \equiv k+1 \bmod p \, ,$$

$$f_k(-2,1) \equiv (-1)^k (k+1) \bmod p \, .$$

The polynomials $f_k(x,1)$ are closely related to the classical Chebyshev polynomials of the second kind.
The polynomials $g_k(x,b)$ and $f_k(x,b)$ satisfy the recurrence relations

$$g_k = xg_{k-1} - bg_{k-2} \, , \text{ with } g_0 = 2, \; g_1 = x$$

$$f_k = xf_{k-1} - bf_{k-2} \, , \text{ with } f_0 = 1, \; f_1 = x \quad .$$

We note that for $b=0$ we have $g_k(x,0) = f_k(x,0) = x^k$.

I. Schur [17] established a number of interesting arithmetic properties and relationships between the Dickson polynomials of the first and second kind. For example

$$f_k(x,b) = \frac{1}{k+1} \, g'_k(x,b).$$

From the definition follows the property $f_k(x,b) = \sum_{i=0}^{\lfloor k/2 \rfloor} g_{k-2i}(x,b)$.

The *Rédei functions* are rational functions which were introduced by L. Rédei in [16] and were investigated more recently in [1], [6], [11], [12], [13]. Let $\mathbb{F}_q$ be of odd order and α be a nonsquare in $\mathbb{F}_q$. then the numerator and denominator of the Rédei function $R_k(x) = \frac{r_k(x)}{s_k(x)}$ for odd k are defined as polynomials over $\mathbb{F}_q$ by the equation

$$(x + \sqrt{\alpha})^k = r_k(x) + s_k(x)\sqrt{\alpha}$$

regarded as an equation in $(\mathbb{F}_q[y]/(y^2-\alpha))[x]$, where $\sqrt{\alpha}$ denotes y. If $(k,q+1) = 1$ then the denominator $s_k(x)$ has no roots in $\mathbb{F}_q$, see [12]. An explicit expression for r_k and s_k is of the form

$$r_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \left[\begin{matrix} k \\ 2i \end{matrix}\right] \alpha^i x^{k-2i} \qquad s_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \left[\begin{matrix} k \\ 2i+1 \end{matrix}\right] \alpha^i x^{k-2i-1}$$

Carlitz [1] gives an alternative description of $R_k(x)$ as follows :

$$R_k(x) = \sqrt{\alpha} \frac{(x+\sqrt{\alpha})^k + (x-\sqrt{\alpha})^k}{(x+\sqrt{\alpha})^k - (x-\sqrt{\alpha})^k}$$

Our first goal is to establish a relationship between the Dickson polynomials and the Rédei functions which is then also amenable to generalization to polynomials in several homogeneous variables.

If char $\mathbb{F}_q \neq 2$, then addition of $(x+\sqrt{\alpha})^k = r_k(x) + s_k(x)\sqrt{\alpha}$ and $(x-\sqrt{\alpha})^k = r_k(x) - s_k(x)\sqrt{\alpha}$ yields

Proposition 1.1. $2r_k(x) = g_k(2x, x^2-\alpha)$, *i.e. the numerator of the Rédei function* R_k *equals half the Dickson polynomial in the variable* $2x$ *with parameter* $b = x^2-\alpha$ (Carlitz [1] and Lidl [4]).

Every polynomial $f(x)$ in $\mathbb{F}_q[x]$ and every rational function $h(x) = \frac{r(x)}{s(x)}$ in $\mathbb{F}_q(x)$ with nonvanishing denominator polynomial $s(x)$ induce, on substitution, a mapping from $\mathbb{F}_q$ into itself, e.g. $f : a \rightarrow f(a)$ for all $a \in \mathbb{F}_q$. In the case that this mapping is a permutation of $\mathbb{F}_q$, the polynomial $f(x)$ and the rational function $h(x)$ are called *permutation polynomial* (p.p.) and *permutation function* (p.f.) of $\mathbb{F}_q$, respectively. We summarise, which of the Dickson polynomials and Rédei functions induce permutations of $\mathbb{F}_q$.

Proposition 1.2.

i. *The Dickson polynomial* $g_k(x,b)$ *over* $\mathbb{F}_q$ *is a p.p. of* $\mathbb{F}_q$ *if and only if* $(k,q^2-1) = 1$. (Nöbauer [14]).

ii. *The Dickson polynomial* $f_k(x,b)$ *over* $\mathbb{F}_q$, *q odd, is a p.p. of* $\mathbb{F}_q$ *if k satisfies the following system of congruences :*

$$k+1 \equiv \pm 2 \mod p$$

$$k+1 \equiv \pm 2 \mod \frac{1}{2}(q-1)$$

$$k+1 \equiv \pm 2 \mod \frac{1}{2}(q+1)$$

(Matthews [9]).

iii. *The Rédei function* $R_k(x)$ *over* $\mathbb{F}_q$ *is a p.f. of* $\mathbb{F}_q$ *if and only if* $(k,q-1) = 1$ *in the case* $\sqrt{\alpha} \in \mathbb{F}_q$, *and* $(k,q+1) = 1$ *in the case* $\sqrt{\alpha} \notin \mathbb{F}_q$. (Carlitz [1] and Rédei [16]).

2. Generalized Dickson polynomials and Rédei functions

In [8], Lidl and Wells considered a generalization of the Dickson polynomials of the first kind, which they called (generalized) Chebyshev polynomials in n indeterminates of the finite field $\mathbb{F}_q$. See also [7], p. 376. This section gives a slightly different generalization of the Dickson polynomials $g_k(x,b)$, based in part on the diagram in Fried [3], p. 576. This generalization will prove useful in extending the Rédei functions to several variables.

Let $\mathbf{u}=(u_1, \ldots, u_{n+1})$ be a vector of indeterminates and consider the polynomial

$$r(z) = z^{n+1}-u_1z^n+\cdots+(-1)^nu_nz+(-1)^{n+1}u_{n+1}$$

Let $\sigma=(\sigma_1, \ldots, \sigma_{n+1})$ be the vector of zeros of the polynomial $r(z)$ over $\mathbb{F}_q$. We denote affine (n+1)–space with variables $(w_1, \ldots, w_{k+1})=\mathbf{w}$ by $\mathbb{A}_{\mathbf{w}}^{n+1}$. Then $r(z)=0$ yields a natural map from $\mathbb{A}_{\sigma}^{n+1}$ into $\mathbb{A}_{\mathbf{u}}^{n+1}$ defined by $\sigma \rightarrow \mathbf{u}$, where u_i is the ith elementary symmetric function in $\sigma_1, \ldots, \sigma_{n+1}$. Instead of elementary symmetric functions in $\sigma_1, \ldots, \sigma_{n+1}$ we also consider elementary symmetric functions in $\sigma_1^k, \ldots, \sigma_{n+1}^k$, for a given integer k, which can be expressed in terms of the $u_1, \ldots, u_{n+1}$. The following commutative diagram defines a polynomial mapping $T_{n+1,k}(\mathbf{u})$, which is a vector consisting of n+1 polynomials in $u_1, \ldots, u_{n+1}$. We call $T_{n+1,k}(\mathbf{u})$ a *Dickson polynomial vector* and its coordinates (generalized) *Dickson polynomials*.

$$\begin{tikzcd}
\mathbb{A}_{\sigma}^{n+1} \arrow[r, "\nu"] \arrow[d, "\pi"'] & \mathbb{A}_{\mathbf{u}}^{n+1} \arrow[d, "T_{n+1,k}"] \\
\mathbb{A}_{\sigma,k}^{n+1} \arrow[r, "\mu"'] & \mathbb{A}_{\mathbf{u},k}^{n+1}
\end{tikzcd} \qquad (1)$$

Here ν maps $(\sigma_1, \ldots, \sigma_{n+1})$ onto $(u_1, \ldots, u_{n+1})$, where the u_i are ith elementary symmetric functions in $\sigma_1, \ldots, \sigma_{n+1}$; π is the kth power map which maps $(\sigma_1, \ldots, \sigma_{n+1})$ onto $(\sigma_1^k, \ldots, \sigma_{n+1}^k)$; μ maps $(\sigma_1^k, \ldots, \sigma_{n+1}^k)$ onto the vector of elementary symmetric functions in $\sigma_1^k, \ldots, \sigma_{n+1}^k$, which by the fundamental theorem on elementary symmetric functions can be expressed in $u_1, \ldots, u_{n+1}$. Therefore the mapping $T_{n+1,k}$ maps

$$(u_1, \ldots, u_{n+1}) \rightarrow T_{n+1,k}(u_1, \ldots, u_{n+1})$$

A connection between a sum of kth powers and the elementary symmetric functions is given by Waring's formula, see [7], p. 30.

Let $\mathbb{A}_{\mathbf{u}}^{n+1}(\mathbb{F}_q)$ denote the points of affine space $\mathbb{A}_{\mathbf{u}}^{n+1}$ in $\mathbb{F}_q$.

Lemma 2.1. *The map* $T_{n+1,k}$ *is one-to-one on the points of* $\mathbb{A}_{\mathbf{u}}^{n+1}(\mathbb{F}_q)$ *if and only if* $(q^s-1,k)=1, s=1, \ldots, n+1$.

Proof. The proof follows the corresponding approach in Fried [2], [3], p. 586, and in [8]. If $y^0 \varepsilon \mathbb{A}_{\mathbf{u},k}^{n+1}(\mathbb{F}_q)$ and if $x^0 \varepsilon \mathbb{A}_{\mathbf{u}}^{n+1}(\mathbb{F}_q)$ lies above it then there exists a $z^0 \varepsilon \mathbb{A}_{\mathbf{u},k}^{n+1}(\mathbb{F}_{q^s})$ for some s between 1 and n+1 which lies above y^0. Under the assumption $(q^s-1,k)=1$ then there exists a unique $w^0 \varepsilon \mathbb{A}_{\sigma}^{n+1}(\mathbb{F}_{q^s})$ above z^0. Thus x^0 is uniquely determined as the image of w^0. □

We note that we obtain the generalized Chebyshev polynomials in n variables as defined in [8] by taking $u_{n+1}=b$ in $\mathbb{F}_q$ and considering the map induced on the first n coordinates of $\mathbb{A}_u^{n+1}$ to find the first n coordinates (i.e. polynomials) of $\mathbb{A}_{u,k}^{n+1}$. Thus we obtain a map from $\mathbb{A}^n$ to $\mathbb{A}^n$.

If $\mathbb{P}_{\sigma_i}^1$ denotes projective 1-space with inhomogeneous coordinate σ_i and $\mathbb{P}_u^{n+1}$ is the natural projective closure of $\mathbb{A}_u^{n+1}$, then we have the commutative diagram

$$\begin{tikzcd}
\prod_{i=1}^{n+1}\mathbb{P}_{\sigma_i}^1 \arrow[r] \arrow[d, "\pi"'] & \mathbb{P}_u^{n+1} \arrow[d, "\overline{T}_{n+1,k}"] \\
\prod_{i=1}^{n+1}\mathbb{P}_{\sigma_i,k}^1 \arrow[r] & \mathbb{P}_{u,k}^{n+1}
\end{tikzcd}$$

We next suggest a generalization of the Rédei functions $R_k(x)$ defined in section 1. Let θ be a generator of $\mathbb{F}_{q^{n+1}}$, for example let θ be of the form $\sqrt[n+1]{\alpha}$, where α is not a k^{th} power for any k dividing n+1,k≠1. We define an (n+1)x(n+1) matrix A

$$A = \begin{bmatrix} 1 & \theta & \theta^2 & \cdots & \theta^n \\ 1 & \theta^q & \theta^{2q} & \cdots & \theta^{nq} \\ . & . & . & \cdots & . \\ 1 & \theta^{q^n} & \theta^{2q^n} & \cdots & \theta^{nq^n} \end{bmatrix}$$

Let $\overline{A}$ denote the matrix which is obtained from A by raising each entry of A to the q^{th} power. The notation $A^{(k)}$ will indicate that each entry of A is raised to the k^{th} power. Then we define :

Def. 2.2. *A Rédei function vector* $R_{\alpha,k}(\tau)$ *in* n+1 *variables* $(\tau_1, \ldots, \tau_{n+1})=\tau$ *is defined by*

$$R_{\alpha,k}(\tau) = A^{-1}(A\tau)^{(k)}$$

If $(k, q^{n+1}-1) = 1$ then $R_{\alpha,k}$ is one-to-one on $\mathbb{A}^{n+1}(\mathbb{F}_q)$, since A is one-to-one on $\mathbb{F}_{q^{n+1}}$ and so is the k^{th} power map. We note that $R_{\alpha,k}$ is define over $\mathbb{F}_q$, since

$$\overline{A}^{-1}(\overline{A}\tau)^{(k)} = A^{-1}(A\tau)^{(k)} \; .$$

In order to obtain a relationship between generalized Rédei functions and generalized Dickson polynomials (of the first kind) similar to Proposition 1.1, we extend diagram (1) by adding a commutative square.

$$\begin{tikzcd}
\mathbb{A}_{\tau}^{n+1} \arrow[r] \arrow[d, "R_{\alpha,k}"'] & \mathbb{A}_{\sigma}^{n+1} \arrow[r, "v"] \arrow[d, "\pi"'] & \mathbb{A}_{u}^{n+1} \arrow[d, "T_{n+1,k}"] \\
\mathbb{A}_{\tau,k}^{n+1} \arrow[r] & \mathbb{A}_{\sigma,k}^{n+1} \arrow[r] & \mathbb{A}_{u,k}^{n+1}
\end{tikzcd} \qquad (2)$$

Going along the top and bottom of the diagram establishes a relationship between $R_{\alpha,k}(\tau)$ and $T_{n+1,k}(\mathbf{u})$. For the top line we obtain a function

$$H(\tau) : \mathbb{A}_{\tau}^{n+1} \rightarrow \mathbb{A}_{u}^{n+1} \ , \quad \tau \rightarrow \mathbf{u} \ ,$$

over $\mathbb{F}_q$, where u_i are the elementary symmetric functions in $A\tau$. An analogous function $\overline{H}$ for the bottom line generalises Proposition 1.1.

It is perhaps instructive to consider the special case n=1 as an example.
Let $\theta = \sqrt{\alpha}$ be a generator of $\mathbb{F}_{q^2}$. Then the matrices defined above are

$$A = \begin{bmatrix} 1 & \sqrt{\alpha} \\ 1 & -\sqrt{\alpha} \end{bmatrix}, \quad A^{-1} = \frac{1}{2\sqrt{\alpha}} \begin{bmatrix} \sqrt{\alpha} & \sqrt{\alpha} \\ 1 & -1 \end{bmatrix}, \quad \overline{A} = \begin{bmatrix} 1 & -\sqrt{\alpha} \\ 1 & \sqrt{\alpha} \end{bmatrix},$$

Therefore, with $\tau = (\tau_1, \tau_2)$

$$R_{\alpha,k}(\tau) = A^{-1}(A\tau)^{(k)} = \frac{1}{2\sqrt{\alpha}}(\sqrt{\alpha}(\tau_1+\sqrt{\alpha}\tau_2)^k + \sqrt{\alpha}(\tau_1-\sqrt{\alpha}\tau_2)^k \ , \ (\tau_1+\sqrt{\alpha}\tau_2)^k - (\tau_1-\sqrt{\alpha}\tau_2)^k).$$

If we assume $\tau_2 \neq 0$ and let $x = \tau_1/\tau_2$, then we can consider $R_{\alpha,k}(x,1)$, or $R_k(x)$ for short, as inducing (permutation) maps from $\mathbb{A}^1$ to $\mathbb{A}^1$, instead of $\mathbb{A}^2$ to $\mathbb{A}^2$. We can verify directly that $R_{\alpha,k}(\tau)$ is defined over $\mathbb{F}_q$. Note that

$$\overline{A}^{-1}(\overline{A}\tau)^{(k)} = A^{-1}(A\tau)^{(k)}$$

holds, since replacing τ by $A^{-1}\tau$ yields

$$(\overline{A}A^{-1}\tau)^{(k)} = \overline{A}A^{-1}\tau^{(k)} \ .$$

But $\overline{A}A^{-1}$ is just a switch of coordinates. Going from homogeneous to inhomogeneous coordinates leads us to the definition of $R_k(x)$ as stated just above Proposition 1.1. The denominator of the rational function $R_k(x)$ is nonzero, since otherwise $(\sqrt{\alpha})^k$ would be an element in $\mathbb{F}_q$.
The function $H(\tau) : \mathbb{A}_{\tau}^2 \rightarrow \mathbb{A}_{u}^2$ has the following coordinates

$$H(\tau_1,\tau_2) = v(A\tau) = (2\tau_1, \tau_1{}^2 - \alpha\tau_2{}^2).$$

Similarly for the bottom line of diagram (2), the map $\overline{H}$ is define by

$$\begin{aligned} \overline{H}(R_{\alpha,k}(\tau)) &= \boldsymbol{\mu}(AR_{\alpha,k}(\tau)) = \boldsymbol{\mu}((A\tau)^{(k)}) \\ &= ((\tau_1+\sqrt{\alpha}\tau_2)^{(k)} + (\tau_1-\sqrt{\alpha}\tau_2)^k, \tau_1{}^2-\alpha\tau_2{}^2) \\ &= T_{2,k}(2\tau_1, \tau_1{}^2-\alpha\tau_2{}^2) = T_{2,k}(u_1,u_2) \end{aligned}$$

This establishes the result of Propostion 1.1.

3. The Fixed Points of $f_k(x,1)$ †

In applications of the Dickson polynomials $g_k(x,b)$ and the Rédei functions $R_k(x)$ in cryptography it is important to know the number of fixed points of the mappings from $\mathbb{F}_q$ into $\mathbb{F}_q$ which are induced by g_k and R_k. In [10] and [12] R. Nöbauer determined the numbers of fixed points of such mappings. Here we give the number of fixed points of mappings induced by Dickson Polynomials $f_k(x,1)$ of the second kind of $\mathbb{F}_q$. We abbreviate $f_k(x,1)$ as $f_k(x)$ for convenience. A formula for the fixed points of $f_k : \mathbb{F}_q \to \mathbb{F}_q$ for odd q and for even q will be given at the end of this section. From the definition of $f_k(x)$ in section 1, we note that $x=u+u^{-1}$ implies $u^2-xu+1=0$. The set of solutions of the q equations $u^2-xu+1=0$, for $x \varepsilon \mathbb{F}_q$, is equal to $u \varepsilon \mathbb{F}_{q^2}$ such that $u+u^{-1} \varepsilon \mathbb{F}_q$. That is

$$M = \{u \varepsilon \mathbb{F}_{q^2} \mid (u+u^{-1})^q = u^q + u^{-q} = u+u^{-1}, \text{ or } u^q = u^{\pm 1}\}.$$

See W. Nöbauer [14], or [7], p. 360.

Let w be a primitive element of $\mathbb{F}_{q^2}$,

$$M_1 = \{u \varepsilon \mathbb{F}_{q^2} \mid u^{q+1} = 1\} = \{w^{r(q-1)} \mid r=0,1,\ldots,q\},$$

$$M_2 = \{u \varepsilon \mathbb{F}_{q^2} \mid u^{q-1} = 1\} = \{w^{r(q+1)} \mid r=0,1,\ldots,q-2\},$$

$$M_3 = M_1 \cap M_2 = \{\pm 1\},$$

$$M_1' = M_1 \backslash M_3 = \{w^{r(q-1)} \mid r=1,2,\ldots,q \text{ but } r \neq \frac{q+1}{2}\},$$

$$M_2' = M_2 \backslash M_3 = \{w^{r(q+1)} \mid r=1,2,\ldots,q-2 \text{ but } r \neq \frac{q-1}{2}\},$$

Then $M = M_1' \cup M_2' \cup M_3$ and M_1', M_2' and M_3 are disjoint.

The definition of $f_k(x)$ implies that $f_k(x)=x$ can be written as

$$\frac{u^{k+1} - u^{-(k+1)}}{u - u^{-1}} = u + u^{-1} .$$

This leads to $(u^{k-1}-1)(u^{k+3}+1) = 0$. Then we sonsider solutions to the follwoing three cases:

α) $u^{k-1} = 1$,

β) $u^{k+3} = -1$,

γ) $u^{k-1} = 1$ and $u^{k+3} = -1$.

For each value of $x \varepsilon \mathbb{F}_q, x \neq \pm 2$, there are two distinct solutions of $u^2-xu+1=0$ in $M' = M_1' \cup M_2'$. Thus if we let

† The second author acknowledges research assistance by N.S. James.

$$\begin{array}{lllllllll}
a_1 & = & \text{number} & \text{of} & \text{solutions} & \text{of} & \alpha) & \text{over} & M_1' \\
a_2 & = & '' & '' & '' & '' & '' & '' & M_2' \\
b_1 & = & '' & '' & '' & '' & \beta) & '' & M_1' \\
b_2 & = & '' & '' & '' & '' & '' & '' & M_2' \\
c_1 & = & '' & '' & '' & '' & \gamma) & '' & M_1' \\
c_2 & = & '' & '' & '' & '' & '' & '' & M_2'
\end{array}$$

then the total number of fixed points of $f_k(x)$, excluding the possibility $x=\pm 2$, is

$$\frac{1}{2}(a_1+a_2+b_1+b_2-c_1-c_2).$$

α) Let $u \varepsilon M_1$. Then $u=w^{r(q-1)}$ for some r with $0 \le r \le q$.

$$\begin{aligned}
u^{k-1}=1 &\Leftrightarrow w^{r(q-1)(k-1)}=1=w^0 \\
&\Leftrightarrow r(q-1)(k-1) \equiv 0 \bmod (q^2-1) \\
&\Leftrightarrow r(k-1) \equiv 0 \bmod (q+1) \ .
\end{aligned}$$

The number of solutions of this congruence is $(q+1, q-1)$. If q and k are both odd then 2 of these solutions are in M_3, otherwise only 1 solution is in M_3. Thus we find that the number of solutions of α) over M_1' is :

$$a_1 = \begin{cases} (q+1,k-1)-2 & \text{q is odd and k is odd} \\ (q+1,k-1)-1 & \text{q is even or k is even} \end{cases}$$

Similarly the number of solutions of α) over M_2' is

$$a_2 = \begin{cases} (q-1,k-1)-2 & \text{q is odd and k is odd} \\ (q-1,k-1)-1 & \text{q is even or k is even} \end{cases}$$

β) Let $u \varepsilon M_1$. then if q is odd we have

$$\begin{aligned}
u^{k+3}=-1 &\Leftrightarrow w^{r(q-1)(k+3)}=-1=w^{(q^2-1)/2} \\
&\Leftrightarrow r(q-1)(k+3) \equiv (q^2-1)/2 \bmod (q^2-1) \\
&\Leftrightarrow 2r(k+3) \equiv 0 \bmod (q+1) \text{ and not } r(k+3) \equiv 0 \bmod (q+1)
\end{aligned}$$

The number of solutions is $(q+1, 2(k+3))-(q+1, k+3)$. If k is even then one of these solutions is in M_3, otherwise none are in M_3. Thus

$$b_1 = \begin{cases} (q+1, 2(k+3))-(q+1, k+3)-1 & \text{if q is odd and k is even} \\ (q+1, 2(k+3))-(q+1, k+3) & \text{if q is odd and k is odd} \end{cases}$$

If q is even then we may argue as in α) to find

$$b_1 = (q+1, k+3)-1 \text{ if q is even}$$

Similarly we find that

$$b_2 = \begin{cases} (q-1,2(k+3))-(q-1,k+3)-1 & \text{if } q \text{ is odd and } k \text{ is even} \\ (q-1,2(k+3))-(q-1,k+3) & \text{if } q \text{ is odd and } k \text{ is odd} \\ (q-1,k+3)-1 & \text{if } q \text{ is even} \end{cases}$$

γ) $u^{k-1}=1$ and $u^{k+3}=-1$

$\Leftrightarrow u^{k-1}=1$ and $u^4=-1$.

Assume q is odd, i.e. $1 \neq -1$. If $u^4=-1$ then u is a primitive 8th root of unity, hence $u^{k-1}=1$ iff $8 \mid k-1$. Futhermore M_1' contains primitive 8th roots of unity iff $8 \mid q+1$, in which case M_1' contains all 4 such roots. Therefore

$$c_1 = \begin{cases} 4 & \text{if } 8 \mid q+1 \text{ and } 8 \mid k-1 \quad \text{and } q \text{ is odd} \\ 0 & \text{if } 8 \nmid q+1 \text{ and } 8 \nmid k-1 \quad \text{and } q \text{ is odd} \end{cases}$$

Similarly

$$c_2 = \begin{cases} 4 & \text{if } 8 \mid q-1 \text{ and } 8 \mid k-1 \quad \text{and } q \text{ is odd} \\ 0 & \text{if } 8 \nmid q-1 \text{ and } 8 \nmid k-1 \quad \text{and } q \text{ is odd} \end{cases}$$

The case q even is very simple.

$$u^{k-1}=1 \text{ and } u^{k+3}=1 \Rightarrow u^4=1.$$

If $u \in M_1$ then $u^{q+1}=1 \Rightarrow u^{(q+1,4)}=1$. Now q+1 is odd so $u=1$, i.e. $u \in M_3$ and $u \notin M_1'$. So $c_1=c_2=0$ if q is even.
If $x=2$ then $f_k(x)=x$

$\Leftrightarrow k+1 \equiv 2 \pmod p$.

If $x=-2$ then $f_k(x)=x$

$\Leftrightarrow (-1)^{k+1}(k+1) \equiv -2 \pmod p$

$\Leftrightarrow k+1 \equiv (-1)^k 2 \pmod p$

We summarise our calculations as a theorem.

Theorem 3.1. *The number* N(q,k) *of fixed points of* f_k *is as follows :*
For q *odd and the integer* d_1 *defined as*

$$d_1 = \begin{cases} 2 & \text{if } k+1 \equiv 2 \text{ and } k+1 \equiv (-1)^k 2 \bmod p \\ 1 & \text{if one of the above congruences holds but not both} \\ 0 & \text{if } k+1 \not\equiv 2 \text{ and } k+1 \equiv (-1)^k 2 \bmod p \end{cases}$$

we have

$$N(q,k) = \frac{1}{2}[(q+1,k-1)+(q-1,k-1)+(q+1,2(k+3)) \\ -(q+1,k+3)+(q-1,2(k+3))-(q-1,k+3)-c_1-c_2-4]+d_1$$

where c_1 *and* c_2 *are defined as above.*

For q *even and the integer* d_2 *defined as*

$$d_2 = \begin{cases} 1 & \text{if k odd} \\ 0 & \text{if k even} \end{cases}$$

we have

$$N(q,k) = \frac{1}{2}[(q+1,k-1)+(q-1,k-1)+(q+1,k+3)+(q-1,k+3)-4]+d_2.$$

4. References

[1] L. Carlitz, A note on permutation functions over a finite field. Duke Math. J. 29 (1969), 325-332.

[2] M. Fried, On a conjecture of Schur. Michigan Math. J. 17 (1970), 41-45.

[3] M. Fried, Exposition on an arithmetic-goup theoretic connection via Riemann's existence theorem. Santa Cruz Conf. 1979, Proc. Symp. Pure Math. 37 (1980), 571-602.

[4] R. Lidl, Reguläre Polynome über endlichen Körpern. Beiträge Alg. u. Geom. 2 (1974), 55-69.

[5] R. Lidl and W.B. Müller, Permutation polynomials in RSA-cryptosystems. Advances in Cryptology, (ed. D. Chaum), Plenum Publ. Corp., New York, 1984, pp. 293-301.

[6] R. Lidl and W.B. Müller, A note on polynomials and functions in algebraic cryptography. Ars Combinatoria, 17 (1984), 223-229.

[7] R. Lidl and H. Niederreiter, Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20. Addison-Wesley, Reading, 1983. Now published by Cambridge University Press.

[8] R. Lidl and C. Wells, Chebyshev polynomials in several variables. J. Reine Angew. Math. 255 (1972), 104-111.

[9] R. Matthews, Permutation polynomials in one and several variables. Ph.D. thesis, University of Tasmania, Hobart, 1982.

[10] R. Nöbauer, Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen. Acta Arith. 45 (1985), 91-99.

[11] R. Nöbauer, Key distribution systems, based on polynomial functions and on Rédei functions. Problems of Control and Information Th. Vol. 15(1). pp.91-100(1986).

[12] R. Nöbauer, Rédei Funktionen und ihre Anwendung in der Kryptographie. Acta Sci. Math. Szeged. To appear.

[13] R. Nöbauer, Cryptanalysis of the Rédei scheme. Contributions to General Alg. 3, Hölder-Pichler-Tempsky, Wien, 1985, pp. 255-264.

[14] W. Nöbauer, Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. J. Reine Angew. Math. 231 (1968), 215-219.

[15] W. Nöbauer, Über die Fixpunkte der Dickson-Permuationen. Osterr. Akad. Wiss. Math.-Natur. K1. S.-B, to appear.

[16] L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern. Acta Sci. Math. Szeged, 11 (1946) 85-92

[17] I.Schur, Arithmetisches über die Tschebysheffschen Polynome. In I. Schur Gesammelte Abhandlungen, vol. 3, Springer-Verlag Berlin, 1973, pp. 422-453.

M.Fried
Department of Mathematics
University of California
Irvine, California 92717
U.S.A.

R.Lidl
Department of Mathematics
University of Tasmania
Hobart, Tas. 7001
Australia