INVOLVE 2:4(2009)

Geometric properties of Shapiro–Rudin polynomials

John J. Benedetto and Jesse D. Sugar Moore

(Communicated by David Larson)

The Shapiro–Rudin polynomials are well traveled, and their relation to Golay complementary pairs is well known. Because of the importance of Golay pairs in recent applications, we spell out, in some detail, properties of Shapiro–Rudin polynomials and Golay complementary pairs. However, the theme of this paper is an apparently new elementary geometric observation concerning cusp-like behavior of certain Shapiro–Rudin polynomials.

1. Introduction

We begin by defining Shapiro–Rudin polynomials [Shapiro 1951; Rudin 1959] (see also [Tseng and Liu 1972]). $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ are the sets of natural numbers, integers, real numbers, and complex numbers, respectively.

Definition 1.1. The *Shapiro–Rudin polynomials*, P_n, Q_n, $n = 0, 1, 2, \ldots$, are defined recursively as follows. For $t \in \mathbb{R}/\mathbb{Z}$, we set $P_0(t) = Q_0(t) = 1$ and

$$P_{n+1}(t) = P_n(t) + e^{2\pi i 2^n t} Q_n(t), \quad Q_{n+1}(t) = P_n(t) - e^{2\pi i 2^n t} Q_n(t). \tag{1-1}$$

The number of terms in the n-th polynomial, P_n or Q_n, is 2^n. Thus, the sequence of coefficients of each polynomial, P_n or Q_n, is a sequence of length 2^n consisting of ± 1s.

Definition 1.2. For any sequence $z = \{z_k\}_{k=0}^{n-1} \subseteq \mathbb{C}$ and for any $m \in \{0, 1, \ldots, n-1\}$, the m-th *aperiodic autocorrelation coefficient*, $A_z(m)$, is defined as

$$A_z(m) = \sum_{j=0}^{n-1-m} z_j \overline{z_{m+j}}. \tag{1-2}$$

We now define a *Golay complementary pair* of sequences. The concept was introduced by Golay [1951; 1961; 1962], but a significant precursor is found in [Golay 1949].

MSC2000: 42A05.
Keywords: Shapiro–Rudin polynomials, Golay pairs, cusp properties.

Definition 1.3. Two sequences, $p = \{p_k\}_{k=0}^{n-1} \subseteq \mathbb{C}$ and $q = \{q_k\}_{k=0}^{n-1} \subseteq \mathbb{C}$, are a *Golay complementary pair* if $A_p(0) + A_q(0) \neq 0$ and

$$A_p(m) + A_q(m) = 0 \quad \text{for all } m = 1, 2, \ldots, n-1. \tag{1-3}$$

It is well known that the Shapiro–Rudin coefficients are Golay pairs; see Proposition 2.1. Further, Welti codes [1960] are intimately related to Golay pairs and Shapiro–Rudin polynomials. In Section 3, we begin with a useful formula for the Shapiro–Rudin polynomials, then record MATLAB code for their evaluation. Page 459 is devoted to graphs of Shapiro–Rudin polynomials; these graphs served as the basis for our geometrical observations about cusps, quantified in Section 4. In fact, in Theorem 4.8, we shall prove that the graph or trajectory of P_{2n} in $\mathbb{C}$, as a function of $t \in \mathbb{R}$, has a quadratic cusp at $t = 2\pi j$, $j \in \mathbb{Z}$. Clearly, P_{2n} is 1-periodic and infinitely differentiable as a function of $t \in \mathbb{R}$.

Remark 1.4. (a) Shapiro–Rudin polynomials have the Pythagorean and quadrature mirror filter (QMF or CMF) property:

$$|P_n(t)|^2 + |Q_n(t)|^2 = 2^{n+1} \quad \text{for all } n \geq 0 \text{ and } t \in \mathbb{R}$$

(see [Vaidyanathan 1993; Daubechies 1992; Mallat 1998]), as well as the sup-norm bound or “flatness” property,

$$\|P_n\|_{C(\mathbb{R}/\mathbb{Z})} \leq 2^{(n+1)/2} \quad \text{and} \quad \|Q_n\|_{C(\mathbb{R}/\mathbb{Z})} \leq 2^{(n+1)/2}, \tag{1-4}$$

where $\|f\|_{C(\mathbb{R}/\mathbb{Z})} = \sup_{t\in\mathbb{R}} |f(t)|$, for continuous and 1-periodic functions $f : \mathbb{R} \to \mathbb{C}$. Note that the $L^2(\mathbb{R}/\mathbb{Z})$ norms of the Shapiro–Rudin polynomials are

$$\|P_n\|_{L^2(\mathbb{R}/\mathbb{Z})} = \left(\int_0^1 |P_n(t)|^2 dt\right)^{1/2} = 2^{n/2} \quad \text{and} \quad \|Q_n\|_{L^2(\mathbb{R}/\mathbb{Z})} = 2^{n/2}.$$

The sup-norm estimates have deep analytic implications in bounding the pseudomeasure norms of important measures arising in the study of restriction algebras of the Fourier algebra of absolutely convergent Fourier series (see, for example, [Kahane 1970]). Benke's analysis and generalization of Shapiro–Rudin polynomials [Benke 1994] provide an understanding of the importance of unitarity in obtaining the low sup-norm bound in (1-4) vis a vis the exponential growth, 2^n, of P_n and Q_n. This issue is central in the Littlewood flatness problem and associated applications dealing with crest factors, $\|f\|_{C(\mathbb{R}/\mathbb{Z})}/\|f\|_{L^2(\mathbb{R}/\mathbb{Z})}$ (see, for example, [Benedetto 1997, page 238]).

(b) In classical Fourier series, Shapiro–Rudin polynomials can be used to construct continuous and 1-periodic functions $f : \mathbb{R} \to \mathbb{C}$ which are of Lipschitz order 1/2, but which do not have an absolutely convergent Fourier series [Katznelson 1976, pages 33-34].

(c) There is a large literature, several research areas, and a plethora of fiendish unresolved problems associated with Shapiro–Rudin polynomials, Golay complementary pairs, and Welti codes. For a sampling of the literature, besides [Benke 1994], we mention [Brillhart and Carlitz 1970; Brillhart 1973; Saffari 1986; 1987; Eliahou et al. 1990; 1991; Brillhart and Morton 1996; Saffari 2001; Jedwab 2005; Jedwab and Yoshida 2006]. This is truly the tip of the iceberg, even for the one-dimensional case, and the references in these articles give a hint of the breadth of the area.

(d) Besides applications to coding theory and to antenna theory, reflected by the analysis of crest factors mentioned above, Golay complementary pairs are now being used in radar waveform design [Levanon and Mozeson 2004; Howard et al. 2006; Searle and Howard 2007; Pezeshki et al. 2008], perhaps inspired by [Lüke 1985; Budišin 1990], and certainly going back to [Welti 1960].

2. Shapiro–Rudin polynomials and Golay complementary pairs

Let $\hat{P}_n = \{\hat{P}_n(k)\}_{k=0}^{2^n-1}$ denote the sequence of ± 1 coefficients of P_n, and let $\hat{Q}_n = \{\hat{Q}_n(k)\}_{k=0}^{2^n-1}$ denote the sequence of ± 1 coefficients of Q_n. Note that $k = 0$ corresponds to the first coefficient, $k = 1$ to the second, and so on.

As a result of the recursive construction of the Shapiro–Rudin polynomials, the coefficients of the $(n+1)$-st polynomials can be given in terms of the coefficients of the n-th polynomials:

$$\begin{aligned} \{\hat{P}_{n+1}(k)\}_{k=0}^{2^{n+1}-1} &= \big\{\{\hat{P}_n(k)\}_{k=0}^{2^n-1}, \{\hat{Q}_n(k)\}_{k=0}^{2^n-1}\big\}, \\ \{\hat{Q}_{n+1}(k)\}_{k=0}^{2^{n+1}-1} &= \big\{\{\hat{P}_n(k)\}_{k=0}^{2^n-1}, -\{\hat{Q}_n(k)\}_{k=0}^{2^n-1}\big\}. \end{aligned} \tag{2-1}$$

For example, we have

$$\begin{aligned} \{\hat{P}_1(k)\}_{k=0}^{1} &= \big\{\{\hat{P}_0\}, \{\hat{Q}_0\}\big\} = \{1, -1\}, \\ \{\hat{Q}_1(k)\}_{k=0}^{1} &= \big\{\{\hat{P}_0\}, -\{\hat{Q}_0\}\big\} = \{1, -1\}, \\ \{\hat{P}_2(k)\}_{k=0}^{3} &= \big\{\{\hat{P}_1(k)\}_{k=0}^{1}, \{\hat{Q}_1(k)\}_{k=0}^{1}\big\} = \{1, 1, 1, -1\}, \\ \{\hat{Q}_2(k)\}_{k=0}^{3} &= \big\{\{\hat{P}_1(k)\}_{k=0}^{1}, -\{\hat{Q}_1(k)\}_{k=0}^{1}\big\} = \{1, 1, -1, 1\}, \\ \{\hat{P}_3(k)\}_{k=0}^{7} &= \big\{\{\hat{P}_2(k)\}_{k=0}^{3}, \{\hat{Q}_2(k)\}_{k=0}^{3}\big\} = \{1, 1, 1, -1, 1, 1, -1, 1\}, \\ \{\hat{Q}_3(k)\}_{k=0}^{7} &= \big\{\{\hat{P}_2(k)\}_{k=0}^{3}, -\{\hat{Q}_2(k)\}_{k=0}^{3}\big\} = \{1, 1, 1, -1, -1, -1, 1, -1\}. \end{aligned}$$

This recursive method of constructing sequences is the *append rule* [Benke 1994]. The following result is well known.

Proposition 2.1. *For each $n \in \mathbb{N}$, the sequences $\hat{P}_n = \{\hat{P}_n(k)\}_{k=0}^{2^n-1}$ and $\hat{Q}_n = \{\hat{Q}_n(k)\}_{k=0}^{2^n-1}$ are a Golay complementary pair, i.e., $A_{\hat{P}_n}(0) + A_{\hat{Q}_n}(0) = 2^{n+1}$ and*

$$A_{\hat{P}_n}(m) + A_{\hat{Q}_n}(m) = 0 \quad \textit{for all } m = 1, 2, \cdots, 2^n - 1. \tag{2-2}$$

Proof. Since $\{\hat{P}_n(k)\}_{k=0}^{2^n-1}, \{\hat{Q}_n(k)\}_{k=0}^{2^n-1} \subseteq \mathbb{R}$, complex conjugation is ignored in the summands $A_{\hat{P}_n}(m)$ and $A_{\hat{Q}_n}(m)$.

Let $n \in \mathbb{N}$. If $m = 0$, then

$$A_{\hat{P}_n}(0) + A_{\hat{Q}_n}(0) = \sum_{j=0}^{2^n-1} \hat{P}_n(j)\hat{P}_n(j) + \sum_{j=0}^{2^n-1} \hat{Q}_n(j)\hat{Q}_n(j)$$
$$= \sum_{j=0}^{2^n-1} \big(\hat{P}_n(j)^2 + \hat{Q}_n(j)^2\big) = \sum_{j=0}^{2^n-1} 2 = 2^{n+1}.$$

For $m \neq 0$, we shall use induction. Two separate cases arise when proving the inductive step. In the first case, we consider m such that $1 \leq m \leq 2^n - 1$, and, in the second case, we consider m such that $2^n \leq m \leq 2^{n+1} - 1$. In both cases, we shall use the fact that, for any $n \in \mathbb{N}$, $\hat{P}_n(j) = \hat{Q}_n(j)$ for $j = 0, 1, \ldots, 2^{n-1} - 1$ and $\hat{P}_n(j) = -\hat{Q}_n(j)$ for $j = 2^{n-1}, \ldots, 2^n - 1$.

For $n = 1$, the only nonzero value m takes is $m = 1$. Consequently,

$$A_{\hat{P}_1}(1) + A_{\hat{Q}_1}(1) = \sum_{j=0}^{0} \hat{P}_1(0)\hat{P}_1(1) + \sum_{j=0}^{0} \hat{Q}_1(0)\hat{Q}_1(1) = 1 + (-1) = 0.$$

We now assume that (2-2) is true for some $n \in \mathbb{N}$ and for each m such that $1 \leq m \leq 2^n - 1$, and we consider the $n+1$ case.

Case 1. If $1 \leq m \leq 2^n - 1$, then

$$A_{\hat{P}_{n+1}}(m) + A_{\hat{Q}_{n+1}}(m) = \sum_{j=0}^{2^{n+1}-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\hat{Q}_{n+1}(m+j)\big)$$
$$= \sum_{j=0}^{2^n-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\hat{Q}_{n+1}(m+j)\big)$$
$$+ \sum_{j=2^n-m}^{2^n-1} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\hat{Q}_{n+1}(m+j)\big)$$
$$+ \sum_{j=2^n}^{2^{n+1}-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\hat{Q}_{n+1}(m+j)\big)$$
$$= \sum_{j=0}^{2^n-1-m} \big(\hat{P}_n(j)\hat{P}_n(m+j) + \hat{P}_n(j)\hat{P}_n(m+j)\big)$$
$$+ \sum_{j=2^n-m}^{2^n-1} \big(\hat{Q}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\big(-\hat{P}_{n+1}(m+j)\big)\big)$$
$$+ \sum_{j=2^n}^{2^{n+1}-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \big(-\hat{P}_{n+1}(j)\big)\big(-\hat{P}_{n+1}(m+j)\big)\big)$$

$$
\begin{aligned}
&= \sum_{j=0}^{2^n-1-m} 2\big(\hat{P}_n(j)\hat{P}_n(m+j)\big) + 0 + \sum_{j=0}^{2^n-1-m} 2\big(\hat{Q}_n(j)\hat{Q}_n(m+j)\big) \\
&= 2\sum_{j=0}^{2^n-1-m} \big(\hat{P}_n(j)\hat{P}_n(m+j) + \hat{Q}_n(j)\hat{Q}_n(m+j)\big) \\
&= 2\big(A_{\hat{P}_n}(m) + A_{\hat{Q}_n}(m)\big).
\end{aligned}
$$

Since $2\big(A_{\hat{P}_n}(m)+A_{\hat{Q}_n}(m)\big)=0$ for all m such that $1 \le m \le 2^n-1$ by the inductive hypothesis, we have that $A_{\hat{P}_{n+1}}(m) + A_{\hat{Q}_{n+1}}(m) = 0$ for all m such that $1 \le m \le 2^n - 1$.

Case 2. If $2^n \le m \le 2^{n+1}-1$, then

$$
\begin{aligned}
&A_{\hat{P}_{n+1}}(m) + A_{\hat{Q}_{n+1}}(m) \\
&\qquad = \sum_{j=0}^{2^{n+1}-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \hat{Q}_{n+1}(j)\hat{Q}_{n+1}(m+j)\big) \\
&\qquad = \sum_{j=0}^{2^{n+1}-1-m} \big(\hat{P}_{n+1}(j)\hat{P}_{n+1}(m+j) + \big(\hat{P}_{n+1}(j)\big)\big(-\hat{P}_{n+1}(m+j)\big)\big) = 0.
\end{aligned}
$$

This gives $A_{\hat{P}_{n+1}}(m)+A_{\hat{Q}_{n+1}}(m)=0$ for all m such that $2^n \le m \le 2^{n+1}-1$, which completes the inductive step, as well as the proof of the proposition. □

Remark 2.2. This proof remains valid if we begin with any complementary pair of sequences, $\{a_0(j)\}_{j=0}^{k-1}$ and $\{b_0(j)\}_{j=0}^{k-1}$, of length k, and we use the append rule to construct a family, $\mathscr{F}$, of pairs of sequences of length $k2^n$, viz., $\mathscr{F} = \big\langle \{a_n(j)\}_{j=0}^{k2^n-1}, \{b_n(j)\}_{j=0}^{k2^n-1} \big\rangle$ for each $n \in \mathbb{N}$. By changing 2^n to $k2^n$ and 2^{n+1} to $k2^{n+1}$ in the proof of Proposition 2.1 we find that each equilength pair of sequences in $\mathscr{F}$ is a Golay complementary pair. Thus, to show the existence of a Golay pair of sequences each of length k is to show the existence of Golay pairs of sequences of length $k2^n$ for each $n \in \mathbb{N}$.

We have proved that the coefficients of Shapiro–Rudin polynomials form Golay complementary pairs. There are many examples of pairs of sequences that are Golay complementary pairs and are not necessarily the coefficients of Shapiro–Rudin polynomials.

Example 2.3. Let $p = \{2, 3\}$ and $q = \{1, -6\}$. Then

$$A_p(0) + A_q(0) = 2^2 + 3^2 + 1^2 + (-6)^2 = 50 \ne 0$$

and $A_p(1) + A_q(1) = 2 \cdot 3 + 1 \cdot (-6) = 0$. Therefore, p and q form a Golay complementary pair, but the corresponding polynomials P and Q are not Shapiro–Rudin polynomials.

Example 2.4. Let $a, b, c, d \in \mathbb{R}$, and let at least one of a, b, c, d be nonzero. Let $ab + cd = 0$, and let $p = \{a, b, c, d\}$ and $q = \{a, b, -c, -d\}$. Then

$$\begin{aligned} A_p(0) + A_q(0) &= 2(a^2 + b^2 + c^2 + d^2) \neq 0 \quad \text{since one of } a, b, c, d \text{ is nonzero}, \\ A_p(1) + A_q(1) &= (ab + bc + cd) + (ab - bc + cd) = 2(ab + cd) = 0, \\ A_p(2) + A_q(2) &= (ac + bd) + (-ac - bd) = 0, \\ A_p(3) + A_q(3) &= (ad + (-ad)) = 0. \end{aligned}$$

Thus, p and q form a Golay complementary pair. By letting $a = b = c = 1$ and $d = -1$, we obtain the special case where $p = \{\hat{P}_2\}$ and $q = \{\hat{Q}_2\}$. Letting a be any nonzero real number and $b = c = -d = a$, we can generate Golay pairs that are not the coefficients of P_2 or Q_2.

Example 2.5. Using the append rule (2-1) and Remark 2.2, we can readily construct a nonbinary Golay complementary pair of sequences of length 2^n for any $n \in \mathbb{N}$. Starting with $p = \{2, 3\}$ and $q = \{1, -6\}$ from Example 2.3, we obtain $\tilde{p} = \{2, 3, 1, -6\}$ and $\tilde{q} = \{2, 3, -1, 6\}$ after one application of the append rule. By Example 2.4, $\tilde{p}$ and $\tilde{q}$ are a Golay complementary pair. After two applications of the append rule, we obtain

$$\tilde{\tilde{p}} = \{2, 3, 1, -6, 2, 3, -1, 6\} \quad \text{and} \quad \tilde{\tilde{q}} = \{2, 3, 1, -6, -2, -3, 1, -6\}.$$

By Remark 2.2, $\tilde{\tilde{p}}$ and $\tilde{\tilde{q}}$ are a Golay complementary pair. Repeated application of the append rule will continue to produce nonbinary Golay complementary pairs of length 2^n for any $n \in \mathbb{N}$.

Example 2.6. It is known that binary Golay complementary pairs of sequences of length $2^a 10^b 26^c$ exist for any nonnegative integers a, b, and c [Turyn 1974]. Earlier, Golay gave examples of Golay complementary sequences of length 10 and 26 [Golay 1961; 1962]. The operation used when calculating the aperiodic autocorrelation coefficients is parity of elements of the sequences (+1 if two elements match, and −1 if they do not). Golay's examples are $p = \{1, 0, 0, 1, 0, 1, 0, 0, 0, 1\}$, $q = \{1, 0, 0, 0, 0, 0, 0, 1, 1, 0\}$ for length 10 sequences, and

$$\begin{aligned} p &= \{1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0\}, \\ q &= \{0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0\} \end{aligned}$$

for length 26 sequences. Using the parity operation on these sequences, as Golay did, is equivalent to replacing the zeros in each sequence with (−1)s and using multiplication in the definition of the aperiodic autocorrelation coefficients, as in Definition 1.2.

3. A formula for Shapiro–Rudin coefficients, and some useful MATLAB code

Coefficient formula. Given an $n \in \mathbb{N}$ and k such that $0 \le k \le 2^n - 1$, the k-th coefficient of P_n is given in [Brillhart and Carlitz 1970] and [Benke 1994] by the formula $\hat{P}_n(k) = (-1)^{\langle B\omega,\omega\rangle}$, where ω is the $j \times 1$ column vector containing coefficients of the binary expansion of k, and B is the $j \times j$ shift operator matrix given by $B_{m,n} = \delta_{m,n+1}$. The expression $\langle B\omega, \omega\rangle$ is interpreted as the number of occurrences of two consecutive 1s in ω. Note that $k = 0$ corresponds to the first coefficient, $k = 1$ corresponds to the second coefficient, and so on.

MATLAB codes for Shapiro–Rudin coefficients. The following programs were coded using MATLAB v.7.0. The first program, `shapcoef.m`, is a function used in the second program, `shapvector.m`.

`shapcoef.m`

```
function matches=shapcoef(n);
    binary=dec2bin(n);
    binaryShifted=binary;
    binaryShifted(1)='0';
    for c=2:length(binary);
       binaryShifted(c)=binary(c-1);
    end;
    binary;
    binaryShifted;
    matches=0;
    for c=1:length(binary);
       if binary(c)==binaryShifted(c) && binary(c)=='1';
          matches=matches+1;
       end;
    end;
```

`shapvector.m`

```
function shapvector(a,b);
for t=a:b;
    coeff(t+1)=(-1)^shapcoef(t);
end;
B = nonzeros(coeff);
transpose(B)
```

One should use the program `shapvector` by choosing two integers a and b such that $0 \le a \le b$, and typing `shapvector(a,b)` into the MATLAB editor window. The program will return the a-th through b-th coefficients of P_n for sufficiently large values of n.

Example 3.1. To compute the coefficients of some P_n, one should use the input `shapvector(0,(2^n)-1)`. For example, the output for $n = 3$ is

```
1    1    1    -1    1    1    -1    1
```

Example 3.2. Suppose we want the coefficients of Q_3. By the append rule (2-1), they coincide with coefficients 8 through 15 of P_4, so we type `shapvector(8,15)`. The output is

```
1    1    1    -1    -1    -1    1    -1
```

Example 3.3. To find the hundredth coefficient of P_n, where $2^n \geq 100$, we type `shapvector(100,100)`. The output is -1.

The program above can be used to construct symbolic Shapiro–Rudin polynomials in MATLAB. One would simply use a for-loop with $k = 0, 1, 2, \ldots, 2^n - 1$ to construct a symbolic vector V whose k-th entry is $e^{2\pi i k t}$, then use the program to compute the vectors C_P of coefficients of P_n, and C_Q of coefficients of Q_n. The dot products $\langle C_P, V\rangle$ and $\langle C_Q, V\rangle$ are P_n and Q_n, respectively.

Parametric images. The parametric image of both P_1 and Q_1 is a circle of unit radius centered at $(1, 0)$. For the next three values of n, we illustrate on the next page the parametric images of P_n and Q_n, with the usual convention: a complex number z is represented by $(\operatorname{Re} z, \operatorname{Im} z)$. Note the complexity of some of these graphs.

4. Geometric descriptions of the curves $(\operatorname{Re} P_n, \operatorname{Im} P_n)$ and $(\operatorname{Re} Q_n, \operatorname{Im} Q_n)$

In Theorem 4.8, we shall show that, for any $n \in \mathbb{N}$, P_{2n} gives rise to a cusp at $t = 0$ while P_{2n+1} and Q_n do not give rise to cusps at $t = 0$. In fact, we shall prove that the cusp of $P_{2n} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ occurs at the point $(2^n, 0) \in \mathbb{C}$, and that it is a so-called *quadratic cusp*.

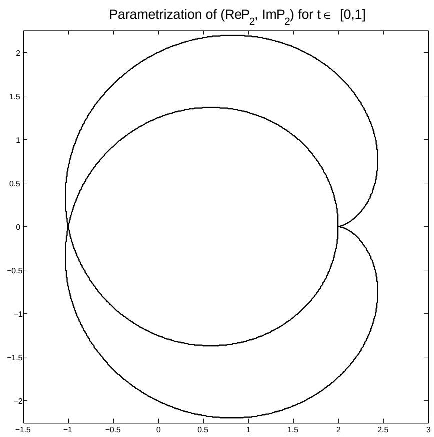
We begin by reinforcing our intuitive notion of a cusp with the following definition [Rutter 2000].

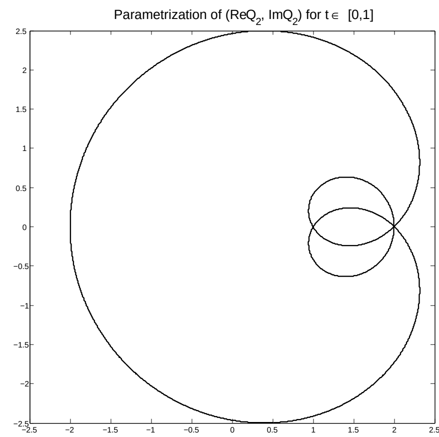
Definition 4.1. A parametrized curve $\gamma : \mathbb{R} \to \mathbb{R}^2$, defined by $\gamma(t) = (u(t), v(t))$, has a *nonregular point* at $t = t_0$ if

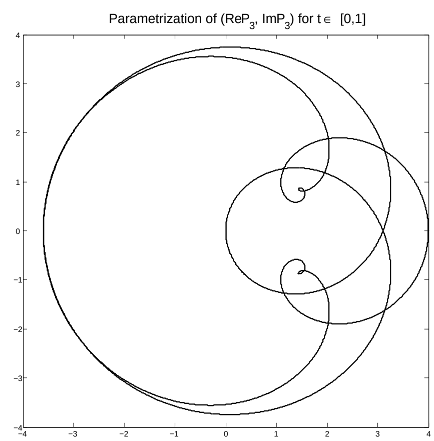
$$\frac{du}{dt}\Big|_{t=t_0} = \frac{dv}{dt}\Big|_{t=t_0} = 0.$$

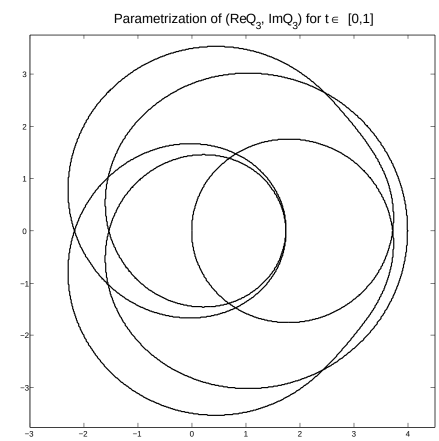
Otherwise, t_0 is a *regular point*. A nonregular point t_0 gives rise to a *quadratic cusp* for γ if

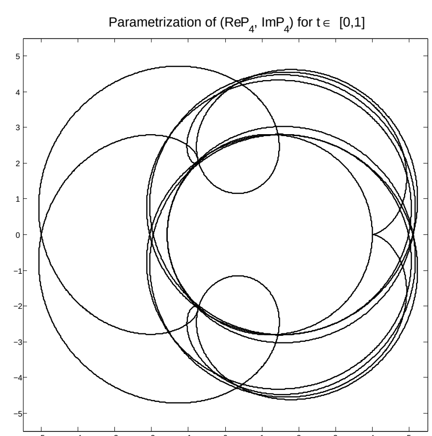
$$\Big(\frac{d^2u}{dt^2}\Big|_{t=t_0}, \frac{d^2v}{dt^2}\Big|_{t=t_0}\Big) \neq (0, 0).$$

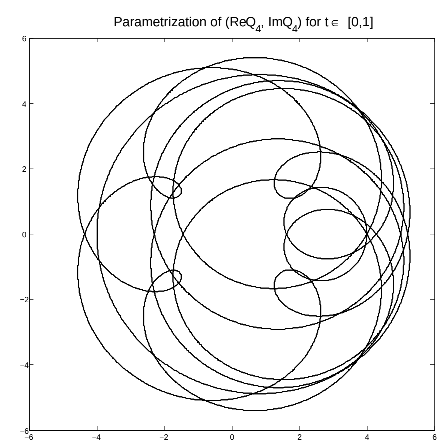

Parametrization of (ReP2, ImP2) for t ∈ [0,1]


Parametrization of (ReQ2, ImQ2) for t ∈ [0,1]


Parametrization of (ReP3, ImP3) for t ∈ [0,1]


Parametrization of (ReQ3, ImQ3) for t ∈ [0,1]


Parametrization of (ReP4, ImP4) for t ∈ [0,1]


Parametrization of (ReQ4, ImQ4) for t ∈ [0,1]

A nonregular point t_0 gives rise to an *ordinary cusp* if it gives rise to a quadratic cusp, and

$$\left(\frac{d^2u}{dt^2}\Big|_{t=t_0}, \frac{d^2v}{dt^2}\Big|_{t=t_0}\right) \quad \text{and} \quad \left(\frac{d^3u}{dt^3}\Big|_{t=t_0}, \frac{d^3v}{dt^3}\Big|_{t=t_0}\right)$$

are linearly independent points of the real vector space $\mathbb{R}^2$, that is, they are not parallel vectors in $\mathbb{R}^2$.

Example 4.2. Let $P(z) = z^2 - 2z$ on $\mathbb{C}$. Then, P' has a zero of multiplicity 1 at $z_0 = 1$. In the notation of Definition 4.1, we consider $\gamma : \mathbb{R} \to \mathbb{R}^2$, where $\gamma(t) = P(e^{2\pi i t})$, $t \in \mathbb{R}$, and so

$$u(t) = \cos(4\pi t) - 2\cos(2\pi t) \quad \text{and} \quad v(t) = \sin(4\pi t) - 2\sin(2\pi t).$$

We compute that γ has a nonregular point at $t_0 = 0$, and, in fact, $t_0 = 0$ gives rise to a quadratic cusp.

Further, if $Q : \mathbb{C} \to \mathbb{C}$ is any polynomial with complex coefficients, then $t = t_0$ gives rise to a quadratic cusp for γ, where $\gamma(t) = Q(e^{2\pi i t})$, if and only if Q' vanishes at $e^{2\pi i t_0}$ with odd multiplicity. The angle at the cusp point $z_0 = e^{2\pi i t_0}$ naturally depends on the order of the multiplicity. This assertion of odd order of multiplicity to characterize a cusp is not restricted to polynomials, but is valid for any complex valued analytic function.

Remark 4.3. To show that P_{2n} gives rise to a quadratic cusp at $t = 0$, we must first show the existence of a nonregular point at $t = 0$, and to show that P_{2n} has a nonregular point at $t = 0$, we must show

$$\frac{d}{dt}\operatorname{Re} P_{2n}\Big|_{t=0} = \frac{d}{dt}\operatorname{Im} P_{2n}\Big|_{t=0} = 0. \tag{4-1}$$

To show that P_{2n+1} and Q_n have regular points at $t = 0$, we shall verify that

$$\frac{d}{dt}\operatorname{Re} P_{2n+1}\Big|_{t=0} \neq 0 \quad \text{or} \quad \frac{d}{dt}\operatorname{Im} P_{2n+1}\Big|_{t=0} \neq 0 \tag{4-2}$$

and

$$\frac{d}{dt}\operatorname{Re} Q_n\Big|_{t=0} \neq 0 \quad \text{or} \quad \frac{d}{dt}\operatorname{Im} Q_n\Big|_{t=0} \neq 0, \tag{4-3}$$

respectively. Clearly, (4-1) is equivalent to showing $(dP_{2n}/dt)|_{t=0} = 0$, while (4-2) is equivalent to showing $(dP_{2n+1}/dt)|_{t=0} \neq 0$ and (4-3) is equivalent to showing $(dQ_n/dt)|_{t=0} \neq 0$. These calculations are contained in the proof of Theorem 4.8.

Example 4.4. We calculate the derivatives of P_n and Q_n. By writing the coefficients of P_n and Q_n as $\{\hat{P}_n(k)\}_{k=0}^{2^n-1}$ and $\{\hat{Q}_n(k)\}_{k=0}^{2^n-1}$, we have

$$P_n(t) = \sum_{k=0}^{2^n-1} \hat{P}_n(k) e^{2\pi i k t} \quad \text{and} \quad Q_n(t) = \sum_{k=0}^{2^n-1} \hat{Q}_n(k) e^{2\pi i k t}.$$

Consequently,

$$\frac{dP_n(t)}{dt} = \frac{d}{dt}\sum_{k=0}^{2^n-1} \hat{P}_n(k)e^{2\pi ikt} = 2\pi i\sum_{k=0}^{2^n-1} k\hat{P}_n(k)e^{2\pi ikt},$$

$$\frac{dQ_n(t)}{dt} = \frac{d}{dt}\sum_{k=0}^{2^n-1} \hat{Q}_n(k)e^{2\pi ikt} = 2\pi i\sum_{k=0}^{2^n-1} k\hat{Q}_n(k)e^{2\pi ikt}.$$

The following well-known formulas for the sums of coefficients of Shapiro–Rudin polynomials are used in the verification of Proposition 4.6.

Proposition 4.5. *For each $n \in \mathbb{N}$,*

$$\sum_{k=0}^{2^n-1} \hat{P}_n(k) = \begin{cases} 2^{(n+1)/2} & \textit{if } n \textit{ is odd},\\ 2^{n/2} & \textit{if } n \textit{ is even};\end{cases} \qquad \sum_{k=0}^{2^n-1} \hat{Q}_n(k) = \begin{cases} 0 & \textit{if } n \textit{ is odd},\\ 2^{n/2} & \textit{if } n \textit{ is even}.\end{cases} \tag{4-4}$$

Proof. From the append rule (2-1), we have

$$\sum_{k=0}^{2^{n+1}-1} \hat{P}_{n+1}(k) = \sum_{k=0}^{2^n-1} \hat{P}_n(k) + \sum_{k=0}^{2^n-1} \hat{Q}_n(k), \tag{4-5}$$

$$\sum_{k=0}^{2^{n+1}-1} \hat{Q}_{n+1}(k) = \sum_{k=0}^{2^n-1} \hat{P}_n(k) - \sum_{k=0}^{2^n-1} \hat{Q}_n(k). \tag{4-6}$$

We complete the proof using induction. To verify the basic cases, we observe: for $n = 1$, $\sum_{k=0}^{1} \hat{P}_1(k) = 1 + 1 = 2^1$ and $\sum_{k=0}^{1} \hat{Q}_1(k) = 1 - 1 = 0$, and for $n = 2$, $\sum_{k=0}^{3} \hat{P}_2(k) = 1+1+1-1 = 2^{(3-1)/2}$ and $\sum_{k=0}^{3} \hat{Q}_2(k) = 1+1-1+1 = 2^{(3-1)/2}$. For the inductive step, suppose (4-4) holds for some $n \in \mathbb{N}$. Then, if n is even, $\sum_{k=0}^{2^n-1} \hat{P}_n(k) = 2^{n/2}$ and $\sum_{k=0}^{2^n-1} \hat{Q}_n(k) = 2^{n/2}$. Hence,

$$\sum_{k=0}^{2^{n+1}-1} \hat{P}_{n+1}(k) = \sum_{k=0}^{2^n-1} \hat{P}_n(k) + \sum_{k=0}^{2^n-1} \hat{Q}_n(k) = 2^{n/2} + 2^{n/2} = 2^{(n/2)+1} = 2^{((n+1)+1)/2},$$

$$\sum_{k=0}^{2^{n+1}-1} \hat{Q}_{n+1}(k) = \sum_{k=0}^{2^n-1} \hat{P}_n(k) - \sum_{k=0}^{2^n-1} \hat{Q}_n(k) = 2^{n/2} - 2^{n/2} = 0,$$

completing the induction step. The verification in the case of n odd is entirely analogous. □

We define the finite sums

$$S_P(n) = \frac{1}{2\pi i}\frac{dP_n}{dt}\Big|_{t=0} = \sum_{k=0}^{2^n-1} k\hat{P}_n(k), \quad S_Q(n) = \frac{1}{2\pi i}\frac{dQ_n}{dt}\Big|_{t=0} = \sum_{k=0}^{2^n-1} k\hat{Q}_n(k).$$

Using this notation, relations (4-1)–(4-3) become, respectively,

$$S_P(2n) = 0, \tag{4-7}$$

$$S_P(2n{+}1) \neq 0, \tag{4-8}$$

$$S_Q(n) \neq 0. \tag{4-9}$$

The following result is used in the proof of Theorem 4.8.

Proposition 4.6. *For all $n \in \mathbb{N}$,*

$$\begin{aligned} S_P(n+1) &= \begin{cases} S_P(n) + S_Q(n) & \text{if } n \text{ is odd},\\ S_P(n) + (S_Q(n) + 2^{3n/2}) & \text{if } n \text{ is even}; \end{cases}\\ S_Q(n+1) &= \begin{cases} S_P(n) + S_Q(n) & \text{if } n \text{ is odd},\\ S_P(n) - (S_Q(n) + 2^{3n/2}) & \text{if } n \text{ is even}. \end{cases} \end{aligned} \tag{4-10}$$

Proof. Using (4-5), we have, for every $n \in \mathbb{N}$,

$$\begin{aligned} S_P(n+1) &= S_P(n) + \Big(S_Q(n) + 2^n \sum_{k=0}^{2^n-1} \hat{Q}_n(k)\Big)\\ &= \sum_{k=0}^{2^n-1} k\hat{P}_{n+1}(k) + \sum_{k=2^n}^{2^{n+1}-1} k\hat{P}_{n+1}(k) = \sum_{k=0}^{2^{n+1}-1} k\hat{P}_{n+1}(k)\\ &= \sum_{k=0}^{2^n-1} k\hat{P}_n(k) + \sum_{k=2^n}^{2^{n+1}-1} \big((k-2^n)+2^n\big)\hat{P}_{n+1}(k)\\ &= \sum_{k=0}^{2^n-1} k\hat{P}_n(k) + \sum_{k=2^n}^{2^{n+1}-1} (k-2^n)\hat{P}_{n+1}(k) + \sum_{k=2^n}^{2^{n+1}-1} 2^n\hat{P}_{n+1}(k)\\ &= \sum_{k=0}^{2^n-1} k\hat{P}_n(k) + \sum_{k=0}^{2^n-1} k\hat{Q}_n(k) + 2^n \sum_{k=0}^{2^n-1} \hat{Q}_n(k)\\ &= \begin{cases} S_P(n) + S_Q(n) & \text{if } n \text{ is odd},\\ S_P(n) + \big(S_Q(n) + 2^{3n/2}\big) & \text{if } n \text{ is even}. \end{cases} \end{aligned}$$

The expression for $S_Q(n+1)$ is proved analogously, starting from (4-6). □

Example 4.7. Define the finite sums

$$S_{P,2}(n) = -\frac{1}{4\pi^2}\frac{d^2P_n}{dt^2}\Big|_{t=0} = \sum_{k=0}^{2^n-1} k^2\hat{P}_n(k),$$

$$S_{Q,2}(n) = -\frac{1}{4\pi^2}\frac{d^2Q_n}{dt^2}\Big|_{t=0} = \sum_{k=0}^{2^n-1} k^2\hat{Q}_n(k).$$

In [Brillhart 1973], the following formulas relating to the second derivatives of Shapiro–Rudin polynomials are proved. These formulas will be used in Theorem 4.8 to classify the cusps of P_n and Q_n.

$$S_{P,2}(2n) = \frac{-2^{n+1}(2^n-1)(2^{2n+2}-1)}{45}, \tag{4-11}$$

$$S_{P,2}(2n+1) = \frac{2^{n+2}(2^{2n}-1)(2^{2n+2}-1)}{9}, \tag{4-12}$$

$$S_{Q,2}(2n) = \frac{2^{n+1}(2^{2n}-1)(13\cdot 2^{2n-1}-11)}{45}, \tag{4-13}$$

$$S_{Q,2}(2n+1) = \frac{-2^{n+3}(2^{2n}-1)(2^{2n+2}-1)}{15}. \tag{4-14}$$

We shall now prove that P_{2n} gives rise to a quadratic cusp at $t=0$. We shall also prove that this cusp occurs at the point $(2^n, 0)$. Lastly, we shall prove that P_{2n+1} and Q_n do not give rise to cusps at $t=0$ as a result of the fact that $t=0$ is a regular point of each of these curves.

Theorem 4.8. *For each $n \in \mathbb{N}$, the parametrization* $(\operatorname{Re} P_{2n}, \operatorname{Im} P_{2n})$ *gives rise to a quadratic cusp at* $(2^n, 0)$, *that is*, *when $t=0$*, *and neither* $(\operatorname{Re} P_{2n+1}, \operatorname{Im} P_{2n+1})$ *nor* $(\operatorname{Re} Q_n, \operatorname{Im} Q_n)$ *gives rise to a cusp when $t=0$.*

Proof. (i) We notice that $P_{2n}(0) = \sum_{k=0}^{2^{2n}-1} \hat{P}_{2n}(k) = 2^{2n/2} = 2^n$ by (4-4). This implies that $\operatorname{Re} P_{2n}(0) = 2^n$ and $\operatorname{Im} P_n(0) = 0$. Thus, at $t=0$, $(\operatorname{Re} P_{2n}, \operatorname{Im} P_{2n}) = (2^n, 0)$. It is clear that none of (4-11), (4-12), (4-13), or (4-14) can ever equal zero, and, hence, none of the second derivatives can equal zero. This proves that $t=0$ is at least a quadratic cusp of the parametrization $(\operatorname{Re} P_{2n}, \operatorname{Im} P_{2n})$, provided $t=0$ is, in fact, a nonregular point of the curve.

To prove that $t=0$ is a nonregular point of P_{2n}, it suffices to prove (4-7). We shall also prove (4-8) and (4-9), which will, in turn, prove that $t=0$ is a regular point of P_{2n+1} and Q_n.

(ii) Using induction, we shall prove (4-7), (4-8), and (4-9) by showing that, for each $n \in \mathbb{N}$,

$$S_P(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ \frac{4}{3}(2^{3(n-1)/2} - 2^{(n-1)/2}) + 2^{(n-1)/2} & \text{if } n \text{ is odd} \end{cases} \tag{4-15}$$

and

$$S_Q(n) = \begin{cases} \frac{1}{3}(2^{3n/2} - 2^{n/2}) & \text{if } n \text{ is even,} \\ -S_P(n) = -\frac{4}{3}(2^{3(n-1)/2} - 2^{(n-1)/2}) - 2^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases} \tag{4-16}$$

We start with $n=1$, where $S_P(1) = 0+1 = 1 = \frac{4}{3}(2^0-1)(2^0)+2^0$ and $S_Q(1) = 0-1 = -1 = -\frac{4}{3}(2^0-1)(2^0)-2^0$, and with $n=2$, we have $S_P(2) = 0+1+2-3 = 0$ and $S_Q(2) = \frac{1}{3}(2^2-1)(2^{2/2}) = 2$.

To prove the inductive step, assume (4-15) and (4-16) hold for some $n \in \mathbb{N}$. Assume first that the case where n is even, n is even, so $n+1$ is odd. By (4-10) we have

$$\begin{aligned} S_P(n{+}1) &= S_P(n) + S_Q(n) + 2^{3n/2} = 0 + \tfrac{1}{3}(2^{3n/2}) - \tfrac{1}{3}(2^{n/2}) + 2^{3n/2} \\ &= \tfrac{4}{3}(2^{3n/2}) - \tfrac{1}{3}(2^{n/2}) = \tfrac{4}{3}(2^{3n/2}) - \tfrac{4}{3}(2^{n/2}) + 2^{n/2} = \tfrac{4}{3}(2^{3n/2} - 2^{n/2}) + 2^{n/2}, \\ S_Q(n{+}1) &= S_P(n) - S_Q(n) - 2^{3n/2} = -\tfrac{1}{3}(2^{3n/2}) + \tfrac{1}{3}(2^{n/2}) - 2^{3n/2}, \\ &= -\tfrac{4}{3}(2^{3n/2}) + \tfrac{4}{3}(2^{n/2}) - 2^{n/2} = -\tfrac{4}{3}(2^{3n/2} - 2^{n/2}) - 2^{n/2}, \end{aligned}$$

completing the induction step in this case. The complementary case is proved similarly. □

Appendix

The cusps arising in P_{2n} can be explicitly studied using only elementary calculations. Although such calculations are not very illuminating, they illustrate the difficulty of discovering and verifying the assertion of Theorem 4.8 by a direct approach, as opposed to the way we have proceeded. In this appendix we spell out the details of the special case $P_2(t)$.

We have

$$\begin{aligned} P_2(t) &= P_{1+1}(t) = P_1(t) + e^{2\pi i 2t} Q_1(t) = P_{0+1} + e^{2\pi i 2t} Q_{0+1} \\ &= P_0(t) + e^{2\pi i t} Q_0(t) + e^{2\pi i 2t}\big(P_0(t) - e^{2\pi i t} Q_0(t)\big) \\ &= 1 + e^{2\pi i t} + e^{2\pi i 2t} - e^{2\pi i 3t}. \end{aligned}$$

Define

$$P_r(t) = \operatorname{Re} P_2(t) = 1 + \cos(2\pi t) + \cos(2\pi\, 2t) - \cos(2\pi\, 3t),$$

$$P_i(t) = \operatorname{Im} P_2(t) = \sin(2\pi t) + \sin(2\pi\, 2t) - \sin(2\pi\, 3t).$$

We know that $P_2(t) = \operatorname{Re} P_2(t) + i \operatorname{Im} P_2(t)$ for $t \in [0, 1]$, and so $P_2(t) = 2 + i0 = (2, 0) \in \mathbb{C}$ at $t = 0$.

Let $\alpha = 1/\pi^5$. We must show several facts:

(a) $P_i(t) > 0$ for $t \in (0, \alpha]$.

(b) $P_i(t) < 0$ for $t \in [-\alpha, 0)$.

(c) $P_r(t) > 0$ for $t \in [-\alpha, \alpha] \setminus \{0\}$.

(d) $P_r(t)$ is strictly increasing on $(0, \alpha]$.

(e) $P_r(t)$ is strictly decreasing on $[-\alpha, 0)$.

(f) $P_i(t)$ is strictly increasing on $[-\alpha, \alpha] \setminus \{0\}$.

(g) $\lim_{t\to 0^+} P_i'(t)/P_r'(t)$ and $\lim_{t\to 0^-} P_i'(t)/P_r'(t)$ both exist as finite real numbers.

These seven facts imply that P_2 gives rise to a cusp at $(2, 0) \in \mathbb{C}$, as follows. Conditions (a), (b), and (f) together show that P_2 is traced out in the complex plane from below the real axis to above it, crossing only when $t = 0$. Conditions (c), (d), and (e) together show that P_2 crosses the real axis on the right side of the line $\{2 + xi \ : \ x \in \mathbb{R}\}$, only touching the line when $t = 0$. Finally, (g) shows that the curve is not smooth at $(2, 0)$; in conjunction with (a)–(f), the limits would need to be $\pm\infty$ for no cusp to arise.

We shall use the following Taylor series estimates. For all $x \in \mathbb{R}$,

$$x - \frac{x^3}{3!} \leq \sin x \leq x - \frac{x^3}{3!} + \frac{x^5}{5!} \tag{A.1}$$

and

$$1 - \frac{x^2}{2!} \leq \cos x \leq 1 - \frac{x^2}{2!} + \frac{x^4}{4!}. \tag{A.2}$$

Verification of (a), viz., $P_i(t) = \sin(2\pi t) + \sin(4\pi t) - \sin(6\pi t) > 0$ for all $t \in (0, \alpha]$. Using (A.1), we make the estimates

$$\sin(2\pi t)+\sin(4\pi t) \geq 2\pi t - \frac{(2\pi t)^3}{3!} + 4\pi t - \frac{(4\pi t)^3}{3!} = 6\pi t - \frac{1}{3!}\left((2\pi t)^3 + (4\pi t)^3\right),$$
$$\sin(6\pi t) \leq 6\pi t - \frac{(6\pi t)^3}{3!} + \frac{(6\pi t)^5}{5!}.$$

Hence, it suffices to show that for all $t \in (0, \alpha]$,

$$6\pi t - \frac{(6\pi t)^3}{3!} + \frac{(6\pi t)^5}{5!} < 6\pi t - \frac{1}{3!}\left((2\pi t)^3 + (4\pi t)^3\right),$$

that is,

$$\frac{(6\pi t)^5}{5!} < \frac{1}{3!}(2\pi)^3\left(-t^3 - (2t)^3 + (3t)^3\right) = \frac{18}{3!}(2\pi)^3 t^3.$$

Since $t > 0$, this simplifies to

$$t^2 < \frac{20}{(2\pi)^2}\frac{18}{3^5},$$

which in turn is solved by $0 < t < \frac{\sqrt{5}}{\pi}\frac{3\sqrt{2}}{3^{5/2}} = \frac{\sqrt{10}}{3^{3/2}\pi}$. Since $\alpha = \frac{1}{\pi^5} < \frac{\sqrt{10}}{3^{3/2}\pi}$, we have proved (a).

Verification of (b), viz., $P_i(t) = \sin(2\pi t) + \sin(4\pi t) - \sin(6\pi t) < 0$ for all $t \in [-\alpha, 0)$. The proof of (b) relies on the fact that the sine function is odd. Let $t = -s$, $s \in (0, \alpha]$. Then

$$\sin(2\pi t) + \sin(4\pi t) = -\sin(2\pi s) - \sin(4\pi s) = -\left(\sin(2\pi s) + \sin(4\pi s)\right).$$

We know from (a) that $\sin(2\pi s)+\sin(4\pi s) > \sin(6\pi s)$ for $s \in (0,\alpha]$. Hence $-\sin(6\pi s) > -(\sin(2\pi s)+\sin(4\pi s))$ for $s \in (0,\alpha]$, and therefore, for $t \in [-\alpha, 0)$,

$$\sin(6\pi t) > \sin(2\pi t)+\sin(4\pi t).$$

Hence, (b) is proved.

Verification of (c), viz., $P_r(t) = 1+\cos(2\pi t)+\cos(4\pi t)-\cos(6\pi t) > 0$ for all $t \in [-\alpha,\alpha]\backslash\{0\}$. It suffices to verify the inequality for $t \in (0,\alpha]$ since the cosine function is even.

Using (A.2), we make the estimates

$$1+\cos(6\pi t) \le 2-\frac{(6\pi t)^2}{2!}+\frac{(6\pi t)^4}{4!}$$
$$\cos(2\pi t)+\cos(4\pi t) \ge 1-\frac{(2\pi t)^2}{2!}+1-\frac{(4\pi t)^2}{2!}.$$

Hence, to prove (c), it suffices to show that, for all $t \in (0,\alpha]$,

$$2-\frac{(6\pi t)^2}{2!}+\frac{(6\pi t)^4}{4!} < 2-\Big(\frac{(2\pi t)^2+(4\pi t)^2}{2!}\Big).$$

Simplifying, we obtain $\frac{(6\pi t)^4}{4!} < -6\pi^2t^2+\frac{36\pi^2t^2}{2}$, which turns into

$$54\pi^4t^4 < 12\pi^2t^2.$$

Since $t > 0$, we divide by $6\pi^2t^2$ to obtain the inequality $9t^2\pi^2 < 2$, which in turn is solved by $0 < t < \sqrt{2}/3\pi$. Since $\alpha = 1/\pi^5 < \sqrt{2}/3\pi$, we have proved (c).

Verification of (d), viz., $P_r'(t) = -2\pi\sin(2\pi t)-4\pi\sin(4\pi t)+6\pi\sin(6\pi t) > 0$ for $t \in (0,\alpha]$. We shall prove $3\sin(6\pi t) > 2\sin(4\pi t)+\sin(2\pi t)$ for all $t \in (0,\alpha]$.

Using (A.1), we make the estimates

$$3\sin(6\pi t) \ge 3\Big(6\pi t-\frac{(6\pi t)^3}{3!}\Big),$$
$$2\sin(4\pi t)+\sin(2\pi t) \le 2\Big(4\pi t-\frac{(4\pi t)^3}{3!}+\frac{(4\pi t)^5}{5!}\Big)+2\pi t-\frac{(2\pi t)^3}{3!}+\frac{(2\pi t)^5}{5!}$$
$$= 10\pi t-\frac{(2\pi)^3}{3!}(t^3)(1+2^4)+\frac{(2\pi)^5}{5!}(t^5)(1+2^6).$$

Hence, to prove (d), it suffices to show that, for all $t \in (0,\alpha]$,

$$10\pi t-\frac{(2\pi)^3}{3!}(t^3)(1+2^4)+\frac{(2\pi)^5}{5!}(t^5)(1+2^6) < 3\Big(6\pi t-\frac{(6\pi t)^3}{3!}\Big).$$

Rearranging the inequality, we obtain

$$10\pi t+\frac{(2\pi)^5}{5!}(t^5)(1+2^6)+\frac{(6\pi t)^3}{2} < 18\pi t+\frac{(2\pi)^3}{3!}(t^3)(1+2^4),$$

that is,

$$\frac{(2\pi)^4}{4!}13t^5+\frac{(2\pi)^2}{2}27t^3<4t+\frac{(2\pi)^2}{3!}17t^3.$$

Since $t>0$, this simplifies to

$$\frac{(2\pi)^4}{4!}13t^4+\frac{(2\pi)^2}{2!}\Big(27-\frac{17}{3}\Big)t^2<4.$$

Since we are attempting to prove that the inequality holds for $t\in(0,\alpha]$ with $\alpha<1$, we take advantage of the fact that $t^4<t^2$ when $0<t<1$ to make the estimate

$$\begin{aligned}\frac{(2\pi)^4}{4!}13t^4+\frac{(2\pi)^2}{2!}\big(27-\tfrac{17}{3}\big)t^2&<t^2\Big(\frac{(2\pi)^4(13)}{4!}+\frac{(2\pi)^2(64)}{3!}\Big)<t^2\Big(\frac{(2\pi)^4(78)}{3!}\Big)\\&=t^2(2\pi)^4(13)<t^2(2\pi)^4(2\pi)^2=t^2(2\pi)^6.\end{aligned}$$

So we obtain the inequality $t^2(2\pi)^6<4$, which is solved by $0<t<\dfrac{2}{(2\pi)^3}=\dfrac{1}{4\pi^3}$. Since $\alpha=\dfrac{1}{\pi^5}<\dfrac{1}{4\pi^3}$, we have proved (d).

Verification of (e), viz., $P_r'(t)=-2\pi\sin(2\pi t)-4\pi\sin(4\pi t)+6\pi\sin(6\pi t)<0$ for $t\in[-\alpha,0)$. We prove that $P_r(t)$ is strictly decreasing on $[-\alpha,0)$ using the fact that the sine function is odd — the same method we used to prove (b).

We know from the calculations in the previous page that $P_r'(t)=-2\pi\sin(2\pi t)-4\pi\sin(4\pi t)+6\pi\sin(6\pi t)>0$ when $t\in(0,\alpha]$. Letting $t=-s$, $s\in(0,\alpha]$, we have

$$-2\pi\sin(2\pi s)-4\pi\sin(4\pi s)+6\pi\sin(6\pi s)>0,\ \ s\in(0,\alpha],$$

which leads to

$$-2\pi\sin(2\pi t)-4\pi\sin(4\pi t)+6\pi\sin(6\pi t)<0,\ \ t\in[-\alpha,0).$$

Thus, for $t\in[-\alpha,0)$, $P_r'(t)<0$, so $P_r(t)$ is strictly decreasing on $[-\alpha,0)$.

Verification of (f), viz., $P_i'(t)=2\pi\cos(2\pi t)+4\pi\cos(4\pi t)-6\pi\cos(6\pi t)>0$ for $t\in[-\alpha,\alpha]\setminus\{0\}$. It suffices to verify the inequality for $t\in(0,\alpha]$ since the cosine function is even.

Using (A.2), we make the estimates

$$\cos(2\pi t)+2\cos(4\pi t)\geq 1-\frac{(2\pi t)^2}{2!}+2-\frac{2(4\pi t)^2}{2!}=3-\Big(\frac{(2\pi t)^2}{2}+(4\pi t)^2\Big),$$

$$3\cos(6\pi t)\leq 3-\frac{3(6\pi t)^2}{2!}+\frac{3(6\pi t)^4}{4!}.$$

Hence, to prove (f), it suffices to show that for all $t\in(0,\alpha]$,

$$3-\frac{3(6\pi t)^2}{2!}+\frac{3(6\pi t)^4}{4!}<3-\Big(\frac{(2\pi t)^2}{2}+(4\pi t)^2\Big),$$

that is, $-54\pi^2 t^2 + \dfrac{2^4 3^5 \pi^4 t^4}{2^3 3} < -18\pi^2 t^2$, which simplifies to

$$162\pi^4 t^4 < 36\pi^2 t^2.$$

Since $t > 0$, we divide by $6\pi^2 t^2$ to obtain the inequality

$$27\pi^2 t^2 < 6,$$

which in turn is solved by $0 < t < \dfrac{\sqrt{6}}{\pi\sqrt{27}}$. Since $\alpha = \dfrac{1}{\pi^5} < \dfrac{\sqrt{6}}{\pi\sqrt{27}}$, this proves (f).

Verification of (g), viz., $\lim_{t\to 0^+} P_i'(t)/P_r'(t)$ and $\lim_{t\to 0^-} P_i'(t)/P_r'(t)$ both exist as finite real numbers. The limits need not be equal, so we evaluate them separately.

$$\lim_{t\to 0^+} \frac{P_i'(t)}{P_r'(t)} = \lim_{t\to 0^+} \frac{2\pi(\cos(2\pi t) + 2\cos(4\pi t) - 3\cos(6\pi t))}{-2\pi(\sin(2\pi t) + 2\sin(4\pi t) - 3\sin(6\pi t))},$$

which has the form $0/0$ when plugging in $t = 0$. We use L'Hôpital's rule to get

$$\begin{aligned}\lim_{t\to 0^+} \frac{P_i'(t)}{P_r'(t)} &= \lim_{t\to 0^+} \frac{P_i''(t)}{P_r''(t)} \\ &= \lim_{t\to 0^+} \frac{-(2\pi)^2(\sin(2\pi t) + 4\sin(4\pi t) - 9\sin(6\pi t))}{-(2\pi)^2(\cos(2\pi t) + 4\cos(4\pi t) - \cos(6\pi t))} = \frac{0}{4(2\pi)^2} = 0.\end{aligned}$$

Thus, the limit exists as a finite real number.

Since $\lim_{t\to 0^-} P_i'(t)/P_r'(t)$ also has the form $0/0$, and since

$$\frac{P_i''(t)}{P_r''(t)} = \frac{-(2\pi)^2(\sin(2\pi t) + 4\sin(4\pi t) - 9\sin(6\pi t))}{-(2\pi)^2(\cos(2\pi t) + 4\cos(4\pi t) - \cos(6\pi t))}$$

is continuous at $t = 0$, we have

$$\lim_{t\to 0^-} \frac{P_i'(t)}{P_r'(t)} = \lim_{t\to 0^+} \frac{P_i'(t)}{P_r'(t)} = \lim_{t\to 0} \frac{P_i'(t)}{P_r'(t)} = \lim_{t\to 0} \frac{P_i''(t)}{P_r''(t)} = \frac{P_i''(0)}{P_r''(0)} = 0$$

as well. Hence, (g) is proved, which also shows that $P_2(t)$ admits a cusp when $t = 0$.

5. Acknowledgements

The authors acknowledge fruitful discussions several years ago with J. Donatelli, T. Dulaney, and S. Gerber. More recently, we acknowledge the invaluable scholarship of B. Saffari and the indispensable assistance of E. Au-Yeung. Benedetto gratefully acknowledges support from the AFOSR grant FA9550-05-1-0443. Sugar Moore gratefully acknowledges support from the University of Maryland, Department of Mathematics NSF VIGRE Grant, as well as the Daniel Sweet Undergraduate Research Fellowship of the Norbert Wiener Center at the University of Maryland.

References

[Benedetto 1997] J. J. Benedetto, *Harmonic analysis and applications*, CRC Press, Boca Raton, FL, 1997. MR 97m:42001

[Benke 1994] G. Benke, "Generalized Rudin–Shapiro systems", *J. Fourier Anal. Appl.* **1**:1 (1994), 87–101. MR 96d:42001 Zbl 0835.42014

[Brillhart 1973] J. Brillhart, "On the Rudin–Shapiro polynomials", *Duke Math. J.* **40** (1973), 335–353. MR 47 #3645 Zbl 0263.33012

[Brillhart and Carlitz 1970] J. Brillhart and L. Carlitz, "Note on the Shapiro polynomials", *Proc. Amer. Math. Soc.* **25** (1970), 114–118. MR 41 #5575 Zbl 0191.35101

[Brillhart and Morton 1996] J. Brillhart and P. Morton, "A case study in mathematical research: the Golay–Rudin–Shapiro sequence", *Amer. Math. Monthly* **103**:10 (1996), 854–869. MR 98g:01048 Zbl 0873.11020

[Budišin 1990] S. Z. Budišin, "New complementary pairs of sequences", *Electronics Let.* **26**:13 (1990), 881–883.

[Daubechies 1992] I. Daubechies, *Ten lectures on wavelets*, CBMS-NSF Regional Conference Series in Applied Mathematics **61**, Soc. Industrial Appl. Math., Philadelphia, 1992. MR 93e:42045 Zbl 0776.42018

[Eliahou et al. 1990] S. Eliahou, M. Kervaire, and B. Saffari, "A new restriction on the lengths of Golay complementary sequences", *J. Combin. Theory Ser. A* **55**:1 (1990), 49–59. MR 91i:11020 Zbl 0705.94012

[Eliahou et al. 1991] S. Eliahou, M. Kervaire, and B. Saffari, "On Golay polynomial pairs", *Adv. in Appl. Math.* **12**:3 (1991), 235–292. MR 93b:68066 Zbl 0767.05004

[Golay 1949] M. J. E. Golay, "Multi-slit spectrometry", *J. Opt. Soc. Amer.* **39**:6 (1949), 437–444.

[Golay 1951] M. J. E. Golay, "Static multslit spectrometry and its application to the panoramic display of infrared spectra", *J. Opt. Soc. Amer.* **41**:7 (1951), 468–472.

[Golay 1961] M. J. E. Golay, "Complementary series", *IRE Trans.* **IT-7**:2 (1961), 82–87. MR 23 #A3096

[Golay 1962] M. J. E. Golay, Note on "Complementary series", 1962. In correspondence section of *Proc. IRE* **50**:1, p. 84.

[Howard et al. 2006] S. D. Howard, A. R. Calderbank, and W. Moran, "The finite Heisenberg–Weyl groups in radar and communications", *EURASIP J. Appl. Signal Process.* (2006), Art. ID 85685. MR 2233868

[Jedwab 2005] J. Jedwab, "A survey of the merit factor problem for binary sequences", pp. 30–55 in *Sequences and their applications: Proceedings of SETA 2004*, Lecture Notes in Computer Science **3486**, Springer, Berlin, 2005.

[Jedwab and Yoshida 2006] J. Jedwab and K. Yoshida, "The peak sidelobe level of families of binary sequences", *IEEE Trans. Inform. Theory* **52**:5 (2006), 2247–2254. MR 2006m:94044

[Kahane 1970] J.-P. Kahane, *Séries de Fourier absolument convergentes*, Ergebnisse der Math. **50**, Springer, Berlin, 1970. MR 43 #801 Zbl 0195.07602

[Katznelson 1976] Y. Katznelson, *An introduction to harmonic analysis*, 2nd corr. ed., Dover Publications, New York, 1976. MR 54 #10976 Zbl 0352.43001

[Levanon and Mozeson 2004] N. Levanon and E. Mozeson, *Radar signals*, Wiley and IEEE Press, Hoboken, NJ, 2004.

[Lüke 1985] H. D. Lüke, "Sets of one and higher dimensional Welti codes and complementary codes", *IEEE Trans. Aerospace and Electronic Systems* **21** (1985), 170–179.

[Mallat 1998] S. Mallat, *A wavelet tour of signal processing*, Academic Press, San Diego, CA, 1998. MR 99m:94012 Zbl 0937.94001

[Pezeshki et al. 2008] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, "Doppler resilient Golay complementary waveforms", *IEEE Trans. Inform. Theory* **54**:9 (2008), 4254–4266.

[Rudin 1959] W. Rudin, "Some theorems on Fourier coefficients", *Proc. Amer. Math. Soc.* **10** (1959), 855–859. MR 22 #6979 Zbl 0091.05706

[Rutter 2000] J. W. Rutter, *Geometry of curves*, Chapman & Hall/CRC, Boca Raton, FL, 2000. MR 2001e:53004 Zbl 0962.53002

[Saffari 1986] B. Saffari, "Une fonction extrémale liée à la suite de Rudin–Shapiro", *C. R. Acad. Sci. Paris Sér. I Math.* **303**:4 (1986), 97–100. MR 88a:11024 Zbl 0608.10051

[Saffari 1987] B. Saffari, "Structure algébrique sur les couples de Rudin–Shapiro: Problème extrémal de Salem sur les polynômes à coefficients ± 1", *C. R. Acad. Sci. Paris Sér. I Math.* **304**:5 (1987), 127–130. MR 88d:30008 Zbl 0608.10052

[Saffari 2001] B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century", pp. 201–233 in *Twentieth century harmonic analysis—a celebration* (Il Ciocco, 2000), NATO Sci. Ser. II Math. Phys. Chem. **33**, Kluwer Acad. Publ., Dordrecht, 2001. MR 2002g:26001 Zbl 0996.42001

[Searle and Howard 2007] S. Searle and S. Howard, "A novel polyphase code for sidelobe suppression", pp. 377–381 in *Proceedings of IEEE Waveform Diversity and Design* (Pisa, Italy, 2007), IEEE, Los Alamitos, CA, 2007.

[Shapiro 1951] H. S. Shapiro, *Extremal problems for polynomials*, M.S. Thesis, Massachusetts Institute of Technology, 1951.

[Tseng and Liu 1972] C. C. Tseng and C. L. Liu, "Complementary sets of sequences", *IEEE Trans. Information Theory* **IT-18** (1972), 644–652. MR 53 #2511

[Turyn 1974] R. J. Turyn, "Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings", *J. Combinatorial Theory Ser. A* **16** (1974), 313–333. MR 49 #10577 Zbl 0291.05016

[Vaidyanathan 1993] P. P. Vaidyanathan, *Multirate systems and filter banks*, Prentice Hall, Englewood Cliffs, NJ, 1993.

[Welti 1960] G. R. Welti, "Quaternary codes for pulsed radar", *IRE Trans.* **6**:3 (1960), 400–408.

Received: 2009-03-24 Accepted: 2009-08-12

jjb@math.umd.edu *Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742-4111, United States*

sugar@math.umd.edu *Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742-4111, United States*