#A6 INTEGERS 12 (2012)

NEWMAN POLYNOMIALS, REDUCIBILITY, AND ROOTS ON THE UNIT CIRCLE

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

Received: 7/11/11, Accepted: 12/14/11, Published: 1/2/12

Abstract

A *length k Newman polynomial* is any polynomial of the form $z^{a_1} + \cdots + z^{a_k}$ (where $a_1 < \cdots < a_k$). Some Newman polynomials are reducible over the rationals, and some are not. Some Newman polynomials have roots on the unit circle, and some do not. Defining, in a natural way, what we mean by the "proportion" of length k Newman polynomials with a given property, we prove that

- 1/4 of length 3 Newman polynomials are reducible over the rationals
- 1/4 of length 3 Newman polynomials have roots on the unit circle
- 3/7 of length 4 Newman polynomials are reducible over the rationals
- 3/7 of length 4 Newman polynomials have roots on the unit circle

We also show that certain plausible conjectures imply that the proportion of length 5 Newman polynomials with roots on the unit circle is 909/9464.

1. Introduction

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

$$P(z) = z^{a_1} + z^{a_2} + \cdots + z^{a_k} \qquad (a_1 < a_2 < \cdots < a_k)$$

and $\mathbb{S}$ denotes the unit circle in the complex plane. Some Newman polynomials have roots on $\mathbb{S}$, and some do not. Some are reducible, and some are not. (Throughout this paper, "reducible" means "reducible over $\mathbb{Q}$" and hence also "reducible over $\mathbb{Z}$".)

If $a_1 > 0$, then $P(z)$ is trivially reducible. The factor $1 + z^{a_2-a_1} + \cdots + z^{a_k-a_1}$ has the same roots as $P(z)$ except for a root at 0. Thus, we will sometimes restrict our attention to the case $a_1 = 0$.

Other authors have explored necessary or sufficient conditions for Newman polynomials of small length to be reducible [2, 3, 6, 8, 10]. In this paper, we are interested in the questions: (1) What proportion of Newman polynomials are reducible? (2) What proportion of Newman polynomials have roots on the unit circle?

To make this more precise, we introduce some notation. If N is a positive integer, we define

$$\mathrm{Newm}_3(N) = \left\{1 + z^a + z^b \;\middle|\; 1 \le a < b \le N\right\}$$
$$\mathrm{Newm}_4(N) = \left\{1 + z^a + z^b + z^c \;\middle|\; 1 \le a < b < c \le N\right\}$$
$$\mathrm{Newm}_k(N) = \left\{1 + z^{a_1} + \cdots + z^{a_{k-1}} \;\middle|\; 1 \le a_1 < \cdots < a_{k-1} \le N\right\}$$

so $|\mathrm{Newm}_k(N)| = \binom{N}{k-1}$. We also define $\mathrm{Newm}_k(\infty) = \bigcup\limits_N \mathrm{Newm}_k(N)$.

A root on $\mathbb{S}$ is a root of unit modulus, or a *unimodular* root. A polynomial with at least one unimodular root will sometimes be called a *UR polynomial*. We then define

$$\mathrm{NewmRed}_k(N) = \left\{P(z) \in \mathrm{Newm}_k(N) \;\middle|\; P(z) \text{ is reducible}\right\}$$
$$\mathrm{NewmUR}_k(N) = \left\{P(z) \in \mathrm{Newm}_k(N) \;\middle|\; P(z) \text{ is UR}\right\}$$

as well as

$$\mathrm{NewmRed}_k(\infty) = \bigcup_N \mathrm{NewmRed}_k(N)$$
$$\mathrm{NewmUR}_k(\infty) = \bigcup_N \mathrm{NewmUR}_k(N).$$

We further define

$$\mathrm{ProbRed}_k(N) = \frac{|\mathrm{NewmRed}_k(N)|}{|\mathrm{Newm}_k(N)|}$$
$$\mathrm{ProbRed}_k(\infty) = \lim_{N\to\infty} \mathrm{ProbRed}_k(N)$$
$$\mathrm{ProbUR}_k(N) = \frac{|\mathrm{NewmUR}_k(N)|}{|\mathrm{Newm}_k(N)|}$$
$$\mathrm{ProbUR}_k(\infty) = \lim_{N\to\infty} \mathrm{ProbUR}_k(N)$$

which we can informally regard as the probability that a Newman polynomial of length k is reducible or UR, as appropriate.

Other authors [5, 9] have asked what proportion of Newman polynomials are reducible. However, they considered the set of all 2^N Newman polynomials of degree at most N, which in our notation would be $\bigcup_k \mathrm{Newm}_k(N)$. In this paper, we consider Newman polynomials of fixed length.

As the main results of this paper, we prove

$$\mathrm{ProbUR}_3(\infty) = \mathrm{ProbRed}_3(\infty) = \frac{1}{4}$$

$$\mathrm{ProbUR}_4(\infty) = \mathrm{ProbRed}_4(\infty) = \frac{3}{7}.$$

We also show that $\mathrm{ProbUR}_5(\infty) \geq 0.096$ and explore some conjectures.

2. Notation and Terminology

We will use $\mathbf{e}_k$ to denote $\exp(2\pi i/k)$. Note that in general, $\mathbf{e}_k^a = \mathbf{e}_k^b$ if and only if $a \equiv b \pmod{k}$. We also always have $\mathbf{e}_k^a = \mathbf{e}_{tk}^{ta}$.

For any integer $m \geq 2$, we denote the integers modulo m by

$$\mathbb{Z}/m = \{0, 1, \ldots, m-1\}.$$

Throughout this document, if we write *coset* with no further explanation, we mean a coset of some nontrivial subgroup of the additive group $\mathbb{Z}/m$. Sometimes the value of m will be understood from the context; if not, we will refer to a *mod m coset*. For example, "mod 6 coset" means any of the following subsets of $\mathbb{Z}/6$

$$\{0,3\} \qquad \{1,4\} \qquad \{2,5\} \qquad \{0,2,4\} \qquad \{1,3,5\} \qquad \{0,1,2,3,4,5\}.$$

We note that if $A = \{a_1, \ldots, a_k\}$ is any mod m coset, then $k \neq 1$ is a divisor of m, and we have

$$\sum_{a \in A} \zeta^a = 0$$

if ζ is a primitive mth root of 1.

We allow curly brackets to denote multisets, where multiplicity matters but order does not matter. For instance, we have

$$\{0,2,3,4,0\} = \{0,0,2,3,4\} \neq \{0,2,3,4\}.$$

The size of a multiset counts repetition, so we say $\{0,0,2,3,4\}$ has size 5.

We use round brackets to denote tuples, where order matters. For example,

$$(0,2,3,4,0) \neq (0,0,2,3,4).$$

We define union of multisets in the obvious way. For example, we have

$$\{0,2,4\} \cup \{0,3\} = \{0,0,2,3,4\}.$$

For multisets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$, we say A and B are *congruent mod* m if, after relabeling if necessary, we have $a_i \equiv b_i \pmod{m}$ for all i. We sometimes abbreviate this by $A \equiv_m B$. For example, we have

$$\{0, 0, 2, 3, 4\} \equiv_6 \{0, 2, 3, 4, 6\}.$$

If $A = (a_1, \ldots, a_k)$ and $B = (b_1, \ldots, b_k)$ are tuples, we say A and B are congruent mod m if we have $a_i \equiv b_i \pmod{m}$ for all i without relabeling. For example,

$$(0, 2, 3, 4, 6) \equiv_6 (0, 2, 3, 4, 0) \not\equiv_6 (0, 0, 2, 3, 4).$$

Let A and B be multisets. If $A \equiv_m B$ and ζ is any mth root of 1, we have

$$\sum_{a \in A} \zeta^a = \sum_{b \in B} \zeta^b.$$

Also, if ζ is a primitive mth root of 1 and A is a union of mod m cosets, then

$$\sum_{a \in A} \zeta^a = 0.$$

(Interestingly, the converse is not true: $P(z) = 1 + z + z^7 + z^{13} + z^{19} + z^{20}$ vanishes at $\mathbf{e}_{30}$, but $\{0, 1, 7, 13, 19, 20\}$ is not a union of mod 30 cosets.)

In this paper, "polynomial" will always be understood to mean "over $\mathbb{Q}$". Given a polynomial $P(z)$ of degree d, we define the *reciprocal* of $P(z)$ to be $\tilde{P}(z) = z^d P(z^{-1})$. If $P(0) \neq 0$, then $\tilde{P}(z)$ has degree d, and the roots of $\tilde{P}(z)$ are the reciprocals of the roots of $P(z)$. If $P(z) = \tilde{P}(z)$, we say $P(z)$ is *reciprocal*.

3. Earlier Results

The following is well-known.

Lemma 1. *If $P(z) \neq z - 1$ is an irreducible UR polynomial, then $P(z)$ is reciprocal.*

Proof. If $P(z) = \kappa_d z^d + \cdots + \kappa_0$ is irreducible, then $\kappa_0 \neq 0$. If $P(\zeta) = 0$ for some $\zeta \in \mathbb{S}$, then $P(z)$ is the minimal polynomial for both ζ and $\overline{\zeta}$. Then $\tilde{P}(z)$ vanishes at $1/\zeta = \overline{\zeta}$, so $\tilde{P}(z)$ must be a multiple of $P(z)$, which implies $\tilde{P}(z) = (\kappa_0/\kappa_d)P(z) \Longrightarrow \kappa_0^2 = \kappa_d^2 \Longrightarrow \kappa_0 = \pm\kappa_d$, so $\tilde{P}(z) = \pm P(z)$. If $\tilde{P}(z) = -P(z)$, we can conclude that $P(1) = 0$. □

We will let $\Phi_k(z)$ denote the kth cyclotomic polynomial, which is the minimal polynomial for $\mathbf{e}_k$. The roots of $\Phi_k(z)$ are the primitive kth roots of unity; there are $\phi(k)$ of those, where ϕ is the Euler totient function.

The next result follows straightforwardly from basic properties of cyclotomic polynomials. We omit the proof.

Lemma 2. *We have*

$$\Phi_k(1) = \begin{cases} p & \text{if } k \text{ is a prime power } p^m \\ 1 & \text{if } k \text{ is divisible by more than one prime.} \end{cases}$$

Of interest to us is the following consequence.

Corollary 3. *The polynomials in* $\mathrm{Newm}_3(\infty)$ *that are cyclotomic are the polynomials* $\Phi_3(z), \Phi_9(z), \Phi_{27}(z), \ldots$. *There are no polynomials in* $\mathrm{Newm}_4(\infty)$ *that are cyclotomic. The polynomials in* $\mathrm{Newm}_5(\infty)$ *that are cyclotomic are the polynomials* $\Phi_5(z), \Phi_{25}(z), \Phi_{125}(z), \ldots$.

We also have the next result, which has a simple geometric proof. The second part of our Lemma 4 is equivalent to Lemma 1 in [1] and to Lemma 1 in [3], but our proof is different.

Lemma 4. *Let* α, β, γ *denote complex numbers of modulus* 1*.*

- *If* $1 + \alpha + \beta = 0$*, then one of* α, β *is* $\mathbf{e}_3$*.*
- *If* $1 + \alpha + \beta + \gamma = 0$*, then one of* α, β, γ *is* -1*.*

Proof. Suppose $1 + \alpha + \beta = 0$. Note that $\alpha \neq \pm 1$. Thus the points 0, 1, and $1 + \alpha$ form a triangle. The triangle has side lengths 1, $|\alpha|$, $|\beta|$ and hence is equilateral. The first claim follows.

Now suppose $1 + \alpha + \beta + \gamma = 0$. If all of α, β, γ are ± 1, we are done, so suppose $\alpha \neq \pm 1$. Then the points $A = 0$, $B = 1$, $C = 1 + \alpha$ form a triangle. Note AB has length 1 and BC has length $|\alpha| = 1$. Let D be the point $1 + \alpha + \beta$. Note CD has length $|\beta| = 1$ and DA has length $|\gamma| = 1$. It follows that triangles ABC and ADC are congruent. Then ABC and ADC either coincide, or they form a rhombus. Either way, the second claim follows. □

There is no counterpart to Lemma 4 for sums of five complex numbers. Note that $P(z) = 1 + z + z^3 + z^5 + z^6$ has roots on $\mathbb{S}$ that are not roots of unity.

The next result appears in [6]. We omit the proof.

Proposition 5. *If a Newman polynomial of length 3 or 4 is reducible, then it has a cyclotomic factor (equivalently, it vanishes at some root of unity).*

The proof of Proposition 5 does not seem to generalize to the length 5 case. However, I cannot find a reducible length 5 Newman polynomial without a cyclotomic factor.

Conjecture 6. If a Newman polynomial of length 5 is reducible, then it has a cyclotomic factor.

Conjecture 6 is true for all length 5 Newman polynomials of degree up to 24. From Theorem 1 in [2], we know that for a reducible length 5 Newman polynomial, at most one of its irreducible factors is non-reciprocal.

4. Main Results

Theorem 7. *We have the following four results.*

1. $\mathrm{NewmUR}_3(\infty) =$
$\left\{1 + z^a + z^b \;\middle|\; \{0, a, b\} \equiv \{0,\ 3^{k-1},\ 2 \cdot 3^{k-1}\} \text{ (mod } 3^k\text{) for some } k\right\}$

2. $\mathrm{NewmRed}_3(\infty) = \mathrm{NewmUR}_3(\infty) \setminus \{\Phi_3(z), \Phi_9(z), \Phi_{27}(z), \ldots\}$

3. $\mathrm{NewmRed}_4(\infty) =$
$\left\{1 + z^a + z^b + z^c \;\middle|\; \{0, a, b, c\} \equiv \{0, 0, 2^{k-1}, 2^{k-1}\} \text{ (mod } 2^k\text{) for some } k\right\}$

4. $\mathrm{NewmUR}_4(\infty) = \mathrm{NewmRed}_4(\infty)$.

Result 1 is equivalent to part 1 of Theorem 3 in [10], where it is stated without proof. Result 3 is equivalent to part 1 of Theorem 2 in [3]. Our proof of Theorem 7 at one point uses a crucial trick taken from the proof of Theorem 2 in [3].

Proof. We will prove results 1 and 2 first. For brevity, define

$$A = \left\{1 + z^a + z^b \;\middle|\; \{0, a, b\} \equiv \{0,\ 3^{k-1},\ 2 \cdot 3^{k-1}\} \pmod{3^k} \text{ for some } k\right\}.$$

Note that $A \subseteq \mathrm{NewmUR}_3(\infty)$ because a polynomial in A must vanish at $\mathbf{e}_{3^k}$. Next, suppose $P(z) = 1+z^a+z^b \in \mathrm{NewmUR}_3(\infty)$. To show $\mathrm{NewmUR}_3(\infty) \subseteq A$, we must show $\{0, a, b\} \equiv \{0,\ 3^{k-1},\ 2 \cdot 3^{k-1}\} \pmod{3^k}$ for some k. Let $a = 3^k a'$, $b = 3^k b'$, where a', b' are not both divisible by 3. Since $P(z)$ is UR, we have $1 + \zeta^a + \zeta^b = 0$ for some $\zeta \in \mathbb{S}$. By Lemma 4, ζ^a and ζ^b are equal to $\mathbf{e}_3$ and $\mathbf{e}_3^2$ in some order; say $\zeta^a = \mathbf{e}_3$ and $\zeta^b = \mathbf{e}_3^2$. Then note that $\zeta^{2b} = \mathbf{e}_3$. Thus,

$$\mathbf{e}_3^{a'} = (\zeta^{2b})^{a'} = (\zeta^a)^{2b'} = \mathbf{e}_3^{2b'}$$

so $a' \equiv 2b' \pmod 3$. Then either $(a', b') \equiv_3 (1, 2)$ or $(a', b') \equiv_3 (2, 1)$, implying $\{0, a, b\} \equiv_{3^k} \{0,\ 3^{k-1},\ 2 \cdot 3^{k-1}\}$ as required. This proves result 1. Note that we have also shown that if $P(z) \in \mathrm{NewmUR}_3(\infty)$, then $P(z)$ vanishes at $\mathbf{e}_{3^k}$ for some k, so $P(z)$ is divisible by $\Phi_{3^k}(z)$. So if $P(z)$ is not itself of the form $\Phi_{3^k}(z)$, then $P(z)$ is reducible. We have thus shown

$$\mathrm{NewmUR}_3(\infty) \setminus \{\Phi_3(z), \Phi_9(z), \Phi_{27}(z), \ldots\} \subseteq \mathrm{NewmRed}_3(\infty)$$

and the reverse inclusion follows from Proposition 5 (note that a reducible polynomial is not cyclotomic). This proves result 2.

Next, we prove results 3 and 4. Define

$$B = \left\{1 + z^a + z^b + z^c \;\middle|\; \{0, a, b, c\} \equiv \{0, 0, 2^{k-1}, 2^{k-1}\} \pmod{2^k} \text{ for some } k\right\}.$$

If $P(z) \in B$, then $P(z)$ vanishes at $\mathbf{e}_{2^k}$, so $P(z)$ is divisible by the cyclotomic polynomial $\Phi_{2^k}(z)$. By Corollary 3, $P(z)$ is not itself cyclotomic. Therefore $P(z)$ is reducible. We have thus shown

$$B \subseteq \mathrm{NewmUR}_4(\infty) \subseteq \mathrm{NewmRed}_4(\infty).$$

Next, we show the reverse inclusions. If $P(z) \in \mathrm{NewmRed}_4(\infty)$, then by Proposition 5, we must have $P(z) \in \mathrm{NewmUR}_4(\infty)$. Now suppose $P(z) = 1+z^a+z^b+z^c \in \mathrm{NewmUR}_4(\infty)$. We must show $\{0, a, b, c\} \equiv \{0, 0, 2^{k-1}, 2^{k-1}\} \pmod{2^k}$ for some k. Let $a = 2^{k-1}a'$, $b = 2^{k-1}b'$, $c = 2^{k-1}c'$, where not all of a', b', c' are divisible by 2. It suffices to show $\{a', b', c'\} \equiv_2 \{0, 1, 1\}$, i.e. exactly one of a', b', c' is even. Since $P(z)$ is UR, then $1+\zeta^a+\zeta^b+\zeta^c = 0$ for some $\zeta \in \mathbb{S}$. By Lemma 4, one of $\zeta^a, \zeta^b, \zeta^c$ is -1; say $\zeta^a = -1$. Then also $\zeta^b + \zeta^c = 0$, implying $\zeta^{c-b} = -1$. As in the proof of Theorem 2 in [3], we then have

$$(-1)^{a'} = (\zeta^{c-b})^{a'} = (\zeta^a)^{c'-b'} = (-1)^{c'-b'}$$

so $a' \equiv_2 c' - b'$. If a' is even, then b', c' have the same parity. They cannot both be even, so $\{a', b', c'\} \equiv_2 \{0, 1, 1\}$. On the other hand, if a' is odd, then b', c' have opposite parity. So again $\{a', b', c'\} \equiv_2 \{0, 1, 1\}$. This completes the proof of results 3 and 4. □

From Theorem 7, we conclude that if $P(z) = 1 + z^a + z^b$ is a UR Newman polynomial of length 3, then one of the following conditions must hold:

$$\begin{gathered}\{0, a, b\} \equiv_3 \{0, 1, 2\}\\ \{0, a, b\} \equiv_9 \{0, 3, 6\}\\ \{0, a, b\} \equiv_{27} \{0, 9, 18\}.\\ \vdots\end{gathered}$$

Note that this list of conditions is pairwise disjoint. Similarly, we conclude that if $P(z) = 1 + z^a + z^b + z^c$ is a UR Newman polynomial of length 4, then one of the following conditions must hold:

$$\begin{gathered}\{0, a, b, c\} \equiv_2 \{0, 0, 1, 1\}\\ \{0, a, b, c\} \equiv_4 \{0, 0, 2, 2\}\\ \{0, a, b, c\} \equiv_8 \{0, 0, 4, 4\}.\\ \vdots\end{gathered}$$

This list of conditions is also pairwise disjoint.

That is what allows us to find the proportion of polynomials in $\mathrm{Newm}_3(N)$ or $\mathrm{Newm}_4(N)$ that are UR. To state this precisely, we introduce more notation. If N

is a positive integer, we define

$$\mathrm{Perm}_k(N) = \Big\{(a_1, \ldots, a_{k-1}) \;\Big|\; \text{the } a_i \text{ are distinct and } 1 \le a_i \le N\Big\},$$

where we do not assume $a_1 < a_2 < \cdots$. Note that $|\mathrm{Perm}_k(N)| = (k-1)!\binom{N}{k-1}$. We then define a function $F : \mathrm{Perm}_k(N) \to \mathrm{Newm}_k(N)$ by

$$F((a_1, \ldots, a_{k-1})) = 1 + z^{a_1} + \cdots + z^{a_{k-1}}.$$

The pre-image of each polynomial in $\mathrm{Newm}_k(N)$ consists of $(k-1)!$ different tuples in $\mathrm{Perm}_k(N)$.

Lemma 8. *Let $\mathcal{P}$ be any property of the form*

$$\{a_1, \ldots, a_{k-1}\} \equiv_m \{u_1, \ldots, u_{k-1}\},$$

where m and the u_i are constants. Let $\mathrm{GoodPerm}_k(N)$ be the set of tuples in $\mathrm{Perm}_k(N)$ that satisfy $\mathcal{P}$, and let $\mathrm{GoodNewm}_k(N)$ be the set of polynomials in $\mathrm{Newm}_k(N)$ that satisfy $\mathcal{P}$. Then

$$\frac{|\mathrm{GoodNewm}_k(N)|}{|\mathrm{Newm}_k(N)|} = \frac{|\mathrm{GoodPerm}_k(N)|}{|\mathrm{Perm}_k(N)|}.$$

Proof. A polynomial $P(z) \in \mathrm{Newm}_k(N)$ satisfies $\mathcal{P}$ if and only if all $(k-1)!$ tuples in $F^{-1}(P(z))$ satisfy $\mathcal{P}$. Therefore

$$|\mathrm{GoodPerm}_k(N)| = (k-1)!\,|\mathrm{GoodNewm}_k(N)|\,.$$

Since also $|\mathrm{Perm}_k(N)| = (k-1)!\,|\mathrm{Newm}_k(N)|$, the result follows. □

Lemma 9. *Let $\mathcal{P}$ be any property of the form*

$$(a_1, \ldots, a_{k-1}) \equiv_m (u_1, \ldots, u_{k-1}),$$

where m and the u_i are constants. Let $\mathrm{GoodPerm}_k(N)$ be the set of tuples in $\mathrm{Perm}_k(N)$ that satisfy $\mathcal{P}$. Then

$$\lim_{N\to\infty} \frac{|\mathrm{GoodPerm}_k(N)|}{|\mathrm{Perm}_k(N)|} = \frac{1}{m^{k-1}}.$$

Proof. Construct such a $(k-1)$-tuple by first choosing a_1, then choosing a_2, and so on. We must have $1 \le a_1 \le N$ and $a_1 \equiv_m u_1$. If W_1 is the number of ways to choose a_1, we have

$$\frac{N}{m} - 1 \le \left\lfloor \frac{N}{m} \right\rfloor \le W_1 \le \left\lceil \frac{N}{m} \right\rceil \le \frac{N}{m} + 1.$$

Next, we must have $1 \le a_2 \le N$, $a_2 \equiv_m u_2$, and $a_2 \ne a_1$. If W_2 is the number of ways to choose a_2, we have

$$\frac{N}{m} - 2 \le \left\lfloor \frac{N}{m} \right\rfloor - 1 \le W_2 \le \left\lceil \frac{N}{m} \right\rceil \le \frac{N}{m} + 1.$$

Continuing in this way, we find that

$$\left(\frac{N}{m} - 1\right)\left(\frac{N}{m} - 2\right) \cdots \left(\frac{N}{m} - k + 1\right) \le |\mathrm{GoodPerm}_k(N)| \le \left(\frac{N}{m} + 1\right)^{k-1}.$$

The upper and lower bound are both of the form

$$\frac{1}{m^{k-1}} N^{k-1} + O(N^{k-2})$$

whereas $|\mathrm{GoodPerm}_k(N)| \sim N^{k-1}$. The result follows. □

Theorem 10. *We have*

$$\mathrm{ProbUR}_3(\infty) = \lim_{N\to\infty} \frac{|\mathrm{NewmUR}_3(N)|}{|\mathrm{Newm}_3(N)|} = \frac{1}{4},$$

$$\mathrm{ProbUR}_4(\infty) = \lim_{N\to\infty} \frac{|\mathrm{NewmUR}_4(N)|}{|\mathrm{Newm}_4(N)|} = \frac{3}{7}.$$

Proof. The set $\mathrm{NewmUR}_3(N)$ is the disjoint union of the sets

$$\begin{aligned}
A_1 &= \left\{ 1 + z^a + z^b \in \mathrm{Newm}_3(N) \;\middle|\; \{a, b\} \equiv_3 \{1, 2\} \right\} \\
A_2 &= \left\{ 1 + z^a + z^b \in \mathrm{Newm}_3(N) \;\middle|\; \{a, b\} \equiv_9 \{3, 6\} \right\} \\
A_3 &= \left\{ 1 + z^a + z^b \in \mathrm{Newm}_3(N) \;\middle|\; \{a, b\} \equiv_{27} \{9, 18\} \right\} \\
&\vdots
\end{aligned}$$

so we have

$$\frac{|\mathrm{NewmUR}_3(N)|}{|\mathrm{Newm}_3(N)|} = \frac{|A_1|}{|\mathrm{Newm}_3(N)|} + \frac{|A_2|}{|\mathrm{Newm}_3(N)|} + \frac{|A_3|}{|\mathrm{Newm}_3(N)|} + \cdots$$

By Lemma 8, we have

$$\frac{|A_k|}{|\mathrm{Newm}_3(N)|} = \frac{|B_k|}{|\mathrm{Perm}_3(N)|},$$

where

$$B_k = \left\{ (a, b) \in \mathrm{Perm}_3(N) \;\middle|\; \{a, b\} \equiv_{3^k} \{3^{k-1},\ 2 \cdot 3^{k-1}\} \right\}.$$

Each set B_k is the disjoint union of the sets

$$C_k = \Big\{(a,b) \in \mathrm{Perm}_3(N) \;\Big|\; (a,b) \equiv_{3^k} (3^{k-1},\ 2{\cdot}3^{k-1})\Big\},$$
$$D_k = \Big\{(a,b) \in \mathrm{Perm}_3(N) \;\Big|\; (a,b) \equiv_{3^k} (2{\cdot}3^{k-1},\ 3^{k-1})\Big\}.$$

We conclude that $\dfrac{|\mathrm{NewmUR}_3(N)|}{|\mathrm{Newm}_3(N)|} =$

$$\frac{|C_1|}{|\mathrm{Perm}_3(N)|} + \frac{|D_1|}{|\mathrm{Perm}_3(N)|} + \frac{|C_2|}{|\mathrm{Perm}_3(N)|} + \frac{|D_2|}{|\mathrm{Perm}_3(N)|} + \cdots$$

By Lemma 9, when $N \to \infty$, the terms of this series approach

$$\frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{9^2} + \frac{1}{9^2} + \frac{1}{27^2} + \frac{1}{27^2} + \cdots = \frac{1}{4}.$$

Similarly, the set $\mathrm{NewmUR}_4(N)$ is the disjoint union of the sets

$$E_1 = \Big\{1 + z^a + z^b + z^c \in \mathrm{Newm}_4(N) \;\Big|\; \{a,b,c\} \equiv_2 \{0,1,1\}\Big\}$$
$$E_2 = \Big\{1 + z^a + z^b + z^c \in \mathrm{Newm}_4(N) \;\Big|\; \{a,b,c\} \equiv_4 \{0,2,2\}\Big\}$$
$$E_3 = \Big\{1 + z^a + z^b + z^c \in \mathrm{Newm}_4(N) \;\Big|\; \{a,b,c\} \equiv_8 \{0,4,4\}\Big\}$$
$$\vdots$$

so we have

$$\frac{|\mathrm{NewmUR}_4(N)|}{|\mathrm{Newm}_4(N)|} = \frac{|E_1|}{|\mathrm{Newm}_4(N)|} + \frac{|E_2|}{|\mathrm{Newm}_4(N)|} + \frac{|E_3|}{|\mathrm{Newm}_4(N)|} + \cdots$$

By Lemma 8, we have

$$\frac{|E_k|}{|\mathrm{Newm}_4(N)|} = \frac{|F_k|}{|\mathrm{Perm}_4(N)|},$$

where

$$F_k = \Big\{(a,b,c) \in \mathrm{Perm}_4(N) \;\Big|\; \{a,b,c\} \equiv_{2^k} \{0, 2^{k-1}, 2^{k-1}\}\Big\}.$$

Each set F_k is the disjoint union of the sets

$$G_k = \Big\{(a,b,c) \in \mathrm{Perm}_4(N) \;\Big|\; (a,b,c) \equiv_{2^k} (0, 2^{k-1}, 2^{k-1})\Big\},$$
$$H_k = \Big\{(a,b,c) \in \mathrm{Perm}_4(N) \;\Big|\; (a,b,c) \equiv_{2^k} (2^{k-1}, 0, 2^{k-1})\Big\},$$
$$I_k = \Big\{(a,b,c) \in \mathrm{Perm}_4(N) \;\Big|\; (a,b,c) \equiv_{2^k} (2^{k-1}, 2^{k-1}, 0)\Big\}.$$

We conclude that $\dfrac{|\mathrm{NewmUR}_4(N)|}{|\mathrm{Newm}_4(N)|} = \dfrac{|G_1| + |H_1| + |I_1|}{|\mathrm{Perm}_4(N)|} + \dfrac{|G_2| + |H_2| + |I_2|}{|\mathrm{Perm}_4(N)|} + \cdots.$

By Lemma 9, when $N \to \infty$, the terms of this series approach

$$\frac{3}{2^3} + \frac{3}{4^3} + \frac{3}{8^3} + \cdots = \frac{3}{7}. \qquad \square$$

Corollary 11. *We have*

$$\mathrm{ProbRed}_3(\infty) = \lim_{N\to\infty} \frac{|\mathrm{NewmRed}_3(N)|}{|\mathrm{Newm}_3(N)|} = \frac{1}{4},$$

$$\mathrm{ProbRed}_4(\infty) = \lim_{N\to\infty} \frac{|\mathrm{NewmRed}_4(N)|}{|\mathrm{Newm}_4(N)|} = \frac{3}{7}.$$

Proof. The second claim follows immediately from Theorem 10 and from result 4 in Theorem 7. As for the first claim, note that because of result 2 in Theorem 7, it would suffice to prove

$$\lim_{N\to\infty} \frac{|\mathrm{Cycl}_3(N)|}{|\mathrm{Newm}_3(N)|} = 0,$$

where $\mathrm{Cycl}_3(N)$ is the set of polynomials in $\mathrm{Newm}_3(N)$ that are cyclotomic. But the polynomials in $\mathrm{Cycl}_3(N)$ are the polynomials of the form

$$1 + z^{3^{k-1}} + z^{2\cdot 3^{k-1}},$$

where $2 \cdot 3^{k-1} \leq N$, so $k \leq 1 + \log_3(N/2)$. That is, we have $|\mathrm{Cycl}_3(N)| \sim \log_3 N$, whereas $|\mathrm{Newm}_3(N)| \sim N^2/2$. The result follows. $\square$

5. The Length 5 Case

It is conceivable that there is no simple necessary and sufficient condition for a polynomial in $\mathrm{Newm}_5(\infty)$ to be UR. However, we can exhibit some particular families of polynomials in $\mathrm{Newm}_5(\infty)$ that are UR.

We define

$$\begin{aligned} A_N &= \left\{ P(z) \in \mathrm{Newm}_5(N) \;\middle|\; P(z) \text{ is reciprocal} \right\} \\ &= \left\{ 1 + z^{m-k} + z^m + z^{m+k} + z^{2m} \;\middle|\; 2 \leq m \leq \left\lfloor \frac{N}{2} \right\rfloor, 1 \leq k \leq m-1 \right\}. \end{aligned}$$

and then define $A = \bigcup_N A_N$. Such polynomials are always UR. (See, for example, Corollary 2 in [4] or Corollary 5 in [7].)

Notice that A is a "small" set. We have $|A_N| = O(N^2)$ because there are at most $N/2$ ways to choose m and at most $N/2$ ways to choose k. It follows that $|A_N| \,/\, |\mathrm{Newm}_5(N)|$ approaches 0 as $N \to \infty$.

We also define B_1, B_2, B_3, ... to be the sets of polynomials $1 + z^a + z^b + z^c + z^d$ in $\mathrm{Newm}_5(\infty)$ that satisfy, respectively, the conditions

$$\begin{gathered}
\{0, a, b, c, d\} \equiv_5 \{0, 1, 2, 3, 4\} \\
\{0, a, b, c, d\} \equiv_{25} \{0, 5, 10, 15, 20\} \\
\{0, a, b, c, d\} \equiv_{125} \{0, 25, 50, 75, 100\} \\
\vdots
\end{gathered}$$

Each polynomial in B_k is UR because it vanishes at $\mathbf{e}_{5^k}$.

We also define C_6, C_{12}, C_{18}, C_{24}, C_{36}, ... (the subscripts are of the form $2^k 3^\ell$) to be the sets of polynomials $1 + z^a + z^b + z^c + z^d$ in $\mathrm{Newm}_5(\infty)$ that satisfy, respectively, the conditions

$$\begin{gathered}
\{0, a, b, c, d\} \equiv_6 \big(\text{some coset of } \{0, 3\}\big) \cup \big(\text{some coset of } \{0, 2, 4\}\big) \\
\{0, a, b, c, d\} \equiv_{12} \big(\text{some coset of } \{0, 6\}\big) \cup \big(\text{some coset of } \{0, 4, 8\}\big) \\
\{0, a, b, c, d\} \equiv_{18} \big(\text{some coset of } \{0, 9\}\big) \cup \big(\text{some coset of } \{0, 6, 12\}\big) \\
\{0, a, b, c, d\} \equiv_{24} \big(\text{some coset of } \{0, 12\}\big) \cup \big(\text{some coset of } \{0, 8, 16\}\big) \\
\{0, a, b, c, d\} \equiv_{36} \big(\text{some coset of } \{0, 18\}\big) \cup \big(\text{some coset of } \{0, 12, 24\}\big) \\
\vdots
\end{gathered}$$

Each polynomial in $C_{2^k 3^\ell}$ is UR because it vanishes at $\mathbf{e}_{2^k 3^\ell}$.

We thus have $A \cup \big(B_1 \cup B_2 \cup \cdots\big) \cup \big(C_6 \cup C_{12} \cup \cdots\big) \subseteq \mathrm{NewmUR}_5(\infty)$.

For brevity, define $B = B_1 \cup B_2 \cup \cdots$ and $C = C_6 \cup C_{12} \cup \cdots$. Also for brevity, if S is any subset of $\mathrm{Newm}_5(\infty)$, we refer to

$$\lim_{N\to\infty} \frac{|S \cap \mathrm{Newm}_5(N)|}{|\mathrm{Newm}_5(N)|}$$

as the "probability" that a length 5 Newman polynomial is in S, or even more briefly, the "measure" of S.

Since $A \cup B \cup C \subseteq \mathrm{NewmUR}_5(\infty)$, a lower bound for $\mathrm{ProbUR}_5(\infty)$ will be the measure of $A \cup B \cup C$. The remarks after the definition of A show that the measure of A is 0. Therefore we are interested in the measure of $B \cup C$.

It is possible to prove that the measure of $B \cup C$ is

$$\begin{gathered}
(\text{measure of } B) + (\text{measure of } C) - (\text{measure of } B \cap C) \\
= \frac{1}{26} + \frac{109}{1820} - \frac{1}{26} \cdot \frac{109}{1820} = \frac{909}{9464} \approx 0.096.
\end{gathered}$$

We give a sketch of the proof later.

At this point, we assemble a few facts and conjectures.

Conjecture 12. $\mathrm{NewmUR}_5(\infty) = A \cup B \cup C$.

Conjecture 13. If $P(z) \in \mathrm{NewmUR}_5(\infty)$ has a cyclotomic factor, then $P(z) \in B \cup C$.

Proposition 14. *If Conjecture 6 and Conjecture 13 are both true, then Conjecture 12 is true.*

Proof. Suppose $P(z) \in \mathrm{NewmUR}_5(\infty)$. Either $P(z)$ is reducible, or $P(z)$ is irreducible. If the former, then Conjecture 6 implies $P(z)$ has a cyclotomic factor, and then Conjecture 13 implies $P(z) \in B \cup C$. If the latter, then Lemma 1 implies $P(z)$ is reciprocal, so $P(z) \in A$. □

Proposition 15. *For any k, we have* $\mathrm{ProbUR}_k(\infty) \leq \mathrm{ProbRed}_k(\infty)$.

Proof. We sketch a proof. It suffices to show $\mathrm{NewmUR}_k(\infty)$ is "almost" a subset of $\mathrm{NewmRed}_k(\infty)$, in the sense that "most" UR Newman polynomials are reducible. But this follows because a UR Newman polynomial that is irreducible must be reciprocal by Lemma 1. And the set of reciprocal Newman polynomials of length k has essentially $k/2$ "degrees of freedom" as in the remarks after the definition of the set A. □

Note that there are reducible Newman polynomials that are not UR, such as

$$1 + z + z^3 + z^4 + z^5 + z^7 + z^9 + z^{10} + z^{12} = (1 + z + z^3)(1 + z^4 + z^9).$$

It is thus conceivable that $\mathrm{ProbUR}_k(\infty) < \mathrm{ProbRed}_k(\infty)$ for some k.

We close by sketching a proof of the following result.

Proposition 16. *If B and C are as defined earlier, then the "measure" of $B \cup C$ is* $909/9464$. *Therefore* $\mathrm{ProbUR}_5(\infty) \geq 909/9464$.

Proof. We sketch a proof. Note that the conditions defining the B_i

$$\begin{aligned} \{a, b, c, d\} &\equiv_5 \{1, 2, 3, 4\} \\ \{a, b, c, d\} &\equiv_{25} \{5, 10, 15, 20\} \\ \{a, b, c, d\} &\equiv_{125} \{25, 50, 75, 100\}. \\ &\vdots \end{aligned}$$

are pairwise disjoint. Therefore the measure of B is the sum of the measures of the B_i, as in the proof of Theorem 10. We also claim that the conditions defining the C_j are pairwise disjoint. This is less obvious; we sketch the proof of that later.

We also claim that for each i and j, the condition defining B_i is "independent" from the condition defining C_j (as far as asymptotics are concerned). We omit a precise definition of this; the key is that if $\mathcal{P}_1$ and $\mathcal{P}_2$ are two properties of the form

$$\{a_1, \dots, a_k\} \equiv_{m_1} \{u_1, \dots, u_k\},$$
$$\{a_1, \dots, a_k\} \equiv_{m_2} \{v_1, \dots, v_k\},$$

where m_1, m_2 are relatively prime, then $\mathcal{P}_1$ and $\mathcal{P}_2$ are "independent" in an asymptotic sense. (The asymptotic probability of $\mathcal{P}_1$ is $1/m_1^k$, the asymptotic probability of $\mathcal{P}_2$ is $1/m_2^k$, and the event $\mathcal{P}_1 \cap \mathcal{P}_2$ is a unique congruence modulo $m_1 m_2$ by the Chinese Remainder Theorem, so $\mathcal{P}_1 \cap \mathcal{P}_2$ has asymptotic probability $1/(m_1 m_2)^k$.)

To prove that the conditions defining $C_6, C_{12}, \dots$ are pairwise disjoint, we introduce a definition.

A mod $6m$ "bicoset" is any multiset that contains 0 and is of the form

$$\big(\text{some coset of } \{0, 3m\}\big) \cup \big(\text{some coset of } \{0, 2m, 4m\}\big)$$

or equivalently, of the form

$$\{0, 3m, w, w + 2m, w + 4m\} \text{ or } \{w, w + 3m, 0, 2m, 4m\}.$$

One can show that if $k \geq 1$ and $\ell \geq 1$, then the three conditions

$$\begin{gathered}\{0, a, b, c, d\} \text{ is congruent to some mod } 6m \text{ bicoset}\\ \{0, a, b, c, d\} \text{ is congruent to some mod } 6m2^k \text{ bicoset}\\ \{0, a, b, c, d\} \text{ is congruent to some mod } 6m3^\ell \text{ bicoset}\end{gathered}$$

are pairwise disjoint. We omit some details, but this follows because a mod $6m2^k$ bicoset has the form

$$\{0, 3m2^k, x, x + 2m2^k, x + 4m2^k\} \text{ or } \{x, x + 3m2^k, 0, 2m2^k, 4m2^k\}$$

which, when taken modulo $6m$, becomes

$$\{0, 0, x, x + 2m, x + 4m\} \text{ or } \{x, x, 0, 2m, 4m\}$$

and a mod $6m3^\ell$ bicoset has the form

$$\{0, 3m3^\ell, y, y + 2m3^\ell, y + 4m3^\ell\} \text{ or } \{y, y + 3m3^\ell, 0, 2m3^\ell, 4m3^\ell\}$$

which, modulo $6m$, becomes

$$\{0, 3m, y, y, y\} \text{ or } \{y, y + 3m, 0, 0, 0\}.$$

A case by case analysis then verifies our disjointness claim.

Now, the "measure" of $B \cup C$ is

$$\big(\text{"measure" of } B\big) + \big(\text{"measure" of } C\big) - \big(\text{"measure" of } B \cap C\big).$$

But the "independence" property implies that the measure of $B \cap C$ is the product of the measure of B and the measure of C. Now because of the disjointness properties previously observed, the remaining step is to find the measures/probabilities of the individual B_i and C_j and then sum them.

That task is easier for the B_i. Informally, the probability of belonging to B_1 is the probability that $\{a, b, c, d\} \equiv_5 \{1, 2, 3, 4\}$, which is the probability that (a, b, c, d) is congruent (mod 5) to one of the 24 permutations of $(1, 2, 3, 4)$, which is $24/5^4$. Similarly, the probability of belonging to B_2 is $24/25^4$, and so on. So the measure of B is

$$\frac{24}{5^4} + \frac{24}{25^4} + \frac{24}{125^4} + \cdots = \frac{1}{26}.$$

The C_j are more subtle. The event of belonging to C_6 is the event that a, b, c, d satisfy one of the following:

$$\begin{array}{lll}
\{0,a,b,c,d\} \equiv_6 \{0,3,0,2,4\} & \text{if and only if} & \{a,b,c,d\} \equiv_6 \{0,2,3,4\} \\
\{0,a,b,c,d\} \equiv_6 \{0,3,1,3,5\} & \text{if and only if} & \{a,b,c,d\} \equiv_6 \{1,3,3,5\}* \\
\{0,a,b,c,d\} \equiv_6 \{1,4,0,2,4\} & \text{if and only if} & \{a,b,c,d\} \equiv_6 \{1,2,4,4\}* \\
\{0,a,b,c,d\} \equiv_6 \{2,5,0,2,4\} & \text{if and only if} & \{a,b,c,d\} \equiv_6 \{2,2,4,5\}*
\end{array}$$

(multisets with repeated elements are labeled with stars for convenience). The event of belonging to C_{12} is the event that a, b, c, d satisfy one of the following:

$$\begin{array}{lll}
\{0,a,b,c,d\} \equiv_{12} \{0,6,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{0,4,6,8\} \\
\{0,a,b,c,d\} \equiv_{12} \{0,6,1,5,9\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{1,5,6,9\} \\
\{0,a,b,c,d\} \equiv_{12} \{0,6,2,6,10\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{2,6,6,10\}* \\
\{0,a,b,c,d\} \equiv_{12} \{0,6,3,7,11\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{3,6,7,11\} \\
\{0,a,b,c,d\} \equiv_{12} \{1,7,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{1,4,7,8\} \\
\{0,a,b,c,d\} \equiv_{12} \{2,8,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{2,4,8,8\}* \\
\{0,a,b,c,d\} \equiv_{12} \{3,9,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{3,4,8,9\} \\
\{0,a,b,c,d\} \equiv_{12} \{4,10,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{4,4,8,10\}* \\
\{0,a,b,c,d\} \equiv_{12} \{5,11,0,4,8\} & \text{if and only if} & \{a,b,c,d\} \equiv_{12} \{4,5,8,11\}
\end{array}$$

(where again stars simply indicate that elements are repeated). In general, the event of belonging to C_{6m} is the event that $\{a, b, c, d\}$ is congruent modulo $6m$ to one of a list of $3m + 2m - 1$ different multisets. Of those $5m - 1$ multisets, exactly 3 will be of the form $\{s, s, t, u\}$ (each of those can be permuted in 12 ways) and the remaining $5m - 4$ will be of the form $\{s, t, u, v\}$ (each of those can be permuted in 24 ways).

It follows that the probability of belonging to C_{6m} is

$$\frac{3\times 12+(5m-4)\times 24}{(6m)^4} \;=\; \frac{5}{54}\cdot\frac{1}{m^3}-\frac{5}{108}\cdot\frac{1}{m^4}.$$

It remains to sum this over all m of the form $2^k 3^\ell$ where $k\geq 0, \ell\geq 0$. But this can be done with the help of the identities

$$\Big(1+\frac{1}{2^3}+\frac{1}{4^3}+\frac{1}{8^3}+\cdots\Big)\Big(1+\frac{1}{3^3}+\frac{1}{9^3}+\frac{1}{27^3}+\cdots\Big)=\frac{8}{7}\cdot\frac{27}{26}=\frac{108}{91},$$

$$\Big(1+\frac{1}{2^4}+\frac{1}{4^4}+\frac{1}{8^4}+\cdots\Big)\Big(1+\frac{1}{3^4}+\frac{1}{9^4}+\frac{1}{27^4}+\cdots\Big)=\frac{16}{15}\cdot\frac{81}{80}=\frac{27}{25}.$$

The measure of C is thus $\frac{5}{54}\cdot\frac{108}{91}-\frac{5}{108}\cdot\frac{27}{25}=\frac{109}{1820}$.

So the measure of $B\cup C$ is $\frac{1}{26}+\frac{109}{1820}-\frac{1}{26}\cdot\frac{109}{1820}=\frac{909}{9464}\approx 0.096$. $\square$

It is perhaps worth mentioning that if we write a computer program that, for a large value of N, generates a large number of pseudorandom polynomials in $\mathrm{Newm}_5(N)$ and keeps track of the proportion that are UR, the results are consistent with a proportion around 0.096.

Acknowledgment The author acknowledges the helpful comments of Michael Filaseta on an earlier draft of this paper.

References

[1] A. Dubickas, *Nonreciprocal algebraic numbers of small measure*, Comment. Math. Univ. Carolin. **45** (2004), no. 4, 693–697.

[2] M. Filaseta and I. Solan, *An extension of a theorem of Ljunggren*, Math. Scand. **84** (1999), no. 1, 5–10.

[3] C. Finch and L. Jones, *On the irreducibility of* $\{-1,0,1\}$*-quadrinomials*, Integers **6** (2006), A16, 4 pp.

[4] J. Konvalina and V. Matache, *Palindrome-polynomials with roots on the unit circle*, C. R. Math. Acad. Sci. Soc. R. Can. **26** (2004), no. 2, 39–44.

[5] S. Konyagin, *On the number of irreducible polynomials with 0,1 coefficients*, Acta Arith. **88** (1999), no. 4, 333–350.

[6] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.

[7] I. Mercer, *Unimodular roots of special Littlewood polynomials*, Canad. Math. Bull. **49** (2006), no. 3, 438–447.

[8] W. Mills, *The factorization of certain quadrinomials*, Math. Scand. **57** (1985), no. 1, 44–50.

[9] A. Odlyzko and B. Poonen, *Zeros of polynomials with 0,1 coefficients*, Enseign. Math. (2) **39** (1993), no. 3–4, 317–348.

[10] E. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.