



NEWMAN POLYNOMIALS NOT VANISHING ON THE UNIT CIRCLE

Idris Mercer

Department of Mathematical Sciences, University of Delaware, Newark, Delaware
idmercer@math.udel.edu

Received: 7/26/12, Revised: 11/7/12, Accepted: 12/7/12, Published: 12/21/12

Abstract

A Newman polynomial is a polynomial in one variable whose coefficients are 0 or 1, and the length of a Newman polynomial is the number of coefficients that are 1. Several authors have asked about the highest minimum modulus of a length n Newman polynomial on the unit circle, but there remains a large gap between what has been conjectured and what has been proved. In this paper, we prove that for each $n > 2$, there is a length n Newman polynomial with no roots on the unit circle.

1. Introduction and Main Result

A *Newman polynomial* of length n is any polynomial of the form

$$\alpha(z) = z^{a_1} + z^{a_2} + \cdots + z^{a_n}$$

where $a_1 < \cdots < a_n$ are distinct nonnegative integers. We let \mathbb{S} denote the unit circle in the complex plane. Many authors have asked questions about roots or reducibility of Newman polynomials [4, 6, 7, 8, 9] and Newman polynomials with high minimum modulus on \mathbb{S} [1, 2, 5].

It has been conjectured that there exist Newman polynomials of length n whose minimum modulus on \mathbb{S} increases with n . More precisely, for any nonnegative integers $a_1 < \cdots < a_n$, define

$$M(a_1, \dots, a_n) = \min_{z \in \mathbb{S}} |z^{a_1} + \cdots + z^{a_n}|$$

and then define

$$\mu(n) = \max M(a_1, \dots, a_n),$$

where the maximum is taken over the (infinitely many) sets of n distinct nonnegative integers. We then state the following conjecture.

Conjecture 1. (i) We have $\lim_{n \rightarrow \infty} \mu(n) = \infty$. (Perhaps $\mu(n) \sim n^c$.) (ii) There exists N such that $\mu(n) > 1$ for all $n \geq N$. (Perhaps $N = 6$.)

Note that (i) implies (ii). Conjecture 1 occurs at the end of [1] in slightly different language. Statement (ii) seems difficult to prove, despite appearing much weaker than (i). Brute-force searches show that $\mu(n) > 1$ for $6 \leq n \leq 20$. That is, for each n from 6 to 20, there is a Newman polynomial α of length n such that $|\alpha(z)| > 1$ for all $z \in \mathbb{S}$. See the end of this paper.

The main purpose of this paper is to prove the following weaker version of Conjecture 1. (For brevity, “nonvanishing” will always mean “not vanishing on \mathbb{S} ”.)

Theorem 2. *For all $n > 2$, there is a nonvanishing Newman polynomial of length n . (In other words, we have $\mu(n) > 0$ for all $n > 2$.)*

To prove Theorem 2, we will rely on several lemmas. The first two are straightforward.

Lemma 3. *If there are nonvanishing Newman polynomials of length n and length m , then there is a nonvanishing Newman polynomial of length nm .*

Proof. Suppose $\alpha(z) = z^{a_1} + \dots + z^{a_n}$ is a nonvanishing Newman polynomial of length n , and suppose $\beta(z) = z^{b_1} + \dots + z^{b_m}$ is a nonvanishing Newman polynomial of length m . Then for any k , $\beta(z^k)$ is nonvanishing. If k is large enough, then the product $\alpha(z)\beta(z^k) = (z^{a_1} + \dots + z^{a_n})(z^{kb_1} + \dots + z^{kb_m})$ will have the property that the nm exponents $a_i + kb_j$ are all distinct, and is hence a Newman polynomial of length nm . □

Our next lemma is equivalent to Lemma 1 in [3], Lemma 1 in [4], and Lemma 4 in [8]. We therefore state it without proof.

Lemma 4. *Suppose z_1, z_2, z_3, z_4 are complex numbers of modulus 1 such that $z_1 + z_2 + z_3 + z_4 = 0$. Then at least one of the three statements*

$$\begin{aligned} z_1 + z_2 = 0 \text{ and } z_3 + z_4 = 0, \\ z_1 + z_3 = 0 \text{ and } z_2 + z_4 = 0, \\ z_1 + z_4 = 0 \text{ and } z_2 + z_3 = 0 \end{aligned}$$

must be true.

Next, we introduce some notation. We will use interval notation for sets of integers:

$$[a, b] = \{a, a + 1, \dots, b - 1, b\}.$$

For any integers $n > 2$ and $0 < k < n$, we define

$$\alpha_{n,k} = \alpha_{n,k}(z) = \sum_{a \in [0,n] \setminus \{k\}} z^a \quad \text{and} \quad \beta_n = \beta_n(z) = \sum_{a \in [0,n-2] \cup \{n+2\}} z^a,$$

which are Newman polynomials of length n . Given an integer n , we will say n is of “type A” if $\alpha_{n,k}$ is nonvanishing for some k , and we will say n is of “type B” if β_n is nonvanishing.

We will prove Theorem 2 in the following way. We will exhibit a specific nonvanishing Newman polynomial of length 6, and we will show that if $n > 2$ and $n \neq 6$, then n is either of type A or B, or can be written as a product of integers of type A or B.

Lemma 5. *The polynomial $\alpha(z) = 1 + z + z^2 + z^4 + z^5 + z^8$ is a nonvanishing Newman polynomial of length 6.*

Proof. The proof is a calculation. First note that $\alpha(1) = 6$ and $\alpha(-1) = 2$, so α does not vanish at ± 1 . Since zeros of α occur in conjugate pairs, it suffices to show α does not vanish on the upper half-circle. So suppose $\alpha(e^{i\theta}) = 0$ for some $\theta \in (0, \pi)$. We then have

$$\begin{aligned} R(\theta) &:= \operatorname{Re} \alpha(e^{i\theta}) = 1 + \cos \theta + \cos 2\theta + \cos 4\theta + \cos 5\theta + \cos 8\theta, \\ J(\theta) &:= \operatorname{Im} \alpha(e^{i\theta}) = \sin \theta + \sin 2\theta + \sin 4\theta + \sin 5\theta + \sin 8\theta. \end{aligned}$$

We want to show $R(\theta)$ and $J(\theta)$ cannot both be 0, which is equivalent to showing $R(\theta)$ and $J(\theta)/\sin \theta$ cannot both be 0. To do this, we rewrite $R(\theta)$ and $J(\theta)/\sin \theta$ using Chebyshev polynomials:

$$\begin{aligned} R(\theta) &= 1 + T_1(x) + T_2(x) + T_4(x) + T_5(x) + T_8(x), \\ J_1(\theta) &:= \frac{J(\theta)}{\sin \theta} = 1 + U_1(x) + U_3(x) + U_4(x) + U_7(x), \end{aligned}$$

where $x = \cos \theta$, and T_n and U_n denote Chebyshev polynomials of the first and second kind respectively. We then have

$$\begin{aligned} R(\theta) &= (1) + (x) + (2x^2 - 1) + (8x^4 - 8x^2 + 1) \\ &\quad + (16x^5 - 20x^3 + 5x) + (128x^8 - 256x^6 + 160x^4 - 32x^2 + 1) \\ &= 128x^8 - 256x^6 + 16x^5 + 168x^4 - 20x^3 - 38x^2 + 6x + 2 =: p(x), \\ J_1(\theta) &= (1) + (2x) + (8x^3 - 4x) + (16x^4 - 12x^2 + 1) \\ &\quad + (128x^7 - 192x^5 + 80x^3 - 8x) \\ &= 128x^7 - 192x^5 + 16x^4 + 88x^3 - 12x^2 - 10x + 2 =: q(x). \end{aligned}$$

Applying the Euclidean algorithm, one can show that the polynomials $p(x)$ and $q(x)$ are relatively prime. It follows that there are no real numbers x such that $p(x)$ and $q(x)$ are both zero, so $R(\theta)$ and $J_1(\theta)$ cannot both be 0. \square

We now give some notation and another straightforward lemma. For any positive integer n , we let $\nu_2(n)$ be the largest k such that 2^k divides n .

Lemma 6. *If $\nu_2(a) \neq \nu_2(b)$, then there does not exist a complex number z satisfying both $z^a = -1$ and $z^b = -1$.*

Proof. Suppose $z^a = -1 = z^b$, and write $a = 2^v(2t + 1)$ and $b = 2^w(2u + 1)$ where $v = \nu_2(a)$ and $w = \nu_2(b)$. Suppose $v < w$ (the other case is similar). Then

$$\begin{aligned} +1 &= (-1)^{2^{w-v}(2u+1)} = (z^a)^{2^{w-v}(2u+1)} \\ &= z^{2^w(2t+1)(2u+1)} = (z^b)^{2t+1} = (-1)^{2t+1} = -1. \end{aligned} \quad \square$$

Next, we show that “most” integers are of type A.

Lemma 7. *For $n > 2$, if $n + 2$ is not a power of 2, then there exists k such that the polynomial $\alpha_{n,k}$ defined earlier is a nonvanishing Newman polynomial of length n .*

Proof. If $n + 2$ is not a power of 2, then $n + 2 = 2^v(2t + 1)$ for integers $v \geq 0$ and $t \geq 1$. We will choose $k = 2^v t - 1$, so $0 < k < n$. Now consider

$$\begin{aligned} \alpha(z) = \alpha_{n,k}(z) &= 1 + z + z^2 + \cdots + z^n - z^k = \frac{z^{n+1} - 1}{z - 1} - z^k, \\ (z - 1)\alpha(z) &= z^{n+1} - 1 - z^{k+1} + z^k. \end{aligned}$$

Suppose that $z \in \mathbb{S}$ is a zero of α . Then $z \neq 1$. Since $z^{n+1} - 1 - z^{k+1} + z^k = 0$, we have the following three cases by Lemma 4. We will show that each of the three cases leads to a contradiction.

Case 1. We have $z^{n+1} - 1 = 0$ and $-z^{k+1} + z^k = 0$. Then $-z^k(z - 1) = 0$, implying $z = 1$, a contradiction.

Case 2. We have $z^{n+1} - z^{k+1} = 0$ and $-1 + z^k = 0$. Then $z^{k+1}(z^{n-k} - 1) = 0$ and $z^k - 1 = 0$, implying $z^k = 1$ and $z^{n-k} = 1$. Then also $1 = z^{n-k}/z^k = z^{n-2k}$ and therefore $z^{t(n-2k)} = 1^t = 1$. This implies $1 = z^{t(n-2k)}/z^k = z^{t(n-2k)-k}$. But now observe that

$$\begin{aligned} t(n - 2k) - k &= t(2^v(2t + 1) - 2 - 2(2^v t - 1)) - (2^v t - 1) \\ &= t(2^v 2t + 2^v - 2 - 2^v 2t + 2) - 2^v t + 1 \\ &= t2^v - 2^v t + 1 = 1. \end{aligned}$$

Thus $z^1 = 1$, a contradiction.

Case 3. We have $z^{n+1} + z^k = 0$ and $-1 - z^{k+1} = 0$. Then $z^k(z^{n-k+1} + 1) = 0$ and $z^{k+1} + 1 = 0$, implying $z^{n-k+1} = -1$ and $z^{k+1} = -1$. By Lemma 6, we will obtain the desired contradiction if $\nu_2(n - k + 1) \neq \nu_2(k + 1)$. Now observe

$$\begin{aligned} n - k + 1 &= (2^v(2t + 1) - 2) - (2^v t - 1) + 1 \\ &= 2^v 2t + 2^v - 2 - 2^v t + 1 + 1 \\ &= 2^v t + 2^v = 2^v(t + 1) \end{aligned}$$

and $k + 1 = 2^v \cdot t$. Since t and $t + 1$ are of opposite parity, we have $\nu_2(2^v t) \neq \nu_2(2^v(t + 1))$. This completes Case 3. \square

Lemma 7 says that if $n > 2$ is not of the form $2^m - 2$, then n is of type A. The values of n that remain to be dealt with are those n of the form $2^m - 2$.

Lemma 8. *If $n = 2^m - 2$ where $m - 1$ is a composite number, then n can be written as the product of two integers of type A.*

Proof. First note that if $m - 1 = 4$, then $n = 2^m - 2 = 30 = 3 \cdot 10$, and both 3 and 10 are of type A. Now suppose $m - 1$ is a composite integer greater than 4. Then $m - 1 = ab$ where at least one of a, b is greater than 2. Without loss of generality, $a > 2$. Now consider $2^{m-1} - 1 = 2^{ab} - 1 = (2^a - 1)k$, where $k = 2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1 > 1$. Since $m - 1 \geq 3$ and $a \geq 3$, it follows that both $2^{m-1} - 1$ and $2^a - 1$ are congruent to 7 mod 8. This further implies that $k \equiv 1 \pmod{8}$. We can then write $n = 2(2^{m-1} - 1) = (2^a - 1) \cdot 2k$, where the two factors $2^a - 1$ and $2k$ are both greater than 2, and are congruent (mod 8) to 7 and 2 respectively. Thus neither factor is congruent to 6 mod 8, so neither factor is 2 less than a power of 2, so both factors are of type A. \square

Lemma 9. *If $n = 2^m - 2$ where $m - 1$ is an odd integer greater than 1, then n is of type B.*

Proof. If $n = 2^m - 2$ where $m - 1 > 1$ is odd, then $m > 2$ is even, so say $m = 2k$ where $k > 1$. Now consider

$$\alpha(z) = \beta_n(z) = 1 + z + z^2 + \dots + z^{n-2} + z^{n+2} = \frac{z^{n-1} - 1}{z - 1} + z^{n+2},$$

$$(z - 1)\alpha(z) = z^{n-1} - 1 + z^{n+3} - z^{n+2}.$$

Suppose that $z \in \mathbb{S}$ is a zero of α . Then $z \neq 1$. Since $z^{n-1} - 1 + z^{n+3} - z^{n+2} = 0$, we have the following three cases by Lemma 4. We will show that each of the three cases leads to a contradiction.

Case 1. We have $z^{n-1} - 1 = 0$ and $z^{n+3} - z^{n+2} = 0$. Then $z^{n+2}(z - 1) = 0$, implying $z = 1$, a contradiction.

Case 2. We have $z^{n-1} + z^{n+3} = 0$ and $-1 - z^{n+2} = 0$. Then $z^{n-1}(1 + z^4) = 0$ and $1 + z^{n+2} = 0$, implying $z^4 = -1$ and $z^{n+2} = -1$. By Lemma 6, we will obtain the desired contradiction if $\nu_2(4) \neq \nu_2(n + 2)$. But this follows because $n + 2 = 2^m$ where $m \geq 4$.

Case 3. We have $z^{n-1} - z^{n+2} = 0$ and $-1 + z^{n+3} = 0$. Then $z^{n-1}(1 - z^3) = 0$ and $z^{n+3} - 1 = 0$, implying $z^3 = 1$ and $z^{n+3} = 1$. Now note that

$$n + 3 = 2^m + 1 = 2^{2k} + 1 = 4^k + 1$$

which is congruent (mod 3) to $1^k + 1 = 2$. Therefore $n + 3 = 3\ell - 1$ for some ℓ . But then $1 = 1^\ell/1 = z^{3\ell}/z^{n+3} = z$ is the desired contradiction. \square

To recap, Lemma 7 takes care of those $n > 2$ that are not of the form $2^m - 2$. Then Lemmas 8 and 9 take care of all n of the form $2^m - 2$ except when $m - 1 \in \{1, 2\}$, i.e., $m \in \{2, 3\}$. But $n = 2^2 - 2 = 2$ is ignored, and $n = 2^3 - 2 = 6$ is taken care of by Lemma 5. Thus we have proved Theorem 2.

2. Further Remarks

We have proved that $\mu(n) > 0$ for all $n > 2$. We suspect that more is true, and in fact, we suspect that $\mu(n)$ approaches infinity with n . Even the conjecture that $\mu(n) > 1$ for all sufficiently large n remains unproved.

Using fairly straightforward brute-force search, we can show that $\mu(n) > 1$ for $6 \leq n \leq 20$. In the table below, for each $n \in \{6, \dots, 20\}$, we give a set A of n nonnegative integers such that the polynomial $\alpha(z) = \sum_{a \in A} z^a$ is a length n Newman polynomial satisfying $|\alpha(z)| > 1$ on \mathbb{S} . We remain ignorant of how to prove that such polynomials exist for all sufficiently large n .

n	A
6	{0, 1, 4, 5, 10, 12}
7	{0, 1, 5, 7, 9, 16, 19}
8	{0, 2, 4, 5, 6, 7, 10, 13}
9	{0, 1, 2, 3, 4, 7, 8, 10, 12}
10	{0, 1, 2, 3, 4, 6, 8, 9, 12, 13}
11	{0, 2, 3, 4, 5, 6, 8, 10, 11, 12, 15}
12	{0, 1, 2, 3, 5, 6, 7, 8, 12, 14, 15, 16}
13	{0, 1, 2, 3, 4, 6, 8, 9, 10, 11, 14, 15, 18}
14	{0, 1, 2, 3, 4, 5, 7, 9, 11, 12, 13, 16, 17, 19}
15	{0, 1, 2, 3, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 19}
16	{0, 1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 17, 20, 21}
17	{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 14, 15, 16, 20, 21, 22}
18	{0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 14, 15, 17, 19, 20, 21}
19	{0, 1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 15, 16, 18, 20, 21, 22, 24}
20	{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 15, 16, 17, 19, 21, 23, 24, 25}

References

[1] D.W. Boyd, *Large Newman polynomials*, in *Diophantine analysis (Kensington, 1985)*, 159–170, London Math. Soc. Lecture Note Ser., 109, Cambridge Univ. Press, Cambridge, 1986.

[2] D.M. Campbell, H.R.P. Ferguson & R.W. Forcade, *Newman polynomials on $|z| = 1$* , Indiana Univ. Math. J. **32** (1983), 517–525.

- [3] A. Dubickas, *Nonreciprocal algebraic numbers of small measure*, Comment. Math. Univ. Carolin. **45** (2004), no. 4, 693–697.
- [4] C. Finch and L. Jones, *On the irreducibility of $\{-1, 0, 1\}$ -quadrinomials*, Integers **6** (2006), A16, 4 pp.
- [5] B. Goddard, *Finite exponential series and Newman polynomials*, Proc. Amer. Math. Soc. **116** (1992), 313–320.
- [6] S. Konyagin, *On the number of irreducible polynomials with 0,1 coefficients*, Acta Arith. **88** (1999), no. 4, 333–350.
- [7] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.
- [8] I. Mercer, *Newman polynomials, reducibility, and roots on the unit circle*, Integers **12** (2012), A6, 16 pp.
- [9] A. Odlyzko and B. Poonen, *Zeros of polynomials with 0,1 coefficients*, Enseign. Math. (2) **39** (1993), no. 3–4, 317–348.