February Fourier talks, 2011

Zeros of some self-reciprocal polynomials

D. Joyner, USNA

FFT 2011 at the
Norbert Wiener Center, UMCP

February 15, 2011

Outline

Outline

Outline

Outline

Outline

Outline

Introduction

This talk is about zeros of a certain family of "symmetric" polynomials which arise naturally in several areas of mathematics -

- coding theory,
- algebraic curves over finite fields,
- knot theory,
- cryptography (pseudo-random number generators),

to name a few.

Introduction

Let p be a polynomial

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n \qquad a_i \in \mathbb{C},$$

and let p^* denote the *reciprocal polynomial* or *reverse polynomial*

$$p^*(z) = a_n + a_{n-1} z + \cdots + a_0 z^n = z^n p(1/z).$$

We say p is *self-reciprocal* if $p = p^*$, i.e., if its coefficients are "symmetric."

Outline

Alexander polynomial of a knot

A *knot* is an embedding of S^1 into $\mathbb{R}^3$. If K is a knot then the *Alexander polynomial* is a polynomial $\Delta_K(t) \in \mathbb{Z}[t, t^{-1}]$ which is a toplological invariant of the knot. One of the key properties is the the fact that

$$\Delta_K(t^{-1}) = \Delta_K(t).$$

If

$$\Delta_K(t) = \sum_{-d}^{d} a_i t^i,$$

then the polynomial $p(t) = t^d \Delta_K(t)$ is a self-reciprocal polynomial in $\mathbb{Z}[t]$.

Outline

Algebraic curves over a finite field

Let X be a smooth projective curve of genus g over a finite field $GF(q)$.

The (Artin-Weil) zeta function of X is a rational function of the form

$$\zeta(z) = \zeta_X(z) = \frac{P(z)}{(1-z)(1-qz)},$$

where $P = P_X$ is a polynomial (sometimes called the *zeta polynomial*) of degree $2g$.

The Riemann hypothesis (RH) for curves over finite fields states that the roots of P have absolute value $1/\sqrt{q}$.

It is well-known that the RH holds for ζ_X.

Artin-Weil zeta polynomial

Example

The smooth projective curve X defined by

$$y^2 = x^5 - x,$$

over $GF(31)$ is a curve of genus 2. The zeta polynomial

$$P_X(z) = 961z^4 + 62z^2 + 1$$

associated to X satisfies the RH. The polynomial $p(z) = P_X(z/\sqrt{31})$ is self-reciprocal, having all its zeros on S^1.

Artin-Weil zeta polynomial

The "functional equation" is

$$P(z) = q^g z^{2g} P(\frac{1}{qz}).$$

"Normalize" this polynomial by replacing z by $z/\sqrt{q}$.

By the RH, we see that curves over finite fields give rise to a large class of self-reciprocal polynomials having roots on the unit circle.

Outline

Error-correcting codes

Let $\mathbb{F} = GF(q)$ denote a finite field, for some prime power q. Fix once and for all a basis for the vector space $V = \mathbb{F}^n$.

If $\mathbb{F} = GF(2)$ then C is called a *binary* code.

The elements of C are called the *codewords*.

Define the *dual code* $C^\perp$ by

$$C^\perp = \{v \in V \mid v \cdot c = 0,\ \forall c \in C\}.$$

We say C is *self-dual* if $C = C^\perp$.

For each vector $v \in V$, let

$$\mathrm{Supp}(v) = \{i \mid v_i \neq 0\}$$

denote the *support* of the vector.

The *weight* of the vector v is $\mathrm{wt}(v) = |\mathrm{Supp}(v)|$.

The *weight distribution vector* or *spectrum* of a code $C \subset \mathbb{F}^n$ is the vector

$$A(C) = \mathrm{spec}(C) = [A_0, A_1, ..., A_n]$$

where $A_i = A_i(C)$ denote the number of codewords in C of weight i, for $0 \leq i \leq n$.

Error-correcting codes

The *weight enumerator polynomial* A_C is defined by

$$A_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = x^n + A_d x^{n-d} y^d + \cdots + A_n y^n.$$

Denote the smallest non-zero weight of any codeword in C by

$$d = d_C$$

(this is the *minimum distance* of C) and the smallest non-zero weight of any codeword in $C^\perp$ by

$$d^\perp = d_{C^\perp}.$$

The number n is called the *length* of C.

Duursma zeta polynomial

A polynomial $P = P_C$ for which

$$\frac{(xT + (1-T)y)^n}{(1-T)(1-qT)} P(T) = \cdots + \frac{A_C(x,y) - x^n}{q-1} T^{n-d} + \ldots .$$

is called a *Duursma zeta polynomial of* C.

The *Duursma zeta function* is defined in terms of the zeta polynomial by

$$\zeta_C(T) = \frac{P(T)}{(1-T)(1-qT)},$$

Duursma zeta polynomial

Proposition

The Duursma zeta polynomial $P = P_C$ exists and is unique, provided $d^\perp \geq 2$, of degree $n + 2 - d - d^\perp$.

If C is self-dual (i.e., $C = C^\perp$), the Duursma zeta polynomial satisfies a functional equation of the form

$$P(T) = q^g T^{2g} P(\frac{1}{qT}),$$

where $g = n + 1 - k - d$.

Therefore, after making a suitable change-of-variable (namely, replacing T by $T/\sqrt{q}$), these polynomials are self-reciprocal.

Duursma zeta polynomial

In general, the analog of the Riemann hypothesis for curves does *not* hold for the Duursma zeta polynomials of self-dual codes.

Example

The Duursma zeta polynomial

$$P_C(T) = (2T^2 + 2T + 1)/5$$

associated to "the" binary self-dual code C of length 8 satisfies the analog of the RH. (Therefore, the "normalized" polynomial $p(z) = P(z/\sqrt{2})$ is self-reciprocal, with all roots on S^1.)

The zeta polynomial associated to C^3 does *not* have all its roots on S^1.

Outline

Duursma zeta polynomial

There is an infinite family of Duursma zeta functions for which Duursma has conjecture that the analog of the Riemann hypothesis always holds. The linear codes used to construct these zeta functions are so-called "extremal self-dual codes."

If $F(x,y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \in \mathbb{Z}[x,y]$ is a homogeneous polynomial with $A_d \neq 0$ then we call

- n the *length* of F and
- d the *minimum distance* of F.

We say F is *virtually self-dual weight enumerator* (over $GF(q)$) if and only if F satisfies the invariance condition

$$F(x,y) = F(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}).$$

Duursma zeta polynomial

Assume F is a virtually self-dual weight enumerator.

We say F is *extremal, Type I* if $q = 2$, n is even, and $d = 2[n/8] + 2$.

We say F is *extremal, Type II* if $q = 2$, $8|n$, and $d = 4[n/24] + 8$.

We say F is *extremal, Type III* if $q = 3$, $4|n$, and $d = 3[n/12] + 3$.

We say F is *extremal, Type IV* if $q = 4$, n is even, and $d = 2[n/6] + 2$.

Duursma zeta polynomial

Let P be a Duursma zeta polynomial as above, and let

$$p(z) = a_0 + a_1 z + \cdots + a_N z^N$$

denote the normalized Duursma zeta polynomial, $p(z) = P(z/\sqrt{q})$.

Examples

Some examples of the lists of coefficients $a_0, a_1, \ldots,$ computed using Sage, are given below.

We have scaled the coefficients so that they sum to 10 and represented the rational coefficients as decimal approximations to give a feeling for their "slow growth."

Duursma zeta polynomial

- Case Type I:
  $m = 2$: [1.1309, 2.3990, 2.9403, 2.3990, 1.1309]
  $m = 3$: [0.45194, 1.2783, 2.0714, 2.3968, 2.0714, 1.2783, 0.45194]
  $m = 4$: [0.18262, 0.64565, 1.2866, 1.8489, 2.0724, 1.8489, 1.2866, 0.64565, 0.18262]

- Case Type II:
  $m = 2$: [0.43425, 0.92119, 1.3028, 1.5353, 1.6129, 1.5353, 1.3028, 0.92119, 0.43425]
  $m = 3$: [0.12659, 0.35805, 0.63295, 0.89512, 1.1052, 1.2394, 1.2854, 1.2394, 1.1052, 0.89512, 0.63295, 0.35805, 0.12659]
  $m = 4$: [0.037621, 0.13301, 0.28216, 0.46554, 0.65783, 0.83451, 0.97533, 1.0656, 1.0967, 1.0656, 0.97533, 0.83451, 0.65783, 0.46554, 0.28216, 0.13301, 0.037621]

Duursma zeta polynomial

- Case Type III:
  $m = 2$: [1.3397, 2.3205, 2.6795, 2.3205, 1.3397]
  $m = 3$: [0.58834, 1.3587, 1.9611, 2.1836, 1.9611, 1.3587, 0.58834]
  $m = 4$: [0.26170, 0.75545, 1.3085, 1.7307, 1.8874, 1.7307, 1.3085, 0.75545, 0.26170]

- Case Type IV:
  $m = 2$: [2.8571, 4.2857, 2.8571]
  $m = 3$: [1.6667, 3.3333, 3.3333, 1.6667]
  $m = 4$: [0.97902, 2.4476, 3.1469, 2.4476, 0.97902]

Hopefully it is clear that, at least in these examples, these "normalized, extremal" Duursma zeta functions have *"slowly growing" coefficients which have "increasing symmetric form."*

Characterizing self-reciprocal polynomials

Let

$$\mathbb{R}[z]_m = \{p \in \mathbb{R}[z] \mid \deg(p) \leq m\}$$

denote the real vector space of polynomials of degree m or less.

Let

$$R_m = \{p \in \mathbb{R}[z]_m \mid p = p^*\}$$

denote the subspace of self-reciprocal ones.

Characterizing self-reciprocal polynomials

Here is a typical lemma characterizing even degree self-reciprocal polynomials. Let

$$p(z) = a_0 + a_1 z + \cdots + a_{2n} z^{2n}, \qquad a_i \in \mathbb{R}.$$

Lemma

(various authors) The polynomial $p \in \mathbb{R}[z]_{2n}$ is self-reciprocal if and only if it can be written

$$p(z) = z^n \cdot (a_n + a_{n+1} \cdot (z + z^{-1}) + \cdots + a_{2n} \cdot (z^n + z^{-n})),$$

if and only if it can be written

$$p(z) = a_{2n} \cdot \prod_{k=1}^{n} (1 - \alpha_k z + z^2),$$

for some real $\alpha_k \in \mathbb{R}$.

Characterizing self-reciprocal polynomials

Example

Note

$$1 + z + z^2 + z^3 + z^4 = (1 + \phi \cdot z + z^2)(1 + \overline{\phi} \cdot z + z^2),$$

where $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$ is the "golden ratio," and $\overline{\phi} = \frac{1-\sqrt{5}}{2} = -0.618...$ is its "conjugate."

Those with all roots in S^1

There are several results concerning the set of self-reciprocal polynomials all of whose roots lie in S^1.

If $p \in R_m$ then $f(z) = z^{-m/2}p(z)$ is invariant under $z \mapsto 1/z$, so $f(e^{i\theta})$ is real-valued. Therefore, $f(e^{i\theta})$ is a cosine transform of its coefficients.

Example

One of the simplest examples of a polynomial in R_m with all it zeros in S^1 is

$$c_m(z) = 1 + z + \cdots + z^m.$$

If m is even then c_m does not have ± 1 as zeros.

Those with all roots in S^1

Many results in the theory fall into the following category.

Meta-theorem: If $p \in R_m$ is "close" to c_m then p has all its roots in the unit circle S^1.

For example, here is one:

Theorem

(Lakatos) Take the notation as in Lemma 3. The polynomial $p \in R_{2n}$ has all its roots in S^1 if and only if $-2 \leq \alpha_k \leq 2$ for all k.

Those with all roots in S^1

Here's another one:

Theorem

(Lakatos) The polynomial $p \in R_m$ given by

$$p(z) = \sum_{j=0}^{m} a_j z^j$$

has all its roots on S^1, provided the coefficients satisfy the following condition

$$|a_m| \geq \sum_{j=0}^{m} |a_j - a_m|.$$

Schur-Cohn theorem

There are several other characterizations of self-reciprocal polynomials all of whose roots lie in S^1.

Theorem

(Schur-Cohn) Let $p = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}[z]_n$. Cohn showed that p has all its zeros on S^1 if and only if

(a) there is a $\mu \in S^1$ such that, for all k with $0 \leq k \leq n$, we have $a_{n-k} = \mu \cdot \overline{a_k}$, and

(b) all the zeros of p' lie inside or on S^1.

This result of Cohn, published in 1922, is closely related to a result of Schur, published in 1918.

Schur-Cohn theorem

The following result is an immediate corollary of this theorem.

Corollary

$p \in R_m$ has all its zeros on S^1 if and only if all the zeros of p' lie inside or on S^1.

Chen-Chinen theorem

The result below provides a very large class of self-reciprocal polynomials having roots on the unit circle.

Theorem

(Chen-Chinen) If $p \in R_m$ has "decreasing symmetric form"

$$p(z) = a_0 + a_1 z + \cdots + a_k z^k + a_k z^{m-k} + a_{k-1} z^{m-k+1} + \cdots + a_0 z^m,$$

with $a_0 > a_1 > \cdots > a_k > 0$ then all roots of $p(z)$ lie on S^1, provided $m \geq k$.

It was proven by Chen and (in a slightly different form) later independently by Chinen.

Chen-Chinen theorem

We can prove the following more general version of this.

Theorem

If $g(z) = a_0 + a_1 z + \cdots + a_k z^k$ and $0 < a_0 < \cdots < a_{k-1} < a_k$ then, for each $r \geq 0$, the roots of $z^r g(z) + g^*(z)$ all lie on the unit circle.

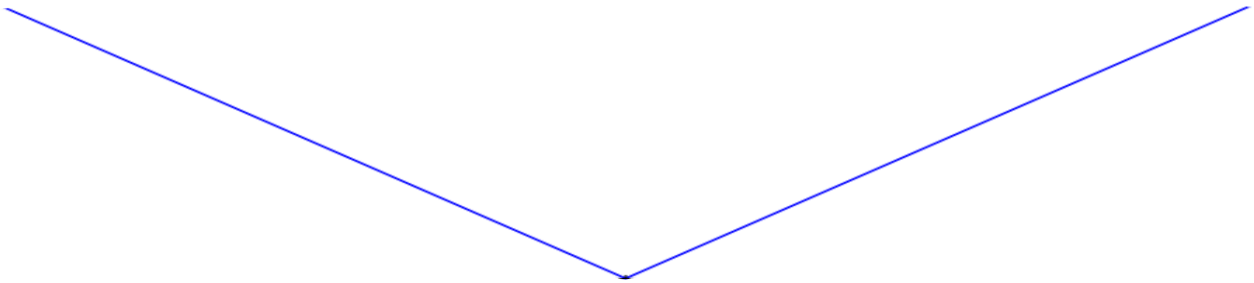

Figure: Pattern of coefficients of a polynomial of "decreasing symmetric form".

Eneström-Kakeya theorem

The easy proof uses the following well-known theorem, discovered independently by Eneström (in the late 1800's) and Kakeya (in the early 1900's).

Let

$$f(z) = a_0 + a_1 z + \cdots + a_k z^k.$$

Theorem

- If $a_0 > a_1 > \cdots > a_k > 0$ then $f(z)$ has no roots in $|z| \leq 1$.
- If $0 < a_0 < a_1 < \cdots < a_k$ then $f(z)$ has no roots in $|z| \geq 1$.

Fell's theorem

If $P_0(z)$ and $P_1(z)$ are polynomials, let

$$P_a(z) = (1-a)P_0(z) + aP_1(z),$$

for $0 \leq a \leq 1$.

Theorem

(Fell) Let $P_0(z)$ and $P_1(z)$ be real monic polynomials of degree n having zeros in $S^1 - \{1, -1\}$. Denote the zeros of $P_0(z)$ by $w_1, w_2, \ldots, w_n$ and of $P_1(z)$ by $z_1, z_2, \ldots, z_n$. Assume $w_i \neq z_j$, for $1 \leq i, j \leq n$. Assume also that

$$0 < \arg(w_i) \leq \arg(w_j) < 2\pi,$$

$$0 < \arg(z_i) \leq \arg(z_j) < 2\pi,$$

for $1 \leq i, j \leq n$. Let A_i be the smaller open arc of S^1 bounded by w_i and z_i, for $1 \leq i \leq n$. Then the locus of $P_a(z)$, $0 \leq a \leq 1$, is contained in S^1 if and only if the arcs A_i are all disjoint.

Smoothness of roots

How "smoothly" do they vary as a function of the coefficients of the polynomial?

Suppose that the coefficients a_i of the polynomial p are functions of a real parameter t.

Identify $p(z) = p(t, z)$ with a function of two variables ($t \in \mathbb{R}$, $z \in \mathbb{C}$).

Let $r = r(t)$ denote a root of this polynomial, regarded as a function of t:

$$p(t, r(t)) = 0.$$

Lemma

$r = r(t)$ is smooth (i.e., continuously differentiable) as a function of t, provided t is restricted to an interval on which $p(t, z)$ has no double roots.

Smoothness of roots

Let $p(z) = p(t, z)$ and $r = r(t)$ be as before. Consider the distance function

$$d(t) = |r(t)|$$

of the root r.

How smooth is the distance function of a root as a function of the coefficients of the polynomial p?

Lemma

$d(t) = |r(t)|$ is smooth (i.e., continuously differentiable) as a function of t, provided t is restricted to an interval one which $p(t, z)$ has no double roots and $r(t) \neq 0$.

Example

Let

$$p(z) = 1 + (1+t)\cdot z + z^2,$$

so we may take

$$r(t) = \frac{-1 - t + \sqrt{(1+t)^2 - 4}}{2}.$$

Note that $r(t)$ is smooth provided t lies in an interval which does not contain 1 or -3. We can directly verify the lemma holds in this case. Observe (for later) that if $-3 < t < 1$ then $|r(t)| = 1$.

Smoothness of roots

Example

This is a continuation of the previous Example. The Figure is a plot of $d(t)$ in the range $-5 < t < 3$.

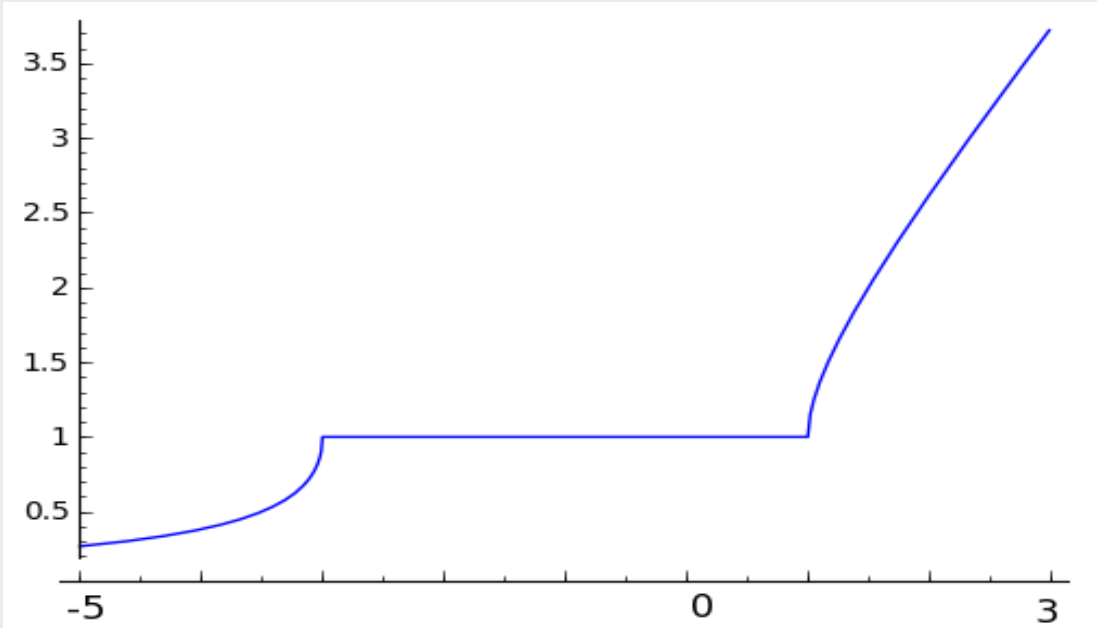

Figure: Size of largest root of the polynomial $1 + (1 + t)z + z^2$, $-5 < t < 3$.

A conjecture

We know that self-reciprocal polynomial with "decreasing symmetric form" have all their roots on S^1.

Under what conditions is the analogous statement true for functions with "increasing symmetric form?"

Are there conditions under which self-reciprocal polynomials with in "increasing symmetric form" have all their zeros on S^1?

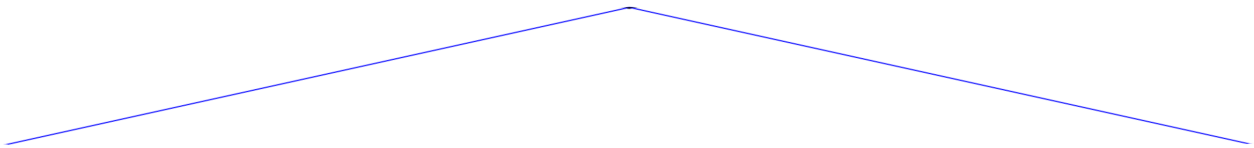

Figure: Pattern of coefficients of a polynomial of "increasing symmetric form".

A conjecture

Conjecture

Let $s : \mathbb{Z}_{>0} \to \mathbb{R}_{>0}$ be a "slowly increasing" function.

- Odd degree case. If $g(z) = a_0 + a_1 z + \cdots + a_k z^k$, where $a_i = s(i)$, then the roots of
$$p(z) = g(z) + z^{k+1} g^*(z)$$
all lie on the unit circle.
- Even degree case. The roots of
$$p(z) = a_0 + a_1 z + \cdots + a_{k-1} z^{k-1} + a_k z^k + a_{k-1} z^{k+1} + \cdots + a_1 z^{2k-1} + a_0 z^{2k}$$
all lie on the unit circle.

This is supported by some experimental data.

If $p(z)$ is as above and d denotes the degree then $f(z) = z^{-d/2}p(z)$ is a real-valued function on S^1.

The above conjecture can be reformulated as a statement about zeros of cosine transforms.

I don't know what "slowly increasing" means but it should allow for the inclusion of the Duursma polynomials!

The End

If $p(z)$ is as above and d denotes the degree then $f(z) = z^{-d/2}p(z)$ is a real-valued function on S^1.

The above conjecture can be reformulated as a statement about zeros of cosine transforms.

I don't know what "slowly increasing" means but it should allow for the inclusion of the Duursma polynomials!

The End