Rédei polynomials over fields of characteristic zero

Simeon Ball*

8 February 2013

Abstract

The possible role of Rédei polynomials over fields of characteristic zero in the quest for solutions to problems in the study of geometries and vector spaces over finite fields is discussed. This note is exploratory and does not attempt to solve any particular problem, although an example problem is considered.

1 Introduction

Rédei polynomials were introduced by Rédei in his book [18]. There, he uses them to classify the functions over a finite prime field that determine less than half of the directions; they are simply the linear functions. Building on his work the classification of functions over a non-prime finite field was all but obtained in [8] and finally obtained in [4]. Since then, and indeed before, Rédei polynomials have been used to solve (or partly solve) a variety of problems related to geometries over finite fields. See [1], [3], [7], [9], [10], [11], [12], [13], [14], [15], [16], [17], [19], [20], [21], [22], [23], [25], for a sample of these. In all these cases Rédei polynomials are defined over the same finite field in which the geometrical problem arises. In this note I propose the usage of Rédei polynomials over fields of characteristic zero to tackle the same problems and mention an example where Rédei polynomials over the complex field and the \( p \)-adic field allow us to improve on the results obtained using Rédei polynomials over finite fields.

Let \( \mathbb{F}_q \) denote the finite field with \( q = p^h \) elements, where \( p \) is a prime. Let \( \text{PG}(n, q) \) and \( \text{AG}(n, q) \) denote the \( n \)-dimensional projective and affine spaces over \( \mathbb{F}_q \) respectively.

Let \( \sigma \) be a linear map from \( \mathbb{F}_q^n \) to \( \mathbb{F}_q \) and let \( b \in \mathbb{F}_q \). The set of affine points

\[
\{ x \mid \sigma(x) = b \}
\]

is the hyperplane of \( \text{AG}(n, q) \) defined by \( \sigma \) and \( b \). The set of projective points

\[
\{ \langle x \rangle \mid \sigma(x) = 0, \ x \neq 0 \}
\]

*The author acknowledges the support of the project MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2009-SGR-01387 of the Catalan Research Council.
is the hyperplane of $\text{PG}(n, q)$ defined by $\sigma$. Note that $\langle x \rangle$ denotes the one-dimensional subspace generated by the vector $x$, which is a point in the projective space $\text{PG}(n, q)$.

Let $b(u, v)$ be a symmetric non-degenerate bilinear form on $F^n_q$. For any non-zero vector $u \in F^n_q$, $b$ defines a map from $F^n_q$ to its dual space, where

$$u^*(v) = b(u, v).$$

That is, $u^*$ is a linear map from $F^n_q$ to $F_q$.

Let $S$ be an arbitrary set of points of $\text{AG}(n, q)$ and let $T$ be a set of arbitrary points of $\text{PG}(n, q)$.

2 Rédei polynomials over finite fields

The Rédei polynomial of an affine point set $S$ is defined as

$$f(X, x) = \prod_{s \in S} (X + s^*(x)),$$

where $x \in F^n_q$. Note that if we fix a basis then $f(X, x)$ is a polynomial in $n + 1$ indeterminates. By evaluating at $x \in F^n_q$, $f$ is a map from $F^n_q$ to $F_q[X]$. In this evaluation, if $x = y \in F^n_q$, $y \neq 0$, then the polynomial $f(X, y)$ has the following property.

**Lemma 2.1.** The polynomial $f(X, y)$ has a factor $X + b$ of multiplicity $m$ if and only if the hyperplane defined by $y^*$ and $b$ contains exactly $m$ points of $S$.

It is Lemma 2.1 that allows us to translate geometric properties of the set $S$ to an algebraic property of the function $f$. For example, if $S$ has the property that every hyperplane contains at least $t$ points of $S$ then $f(X, y)$ has the property that $(X^q - X)^t$ divides it, for all $y \in F^n_q$, $y \neq 0$.

The usual method employed is to exploit the fact that, with respect to a basis, if we write

$$f(X, x) = \sum_{j=0}^{\left|S\right|} f_j(x)X^j$$

then the function $f_j(x)$ is a polynomial of degree at most $\left|S\right| - j$. In this vein, the following lemma, the Szőnyi-Weiner Lemma [24] (see also [17]) is frequently applied to the affine Rédei polynomial and can give valuable information about the set $S$. For any $r \in \mathbb{Z}$, let $r^+ = \max\{0, r\}$.

**Lemma 2.2.** Let $f, g \in F_q[X, Y]$ and suppose that the coefficient of $X^d$ in $f$ is non-zero, where $d = \deg f$. Let $k(y) = \deg \gcd(f(X, y), g(X, y))$. For all $z \in F_q$,

$$\sum_{y \in F_q} (k(y) - k(z))^+ \leq (\deg f - k(z))(\deg g - k(z)).$$
The Rédei polynomial of a projective point set $T$ is defined, up to an arbitrarily chosen scalar factor, as

$$F(x) = \prod_{\langle t \rangle \in T} t^*(x).$$

Note that, with respect to a fixed basis, $F(x)$ is a polynomial in $n+1$ indeterminates. In practice the projective Rédei polynomial is not used that often and frequently more information can be obtained by fixing a hyperplane $\pi$ of $\text{PG}(n,q)$ and considering the Rédei polynomial of the affine point set $T \setminus \pi$. However, this is not always the case, examples where projective Rédei polynomials were used can be found in [2], [20] and [21].

## 3 Rédei polynomials over the complex numbers

For any vector $u \in \mathbb{F}_q^n$, let $\chi_u$ denote the complex character, a map from $\mathbb{F}_q^n$ to $\mathbb{C}$, defined by

$$\chi_u(x) = e^{2\pi i \text{Tr}(u^*(x))/p},$$

where $\text{Tr}$ is the Trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

The complex Rédei polynomial of $S$ is defined as

$$g(X, x) = \prod_{s \in S} (X + \chi_s(x)),$$

where $x \in \mathbb{F}_q^n$. Strictly speaking $g$ is a map from $\mathbb{F}_q^n$ to $\mathbb{C}[X]$. In other words it is only after evaluation at $x \in \mathbb{F}_q^n$ that we obtain a polynomial.

If we fix the vector $x = y \in \mathbb{F}_q^n$, $y \neq 0$, then the polynomial $g(X, y)$ has the following property.

**Lemma 3.1.** The polynomial $g(X, y)$ has a factor $X + e^{2\pi ib/p}$ of multiplicity $m$ if and only if the $q/p$ hyperplanes defined by $y^*$ and $\{a \in \mathbb{F}_q \mid \text{Tr}(a) = b\}$ contain (all together) exactly $m$ points of $S$.

Lemma 3.1 shows us that the above definition of the complex Rédei polynomial may not be good enough in the case that $q$ is not prime; for most problems we will need something like Lemma 2.1. This, can be avoided by fixing elements $\lambda_1, \ldots, \lambda_h \in \mathbb{F}_q$ such that

$$a \mapsto (\text{Tr}(\lambda_1 a), \text{Tr}(\lambda_2 a), \ldots, \text{Tr}(\lambda_h a))$$

is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_p^h$, and defining

$$g^+(X_0, \ldots, X_n, x) = \prod_{s \in S} (X_0 + \sum_{i=1}^h \chi_s(\lambda_i x) X_i).$$
If we fix the vector \( x = y \in \mathbb{F}_q^n, y \neq 0 \), then the polynomial \( g^+(X_0, \ldots, X_n, y) \) has the following property.

**Lemma 3.2.** The polynomial \( g^+(X_0, \ldots, X_n, y) \) has a factor \( X_0 + \sum_{i=1}^h e^{2\pi i \text{Tr}(\lambda_i b)} X_i \) of multiplicity \( m \) if and only if the hyperplane defined by \( y^* \) and \( b \) contains exactly \( m \) points of \( S \).

For the sake of simplicity consider only \( g(X, y) \). As in the finite field case, we write

\[
g(X, x) = \sum_{j=0}^{|S|} g_j(x) X^j.
\]

The function \( g_j(x) \) is not a polynomial, as in the finite field case, but it is of the form

\[
g_j(x) = \sum_{u \in \mathbb{F}_q^n} c_u \chi_u(x),
\]

for some \( c_u \in \mathbb{Z} \). The fact that \( c_u \) is an integer allows us to exploit properties of \( g_j(x) \).

Let us consider the previously mentioned example where \( S \) has the property that every hyperplane of \( \text{AG}(n, q) \) contains at least \( t \) points of \( S \). We have that for all \( y \in \mathbb{F}_q^n, y \neq 0 \), the polynomial \( g(X, y) \) is divisible by \( (X^p + 1)^{hq/p} \). This allows us to construct functions which are integer sums of characters (they are in fact integer sums of some of the functions \( g_j \) which are zero, for all \( x \in \mathbb{F}_q^n, x \neq 0 \). The following lemma then gives a divisibility which we exploit to improve the lower bounds on \( |S| \), obtained by using the finite field Rédei polynomial in [3] and [11].

**Lemma 3.3.** Let \( G \) be an abelian group and suppose \( g(x) = \sum_{u \in G} c_u \chi_u(x) \), where \( c_u \in \mathbb{Z} \). If \( g(x) = 0 \) for all \( x \in G \setminus \{0\} \), then \( |G| \) divides \( g(0) \).

For a detailed account of this example and its consequences for linear codes, see [6].

It is not clear to me if there is a useful definition of a complex Rédei polynomial for a projective point set.

The advantage of using complex numbers is that the characteristic is zero, so we can obtained congruences modulo \( p^e \), where \( e \geq 2 \), which is what happens in the aforementioned example. The disadvantage is that \( g_j(x) \), the coefficient of \( X^j \), is not a polynomial, as is the case for \( f_j(x) \) in the finite field case.

To combine the advantage of a field of characteristic zero with the coefficients being polynomials, one possibility is to define Rédei polynomials over the \( p \)-adic numbers. This we shall do in the next section.
4 Rédei polynomials over the $p$-adic numbers

Let $\mathbb{Q}_p$ be the field of $p$-adic numbers and let $\mathbb{K} = \mathbb{Q}_p(\epsilon)$ be the unique unramified extension of $\mathbb{Q}_p$ of degree $h$. Let $\mathcal{R}$ be the ring of integral $p$-adic numbers of $\mathbb{K}$ and let $\mathcal{T}$ be the set of solutions of the equation $x^q = x$ in $\mathcal{R}$.

Let $\tau$ be a lifting of $\mathbb{F}_q$ to $\mathcal{R}$, i.e. it preserves the additive and multiplicative structure of $\mathbb{F}_q$ modulo $p$. By using the canonical basis of $\mathbb{F}_q^n$ we can extend the lifting to a lift of $\mathbb{F}_q^n$ to $\mathcal{R}^n$ by defining

$$\tau((x_1, \ldots, x_n)) = (\tau(x_1), \ldots, \tau(x_n)).$$

As in the finite field case we fix a non-degenerate symmetric bilinear form on $\mathbb{K}^n$, and define $u^*$ as the linear map from $\mathbb{K}^n$ to $\mathbb{K}$ which is the dual of the vector $u \in \mathbb{K}^n$.

The $p$-adic Rédei polynomial of $S$ is defined as

$$h(X, x) = \prod_{s \in S} (X + \tau(s)^*(x)).$$

We can write down an analogous version of Lemma 2.1.

**Lemma 4.1.** For any $a \in \mathcal{R}$ and $x \in \mathcal{R}^n$, $x \neq 0 \pmod{p}$, we have $f(a, x) = 0 \pmod{p^m}$ if and only if the hyperplane defined by $x^* \pmod{p}$ and $a \pmod{p}$ contains $m$ points of $S$.

Then we need to use something like Lemma 4.2.

**Lemma 4.2.** If $f \in \mathcal{R}[X]$ is the product of linear factors where for each $s \in \mathcal{T}$ there are at least $t$ factors $X + a$ of $f$ for which $a = s \pmod{p}$ then

$$f(X) = \sum_{j=0}^{t} (X^q - X)^{t-j} p^j h_j(X),$$

for some polynomials $h_j$, where $\deg h_j \leq \deg f - (t - j)|S|$.

This lemma may also be applicable to the projective version of the $p$-adic Rédei polynomial for $T$ which is defined as

$$H(x) = \prod_{t \in T} \tau(t)^*(x).$$

5 The maximum weight of a linear code

In this section we shall give three theorems on the maximum weight of a linear code, one obtained with each of the different Rédei polynomials considered in the previous sections.
A $k$-dimensional linear code of length $n$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$. After fixing a basis we define the weight of a vector of $\mathbb{F}_q^n$ to be the number of non-zero coordinates. The minimum weight is denoted by $d$ and the maximum weight is denoted by $m$. Recall that $q = p^h$, for some $h$.

Using the Rédei polynomial over $\mathbb{F}_q$ we can prove the following, see [5].

**Theorem 5.1.** If $m = (n - d - k + 1)q + k + F$ then, for all $E \in \{1, \ldots, F\}$ the coefficient of $X^{k(q-1)-q+E-F}$ in

$$(1 + X)^{-m}(1 - X^{q-1})^{n-d}$$

is zero modulo $p$.

Using the Rédei polynomial over $\mathbb{C}$ we have the following from [6].

**Theorem 5.2.** If $m \geq n - d + 1$ then, for all $E \geq 1$, the coefficient of $X^{(n-d)q-m+E}$ in

$$(1 - X)^{-m}(1 - X^p)^{(n-d)q/p}$$

is zero modulo $q^{k-1}$.

Theorem 5.2 turns out to be much stronger than Theorem 5.1 when $q$ is prime. It seems not to be so strong when $q$ is not prime. However, we can extend Theorem 5.1 to the following if we use the $p$-adic Rédei polynomial, see [5].

**Theorem 5.3.** If $m = (n - d + k + e)q + k + F$ then, for all $E \in \{1, \ldots, F\}$ the coefficient of $X^{k(q-1)-q+E-F}$ in

$$(1 + X)^{-m}(1 - X^{q-1})^{n-d+e-1}$$

is zero modulo $p^e$.

**References**


