Zeros of some self-reciprocal polynomials

David Joyner

Department of Mathematics, US Naval Academy, Annapolis, MD. Email: wdj@usna.edu

Abstract. We say that a polynomial p of degree n is *self-reciprocal polynomial* if $p(z) = z^n p(1/z)$, i.e., if its coefficients are "symmetric." This paper surveys the literature on zeros of this family of complex polynomials, with the focus on criteria determining when such polynomials have all their roots on the unit circle. The last section contains a new conjectural criteria which, if true, would have very interesting applications.

1 Introduction

This talk is about zeros of a certain family of complex polynomials which arise naturally in several areas of mathematics, but are also of independent interest. We are especially interested in polynomials which have all their zeros in the unit circle

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Let p be a polynomial

$$p(z) = a_0 + a_1 z + \ldots + a_n z^n \qquad a_i \in \mathbb{C}, \tag{1}$$

and let p^* denote[1] the *reciprocal polynomial* or *reverse polynomial*

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

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

The types of polynomials we will be most interested in this talk are self-reciprocal polynomials. The first several sections are

[1] Some authors, such as Chen [2], have p^* denote the complex conjugate of the reverse polynomial. It will not matter for us, since we will eventually assume that the coefficients are real.

surveys. The last section contains a conjecture which is vague enough to probably be new and sufficiently general to hopefully have interesting applications, if true.

2 Where these self-reciprocal polynomials occur

Self-reciprocal polynomials occur in many areas of mathematics - coding theory, algebraic curves over finite fields , knot theory, linear feedback shift registers, to name several. This section discusses some of these.

2.1 Littlewood polynomials

This section discusses a very interesting class of polynomials named after the late British mathematician J. E. Littlewood, famous for his collaboration with G. Hardy in the early 1900's. Although the main questions about these polynomials do not involve their zeros, so this section is a bit tangential, there are some aspects related to our main theme. Basically, we present just enough to whet the readers' taste to perhaps pursue the literature further on their own.

This section recalls some relavant facts from Mercer's thesis [16].

A polynomial $p(z)$ as in (1) is a *Littlewood polynomial* if $a_i \in \{\pm 1\}$, for all i, where $a_i = a_i(p)$ is the i-th coefficient of the polynomial p. Let L_n denote the set of all Littlewood polynomials of degree n.

Conjecture 1. (Littlewood's "two-sided" conjecture) There are positive constants K_1, K_2 such that, for all $n > 1$, there exists a $p \in L_n$ such that

$$K_1\sqrt{n} \leq |p(z)| \leq K_2\sqrt{n}. \tag{2}$$

The *autocorrelations* of the sequence $\{a_i\}_{i=0}^n$ are the elements of the sequence given by

$$c_k = c_k(p) = \sum_{j=0}^{n-k} a_j a_{j+k}, \qquad 0 \le k \le n. \tag{3}$$

One can show that

$$p(z)p^*(z) = c_n + c_{n-1}z + \ldots + c_1 z^{n-1} + c_0 z^n + c_1 z^{n+1} + \ldots + c_n z^{2n}.$$

Littlewood polynomials are studied in an attempt to gain further understanding of pseudo-random sequences of ± 1's. In this connection, one is especially interested in Littlewood polynomials with "small" autocorrelations. A Littlewood polynomial having the property that $|c_k| \le 1$ is called a *Barker polynomial*. It is an open problem to find a Barker polynomial for $n > 13$ (or show one does not exist). Let

$$b(n) = \min_{p \in L_n} \max_{1 \le k \le n} |c_k(p)|,$$

where c_k is as in (3). If $b(n) > 1$ then there is no Barker polynomial of degree n. The asymptotic growth of $b(n)$, as $n \to \infty$ is an open question, although there is a conjecture of Turyn that

$$b(n) \sim K \log(n),$$

for some constant $K > 0$. It is known that $b(n) = O(\sqrt{n \log(n)})$.

The zeros of Littlewood polynomials on the unit circle are of tangential interest to this question. It is known that self-reciprocal Littlewood polynomials have at least one zero on S^1. Such a polynomial would obviously violate (2). A Littlewood polynomial p as in (1) is *skew-reciprocal* if, for all j, $a_{d+j} = (-1)^j a_{d-j}$, where $d = m/2$ (m even) or $d = (m-1)/2$ (m odd). A skew-reciprocal Littlewood polynomials has no zeros on S^1. (The Littlewood polynomials having small autocorrelations also tend to be skew-reciprocal.)

We refer to Mercer [16] for more details.

2.2 Algebraic curves over a finite field

Let X be a smooth projective curve of genus [2] g over a finite field $GF(q)$.

Example 1. The curve

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

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

Suppose X is defined by a polynomial equation $F(x, y) = 0$, where F is a polynomial with coefficients in $GF(q)$. Let N_k denote the number of solutions in $GF(q^k)$ and create the generating function

$$G(z) = N_1 z + N_2 z^2/2 + N_3 z^3/3 + \cdots .$$

Define the (Artin-Weil) zeta function of X by the formal power series

$$\zeta(z) = \zeta_X(z) = \exp(G(z)) \tag{4}$$

so $\zeta(0) = 1$. The logarithmic derivative of ζ_X is the generating function of the sequence of counting numbers $\{N_1, N_2, \ldots\}$. In particular, the logaritmic derivative of $\zeta(z)$ has integral coefficients.

It is known that ζ is a rational function of the form

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

where $P = P_X$ is a polynomial[3], of degree $2g$ where g is the genus of X. This has a "functional equation" of the form

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

[2] These terms will not be defined precisely here. Please see standard texts for a rigorous treatment.

[3] Sometimes called the reciprocal of the *Frobenius polynomial*, or the *zeta polynomial*.

The Riemann hypothesis (RH) for curves over finite fields states that the roots of P have absolute value $q^{-1/2}$. It is well-known that the RH holds for ζ_X (this is a theorem of André Weil from the 1940's). By a suitable change-of-variable (namely, replacing z by $z/\sqrt{q}$), we thus see that curves over finite fields give rise to a large class of self-reciprocal polynomials having roots on the unit circle.

Example 2. We use Sage to compute an example.

Sage

```
sage: R.<x> = PolynomialRing(GF(31))
sage: H = HyperellipticCurve(x^5 - x)
sage: time H.frobenius_polynomial()
CPU times: user 0.04 s, sys: 0.01 s, total: 0.05 s
Wall time: 0.16 s
x^4 + 62*x^2 + 961
sage: C.<z> = PolynomialRing(CC, "z")
sage: f = z^4+62*z^2+961
sage: rts = f.roots()
sage: [abs(z[0]) for z in rts]
[5.56776436283002, 5.56776436283002]
sage: RR(sqrt(31))
5.56776436283002
```

In other words, the zeta polynomial

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

associated to the hyperelliptic curve H defined by $y^2 = x^5 - x$ over $GF(31)$ satisfies the RH. The polynomial $p(z) = P_H(z/\sqrt{31})$ is self-reciprocal, having all its zeros on S^1.

It can be shown that if X_1 and X_2 are "isomorphic" curves then the corresponding zeta polynomials are equal. Therefore, these polynomials can be used to help classify curves.

2.3 Error-correcting codes

Let $\mathbb{F} = GF(q)$ denote a finite field, for some prime power q.

Definition 1. Fix once and for all a basis for the vector space $V = \mathbb{F}^n$. A subset C of $V = \mathbb{F}^n$ is called a *code of length* n. A

subspace of V is called a *linear code of length* n. If $\mathbb{F} = GF(2)$ then C is called a *binary* code. The elements of a code C are called *codewords*.

If $\cdot$ denotes the usual inner product,

$$v \cdot w = v_1 w_1 + \ldots + v_n w_n,$$

where $v = (v_1, \ldots, v_n) \in V$ and $w = (w_1, \ldots, w_n) \in V$, then we 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 $0 \leq i \leq n$. Note that for a linear code C, $A_0(C) = 1$, since any vector space contains the zero vector. The *weight enumerator polynomial* A_C is defined by

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

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

Example 3. Let $\mathbb{F} = GF(2)$ and

$$C = \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\}.$$

This is a self-dual linear binary code which is a 2-dimensional subspace of $V = GF(2)^4$.

The connection between the weight enumerator of C and that of its dual is very close, as the following well-known result shows.

Theorem 1. *(MacWilliams' identity)* If C is a linear code over $GF(q)$ then

$$A_{C^\perp}(x,y) = |C|^{-1} A_C(x + (q-1)y, x - y).$$

2.4 Duursma zeta function

Let $C \subset GF(q)^n$ be a linear error-correcting code.

Definition 2. A polynomial $P = P_C$ for which

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

is called a *Duursma zeta polynomial of* C. The *Duursma zeta function* is defined in terms of the zeta polynomial by means of

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

It can be shown that if C_1 and C_2 are "equivalent" codes then the corresponding zeta polynomials are equal. Therefore, these polynomials can be used to help classify codes.

Proposition 1. The Duursma zeta polynomial $P = P_C$ exists and is unique, provided $d^\perp \geq 2$. In that case, its degree is $n + 2 - d - d^\perp$.

This is proven, for example, in Joyner-Kim [9].

It is a consequence of the MacWilliams identity that if C is self-dual (i.e., $C = C^\perp$), then then associated 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.

Unfortunately, the analog of the Riemann hypothesis for curves does *not* hold for the Duursma zeta polynomials of self-dual codes. Some counterexamples can be found, for example, in [9].

Example 4. We use Sage to compute an example.

Sage

```
sage: MS = MatrixSpace(GF(2),4,8)
sage: G = MS([[1,1,1,1,0,0,0,0],[0,0,1,1,1,1,0,0],
              [0,0,0,0,1,1,1,1],[1,0,1,0,1,0,1,0]])
sage: C = LinearCode(G)
sage: C == C.dual_code()
True
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: C.<z> = PolynomialRing(CC, "z")
sage: f = (2*z^2+2*z+1)/5
sage: rts = f.roots()
sage: [abs(z[0]) for z in rts]
[0.707106781186548, 0.707106781186548]
sage: RR(sqrt(2))
1.41421356237310
sage: RR(1/sqrt(2))
0.707106781186548
```

In other words, the Duursma zeta polynomial

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

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

Duursma's conjecture 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."

To be more precise, we must take a more algebraic approach and replace "codes" by "weight enumerators." This tactic avoids some constraints which hold for codes and not for weight enumerators. We briefly describe how to do this. (For details, see Joyner-Kim [9], Chapter 2.) 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

$$F(x,y) = F(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}). \tag{5}$$

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 $d = 2[n/6]+2$.

If F is an extremal virtually self-dual weight enumerator then the zeta function $Z = Z_F$ can be explicitly computed. First, some notation. If F is a virtually self-dual weight enumerator of minimum distance d and $P = P_F$ is its zeta polynomial then define

$$Q(T) = \begin{cases} P(T), & \text{Type I,} \\ P(T)(1-2T+2T^2), & \text{Type II,} \\ P(T)(1+3T^2), & \text{Type III,} \\ P(T)(1+2T), & \text{Type IV.} \end{cases} \tag{6}$$

Let $(a)_m = a(a+1)\dots(a+m-1)$ denote the *rising generalized factorial* and write $Q(T) = \sum_j q_j T^j$, for some $q_j \in \mathbb{Q}$. Let

$$\gamma_1(n,d,b) = (n-d)(d-b)_{b+1} A_d/(n-b-1)_{b+2},$$

and

$$\gamma_2(n,d,b,q) = (d-b)_{b+1} \frac{A_d}{(q-1)(n-b)_{b+1}},$$

where recall A_d denoted the coefficient of $x^{n-d}y^d$ in the virtual weight enumerator $F(x,y)$.

Theorem 2. *(Duursma [6])* If F is an extremal virtually self-dual weight enumerator then the coefficients of $Q(T)$ satisfy the following conditions.

(a) If F is Type I then

$$\sum_{i=0}^{2m+2\nu} \binom{4m+2\nu}{m+i} q_i T^i = \gamma_1(n,d,2)\cdot(1+T)^m(1+2T)^m(1+2T+2T^2)^\nu,$$

where $m = d-3$, $4m+2\nu = n-4$, $b = q = 2$, $0 \le \nu \le 3$.

(b) If F is Type II then

$$\sum_{i=0}^{4m+8\nu} \binom{6m+8\nu}{m+i} q_i T^i$$
$$= \gamma_1(n,d,2)\cdot(1+T)^m(1+2T)^m(1+2T+2T^2)^m B(T)^\nu,$$

where $m = d-5$, $6m+8\nu = n-6$, $b = 4$, $q = 2$, $0 \le \nu \le 2$, and $B(T) = W_5(1+T,T)$, where $W_5(x,y) = x^8 + 14x^4y^4 + y^8$ is the weight enumerator of the Type II $[8,4,4]$ self-dual code.

(c) If F is Type III then

$$\sum_{i=0}^{2m+4\nu} \binom{4m+4\nu}{m+i} q_i T^i = \gamma_2(n,d,3,3)\cdot(1+3T+3T^2)^m B(T)^\nu,$$

where $m = d-4$, $4m+4\nu = n-4$, $b = q = 3$, $0 \le \nu \le 2$, and $B(T) = W_9(1+T,T)$, where $W_9(x,y) = x^4 + 8xy^3$ is the weight enumerator of the Type III self-dual ternary code.

(d) If F is Type VI then

$$\sum_{i=0}^{m+2\nu} \binom{3m+2\nu}{m+i} q_i T^i = \gamma_2(n,d,2,4)\cdot(1+2T)^m(1+2T+4T^2)^\nu,$$

where $m = d-3$, $3m+2\nu = n-3$, $b = 2$, $q = 4$, and $0 \le \nu \le 2$.

Although the construction of these codes is fairly technical (see [9] for an expository treatment), we can give some examples.

Example 5. Let P be a Duursma zeta polynomial as above, and let

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

denote the normalized Duursma zeta polynomial, $p(z) = P(z/\sqrt{q})$. By the functional equation for P, p is self-reciprocal. Some examples of the lists of coefficients $a_0, a_1, \ldots$, computed using Sage, are

given below. We have normalized the coefficients so that they sum to 10 and represented the rational coefficients as decimal approximations to give a feeling for their relative sizes. The notation for m below is that in (6) and Theorem 2.

- 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]
- 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 coefficients which have "increasing symmetric form." We discuss this further in §6 below.

2.5 Knots

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. For the definition, we refer, for example, to [1]. 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 $\mathbb{Z}[t]$. There is a special class of knots ("special alternating knots") which have the property that all its roots lie on the unit circle (see [17], [18]).

Kulikov [10] constructed an analogous Alexander polynomial Δ associated to a complex plane algebraic curve. Under certain technical conditions, such a Δ is a self-reciprocal polynomial in $\mathbb{Z}[t]$, all of whose roots lie on the unit circle.

Example 6. In Figure 1, we give several examples of knots. These figures can be found in several places, for example, from [20].

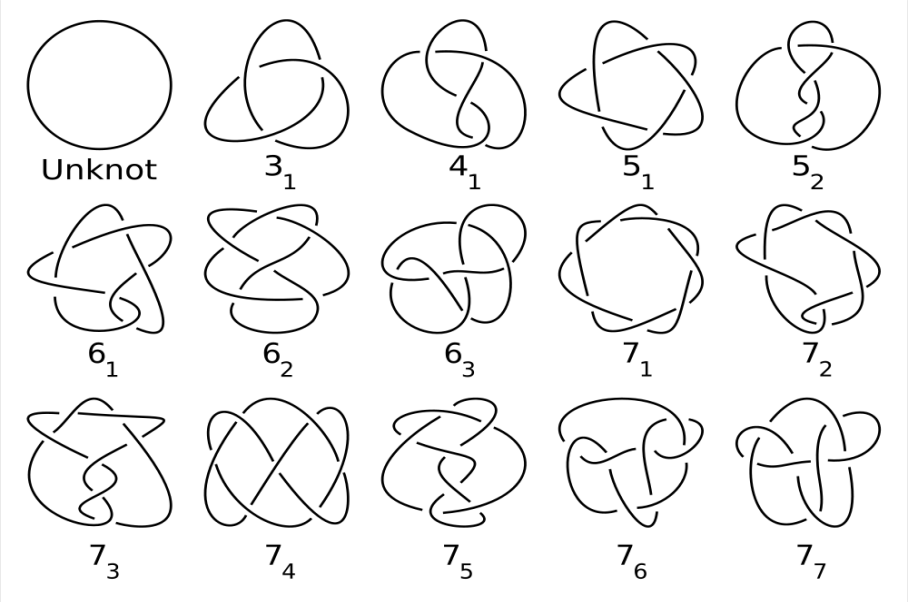

Fig. 1. Examples of knots.

The Alexander polynomial of the "unknot" is the constant function $\Delta_{S^1}(t) = 1$. The Alexander polynomials of the other knots Figure 1 are:

$$\begin{array}{cc}
\Delta_{3_1}(t) = t^{-1} - 1 + t, & \Delta_{7_1}(t) = t^{-3} - t^{-2} + t^{-1} - 1 + t - t^2 + t^3, \\
\Delta_{4_1}(t) = -t^{-1} + 3 - t, & \Delta_{7_2}(t) = 3t^{-1} - 5 + 3t, \\
\Delta_{5_1}(t) = t^{-2} - t^{-1} + 1 - t + t^2, & \Delta_{7_3}(t) = 2t^{-2} - 3t^{-1} + 3 + 3t + 2t^2, \\
\Delta_{5_2}(t) = 2t^{-1} - 3 + 2t, & \Delta_{7_4}(t) = 4t^{-1} - 7 + 4t, \\
\Delta_{6_1}(t) = -2t^{-1} + 5 - 2t, & \Delta_{7_5}(t) = t^{-2} - 4t^{-1} + 5 - 4t + 2t^2, \\
\Delta_{6_2}(t) = -t^{-2} + 3t^{-1} - 3 + 3t - t^2, & \Delta_{7_6}(t) = -t^{-2} + 5t^{-1} - 7 + 5t - t^2, \\
\Delta_{6_3}(t) = t^{-2} - 3t^{-1} + 5 - 3t + t^2, & \Delta_{7_6}(t) = t^{-2} - 5t^{-1} + 9 - 5t + t^2.
\end{array}$$

We use Sage to compute their roots in several examples.

Sage

```
sage: t = var('t')
sage: RC.<z> = PolynomialRing(CC,"z")
sage: z = RC.gen()

sage: Delta51 = (t^(-2)-t^(-1)+1-t+t^2)*t^2
sage: f = RC(expand(Delta51)(t=z))
sage: [r.abs() for r in f.complex_roots()]
[1.00000000000000, 1.00000000000000, 1.00000000000000,
 1.00000000000000]

sage: Delta63 = (t^(-2)-3*t^(-1)+5-3*t+t^2)*t^2
sage: f = RC(expand(Delta63)(t=z))
sage: [r.abs() for r in f.complex_roots()]
[0.580691831992952, 0.580691831992952, 1.72208380573904,
 1.72208380573904]

sage: Delta71 = (t^(-3)-t^(-2)+t^(-1)-1+t-t^2+t^3)*t^3
sage: f = RC(expand(Delta71)(t=z))
sage: [r.abs() for r in f.complex_roots()]
[1.00000000000000, 1.00000000000000, 1.00000000000000,
 1.00000000000000, 1.00000000000000, 1.00000000000000]

sage: Delta75 = (2*t^(-2)-4*t^(-1)+5-4*t+2*t^2)*t^2
sage: f = RC(expand(Delta75)(t=z))
sage: [r.abs() for r in f.complex_roots()]
[1.00000000000000, 1.00000000000000, 1.00000000000000,
 1.00000000000000]

sage: Delta77 = (t^(-2)-5*t^(-1)+9-5*t+t^2)*t^2
sage: f = RC(expand(Delta77)(t=z))
sage: [r.abs() for r in f.complex_roots()]
[0.422082440385454, 0.422082440385454, 2.36920540709247,
```

```
2.36920540709247]
```

2.6 Cryptography and related fields

The class of self-reciprocal polynomials also arise naturally in the field of cryptography (e.g., in the construction of "symmetric" linear feedback shift registers) and coding theory (e.g., in the construction of "symmetric" cyclic codes). However, such polynomials have coefficients in a finite field, so would take us away from our main topic. We refer the interested reader, for example, to Gulliver [8] and Massey [15].

3 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.

Here is a basic fact about even degree self-reciprocal polynomials. Let

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

Lemma 1. *([4], §2.1; see also [12])* The polynomial $p \in \mathbb{R}[z]_{2n}$ is self-reciprocal if and only if it can be written

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

if and only if it can be written

$$p(z) = a_{2n} \cdot \prod_{k=1}^{n} (1 - \alpha_k z + z^2), \tag{7}$$

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

Example 7. 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."

The *Chebyshev transformation* $T : R_{2n} \to \mathbb{R}[x]_n$ is defined on the subset[4] of polynomials of degree $2n$ by

$$T_p(x) = a_{2n} \prod_{k=1}^{n} (x - \alpha_k),$$

where $x = z + z^{-1}$, and p and the α_i's are as in (7).

The following statement is proven in Lakatos [12].

Lemma 2. The Chebyshev transformation $T : R_{2n} \to \mathbb{R}[x]_n$ is a vector space isomorphism.

For any $X_i \in \mathbb{C}$ $(1 \leq i \leq n)$, let

$$\begin{aligned}
&e_0(X_1, X_2, \ldots, X_n) = 1,\\
&e_1(X_1, X_2, \ldots, X_n) = \textstyle\sum_{1\leq j\leq n} X_j,\\
&e_2(X_1, X_2, \ldots, X_n) = \textstyle\sum_{1\leq j<k\leq n} X_j X_k,\\
&e_3(X_1, X_2, \ldots, X_n) = \textstyle\sum_{1\leq j<k<l\leq n} X_j X_k X_l,\\
&\vdots\\
&e_n(X_1, X_2, \ldots, X_n) = X_1 X_2 \cdots X_n.
\end{aligned}$$

It is possible to describe explicitly how the α_k's determine the a_j's in (7). The following result is proven in Losonczi [13].

Lemma 3. For each $n \geq 1$ and $\alpha_i \in \mathbb{C}$, we have

$$\prod_{k=1}^{n} (z^2 - \alpha_k z + 1) = \sum_{k=1}^{2n} c_{2n,k} z^k,$$

where $c_{2n,k} = c_{2n,2n-k}$ and

$$c_{2n,k} = (-1)^k \sum_{\ell=1}^{[k/2]} \binom{n-k+2\ell}{\ell} e_{k-2\ell}(\alpha_1, \ldots, \alpha_n),$$

for $0 \leq k \leq n$.

[4] In this definition, we assume for simplicity $a_{2n} \neq 0$ - see [12] for the general definition of $p \mapsto T_p$.

4 Those with all roots on S^1

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

Remark 1. Note that if $p \in R_m$ is a real self-reciprocal polynomial of degree m then $f(z) = z^{-m/2}p(z)$ is invariant under $z \mapsto z^{-1}$. Therefore, $f(z)$ is a real-valued on S^1, which implies that it is a cosine transform of its coefficients. Saying $p(z)$ has all its roots on S^1 is equivalent to saying $f(e^{i\theta})$ has n zeros on $[0, 2\pi)$.

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

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

If m is even then c_m does not have ± 1 as roots. Many results in the theory fall into the following category.

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

For example, the polynomials c_m above satisfy this.

Theorem 3. *(Lakatos [11])* Take the notation as in Lemma 1. 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.

Here's another one of those metatheorem-type results.

Theorem 4. *(Lakatos [11])* 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

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

Example 8. Let $p(z) = p(t, z) = c_2(z) + t \cdot z$. The theorem above says, in this case, $|t| \leq 1$ implies all roots of $p(z)$ belong to S^1.

There are several other characterizations of self-reciprocal polynomials all of whose roots lie on S^1. Those due to Cohn, Chinen, Chen, and Fell, are discussed next.

Theorem 5. *(Schur-Cohn[5])* Let $p \in \mathbb{C}[z]_n$ be as in (1). The polynomial 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.

According to Chen [2], this result of Cohn, published in 1922, is closely related[6] to a result of Schur, published in 1918. The following result is an immediate corollary of this theorem.

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

Remark 2.
- As a corollary to the corollary, by "version 2" of the Eneström-Kakeya Theorem (see Remark 3 below), if $p \in R_m$ is "near" c_m then the coefficients of p' are increasing and positive, so all roots of p' are inside S^1.
- For example, if $|a_i - a_{i-1}| < a_{i-1}/i$ for all i, then the corollary above and the Eneström-Kakeya Theorem imply that (all roots of p' are inside S^1 and so) $p(z)$ has all its roots on S^1. However, this rate of growth is not sufficient for application to the Duursma zeta polynomials of extremal type.

The next result was proven by Chen [2] and later independently by Chinen[7] [3]. It provides a very large class of self-reciprocal polynomials having roots on the unit circle.

[5] See for example, Chen [2], §1.
[6] In fact, both are exercises in Marden [14].
[7] In one sense, Chinen's version is slightly stonger, and it is that version which we are stating.

Theorem 6. *(Chen-Chinen)* If $p \in R_m$ has "decreasing symmetric form"

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

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

We prove the following more general version of this.

Theorem 7. If $g(z) = a_0 + a_1 z + \ldots + a_k z^k$ and $0 < a_0 < \ldots < a_{k-1} < a_k$ then, for each $r \geq 0$, the roots of $z^r g(z) + g^*(z)$ all lie on the unit circle.

proof: We shall adapt some ideas from Chinen [3] for our argument.

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

Theorem 8. *(Eneström-Kakeya, version 1)* Let $f(z) = a_0 + a_1 z + \ldots + a_k z^k$ satisfy $a_0 > a_1 > \ldots > a_k > 0$. Then $f(z)$ has no roots in $|z| \leq 1$.

Remark 3. Replacing the polynomial by its reverse, here is "version 2" of the Eneström-Kakeya Theorem: Let $f(z) = a_0 + a_1 z + \ldots + a_k z^k$ satisfy $0 < a_0 < a_1 < \ldots < a_k$. Then $f(z)$ has no roots in $|z| \geq 1$.

Back to the proof of Theorem 7.
Claim: $g^*(z)$ has no roots in $|z| \leq 1$.
proof: This is equivalent to the statement of the Eneström-Kakeya Theorem (Theorem 8). □
Claim: $g(z)$ has no roots in $|z| \geq 1$.
proof: This follows from the previous claim and the observation that the roots of $g(z)$ correspond to the inverse of the roots of $g^*(z)$. □
Claim: $|g(z)| < |g^*(z)|$ on $|z| < 1$.
proof: By the above claims, the function $\phi(z) = g(z)/g^*(z)$ is holomorphic on $|z| \leq 1$. Since $g(z^{-1}) = \overline{g(z)}$ on $|z| = 1$, we have

$|g(z)| = |g^*(z)|$ on $|z| = 1$. The claim follows from the maximum modulus principle. $\square$

Claim: The roots of $z^r g(z) + g^*(z)$ all lie on the unit circle, $r \geq 0$.

proof: By the previous claim, $z^r g(z) + g^*(z)$ has the same number of zeros as $g^*(z)$ in the unit disc $|z| < 1$ (indeed, the function $\frac{z^r g(z)+g^*(z)}{g^*(z)} = 1 + \frac{z^r g(z)}{g^*(z)}$ has no zeros). Since $g^*(z)$ has no roots in $|z| < 1$, neither does $z^r g(z) + g^*(z)$. But since $z^r g(z) + g^*(z)$ is self-reciprocal, it has no zeros in $|z| > 1$ either. $\square$

This proves Theorem 7. $\square$

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

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

for $0 \leq a \leq 1$. Next, we recall an interesting characterization of polynomials (not necessarily self-reciprocal ones) with roots on S^1, due to Fell [7].

Theorem 9. *(Fell)* Let $P_0(z)$ and $P_1(z)$ be real monic polynomials of degree n having zeros on $S^1 - \{1, -1\}$. 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 on S^1 if and only if the arcs A_i are all disjoint.

This theorem is used in the "heuristic argument" given in section 6.

5 Smoothness of roots

A natural question to ask about zeros of polynomials is how "smoothly" do they vary as a function of the coefficients of the polynomial?

To address this, suppose that the coefficients a_i of the polynomial p are functions of a real parameter t. Abusing notation slightly, 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:

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

Using the two-dimensional chain rule,

$$0 = \frac{d}{dt} p(t, r(t)) = p_t(t, r(t)) + r'(t) \cdot p_z(t, r(t)),$$

so $r'(t) = -p_t(t, r(t))/p_z(t, r(t))$. Since $p_z(t, r(t)) = p'(r)$, the denominator of this expression for $r'(t)$ is zero if and only if r is a double root of p (i.e., a root of multiplicity 2 or more).

In answer to the above question, we have proven the following result on the "smoothness of roots."

Lemma 4. $r = r(t)$ 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.

Example 9. 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 $|r(t)| = 1$.

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. Another natural question is: How smooth is the distance function of a root as a function of the coefficients of the polynomial p?

The analog to Lemma 4 holds, with one extra condition.

Lemma 5. $d(t) = |r(t)|$ 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 $r(t) \neq 0$.

proof: This is basically an immediate consequence of the above lemma and the chain rule,

$$\frac{d}{dt}|r(t)| = r'(t) \cdot \left(\frac{d|x|}{dx}|_{x=r(t)} \right).$$

□

Example 10. This is a continuation of the previous Example 9. Figure 2 is a plot of $d(t)$ in the range $-5 < t < 3$.

In the next section, we will find this "smoothness" useful.

6 A conjecture

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

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?" The remainder of this section considers this question for polynomials of even degree.

Let d be an odd integer and let $f(z) = f_0 + f_1 z + \ldots f_{d-1} z^{d-1} \in R_{d-1}$ be a self-reciprocal polynomial with "increasing symmetric form"

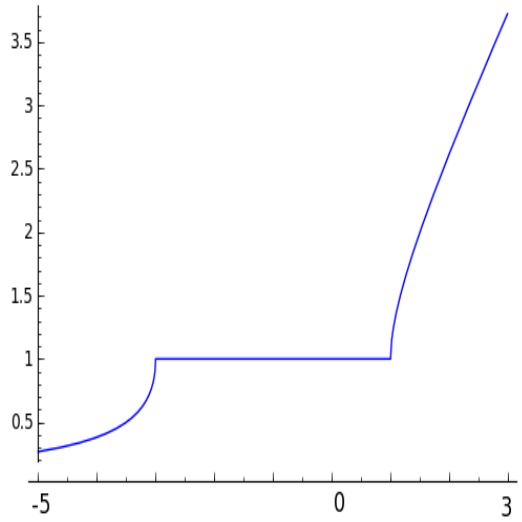

Fig. 2. Size of largest root of the polynomial $1 + (1 + t)z + z^2$, $-5 < t < 3$.
The plot was created using Sage's `list_plot` command, though the axes labels were modified using GIMP for ease of reading.

$$0 < f_0 < f_1 < \ldots < f_{\frac{d-1}{2}}.$$

For each $c \geq f_{\frac{d-1}{2}}$, the polynomial

$$g(z) = c\cdot(1+z+\ldots+z^{d-1}) - f(z) = g_0+g_1z+\ldots g_{d-1}z^{d-1} \in R_{d-1},$$

is a self-reciprocal polynomial having non-negative coefficients with "decreasing symmetric form." If $c > f_{\frac{d-1}{2}}$, the Chen-Chinen theorem (Theorem 7) implies, all the zeros of $g(z)$ are on S^1. Let

$$P_0(z) = \frac{g(z)}{g_{d-1}}, \quad P_1(z) = \frac{f(z)}{f_{d-1}}, \quad P_a(z) = (1-a)P_0(z) + aP_1(z),$$

for $0 \leq a \leq 1$. By the Chen-Chinen theorem, there is a $t_0 \in (0, 1)$ such that all zeros of $P_t(z)$ are on S^1 for $0 \leq t < t_0$. In fact, if

$$t = \frac{f_{\frac{d-1}{2}} - f_{d-1}}{f_{\frac{d-1}{2}}},$$

then $P_t(z)$ is a multiple of $1 + z + \ldots + z^{d-1}$.

Do any of the polynomials $P_t(z)$ have multiple roots ($0 < t < 1$)? Using the notation of §5, in the case $p(t, z) = P_t(z)$, we have

$$r'(t) = -p_t(t, r(t))/p_z(t, r(t)) = \frac{P_1(r(t)) - P_0(r(t))}{P_t'(r(t))}.$$

If no $P_t(z)$ has a multiple root, then by the second "smoothness of roots lemma" (Lemma 5), all the roots of $f(z)$ are also on S^1. This heuristic argument supports the hope expressed in the following statement.

Conjecture 2. Let $s : \mathbb{Z}_{>0} \to \mathbb{R}_{>0}$ be a "slowly increasing" function.

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

  $$p(z) = a_0 + a_1 z + \ldots + a_{d-1} z^{d-1} + a_d z^d + a_{d-1} z^{d+1} + \ldots + a_1 z^{2d-1} + a_0 z^{2d}$$

  all lie on the unit circle.

Remark 4.

- Though this is supported by some numerical evidence, I don't know what "slowly increasing" should be here[8]. In any case, the correct statement of this form, whatever it is, would hopefully allow for the inclusion of the extremal type Duursma polynomials!
- Note that if $p(z)$ is as above and m denotes the degree then $f(z) = z^{-m/2} p(z)$ is a real-valued function on S^1. Therefore, the above conjecture can be reformulated as a statement about zeros of cosine transforms.

Acknowledgements: I thank Mark Kidwell for discussions of knots and the references in §2.5, Geoff Price for pointing out the applications in §2.6, and George Benke for helpful suggestions.

[8] For example, numerical experiments suggest "linear growth" seems too fast but "logarithmic growth" seems sufficient.

References

1. Colin Adams, **The Knot Book: An elementary introduction to the mathematical theory of knots**, Providence, RI: American Mathematical Society, 2004.
2. W. Chen, *On the polynomials with all there zeros on the unit circle*, J. Math. Anal. and Appl. 190 (1995)714-724.
3. K. Chinen, *An abundance of invariant polynomials satisfying the Riemann hypothesis,* preprint. Available: `http://arxiv.org/abs/0704.3903`
4. S. DiPippo, E. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory 78(1998)426-450. Available: `http://arxiv.org/abs/math/9803097`
5. Iwan Duursma, *Weight distributions of geometric Goppa codes*, Transactions of the AMS, vol. 351, pp. 3609-3639, September 1999. Available: `http://www.math.uiuc.edu/~duursma/pub/`
6. ——, *Extremal weight enumerators and ultraspherical polynomials*, Discrete Mathematics, vol. 268, no. 1-3, pp. 103-127, July 2003.
7. H. J. Fell, *On the zeros of convex combinations of polynomials*, Pac. J. Math. 89 (1980)43-50.
8. T. Aaron Gulliver, *Self-reciprocal polynomials and generalized Fermat numbers*, IEEE Trans. Info. Theory 38(1992)1149-1154.
9. D. Joyner and J.-L. Kim, **Selected Unsolved Problems in Coding Theory**, to be published by Birkhäuser, 2011.
10. V. Kulikov, *Alexander polynomials of plane algebraic curves*, Russian Acad. Sci. Izv. Math. 42(1994)67-88.
11. P. Lakatos, *On polynomials having zeros on the unit circle*, C. R. Math. Acad. Sci. Soc. R. Can. 24 , (2), (2002), 9196.
12. ——, *On zeros of reciprocal polynomials*, Publ. Math. Debrecen 61, (2002), 645661.
13. L. Losonczi, *On reciprocal polynomials with zeros of modulus one* Mathematical Inequalities & Applications 9 (2006), 286-298. `http://mia.ele-math.com/09-29/`
14. M. Marden, **Geometry of Polynomials**, American Mathematical Society, 1970.
15. J. L. Massey, *Reversible codes*, Information & Control, Vol. 7, pages 369-380, Sept. 1964. Available at: `http://www.isiweb.ee.ethz.ch/archive/massey_pub/dir/pdf.html`
16. I. D. Mercer, *Autocorrelation and Flatness of Height One Polynomials,* PhD thesis, Simon Fraser University, 2005. `http://www.idmercer.com/publications.html`
17. K. Murasugi, *On alternating knots,* Osaka Math. J., 12 (1960), 227-303.
18. R. Riley, *A finiteness theorem for alternating links,* Journal of the London Mathematical Society 5(1972)263-266.
19. W. Stein and the Sage group, Sage - Mathematical Software, version 4.5, 2010. `http://www.sagemath.org/`.
20. *Knot theory*, Wikipedia `http://en.wikipedia.org/wiki/Knot_theory`