# Formal Power Series



Emma Franz

April 28, 2015

## 1 Introduction

The set $S[[x]]$ of formal power series in $x$ over a set $S$ is the set of functions from the nonnegative integers to $S$. However, the way that we represent elements of $S[[x]]$ will be as an infinite series, and operations in $S[[x]]$ will be closely linked to the addition and multiplication of finite-degree polynomials. This paper will introduce a bit of the structure of sets of formal power series and then transfer over to a discussion of generating functions in combinatorics.

The most familiar conceptualization of formal power series will come from taking coefficients of a power series from some sequence. Let $\{a_n\} = a_0, a_1, a_2, \dots$ be a sequence of numbers. Then the formal power series associated with $\{a_n\}$ is the series $A(s) = a_0 + a_1 s + a_2 s^2 + \dots$, where $s$ is a formal variable. That is, we are not treating $A$ as a function that can be evaluated for some $s_0$. In general, $A(s_0)$ is not defined, but we will define $A(0)$ to be $a_0$.

## 2 Algebraic Structure

Let $R$ be a ring. We define $R[[s]]$ to be the set of formal power series in $s$ over $R$. Then $R[[s]]$ is itself a ring, with the definitions of multiplication and addition following closely from how we define these operations for polynomials.

Let $A(s) = a_0 + a_1 s + a_2 s^2 + \dots$ and $B(s) = b_0 + b_1 s + b_1 s^2 + \dots$ be elements of $R[[s]]$. Then the sum $A(s) + B(s)$ is defined to be $C(s) = c_0 + c_1 s + c_2 s^2 + \dots$, where $c_i = a_i + bi$ for all $i \geq 0$. Then

- the **sum** $A(s) + B(s)$ is defined to be $C(s) = c_0 + c_1 s + c_2 s^2 + \dots$, where $c_i = a_i + bi$ for all $i \geq 0$, and
- the **product** $A(s)B(s)$ is defined to be $C(s) = a_0 b_0 + (a_0 b_1 + a_1 b_0)s + \dots + \left(\sum_{i=0}^{k} a_i b_{k-i}\right) s^k + \dots$.

The closure of both of these operations follows from the closure of the operations in $R$. The commutativity and associativity of addition and distributivity of multiplication over addition also follow from these properties in $R$. The additive identity of $R[[s]]$ is the power series where each coefficient is the zero element of $R$, and so given a series $A(s)$, its inverse $-A(s)$ is the series whose coefficients are the inverses in $R$ of the coefficients of $A(s)$. In order to prove multiplicative associativity, we simply need to tease through the definition of multiplication and use the multiplicative associativity of $R$. Multiplicative commutativity and the existence of a multiplicative identity in $R[[x]]$ depend, respectively, on those two properties in $R$. We will show this in the proof of the following theorem.

**Theorem 2.1.** *If $R$ is an integral domain, then $R[[s]]$ is an integral domain.*

*Proof.* Let $A(s)$ and $B(s)$ be two series in $R[[s]]$. Then the coefficient of $x^i$ in the product $A(s)B(s)$ is

$$a_0b_i + a_1b_{i-1} + \ldots + a_ib_0$$

which by the commutativity of $R$ can be rearranged as

$$b_0a_i + b_1a_{i-1} + \ldots + b_ia_0.$$

These are precisely the coefficient of $x^i$ in the product $B(s)A(s)$. Since the coefficients of $x^i$ are equal in $A(s)B(s)$ and in $B(s)A(s)$ for all $i$, multiplication of elements in $R[[s]]$ is commutative.

Since $R$ is an integral domain, $R$ has a multiplicative identity 1. For any series $A(s) = a_0 + a_1s + \ldots$ in $R[[s]]$,

$$\begin{aligned} A(s) &= (1a_0) + (1a_1 + 0a_0)s + (1a_2 + 0a_1 + 0a_0)s^2 + \ldots \\ &= C(s)A(s), \end{aligned}$$

where $C(s) = 1 + 0s + 0s^2 + \ldots = 1$. Also,

$$\begin{aligned} A(s) &= (a_01) + (a_00 + a_11)s + (1a_2 + 0a_1 + a_00 + a_10 + a_21)s^2 + \ldots \\ &= A(s)C(s). \end{aligned}$$

Thus the series $C(s) = 1$ is the identity in $R[[s]]$.

Finally, we must show that there are no zero divisors in $R[[s]]$. Let $A(s)$ and $B(s)$ be two nonzero elements in $R[[s]]$. Then for exist minimal $i$ and $j$ such that $a_i \neq 0$ and $b_j \neq 0$. The coefficient of $s^{i+j}$ in $A(s)B(s)$ is

$$\sum_{k=0}^{i+j} a_kb_{i+j-k}$$

. Where $k < i$, $a_k = 0$ by the minimality of $i$. Where $k > i$, $i + j - k < j$ and so $b_{i+j-k} = 0$ by the minimality of $j$. Thus the only nonzero term of the sum is where $k = i$, $i + j - k = j$. The coefficient of $s^{i+j}$ is equal to $a_ib_j$, which is the product of two nonzero elements in $R$. Thus $a_ib_j$ is nonzero and so $A(s)B(s)$ is also nonzero. Hence $R[[s]]$ has no zero divisors. □

When $F$ is a field, we can also look at $F[[s]]$ as an algebra, where the scalars are elements from $F$.

In order to study the ideals in $F[[s]]$, we must first explore inverses and division. Let $R$ be an integral domain. We can find a multiplicative inverse for any series $A(s) \in R[[s]]$ provided that $a_0$ is a unit in $R$. That is, there is some series $B(s) \in R[[s]]$ such that $A(s)B(s) = 1$. We can prove the existence of $B(s)$ by induction on the number of known coefficients.

The series $A(s)B(s)$ has a constant term of 1 and zeroes for all other coefficients. Since $a_0$ is a unit, $a_0$ has a multiplicative inverse $\frac{1}{a_0}$ and clearly, $b_0 = \frac{1}{a_0}$. Suppose that for some natural number $n$, we know the coefficients of $B(s)$ up to degree $n-1$. Since the coefficient of degree $n$ of $A(s)B(s)$ is equal to zero, we can write

$$\begin{aligned} 0 &= a_0 b_n + a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0 && \text{and, rearranging,} \\ a_0 b_n &= -(a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0) && \\ b_n &= -\frac{1}{a_0}(a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0) && \text{since } a_0 \text{ is a unit.} \end{aligned}$$

Hence, by induction, we can find terms of a series $B(s)$ which satisfies $A(s)B(s) = 1$. Also, since $R$ is commutative it follows that $B(s)A(s) = 1$.

We only have multiplicative inverses for elements of $R[[s]]$ where the constant term is a unit, but we will be able to use this fact to show that all ideals in $F[[s]]$, where $F$ is a field, are principal.

**Theorem 2.2.** *Let $F$ be a field. Then $F[[s]]$ is a principal ideal domain.*

*Proof.* Let $I$ be an ideal in $F[[s]]$, the set of formal power series over an integral domain $F$. The ideal containing only the zero element is principal, so let us assume that $I$ contains at least one nonzero element. For each nonzero element $A(S)$ in $F[[s]]$, there exists $m$ such that $a_m \neq 0$ and $a_n = 0$ for all $n < m$. Let $M$ be the minimal such $m$ over all the nonzero elements of $F[[s]]$. Therefore, there exists some series $A(s)$ such that $a_n = 0$ for $n < M$ and $a_M \neq 0$. Let $B(s)$ be the series $a_M + a_{M+1}s + \ldots$. Then by construction, $A(s) = s^M B(s)$. Since $B(s)$ has a nonzero constant term, the series has a multiplicative inverse $\frac{1}{B(s)}$. Thus we can write $A(s)\frac{1}{B(s)} = s^M$, and so by the absorption property of the ideal, $s^M \in I$. Thus $s^M F[[s]] \subseteq I$. Also, each element of $I$ has zeroes for coefficients of up to $s^M$, and so each can be written as the product of $s^M$ with a series in $F[[s]]$, implying that $I \subseteq s^M f[[s]]$. Therefore $I$ is generated by the element $s^M$ and so $I$ is a principal ideal. □

An ascending chain of ideals for $F[[s]]$ would look like $s^k F[[s]] \subset s^{k-1} F[[s]] \subset \ldots \subset sF[[s]] \subset F[[s]]$.

If $R$ is not a field, it is more difficult to state anything about the ideals of $R[[s]]$. The following lemma will help with that.

**Lemma 2.3.** *Let $R$ be a ring and let $I$ be an ideal in $R[[s]]$. For $A(s)$ in $R[[s]]$, let $a_m$ be the coefficient of the nonzero term of lowest degree. Let $J = \{a_m | A(s) \in R[[s]]\}$. Then $J$ is an ideal in $R$.*

*Proof.* Let $c$ be an element in $R$ and assume $I$ nonempty. Let $j$ be in $J$. Then for some $A(s)$ in $I$, $A(s) = 0 + 0s + 0s^2 + \ldots + js^g + \ldots$. Since $I$ is an ideal and $c = c + 0s + 0s^2 + \ldots$ is an element of $R[[s]]$, $cA(s)$ is also an element of $I$. The coefficient of the nonzero term of lowest degree for $A(s)$ is $cj$. Thus $cj \in J$. Therefore $J$ is an ideal in $R$. □

A more complicated proof is that of the statement:

**Proposition 2.4.** *Let $R$ be a Noetherian ring. Then $R[[s]]$ is Noetherian.*

The proof requires us to take an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ in $R[[s]]$ and find the corresponding chain $J_1 \subseteq J_2 \subseteq J_3 \subseteq \dots$ in $R$ where $J_i$ is defined for $I_i$ the same way that $J$ is for $I$ in the lemma. Since $R$ is Noetherian, we can use the equality of $J_m$ with $J_n$ for all $m \geq n$, for some $n$, to show that each ideal $I_i$ is finitely generated. Then we know that $R[[s]]$ is Noetherian.

## 3 Formal Power Series in Combinatorics

One of the settings where formal power series appear is in the context of combinatorics, where it can be valuable to look at these power series without worrying about questions of convergence. The formal power series $a_0 + a_1 s + a_2 s^2 + \dots$ appears as the generating function of the sequence $a_0, a_1, a_2, \dots$. We will look at two examples from [3].

An example of how generating functions might appear that does not get into the question of infinite series is a problem that deals with finding the number of nonnegative integers whose digits add up to a desired number. We allow the digits to range from 0 to 9, allowing for numbers like "003" or "00." For example, if $n = 5$, then 0140, 23, and 5 are examples of four-digit, two-digit, and one-digit numbers (respectively).

Consider the series

$$A_1(s) = 1 + s + s^2 + s^3 + \dots + s^9.$$

The coefficient $a_n$ of $s^n$ is the number of one-digit numbers $m$ with the sum of the digits of $m$ equal to $n$. Let us take a look at the series where $a_n$ is the number of two-digit numbers with sums of the digits equal to $n$. The first few terms of the series can be easily shown to be

$$A_2(s) = 1 + 2s + 3s^2 + 4s^3 + \dots.$$

It is also clear that $A_2(s)$ will be a polynomial of degree 18, since 18 is the highest number that can be written as the sum of two digits.

**Lemma 3.1.** *Let $a_n$ be the coefficient of $s^n$ in $A_1(s)$ and let $a'_n$ be the coefficient of $s^n$ in $A_2(s)$. Then $a'_n = a_0 a_n + a_1 a_{n-1} + \dots a_n a_0$. Equivalently, $A_2(s) = (A_1(s))^2$.*

*Proof.* Each term $a_k a_j$ in the sum represents the total number of ways to write a two-digit number where the first digit is $k$ and the second digit is $j$. We sum up over all choices of $k$ and $j$ where $k + j = n$. □

**Lemma 3.2.** *Let the coefficient $a''_n$ of $s^n$ in $A_3(s)$ be equal to the number of three-digit numbers whose the sum of the digits is $n$. Then $A_3(s) = (A_1(s))^3$.*

*Proof.* Let $A_1(s) = a_0 + a_1 s + a_2 s^2 + \dots$ and let $A_2(s) = a'_0 + a'_1 s + a'_2 s^2 + \dots$. We can write a three-digit number whose digits add up to $n$ by juxtaposing a two-digit number whose digits add up to $k$ with a one-digit number whose digits add up to $j$, where $n = j + k$. There are $a'_k a_j$ juxtapositions of this form. Summing up over all possibilities for $j$ and $k$ yields

$$\sum_{i=0}^{n} a'_i a_{n-i}.$$

Thus $A_3(s) = A_2(s) A_1(s) = (A_1(s))^3$. □

We can use this process to find a generating function whose coefficients tell us how many $k$-digit numbers there are with digits adding up to some nonnegative integer.

Let us look at a related example where the generating function we will find has infinitely many terms.

A *partition* of a number $n$ is a set of positive integers that sum to $n$. We no longer have the restriction from 0 to 9 of the summands, and now we have that two sums that have the same summands listed in a different order are equivalent. The partitions of a few small numbers are as follows:

$$\begin{array}{ll} n=1 & 1 \\ n=2 & 2=1+1 \\ n=3 & 3=2+1=1+1+1 \\ n=4 & 4=3+1=2+2=2+1+1=1+1+1+1 \end{array}$$

Let $p_n$ be the number of partitions of $n$. Then $p_0 = 1$, since the empty sum is a partition, and as we see from above $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, and $p_4 = 5$.

What is the generating function for $p_n$? Let $P_1(s)$ be the generating function for the number of partitions of $n$ where each of the summands is 1. Since there is one such partition for each $n$, where $n \geq 0$,

$$P_1(s) = 1 + s + s^2 + \ldots.$$

Multiplying each side of this equation by $s$ yields

$$\begin{aligned} sP_1(s) &= s + s^2 + s^3 + \ldots \\ &= P_1(s) - 1 \end{aligned}$$

which allows us to write

$$P_1(s) = \frac{1}{1-s}.$$

Let $P_2(s)$ be the generating function for the number of partitions of $n$ where each of the summands is 2. For $n$ even, there is one such partition of $n$. For $n$ odd, there are no such partitions. Thus

$$P_2(s) = 1 + s^2 + s^4 + \ldots.$$

Then we can multiply each side by $s^2$ to get

$$\begin{aligned} s^2P_2(s) &= s^2 + s^4 + s^6 + \ldots \\ &= P_2(s) - 1 \end{aligned}$$

and so

$$\begin{aligned} 1 &= (1-s^2)P_2(s) \\ \frac{1}{1-s^2} &= P_2(s). \end{aligned}$$

The partitions of $n$ where the summands are all either 1 or 2 can be constructed as sums of partitions of $k$ where the summands are all 1 and partitions of $n-k$ where the summands are all 2. Summing up over all possibilities for $k$, we find that the number of partitions of $n$ with summands all equal to 1 or 2 is

$$\sum_{k=0}^{n} b_k c_{n-k},$$

where $b_k$ is the number of partitions of $k$ with summands all equal to 1 and $cn - k$ is the number of partitions of $n-k$ with summands all equal to 2. Therefore the generating function for the number of partitions of $n$ where the summands are 1 or 2 is

$$P_1(s)P_2(s) = \frac{1}{(1-s)(1-s^2)}.$$

Repeating this process, we find that the generating function for the number of partitions of $n$ where the summands are no greater than $k$ is equal to

$$P_1(s)P_2(s)P_3(s)\dots P_k(s) = \frac{1}{(1-s)(1-s^2)(1-s^3)\dots(1-s^k)}.$$

The generating function for the number of partitions of $n$ with no restrictions on $n$ is thus

$$\begin{aligned} P(s) &= P_1(s)P_2(s)P_3(s)\dots \\ &= \frac{1}{(1-s)(1-s^2)(1-s^3)\dots}. \end{aligned}$$

Define the formal power series $Q(s)$ to be

$$Q(s) = (1-s)(1-s^2)\dots.$$

Let us consider how to find the coefficient $q_k$ of $Q(s)$. Define the series

$$Q_k(s) = (1-s)(1-s^2)\dots(1-s^k)$$

and let $q'_k$ be the coefficient of $s^k$ in $Q_k(s)$. Notice that

$$\begin{aligned} Q_{k+1}(s) &= (1-s^{k+1})Q_k(s) \\ &= Q_k(s) - s^{k+1}Q_k(s) \end{aligned}$$

. Thus the coefficient of $s^k$ in $Q_{k+1}(s)$ is also equal to $q'_k$. By repeating this process, we will find that the coefficient of $s^k$ is unaffected by multiplications of $(1-s^{k+i})$ for $i > 0$. Hence $q_k = q'_k$. We can find the coefficients up to $q_k$ of $Q(s)$ by taking the coefficients from $Q_k(s)$. The first few terms of $Q(s)$ are as follows:

$$Q(s) = 1 - s - s^2 + s^5 + s^7 - s^12 - \dots. \tag{1}$$

An identity for $Q(s)$ was conjectured by Euler:

**Theorem 3.3.**

$$Q(s) = 1 + \sum_{k=1}^{\infty} (-1)^k \left( s^{\frac{3k^2-k}{2}} + s^{\frac{3k^2+k}{2}} \right).$$

We have that

$$P(s) = \frac{1}{Q(s)}, \qquad \text{which gives us that}$$
$$P(s)Q(s) = 1.$$

We already know that $p_0 q_0 = 1$. Then

$$\sum_{i=0}^{k} q_i p_{k-i} = 0$$

for all $k > 0$. This yields

$$0 = p_k + \sum_{i=1}^{k} q_i p_{k-i}$$
$$p_k = -\sum_{i=1}^{k} q_i p_{k-i}.$$

Along with (1), this yields the recurrence relation

$$p_n = p_{n-1} + p_{n-2} - p_{n-5} - p_{n-7} + \dots,$$

which is a finite sum since $p_k = 0$ for all negative $k$.

Although this did not give us a closed form for the number of partitions of an integer $n$, we do now have a way to calculate $p_n$ based on the number of partitions for integers smaller than $n$, and we have hopefully had a taste for how formal power series might be used in combinatorial problems. Even in situations where an infinite power series' convergence is in doubt or depends on where it is evaluated, we can use formal power series and the operations we have defined on formal power series to create a meaningful representation of what is going on and generate solutions.

## References


[1] Chaieb, A. (2011). *Formal Power Series.* Journal of Automated Reasoning, 47(3), 291-318.

[2] Godsil, C. (1993). *Algebraic Combinatorics.*

[3] Lando, S. (2003). *Lectures on Generating Functions.*

[4] Niven, I. (1969). *Formal Power Series.* The American Mathematical Monthly, 76(8), 871-889.