On Lacunary Polynomials

József Solymosi, U. of British Columbia

August 5, 2021

Rédei polynomial

Definition (Lacunary polynomial)

A polynomial is *lacunary* if a long run of zeroes appears in its sequence of coefficients (usually between the highest and second highest term). For example, $x^{100} + x + 1$.

Rédei polynomial

Definition (Lacunary polynomial)

A polynomial is *lacunary* if a long run of zeroes appears in its sequence of coefficients (usually between the highest and second highest term). For example, $x^{100} + x + 1$.

Rédei polynomials have many interesting applications, but the most famous application is bounding the number of directions.

Rédei polynomial

Definition (Lacunary polynomial)

A polynomial is *lacunary* if a long run of zeroes appears in its sequence of coefficients (usually between the highest and second highest term). For example, $x^{100} + x + 1$.

Rédei polynomials have many interesting applications, but the most famous application is bounding the number of directions.

Definition (Rédei polynomial)

Let $U = \{(a_i, b_i)\}_{i=1}^{n} \subset AG(2, p)$. The *Rédei polynomial* of U is

$$H(x, y) = \prod_{i=1}^{n} (x + a_i y - b_i)$$

$$= x^n + h_1(y)x^{n-1} + \cdots + h_n(y).$$

Determined directions

Definition (Directions)

Let U be a subset of the affine plane $AG(2, p)$, where p is a prime number. A direction is *determined* by U if two points of U lie on a line in that direction.

Determined directions

Definition (Directions)

Let U be a subset of the affine plane $AG(2, p)$, where p is a prime number. A direction is *determined* by U if two points of U lie on a line in that direction.

$AG(2, p)$ can be coordinatized so that $U = \{(a_i, b_i) \colon 1 \leq i \leq |U|\}$, where $a_i, b_i \in GF(p)$ for all $1 \leq i \leq |U|$. The set of directions determined by U is given by

$$D = \left\{ \frac{b_i - b_j}{a_i - a_j} \colon 1 \leq i < j \leq n \right\}.$$

Determined directions

Definition (Directions)

Let U be a subset of the affine plane $AG(2,p)$, where p is a prime number. A direction is *determined* by U if two points of U lie on a line in that direction.

$AG(2,p)$ can be coordinatized so that $U = \{(a_i, b_i) \colon 1 \leq i \leq |U|\}$, where $a_i, b_i \in GF(p)$ for all $1 \leq i \leq |U|$. The set of directions determined by U is given by

$$D = \left\{ \frac{b_i - b_j}{a_i - a_j} \colon 1 \leq i < j \leq n \right\}.$$

Note that D is a subset of $GF(p) \cup \{\infty\}$. If U is a subset of a line, then $|D| = 1$ (for example).

Rédei polynomial, $|U| = p$

Notice that for any $U \subset AG(2,p)$ such that $|U| \geq p+1$, U will determine all $p+1$ directions.

Lets first use the Rédei polynomial in the case $|U| = p$. If for some pair $1 \leq i, j \leq p$ we have

$$a_i y - b_i = a_j y - b_j,$$

then $y \in D$, since

$$y = \frac{b_j - b_i}{a_j - a_i}.$$

Rédei polynomial, $|U| = p$

Notice that for any $U \subset AG(2,p)$ such that $|U| \geq p+1$, U will determine all $p+1$ directions.

Lets first use the Rédei polynomial in the case $|U| = p$. If for some pair $1 \leq i,j \leq p$ we have

$$a_i y - b_i = a_j y - b_j,$$

then $y \in D$, since

$$y = \frac{b_j - b_i}{a_j - a_i}.$$

Conversely, if $y \notin D$, then $\{a_i y - b_i\}_{i=1}^{p}$ are all distinct, and therefore

$$H(x,y) = \prod_{i=1}^{p}(x + a_i y - b_i) = x^p - x.$$

Rédei polynomial, $|U| = p$

$$H(x,y) = \prod_{i=1}^{p} (x + a_i y - b_i)$$
$$= x^p + h_1(y)x^{p-1} + \cdots + h_n(y).$$

Every $y \notin D$ is a zero of $h_i(y)$, $1 \leq i \leq p-2$.

Since $\deg h_i \leq i$, $h_i \equiv 0$ for $1 \leq i \leq p - |D|$.

Equivalently, if $h_i \not\equiv 0$, then $|D| \geq p + 1 - i$.

For some $y \in D$, put $H_y(x) = x^p + g_y(x)$. Then $|D| \geq \deg(g_y) + 1$

Rédei polynomial, $|U| = p$

$$H(x, y) = \prod_{i=1}^{p} (x + a_i y - b_i)$$
$$= x^p + h_1(y)x^{p-1} + \cdots + h_n(y).$$

Every $y \notin D$ is a zero of $h_i(y)$, $1 \leq i \leq p - 2$.

Since $\deg h_i \leq i$, $h_i \equiv 0$ for $1 \leq i \leq p - |D|$.

Equivalently, if $h_i \not\equiv 0$, then $|D| \geq p + 1 - i$.

For some $y \in D$, put $H_y(x) = x^p + g_y(x)$. Then $|D| \geq \deg(g_y) + 1$

Theorem (Rédei)

Let $f(x) = x^p + g(x)$ be fully reducible and suppose that $f'(x) \not\equiv 0$. Then $\deg(g) \geq \frac{p+1}{2}$; or $f(x) = x^p - x$.

Rédei polynomial, $|U| = p$

Theorem (Rédei and Megyesi, 1970)

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

Rédei polynomial, $|U| = p$

Theorem (Rédei and Megyesi, 1970)

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

Sets of p points that determine the minimum number of directions are understood.

Theorem (Lovász and Schrijver, 1981)

If a set of p points in $AG(2, p)$ determines $\frac{p+3}{2}$ directions, then it can be coordinatized as

$$\{(k, k^{\frac{p+1}{2}}) \colon k \in GF(p)\}.$$

Szőnyi's extension

Theorem (Szőnyi, 1991)

A set of n points in $AG(2,p)$ is either contained in a line or determines at least $\frac{n+3}{2}$ directions.

Szőnyi's above generalization follows a similar argument to Rédei and Megyesi's with the addition of an 'extension polynomial'.

Szőnyi's extension

Let $U = \{(a_i, b_i)\}_{i=1}^n \subset AG(2,p)$. As before, if $y \notin D$, then

$$H(x,y) = \prod_{i=1}^{n}(x + a_i y - b_i),$$

has all distinct roots. Construct the polynomial $f(x,y)$ such that for every $y \notin D$ we have

$$H(x,y)f(x,y) = x^p - x.$$

For $y \in D$, put

$$H(x,y)f(x,y) = x^p + g_y(x).$$

Once again, we'll have the property

$$|D| \geq \deg(g_y) + 1.$$

Rédei polynomial for a Cartesian product

Let $A = \{a_i\}_{i=1}^m, B = \{b_j\}_{j=1}^n$. The Rédei polynomial of $A \times B$ is

$$H(x, y) = \prod_{i,j}(x + a_i y - b_j).$$

The direction $y = 0$ is in D. Put

$$\begin{aligned} H(x, 0)f(x, 0) &= f(x, 0)\prod_{j}(x - b_j)^m \\ &= x^p + c_1 x^{p-1} + \cdots + c_p. \end{aligned}$$

Main theorem

Theorem (Di Benedetto, S., White, 2020)

Let $A, B \subset GF(p)$ be sets each of size at least two such that $|A||B| < p$. Then the set of points $A \times B \subset AG(2,p)$ determines at least

$$|A||B| - \min\{|A|, |B|\} + 2$$

directions.

Paley graph

Let $p \equiv 1 \pmod 4$ be prime. The Paley graph P_p has vertex set $\{0, 1, \ldots, p-1\}$. There is an edge between x and y if $x - y$ is a quadratic residue, $\chi(x - y) = 1$. (χ is the quadratic character, $\chi(a) = \pm 1$ or 0)

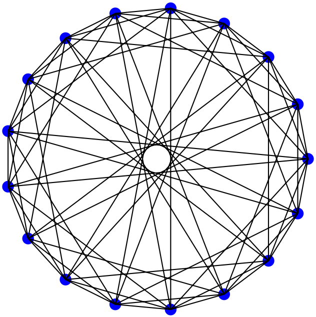

Figure: Paley graph, $p = 17$

Paley clique

Estimating the size of the clique number of P_p is a difficult open problem.

$$\Omega(\log p \log\log\log p) \lesssim \omega(P_p) \le \frac{\sqrt{2p-1}+1}{2}.$$

- Lower bound (for some primes p): Graham and Ringrose (1990)
- Upper bound: Hanson and Petridis (2019)
- Lower bound for some primes can be improved under GRH

Paley clique

Estimating the size of the clique number of P_p is a difficult open problem.

$$\Omega(\log p \log\log\log p) \lesssim \omega(P_p) \leq \frac{\sqrt{2p-1}+1}{2}.$$

- Lower bound (for some primes p): Graham and Ringrose (1990)
- Upper bound: Hanson and Petridis (2019)
- Lower bound for some primes can be improved under GRH

The best general lower bound for all p^r, when $p \equiv 1 \pmod 4$, was given by Cohen (1988), but for primes the bound is weaker than the present bound for arbitrary graphs.

Diagonal Ramsey

The current best bound on the diagonal Ramsey number is due to Ashwin Sah (2020)

$$R(k+1,k+1) \leq \exp(-c(\log k)^2)\binom{2k}{k} << 4^k$$

One would expect that in a Paley graph the algebraic structure allows us to get a better bound.

Diagonal Ramsey

The current best bound on the diagonal Ramsey number is due to Ashwin Sah (2020)

$$R(k+1,k+1) \leq \exp(-c(\log k)^2)\binom{2k}{k} << 4^k$$

One would expect that in a Paley graph the algebraic structure allows us to get a better bound.

Theorem

If $p \geq 3.009^k$ then the Paley graph in $\mathbb{F}_p$ has a clique of size k.

Application of the direction bound: Paley clique

Corollary

If $A \subset GF(p)$ is a Paley clique, then the number of directions determined by $A \times A$ is at most $\frac{p-1}{2} + 2$. Therefore,

$$|A|^2 - |A| + 2 \leq \text{Number of directions in } A \times A \leq \frac{p+3}{2}.$$

Directions and additive combinatorics

Let $A, B \subset GF(p)$. Suppose $A - A$ and $B - B$ belong to a subgroup G of $GF(p)^*$. Then all directions determined by $A \times B$ belong to $G \cup \{0, \infty\}$.

$$\left\{ \frac{b - b'}{a - a'} : a, a' \in A,\ b, b' \in B \right\} \subseteq G \cup \{0, \infty\}.$$

Directions and additive combinatorics

Let $A, B \subset GF(p)$. Suppose $A - A$ and $B - B$ belong to a subgroup G of $GF(p)^*$. Then all directions determined by $A \times B$ belong to $G \cup \{0, \infty\}$.

$$\left\{ \frac{b - b'}{a - a'} : a, a' \in A,\ b, b' \in B \right\} \subseteq G \cup \{0, \infty\}.$$

Observation

A lower bound on the directions in $A \times B$ results in a lower bound on $|G|$.

Thank you!

Kyle Yip will talk about the Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields and then Ethan White will talk about the number of distinct roots of a lacunary polynomial over finite fields.