Integer Valued Polynomials

Rama Kocherlakota

December 14, 2019

1 Beginning

Let's start with a simple question: which polynomials with integer coefficients only produce integers when applied to integers? In other words, if

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

is a polynomial with $a_k \in \mathbb{Q}$, then what are necessary and sufficient conditions on a_k for $p(\mathbb{Z}) \subset \mathbb{Z}$?

It's not hard to come up with an obvious sufficient condition: if $a_k \in \mathbb{Z}$ for all k then clearly $p(j)$ is going to be an integer for every integer value of j. But a little thought tells us that this condition is not necessasry. For instance,

$$\frac{x(x-1)}{2} = \frac{x^2 - x}{2}$$

is always an integer because $x^2 \equiv x \pmod 2$.

It's worth noting that $\frac{x(x-1)}{2}$ is a special kind of polynomial - it's the binomial coefficient $\binom{x}{2}$. This turns out not be coincidental. In particular:

Theorem 1. *Let $p(x)$ be a polynomial of degree n with rational coefficients. Then $p(\mathbb{Z}) \subset \mathbb{Z}$ if and only if there exist integers a_i such that:*

$$p(x) = \sum_{i=0}^{n} a_i \binom{x}{i}$$

Proof. One direction is simple - if x is an integer then so is $\binom{x}{i}$ and so is an integer linear combination of $\binom{x}{i}$. The converse is more interesting and it is what we need to prove.

First, note that the polynmoial

$$c_i(x) = \binom{x}{i}$$

is a product of i linear polynomials in x and thus has degree i and a non-zero coefficient on x^i. It is therefore clear that the $n+1$ polynomials $\{c_0(x), c_1(x), \ldots c_n(x)\}$ are linearly independent over $\mathbb{Q}$ and hence form a basis for the rational polynomials of degree at most n.

Now, let $p(x)$ be a rational polynomial of degree n with $p(x) \in \mathbb{Z}$ whenever $x \in \mathbb{Z}$. Choose rational numbers $a_0, a_1, \ldots a_n$ so that

$$p(x) = \sum_{i=0}^{n} a_i c_i(x)$$

We want to prove that $a_i \in \mathbb{Z}$ for all i. Consider:

$$\begin{aligned} p(x+1) - p(x) &= \sum_{i=0}^{n} a_i (c_i(x+1) - c_i(x)) \\ &= \sum_{i=0}^{n} a_i \left(\binom{x+1}{i} - \binom{x}{i} \right) \end{aligned}$$

But by Pascal's Identity, when $i > 0$

$$\binom{x+1}{i} - \binom{x}{i} = \binom{x}{i-1}$$

and when $i = 0$, $\binom{x+1}{i} - \binom{x}{i} = 0$. We have:

$$\begin{aligned} p(x+1) - p(x) &= \sum_{i=0}^{n} a_i (c_{i-1}(x)) \\ &= \sum_{j=0}^{n-1} a_{j+1} c_j(x) \end{aligned}$$

We can now proceed by induction. First, consider the case $n = 0$. Because $c_0(x) = 1$, if $p(x)$ is an integer for all (even just one) x and $p(x) = a_0 c_0(x)$, it's clear that a_0 is an integer.

Now, for the general inductive case. If $p(x)$ of degree n is always an integer for integer x, then so is $q(x) = p(x+1) - p(x)$. But $q(x)$ is of degree at most $n-1$ and by the above equation

$$q(x) = \sum_{j=0}^{n-1} a_{j+1} c_j(x)$$

By our induction hypothesis, that implies that a_j is an integer for all $j > 0$. Finally, $a_0 = p(0)$ must be an integer, so that proves that all of the a_i are integers. $\square$

2 Relationship between $\binom{x}{n}$ and x^n

Since x^n is an integer whenever x is an integer, Theorem 1 shows that x^n must be expressible as an integer linear combination of the polynomials $c_j(x) = \binom{x}{j}$. Specifically, there must be integers $b_{n,r}$ such that:

$$x^n = \sum_{r=0}^{n} b_{n,r} \binom{x}{r}$$

What are these integers?

What we are doing here is just changing the basis on the vector space of polynomials over $\mathbb{Q}$ of degree at most n from the standard basis $\{1, x, x^2, \dots x^n\}$ to the new basis $\{c_0(x), c_1(x), c_2(x), \dots c_n(x)\}$. This change of basis can be expressed by a rational matrix $(a_{i,j})$ where

$$c_i(x) = \sum_{j=0}^{i} a_{i,j} x^j$$

and the matrix $(b_{i,j})$ corresponds to the opposite change in basis, i.e. to the inverse matrix $(a_{i,j})^{-1}$.

We can explicitly compute $a_{i,j}$ using our formula for $c_j(x)$.

$$c_j(x) = \frac{x(x-1)(x-2)\cdots 1}{n(n-1)(n-2)\cdots 1}$$

We can write a simple Python program using sympy to compute $(a_{i,j})$ and its inverse $(b_{i,j})$. A version of this program is at https://github.com/ramakocherlakota/c-matrix/blob/master/rows.py and its output (for the first few rows and columns of the b matrix) is:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 6 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 14 & 36 & 24 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 30 & 150 & 240 & 120 & 0 & 0 & 0 & 0 \\
0 & 1 & 62 & 540 & 1560 & 1800 & 720 & 0 & 0 & 0 \\
0 & 1 & 126 & 1806 & 8400 & 16800 & 15120 & 5040 & 0 & 0 \\
0 & 1 & 254 & 5796 & 40824 & 126000 & 191520 & 141120 & 40320 & 0 \\
0 & 1 & 510 & 18150 & 186480 & 834120 & 1905120 & 2328480 & 1451520 & 362880
\end{pmatrix}$$

Some facts about this matrix are not surprising. It is lower triangular and the diagonal terms are factorials (this follows from the fact that the coefficient on x^n in $\binom{x}{n}$ is $\frac{1}{n!}$). The zero'th column is just 1 followed by 0's and the first column is 0 followed by 1's (this follows from the facts that $c_0(x) = 1$ and $c_1(x) = x$).

Theorem 2. *(Recurrence relation) The coefficients $b_{n,r}$ of $\binom{x}{n}$ in x^n, defined by*

$$x^n = \sum_{r=0}^{n} b_{n,r} \binom{x}{n}$$

satisfy the following recurrence relation, for $n > 0, r > 0$:

$$b_{n,r+1} = \sum_{i=1}^{n-1} \binom{n}{i} b_{i,r}$$

Proof. By defintion of $b_{n,r}$

$$x^n = \sum_{i=0}^{n} b_{n,i} \binom{x}{i}$$

So

$$\begin{aligned}
(x+1)^n &= \sum_{i=0}^{n} b_{n,i}\binom{x+1}{i} \\
&= \sum_{i=0}^{n} b_{n,i}\left(\binom{x}{i}+\binom{x}{i-1}\right) \\
&= \sum_{i=0}^{n} b_{n,i}\binom{x}{i}+\sum_{i=0}^{n} b_{n,i}\binom{x}{i-1} \\
&= x^n+\sum_{i=0}^{n} b_{n,i}\binom{x}{i-1}
\end{aligned}$$

Because

$$(x+1)^n - x^n = \sum_{r=0}^{n-1}\binom{n}{r}x^r$$

we see that

$$\begin{aligned}
\sum_{j=0}^{n-1}\binom{x}{j}b_{n,j+1} &= \sum_{r=0}^{n-1}\binom{n}{r}x^r \\
&= \sum_{r=0}^{n-1}\binom{n}{r}\sum_{i=0}^{r} b_{r,i}\binom{x}{i} \\
&= \sum_{r=0}^{n-1}\sum_{i=0}^{r} b_{r,i}\binom{n}{r}\binom{x}{i} \\
&= \sum_{i=0}^{n-1}\sum_{r=0}^{n-1} b_{r,i}\binom{n}{r}\binom{x}{i} \\
&= \sum_{i=0}^{n-1}\sum_{r=1}^{n-1} b_{r,i}\binom{n}{r}\binom{x}{i}
\end{aligned}$$

The last two equalities rely on the facts that the b matrix is lower triangular, so that $b_{r,i}=0$ for $i>r$ and further, that $b_{i,0}=0$ when $i>0$.

Since the $\{\binom{x}{i}\}$ form a basis for the polynomials of a given degree, we can equate coefficeints of $\binom{x}{i}$ on the left and right hand sides of the above and conclude that

$$b_{n,i+1} = \sum_{r=1}^{n-1} b_{r,i}\binom{n}{r}$$

Hence the recurrence relation. $\square$

The recurrence relation, together with the already observed values for $b_{0,r}$, means that $b_{n,r} >= 0$ for all n, r. Of course, (by virtue of Theorem 1) they are also integers. Can we find an explicit formula for the entries?

Since the n'th enry in column 1 $b_{n,1} = 1$ for $n > 1$, the recurrence relation implies that

$$b_{n,2} = \sum_{r=1}^{n-1} \binom{n}{r} = 2^n - 2$$

And

$$\begin{aligned}
b_{n,3} &= \sum_{r=1}^{n-1} \binom{n}{r} b_{n,2} \\
&= \sum_{r=1}^{n-1} \binom{n}{r} (2^n - 2) \\
&= \sum_{r=1}^{n-1} \binom{n}{r} 2^n - 2 \sum_{r=1}^{n-1} \binom{n}{r} \\
&= (3^n - 2^n - 1) - 2(2^n - 2) \\
&= 3^n - 3 \cdot 2^n + 3
\end{aligned}$$

More generally, $b_{n,r}$ is the alternating sum of n-th powers, up to r^n, multiplied by binomial coefficients.

Theorem 3. *(Explicit formula) The coefficients $b_{n,r}$ can be written as follows, for $n > 0, r > 0$:*

$$b_{n,r} = (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} j^n$$

Proof. We proceed by induction on r. We have already seen the equation is valid for $r = 1$. By the recurrence relation,

$$\begin{aligned}
b_{n,r+1} &= \sum_{i=1}^{n-1} \binom{n}{i} b_{i,r} \\
&= \sum_{i=1}^{n-1} \binom{n}{i} (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} j^i \\
&= (-1)^r \sum_{j=1}^{r} \sum_{i=1}^{n-1} \binom{n}{i} (-1)^j \binom{r}{j} j^i \\
&= (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} \sum_{i=1}^{n-1} \binom{n}{i} j^i \\
&= (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} ((j+1)^n - j^n - 1) \\
&= (-1)^r \left\{ \left(\sum_{j=1}^{r} (-1)^j \binom{r}{j} (j+1)^n \right) - \left(\sum_{j=1}^{r} (-1)^j \binom{r}{j} j^n \right) - \left(\sum_{j=1}^{r} (-1)^j \binom{r}{j} \right) \right\}
\end{aligned}$$

The third term in the braces is:

$$\sum_{j=1}^{r} (-1)^j \binom{r}{j} = (1-1)^n - 1 = -1$$

The second term is:

$$\sum_{j=1}^{r} (-1)^j \binom{r}{j} j^n = -\sum_{i=0}^{r-1} (-1)^{i+1} \binom{r}{i+1} (i+1)^n$$

Taking the sum of the first and second terms we have:

$$\left(\sum_{j=1}^{r} (-1)^j \binom{r}{j} (j+1)^n \right) + \left(\sum_{i=0}^{r-1} (-1)^{i+1} \binom{r}{i+1} (i+1)^n \right)$$

Again using Pascal's Identity to combine the binomial coefficients, the above expression is:

$$\left(\sum_{j=1}^{r-1} (-1)^j \binom{r+1}{j+1} (j+1)^n \right) - \binom{r}{1} - (-1)^r (r+1)^n = -\sum_{k=2}^{r} (-1)^k \binom{r+1}{k} k^n - r + (-1)^r (r+1)^n$$

Combining all the terms (including the -1 from the third term) and not neglecting to multiply by $(-1)^r$ we end up with:

$$\begin{aligned}
b_{n,r+1} &= (r+1)^n + (-1)^r(-r-1) - \sum_{k=2}^{r}(-1)^{r+k}\binom{r+1}{k}k^n \\
&= (-1)^{r+1}\left((-1)^{r+1}(r+1)^n + \sum_{k=2}^{r}(-1)^k\binom{r+1}{k}k^n - (r+1)\right) \\
&= (-1)^{r+1}\sum_{k=1}^{r+1}(-1)^k\binom{r+1}{k}k^n
\end{aligned}$$

□

Looking specifically at the diagonal and above-diagonal elements of the matrix, we have:

Corollary 1. *For $n > 0$*

$$(-1)^n\sum_{j=1}^{n}(-1)^j\binom{n}{j}j^n = n!$$

For $r > n > 0$,

$$\sum_{j=1}^{r}(-1)^j\binom{r}{j}j^n = 0$$

For example, taking $n = r = 3$:

$$3! = \binom{3}{1} - \binom{3}{2}2^3 + 3^3 = 3 - 24 + 27 = 6$$

And, taking $n = 3$ and $r = 4$,

$$\binom{4}{1} - \binom{4}{2}2^3 + \binom{4}{3}3^3 - 4^3 = 4 - 6\cdot 8 + 4\cdot 27 - 64 = 0$$

Taking $n = 3$ and $r = 5$,

$$\binom{5}{1} - \binom{5}{2}2^3 + \binom{5}{3}3^3 - \binom{5}{4}4^3 + 5^3 = 5 - 10\cdot 8 + 10\cdot 27 - 5\cdot 64 + 125 = -75 + 270 - 320 + 125 = 0$$

3 Conditions for a polynomial to take integer values

We're now in a position to give necessary and sufficient conditions for a polynomial with rational coefficients to map integers to integers.

Theorem 4. *A polynomial $f(x)$ of degree n satisfies $f(\mathbb{Z}) \subset \mathbb{Z}$ if and only if $f(i) \in \mathbb{Z}$ for $i \in \{0, 1, 2, \dots n\}$.*

Proof. One direction is clear - if $f(\mathbb{Z}) \subset \mathbb{Z}$ then $f(\{0, 1, 2, \dots n\}) \subset \mathbb{Z}$. What we want to prove is that $f(\{0, 1, 2, \dots n\}) \in \mathbb{Z}$ implies that $f(\mathbb{Z}) \subset \mathbb{Z}$.

First choose $a_i \in \mathbb{Q}$ so that

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

By the definition of $b_{i,r}$,

$$f(x) = \sum_{i=0}^{n} a_i \sum_{r=0}^{i} b_{i,r} \binom{x}{r}$$

Because, by the Corollary to the Explicit Formula, $b_{i,r} = 0$ for $r > i$,

$$f(x) = \sum_{r=0}^{n} \left(\sum_{i=0}^{n} a_i b_{i,r} \right) \binom{x}{r}$$

Because the $\binom{x}{r}$ are integer-valued, it is enough to prove, that for all $r \in \{0, 1, \dots n\}$

$$\sum_{i=0}^{n} a_i b_{i,r} \in \mathbb{Z}$$

We can use the Explicit Formula for $b_{i,r}$ to prove this.

$$\sum_{i=0}^{n} a_i b_{i,r} = (-1)^r \sum_{i=0}^{n} a_i \sum_{j=1}^{r} (-1)^j \binom{r}{j} j^i \;\; = (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} \sum_{i=0}^{n} a_i j^i = (-1)^r \sum_{j=1}^{r} (-1)^j \binom{r}{j} f(j)$$

But, because $\sum_{i=0}^{n} a_i j^i \in \mathbb{Z}$ for all $j \in \{0, 1, 2, \dots n\}$, this last expression must be an integer. So the coefficients of $\binom{x}{r}$ in the expression for $f(x)$ are integers and $f(x)$ maps integers to integers. $\square$