Lacunary polynomials and finite geometry

Tamás Szőnyi

ELTE, CAI HAS

June 13th, 2013, Szeged, Hungary

Fully reducible, and lacunary polynomials

Definition

A polynomial over a field F is called *fully reducible* if it factors into linear factors over F. A polynomial is *lacunary* if in the sequence of its coefficients a long run of zeroes occurs.

The monograph *Lacunary polynomials over finite fields* by **László Rédei** is devoted entirely to such polynomials and their applications.
We survey the results of that book and some more recent applications of the theory.

Rédei's problems

Problem

Let d be a fixed divisor of $q-1$. Determine those polynomials $f(x) = x^{(q-1)/d} + g(x)$ which are fully reducible, are not divisible by x, do not have multiple roots, and $\deg(g) \leq \frac{q-1}{d^2}$.

Problem

Determine the polynomials $f(x) \in GF(q)[x] \setminus GF(q)[x^p]$, which have the form $f(x) = x^q + h(x)$, are fully reducible and $\deg(h) \leq \frac{q+1}{2}$.

Problem I

Theorem (Rédei)

For $d > 2$ the solutions of Problem 1 are the Euler-binomials $x^{(q-1)/d} - \alpha$ (where $\alpha = u^{(q-1)/d}$ for a nonzero u). For $d = 2$ there are other solutions, namely the polynomials:

$$\left(x^{\frac{q-1}{4}} - \beta\right)\left(x^{\frac{q-1}{4}} - \gamma\right), \quad (\beta^2 = 1,\ \gamma^2 = -1),$$

when $q \equiv 1 \pmod 4$.

This is Theorem 5 in Paragraph 9 in Rédei's book.

Part of the solution to Problem II

Theorem (Rédei)

Let $f(x) = x^q + g(x)$ be fully reducible and suppose that $f'(x) \neq 0$. Then $deg(g) \geq (q+1)/2$, or $f(x) = x^q - x$.

This is proven in Paragraph 10 of Rédei's book: Let $f(x) = s(x)m(x)$, where $s(x) =$ product of roots with multiplicity 1, and let $m(x) =$ multiple roots. Then

$$s(x)|f(x) - (x^q - x) = g(x) + x, \quad m(x)|f'(x) = g'(x).$$

If $f(x) \neq x^q - x$, then $f(x)|(g(x) + x)g'(x)$. Hence $\deg f \leq \deg(g) + \deg(g) - 1)$.

Solutions for $q = p$

Theorem (Rédei)

If $q = p \neq 2$ prime, then the solutions of Problem II are

$$f(x) = (x+a)\left((x+a)^{\frac{p-1}{2}} - \sigma\right)\left((x+a)^{\frac{p-1}{2}} - \sigma\tau\right), \quad (\sigma = \pm 1,\ \tau = 0, 1)$$

Sketch of the proof. Let $g(x) = a_0 x^{(p+1)/2} + a_1 x^{(p-1)/2} + \ldots + a_{(p+1)/2}$. Using a translation $x \to x + c$ we can suppose that $a_1 = 0$.

$$\frac{a_0^2}{2}(x^q + g(x)) = (g(x) + x)g'(x). \tag{1}$$

Therefore, (i) $g(x) + x$ and $g'(x)$ are fully reducible

(ii) $g(x) + x$ divides $x^q - x$, that is it has only simple roots.

Solution for $q = p$, II.

In equation (1), left-hand side is lacunary, i.e. coefficient of $x^{p-1}, \ldots, x^{(p+3)/2}$ is zero. Hence

$$(2) \qquad \sum_{i=0}^{k}(1-2i)a_i a_{k-i} = 0, \quad (k = 1, \ldots (p-3)/2).$$

(this comes from the coefficient of x^{p-k}).
Using $a_1 = 0$ it implies $a_1 = a_2 = \ldots = a_{(p-3)/2} = 0$.
Therefore $g(x) = a_0 x^{(p+1)/2} + a_{(p-1)/2} x + a_{(p+1)/2}$.

General solutions

The actual theorem of Rédei is too complicated, so we just illustrate it. Let us take $q = p^2$: then not only $x(x^{(q-1)/2} - 1)^2$ is a solution but e.g. $x((x^{p+1} - 1)^{(p-1)/2} - 1)^2$ is also a solution.

Intuitively, what happened is that in place of $x + a$ we put the expression $N(x + \varrho) + a$ in the solutions given in Theorem 2.3. In the general case we can repeat this procedure for each chain of subfields in GF(q).

Howevere, in the geometric applications, this general theorem was not (yet) used.

The degenerate solutions

Theorem (Rédei, Thm. 18)

Let $h(x) = x^{q/p^e} + g(x)$ *for some* $1 \leq e < n$ *(where* $q = p^n$, $n \geq 2$*). Suppose that* h *is fully reducible and* $h'(x) \neq 0$*. If* $e \leq n/2$*, then*

$$\deg(g) \geq \frac{q + p^e}{p^e(p^e + 1)}.$$

If $e > n/2$*, then* $\deg(g) \geq p^e$.

Blokhuis' generalizations I.

Theorem (Blokhuis)

Let $f(x) = x^q g(x) + h(x)$ be a fully reducible lacunary polynomial over $\mathrm{GF}(q)$ and assume that $(g(x), h(c)) = 1$ and $f'(x) \neq 0$. Then either $x^q - x$ divides $f(x)$, or the maximum of the degrees of g and h is at least $(q+1)/2$.

Sketch of the proof. Copy Rédei's proof and observe that $s(x)|xg(x) + h(x)$ and $m(x)|f(x)g'(x) - f'(x)g(x)$.

Blokhuis' generalizations II.

Theorem (Blokhuis)

Let $h(x) = x^{q/p^e} f(x) + g(x)$ *for some* $1 \leq e < n$ *(where* $q = p^n$, $n \geq 2$*). Suppose that* h *is fully reducible,* $(f(x), g(x)) = 1$ *and* $h'(x) \neq 0$*. If* $e \leq n/2$*, then*

$$\max\{\deg(f), \deg(g)\} \geq \frac{q + p^e}{p^e(p^e + 1)}.$$

If $e > n/2$*, then* $\max\{\deg(f), \deg(g)\} \geq p^e$

Combine the proof of the previous result and Rédei's proof to bound the degree in case of the degenerate solutions. The bound can be further improved:
$\max\{\deg(g), \deg(f)\} \geq \lceil (q/p^e + 1)/(p^e + 1) \rceil \cdot p^e$.
Remark: For $e|n$ the theorem is essentially sharp.

Trace and Norm

In the special case $e = n/2$, the previous bound gives $\max\{\deg(g), \deg(f)\} \geq \sqrt{q}$.

In case of equality BALL and GÁCS-SZT proved that $h(x)$ is either the Trace or the Norm function from $\mathrm{GF}(q)$ to $\mathrm{GF}(\sqrt{q})$.

They also showed that $\max\{\deg(f), \deg(g)\} = 2\sqrt{q}$ is not possible.

Improvements by Blokhuis, Storme, SzT

Theorem (Blokhuis, Storme, SzT)

Let $f \in GF(q)[x]$ be fully reducible, $f(x) = x^q g(x) + h(x)$, where $(g, h) = 1$. Let $k < q$ be $\max(\deg(g), \deg(h))$. Let e be maximal such that f is a p^e-th power. Then we have one of the following:

- *(1) $e = n$ and $k = 0$,*
- *(2) $e \geq 2n/3$ and $k \geq p^e$,*
- *(3) $2n/3 > e > n/2$ and $k \geq p^{n-e/2} - \frac{3}{2}p^{n-e}$,*
- *(4) $e = n/2$ and $k = p^e$ and $f(x) = aTr(bx + c) + d$ or $f(x) = aN(bx + c) + d$ for suitable constants a, b, c, d. Here Tr and N respectively denote the trace and the norm function from $GF(q)$ to $GF(\sqrt{q})$,*

Improvements by Blokhuis, Storme, SzT, II

Theorem (BBS continued)

Let $f \in GF(q)[x]$ be fully reducible, $f(x) = x^q g(x) + h(x)$, where $(g, h) = 1$. Let $k < q$ be $\max(\deg(g), \deg(h))$. *Let e be maximal such that f is a p^e-th power. Then we have one of the following:*

- *(5) $e = n/2$ and $k \geq p^e \left\lceil \frac{1}{4} + \sqrt{(p^e+1)/2} \right\rceil$*
- *(6) $n/2 > e > n/3$ and $k \geq p^{(n+e)/2} - p^{n-e} - p^e/2$, or if $3e = n+1$ and $p \leq 3$, then $k \geq p^e(p^e+1)/2$,*
- *(7) $n/3 \geq e > 0$ and $k \geq p^e \lceil (p^{n-e}+1)/(p^e+1) \rceil$,*
- *(8) $e = 0$ and $k \geq (q+1)/2$*
- *(9) $e = 0$, $k = 1$ and $f(x) = a(x^q - x)$.*

Directions

Problem (Rédei, Par. 36)

Given a function f on $GF(q)$ how many different values can the difference quotients $(f(x) - f(y))/(x - y)$ take?

Geometrically, this is equivalent to the following question. How many directions are determined by a set U of q points in the affine plane $\mathrm{AG}(2, q)$?

Definition

A direction (or an infinite point of $\mathrm{AG}(2, q)$) is determined by U if there is a pair of points in U so that the line joining them passes through this infinite point.

The Rédei polynomial

Consider a subset $U = \{(a_i, b_i) : i = 1, \ldots, |U|\}$ of the affine plane $\mathrm{AG}(2, q)$. Recall that the lines of this plane have equation $X = c$ or $Y - yX + x = 0$. The *Rédei polynomial* of U is

$$H(X, Y) := \prod_i (X + a_i Y - b_i) = X^{|U|} + h_1(Y)X^{|U|-1} + \ldots + h_{|U|}(Y).$$

Note that for all $j = 1, \ldots, |U|$: $\deg(h_j) \leq j$. The trick will always be to consider $H(X, Y)$ for a fixed $Y = y$. It encodes line intersections of U.

Lemma

The value $X = b$ is an r-fold root of the polynomial $H(X, m)$ if and only if the line with equation $Y = mX + b$ meets U in exactly r points.

The Rédei-Megyesi theorem

Theorem (Rédei-Megyesi, Thm. 24')

A set of p points in $AG(2,p)$, (p prime), is either a line or determines at least $(p+3)/2$ directions.

Sketch of the proof. Let D be the set of directions determined by U and suppose that $\infty \in D$. The point (y) is not determined by U if and only if $H_y(x) = x^p - x$.

Proof of Rédei-Megyesi

Therefore $h_j(y) = 0$ for at least $q + 1 - |D|$ different y's, which implies that $h_1(y), \ldots, h_{q-|D|}(y)$ are identically zero.

If one considers $H_y(x)$ for $y \in D$, then $H_y(x) = x^p + g_y(x)$ with $\deg(g_y) \leq |D| - 1$ and it is fully reducible. $|D| - 1 \geq (p+1)/2$, by the theorem of Rédei on lacunary polynomials (case $q = p$).

This result, together with the theorem on lacunary polynomials was rediscovered by Dress, Klin, Muzychuk.

The Lovász-Schrijver theorem

Theorem (Lovász-Schrijver)

A set U determining $(p+3)/2$ directions is projectively equivalent to

$$\{(0,a) \ : \ a^{(p-1)/2}=1\} \cup \{(b,0) \ : \ b^{(p-1)/2}=1\} \cup \{(0,0)\}.$$

This actually follows from Rédei's characterization of the solutions of his Problem II for $q=p$. Geometrically, it gives that lines through an ideal point either meet the set U in 2 points ($(p-1)/2$ times) and 1 point once, or there is a line with $(p+1)/2$ points and the remaining lines meet U in 1 point.

Gács's theorem for $q = p$

Looking at the examples given when $q = p$ is a prime, we see that one can obtain Rédei type blocking sets of size $3(p+1)/2$, and the next example coming from Megyesi's construction will have size at least $p + (2p+2)/3$. The following theorem almost reaches this bound.

Theorem (Gács)

Let B be a Rédei type blocking set of $\mathrm{PG}(2, p)$, where p is prime. Then either B is the projective triangle or $|B| \geq p + [2(p-1)/3] + 1$.

Gács-Lovász-SzT for $q = p^2$

Theorem (GLS)

Any blocking set in $\mathrm{PG}(2, p^2)$ *of Rédei type of size* $3(p^2+1)/2$ *has to be equivalent to the projective triangle. If the Rédei type blocking set has more than this number of points, then it has at least* $1 + (3p^2 + p)/2$ *points.*

This does not use Rédei's general (and difficult) theorem on the solutions of Problem II. The bound here is sharp, Polverino, SzT and Weiner constructed examples of this size.

Rédei's results on directions for general q

Theorem (Rédei, Thm 24)

Let $f : K \to K$ ($K = GF(q)$) be any function, and let N be the number of directions determined by the graph of f. Then either $N = 1$, and f is linear, or $N \geq (q+1)/2$, or $1 + (q-1)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some e, $1 \leq e \leq [n/2]$.

Slight improvements on Rédei's theorem are contained in Blokhuis, Brouwer, Szőnyi [BBS]. For example, we proved that $N \geq (q+3)/2$ (instead of $(q+1)/2$) and that the e's for which $n/3 < e < n/2$ do not occur.

The Blokhuis,Ball,Brouwer,Storme, SzT thm

Theorem (Blokhuis, Ball, Brouwer, Storme, SzT)

Let $U \subset K^2$ be a point set of size q containing the origin, let D be the set of directions determined by U, and put $N := |D|$. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then we have one of the following:

(i) $e = 0$ *and* $(q+3)/2 \leq N \leq q+1$,

(ii) $e = 1$, $p = 2$, *and* $(q+5)/3 \leq N \leq q-1$,

(iii) $p^e > 2$, $e|n$, *and* $q/p^e + 1 \leq N \leq (q-1)/(p^e-1)$,

(iv) $e = n$ *and* $N = 1$.

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3+1$), then U is $\mathrm{GF}(p^e)$-linear, and all possibilities for N can be determined explicitly (in principle).

Ball's improvement

Simeon Ball found a beautiful new proof of this result, which deals with the missing cases. This means that for $p^e = 2$ he proved the lower bound $q/2 + 1 \leq N$, and for $p^e = 3$ his method gives the $\mathrm{GF}(3)$-linearity of the set U.

Directions determined by $< q$ pts

Theorem (SzT)

A set of $k = p - n$ points in $AG(2, p)$ is either contained in a line, or it determines at least $(p + 3 - n)/2 = (k + 3)/2$ directions.

Sometimes sharp: put a multiplicative subgroup on the two axes.
About the proof: Rédei type results for polynomials which are not fully reducible, but have many roots in $\mathrm{GF}(q)$.
Generalization for $q = p^h$: FANCSALI, SZIKLAI, TAKÁTS

The Fancsali, Sziklai, Takáts thm

Theorem

Let U be a subset of $\mathrm{AG}(2,q)$, D be the set of determined directions. Let $s=p^e$ be max. s.t. every line meets U in 0 mod s points. Let T denote another parameter defined by using the Rédei pol. Then $s \le t$. If U is not contained in a line then either

- *(1)* $1=s\le t<q$, *and* $\frac{|U|-1}{t+1}+2\le |D|\le q+1$, *or*
- *(2)* $1<s\le t<q$, *and* $\frac{|U|-1}{t+1}+2\le |D|\le \frac{|U|-1}{s-1}$.

Blocking sets

Definition

A *blocking set* is a set of points in $\mathrm{PG}(2,q)$ which meets every line. It is called *non-trivial* if it contains no line. It is *minimal* if deletion of any of its points results in a set which does not meet every line. Geometrically, this means that there is a tangent line at each point of the blocking set.

Combinatorial result: BRUEN(-PELIKÁN) for a non-trivial blocking set $|B| \geq q + \sqrt{q} + 1$, and in case of equality we have a subplane of order $\sqrt{q}$. A blocking set is *of Rédei type* if there is a line ℓ with $|B \setminus \ell| = q$. This is essentially equivalent with the direction problem.

Lower bound for blocking sets

Theorem (Blokhuis)

Let B be a non-trivial blocking set of $\mathrm{PG}(2,q)$. If q is a prime, then $|B| \geq 3(p+1)/2$. If $q = p^h$ is not a prime, then $|B| \geq q + \sqrt{pq} + 1$.

The proof uses lacunary polynomials and the Rédei polynomial.

Small minimal blocking sets

A blocking set is called *small* if it has size less than $3(q+1)/2$. Such minimal blocking sets are characterized in some cases.

Theorem

(1) *(Blokhuis) If $q = p$ prime, then there are no small minimal non-trivial blocking sets in $\mathrm{PG}(2, p)$ at all;*

(2) *(Szőnyi) If $q = p^2$, p prime, then small minimal non-trivial blocking sets in $\mathrm{PG}(2, p^2)$ are Baer subplanes;*

(3) *(Polverino) If $q = p^3$, p prime, $p \geq 7$, then small minimal non-trivial blocking sets in $\mathrm{PG}(2, p^3)$ have size $p^3 + p^2 + 1$ or $p^3 + p^2 + p + 1$ and they are of Rédei type.*

1 modulo p results

There is a result which serves as a main tool in the proof of many particular cases of the Linearity Conjecture.

Theorem

(i) (Szőnyi) *In* $\mathrm{PG}(2,q)$, $q=p^h$, *if* B *is a minimal blocking set of size less than* $3(q+1)/2$, *then each line intersects it in 1 modulo* p^e *points for some* $e \geq 1$;

(ii) (Sziklai) *here* $e|h$, *so* $\mathrm{GF}(p^e)$ *is a subfield of* $\mathrm{GF}(q)$. *Moreover, most of the secant lines intersect* B *in a pointset isomorphic to* $\mathrm{PG}(1,p^e)$, *i.e. in a linear pointset.*

These results, together with standard counting arguments give lower and upper bounds for the possible sizes of minimal blocking sets.

A stability result

Theorem (Weiner-SzT)

Let B be a set of points of $\mathrm{PG}(2,q)$, $q=p$ prime, with at most $\frac{3}{2}(q+1)-\beta$ points. Suppose that the number δ of 0-secants is less than $(\frac{2}{3}(\beta+1))^2/2$. Then there is a line that contains at least $q-\frac{2\delta}{q+1}$ points.

The proof is again by using almost fully reducible lacunary polynomials.

An application for character sums

Theorem (Rédei, Thm. 26)

Let ϱ be a p-th root of unity, $S = a_0 + a_1\varrho + \ldots + a_{p-1}\varrho^{p-1} \neq 0$, $a_0 + \ldots + a_{p-1} = p$, $a_i \in \mathbf{N}$, $a_i < p$. In other words, S is a p-term sum consisting of p-th roots of unity ($p \neq 2$), so that not all terms in S are equal and S is not $1 + \varrho + \ldots + \varrho^{p-1}$. If S is divisible by $(1-\varrho)^t$ then $t \leq (p-1)/2$. Let Γ be the Gaussian sum $\sum \varrho^{i^2}$. If S is divisible by $(1-\varrho)^{(p-1)/2}$ then for some integer a we have

$$\varrho^a S = \Gamma, \quad \text{or} \quad \varrho^a S = -\Gamma, \quad \text{or} \quad \varrho^a S = \frac{1}{2}(p \pm \Gamma).$$

Character sums II.

Then Rédei goes on to specialize Theorem 2.7 for sums of type $S = \pm\varrho \pm \varrho^2 \pm \ldots \pm \varrho^{p-1}$. Using Theorem 2.1 he proves that such an S can be divisible by at most the $(p-1)/4$-th power of $(1-\varrho)$ if it is different from the exceptions given in Theorem 2.7. Using Theorem 2.1 also the case of equality can be characterized. As far as I know, this is the only place where Theorem 2.1 is applied. These results were proved independently by Carlitz. Rédei also proved similar divisibility conditions for certain signed sums, in which not all p-th roots of unity occur, see Thm. 27.

Application to planar functions

Definition

A function $f : F \to F$ is *planar* if $x \to f(x+a) - f(x)$ is bijective for every $a \neq 0$.

Trivial examples of planar functions are quadratic functions over fields of odd characteristic.

Theorem (Hiramine, Gluck, Rónyai-SzT)

Over the field GF(p), p prime, every planar function is quadratic.

THANK YOU

THANK YOU FOR YOUR ATTENTION