NOTE ON THE SHAPIRO POLYNOMIALS

JOHN BRILLHART AND L. CARLITZ

1. Introduction. The polynomials \( P_n(x) \) and \( Q_n(x) \), which we are concerned with here, were introduced in 1951 by H. S. Shapiro [5, p. 39] in his study of the magnitude of certain trigonometric sums. They are defined recursively by the formulas

\[
(1) \quad P_{n+1}(x) = P_n(x) + x^2 Q_n(x), \quad Q_{n+1}(x) = P_n(x) - x^2 Q_n(x),
\]

where \( n \geq 0 \) and \( P_0(x) = Q_0(x) = 1 \). (See [4] also. Note in this reference that \( P_0(x) = Q_0(x) = x \).

These polynomials have been used by Kahane and Salem in their book [1] to prove several theorems about trigonometric series. Rider [2] used a generalization of these polynomials to complete the solution of a problem partially solved in [4]. In a more recent paper Rider [3] employed the polynomials to exhibit certain subalgebras of the group algebra of the unit circle. In particular, in this paper Rider obtained a special case of Theorem 4 below.

The first few polynomials are

\[
\begin{align*}
P_1(x) &= 1 + x, \\
P_2(x) &= 1 + x + x^2 - x^3, \\
P_3(x) &= 1 + x + x^2 - x^3 + x^4 + x^5 - x^6 + x^7, \\
Q_1(x) &= 1 - x, \\
Q_2(x) &= 1 + x - x^2 + x^3, \\
Q_3(x) &= 1 + x + x^2 - x^3 - x^4 + x^5 + x^6 - x^7.
\end{align*}
\]

It is clear from this definition that \( \deg P_n = \deg Q_n = 2^n - 1 \).

In this note we will derive a relation between \( P_n(x) \) and \( Q_n(x) \) and use it to show that these polynomials have equal discriminants. We will also find a formula for the resultant of the two polynomials, and develop an explicit formula for their coefficients. The latter will then be used to compute the value of \( P_n(x) \) at \( x = \pm 1, \pm i \), and certain other points on the unit circle.

2. We begin by deriving the relation that exists between \( P_n(x) \) and \( Q_n(x) \).

**Theorem 1.** \( Q_n(x) = (-1)^{n+1} P_n(-1/x), \) \( n \geq 0 \).

**Proof.** By induction. The theorem holds for \( n = 0, 1 \). Assume the relation for \( n, n \geq 1 \). Then

Received by the editors February 13, 1969 and, in revised form, September 18, 1969.
(−1)^{n+1}x^{n+1}−1P_{n+1}(−1/x).

= (−1)^{n+1}x^{n+1}−1[P_n(−1/x) + (−1/x)^nQ_n(−1/x)]

= (−1)^{n+1}x^{n+1}−1[−(−1)^nQ_n(x) + x^{n−1} + x^{−n} (−1)^n(−1/x)^{n−1}P_n(x)]

= P_n(x) − x^nQ_n(x) = Q_{n+1}(x).

The following properties of the discriminant D of a polynomial will be of use in establishing the corollary below. Let c≠0 be a constant and f(x) by a polynomial of degree n. Then

(i) D(f(cx)) = c^{n−1}D(f(x)).

(ii) D(f(1/x)) = D(f(x)).

(iii) D(1/f(x)) = D(f(x)).

**Corollary.** D(P_n(x)) = D(Q_n(x)), n ≥ 0.

**Proof.**

\[
D(Q_n(x)) = D((-1)^n x^{n−1}P_n(1/x))
\]

= D((-1)^{n+1}x^{n−1}P_{n+1}(1/x)),

using (i) with c = −1. The corollary then follows from (ii) and (iii).

The first few completely factored values of D(P_n(x)) are listed in the table below.

<table>
<thead>
<tr>
<th>n</th>
<th>D(P_n(x))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>(-2\cdot11 = -44)</td>
</tr>
<tr>
<td>3</td>
<td>(2^{10} \cdot 5^2 \cdot 193)</td>
</tr>
<tr>
<td>4</td>
<td>(2^{34} \cdot 3283409652827)</td>
</tr>
</tbody>
</table>

We next recall several properties of the resultant R of two polynomials f and g of degree n and m respectively.

(i) R(f, cg) = c^nR(f, g), c a constant.

(ii) R(f, g) = a^dR(f, g + λf), where a is the leading coefficient of f, λ is an arbitrary polynomial, and d = deg g − deg (g + λf).

(iii) R(f, g) = (−1)^{m+n}R(g, f).

(iv) R(f, gh) = R(f, g)R(f, h).

**Theorem 2.** R(P_n(x), Q_n(x)) = (−1)^{n−1}x^{n+1}−1, n ≥ 1.

**Proof.** For n = 1 we have R(P_1, Q_1) = 2. Suppose n > 1. Then
\[ R(P_n, Q_n) = R(P_{n-1} + x^{2^{n-1}}Q_{n-1}, P_{n-1} + x^{2^{n-1}}Q_{n-1}) \]
\[ = R(P_{n-1} + x^{2^{n-1}}Q_{n-1}, 2P_{n-1}) \]
\[ = -2^{2^{n-1}}R(P_{n-1}, P_{n-1} + x^{2^{n-1}}Q_{n-1}) \]
\[ = -2^{2^{n-1}}R(P_{n-1}, x^{2^{n-1}}Q_{n-1}) \]
\[ = -2^{2^n-1}R(P_{n-1}, x^{2^{n-1}})R(P_{n-1}, Q_{n-1}). \]

But \( R(P_{n-1}, x^{2^{n-1}}) = 1 \). Hence \( R(P_n, Q_n) = -2^{2^n-1} R(P_{n-1}, Q_{n-1}) \). From this reduction step, used repeatedly, we obtain the evaluation \( R(P_n, Q_n) = \prod_{i=2}^{n} (-2^{2^{i-1}}) \{ R(P_1, Q_1) = (-1)^{n-1}2^{2^n-n-1}. \]

The next theorem permits the generation of \( P_n(x) \) and \( Q_n(x) \) without combining the two types of polynomials.

**Theorem 3.**

\[ P_{n+1}(x) = P_n(x^2) + xP_n(-x^2), \quad n \geq 0. \]
\[ Q_{n+1}(x) = Q_n(x^2) + xQ_n(-x^2), \quad n \geq 1. \]

**Proof.** By induction. The formulas are true for \( n = 0, 1 \). Assume both formulas hold for \( n, n \geq 1 \). Then

\[ P_{n+1}(x) = P_n(x) + x^2Q_n(x) \]
\[ = [P_{n-1}(x^2) + xP_{n-1}(-x^2)] + x^2[Q_{n-1}(x^2) + xQ_{n-1}(-x^2)] \]
\[ = [P_{n-1}(x^2) + xQ_{n-1}(x^2)] + x[P_{n-1}(-x^2) + x^2Q_{n-1}(-x^2)]. \]

Hence,

\[ P_{n+1}(x) = P_n(x^2) + xP_n(-x^2). \]

The formula for \( Q_{n+1}(x) \) is established in a similar manner.

3. We now turn to an investigation of the coefficients of \( P_n(x) \). (The corresponding results can be obtained for \( Q_n(x) \) through the use of Theorem 1.)

It is clear from (1) that \( P_n(x) \) has coefficients \( \pm 1 \), without gaps, and that the first \( 2^n \) coefficients of \( P_{n+1}(x) \) are identical with those of \( P_n(x) \). It follows then that these coefficients do not depend on \( n \), so we can write \( P_n(x) = \sum_{r=0}^{2^n-1} a(r)x^r, \quad n \geq 0. \) (We may, of course, also consider \( P_n(x) \) as the first \( 2^n \) terms of the infinite series \( P_n(x) = \sum_{r=0}^{\infty} a(r)x^r. \))

We will now derive an explicit formula for \( a(r) \).

**Theorem 4.** If we write \( r = r_0 + r_1 \cdot 2 + r_2 \cdot 2^2 + \cdots + r_k \cdot 2^k, \quad k \geq 0, \)
\( r_i = 0 \) or \( 1 \), then
\[ a(r) = (-1)^{r_0 + r_2 + \cdots + r_{k-1}}. \]

**Proof.** We observe in (2) that the even and odd degree terms on the right side are separated, which allows us to equate coefficients, obtaining the relations \( a(2r) = a(r) \) and \( a(2r+1) = (-1)^r a(r) \). If we write \( a(r) = (-1)^r c(r) \), then

\[ c(2r) = c(r) \quad \text{and} \quad c(2r + 1) \equiv r + c(r) \pmod{2}. \]

Proceeding by induction on \( k \), we verify for \( k = 0 \) that \( 1 = a(r_0) = (-1)^0 \), where \( r_0 = 0 \) or 1. Assume next that \( c(r) = r_0^2 + r_2^2 + \cdots + r_{k-1}^2 \) for any \( r = r_1 + r_2 + 2 + \cdots + r_{k-1} \cdot 2^{k-1} \) of \( k \) digits. Consider the number \( 2r + r_0 \), where \( r_0 = 0 \) or 1. Then using \( (4) \) \( c(2r + r_0) = r_0 r + c(r) \)

\[ \equiv r_0 r_1 + c(r) = r_0 r_1 + r_1 r_2 + \cdots + r_{k-1} r_k \pmod{2}. \]

(Note the particular case \( a(2^k) = 1 \).

4. We next consider the problem of evaluating \( P_n(x) \) at certain points on the unit circle. We begin with

**Theorem 5.**

\[
P_{2n}(1) = 2^n, \quad P_{2n+1}(1) = 2^{n+1}, \quad n \geq 0.
\]

\[
P_{2n}(-1) = 2^n, \quad P_{2n+1}(-1) = 0, \quad n \geq 0.
\]

**Proof.** Let \( \theta(n) \) be the number of \( a(r) \) in \( P_n(x) \) that are positive. In particular, let \( \theta_0(n) \) be the number of \( a(2r) \) and \( \theta_1(n) \) be the number of \( a(2r+1) \) in \( P_n(x) \) that are positive. Then certainly

\[ \theta(n) = \theta_0(n) + \theta_1(n). \]

Since the first term on the right side of (2) contains all the terms of even degree, we have

\[ \theta_0(n + 1) = \theta_0(n), \]

and hence by (5)

\[ \theta_0(n + 1) = \theta_0(n) + \theta_1(n). \]

Also, since the second term on the right side of (2) can be written as \( \sum_{r=0}^{2^{n+1}} (-1)^r a(r) x^{2r+1} \), we find that

\[ \theta_1(n + 1) = \theta_0(n) + [2^{n+1} - \theta_1(n)]. \]

Adding this equation to (7), and using (5), we obtain

\[ \theta(n + 1) = \theta_0(n + 1) + \theta_1(n + 1) = 2\theta_0(n) + 2^{n-1}. \]

Finally, from (6) we derive the recursion relation
\[ \theta(n + 1) = 2\theta(n - 1) + 2^{n-1}. \]

With the initial conditions \( \theta(0) = 1 \), and \( \theta(1) = 2 \), the solution is readily found to be

\[ \theta(2n) = 2^{2n-1} + 2^{n-1}, \quad \theta(2n + 1) = 2^{2n} + 2^n, \quad n \geq 0. \]

From the equation \( P_n(1) = \theta(n) - [2^n - \theta(n)] = 2\theta(n) - 2^n \), we conclude that \( P_{2n}(1) = 2^n \) and \( P_{2n+1}(1) = 2^{n+1} \). If we now set \( x = 1 \) in (2), we have \( P_n(-1) = P_{n+1}(1) - P_n(1) \), whence \( P_{2n}(-1) = 2^n \) and \( P_{2n+1}(-1) = 0 \).

With a knowledge of \( P_n(\pm 1) \), we are in a position to find the values at \( x = e^{it} \). For example, setting \( x = i \) in (2), we obtain \( P_{n+1}(i) = P_n(-1) + iP_n(1) \), whence \( P_{2n}(i) = i \cdot 2^n \) and \( P_{2n+1}(i) = (1 + i)2^n \). The values at \( x = -i \) are found by conjugating.

Remark. It can readily be shown by repeated use of (2) that the series \( P_n(x) \) diverges at the dense set of points \( \exp(2\pi i/2^n) \) on the unit circle.

The authors would like to thank Michael Garvey for his suggestions on parts of the paper.

References