

**RELATIONS IN  $\mathbb{N}[X]$  LEADING TO  
FINITE DIMENSIONAL POLYNOMIAL RIGS  
AND EPIMORPHIC IMAGES OF  $\mathbb{N}$  \***

Bertrand J. Guillou

bertg@umich.edu

Department of Mathematics,  
Undergraduate Programs Office,  
University of Michigan,  
Ann Arbor, MI 48109, USA

**Abstract**

In the paper “Seven trees in one”, *J. Pure Appl. Algebra* 103 (1995) 1-21, it was demonstrated that in the polynomial rig  $\mathbb{N}[x]$  and under the relation  $x = x^2 + 1$ , every polynomial is equivalent to a polynomial of degree  $\leq 4$  due to the reduction  $x^5 = x^4 + 1$ , which was derived from the relation  $x = x^2 + 1$ . The question then arises, for what other relations  $\Phi$  is it true that every polynomial in  $\mathbb{N}[x]$  under the relation  $\Phi$  is equivalent to a polynomial of degree less than  $c$  for some fixed  $c \in \mathbb{N}$ ? We offer a theorem which lists explicitly these relations  $\Phi$ .

We also begin an investigation of what rigs are epimorphic images of  $\mathbb{N}$ , which leads into the topic of Schanuel’s dimension rigs.

I. INTRODUCTION

A commutative semiring is a set of elements together with  $+$  and  $\times$  in which all the ring axioms (in addition to commutativity of multiplication) hold, except for the existence of additive inverses. This is also sometimes called a *rig*, as it is a commutative ring without negatives. Let  $R$  be a rig (or ring) and let  $p, q \in R$ . Then we will denote by  $R/(p = q)$  the rig (or ring) of equivalence classes in  $R$  under the relation  $p = q$ . We define  $\sim$  to be the smallest equivalence relation such that  $r + jp \sim r + jq \forall r, j \in R$ . Throughout this paper, when working in  $R/(p = q)$ , we will write  $g = h$  when we really mean  $[g] = [h]$ , where  $[g]$  denotes the equivalence class of  $g \in R$  under  $\sim$ .

---

\*This REU project was conducted under the direction of Professor Andreas Blass.

In the paper [1], it was demonstrated that in the polynomial rig  $\mathbb{N}[x]$  under the relation  $x = x^2 + 1$ , every polynomial is equivalent to a polynomial of degree  $\leq 4$  due to the reduction  $x^5 = x^4 + 1$ , which was derived from the relation  $x = x^2 + 1$ . The relation  $x = x^2 + 1$  has the two primitive sixth roots of unity as its solutions, and  $x^2 - x + 1$  is  $\Phi_6(x)$ , the sixth cyclotomic polynomial. Observation of this led to an investigation of rigs  $\mathbb{N}[x]/(\Phi_n(x) = 0)$  for general  $n$ , and we categorize in section II. the  $n$ 's leading to a rig in which every polynomial is equivalent to a polynomial of degree less than some fixed  $c \in \mathbb{N}$ . In addition we explicitly give a value for  $c$  for a given  $n$ , and we show that the particular  $c$  we obtain is optimal; that is, there is no polynomial  $q(x) \in \mathbb{N}[x]$  of degree  $< c$  such that  $[x^c] = [q(x)]$  in  $\mathbb{N}/(\Phi_n(x) = 0)$ .

In section III. we treat the case of general (not necessarily cyclotomic) relations. We offer a theorem which lists explicitly which relations  $\Phi$  in  $\mathbb{N}[x]$  yield such finite-dimensional rigs, although we do not give optimal  $c$ 's in this case.

## II. QUOTIENTS BY CYCLOTOMIC POLYNOMIALS

**Theorem 1.** *Let  $n$  be the power of a prime. In  $\mathbb{N}[x]/(\Phi_n(x) = 0)$ , where  $\Phi_n(x)$  is the  $n^{\text{th}}$  cyclotomic polynomial, every element is the equivalence class of some polynomial in  $\mathbb{N}[x]$  of degree  $\leq n - 1$ , and this  $n - 1$  is optimal.*

*Proof.* It turns out that if  $n = p^m$  for some prime  $p$ , then the relation  $\Phi_n(x) = 0$  is

$$x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}} + 1 = 0. \quad (1)$$

This means that  $\mathbb{N}[x]/(\Phi_n(x) = 0)$  is a ring if  $n$  is a prime power, for  $[x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}}]$  functions as  $-1$ . Now using (1), we see that

$$\begin{aligned} x^n &= x^{p^m} = x^{p^m} + x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}} + 1 \\ &= x^{p^{m-1}}(x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}} + 1) + 1 \\ &= 1, \end{aligned}$$

so that any polynomial containing any terms of degree  $\geq n$  can easily be reduced to a polynomial of degree  $\leq n - 1$ .

Let us temporarily suppose  $m = 1$ , so that  $n = p$ . In  $\mathbb{C}[x]$ , we have  $\Phi_p(x) = (x - r_1)(x - r_2) \dots (x - r_{p-1})$ . Now consider the ring homomorphism

$$\varphi : \mathbb{C}[x] \rightarrow \underbrace{\mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}}_{p-1 \text{ C's}}$$

given by  $\varphi(q) = (q(r_1), q(r_2), \dots, q(r_{p-1}))$ . We can see that the kernel of  $\varphi$  is the ideal generated by  $\Phi_p(x)$ . Thus, the First Isomorphism Theorem tells us that  $\varphi$  maps  $\mathbb{C}[x]/(\Phi_p(x))$  isomorphically to

the image of  $\varphi$ . As  $\varphi$  is surjective, it maps  $\mathbb{C}[x]/(\Phi_p(x))$  isomorphically to  $\mathbb{C}^{p-1}$ . Clearly,  $\mathbb{C}^{p-1}$  has dimension  $p-1$ , so  $\mathbb{C}[x]/(\Phi_p(x))$  must similarly have dimension  $p-1$ . Using the relation

$$x^{p-1} = -x^{p-2} - x^{p-3} - \dots - x - 1, \quad (2)$$

we see that every element of  $\mathbb{C}[x]/(\Phi_p(x))$  is a linear combination of  $[1], [x], \dots, [x^{p-2}]$ , so that these elements constitute a basis for  $\mathbb{C}[x]/(\Phi_p(x))$ . That is, they are linearly independent; there is no reduction of  $x^{p-2}$  to a polynomial of lower degree in  $\mathbb{C}[x]$  under the relation  $\Phi_p(x) = 0$ . Because these elements are linearly independent, every element of  $\mathbb{C}[x]/(\Phi_p(x))$  can be expressed as a unique linear combination of these elements. In particular, (2) gives us that  $x^{p-1}$  is expressible only as a polynomial with negative coefficients. As the relations we are permitted in  $\mathbb{N}[x]/(\Phi_p(x) = 0)$  are weaker than those permitted in  $\mathbb{C}[x]/(\Phi_p(x))$ , we know that we can at most reduce elements of  $\mathbb{N}[x]$  to polynomials of degree  $\leq p-2$  under the relation  $\Phi_p(x) = 0$ . The above argument shows that  $x^{p-1}$  is also necessary so that all polynomials may have nonnegative coefficients. Thus, for  $n$  prime,  $n-1$  is optimal.

The more general situation for  $n = p^m$  is quite similar. This time, in  $\mathbb{C}[x]$ , we have  $\Phi_n(x) = (x - r_1)(x - r_2) \dots (x - r_{p^{m-1}(p-1)})$ . Now consider the ring homomorphism

$$\varphi : \mathbb{C}[x] \rightarrow \underbrace{\mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}}_{p^{m-1}(p-1) \text{ C's}}$$

given by  $\varphi(q) = (q(r_1), q(r_2), \dots, q(r_{p^{m-1}(p-1)}))$ . Again, we can see that the kernel of  $\varphi$  is the ideal generated by  $\Phi_n(x)$ . Thus, the First Isomorphism Theorem tells us that  $\varphi$  maps  $\mathbb{C}[x]/(\Phi_n(x))$  isomorphically to the image of  $\varphi$ . As  $\varphi$  is surjective, it maps  $\mathbb{C}[x]/(\Phi_n(x))$  isomorphically to  $\mathbb{C}^{p^{m-1}(p-1)}$ . Clearly,  $\mathbb{C}^{p^{m-1}(p-1)}$  has dimension  $p^{m-1}(p-1)$ , so  $\mathbb{C}[x]/(\Phi_n(x))$  must similarly have dimension  $p^{m-1}(p-1)$ . Using the relation

$$x^{p^{m-1}(p-1)} = -x^{p^{m-1}(p-2)} - x^{p^{m-1}(p-3)} - \dots - x^{p^{m-1}} - 1, \quad (3)$$

we see that every element of  $\mathbb{C}[x]/(\Phi_n(x))$  is a linear combination of  $[1], [x], \dots, [x^{p^{m-1}(p-1)-1}]$ , so that these elements constitute a basis for  $\mathbb{C}[x]/(\Phi_n(x))$ . That is, they are linearly independent; there is no reduction of  $x^{p^{m-1}(p-1)-1}$  to a polynomial of lower degree in  $\mathbb{C}[x]$  under the relation  $\Phi_n(x) = 0$ . Because these elements are linearly independent, every element of  $\mathbb{C}[x]/(\Phi_n(x))$  can be expressed as a unique linear combination of these elements. In particular, (3) gives us that  $x^{p^{m-1}(p-1)}$  is expressible only as a polynomial with negative coefficients. In contrast to the case where  $n = p$ , we cannot simply introduce  $x^{p^{m-1}(p-1)}$ , for (1) only relates elements whose powers are congruent modulo  $p^{m-1}$ ; to ensure that  $x^{p^{m-1}(p-1)-1}$  has a positive coefficient, we must introduce  $x^{p^{m-1}}$  and others in between to ensure nonnegativity of other powers. As the relations we are permitted in  $\mathbb{N}[x]$  are weaker than those permitted in  $\mathbb{C}[x]$ , we know that we can at most reduce

elements of  $\mathbb{N}[x]$  to polynomials of degree  $\leq p^{m-1}(p-1) - 1$  under the relation  $\Phi_n(x) = 0$ . The above argument shows that monomials up to  $x^{p^{m-1}}$  are also necessary so that all polynomials may have nonnegative coefficients. Thus, for  $n$  a prime power,  $p^m - 1 = n - 1$  is optimal.  $\square$

Note that we can also derive  $x^{n+1} = x$  by introducing and removing  $x^{p^{m-1}(p-1)+k} + x^{p^{m-1}(p-2)+k} + \dots + x^{p^{m-1}+k} + x^k$  through the use of a catalyst, as in “Seven trees in one”, by simply using

$$x = x^{p^{m-1}(p-1)} + x^{p^{m-1}(p-2)} + \dots + x^{p^{m-1}} + x + 1.$$

**Theorem 2.** *In  $\mathbb{N}[x]/(\Phi'_n(x))$ , where  $\Phi_n(x)$  is the  $n^{\text{th}}$  cyclotomic polynomial and  $\Phi'_n(x)$  is the equation  $\Phi_n(x) = 0$  rearranged so that only terms of nonnegative coefficients appear, every element is the equivalence class of some polynomial in  $\mathbb{N}[x]$  of degree  $\leq \frac{5}{6}n - 1$  if 2 and 3 are exactly the prime divisors of  $n$ , and this  $\frac{5}{6}n - 1$  is optimal.*

*Proof.* It turns out that if  $n = 2^{m_2}3^{m_3}$ , for  $m_2, m_3 \geq 1$ , then  $\Phi_n(x)$  is  $x^{\frac{n}{3}} - x^{\frac{n}{6}} + 1$  so that  $\Phi'_n(x)$  is

$$x^{\frac{n}{3}} + 1 = x^{\frac{n}{6}}. \quad (4)$$

Now using (4), we see that

$$\begin{aligned} x^{\frac{5}{6}n} &= x^n + x^{\frac{2}{3}n} = x^n + x^{\frac{5}{6}n} + x^{\frac{n}{2}} = x^n + x^{\frac{5}{6}n} + x^{\frac{2}{3}n} + x^{\frac{n}{3}} \\ &= 2x^{\frac{5}{6}n} + x^{\frac{n}{3}} = 2x^{\frac{5}{6}n} + x^{\frac{n}{2}} + x^{\frac{n}{6}} = x^{\frac{5}{6}n} + x^{\frac{2}{3}n} + x^{\frac{n}{6}} \\ &= x^{\frac{5}{6}n} + x^{\frac{2}{3}n} + x^{\frac{n}{3}} + 1 = x^{\frac{5}{6}n} + x^{\frac{n}{2}} + 1 = x^{\frac{2}{3}n} + 1 \end{aligned}$$

so that any polynomial containing any terms of degree  $\geq \frac{5}{6}n$  can easily be reduced to a polynomial of degree  $\leq \frac{5}{6}n - 1$ .

We will now follow a similar idea to the one of the proof of Theorem 1. In  $\mathbb{C}[x]$ , we have  $\Phi_n(x) = (x - r_1)(x - r_2) \dots (x - r_{\frac{n}{3}})$ . Consider the ring homomorphism

$$\varphi : \mathbb{C}[x] \rightarrow \mathbb{C}^{\frac{n}{3}}$$

given by  $\varphi(q(x)) = (q(r_1), q(r_2), \dots, q(r_{\frac{n}{3}}))$ . As above, the kernel is the ideal generated by  $(\Phi_n(x))$  and we get an isomorphism  $\varphi : \mathbb{C}[x]/(\Phi_n(x)) \approx \mathbb{C}^{\frac{n}{3}}$ . We find that  $[1], [x], [x^2], \dots, [x^{\frac{n}{3}-1}]$  are linearly independent and that every element of  $\mathbb{C}[x]/(\Phi_n(x))$  can be expressed as a linear combination of these elements. All polynomials of degree  $\geq \frac{n}{3}$  can be reduced to a linear combination of these elements by using the relation

$$x^{\frac{n}{3}} = x^{\frac{n}{6}} - 1 \quad (5)$$

in  $\mathbb{C}[x]$ . We can see that in  $\mathbb{C}[x]/(\Phi_n(x))$ ,  $x^{\frac{n}{2}} = -1$ , but we may ask if there is a polynomial  $p(x) \sim -1$  such that  $p(x)$  has natural number coefficients and such that  $\frac{n}{3} \leq \deg p(x) < \frac{n}{2}$ . Let us

suppose for a contradiction that there is such a  $p(x)$ . Using (5), we can reduce  $p(x)$  to a polynomial of degree  $\leq \frac{n}{3} - 1$ . The reduction (5) fixes all powers modulo  $\frac{n}{6}$ , so  $p(x)$  could not have any powers of  $x$  not congruent to 0. Thus  $p(x) = ax^{\frac{n}{3}} + bx^{\frac{n}{6}} + c$  for some  $a, b, c \in \mathbb{N}$ , but this reduces to  $\bar{p}(x) = (a + b)x^{\frac{n}{6}} + c - a$ . If  $\bar{p}(x) = -1$ , then  $a + b = 0$ , which is impossible since  $a, b \in \mathbb{N}$ . There can be no such  $p(x)$ , and so  $x^{\frac{n}{2}}$  is the polynomial with nonnegative coefficients of minimal degree identical to  $-1$  in this ring. It is then reasonable to suppose that  $x^{\frac{5}{6}n-1}$  is the polynomial with nonnegative coefficients of minimal degree equivalent to  $-x^{\frac{n}{3}-1}$  in this ring, and this is easy to verify in the same way. This shows that in  $\mathbb{N}[x]/(\Phi'_n(x))$ , we could at most reduce to polynomials of degree  $\leq \frac{n}{3} - 1$  but that we also need polynomials of degree up to  $\frac{5}{6}n - 1$  in order to express everything as an element of  $\mathbb{N}[x]/(\Phi'_n(x))$ . Thus, for  $n = 2^{m_2}3^{m_3}$  with  $m_2, m_3 \geq 1$ , this  $\frac{5}{6}n - 1$  is optimal.  $\square$

Note that we can also derive  $x^{\frac{7}{6}n} = x^{\frac{n}{6}}$  by introducing and removing  $x^{\frac{n}{2}+k} + x^k$  through the use of a catalyst, as in ‘‘Seven trees in one’’, by simply using the relations

$$x^{\frac{n}{6}} = x^{\frac{n}{2}} + x^{\frac{n}{6}} + 1 \quad \text{and} \quad x^{\frac{n}{3}} = x^{\frac{n}{2}} + x^{\frac{n}{3}} + 1.$$

**Theorem 3.** *In  $\mathbb{N}[x]$  under the relation  $\Phi'_n(x)$ , where  $\Phi_n(x)$  is the  $n^{\text{th}}$  cyclotomic polynomial,  $\Phi'_n(x)$  is the equation  $\Phi_n(x) = 0$  rearranged so that only terms of nonnegative coefficients appear and  $n$  is neither a prime power nor a product of powers of 2 and 3, there are polynomials of every degree which are not equivalent to any polynomial of lower degree.*

We will first need a lemma.

**Lemma 1.** *If  $n$  is not the power of a prime, then  $\Phi_n(x) = 0$  is not expressible in  $\mathbb{N}[x]$  as  $ax^k = q(x)$ , where  $a \geq 0$  and  $q$  has nonnegative coefficients, unless  $n = 2^{m_2}3^{m_3}$ , for  $m_2, m_3 \geq 1$ .*

*Proof.* First quickly note that all cyclotomic polynomials are monic, so that they all have at least one positive coefficient. Also, note that all cyclotomic polynomials for  $n \geq 2$  have palindromic coefficients, i.e., if  $\Phi_n(x)$  is  $a_0 + a_1x + \cdots + a_r x^r$ , then  $a_0 = a_r$ ,  $a_1 = a_{r-1}$ , etc. Thus all cyclotomic polynomials, for  $n \geq 2$ , have at least 2 positive coefficients.

Note that we need only consider cases where  $n$  has prime factors only of multiplicity 1, for  $\Phi_{pm}(x) = \Phi_m(x^p)$  if  $p \mid m$  (cf. [2]). Thus we let  $n = p_1 p_2 \cdots p_r$ , where each of the  $p_i$  are primes and  $p_i < p_{i+1}$ . We now call upon two further lemmas:

**Lemma 2.** *Let  $n$  be as described above. If  $r$  is even,  $\Phi_n(x)$  has a linear coefficient of  $-1$ , while if  $r$  is odd,  $\Phi_n(x)$  has a linear coefficient of 1.*

**Lemma 3.** *Let  $n$  be as described above. If  $r$  is even,  $\Phi_n(x) = 1 - x + x^{p_1} + x^{p_1+1}k(x)$ , for some polynomial  $k(x)$ , while if  $r$  is odd,  $\Phi_n(x) = 1 + x + x^2 + x^3 + \cdots + x^{p_1-1} - x^{p_2} + x^{p_2+1}k(x)$ , for some polynomial  $k(x)$ .*

*Proof of Lemma 2.* We will prove this inductively. We already know this to be true for the initial case of  $r = 1$ , where  $n$  is prime. Now assume that this  $r$  is even and that the lemma holds for  $r - 1$ . Let  $n = p_1 p_2 \cdots p_r$ . Using the fact that

$$\Phi_{pm}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \quad (6)$$

when  $p \nmid m$  (cf. [2]), we find that

$$\Phi_{p_1 p_2 \cdots p_r}(x) = \frac{\Phi_{p_2 p_3 \cdots p_r}(x^{p_1})}{\Phi_{p_2 p_3 \cdots p_r}(x)}$$

or

$$\Phi_{p_1 p_2 \cdots p_r}(x) \Phi_{p_2 p_3 \cdots p_r}(x) = \Phi_{p_2 p_3 \cdots p_r}(x^{p_1}).$$

Let us write  $\Phi_{p_1 p_2 \cdots p_r} = (1 + \alpha x + x^2 k(x))$  for some polynomial  $k(x)$ . Then the inductive assumption gives us

$$(1 + \alpha x + x^2 k(x))(1 + x + x^2 m(x)) = (1 + x^{p_1} + x^{p_1+1} q(x)),$$

for some polynomials  $m(x)$  and  $q(x)$ . As  $p_1 > 1$ , we see right away that  $\alpha = -1$ .

Now we assume that  $r$  is odd and that the lemma holds for  $r - 1$ . Again, using (6), we find that

$$\Phi_{p_1 p_2 \cdots p_r}(x) \Phi_{p_2 p_3 \cdots p_r}(x) = \Phi_{p_2 p_3 \cdots p_r}(x^{p_1}).$$

This time, however, the induction assumption gives us

$$(1 + \alpha x + x^2 k(x))(1 - x + x^2 m(x)) = 1 - x^{p_1} + x^{p_1+1} q(x),$$

for some polynomials  $m(x)$  and  $q(x)$ . As  $p_1 > 1$ , we see right away that  $\alpha = 1$ . □

*Proof of Lemma 3.* As above, we will offer an inductive proof. We know that this holds for the case  $r = 1$ , where  $n$  is prime. Now we will assume that  $r$  is even and that the lemma holds for  $r - 1$ . We let  $\Phi_n(x) = (1 - x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots + \alpha_{p_1} x^{p_1} + x^{p_1+1} k(x))$  for some polynomial  $k(x)$ . We know that the coefficient of the linear term is  $-1$  from Lemma 2. Using (6) once again, we find that

$$\begin{aligned} (1 - x + \alpha_2 x^2 + \cdots + \alpha_{p_1} x^{p_1} + x^{p_1+1} k(x))(1 + x + x^2 + \cdots + x^{p_2-1} - x^{p_3} + x^{p_3+1} m(x)) \\ = 1 + x^{p_1} + x^{p_1+1} q(x) \end{aligned}$$

for some polynomials  $m(x)$  and  $q(x)$ . Multiplying the left hand side, we have

$$1 + \alpha_2 x^2 + (\alpha_3 + \alpha_2) x^3 + \cdots + (\alpha_{p_1} + \cdots + \alpha_3 + \alpha_2) x^{p_1} + O(x^{p_1+1}) = 1 + x^{p_1} + O(x^{p_1+1}),$$

where we use  $O(x^{p_1+1})$  to denote terms of order higher than  $p_1$ . We then deduce that  $\alpha_2 = \alpha_3 = \dots = \alpha_{p_1-1} = 0$  and that  $\alpha_{p_1} = 1$ . But then  $\Phi_n(x) = 1 - x + x^{p_1} + x^{p_1+1}k(x)$  as desired.

Now assume that  $r$  is odd and that the lemma holds for  $r - 1$ . Let  $\Phi_n(x) = (1 + x + \alpha_2x^2 + \dots + \alpha_{p_2}x^{p_2} + x^{p_2+1}k(x))$ . We know that the coefficient of the linear term is 1 from Lemma 2. Using (6), we have

$$(1 + x + \alpha_2x^2 + \dots + \alpha_{p_2}x^{p_2} + x^{p_2+1}k(x))(1 - x + x^{p_2} + x^{p_2+1}m(x)) = 1 - x^{p_1} + x^{p_1p_2} + x^{p_1p_2+1}q(x)$$

for some polynomials  $m(x)$  and  $q(x)$ . Multiplying the left hand side, we have

$$1 + (\alpha_2 - 1)x^2 + (\alpha_3 - \alpha_2)x^3 + \dots + (\alpha_{p_1} - \alpha_{p_1-1})x^{p_1} + (\alpha_{p_1+1} - \alpha_{p_1})x^{p_1+1} + \dots + (1 + \alpha_{p_2} - \alpha_{p_2-1})x^{p_2} + O(x^{p_2+1}) = 1 - x^{p_1} + x^{p_1p_2} + O(x^{p_1p_2+1}).$$

We deduce that  $\alpha_2 = \alpha_3 = \dots = \alpha_{p_1-1} = 1$ ,  $\alpha_{p_1} = \alpha_{p_1+1} = \dots = \alpha_{p_2-1} = 0$ , and  $\alpha_{p_2} = -1$ . But then  $\Phi_n(x) = 1 + x + x^2 + \dots + x^{p_1-1} - x^{p_2} + x^{p_2+1}k(x)$  as desired.  $\square$

If  $r$  is even, Lemma 3 and the palindrome property of cyclotomic polynomials show us that  $\Phi_n(x)$  has at least two negative coefficients unless  $\Phi_n(x) = 1 - x + x^2$ , which is the case for  $n = 6$ .

If  $r$  is odd and greater than or equal to 3, then, since  $p_2 \geq 3$  and  $p_3 \geq 5$ , we can see that

$$\deg \Phi_n(x) = \varphi(n) \geq \varphi(p_1p_2p_3) = (p_1 - 1)(p_2 - 1)(p_3 - 1) \geq (p_2 - 1)(p_3 - 1) \geq 4(p_2 - 1) > 2p_2.$$

This means that  $p_2$  is less than the degree of the middle term of  $\Phi_n(x)$ , which means that (at least) one other term of the polynomial has the coefficient  $-1$ , and we are done.  $\square$

We are now ready to prove Theorem 3.

*Proof of Theorem 3.* Lemma 1 really does all of the work in this proof. It tells us that if  $n$  is as stated in the theorem, then  $\Phi_n(x) = 0$  is not expressible as  $ax^k = q(x)$ , where  $a \geq 0$  and  $q$  has nonnegative coefficients. But then given any monomial  $bx^m$ , for  $b > 0$ , there is no reduction that can be performed. The cyclotomic polynomial does not express any equation between  $bx^m$  and any other element of  $\mathbb{N}[x]/(\Phi'_n(x))$ , so the monomial is not expressible in any other way in this semiring.  $\square$

### III. QUOTIENTS BY MORE GENERAL POLYNOMIALS

**Theorem 4.** *In  $\mathbb{N}[x]$  under either the relation  $x = \sum_{k=0}^n x^k$  or  $0 = 1 + \sum_{k=2}^n x^k$ , where  $n \geq 2$ , every element is equivalent to a polynomial with coefficients  $\geq 0$  of degree  $\leq n+1$  by the reduction  $x^{n+2} = 1 + x + x^3 + \sum_{k=3}^n x^k$ .*

*Proof.* We will first look at  $\mathbb{N}[x]/(x = \sum_{k=0}^n x^k)$ . We see that

$$\begin{aligned} x^{n+2} &= x^{2n+1} + x^{2n} + \cdots + x^{n+1} \\ &= x^{2n+1} + 2x^{2n} + 2x^{2n-1} + \cdots + 2x^{n+2} + x^{n+1} + x^n \\ &= x^{2n+1} + 2x^{2n} + 3x^{2n-1} + \cdots + 3x^{n+2} + 2x^{n+1} + x^n + x^{n-1}. \end{aligned} \tag{7}$$

We then continue in this fashion, at each step replacing the term of lowest degree with the appropriate multiple of  $\sum_{k=0}^n x^k$  until we arrive at

$$x^{n+2} = x^{2n+1} + 2x^{2n} + 3x^{2n-1} + \cdots + (n-1)x^{n+3} + nx^{n+2}.$$

Now we start from the highest power terms, replacing multiples of  $\sum_{k=0}^n x^k$  with the appropriate monomials until we arrive at

$$x^{n+2} = 2x^{n+2} + 2x^{n+1} + 3x^n + 3x^{n-1} + 3x^{n-2} + \cdots + 3x^5 + 3x^4 + 2x^3 + 2x^2 + x + 1.$$

We finally replace two copies of  $x^2 \sum_{k=0}^n x^k$  with two copies of  $x^3$  and end with

$$x^{n+2} = x^n + x^{n-1} + x^{n-2} + \cdots + x^5 + x^4 + 2x^3 + x + 1,$$

which is the desired reduction. In  $\mathbb{N}[x]/(0 = 1 + \sum_{k=2}^n x^k)$  we can derive the relation  $x = \sum_{k=0}^n x^k$  and so the above reduction holds in this rig as well. □

**Theorem 5.** *In  $\mathbb{N}[x]$  under the relation  $x = 1 + x^n$ , where  $n \geq 2$ , every element is equivalent to a polynomial with coefficients  $\geq 0$  of degree  $\leq 2n$  by the reduction  $x^{2n+1} = 1 + x + x^{n+2} + \sum_{k=n+2}^{2n-1} 2x^k + x^{2n}$ .*

*Proof.* In  $\mathbb{N}[x]/(x = 1 + x^n)$ , we see that

$$\begin{aligned} x^{2n+1} &= x^{3n} + x^{2n} = x^{3n} + x^{3n-1} + x^{2n-1} \\ &= x^{3n} + x^{3n-1} + x^{3n-2} + x^{2n-2}. \end{aligned} \tag{8}$$

We then continue in this fashion, at each step replacing the term of lowest degree with the appropriate multiple of  $1 + x^n$  until we arrive at

$$x^{2n+1} = x^{3n} + x^{3n-1} + \sum_{k=2n+1}^{3n-2} x^k + x^{2n} + x^n.$$

Now we start replacing multiples of  $1 + x^n$  with the appropriate monomials:

$$\begin{aligned} x^{2n+1} &= x^{3n-1} + \sum_{k=2n+1}^{3n-2} x^k + 2x^{2n+1} + x^n \\ &= x^{3n-1} + \sum_{k=2n+1}^{3n-2} x^k + x^{2n+1} + x^{2n-1} + x^{n-1} \\ &= \sum_{k=2n+1}^{3n-2} x^k + x^{2n+1} + x^{2n} + x^{n-1}. \end{aligned}$$

Continuing in this vein, we obtain

$$x^{2n+1} = x^{2n+1} + x^{2n} + \sum_{k=n+2}^{2n-1} x^k + x.$$

We now replace  $x$  with  $x^n + 1$ ,

$$x^{2n+1} = x^{2n+1} + x^{2n} + \sum_{k=n+2}^{2n-1} x^k + x^n + 1,$$

and then continue as before:

$$\begin{aligned} x^{2n+1} &= x^{2n+1} + x^{2n} + x^{2n-1} + \sum_{k=n+2}^{2n-1} x^k + x^{n-1} + 1 \\ &\vdots \\ &= x^{2n+1} + x^{2n} + \sum_{k=n+2}^{2n-1} 2x^k + x^{n+1} + x + 1. \end{aligned}$$

We finally replace  $x^{2n+1} + x^{n+1}$  with  $x^{n+2}$  to get

$$x^{2n+1} = x^{2n} + \sum_{k=n+2}^{2n-1} 2x^k + x^{n+2} + x + 1.$$

Note that the  $\sum$  notation is necessary here so that we do not unintentionally make the assumption that there are any elements of power  $m$ , where  $2n < m < 3n - 1$ .  $\square$

**Theorem 6.** *In  $\mathbb{N}[x]$  under the relation  $ax^k = p(x)$ , where  $p(x)$  is a polynomial in  $\mathbb{N}[x]$  and  $a, k \in \mathbb{N}$ , every element is equivalent to a polynomial with coefficients in  $\mathbb{N}$  of degree  $\leq c$  for some constant  $c \in \mathbb{N}$  iff one of the following hold*

- (i)  $a = 0$  and the leading coefficient of  $p(x)$  is 1
- (ii)  $a = 1$  and  $\deg p(x) < k$
- (iii)  $a > 0$  and  $n = \deg p(x) > k$  and  $p(x) = x^n$
- (iv)  $a = 1$  and  $n = \deg p(x) > k$  and  $p(x)$  has leading term coefficient 1 and has a term of degree  $< k$  with nonzero coefficient.

*Proof.* Let us denote by  $(\dagger)$  the statement that every element is equivalent to a polynomial with coefficients in  $\mathbb{N}$  of degree  $\leq c$  for some constant  $c \in \mathbb{N}$ .

(i)  $\Rightarrow (\dagger)$  Let  $p(x) = x^n + q(x)$ , where  $\deg q(x) < n$ . Then we can see that

$$\begin{aligned} x^{2n} &= x^{2n} + q(x)p(x) \\ &= x^{2n} + q(x)(x^n + q(x)) \\ &= x^{2n} + q(x)x^n + q(x)q(x) \\ &= x^n p(x) + q(x)^2 \\ &= q(x)^2. \end{aligned} \tag{9}$$

Using this reduction, we can then express every polynomial of degree  $\geq 2n$  as a polynomial of degree  $\leq 2n - 1$ .

(ii)  $\Rightarrow (\dagger)$  This is easy. Using the reduction  $x^k = p(x)$ , we can express any polynomial of degree  $\geq k$  as a polynomial of degree  $\leq k - 1$ .

(iii)  $\Rightarrow (\dagger)$  Here too we are already given a reduction which allows us to express polynomials of degree  $\geq n$  as polynomials of degree  $\leq n - 1$ .

(iv)  $\Rightarrow$  (†) Let us write  $p(x)$  as  $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_{k-d+1}x^{k-d+1} + \beta x^{k-d}$  where  $\alpha_i, \beta, d \in \mathbb{N}$ ,  $\beta \geq 1$ , and  $1 \leq d \leq k$ . We will now consider three cases:

Case 1:  $d = n - k$ . Then we write  $p(x) = x^n + q(x) + \beta x^{n-2d}$ , where  $\deg q(x) < n$  and  $q(x)$  has no terms of order  $< n - 2d + 1$ , and  $x^k = x^{n-d}$ . This gives us

$$\begin{aligned}
x^{3n-d} &= x^{3n} + q(x)x^{2n} + \beta x^{3n-2d} \\
&= x^{3n} + q(x)x^{2n} + \beta x^{3n-d} + \beta q(x)x^{2n-d} + \beta^2 x^{3n-3d} \\
&= x^{3n} + q(x)x^{2n} + \beta x^{3n-d} + \beta q(x)x^{2n-d} + \beta^2 x^{3n-2d} + \beta^2 q(x)x^{2n-2d} + \beta^3 x^{3n-4d} \\
&= (\beta + 1)x^{3n-d} + \beta q(x)x^{2n-d} + (\beta^2 - \beta)x^{3n-2d} + \beta^2 q(x)x^{2n-2d} + \beta^3 x^{3n-4d} \\
&= (\beta + 1)x^{3n-d} + \beta q(x)x^{2n-d} + (\beta^2 - \beta)x^{3n-2d} + \beta^2 q(x)x^{2n-2d} + \beta^3 x^{3n-3d} \\
&\quad + \beta^3 q(x)x^{2n-3d} + \beta^4 x^{3n-5d} \\
&= x^{3n-d} + \beta^2 x^{3n-2d} + \beta^2 q(x)x^{2n-2d} + (\beta^3 - \beta^2)x^{3n-3d} \\
&\quad + \beta^3 q(x)x^{2n-3d} + \beta^4 x^{3n-5d}
\end{aligned} \tag{10}$$

The final part of the calculation becomes quite messy but can be described rather easily. The idea is to expand each term of  $\beta^2 q(x)x^{2n-2d}$ . Next, expand  $\beta^4 x^{3n-5d}$ . This gives us a  $\beta^4 x^{3n-4d}$  term, which we further expand to yield a  $\beta^4 x^{3n-3d}$  term. Now we have enough terms to collapse  $x^{3n-d} + q(x)x^{2n-d} + \beta x^{3n-3d}$  to  $x^{3n-2d}$ . Throughout this calculation, it is essential that  $\beta \geq 1$ . The lowest degree term in this calculation is  $\beta^5 x^{3n-6d}$ . We know that the minimal power that can result from a reduction is  $n - 2d \geq 0$ , but as  $3n - 6d = 3(n - 2d) \geq (n - 2d)$ , we encounter no difficulties here.

Case 2:  $d > n - k$ . Here, we will first look at the simpler case where  $d \equiv 0 \pmod{n - k}$ .

Case 2a:  $d \equiv 0 \pmod{n - k}$ . We can now produce a reduction from  $x^{k+5d}$  in much the same way as we reduced from  $x^{3n-d}$  in Case 1, the only difference being that, in Case 1 if we wanted to add to the coefficient of  $x^m$  we simply expanded  $x^{m-d}$ , whereas in this case if we want to add to the coefficient of  $x^m$ , we first expand  $x^{m-d}$ , which adds to the coefficient of  $x^{m-d+n-k}$ , and we then expand  $x^{m-d+n-k}$  and so on until we reach  $x^m$ .

Case 2b:  $d \not\equiv 0 \pmod{n - k}$ . We can similarly here produce a reduction from  $x^{k+5d}$ . However, we can see that expanding  $x^{m-d}$  and next  $x^{m-d+n-k}$  and so on will not increase the coefficient of  $x^m$ , since  $d \not\equiv 0 \pmod{n - k}$ . Rather, we expand  $x^{m-d}$  and next  $x^{m-d+n-k}$  and so on until we have  $x^{m-d+u(n-k)}$ , where  $d - u(n-k) < n - k$ . Now, instead of expanding  $x^{m-d+u(n-k)}$ , which would yield terms of power greater than  $m$ , we expand  $x^{m-d+(u-1)(n-k)-d}$ , which was the lowest term introduced by the expansion introducing  $x^{m-d+u(n-k)}$ . We repeat this process until we can finally increase the coefficient of  $x^m$ .

without increasing the coefficients of any higher power terms. Notice that, at most, we must carry out this process  $n - k$  times, as  $d(n - k) - (n - k - 1)d = d$ . Finally, when increasing the coefficient of  $x^{k+d}$  from  $x^k$  (as we increase the coefficient of  $x^{3n-4d}$  from  $x^{3n-5d}$  in Case 1), we must be sure to not involve terms of power lower than  $k - d$ , although here it is safe to add terms of power greater than  $k + d$ , as long as we do not add terms of power greater than or equal to  $k + 5d$ .

Case 3:  $d < n - k$ . Using similar ideas as those outlined in Case 2, we can produce a reduction from  $x^{5n-4k}$ .

( $\dagger$ )  $\Rightarrow$  (i) or (ii) or (iii) or (iv) We assume that ( $\dagger$ ) is true. Let us denote by an *expansion* a substitution of  $p(x)h(x)$  for  $ax^k h(x)$  for any  $h(x) \in \mathbb{N}[x]$  and by a *collapse* a substitution of  $ax^k h(x)$  for  $p(x)h(x)$  for any  $h(x) \in \mathbb{N}[x]$ . We will sometimes refer to either an expansion or a collapse as a *move*.

Temporarily assume also that  $a = 0$ . Now assume for a contradiction that the leading coefficient of  $p(x)$  is  $m > 1$ . We have assumed that there is a reduction from  $x^{c+1}$  to terms of lower degree. We cannot simply proceed as in the proof of ( $\dagger$ )  $\Rightarrow$  (i), for the coefficient of  $x^{c+1}$  is 1, which is less than  $m$ . Furthermore, we see that we cannot simply add multiples of  $x^{c+1-n}p(x)$ , where  $n = \deg p(x)$ , for the coefficient of  $x^{c+1}$  will still be  $\equiv 1 \pmod{m}$ . Therefore, any reduction must involve some terms of degree higher than  $c + 1$ . Our reduction involves a finite number of moves, which means that there is a maximal degree involved in the reduction. Let us call this  $\mu$ . As  $\mu > c + 1$ , the term of order  $\mu$  must be removed by one or more collapses at some point in the reduction. We can suppose without loss of generality that our reduction does not involve any expendable moves—any series of moves followed at some later point by the reverse of that series and whose terms are not involved in any other moves in the interim—for if the reduction does contain a series of expendable moves, we may remove them and consider the remaining reduction. Therefore, the expansions that introduced the term of degree  $\mu$  were necessary, so some of the terms of  $\lambda p(x)x^{\mu-n}$ , where  $\lambda \in \mathbb{N}$  is the appropriate coefficient, must be involved in some move. In other words some of these terms must be involved in a collapse, which means they are removed at some point of the reduction. However, the only way to remove the term of order  $\mu$  is to perform a collapse requiring these removed terms. If the introduction of  $\lambda p(x)x^{\mu-n}$  is not to be expendable, the needed terms must be reintroduced through some lower degree expansions. But now we see that we could just as easily have originally introduced those terms via the lower degree expansions. Thus, if we have a reduction involving terms of order only up to  $\mu > c + 1$ , we can in this way produce a reduction involving terms of order only up to some  $\mu' < \mu$ . Inductively, we can then produce a reduction involving no terms of order  $> c + 1$ , which is a contradiction, so there can be no reduction if  $a = 0$  and the leading coefficient of  $p(x)$  is greater than 1.

Assume now that  $a > 1$  and assume for a contradiction that  $p(x) \neq x^n$ . Then, writing out the equation as

$$\underbrace{x^k + x^k + \cdots + x^k}_{a \text{ of these}} = p(x),$$

we have more than one term on each side. There is no possibility of beginning a reduction from any monomial of only one term  $x^{c+1}$ . Thus if  $p(x) \neq x^n$  we can have no reduction, which contradicts (†).

Assume that  $a > 1$  and that  $p(x) = x^n$  and assume for a contradiction that  $\deg p(x) = n < k$ . Let  $C \subset \mathbb{N}[x]$  consist of polynomials of the form

$$(1 - \lambda_1)x^{c+1} + (\lambda_1 a - \lambda_2)x^{c+1+(k-n)} + \cdots + (\lambda_{m-1} a - \lambda_m)x^{c+1+(m-1)(k-n)} + \lambda_m a x^{c+1+m(k-n)},$$

where  $m, \lambda_i \in \mathbb{N}$ ,  $\lambda_1 \leq 1$ , and  $\lambda_i \leq a\lambda_{i-1}$  for  $i \geq 2$ .  $x^{c+1}$  is clearly in  $C$ , for setting  $\lambda_1 = 0$  forces  $\lambda_i = 0 \forall i$ . It can be easily verified that  $C$  is closed under an expansion or collapse. As  $C$  does not contain any polynomials of degree  $< c + 1$ , there can be no reduction from  $x^{c+1}$  to a polynomial of lower degree, contradicting (†).

Assume that  $a \geq 1$  and assume for a contradiction that  $\deg p(x) = k$ . Given any polynomial, an expansion will only introduce (if anything) lower degree terms and so will not affect the degree of the polynomial. On the other hand, a collapse will remove (if anything) terms of power less than some term without totally removing that higher power term; a collapse will therefore not affect the degree of the polynomial. Thus, no reduction step can affect the degree of a polynomial, and no reduction from  $x^{c+1}$  to a polynomial of lower degree is possible, contradicting (†).

Assume that  $a = 1$ , that  $p(x) \neq x^n$ , and that  $\deg p(x) > k$  and assume for a contradiction that  $p(x)$  has no term of power  $< k$ . If  $p(x)$  has a term of power  $k$ , then neither an expansion nor a collapse introduces terms of lower degree, which means that no reduction is possible. Let us then assume for a contradiction that  $p(x)$  has no term of power  $< k + 1$ . The first move of the reduction must be an expansion, giving us a polynomial of order  $c + 1 - k + n$ . The next move must also be an expansion, for there is only one possible collapse, which will simply return us to  $x^{c+1}$ . This second expansion will give us a polynomial of degree greater than  $c + 1 - k + n$ . Our reduction must involve a finite number of a moves, so there is a  $\mu \in \mathbb{N}$  which is the degree of the highest degree term in this reduction. This term must be introduced as the result of an expansion, and we may assume as above that there are no expendable moves in this reduction. Thus, some of the lower degree terms introduced by this expansion must be involved in some move. In fact, they must be involved in collapses, which means that they are removed at some point in the reduction. However the term introduced by this collapse cannot be involved in an expansion, for that expansion would simply be the reverse of the collapse. Thus, this term must be either involved in another collapse or must not be involved in any other move in the

reduction. This applies to any term introduced by a collapse at any point in the reduction. However, the term of order  $\mu$  must be removed by a collapse at some point in the reduction, so the terms that were removed must be replaced at some point. They cannot be replaced by any move resulting from any of the collapses involved in the original removal of these terms. Thus they must be introduced by some expansions independent of the collapses involved in any of those terms, which means that they must be introduced by some expansions independent of expansions introducing terms of order  $\mu$ . But then those terms that were removed could have been originally introduced by these expansions rather than any expansions introducing terms of order  $\mu$ , which means that there is a possible reduction involving terms of order only up to some  $\mu' < \mu$ . Inductively, we can then produce a reduction involving only terms of order up to  $c + 1 - k + n$ , which contradicts what we said above. It should be clear now that there cannot be a reduction if  $a = 1$ ,  $p(x) \neq x^n$ ,  $n = \deg p(x) > k$ , and  $p(x)$  does not have any terms of order  $< k$ .

Finally, assume that  $a = 1$ , that  $\deg p(x) > k$ , and that  $p(x)$  has at least one term of power  $< k$  with nonzero coefficient and assume for a contradiction that the leading coefficient of  $p(x)$  is  $m > 1$ . Every polynomial that is produced in any series of moves beginning with  $x^{c+1}$  will be of the form  $x^{c+1} + (p(x) - x^k)h(x)$ , where  $h(x) \in \mathbb{Z}[x]$ . In particular, this means that any polynomial of degree  $> c + 1$  will have leading coefficient  $\equiv 0 \pmod{m}$ . Our reduction gives us a sequence of moves from  $x^{c+1}$  to a polynomial of lower degree; we can similarly apply this sequence of moves to  $x^{c+1+n-k}$  to get a polynomial of lower degree. But now if we perform an expansion on  $x^{c+1}$  we will have  $p(x)x^{c+1-k}$ ; if we next perform a reduction on only one of the  $x^{c+1+n-k}$  terms, we will obtain a polynomial with leading coefficient  $\equiv -1 \pmod{m}$ , which contradicts the observation that the leading coefficient will always be  $\equiv 0 \pmod{m}$ . Thus, there can be no reduction if the leading term is greater than 1.

To sum up, if  $(\dagger)$  holds and  $a = 0$ , then the leading coefficient must be 1, so  $(i)$  holds. If  $(\dagger)$  holds and  $a > 1$ , then  $p(x) = x^n$ ; if  $a > 1$  and  $p(x) = x^n$ , then  $\deg p(x) > k$ . In other words, if  $a > 1$  then  $(iii)$  holds. If  $(\dagger)$  holds and  $a = 1$  then either  $\deg p(x) < k$  or  $\deg p(x) > k$ ; if  $a = 1$  and  $\deg p(x) > k$  then either  $p(x) = x^n$  or  $p(x) \neq x^n$ ; if  $a = 1$  and  $\deg p(x) > k$  and  $p(x) \neq x^n$  then  $p(x)$  has at least one term of power  $< k$  with nonzero coefficients. Finally, if  $a = 1$ ,  $\deg p(x) > k$ ,  $p(x) \neq x^n$ , and  $p(x)$  has at least one term of power  $< k$  with nonzero coefficients, then  $p(x)$  has leading coefficient 1. This shows that if  $(\dagger)$  holds and  $a = 1$ , then either  $(ii)$ ,  $(iii)$ , or  $(iv)$  holds, and we are done.

□

#### IV. EPIMORPHISMS OF $\mathbb{N}$

An *epimorphism* is a map  $f : R \rightarrow S$  such that given maps  $\varphi : S \rightarrow Q$  and  $\psi : S \rightarrow Q$ , if  $\varphi \circ f = \psi \circ f$ , then  $\varphi = \psi$ . It is a long-standing problem to describe the epimorphic images of a given algebra  $A$ , and Isbell addresses this issue in [3]. In particular, he provides bounds for the size of the collection of epimorphic images of certain kinds of algebras.

We can ask this question with respect to one of the simplest algebras: the natural numbers. We know that there is exactly one rig-homomorphism from  $\mathbb{N}$  to any given rig, so  $\varphi \circ f = \psi \circ f$ . The problem of finding the epimorphic images of  $\mathbb{N}$  is then equivalent to finding the rigs  $R$  for which there is at most *one* homomorphism to any other given rig  $S$ . We will denote the collection of such rigs by  $\Omega$ . Note that we have already found that  $\mathbb{N} \in \Omega$ , but what other rigs can we show to be in  $\Omega$ ?

We can write  $\mathbb{Z} = \mathbb{N}[x]/(x + 1 = 0)$ . Then let  $\varphi, \psi : \mathbb{Z} \rightarrow S$  for some rig  $S$ . We have

$$\varphi(x) + \varphi(1) = \varphi(x + 1) = 0 = \psi(x + 1) = \psi(x) + \psi(1)$$

so that  $\varphi(x)$  and  $\psi(x)$  are both the additive inverse of 1 in the rig  $S$ . It follows that  $\varphi(x) = \psi(x)$  and so  $\mathbb{Z} \in \Omega$ .

Now let  $\varphi, \psi : \mathbb{Q} \rightarrow S$  for some rig  $S$ . Here we have

$$\varphi\left(\frac{1}{n}\right) - \psi\left(\frac{1}{n}\right) = \varphi\left(\frac{1}{n}\right) \varphi(n) \left(\varphi\left(\frac{1}{n}\right) - \psi\left(\frac{1}{n}\right)\right) = \varphi\left(\frac{1}{n}\right) (\varphi(1) - \psi(1)) = \varphi\left(\frac{1}{n}\right) \cdot 0 = 0$$

since  $\varphi$  and  $\psi$  must agree on  $\mathbb{N}$  (and as we have just shown, on  $\mathbb{Z}$ ). Note that it is valid to write  $\varphi(\frac{1}{n}) - \psi(\frac{1}{n})$  since  $S$  contains an image of  $\mathbb{Q}$  and thus must have an additive inverse. Then  $\varphi$  and  $\psi$  must agree at every  $\frac{1}{n}$  and therefore also at every  $\frac{m}{n}$ . Thus  $\mathbb{Q} \in \Omega$ .

It is also easy to see that if  $R \in \Omega$ , then every subrig of  $R$  must also be in  $\Omega$ . This means that all quotients of  $\mathbb{N}$  and  $\mathbb{Q}$ , such as  $\mathbb{N}/(5 = 7)$ , must be in  $\Omega$ .

In fact, Isbell's Corollary 1.6 tells us that  $\Omega$  cannot be a proper class, and his Corollary 1.5 gives us that  $\Omega$  is countable.

**Claim.** No rig of the form  $\mathbb{N}[x]/(\Phi)$ , where  $\Phi$  is some relation in non-negative coefficients with at least quadratic terms in  $x$ , is in  $\Omega$ .

This is easy to see if the relation has more than one complex root, for we can construct two maps from the rig to  $\mathbb{C}$ , each sending  $x$  to a different complex solution.

If the relation has a single root, it must be real and in fact rational. Thus  $\Phi$  must be of the form

$$(ax + b)^n + q(x) = q(x),$$

where  $a$  and  $b$  are integers,  $n \geq 2$ , and  $q(x)$  is a polynomial with non-negative coefficients.<sup>1</sup> But now

---

<sup>1</sup>Actually, this is only accurate if the rational solution is negative. If the solution is positive, some terms will have to be moved to the other side in order to have only non-negative coefficients.

consider  $\varphi, \psi : \mathbb{N}[x]/(\Phi) \rightarrow \mathbb{C}[y]/(y^2 = 0)$  such that  $\varphi(x) = -\frac{b}{a}$  and  $\psi(x) = \frac{y-b}{a}$ .

We now have that the only rigs on one generator with one relation that could possibly be in  $\Omega$  are those with linear relations. Here are the remaining candidates:

$$\begin{array}{llll} (i) \mathbb{N}[x] & (ii) \mathbb{N}[x]/(a = 0) & (iii) \mathbb{N}[x]/(ax = 0) & (iv) \mathbb{N}[x]/(ax + b = 0) \\ (v) \mathbb{N}[x]/(a = b) & (vi) \mathbb{N}[x]/(ax = b) & (vii) \mathbb{N}[x]/(ax + b = c) & (viii) \mathbb{N}[x]/(ax = bx) \\ (ix) \mathbb{N}[x]/(ax + b = cx) & (x) \mathbb{N}[x]/(ax + b = cx + d). & & \end{array}$$

We can immediately see that (i)  $\notin \Omega$ , whereas it is not difficult to show that (ii), (iii), and (v) are in  $\Omega$  only if  $a = 1$  and  $b = 0$ .

(iv) is equivalent to  $\mathbb{Z}[x]/(ax = b)$ . If  $a = 1$ , it is easy to see that (iv) and (vi) are in  $\Omega$ . If  $b = 1$ , we have already shown that (iv) and (vi) are in  $\Omega$ . If both  $a$  and  $b$  are greater than 1, then we can construct maps  $\varphi$  and  $\psi$  mapping from (iv) and (vi) to  $\mathbb{Z}[x][y]/(ax = -b), (ay = -b)$  (or  $= b$ ).  $x$  and  $y$  are distinct elements in this rig if  $a, b > 1$ , so (iv) and (vi) are in  $\Omega$  if and only if at least one of  $a$  and  $b$  is equal to 1.

To eliminate many of the others, we turn to Schanuel.

### Dimension rigs

It turns out that Schanuel's dimension rigs can help us in classifying the rigs in  $\Omega$ . Schanuel defines the dimension rig of the rig  $R$  to be  $\dim R = R/(1 + 1 = 1)$ . For example,  $\dim \mathbb{N}$  is the two-element rig such that  $1 + 0 = 1 + 1 = 1$ ,  $0 + 0 = 0$ , and multiplication is the usual multiplication. Similarly, we find that  $\dim \mathbb{N}[x]$  is the rig consisting of polynomials having coefficients of 1 or 0.

We can calculate the dimension rig of the seven trees rig,  $\dim \mathbb{N}[x]/(x = x^2 + 1)$ , to be the rig consisting of only the three elements 0, 1, and  $x$ , where  $x = x^2 = x + x = x + 1$  and  $1 + 1 = 1$ . To see that  $x = x^2 = x + 1$ , observe that

$$x + 1 = x^2 + 1 + 1 = x^2 + 1 = x = x^2 + 1 = x^2 + x^2 + 1 = x^2 + x = x^3 + x + x = x^3 + x = x^2.$$

In order to use the concept of a dimension rig to our advantage, we will first introduce a definition:

**Definition.** A polynomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , where  $a_i := 0$  for  $i > n$ , is said to be in the same *family* as a polynomial  $b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ , where  $b_i := 0$  for  $i > m$ , if  $a_i = 0$  if and only if  $b_i = 0$ . The idea is that  $p(x)$  and  $q(x)$  are in the same family if  $p(x)$  has a non-zero constant term if and only if  $q(x)$ ,  $p(x)$  has a non-zero linear term if and only if  $q(x)$  does, and so on.

This is clearly an equivalence relation. We will generalize this to polynomial rigs by defining  $\mathbb{N}[x]/(\Phi_1(x) = \Psi_1(x))$  to be in the same family as  $\mathbb{N}[x]/(\Phi_2(x) = \Psi_2(x))$  if  $\Phi_1(x)$  is in the family of  $\Phi_2(x)$  and  $\Psi_1(x)$  is in the family of  $\Psi_2(x)$ .

Note that two rigs in the same family will necessarily have the same dimension rig. In relation to the first portion of the paper, we can see that any rig on one generator that has a reduction must have a finite dimension rig. Therefore any rig in the family of an infinite-dimensional rig cannot have a reduction.

We saw that the dimension rig of the seven trees rig is the three element rig  $\{0, 1, x\}$  such that  $x = x^2 = x + x = x + 1$  and  $1 + 1 = 1$ . But  $x$  and  $1$  both satisfy the relation  $x = x^2 + 1$  in this dimension rig. Therefore, we can define  $\varphi, \psi : \mathbb{N}[x]/(x = x^2 + 1) \rightarrow \dim \mathbb{N}[x]/(x = x^2 + 1)$  such that  $\varphi(x) = x$  and  $\psi(x) = 1$ . It follows that the seven trees rig is not in  $\Omega$ . Furthermore, any rig in the family of the seven trees rig will have the same dimension rig, so similar  $\varphi$ 's and  $\psi$ 's can be constructed, so that for similar reasons we see that no rig of the form  $\mathbb{N}[x]/(ax = bx^2 + c)$ , where  $a$ ,  $b$ , and  $c$  are positive integers, can be in  $\Omega$ .

The dimension rig of  $\mathbb{N}[x]/(x + 1 = 1)$  is  $\{0, 1, x, x^2, \dots\}$ , where  $x^k + x^l = x^{\min\{k,l\}}$ ,  $0 + x^k = x^k$ , and where multiplication is the usual multiplication. We can construct maps  $\varphi, \psi$  from this rig to its dimension rig, where  $\varphi(x) = x$  and  $\psi(x) = 0$ . This rules out (vii).

We can see that  $\mathbb{N}[x]/(x = x) \cong \mathbb{N}[x]$ , so

$$\dim \mathbb{N}[x]/(x = x) = \{1, x, x + 1, x^2, \dots\}.$$

But then we have  $\varphi, \psi : \mathbb{N}[x]/(x = x) \rightarrow \dim \mathbb{N}[x]/(x = x)$  such that  $\varphi(x) = x$  and  $\psi(x) = 1$ . This rules out (viii).

By similar considerations we can see that Schanuel's "rig of geometric quantities",  $\mathbb{N}[x]/(x = 2x + 1)$  is not in  $\Omega$  (it has an infinite dimension rig), nor is any rig in its family. This rules out (ix).

Now it is clear that  $\mathbb{N}[x]/(x + 1 = x + 1) \cong \mathbb{N}[x]$ , so this rig has infinite dimension. This rules out (x).

We have now characterized all rigs on one generator and one relation which are in  $\Omega$ , and they are the trivial rig,  $\mathbb{N}$ ,  $\mathbb{N}[\frac{1}{a}]$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}[\frac{1}{a}]$ . We also know that  $\mathbb{Q} \in \Omega$  and that all quotients of the aforementioned rigs are also in  $\Omega$ .

Further questions open for exploration are:

- (i) What happens when we adjoin more elements?
- (ii) What happens when we quotient by more relations?

Though our exploration of the epimorphic images of  $\mathbb{N}$  is far from complete, it is nonetheless a first step which suggests the question to be not altogether out of reach. Furthermore, our treatment exhibits an interesting application of dimension rigs.

## REFERENCES

- [1] A. Blass, “Seven trees in one”, *J. Pure Appl. Algebra* 103 (1995) 1-21.
- [2] Y. Gallot, “Cyclotomic polynomials and prime numbers”, 2000, <http://perso.wanadoo.fr/yves.gallot/papers/cyclotomic.html>
- [3] J. Isbell, “Epimorphisms and Dominions”, *Proc. Conf. Categorical Algebra* Springer, New York (1966) 232-246.
- [4] S. Schanuel, “Negative sets have Euler characteristic and dimension”, in: A. Carboni, M. C. Pedicchio and G. Rosolini, eds., *Category Theory, Proceedings, Como 1990*, Lecture Notes in Mathematics, Vol. 1488 (Springer, Berlin, 1991) 379-385.