The Journal of Fourier Analysis and Applications

Volume 10, Issue 5, 2004

Moments of the Rudin–Shapiro Polynomials

Christophe Doche and Laurent Habsieger

Communicated by John J. Benedetto

ABSTRACT. We develop a new approach of the Rudin–Shapiro polynomials. This enables us to compute their moments of even order q for $q \leqslant 32$, and to check a conjecture on the asymptotic behavior of these moments for q even and $q \leqslant 52$.

1. Introduction

The Rudin–Shapiro polynomials [6, 8] are polynomials of ± 1 coefficients. They are defined by the recurrence relation

$$\begin{cases} P_{n+1}(z) = P_n(z) + z^{2^n} Q_n(z)\,, \\ Q_{n+1}(z) = P_n(z) - z^{2^n} Q_n(z)\,, \end{cases} \tag{1.1}$$

and the first values $P_0(z) = Q_0(z) = 1$. One easily proves by induction that the degree of P_n and Q_n is $2^n - 1$. The moment of order $q > 0$ of a polynomial P is given by the formula

$$M_q(P) = \int_0^1 \left| P\left(\mathrm{e}^{2i\pi\theta}\right)\right|^q \mathrm{d}\theta\,.$$

Since P_n and Q_n have ± 1 coefficients, we obviously get $M_2(P_n) = M_2(Q_n) = 2^n$. In 1968 Littlewood [3] evaluated $M_4(P_n) = M_4(Q_n)$, a result which was found again by many authors since. In 1980 Saffari [7] showed that the moments of order $4Q+2$ may be computed from the moments of order $4q$ with $q \leqslant Q$, and he proposed the following conjecture about the asymptotic behavior of the moments of the Rudin–Shapiro polynomials.

Math Subject Classifications. 11B83, 42A05.
Keywords and Phrases. Rudin–Shapiro polynomials, Golay polynomials, signal theory.
Acknowledgements and Notes. Authors partially supported by the European Community IHRP Program, within the Research Training Network "Algebraic Combinatorics in Europe," grant HPRN-CT-2001-00272.

ISSN 1069-5869 DOI: 10.1007/s00041-004-3049-y

Conjecture 1.

For any even integer q we have

$$M_q(P_n) \sim \frac{2^{q/2(n+1)}}{q/2+1}\,.$$

In this article we show that the moments of order q satisfy a linear recurrence relation in n, with constant coefficients. For $q \leqslant 32$, $q \equiv 0 \mod 2$, we compute the minimal recurrence relation and the first values of the moments, which enables us to check the conjecture for these q's. Our approach leads to a conjecture which implies Conjecture 1. We check this new conjecture for $q \leqslant 52$, $q \equiv 0 \mod 4$, thus, proving Conjecture 1 for even $q \leqslant 52$.

In Section 2 we show the existence of a linear recurrence relation. In Section 3, we use linear algebra tools to reduce Conjecture 1 to an eigenvalue problem, and we state another stronger conjecture. Section 4 is devoted to the description of our experimental results.

2. Existence of a Recurrence Relation

Let q denote a fixed even integer. For any set of variables (a, a', b, b'), let us introduce

$$R_n\big(z, a, a', b, b'\big) = \Big(\big(a\,P_n(z) + b\,Q_n(z)\big)\big(a'\,P_n\big(z^{-1}\big) + b'\,Q_n\big(z^{-1}\big)\big)\Big)^{q/2}\,.$$

The expansion of R_n may be written as

$$R_n\big(z, a, a', b, b'\big) = \sum_{k=-q(2^n-1)/2}^{q(2^n-1)/2} c_{k,n}\big(a, a', b, b'\big)z^k\,.$$

We define the fundamental polynomial

$$S_n\big(z, a, a', b, b'\big) = \sum_{k=-q/2+1}^{q/2-1} c_{k2^n,n}\big(a, a', b, b'\big)z^k = \frac{1}{2^n}\sum_{y^{2^n}=z} R_n\big(y, a, a', b, b'\big)\,.$$

Let us note that, for any pair of complex numbers (a, b), the moment of order q of the polynomial $a\,P_n(z) + b\,Q_n(z)$ equals $c_{0,n}(a, \bar{a}, b, \bar{b})$, i.e., the constant term (in z) of the polynomial $S_n(z, a, \bar{a}, b, \bar{b})$. Thus, any linear recurrence relation satisfied by the polynomial $S_n(z, a, a', b, b')$ will also be satisfied by the moments of order q of the polynomial $a\,P_n(z) + b\,Q_n(z)$, for any choice of (a, b). The Rudin–Shapiro polynomials correspond to the special case $(a, b) = (1, 0)$.

We start with a basic formula.

Lemma 1.

For every nonnegative integer n, we have

$$S_{n+1}\big(z, a, a', b, b'\big) = \frac{1}{2}\sum_{y^2=z} S_n\Big(y, a+b, a'+b', (a-b)y, \big(a'-b'\big)y^{-1}\Big)\,.$$

Proof. By definition, the polynomial $S_{n+1}(z, a, a', b, b')$ equals

$$\frac{1}{2^{n+1}}\sum_{y^{2^{n+1}}=z} R_{n+1}\big(y, a, a', b, b'\big) = \frac{1}{2}\sum_{y_1^2=z}\frac{1}{2^n}\sum_{y_2^{2^n}=y_1} R_{n+1}\big(y_2, a, a', b, b'\big)\,.$$

By (1.1), we have

$$aP_{n+1}(z) + bQ_{n+1}(z) = (a+b)P_n(z) + (a-b)z^{2^n}Q_n(z)\,,$$
$$a'P_{n+1}\big(z^{-1}\big) + b'Q_{n+1}\big(z^{-1}\big) = \big(a'+b'\big)P_n\big(z^{-1}\big) + \big(a'-b'\big)z^{-2^n}Q_n\big(z^{-1}\big)\,,$$

and therefore

$$R_{n+1}\big(z,a,a',b,b'\big) = R_n\left(z, a+b, a'+b', (a-b)z^{2^n}, \big(a'-b'\big)z^{-2^n}\right).$$

We then deduce that

$$\begin{aligned} &S_{n+1}\big(z,a,a',b,b'\big)\\ &\quad= \frac{1}{2}\sum_{y_1^2=z}\frac{1}{2^n}\sum_{y_2^{2^n}=y_1} R_n\left(y_2, a+b, a'+b', (a-b)y_2^{2^n}, \big(a'-b'\big)y_2^{-2^n}\right)\\ &\quad= \frac{1}{2}\sum_{y_1^2=z} S_n\big(y_1, a+b, a'+b', (a-b)y_1, \big(a'-b'\big)y_1^{-1}\big)\,, \end{aligned}$$

and the lemma follows. □

We now look for a finite-dimensional vector space which contains the polynomials $S_n(z,a,a',b,b')$ and which is invariant under the transformation described in Lemma 1.

The polynomials $S_n(z,a,a',b,b')$ are bihomogeneous in $\big((a,b),(a',b')\big)$ of bidegree $(q/2, q/2)$, and their degree in z belongs to the set $\{-q/2+1,\dots,q/2-1\}$. Let us introduce the new set of variables

$$\begin{aligned} u &= aa'+bb', \qquad v = ab'+a'b\,,\\ w &= aa'-bb', \qquad x = ab'-a'b \end{aligned}$$

so that $u^2 - v^2 = w^2 - x^2$ and

$$S_0\big(z,a,a',b,b'\big) = (u+v)^{q/2}\,.$$

Let E be the complex vector space of the polynomials in (z, z^{-1}, u, v, w, x) which are homogeneous in (u, v, w, x) of degree $q/2$, and whose degree in z belongs to $\{-q/2+1,\dots,q/2-1\}$. Let E^0 be the subspace of E consisting of the elements of E which are invariant under the conjugacy action $(x,z)\to(-x,z^{-1})$. Let F be the quotient space of E^0 by the principal ideal generated by the polynomial $u^2 - v^2 - w^2 + x^2$. We shall now consider $S_0(z,a,a',b,b')$ as an element of F. Let us define on F a linear map T by

$$T\Big(P\big(z,z^{-1},u,v,w,x\big)\Big) = \frac{1}{2}\sum_{y^2=z} P\big(y, y^{-1}, 2u, 2(c_y w + s_y x), 2v, -2(s_y w + c_y x)\big)$$

where $c_y = (y+y^{-1})/2$ and $s_y = (y-y^{-1})/2$. One easily checks that T is well-defined on F, and corresponds to the transformation given in Lemma 1:

$$S_n\big(z,a,a',b,b'\big) = T^n\big(S_0\big(z,a,a',b,b'\big)\big)\,.$$

Since F is finite-dimensional, the characteristic polynomial of T induces a linear recurrence relation satisfied by $S_n(z,a,a',b,b')$, with constant coefficients. It appears that the minimal recurrence relation comes from the minimal polynomial of T, whose degree is smaller than the dimension of F.

3. Another Conjecture

It is obvious that $u^{q/2}$ is an eigenvector of T, associated to the eigenvalue $2^{q/2}$. It would be nice to prove that this eigenspace is of dimension one, to compute the projection of $S_0(z,a,a',b,b')$ and to show that the other eigenvalues of T have a smaller modulus. We shall give partial results in that direction, using smaller vector spaces.

An easy computation gives

$$\begin{aligned} T\big(S_0(z,a,a',b,b')\big) &= T\big((u+v)^{q/2}\big) \\ &= 2^{q/2} \sum_{0\leqslant 2k\leqslant q/2} \binom{q/2}{2k} u^{q/2-2k}\,(c_z w + s_z x)^{2k}\ . \end{aligned}$$

We define

$$\begin{aligned} S'_0(z,a,a',b,b') &= \frac{S_0(z,a,a',b,b') + S_0(z,a,a',-b,-b')}{2} \\ &= \sum_{0\leqslant 2k\leqslant q/2} \binom{q/2}{2k} u^{q/2-2k} v^{2k}\,, \end{aligned}$$

so that $T\big(S_0(z,a,a',b,b')\big) = T\big(S'_0(z,a,a',b,b')\big)$. Let us study the subspace $G \subset F$ spanned by $\mathcal{B}_1 \cup \mathcal{B}_2$ where

$$\mathcal{B}_1 = \bigcup_{m=0}^{q/2-1} \bigcup_{\substack{j,k,l\geqslant 0 \\ j+2k+l=q/2}} \Big\{ (z^m + z^{-m}) u^j v^{2k} w^l \Big\}$$

and

$$\mathcal{B}_2 = \bigcup_{m=1}^{q/2-1} \bigcup_{\substack{j,k,l\geqslant 0 \\ j+2k+l=q/2-1}} \Big\{ (z^m - z^{-m}) u^j v^{2k} w^l x \Big\}\ .$$

Then $S'_0(z,a,a',b,b')$ belongs to G and $T(G) \subset G$. Indeed, for every element $(z^m + z^{-m})u^j v^{2k} w^l$ of $\mathcal{B}_1$, we have $T\left((z^m + z^{-m})u^j v^{2k} w^l\right) = 0$ if m is odd and

$$T\left((z^m + z^{-m})u^j v^{2k} w^l\right) = 2^{q/2}\big(z^{m/2} + z^{-m/2}\big) u^j \left(\frac{c_z+1}{2} w^2 + \frac{c_z-1}{2} x^2 + s_z w x\right)^k v^l$$

if m is even. Similarly, for every element $(z^m - z^{-m})u^j v^{2k} w^l x$ of $\mathcal{B}_2$, we have $T\big((z^m -$

$z^{-m})u^j v^{2k} w^l x\big) = 0$ if m is even and

$$\begin{aligned}
&T\left(\big(z^m - z^{-m}\big)u^j v^{2k} w^l x\right)\\
&\quad = 2^{q/2}\big(z^{(m-1)/2} + z^{-(m-1)/2}\big)u^j \left(\frac{c_z+1}{2}w^2 + \frac{c_z-1}{2}x^2 + s_z wx\right)^k v^l w\\
&\qquad - 2^{q/2}\big(z^{(m+1)/2} + z^{-(m+1)/2}\big)u^j \left(\frac{c_z+1}{2}w^2 + \frac{c_z-1}{2}x^2 + s_z wx\right)^k v^l w\\
&\qquad - 2^{q/2}\big(z^{(m-1)/2} - z^{-(m-1)/2}\big)u^j \left(\frac{c_z+1}{2}w^2 + \frac{c_z-1}{2}x^2 + s_z wx\right)^k v^l x\\
&\qquad - 2^{q/2}\big(z^{(m+1)/2} - z^{-(m+1)/2}\big)u^j \left(\frac{c_z+1}{2}w^2 + \frac{c_z-1}{2}x^2 + s_z wx\right)^k v^l x
\end{aligned}$$

if m is odd. We then use hyperbolic trigonometry formulas to express these images as a linear combination of elements of $\mathcal{B}_1 \cup \mathcal{B}_2$.

Let

$$\mathcal{B}_0 = \left\{u^{q/2-2k}v^{2k} \;:\; 0 \leqslant k \leqslant q/2\right\},$$

$$\mathcal{B}_0' = \left\{u^{q/2}\right\} \cup \bigcup_{\substack{k,l\geqslant 0\\ 0<k+l\leqslant q/4}} \left\{u^{q/2-2k-2l}v^{2k}w^{2l} - \frac{(2k)!(k+l)!(2l)!}{k!l!(2k+2l)!}\frac{u^{q/2}}{2k+2l+1}\right\}$$

$$\mathcal{B}_1' = \bigcup_{\substack{j,k,l\geqslant 0\\ j+2k+2l+1=q/2}} \left\{u^j v^{2k} w^{2l+1}\right\},$$

$$\mathcal{B}_1'' = \bigcup_{m=1}^{q/2-1} \bigcup_{\substack{j,k,l\geqslant 0\\ j+2k+l=q/2}} \left\{\big(z^m + z^{-m}\big)u^j v^{2k} w^l\right\}.$$

Put $\mathcal{B} = \mathcal{B}_0' \cup \mathcal{B}_1' \cup \mathcal{B}_1'' \cup \mathcal{B}_2$; it is still a basis of G. Let G_0 denote the subspace spanned by $u^{q/2}$ and let G_1 be the subspace of G spanned by the elements of $\mathcal{B}$ distinct from $u^{q/2}$. This choice of basis is motivated by the following lemma.

Lemma 2.
$T(G_1) \subset G_1$.

Proof. Let π denote the projection on the subspace spanned by $\mathcal{B}_0$. For every element $(z^m + z^{-m})u^j v^{2k} w^l$ of $\mathcal{B}_1$, we find

$$\pi\left(T\left(\big(z^m + z^{-m}\big)u^j v^{2k} w^l\right)\right) = \begin{cases} 0 & \text{if } m > 0\,,\\ 0 & \text{if } m = 0 \text{ and } l \equiv 1 \mod 2\,.\end{cases}$$

When $m = 0$ and $l \equiv 0 \mod 2$, we obtain

$$\pi\left(T\big(u^j v^{2k} w^l\big)\right) = 2^{q/2-2k}\binom{2k}{k} u^j \big(u^2 - v^2\big)^k v^l\,.$$

Moreover, for every element $(z^m - z^{-m})u^j v^{2k} w^l x$ of $\mathcal{B}_2$, we have

$$\pi\left(T\left(\big(z^m - z^{-m}\big)u^j v^{2k} w^l x\right)\right) = 0\,.$$

Let us take a vector $u^{q/2-2k-2l}v^{2k}w^{2l}$, with $k, l \geqslant 0$ and $k + l \leqslant q/4$, and let us decompose its image by $\pi \circ T$ in the basis $\mathcal{B}'_0$. We obtain

$$\pi\left(T\left(u^{q/2-2k-2l}v^{2k}w^{2l}\right)\right)$$
$$= 2^{q/2-2k}\binom{2k}{k}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\left(u^{q/2-2i-2l}v^{2i+2l} - \frac{u^{q/2}}{2i+2l+1}\right) + C_{k,l}u^{q/2},$$

with

$$\begin{aligned} C_{k,l} &= 2^{q/2-2k}\binom{2k}{k}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\frac{1}{2i+2l+1} \\ &= 2^{q/2-2k}\binom{2k}{k}\sum_{i=0}^{k}(-1)^i\binom{k}{i}\int_0^1 t^{2i+2l}\,\mathrm{d}t \\ &= 2^{q/2-2k}\binom{2k}{k}\int_0^1 t^{2l}\left(1-t^2\right)^k\,\mathrm{d}t \\ &= \frac{(2k)!(k+l)!(2l)!}{k!l!(2k+2l)!}\frac{2^{q/2}}{2k+2l+1}\,. \end{aligned}$$

Therefore we always get

$$\pi\left(T\left(u^j v^{2k}w^{2l} - \frac{(2k)!(k+l)!(2l)!}{k!l!(2k+2l)!}\frac{u^{q/2}}{2k+2l+1}\right)\right) \in G_1\,. \qquad \square$$

Let us now compute the projection of $S'_0(z, a, a', b, b')$ on G_0.

Lemma 3.
$S'_0(z, a, a', b, b') - (2u)^{q/2}/(q/2+1) \in G_1$.

Proof. We have

$$\begin{aligned} S'_0\left(z, a, a', b, b'\right) &= \sum_{0\leqslant 2k\leqslant q/2}\binom{q/2}{2k}u^{q/2-2k}v^{2k} \\ &= \sum_{0\leqslant 2k\leqslant q/2}\binom{q/2}{2k}\left(u^{q/2-2k}v^{2k} - \frac{u^{q/2}}{2k+1}\right) + Cu^{q/2}\,. \end{aligned}$$

This shows that $S'_0(z, a, a', b, b') - Cu^{q/2} \in G_1$ with

$$\begin{aligned} C &= \sum_{0\leqslant 2k\leqslant q/2}\binom{q/2}{2k}\frac{1}{2k+1} = \frac{1}{2}\sum_{0\leqslant k\leqslant q/2}\binom{q/2}{k}\int_{-1}^1 t^k\,\mathrm{d}t \\ &= \frac{1}{2}\int_{-1}^1 (1+t)^{q/2}\,\mathrm{d}t = \frac{2^{q/2}}{q/2+1}\,, \end{aligned}$$

and the lemma is proved. $\square$

We can now state a conjecture which implies Conjecture 1.

Conjecture 2.

The eigenvalues of the restriction of T to G_1 have a modulus smaller than $2^{q/2}$.

Let us now give a few applications of this conjecture. By Lemmas 2 and 3, we have the following result.

Theorem 1.

Assume Conjecture 2 is true. For $(a, a', b, b') \in \mathbb{C}^4$, we then have

$$S_n(z, a, a', b, b') \sim \frac{2^{q/2}}{q/2+1}\left(2^{q/2}(aa' + bb')\right)^n$$

when n goes to infinity.

Considering the constant term of $S_n(a, \bar{a}, b, \bar{b})$ leads to the following corollary.

Corollary 1.

Assume Conjecture 2 is true. For $(a, b) \in \mathbb{C}^2$, the moment of order q of $aP_n(z) + bQ_n(z)$ is equivalent to

$$\frac{2^{q/2}}{q/2+1}\left(2^{q/2}(|a|^2 + |b|^2)\right)^n,$$

when n goes to infinity.

The case $(a, b) = (1, 0)$ gives the asymptotic behavior of the moments of order q of the Rudin–Shapiro polynomials.

4. Experimental Results

We get an exact formula for the moments of order q of the Rudin–Shapiro polynomials as soon as we find a recurrence formula they satisfy, and the first values of the moments (at least up to the order of the recurrence). We compute these first moments using the polynomials $S_n(z, a, a', b, b')$. We determine them by induction with Lemma 1. At each step we save the constant term of $S_n(z, 1, 1, 0, 0)$, which is the moment of order q of $P_n(z)$.

We compute the minimal recurrence relation R_q studying the corresponding operator T_q. For $q \equiv 0 \mod 4$, $q \leqslant 32$, we get the characteristic polynomial of T_q using the command `charpoly` of PARI [5]. For $q = 28$ and 32, the computations are first made modulo large primes and the Chinese Remainder Theorem allows to find the requested polynomial. We then test all the divisors of this characteristic polynomial on the first moments to obtain the minimal recurrence relation.

Obviously $R_2(X) = X - 2$ and it is known that $R_4(X) = X^2 - 2X - 8$. We find

$$\begin{aligned} R_8(X) = X^{12} &- 16X^{11} - 212X^{10} + 4416X^9 + 3904X^8 - 474112X^7 \\ &+ 1339392X^6 + 23461888X^5 - 47185920X^4 - 469762048X^3 \\ &- 6811549696X^2 - 22548578304X + 180388626432\,. \end{aligned}$$

Now it is not hard to ensure that $R_q(X)$ splits into $R_{q-2}(X/2)$ (up to a suitable power of 2 to make it monic) times a new factor $F_q(X)$. This relies on the fact that $T_2(u) = 2u$. So when λ is an eigenvalue of T_q associated with the eigenvector V_λ, then 2λ is an eigenvalue of T_{q+2} with the eigenvector uV_λ. Each new recurrence relation is thus obtained by multiplying a new factor F_q to a known one.

Let $\sigma(F_q)$ be the maximal modulus of the roots of F_q. We observe on the computed examples that $\sigma(F_q) < 2^{q/2}$ for all even q less than 32 so that $2^{q/2}$ is the largest root of R_q in modulus and that it is simple. Further details on the recurrences can be found in Table 4.1.

TABLE 4.1

q	deg R_q	deg F_q	$\sigma(F_q)/2^{q/2}$	c_q
4	2	1	0.50	4/3
8	12	10	0.69	16/5
12	36	24	0.74	64/7
16	78	42	0.76	256/9
20	144	66	0.75	1024/11
24	240	96	0.72	4096/13
28	369	129	0.73	16384/15
32	536	167	0.75	65536/17

This implies that the moment of order q of $P_n(z)$ is equivalent to $c_q 2^{nq/2}$. Considering the sequence of linear combinations of the moments associated to the polynomial $R_q(X)/(X - 2^{q/2})$, we obtain a geometric sequence with ratio $2^{q/2}$, whose first term is known. This enables us to compute c_q and to check Conjecture 1 directly for $q \leqslant 32$.

Nevertheless, in order to prove Conjecture 2 it is enough to study the spectral radius of the restriction of T_q to G_1. This is how we show Conjecture 1 for $36 \leqslant q \leqslant 52$, $q \equiv 0 \mod 4$. More precisely, let N_1 be the matrix of T_q in the basis $\mathcal{B} \setminus \{u^{q/2}\}$. Let $\|N\|_2$ denote the ℓ_2 norm of the matrix N and let $\rho(N)$ be the spectral radius of N. It is known [4] that $\rho(N) \leqslant \|N^k\|_2^{1/k}$ for every positive integer k. We computed $\|N_1^k\|_2^{1/k}$ for small values of k and checked Conjecture 2 in this way. Thus, Conjecture 1 is also true for these values of q, even though we do not know the corresponding recurrence relations.

Some of these results have been recently extended to generalized Rudin–Shapiro polynomials [1] and a fast program to compute the exact value of the moments of these polynomials is available at [2]. It includes all the corresponding minimal recurrences as well as the initial moments.

References

[1] Doche, C. Even moments of generalized Rudin–Shapiro polynomials, submitted to *Math. Comp.*. Available from `http://www.math.u-bordeaux.fr/~cdoche`.

[2] Doche, C. A GP–PARI program to compute the moments of some generalized Rudin–Shapiro polynomials, Available from `http://www.math.u-bordeaux.fr/~cdoche`.

[3] Littlewood, J.E. (1968). *Some Problems in Real and Complex Analysis,* D.C. Heath and Co. Raytheon Education Co., Lexington, MA.

[4] Ljubič, Ju.I. (1965). An algorithm for calculating the spectral radius of an arbitrary matrix, *Ukrain. Mat. Z.,* **17**, 128–135.

[5] The PARI Group, Bordeaux, PARI/GP, Version 2.1.5. (2002). Available from `http://www.parigp-home.de/`.

[6] Rudin, W. (1959). Some theorems on Fourier coefficients, *Proc. Am. Math. Soc.,* **10**, 855–859.

[7] Saffari, B. (2001). Personal communication.

[8] Shapiro, H.S. (1951). Extremal problems for polynomials and power series, PhD thesis, MIT.

Received July 16, 2003

Division of ICS, Building E6A Room 360, Macquarie University, NSW 2109, Australia
e-mail: doche@ics.mq.edu.au

IGD, CNRS UMR 5028, Université Claude Bernard Lyon 1, 43,
boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France
e-mail: Laurent.Habsieger@euler.univ-lyon1.fr