On a Perplexing Polynomial Puzzle

Bettina Richmond

Bettina Zoeller Richmond received her vordiplom from Würzburg, Germany and her Ph.D. from Florida State University. The Nichols-Zoeller theorem, a type of Lagrange theorem for Hopf algebras, is celebrated as a central contribution to the field. Besides Hopf algebras, she wrote on semigroups and ring theory, as well as a textbook in discrete mathematics and several articles for MAA journals. On November 22, 2009, she died unexpectedly at the age of 51.

It seems rather surprising that any given polynomial $p(x)$ with nonnegative integer coefficients can be determined by just the two values $p(1)$ and $p(a)$, where a is any integer greater than $p(1)$. This result has become known as a "perplexing polynomial puzzle" in [2, 3]. Here, we address the natural question of what might be required to determine a polynomial with integer coefficients, if the condition that the coefficients be nonnegative is removed.

Let us analyze the original puzzle. Requiring that $p(x) = c_0 + c_1x + \cdots + c_nx^n$ has nonnegative integer coefficients gives zero as a lower bound and $p(1) = c_0 + c_1 + \ldots + c_n$ as an upper bound for the coefficients. Then if $a > p(1)$, writing $p(a)$ as $c_0 + c_1a + \ldots + c_na^n$ gives the unique base a representation of $p(a)$, so the nonnegative integer coefficients $c_0, c_1, \ldots, c_n$ of $p(x)$ are completely determined by $p(a)$. The coefficients of $p(x)$, which serve as the base a digits, must fall in the appropriate set $\{0, 1, \ldots, a-1\}$, so we must choose a to be an upper bound of the coefficients.

If we allow negative coefficients and find a bound b on the coefficients so that $-b \le c_i \le b$ for all i, then we wonder whether the coefficients are uniquely determined by the value of $p(a) = c_0 + c_1a + \cdots + c_na^n$ for a suitable choice of a. Theorem 3 answers this question affirmatively, giving $a = 2b + 1$ as a suitable choice. In effect, we ask whether $p(a)$ has a unique base a representation if the *digits* c_i assume values from the set $\{-b, -b+1, \ldots, 0, \ldots, b-1, b\}$. Theorem 2 confirms the existence of such a representation.

Nonstandard radix representations.

First we start with the uniqueness of the base a representation with a possibly nonstandard set of *digits*.

Theorem 1 *Let a be a natural number and $R = \{r_i \mid i = 0, 1, \ldots, n\}$ be a set of integers such that $r_i \not\equiv r_j \mod a$ if $i \neq j$. If an integer z has a representation as a sum of powers of a with coefficients from R, then that representation is unique.*

Proof: Let $z = \sum_{i=0}^{m} \lambda_i a^i = \sum_{j=0}^{m'} \mu_j a^j$ where all λ_i and all μ_j are elements of R, and without loss of generality, $m \leq m'$. If $\lambda_i = \mu_i$ for $i = 0, 1, \ldots, m$, then clearly $m = m'$ and we are done. Otherwise, assume s is the smallest index such that $\lambda_s \neq \mu_s$, and thus $\lambda_i = \mu_i$ for $i = 0, 1, \ldots, s-1$. Consider the number u defined by

$$u = \frac{z - \sum_{i=0}^{s-1} \lambda_i a^i}{a^s} = \frac{z - \sum_{i=0}^{s-1} \mu_i a^i}{a^s} = \sum_{i=s}^{m} \lambda_i a^{i-s} = \sum_{j=s}^{m'} \mu_j a^{j-s}.$$

Now $u \equiv \lambda_s \equiv \mu_s \mod a$. By assumption there exists at most one element in R, say r_s, such that $r_s \equiv \lambda_s \mod a$ and hence $r_s = \mu_s = \lambda_s$. So, there exists no smallest index s with $\lambda_s \neq \mu_s$, and the representation of z as a sum of powers of a with coefficients from R is unique. ∎

Any integer z can be uniquely represented in base a as a sum of powers of a using coefficients from $\{0, 1, \ldots, a-1\}$. Next we show that unique representation as a sum of powers of a remains if we specify a different set of permissible coefficients, centered around 0.

Theorem 2 *Let b be a natural number and let $a = 2b+1$. Then every integer z can be uniquely written as $z = \sum_{i=0}^{m} \lambda_i a^i$ where $m \in \mathbb{N}$, $\lambda_i \in \mathbb{Z}$, and $|\lambda_i| \leq b$ for each $i = 0, \ldots, m$.*

Proof: If $\sum_{i=0}^{m} \lambda_i a^i$ is the required representation of a nonnegative integer z, then $\sum_{i=0}^{m} (-\lambda_i) a^i$ is the required representation of $-z$, so without loss of generality, we assume z is a nonnegative integer. Now z has a unique representation in base a as $z = \sum_{i=0}^{m} \mu_i a^i$ where the integers μ_i satisfy $0 \leq \mu_i \leq 2b = a-1$ for all $i = 0, \ldots, m$. To shift the base a digits of z down by b, we add to z the base a number of equal length, all of whose digits are b, find the base a representation for this sum, then subtract the number to recover z. Specifically, consider $z + \sum_{i=0}^{m} b a^i$, which in base a is

$$z + \sum_{i=0}^{m} b a^i = \sum_{k=0}^{m'} \mu'_k a^k,$$

where $0 \leq \mu'_k \leq 2b$ for each k. Observe that $m' = m$ or $m' = m+1$ and $\mu'_{m'} = 1$. Hence

$$z = \sum_{k=0}^{m'} \mu'_k a^k - \sum_{i=0}^{m} b a^i = \begin{cases} \sum_{k=0}^{m'} (\mu'_k - b) a^k & \text{if } m' = m \\[2ex] a^{m'} + \sum_{k=0}^{m'-1} (\mu'_k - b) a^k & \text{if } m' = m+1. \end{cases}$$

Letting λ_k be the coefficient of a^k, the leading coefficient $\lambda_{m'}$ is either $\mu'_m - b$ or 1, and the trailing coefficients are $\lambda_k = \mu'_k - b$. Since $0 \leq \mu'_k \leq 2b$, we have $|\mu'_k - b| \leq b$ and thus $|\lambda_k| \leq b$ for all $k = 0, 1, \ldots, m'$, as required. The uniqueness of the representation follows from Theorem 1. ▪

We next see that, with a bound on the integer coefficients of a polynomial, the polynomial is uniquely determined by its value at one appropriately chosen input.

Theorem 3 *Let $p(x) = c_0 + c_1 x + \cdots + c_n x^n = \sum_{i=0}^{n} c_i x^i$ be a polynomial with integer coefficients $c_0, c_1, \ldots, c_n$. Assume b is a natural number such that $|c_i| \leq b$ for all $i = 0, 1, \ldots, n$. Let $a = 2b+1$. Then the value $p(a)$ uniquely determines the polynomial $p(x)$.*

Proof: Let $p(x), a$, and b be as in the statement of the theorem. By Theorem 2, $p(a) = \sum_{i=0}^{m} c_i a^i$ can be uniquely written as $\sum_{i=0}^{m} \lambda_i a^i$, so $p(a)$ uniquely determines the values of the coefficients c_i and thus of $p(x)$. ▪

Example: Ask a friend to think of a polynomial $p(x)$ with integer coefficients c_i satisfying $|c_i| \leq 10$ for all i. We want to determine $p(x)$ from just one value of $p(x)$. Applying Theorem 3, the bound on the coefficients is $b = 10$, so $a = 2b + 1 = 21$ and we ask for the value $p(21)$. Suppose your friend's concealed polynomial was $p(x) = 3x^4 - 5x^3 + 10x - 6$. She would report $p(21) = 537342$.

Following the idea of the proof of Theorem 1 and using the Euclidean algorithm, we find the unique representation of $p(21)$ as a linear combination $\sum_{i=0}^{m} c_i 21^i$ of powers of 21 using integer coefficients c_i with $|c_i| \leq 10$. Since $p(21) = 537342 = 25587(21) + 15 = 25588(21) - 6$, we know $c_0 = -6$ is the constant term of $p(x)$. We move to the next higher power of 21 and note that, besides the -6 units, $p(21)$ includes $25588(21)$, or 25588 in the 21's place. Now $25588 = 1218(21) + 10$, and since the remainder is between ± 10 inclusive, this remainder 10 must be c_1. Continuing in this manner, $1218 = 58(21) + 0$, and $|0| \leq 10$, so $c_2 = 0$; $58 = 2(21) + 16 = 3(21) - 5$, and $|-5| \leq 10$, so $c_3 = -5$; and finally, $3 = 0(21) + 3$ so $c_4 = 3$. We have now recovered the polynomial $p(x) = \sum_{i=0}^{m} c_i x^i = 3x^4 - 5x^3 + 0x^2 + 10x - 6$.

Refinements.

To apply Theorem 3, we need upper and lower bounds on the coefficients of the polynomial, which we then use to find a single bound b with $|c_i| \leq b$ for each coefficient c_i. In the original puzzle, the requirement that the coefficients be nonnegative gave the lower bound on the coefficients as zero, while the upper bound could be subsequently deduced from $p(1)$. If we are only given a negative lower bound $-b \in \mathbb{Z}$ for the integer coefficients of a polynomial $p(x)$, what else would be needed to deduce an upper bound for the coefficients? Giving one additional value of $p(x)$ will no longer suffice: If $p(a) = v$ is given for $a \neq 0$, the possibilities for p include all polynomials

$$q(x) = v + (a^2 + a^4 + a^6 + \cdots + a^{2n}) - (x^2 + x^4 + x^6 + \cdots + x^{2n}),$$

and since the constant terms of these become arbitrarily large as n increases, no upper bound for the coefficients can be determined from only this information. If $p(a) = v$ is given for $a = 0$, the possibilities for p include all polynomials $q(x) = v + nx$, and again the coefficients are unbounded. In the present case, assuming that a negative lower bound $-b$ for the coefficients has been given, let us additionally assume that the leading coefficient is positive. Then, for $a = 2b + 1$, a is positive, and, if n is the degree of p,

$$p(a) \geq a^n + \sum_{i=0}^{n-1} (-b)a^i = a^n - b\sum_{i=0}^{n-1} a^i = a^n - b\frac{1-a^n}{1-a} = a^n + \frac{1}{2}(1-a^n) = \frac{1}{2}(a^n+1).$$

So, given $p(a) = p(2b+1)$, the largest possible n satisfying $(a^n+1)/2 \leq p(a)$ is an upper bound on the degree of $p(x)$. This, in turn, can be used to find an upper bound for the coefficients c_i of $p(x)$. If $p(x)$ has degree n, less than or equal to n_0, then $p(a) = \sum_{i=0}^{n} c_i a^i$ and thus for $0 \leq j \leq n$, we have

$$c_j \leq c_j a^j = p(a) - \sum_{\substack{i=0 \\ i \neq j}}^{n} c_i a^i \leq p(a) + \sum_{\substack{i=0 \\ i \neq j}}^{n} b a^i \leq p(a) + \sum_{i=0}^{n_0} b a^i,$$

and the coefficients of $p(x)$ have an upper bound. Now, as before, one more value of $p(x)$, chosen according to Theorem 3, will determine the whole polynomial. Thus, a lower bound on the integer coefficients, assuming the leading coefficient is positive, allows a polynomial to be determined by just two values at appropriate integers.

In [1] it was shown that a polynomial $p(x)$ with nonnegative integer coefficients can actually be determined from sufficiently many digits of the value $p(\pi)$. Analogously, given a polynomial $p(x)$ with integer coefficients bounded below by $-b$ ($b \in \mathbb{N}$) and with positive leading coefficient, $p(x)$ can be determined from sufficiently many digits of $p(t)$ for any transcendental number

$t > a = 2b+1$: If $p(x)$ has degree n, we see that

$$\begin{aligned} p(t) &\geq t^n - b\sum_{k=0}^{n-1} t^k = t^n - b\frac{1-t^n}{1-t} \\ &\geq t^n - b\frac{1-t^n}{1-(2b+1)} = \frac{1}{2}(t^n+1). \end{aligned}$$

As before, the largest possible n with $(t^n+1)/2 \leq p(t)$ gives the maximal possible degree of $p(x)$ and, as before, an upper bound on the coefficients of $p(x)$. Since the bound on the degree and the bounds on the integer coefficients of the polynomial in question narrow the possibilities to a finite number of polynomials, a sufficiently large finite number of digits of the value $p(t)$ will determine the given polynomial.

It is easy to verify that an upper bound on the integer coefficients of a polynomial with negative leading coefficient can analogously be determined by either two of its values at appropriate integers or by one value at an appropriate transcendental number.

References

[1] F. Bornemann and S. Wagon, A perplexing polynomial puzzle revisited, College Math. J. **36** (2005) 288.

[2] D. Kalman, *Uncommon Mathematical Excursions: Polynomia and Related Realms*, Dolciani Mathematical Expositions 35, MAA, Washington DC, 2009.

[3] I. B. Keene, A perplexing polynomial puzzle, College Math. J. **36** (2005) 100, solution p. 159.