Internat. J. Math. & Math. Sci.
VOL. 11 NO. 4 (1988) 625-634

ON GENERALIZED REDEI FUNCTIONS

R. MATTHEWS and R. LIDL

Department of Mathematics
University of Tasmania
Hobart, Tasmania, 7001
Australia

(Received November 18, 1987)

ABSTRACT. A generalization of Rédei functions to polynomial vectors in n indeterminates over finite fields or residue class rings of integers is given by considering special types of polynomial vectors. Properties such as polynomial composition, change of basis, group structure and fixed points are studied together with applications in cryptography.

KEYWORDS AND PHRASES. Permutation polynomials, cryptosystems.
1980 AMS SUBJECT CLASSIFICATION CODE. 12C05.

1. INTRODUCTION.

L. Rédei [1] introduced an interesting class of rational functions which give rise to permutations of a finite field on substitution of the elements of the finite field. More recently these functions were studied in detail for cryptographic applications, see Lidl and Müller [2], Nöbauer [3-5]. Fried and Lidl [6] presented a generalized version of Rédei functions by considering the ordered pair formed from the numerator and denominator of a Rédei function and extending this approach to polynomial vectors in n indeterminates over a finite field. In the following we shall use a different approach to obtaining such polynomial vectors, which makes it possible to study the vectors over finite fields as well as residue class rings of integers. In section 5 we shall give a connection between the matrix definition used by Fried and Lidl [6] and the definition which relies on bases used in this paper.

Let L be an extension field of a field K and $\{\theta_1,\ldots,\theta_n\}$ be a basis of L over K. Carlitz [7] and Lidl and Niederreiter [8, P. 375], showed how to obtain a polynomial vector in n variables over K, given a polynomial over L. We define a polynomial vector

$$\bar{f} = (f_1,\ldots,f_n)$$

based on the polynomial $f \in K[x]$,
where $f_i \in K[x_1,\ldots,x_n]$ are defined by

$$f\Big(\sum_{i=1}^{n} v_i\theta_i\Big) = \sum_{i=1}^{n} f_i\theta_i, \text{ and } v_i \in K,\ i = 1,\ldots,n. \tag{1.1}$$

Here $\bar{f}$ depends on the polynomial f and the choice of basis of L over K. The polynomial vector $\bar{f}$ reflects various properties of f which will be presented in the following sections.

2. COMPOSITION PROPERTY.

Let 0 denote composition of polynomials or polynomial vectors. We use the notation introduced in (1.1).

PROPOSITION 1. Suppose $f,g,h \in K[x]$ and $h = f \circ g$. If $\bar{f},\bar{g},\bar{h}$ are the corresponding polynomial vectors according to (1.1), then

$$\bar{h} = \bar{f} \circ \bar{g} \tag{2.1}$$

PROOF. We have

$$\sum_{i=1}^{n} h_i\theta_i = h\Big(\sum_{i=1}^{n} v_i\theta_i\Big) = f\Big(g\Big(\sum_{i=1}^{n} v_i\theta_i\Big)\Big)$$

$$= f\Big(\sum_{i=1}^{n} g_i\theta_i\Big) = \sum_{i=1}^{n} f_i(g_1,\dots,g_n)\theta_i$$

and thus

$$h_i = f_i(g_1,\dots,g_n).$$

It can readily be seen that if f ranges over the elements of a set of polynomials which are closed under composition, then $\bar{f}$ ranges over the corresponding set of polynomial vectors which are closed under composition of polynomial vectors. Specific examples of sets of polynomials which are closed under composition are the set of power polynomials $S = \{x^k \mid \in Z\}$ and the set of Dickson polynomials $D = \{g_k(x,1) \mid k \in Z\}$. For a definition of g_k we refer to Lidl and Niederreiter [8, P.355].

3. CHANGE OF BASIS.

Since the definition of $\bar{f}$ in (1.1) depends on the basis $\theta_1,\dots,\theta_n$ of L over K, we would like to know the effect of changing the basis while keeping f fixed. Suppose $\psi_1,\dots,\psi_n$ is another basis of Lover K and let $\theta = (\theta_1,\dots,\theta_n)$, $\psi = (\psi_1,\dots,\psi_n)$ and $\theta^T = M\psi^T$. We use the notation

$$\bar{f}^{\theta} = (f_1^{\theta},\dots,f_n^{\theta}) \ , \ \bar{f}^{\psi} = (f_1^{\psi},\dots,f_n^{\psi})$$

and $v = (v_1,\dots,v_n)$.

Then

$$f(v\theta^T) = f(v(M\psi^T)) = f((vM)\psi^T) = (\bar{f}^{\psi}(vM))\psi^T.$$

But

$$f(v\theta^T) = (\bar{f}^{\theta}(v))\theta^T = (\bar{f}^{\theta}(v))(M\psi^T) = (\bar{f}^{\theta}(v)M)\psi^T.$$

Since ψ is a basis of L over K,

$$\bar{f}^{\psi}(vM) = \bar{f}^{\theta}(v)M.$$

Thus we have shown:

PROPOSITION 2. Let θ and ψ denote bases of L over K and $\bar{f}^{\theta},\bar{f}^{\psi}$ be the polynomial vectors defined in (1.1) with a fixed polynomial f. Then

$\bar{f}^{\theta}(v) = \bar{f}^{\psi}(vM)M^{-1}$, where M is the matrix relating θ to ψ.

4. CONSTRUCTION OVER Z and F_p.

Suppose K = **Q**, L is an algebraic extension of **Q** of degree n and $f \in Z[x]$. If $\{\theta_1,\dots,\theta_n\}$ is a basis of L over **Q**, let $\theta_i\theta_j \in \mathbf{Z}[\theta_1,\dots,\theta_n]$ for each i,j = 1,...,n. Then $\bar{f}$ as defined in (1.1) will be an element of $\mathbf{Z}[x_1,\dots x_n]$ and therefore can also be considered as a polynomial vector with integer coefficients mod n, $n \in \mathbf{N}$.

A second approach is as follows. Let A denote the ring of algebraic integers of K where $\{\theta_1,\dots,\theta_n\}$ is an integral basis for K then $A \cong \mathbf{Z}[\theta_1,\dots,\theta_n]$. If P is a prime ideal of A and $p \in P$ for a prime p in **Z**, then when reduced mod P the polynomial vector $\bar{f}$ of (1.1) is defined over A/P and has coefficients in $\mathbf{F}_p$.

Alternatively, in the construction of section 1, let $K = \mathbf{F}_q$ and $L = \mathbf{F}_q n$. A system of n polynomials in n variables is called orthogonal (or a permutation polynomial vector) over $\mathbf{F}_q$ if on substitution of the elements of $\mathbf{F}_q^n$ the polynomial vector of n polynomials gives a permutation of the elements of $\mathbf{F}_q^n$, see [8, P. 368]. Every element of $\mathbf{F}_q n$ has a unique representation as $\Sigma v_i\theta_i$. A polynomial $f \in \mathbf{F}_q[x]$ is a permutation polynomial of $\mathbf{F}_q$ if on substitution of the elements of $\mathbf{F}_q$ the polynomial gives a permutation of $\mathbf{F}_q$. Now we can state:

PROPOSITION 3. The system of components f_i of the polynomial vector $\bar{f}$ as defined in (1.1) is orthogonal over $\mathbf{F}_q$ if and only if f is a permutation polynomial of $\mathbf{F}_q n$.

5. THE MATRIX APPROACH AND GENERALIZED REDEI FUNCTIONS.

This section is the central part of this paper, it represents a generalization of the Redei funtion vectors of Fried and Lidl [6] in two ways: instead of power polynomials x^k we first let f(x) be arbitrary and secondly the underlying structures are not necessarily finite fields. As in section 1 let L be an extension field of K and let $\{\theta_1,\dots,\theta_n\}$ be a basis of L over K. The discriminant matrix of L over K with respect to this basis is defined as the matrix D whose i,j entry is $\sigma_i(\theta_j)$. Here

$\sigma_1,\ldots,\sigma_n$ are the n embeddings of L into $\mathbf{C}$ that fix K, or the n isomorphisms of L over K in the case that L is finite.

Let $f \in K[x]$ then we define $f((x_1,\ldots,x_n)) = (f(x_1),\ldots,f(x_n))$. Let $x = (x_1,\ldots,x_n)$, then $Dx^T = (\sum_{i=1}^{n} x_j\sigma_i(\theta_j))^T$, hence $f(Dx^T) = (f(\sum_{i=1}^{n} x_j\sigma_i(\theta_j))^T$.

Since $f \in K[x]$, σ_i leaves f fixed, so

$$f(Dx^T) = (\sigma_i(f(\sum_{j=i}^{n} x_j\theta_i)))^T = (\sigma_i(\sum_{j=1}^{n} f_j^\theta\theta_j))^T$$

$$= (\sum_{j=1}^{n} f_j^\theta(x_1,\ldots,x_n)\ \sigma_i(\theta_j))^T.$$

But

$$\bar{f}^\theta(x^T) = (f_1^\theta(x_1,\ldots,x_n),\ldots,f_n^\theta(x_1,\ldots,x_n))^T$$

$$D(\bar{f}^\theta(x^T)) = (\sum_j f_j^\theta(x_1,\ldots,x_n)\ \sigma_i(\theta_j))^T = f(Dx^T).$$

Therefore we obtain the following definition of the polynomial vector $\bar{f}^\theta$ in terms of the polynomial f and the discriminant matrix D of L over K:

$$\bar{f}^\theta(x^T) = D^{-1}f(Dx^T) \tag{5.1}$$

We note that the square of the determinant of D equals the discriminant of $\theta_1,\ldots,\theta_n$, which is nonzero. Therefore D^{-1} is always defined. Now in order to obtain the special case of Redei vectors presented in [6] we let $f(x) = x^k$ and $\{\theta_1,\ldots,\theta_n\} = \{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$, where L is a finite extension of $K = \mathbf{F}_q$. In this case we obtain the Redei function vectors similar to those defined in Definition 2.2 of [6]. We call the corresponding vector of polynomials in n variables defined in (5.1) above a generalized Redei (function) vector and denote it by $\bar{f}_k^\theta$. In this case we note that the system of components of $\bar{f}^\theta$ is orthogonal if and only if $(k,q^n-1) = 1$.

PROPOSITION 4. The Redei vector $\bar{f}_k^\theta$ induces a permutation of $\mathbf{F}_q^n$ if and only if the exponent of the defining power polynomial f is coprime with q^n-1. We give explicit examples of Redei function vectors for n = 2 and n = 3 and $K = \mathbf{F}_q$. Let $f(x) = x^k$.

EXAMPLE 1. Let n = 2, $K = \mathbf{F}_q$, $L = \mathbf{F}_{q^2}$ and $\{1,\theta\}$ be a basis of L over K, where $\theta = \sqrt{\alpha}$ is a generator of $\mathbf{F}_{q^2}$. Then the discriminant matrix D is of the form

$$D = \begin{pmatrix} 1 & \theta \\ 1 & \theta^q \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{\alpha} \\ 1 & -\sqrt{\alpha} \end{pmatrix}.$$

The definition (5.1) and the remarks below (5.1) give the following vector.

$$\overline{f}_k^\theta = (\tfrac{1}{2}((x+\sqrt{\alpha}\,y)^k + (x-\sqrt{\alpha}\,y)^k, \frac{a}{2\sqrt{\alpha}}((x+\sqrt{\alpha}\,y)^k - (x-\sqrt{\alpha}\,y)).$$

This vector induces a permutation of $\mathbf{F}_q^2$ iff $(k,q^2-1) = 1$. It corresponds to the Redei function vector $R_{\alpha,k}$ as defined in Fried and Lidl [3] in the case $n = 1$.

EXAMPLE 2. Let $n = 3$, $K = \mathbf{F}_q$, and $1,\theta,\theta^2$ a basis of the extension L over $\mathbf{F}_q$. For $k = 1$ definition (5.1) yields $\overline{f}_1^\theta = (x_1,x_2,x_3)$. For $k = 2$ let

$$D = \begin{matrix} 1 & \theta & \theta^2 \\ 1 & \theta^q & \theta^{2q} \\ 1 & \theta^{q^2} & \theta^{2q^2} \end{matrix}.$$

Then

$$\overline{f}_2^\theta = (x_1^2 + 2x_2x_3\theta^{1+q+q^2} + x_3^2\,(\theta+\theta^q+\theta q^2),$$
$$x_3^2a + 2x_1x_2 + 2x_2x_3b,$$
$$x_2^2 + x_3^2c + 2x_1x_3 + 2x_2x_3(\theta+\theta^q+\theta^{q^2})),$$

where

$$a = -(\theta^{q^2} + \theta^q)\,(\theta^{q^2} + \theta)\,(\theta^q + \theta),\ b = -(\theta^{q+1}+\theta^{q^2+1}+\theta^{q^2+q}),$$

$c = \theta^2q^2 + \theta^{q^2+q} + \theta^{2q} + \theta^{q^2+1} + \theta^{q+1} + \theta^2$. All the coefficients of the components of $\overline{f}_2^\theta$ are in $\mathbf{F}_q$.

Specifically, for $q = 2$ and $\theta^3+\theta^2+1 = 0$ we obtain

$$\overline{f}_2^\theta = (x_1^2 + x_3^2,\ x_3^2,\ x_2^2 + x_3^2).$$

For $q = 3$ and $\theta^3 + 2\theta^2 + 1 = 0$ we get

$$\overline{f}_2^\theta = (x_1^2 + x_2x_3 + x_3^2,\ 2x_3^2 + 2x_1x_2,\ x_2^2 + x_3^2 + 2x_1x_3 + 2x_2x_3)$$

and for $q = 5$ and $\theta^3 + \theta^2 + 2 = 0$

$$\overline{f}_2^\theta = (x_1^2 + x_2x_3 + 4x_3^2,\ 3x_3^2 + 2x_1x_2,\ x_2^2 + x_3^2 + 2x_1x_3 + 3x_2x_3).$$

We recall composition properties from section 2 and note that if f is an element of a set of polynomials which induce a group G of mappings on $\mathbf{F}_{q^n}$, then the coresponding family of polynomial vectors $\bar{f}$ induces the ssame group of mappings on $(\mathbf{F}_q)^n$. It can also be shown easily that the fixed points of $\bar{f}$ over $\mathbf{F}_q$ may be identified with the fixed points of f over $\mathbf{F}_{q^n}$, by using representation of $(x_1,\dots,x_n)$ as $\sum x_i\theta_i$ in $\mathbf{F}_{q^n}$.

6. REGULARITY AND POLYNOMIALS OVER Z

From the definition (5.1) of $\bar{f}^\theta$ with respect to a given basis θ we see that $(v_1,\dots,v_n) \in K^n$ is a zero of $\bar{f}$ if and only if $\sum_i v_i\theta_i \in L$ is a zero of f. Recall that

$$f(\sum_i x_i\theta_i) = \sum_i f_i(x_1,\dots,x_n)\theta_i.$$

Differentiating with respect to x_j yields

$$f'(\sum x_i\theta_i)\theta_j = \sum_i \frac{\partial f_i}{\partial x_j}\theta_i.$$

The map $\theta_j \to \sum_i \frac{\partial f_i}{\partial x_j}\theta_j$ defines a linear transformation of L over K for fixed $x_1,\dots,x_n$. If $m= f'(\sum x_i\theta_i)$ then this transformation is the same as $\theta_j \to m\theta_j$. This map is invertible if and only if $m \neq 0$. A different condition for invertibility is that the Jacobian determinant of $\bar{f}$ is nonzero.

Thus we have

PROPOSITION 5. f' vanishes on L if and only if the Jacobian determinant $(\frac{\partial f_i}{\partial x_j})$ is zero.

Lausch and Nobauer [9] call a polynomial $f \in K[x]$ regular if $f'(a) \neq 0$ for all $a \in K$. Lidl [10] generalized the concept of regularity to polynomials in several variables. We can say that $\bar{f}$ is regular if its Jacobian determinant is nonzero. Now we consider the behaviour of the polynomial vectors $\bar{f}$ with integer coefficients modulo p^e. We say that n polynomials in n variables form a permutation polynomial vector mod p^e if on substitution of elements of $(\mathbf{Z}_{p^e})^n$ we obtain a permutation of $(\mathbf{Z}_{p^e})^n$. Then, based on results from [11] and [12], we have

PROPOSITIION 6. The following conditions are equivalent:

(i) $\bar{f}$ is a permutation polynomial vector mod p^e, $e > 1$;

(ii) $\bar{f}$ is a permutation polynomial vector mod p and the Jacobian deteminant of $\bar{f}$ is nonzero mod p;

(iii) f is a permutation polynomial of $\mathbf{F}_{p^n}$ and $f'(a) \neq 0$ for all a $\mathbf{F}_{p^n}$, i.e. f is a regular permutation polynomial of $\mathbf{F}_{p^n}$.

If we specialize the polynomial f to be the power polynomial x^k then the corresponding polynomial vector $\bar{f}_k$ can be regarded as a generalized Redei vector with integral coefficients. Since x^k is regular only in the case k = 1 we cannot get any non-trivial Redei permutation vectors mod p^e, for e > 1, because of part (iii) in Proposition 6. However, if f(x) is not a power polynomial but a Dickson polynomial $\underline{g}_k(x,a)$ over K then Proposition 6 will yield permutation polynomial vectors $\bar{f}$ mod p^e, e > 1. This follows from the fact that there are regular Dickson polynomials over $K = \mathbf{F}_q$, namely all those $g_k(x,a)$ for which (k, char $\mathbf{F}_q$) = 1. The Chinese Remainder Theorem enables us to generalize to residue class rings $\mathbf{Z}_m$.

PROPOSITION 7. Let f(x) be a Dickson polynomial $g_k(x,a)$ over **Z**, and let

$$m = \prod_{i=1}^{r} p_i^{e_i}, \quad a \neq 0.$$

Then the polynomial vector $\bar{f}$ as defined in section 4 for f(x) replaced by $g_k(x,a)$ is a permutation polynomial vector mod m if and only if (k,v) = 1 where

$$= \underset{1 \leq i \leq r}{\mathrm{lcm}} \{p_i(p_i^{2n} - 1)\}.$$

PROOF. The result follows from: the regularity of $g_k(x,a)$ over $\mathbf{F}_{p_i^n}$ (see Lausch and Nobauer [9] p. 209), $g_k(x,a)$ being a permutation polynomial of $\mathbf{F}_{p_i^n}$ (see [9, P. 209], the Chinese Remainder Theorem and Proposition 6.

7. APPLICATIONS IN CRYPTOLOGY.

Over the past few years there has been considerable interest in applications of algebraic and number theoretic properties of polynomials to the design and anlaysis of algebraic cryptosystems. Two of the most influential papers Diffie and Hellman [13] and Rivest et all [14]; a brief survey of some cryptosystems based on finite fields can be found in Lidl and Niederreiter [15, chapter 9]. Recently, a number of papers consider the use of polynomials and rational functions in defining cryptosystem; in particular, Muler and Nobauer [16, 17], Nobauer [18] study Dickson polynomial cryptosystems and in Nobauer [3-5], Redei functions in one variable are used to define cryptosystems over finite fields and residue class rings of integers. Such invesigations were not confined to polynomials in one variable. Muller and Nobauer [17] and Lidl and Muller [2], [19] introduced cryptosystems which are based on polynomials in several variables. Here we show in examples that some polynomial vectors $\bar{f}$, $\bar{f}^\theta$ and $\bar{f}_k^\theta$ as defined in the previous sections can be used for cryptographic purposes.

EXAMPLE 3. Take the Redei function vectors $\bar{f}_k^\theta$ defined before Proposition 4. These vectors can be used in a conventional cryptosystem over $\mathbf{F}_q$, since they induce permutations of $\mathbf{F}_q^n$ iff $(k,q^n-1) = 1$. For k = 1 the vector $\bar{f}_1^\theta$ induces the identity mapping of $\mathbf{F}_q^n$ into itself and the inverse of the mapping $\bar{f}_k^\theta$ is given by $\bar{f}_{k'}^\theta$, where

$kk' \equiv 1 \pmod{q^n - 1}$. The secret key of a conventional cryptosystem involving Redei function vectors is the parameter k. A message $m \in \mathbf{F}_q^n$ is encrypted as $\bar{f}_k^\theta(m)$ and decrypted by $\bar{f}_{k'}^\theta(\bar{f}_k^\theta(m)) = \bar{f}_1^\theta(m) = m$.

EXAMPLE 4. Redei function vectors can also be used in no-key algorithms or three-pass algorithms (see Lidl and Niederreiter [15], Nobauer [3,4]). The analogy with the one-variable case of Redei functions or Dickson polynomials is straightforward, therfore we omit the details.

EXAMPLE 5. The vectors $\bar{f}_k^\theta$ can also be used in a Diffie-Hellman key distribution scheme for establishing common keys (see Lidl and Niederreiter [15] p. 348, for a description of the scheme introduced by Diffie and Hellman [13]; Muller and Nobuauer [16], and Nobauer [3] contain details for schemes based on Dickson polynomials and Redei functions, respectively). Suppose we have a communications network and a number of users. First we choose a finite field $\mathbf{F}_q$, a polynomial $f \in \mathbf{F}_q[x]$, a basis θ of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ and a vector $c \in \mathbf{F}_q^n$ and make these known to all participants of the network. every user U chooses a positive integer k(U) as a secret key and calculates $\bar{f}_{k(U)}^\theta(c)$ which is stored in a public file accessible to all other users. Two users A and B of the network establish a common key as follows.

1. A obtains $\bar{f}_{k(B)}^\theta(c)$ from the public file;

2. A forms
$$\bar{f}_{k(A)}^\theta(\bar{f}_{k(B)}^\theta(c)) = \bar{f}_{k(A)k(B)}^\theta(c);$$

3. B gets $\bar{f}_{k(A)}^\theta(c)$ from the public file;

4. B forms $\bar{f}_{k(B)}^\theta(\bar{f}_{k(A)}^\theta(c)) = \bar{f}_{k(B)k(A)}^\theta(c)$.

The element $\bar{f}_{k(A)k(B)}^\theta(c) = k(AB)$ is the common key for users A and B.

EXAMPLE 6. Proposition 4 and Proposition 7 enable us to define a public key cryptosystem based on Redei function vectors mod m. Such a system is an RSA type cryptosystem similar to those introduced in Lidl and Muller [2], Nobauer [3,4]. Let m be the product of two primes p_1 and p_2 and let $f(x) = x^k$. Then the Redei function vectors $\bar{f}_k$ induce a permutation of $\mathbf{Z}_m$ iff $(k, \text{l cm}\{p_1^n - 1, p_2^n - 1\}) = 1$. We denote $\text{l cm}\{p_1^n - 1, p_2^n - 1\}$ by v. Then the inverse of the permutation $\bar{f}_k: \mathbf{Z}_m \to \mathbf{Z}_m$ is the permutation $\bar{f}_\ell$ of $\mathbf{Z}_m$ where $k\ell \equiv 1 \pmod{v}$. As in other cryptosystems which are based on polynomials we take $\bar{f}_k$ as he encryption function $\bar{f}_\ell$ as the decryption function, m and k as the public key and p_1, p_2 or ℓ as the private key. Note that by Proposition 7 we can only consider m to be a product of primes and not prime powers. If, however, f(x) is a Dickson polynomial $g_k(x,a)$

then the corresponding Redei function vector $\bar{f}_k$ as defined by (5.1) can give a permutation of $\mathbf{Z}_m$, $m = \Pi p_i^{e_i}$, $e_i \geq 1$, by Proposition 7, and can be used in a public-key cryptosystem mod m.

ACKNOWLEDGEMENT. We acknowledge suport from the ARGS, grant F8415183.

REFERENCES

1. REDEI, L. Uber eindeutig umkehrbare Polynome in endlichen Korpern. Acta Sci. Math. Szeged 11 (1946), 85-92.
2. LIDL, R. and MULLER, W.B. Permutation polynomials in RSA-cryptosystems. Advances in Cryptology, (ed. D. Chaum), Plenum Publ. Corp., New York, pp. 293-301.
3. NOBAUER, R. Key distribution systems, based on polynomial functions and on Redei functions. Problems of Control and Information Th. 15 (1986) 91-100.
4. NOBAUER, R. Redei Funktionen and ihre Anwendung in der Kryptographie. Acta Sci. math. Szeged 50 (1986) 287-298.
5. NOBAUER, R. Cryptanalysis of the Redei scheme. Contributions to General Alg. 3, Holder-Pichler-Tempsky, Wien, 1985, pp. 255-264.
6. FRIED, M. and LIDL, R. On Dickson Polynomials and Redei Functions. Contributions to General Algebra 4. Proceedings of meeting at Salzburg, 1986. Verlag B.G. Teubner, Stuttgart 1987, pp. 139-149.
7. CARLITZ,L. A note on permutation functions over a finte field. duke Math. J. 29 (1969), 325-332.
8. LIDL, R. and NIEDERREITER, H. Finite Fields. Encyclopedia of Mathematics and its Applications Vol. 20. Addison-Wesley, Reading, 1983. Now published by Cambridge University Press.
9. LAUSCH, H. and NOBAUER, W. Algebra of Polynomials. North Holland, Amsterdam, 1973.
10. LIDL, R. Regulare Polynome uber endlichen Korpern. Beitrage Alg. u. Geom 2 (1974), 55-69.
11. NOBAUER, W. Redei-Funktionen fur Zweierpotenzen. Periodica Mathematica Hungaria, 17 (1) (1986) pp. 37-44.
12. NOBAUER, W. Uber Permutationspolynome und Permutationsfunktionen fur Primzahlpotenzen. Monatsch. Math. 69 230-238, 1965.
13. DIFFIE, W. and HELLMAN, M.E. New directions in cryptography. IEEE transactions on Information Theory, IT-22,(1976), 644-654.
14. RIVEST, R.L., SHAMIR, A. and ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21,(1978), 120-126.
15. LIDL, R. and NIEDERREITER, H. Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge, 1986.

16. MULLER, W.B. and NOBAUER, R. Cryptanalysis of the Dickson-Scheme. Springer-Verlag, Lecture Notes in Computer Science, Vol. 219 (1986) 50-61.

17. MULLER, W.B. and NOBAUER, W. Some remarks on public-key cryptosystems. Studia Sci. Math. Hungar. 16, 71-76, 1981.

18. NOBAUER, R. Uber die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen. Acta Arith. 45 (1985), 91-99.

19. LIDL, R. and MULLER, W.B. A note on polynomials and functions in algebraic cryptography. Ars Combinatoria, 17 (1984), 223-229.