MA294 Lecture

Timothy Kohl

Boston University

April 11, 2024

Generating Functions

Recall, in the ring $F[x]$ (for F a field) the elements are of the form

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

for $a_i \in F$ where addition is performed degree by degree, and multiplication is carried out as follows:

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m)$$
$$= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + (a_nb_m)x^{n+m}$$

where, in particular, to determine the coefficient of x^k one considers which coefficients 'contribute' in degree k, in particular it is:

$$a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$$

namely the those a_ib_j where $i + j = k$.

As a result, since 1 is the multiplicative identity, one finds that, since $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$ that

$$U(F[x]) = \{a_0 \mid a_0 \in F^*\}$$

i.e. non-zero constant polynomials

i.e. $F[x]$ doesn't contain inverses for most of its elements!

If we extend our view from polynomials to power series (like in Calculus):

$$a_0 + a_1 x + a_2 x^2 + \dots$$

then one has a ring (which contains all polynomials) but with a much richer structure.

Definition

For F a field, the ring of formal power series is

$$F[[x]] = \{a_0 + a_1x + a_2x^2 + \dots \mid a_i \in F\}$$

where addition (like for polynomials) is degree by degree, and multiplication is given by:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{k=0}^{\infty} c_k x^k$$

where

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ &\vdots \\ c_k &= \sum_{t=0}^{k} a_t b_{k-t} \end{aligned}$$

The additive identity is $0 + 0x + 0x^2 + \ldots$ and multiplicative identity is $1 + 0x + 0x^2 + \ldots$ (Exercise!)

Two Important Points:

- A given series $\sum_{i=0}^{\infty} a_i x^i$ is determined by the sequence of coefficients $a_0, a_1, \ldots$
- The variable 'x' is just an indeterminate, we don't consider questions of convergence as one might in calculus, for example, $F[[x]]$ contains series like $1 + x + 2x^2 + 3x^3 + \ldots$ which by (say the ratio test) are divergent.

As indicated earlier $F[[x]]$ has a richer structure and contains all the polynomials in $F[x]$ as a subring.

In particular, (and most importantly for the applications we are trying to develop) many polynomials, for example $f(x) = 1 - x$ have inverses when viewed as elements of $F[[x]]$ in sharp contrast with the fact that $U(F[x]) = F^*$.

Theorem

$\sum_{i=0}^{\infty} a_i x^i \in F[[x]]$ *is invertible if and only if* $a_0 \neq 0$.

Proof:

If $\sum_{j=0}^{\infty} b_j x^j$ has the property that $\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) = 1$ then this implies

$$\begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \\ &\vdots \end{aligned}$$

Assuming $a_0 \neq 0$ then $a_0 b_0 = 1$ implies $b_0 = 1/a_0$. So now, let's try and determine b_1.
Looking at the second equation $a_0 b_1 + a_1 b_0 = 0$ we use what we've just discovered to rewrite this as

$$a_0 b_1 + a_1(1/a_0) = 0$$

which can be solved to yield $b_1 = (-a_1/a_0^2)$, and we can then solve for b_2 by using the third equation:

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$$

which, given that we have already determined b_0 and b_1 (and we alread know all the a_i since they are given in the first place) we can solve for b_2 to get

$$b_2 = a_1^2 a_0^{-2} - a_2 a_0^{-1}$$

and so on...

The point is that $a_0 \neq 0$ implies the existence of b_0 and therefore *all* the remaining b_j which therefore yields that

$$\sum_{j=0}^{\infty} b_j x^j$$

is the inverse of $\sum_{i=0}^{\infty} a_i x^i$. □

What we have shown then is that

$$U(F[[x]]) = \{\sum_{i=0}^{\infty} a_i x^i \mid a_0 \neq 0\}$$

which is much 'larger' than $U(F[x])$ in that it contains more than just 'constants'.

How about $\frac{1}{1-x}$? i.e. $(1-x)^{-1}$

Even though $1-x$ is polynomial, it is technically a series, it's just that the coefficients of all terms beyond degree 1 are zero.

And since the constant term of $1-x$ is non-zero, it has an inverse, which (if you think about it) is a series rather than a polynomial, so it will have infinitely many non-zero terms. Let's find it!

$$(b_0 + b_1 x + b_2 x^2 + \dots)(1-x) = 1$$

implies (after distributing the $(1-x)$) that

$$b_0 + (b_1 - b_0)x + (b_2 - b_1)x^2 + \cdots = 1$$

$b_0 + (b_1 - b_0)x + (b_2 - b_1)x^2 + \cdots = 1 = 1 + 0x + 0x^2 + \ldots$
implies that $b_0 = 1$, and since $b_1 - b_0 = 0$ then $b_1 = 1$, and since $b_2 - b_1 = 0$ then $b_2 = 1$ etc.

Therefore

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots$$

which should be a familiar fact from Calculus! (i.e. geometric series)

And keep in mind, this is formal algebra, we are not concerned about convergence, so we don't 'restrict' x to the interval $(-1, 1)$ which one usually does in that setting.

In general, if $B(x)$ is a polynomial in $F[x]$ then we may regard it as a series in $F[[x]]$ and, if it's invertible, denote its inverse $B(x)^{-1} = \frac{1}{B(x)}$ and if $A(x) \in F[x]$ too, then we have $\frac{A(x)}{B(x)} \in F[[x]]$.

The series for $\frac{A(x)}{B(x)}$ can be computed by a technique known as long division even though the result is generally a series and not a polynomial.

However, this is not terribly efficient, instead we can use a technique that you first see in Calculus 2 typically.

Partial Fractions

$\frac{A(x)}{B(x)}$ is not unfamiliar, recall the technique of partial fractions.

Example: If $B(x) = S(x)T(x)$ where $gcd(S(x), T(x)) = 1$ and $deg(A(x)) < deg(B(x))$ then there exists polynomials $F(x)$, $G(x)$ (where $deg(F) < deg(S)$ and $deg(G) < deg(T)$) such that

$$\frac{A(x)}{B(x)} = \frac{F(x)}{S(x)} + \frac{G(x)}{T(x)}$$

For example, since $2 - 3x + x^2 = (1-x)(2-x)$ then

$$\frac{5-3x}{2-3x+x^2} = \frac{2}{1-x} + \frac{1}{2-x}$$

where, indeed, the numerators on the right are lower degree than the denominators.

The partial fractions algorithm is based on the following basic fact.

Theorem

Let F be a field and $A(x), B(x) \in F[x]$ such that
(i) $deg(A(x)) < deg(B(x))$
(ii) $B(x) = S(x)T(x)$ *where* $gcd(S(x), T(x)) = 1$
(iii) $B_0 \neq 0$
Then there are polynomials $f(x)$ and $g(x)$ such that $deg(f(x)) < deg(S(x))$ *and* $deg(g(x)) < deg(T(x))$ *where*

$$\frac{A(x)}{B(x)} = \frac{f(x)}{S(x)} + \frac{g(x)}{T(x)}$$

where this equation holds in $F[[x]]$.

As far as the determination of the numerators, that is a computational problem, fundamentally a linear algebra question.

Example: $\frac{2+3x+x^2}{(1-x)(2+x)(3-x)} = \frac{A}{1-x} + \frac{B}{2+x} + \frac{C}{3-x}$

So how do we find A, B, C?

If we multiply the above equation by the denominator on the left, $(1-x)(2+x)(3-x)$ we get the following

$$2 + 3x + x^2 = A(2+x)(3-x) + B(1-x)(3-x) + C(1-x)(2+x)$$

which can be simplified.

$$
\begin{aligned}
2 + 3x + x^2 &= A(2+x)(3-x) + B(1-x)(3-x) + C(1-x)(2+x) \\
&= A(6 + x - x^2) + B(3 - 4x + x^2) + C(2 - x - x^2) \\
&= (6A + 3B + 2C) + (A - 4B - C)x + (-A + B - C)x^2
\end{aligned}
$$

So by equating coefficients, this implies

$$
\begin{aligned}
6A + 3B + 2C &= 2 \\
A - 4B - C &= 3 \\
-A + B - C &= 1
\end{aligned}
$$

To solve for A,B, and C we can employ different strategies, but basically we want to eliminate variables.

So if we add the second and third equations:

$$A - 4B - C = 3$$
$$-A + B - C = 1$$

we get $-3B - 2C = 4$.

And if we add $6(-A + B - C = 1)$, namely $-6A + 6B - 6C = 6$ to the *first equation* $6A + 3B + 2C = 2$ we get $9B - 4C = 8$ resulting in the system

$$-3B - 2C = 4$$
$$9B - 4C = 8$$

which can be solved to yield $C = -2$ and $B = 0$, which, in turn, implies $A = 1$.

As such

$$\frac{2+3x+x^2}{(1-x)(2+x)(3-x)} = \frac{A}{1-x} + \frac{B}{2+x} + \frac{C}{3-x}$$
$$= \frac{1}{1-x} - \frac{2}{3-x}$$

and we note that, for examples like the one we just did, where the denominators are all distinct, that one could use a simpler approach to solve for A , B, and C.

Going back to this stage of the calculation:

$$2 + 3x + x^2 = A(2 + x)(3 - x) + B(1 - x)(3 - x) + C(1 - x)(2 + x)$$

we observe that this is true for all $x \in F$ so, in particular we can let $x = 1$, (which makes $1 - x = 0!$):

$$2 + 3 \cdot 1 + 1^2 = A(2 + 1)(3 - 1) + B(1 - 1)(3 - 1) + C(1 - 1)(2 + 1)$$
$$\downarrow$$
$$6 = A \cdot 6$$

namely that $A = 1$, and similarly if we let $x = 3$ two of the terms vanish to yield $20 = C \cdot (-10)$ which implies $C = -2$ of course, a nd similarly, letting $x = -2$ yields $B = 0$.

You may recall a variation of the partial fractions algorithm when one has repeated factors.

If $B(x) = P(x)^m$ where $deg(A(x)) < deg(B(x))$ one has

$$\frac{A(x)}{B(x)} = \frac{H_1(x)}{P(x)^1} + \frac{H_2(x)}{P(x)^2} + \cdots + \frac{H_m(x)}{P(x)^m}$$

We consider an example:

$$\frac{x^3+x^2+x+1}{(x-1)(x-2)^3} = \frac{A}{x-1} + \frac{B}{x-2} + \frac{C}{(x-2)^2} + \frac{D}{(x-2)^3}$$

which is a step up in computational, but not theoretical complexity.
If we do the same 'multiply by the denominator on the left' we get

$$\begin{aligned} x^3+x^2+x+1 = {} & A(x-2)^3 + B(x-1)(x-2)^2 + \\ & C(x-1)(x-2) + D(x-1) \\ & \downarrow \\ & = (A+B)x^3 + (-6A-5B+C)x^2 + \\ & (12A+8B-3C+D)x^2 + (-8A-4B+2C-D) \end{aligned}$$

And if we set $x = 2$ we immediately find that $D = 15$, and letting $x = 1$ we find that $A = -4$ which, since $A + B = 1$ yields $B = 5$, and, from $-6A - 5B + C = 1$ that $C = 2$.

If one has had linear algebra fairly recently, one *could* solve the previous problem using matrices, namely

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ -6 & -5 & 1 & 0 \\ 12 & 8 & -3 & 1 \\ -8 & -4 & 2 & -1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

whose solution

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \begin{pmatrix} -4 \\ 5 \\ 2 \\ 15 \end{pmatrix}$$

is unique (which is guaranteed by the theorem) and agrees with the method used earlier.