On the arithmetic of generalized Fekete polynomials

Tung T. Nguyen

Western University

Fields Institute Number Theory Seminar, 10/2022.

Contents

- Generalized Fekete polynomials.
- Galois theory for generalized Fekete polynomials.
- Applications to graph theory.

This talk is a report on joint work with Jan Mináč and Nguyễn Duy Tân, which is a continuation of our previous work "Fekete polynomials, quadratic residues, and arithmetic" (Journal of Number Theory, 2022).

Legendre symbol, Jacobi symbol

Let a be an integer.

- The Legendre symbol $\left(\frac{a}{p}\right)$, where p is a prime, is defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a square modulo p} \\ -1 & \text{else.} \end{cases}$$

- The Jacobi symbol $\left(\frac{a}{b}\right)$, where b is an odd positive integer, is a generalization of the Legendre symbol. Specifically, let us suppose that b has the following prime factorization

$$b = p_1^{e_q} p_2^{e_2} \ldots p_r^{e_r}.$$

Then

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_r}\right)^{e_r},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

Kronecker symbol

The Kronecker symbol, which generalizes both the Legendre and the Jacobi symbols. Let n be an integer.

- $\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0 \\ -1 & \text{if } a < 0, \end{cases}$
- $\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2|a \\ 1 & \text{if } a \equiv \pm 1 \pmod 8 \\ -1 & \text{if } a \equiv \pm 3 \pmod 8), \end{cases}$
- Suppose that n has the following factorization into product of distinct prime numbers

  $$n = \operatorname{sgn}(n) p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}.$$

  Here $\operatorname{sgn}(n)$ is the sign of n, which is 1 if $n > 0$ and -1 otherwise. Then,

  $$\left(\frac{a}{n}\right) = \left(\frac{a}{\operatorname{sgn(n)}}\right) \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \ldots \left(\frac{a}{p_r}\right)^{e_r}.$$

Quadratic characters

- d a squarefree integer, Δ the discriminant of the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, which is given by

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

- Let $\chi_\Delta : \mathbb{Z} \to \mathbb{C}^\times$ be the function given by

$$\chi_\Delta(a) = \left(\frac{\Delta}{a}\right),$$

  where $\left(\frac{\Delta}{a}\right)$ is the Kronecker symbol. Then χ_Δ is a primitive quadratic character of conductor $D = |\Delta|$.

Special value of L-function at 1

- The L-function associated to χ_Δ is

$$L(\chi_\Delta, s) = \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s}.$$

- The special value at $s = 1$ has a nice formula

$$L(\chi_\Delta, 1) = \int_0^1 \frac{F_\Delta(x)}{x(1-x^D)} dx.$$

- Here

$$F_\Delta(x) = F_{\chi_\Delta}(x) = \sum_{a=1}^{D-1} \chi_\Delta(a) x^a = \sum_{a=1}^{D-1} \left(\frac{\Delta}{a}\right) x^a.$$

Definition

The polynomial

$$F_\Delta(x) = F_{\chi_\Delta}(x) = \sum_{a=1}^{D-1} \chi_\Delta(a) x^a = \sum_{a=1}^{D-1} \left(\frac{\Delta}{a}\right) x^a$$

is called the generalized Fekete polynomial associated with χ_Δ (or Δ).

- The case $D = |\Delta| = p$ prime was first studied by Fekete (hence the name). He observed that if $F_\Delta(x)$ has no real roots on $(0, 1)$ then $L(s, \chi) \neq 0$ for $s \in (0, 1)$.
- We are interested in arithmetic properties of $F_\Delta(x)$.

Examples

Let Φ_n be the n-th cyclotomic polynomial.

- $\Delta = -3 \times 5$:

$$\begin{aligned} F_\Delta(x) &= -x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1) \\ &\quad \times (x^6 - x^4 + 2x^3 - x^2 + 1) \\ &= -x\Phi_1(x)\Phi_3(x)\Phi_5(x)(x^6 - x^4 + 2x^3 - x^2 + 1). \end{aligned}$$

- $\Delta = 3 \times 7$:

$$\begin{aligned} F_\Delta(x) = {} & x(x+1)(x-1)^2(x^2+x+1)\times \\ & (x^6+x^5+x^4+x^3+x^2+x+1)\times \\ & (x^8 - 2x^7 + 2x^6 + 2x^2 - 2x + 1) \\ & = x\Phi_1(x)^2\Phi_2(x)\Phi_3(x)\Phi_7(x)(x^8 - 2x^7 + 2x^6 + 2x^2 - 2x + 1). \end{aligned}$$

Example

$\Delta = 4 \times 11$:

$$\begin{aligned} F_\Delta(x) =& x(\Phi_1(x))^2(\Phi_2(x))^2\Phi_4(x)\Phi_{11}(x)\Phi_{22}(x)\times \\ & (x^{16} - x^{14} + 2x^{12} + 3x^8 + 2x^4 - x^2 + 1) \\ =& x\Phi_1(x^2)^2\Phi_2(x^2)\Phi_{11}(x^2)f_\Delta(x^2), \end{aligned}$$

where

$$f_\Delta(x) = x^8 - x^7 + 2x^6 + 3x^4 + 2x^2 - x + 1.$$

Modified Fekete polynomials

Note that if Δ is even, $\chi_\Delta(a) = 0$ for a even. Consequently, $F_\Delta(x)/x$ is a polynomial in x^2.

Definition

Suppose that Δ is an even number. The modified Fekete polynomial $\tilde{F}_\Delta(x)$ associated with Δ is given by

$$F_\Delta(x) = x\tilde{F}_\Delta(x^2).$$

Concretely

$$\tilde{F}_\Delta(x) = \sum_{a=0}^{D/2-1} \left(\frac{\Delta}{2a+1}\right) x^a.$$

Example: if $\Delta = 4 \times 11$,

$$\tilde{F}_\Delta(x) = \Phi_1(x)^2\Phi_2(x)\Phi_{11}(x)f_\Delta(x),$$

where

$$f_\Delta(x) = x^8 - x^7 + 2x^6 + 3x^4 + 2x^2 - x + 1$$

Cyclotomic factors

Recall $D = |\Delta|$.

Observation

if $n \mid D$ and $n \neq D$ then $\Phi_n(x)$ is a factor of F_Δ.

Let b an integer. Let $\zeta_D = \exp\left(\frac{2\pi i}{D}\right)$ be a primitive D-root of unity.

Definition

The Gauss sum $G(b, \chi_\Delta)$ is defined as follow

$$G(b, \chi_\Delta) = \sum_{a=1}^{D-1} \chi_\Delta(a) \zeta_D^{ab} = F_\Delta(\zeta_D^b).$$

We have the following fundamental property

$$G(b, \chi_\Delta) = \chi_\Delta(b) G(1, \chi_\Delta).$$

Consequencely, if $\gcd(b, D) > 1$ then $F_\Delta(\zeta_D^b) = 0$. In other words, if $n \mid D$ and $n \neq D$ then $F_\Delta(\zeta_n) = 0$.

Question

Let n be a positive integer. What is the multiplicity of ζ_n as a root of $F_\Delta(x)$?

- We remark that in the above question, we do not require n to be a divisor of D.
- For simplicity, we will write $r_\Delta(\Phi_n) = r_\Delta(n)$ (respectively $\tilde{r}_\Delta(\Phi_n) = \tilde{r}_\Delta(n)$) for the multiplicity of $\Phi_n(x)$ in $F_\Delta(x)$ (respectively $\tilde{F}_\Delta(x)$.)
- For simplicity, we will only consider Δ odd in this talk.

The multiplicities of Φ_1 and Φ_2

Proposition 1.

Suppose that Δ is odd. Then

$$r_{\Delta}(\Phi_1) = \begin{cases} 1 & \text{if } \Delta < 0 \\ 2 & \text{if } \Delta > 0, \end{cases}$$

$$r_{\Delta}(\Phi_2) = \begin{cases} 0 & \text{if } \Delta < 0 \\ 1 & \text{if } \Delta > 0. \end{cases}$$

Proof of Proposition 1

We observe that

$$F_\Delta(1) = \sum_{a=1}^{D-1} \chi_\Delta(a) = 0.$$

So, $x = 1$ is a root of F_Δ. To study its multiplicity, we need to consider higher order derivatives $F^{(n)}(1)$. Our strategy is to connect the following objects

$$\begin{tikzcd}
 & \text{Higher derivatives of } F_\Delta(x) \arrow[dl] \\
\text{Bernoulli numbers} \arrow[r] & \text{Special values of L-functions} \arrow[u]
\end{tikzcd}$$

Bernoulli numbers and Bernoulli polynomials

Definition

Let χ be a primitive Dirichlet character of conductor $f = f_\chi$. The generalized Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}$$

The Bernoulli polynomials $B_{n,\chi}(x)$ are defined as follow

$$B_{n,\chi}(x) = \sum_{k=0}^{n} \binom{n}{k} B_{k,\chi}x^{n-k}, \quad n \geq 0.$$

Bernoulli numbers and special values of L-functions

Let χ be as above. Recall that the L-function of χ is defined as

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Its values at integers have the following neat formula.

Theorem 1

For $n \geq 1$

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

Theorem 2

- $B_{0,\chi} = 0.$
- $B_{n,\chi} \neq 0$ *if* $n \equiv \delta_\chi \pmod{2}.$
- $B_{n,\chi} = 0$ *if* $n \not\equiv \delta_\chi \pmod{2}.$

Here $\delta_\chi = 0$ *if* $\chi(-1) = 1$ *and* $\delta_\chi = 1$ *if* $\chi(-1) = -1.$

Proof of Proposition 1

We recall that $\chi = \chi_\Delta$ is the quadratic character mentioned before. Then $\delta_\chi = 0$ if $\Delta > 0$ and $\delta_\chi = 1$ if $\Delta < 0$. Since $F_\Delta(1) = 0$, we consider the first derivative.

$$F'_\Delta(1) = \sum_{a=0}^{D-1} \chi(a)a = DB_{1,\chi} = \begin{cases} 0 & \text{if } \Delta > 0 \\ \neq 0 & \text{if } \Delta < 0 \end{cases}.$$

For $\Delta > 0$ we have

$$F''_\Delta(1) = \sum_{a=0}^{D-1} a(a-1)\chi(a) = \sum_{a=0}^{D-1} a^2\chi(a) = DB_{2,\chi} \neq 0.$$

This shows that

$$r_\Delta(\Phi_1) = \begin{cases} 1 & \text{if } \Delta < 0 \\ 2 & \text{if } \Delta > 0, \end{cases}$$

The case $\Delta = 3p$, p prime, $p \equiv 3 \pmod 4)$

Some numerical experiments.

- $\Delta = 3 \times 7$.

$$F_\Delta(x) = x\Phi_1(x)^2\Phi_2(x)\Phi_3(x)\Phi_7(x) \times (x^8 - 2x^7 + 2x^6 + 2x^2 - 2x + 1).$$

- $\Delta = 3 \times 11$.

$$F_\Delta(x) = x\Phi_1(x)^2\Phi_2(x)\Phi_6(x)\Phi_3(x)^2\Phi_{11}(x) \times (x^{12} - x^{10} + 2x^9 - 2x^8 + 2x^6 - 2x^4 + 2x^3 - x^2 + 1).$$

- $\Delta = 3 \times 19$.

$$F_\Delta(x) = x\Phi_1(x)^2\Phi_2(x)\Phi_3(x)\Phi_{19}(x)f_\Delta(x),$$

where $f_\Delta(x)$ is an irreducible polynomial over $\mathbb{Z}$.

The case $\Delta = 3p$, p prime, $p \equiv 3 \pmod 4$

p	$r_\Delta(\Phi_3)$	$r_\Delta(\Phi_6)$
7	1	0
11	2	1
19	1	0
23	2	1
31	1	0
43	1	0

The case $\Delta = 3p$, p prime, $p \equiv 3 \pmod 4$

p	$r_\Delta(\Phi_3)$	$r_\Delta(\Phi_6)$
7	1	0
11	2	1
19	1	0
23	2	1
31	1	0
43	1	0

Theorem

Let $\Delta = 3p$ with p prime and $p \equiv 3 \pmod 4$. Then

$$r_\Delta(\Phi_3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ 2 & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

$$r_\Delta(\Phi_6) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 3 \\ 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Generalized Fekete polynomials

It is easy to show that $r_\Delta(\Phi_p) = 1$. This leads to the following definition.

Definition

The Fekete polynomial $f_\Delta(x)$ is given by the following formula

$$f_\Delta(x) = \begin{cases} \dfrac{F_\Delta(x)}{x\Phi_1(x)^2\Phi_2(x)\Phi_3(x)^2\Phi_6(x)\Phi_p(x)} & \text{if } p \equiv 2 \pmod 3 \\ \dfrac{F_\Delta(x)}{x\Phi_1(x)^2\Phi_2(x)\Phi_3(x)\Phi_p(x)} & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

Proposition 3

$f_\Delta(x)$ is a reciprocal polynomial of even degree

$$\deg(f_\Delta) = \begin{cases} 2(p-5) & \textit{if } p \equiv 2 \pmod 3 \\ 2(p-3) & \textit{if } p \equiv 1 \pmod 3. \end{cases}$$

The case $\Delta = -3p$, $p \equiv 1 \pmod 4$

Theorem

We have
$$r_\Delta(\Phi_3) = r_\Delta(\Phi_p) = 1.$$

Definition

The Fekete polynomial $f_\Delta(x)$ is given by the following formula
$$f_\Delta(x) = \frac{-F_\Delta(x)}{x\Phi_1(x)\Phi_3(x)\Phi_p(x)}.$$

Proposition

$f_\Delta(x)$ is a reciprocal polynomial of degree $2(p-2)$.

Galois theory for generalized Fekete polynomials.

- Because f_Δ is a reciprocal polynomial of even degree, there exists a polynomial $g_\Delta \in \mathbb{Z}[x]$ such that

$$f_\Delta(x) = x^{\frac{\deg(f_\Delta)}{2}} g_\Delta(x + \frac{1}{x}).$$

- The Galois group of g_Δ acts on the set of its roots of, so it is naturally a subgroup of S_{h_Δ} where $h_\Delta = \deg(g_\Delta)$.
- The Galois group of f_Δ fits into the following exact sequence

$$1 \to \mathrm{Gal}(\mathbb{Q}(f_\Delta)/\mathbb{Q}(g_\Delta)) \to \mathrm{Gal}(\mathbb{Q}(f_\Delta)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(g_\Delta)/\mathbb{Q}) \to 1.$$

By definition, $\mathrm{Gal}(\mathbb{Q}(f_\Delta)/\mathbb{Q}(g_\Delta))$ is naturally a subgroup of $(\mathbb{Z}/2)^{h_\Delta}$. Therefore, Galois group $\mathrm{Gal}(\mathbb{Q}(f_\Delta)/\mathbb{Q}(g_\Delta))$ is a subgroup of the semi-direct product $(\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta}$. Note that $(\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta}$ is also naturally a subgroup of S_{2h_Δ}.

Galois theory for generalized Fekete polynomials.

In the case $|\Delta| = p$, we showed in a previous work that

Theorem 4

For $p \leq 1000$, the Galois group of f_Δ is $(\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta}$. Additionally, the Galois group of g_Δ is S_{h_Δ}. Here $h_\Delta = \deg(g_\Delta)$.

In other words, when $|\Delta|$ is a prime, the Galois group of f_Δ and g_Δ are both as large as possible.

Corollary

For $p < 1000$, f_Δ and g_Δ are irreducible.

A cretirion for $\mathrm{Gal}(g_\Delta)$ being maximal

Proposition

Let $g(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Assume that there exists a triple of prime numbers (q_1, q_2, q_3) such that

1. $g(x)$ is irreducible in $\mathbb{F}_{q_1}[x]$.
2. $g(x)$ has the following factorization in $\mathbb{F}_{q_2}[x]$
$$g(x) = (x+c)h(x),$$
where $c \in \mathbb{F}_{q_2}$ and $h(x)$ is an irred. poly. of degree $n-1$.
3. $g(x)$ has the following factorization in $\mathbb{F}_{q_3}[x]$
$$g(x) = m_1(x)m_2(x),$$
where $m_1(x)$ is an irreducible polynomial of degree 2 and $m_2(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of g is S_n.

A cretirion for $\mathrm{Gal}(f_\Delta)$ being maximal

Theorem 5 (Davis, Duke, Sun)

Let $f(x) \in \mathbb{Z}[x]$ be a monic reciprocal polynomial of even degree $2n$. Assume that there exists a quadruple of prime numbers (q_1, q_2, q_3, q_4) s.t.

1. *$f(x)$ is irreducible in $\mathbb{F}_{q_1}[x]$.*
2. *In $\mathbb{F}_{q_2}[x]$: $f(x) = (x + c_1)(x + c_2)h(x)$, where c_1, c_2 are distinct elements in $\mathbb{F}_{q_2}$ and $h(x)$ is an irred. poly. of degree $2n - 2$.*
3. *In $\mathbb{F}_{q_3}[x]$ $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ is a irred. poly. of degree 2 and $m_2(x)$ is a product of distinct irreducible polynomials of odd degrees.*
4. *In $\mathbb{F}_{q_4}[x]$ $f(x) = p_1(x)p_2(x)$, where $p_1(x)$ is an irred. poly. of degree 4 and $p_2(x)$ is a product of distinct irreducible polynomials of odd degrees.*

Then the Galois group of $\mathbb{Q}(f)/\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$

Exceptional symmetry

We applied the above criteria for $\Delta \in \{-4p, 4p, -3p, 3p\}$ (for $p \leq 500$). It worked in most cases except the case $\Delta = -3p$ where $p \equiv 5 \pmod 8$. In this case, $\mathrm{Gal}(f_\Delta)$ is a proper subgroup of $(\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta}$ and $\mathrm{Gal}(g_\Delta)$ is still S_{h_Δ}. It turns out that in this case, there is an hidden/exceptional symmetry.

Theorem 6

Let $\Delta = -3p$ then $\mathrm{disc}(f_\Delta)$ is a perfect square if and only if $p \equiv 5 \pmod 8$.

Lemma

$$\begin{tikzcd}
(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n \arrow[r, hook] \arrow[dr, "\Sigma"] & S_{2n} \arrow[d, "\mathrm{sgn}"] \\
& \mathbb{Z}/2
\end{tikzcd}$$

Here sgn is the signature map and Σ is the following map

$$\Sigma(a_1, a_2, \ldots, a_{h_\Delta}, \sigma) = \sum_{i=1}^{n} a_i.$$

Corollary

Suppose that $\mathrm{disc}(f_\Delta)$ is a perfect square. Then $\mathrm{Gal}(f_\Delta)$ is contained in the kernel of

$$\Sigma : (\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta} \to \mathbb{Z}/2.$$

Note further that $\ker \Sigma \simeq \ker(\Sigma') \rtimes S_{h_\Delta}$, where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^{h_\Delta} \to \mathbb{Z}/2.$$

Lemma

$$\begin{tikzcd} (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n \arrow[r, hook] \arrow[dr, "\Sigma"] & S_{2n} \arrow[d, "\mathrm{sgn}"] \\ & \mathbb{Z}/2 \end{tikzcd}$$

Here sgn is the signature map and Σ is the following map

$$\Sigma(a_1, a_2, \ldots, a_{h_\Delta}, \sigma) = \sum_{i=1}^{n} a_i.$$

Corollary

Suppose that $\mathrm{disc}(f_\Delta)$ is a perfect square. Then $\mathrm{Gal}(f_\Delta)$ is contained in the kernel of

$$\Sigma : (\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta} \to \mathbb{Z}/2.$$

Note further that $\ker \Sigma \simeq \ker(\Sigma') \rtimes S_{h_\Delta}$, where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^{h_\Delta} \to \mathbb{Z}/2.$$

Remark

A quite interesting consequence of the above corollary is that, when $\text{dics}(f)$ is a perfect square, even though f_Δ is expected to be irreducible over $\mathbb{Z}$, it is reducible over $\mathbb{F}_q$ for all prime q. In fact, if f_Δ is irreducible modulo q then the Galois group of f_Δ must contain a $2h_\Delta$-cycle. Since an $2h_\Delta$-cycle is an odd permutation, this contradicts that fact that all elements of the Galois group of f_Δ are even.

Lemma

Let H be a subgroup of $(\mathbb{Z}/2)^n \rtimes S_n \subset S_{2n}$ such that

1. The natural projection map $H \to S_n$ is surjective.
2. H contains a product of a 2-cycle and another 4-cycle (these two cycles are disjoint).

Then H contains $\ker(\Sigma') \rtimes S_n$ where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^n \to \mathbb{Z}/2.$$

A criterion

Proposition

Let $f(x)$ be a monic reciprocal polynomial with integer coefficients of even degree $2n$. Let g be the trace polynomial of f. Assume that

1. The discriminant of f is a perfect square.
2. The Galois group of g is S_n.
3. There exists a prime number q such that $f(x)$ has the following factorization in $\mathbb{F}_q(x)$

   $$f(x) = p_2(x)p_4(x)h(x),$$

   where $p_2(x)$ is an irreducible polynomial of degree 2, $p_4(x)$ is an irreducible polynomial of degree 4, and $h(x)$ is a product of distinct irreducible polynomials of odd degrees.

Then the Galois group of f is $\ker(\Sigma') \rtimes S_n$.

Example: $\Delta = 4 \times 19$

- In this case

$$f_\Delta(x) = x^{16} + x^{15} + 2x^{14} + 3x^{12} - x^{11} + 2x^{10} + 3x^8 \\ +2x^6 - x^5 + 3x^4 + 2x^2 + x + 1.$$

- $\mathrm{disc}(f_\Delta)$ is a perfect square.
- $\mathrm{Gal}(f_\Delta)$ is a subgroup of the semi-direct product $\ker(\Sigma') \rtimes S_8$.
- The Galois group of g_Δ is S_8.
- Furthermore, at $q = 227$, the factorization of f_Δ is

$$(x^2 + 153x + 1)(x^4 + 177x^3 + 43x^2 + 177x + 1)\times \\ (x^5 + 44x^4 + 148x^3 + 23x^2 + 196x + 207)\times \\ (x^5 + 81x^4 + 101x^3 + 38x^2 + 134x + 34).$$

- Therefore, $\mathrm{Gal}(f_\Delta) = \ker(\Sigma') \rtimes S_8$.

A better criterion to dectect when $\mathrm{Gal}(f_\Delta)$ is maximal

Lemma

Let H be a subgroup of $(\mathbb{Z}/2)^n \rtimes S_n \subset S_{2n}$ such that

1. The natural projection map $H \to S_n$ is surjective,
2. H contains a 2-cycle.

Then $H = (\mathbb{Z}/2)^n \rtimes S_n$.

Theorem 7

Let $f(x) \in \mathbb{Z}[x]$ be a monic reciprocal polynomial of even degree $2n$. Let g be the trace polynomial of f. Assume that

1. *The Galois group of g is S_n.*
2. *$\exists q$ prime s.t. in $\mathbb{F}_q[x]$: $f(x) = p_2(x)h(x)$, where $p_2(x)$ is an irred. poly. of degree 2, and $h(x)$ is a product of distinct irreducible polynomials of odd degrees.*

Then the Galois group of f is $(\mathbb{Z}/2)^n \rtimes S_n$.

From experimental data, it seems reasonable to make the following prediction.

Conjecture

Let $\Delta \in \{4p, -4p, 3p, -3p\}$ and h_Δ be the degree of g_Δ. Then

1. If $\mathrm{disc}(f_\Delta)$ is not a perfect square then the Galois group of f_Δ is equal to $(\mathbb{Z}/2\mathbb{Z})^{h_\Delta} \rtimes S_{h_\Delta}$.
2. If $\mathrm{disc}(f_\Delta)$ is a perfect square then the Galois group of f_Δ is equal to $\ker(\Sigma') \rtimes S_{h_\Delta}$ where Σ' is the summation map

$$\Sigma' : (\mathbb{Z}/2)^{h_\Delta} \to \mathbb{Z}/2.$$

This conjecture has been verified for $p \leq 1000$.

Generalized Paley graphs

Let $\chi = \chi_\Delta$ be the quadratic character associated with Δ.

Definition 8

The Paley graph P_Δ is the graph with the following data

1. The vertices of P_Δ are $\{0, 1, \ldots, D-1\}$.
2. Two vertices (u, v) are connected iff $\chi_\Delta(v-u) = 1$.

Because the connection in P_Δ is determined by $(v-u) \mod D$, P_Δ is a circulant graph with respect to the cyclic group $\mathbb{Z}/D$. In fact, its adjacency matrix is generated by the following vector

$$v = \left[\frac{1}{2}\chi(a)(\chi(a)+1)\right]_{0 \le a \le D-1}.$$

Corollary

The degree of P_Δ is $\frac{\varphi(D)}{2}$.

Generalized Paley graphs

By the Circulant Diagonalization Theorem, the spectrum of P_Δ is given by

$$\left\{\lambda(\omega) := \frac{1}{2}\sum_{a=0}^{D-1}\chi(a)(1+\chi(a))\omega^a\right\}$$
$$= \left\{\lambda(\omega) := \frac{1}{2}\sum_{a=0}^{D-1}\chi(a)\omega^a + \frac{1}{2}\sum_{a=0}^{D-1}\chi(a)^2\omega^a\right\}$$

where ω runs over the set of all D-roots of unity.

Let us write $[a]_b$ for the multiset $\{\underbrace{a, \ldots, a}_{b \text{ times}}\}$. Then by the theory of Gauss sums, we have.

Theorem 9

The spectrum of the Paley graph P_Δ is the union of the following multisets

$$\left[\frac{1}{2}\frac{\varphi(D)}{\varphi(d)}\mu(d)\right]_{\varphi(d)} \quad \textit{for } d|D \quad \textit{and } d < D,$$

and

$$\left[\frac{1}{2}(\sqrt{\Delta} + \mu(D))\right]_{\frac{\varphi(D)}{2}}, \left[\frac{1}{2}(-\sqrt{\Delta} + \mu(D))\right]_{\frac{\varphi(D)}{2}}.$$

Generalized Paley graphs

Definition

Let G be a connected r-regular graph with N vertices, and let $r = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ be the eigenvalues of the adjacency matrix of G. Since G is connected and r-regular, its eigenvalues satisfy $|\lambda_i| \leq r, 1 \leq i \leq N$. Let

$$\lambda(G) = \max_{|\lambda_i| < r} |\lambda_i|.$$

The graph G is a *Ramanujan graph* if

$$\lambda(G) \leq 2\sqrt{r-1}.$$

Theorem 10

The graph P_Δ is a Ramanujan graph if and only if

1. $D = 4p$, *where p is a prime number,* $p \equiv 3 \pmod 4$,
2. *or* $D = 8p$, *where p is an odd prime number ($p = 1$ counts),*
3. *or* $D = 4p_1p_2$ *where p_1 and p_2 are distinct primes,* $p_1p_2 \equiv 3 \pmod 4$, $p_1 < p_2$, *and*
$$\frac{p_2 - 1}{p_1 - 1} + \frac{4}{(p_1 - 1)(p_2 - 1)} \leq 4.$$
4. *or* $D = 8p_1p_2$ *where p_1 and p_2 are distinct primes,* $2 < p_1 < p_2$, *and*
$$\frac{p_2 - 1}{p_1 - 1} + \frac{1}{(p_1 - 1)(p_2 - 1)} \leq 2.$$
5. *or D is a prime number p with* $p \equiv 1 \pmod 4$,
6. *or* $D = p_1p_2$ *where p_1 and p_2 are distinct primes,* $p_1p_2 \equiv 1 \pmod 4$, $p_1 < p_2$, *and*
$$\frac{p_2 - 1}{p_1 - 1} + \frac{16}{(p_1 - 1)(p_2 - 1)} \leq 8.$$

Thank you