Noncommutativity and Combinatorial Problems

Professor D.M. Jackson

Department of Combinatorics and Optimization
Faculty of Mathematics
University of Waterloo

June 12, 2002

Contents

Chapter 1

Introduction

This talk is about methods of solution of a wide class of problems in Combinatorics (or Discrete Mathematics) called sequence problems. The general question in this class is to determine the number of sequences in a given set of symbols (called the *alphabet*) that satisfy prescribed conditions. It is also a talk about an approach that uses a combination of combinatorial ideas and ideas from abstract algebra, but in a concrete setting. Finally, it is a talk about the concrete benefits that occur when good abstractions are made.

I have prepared this set of Notes so that you will have a full and accurate record of the talk, and so that you will be able to study the material further on your own, if the ideas attract you. There are problems for you to work on in the last chapter.

1.1 An example of a sequence problem

It is reasonable to ask why is the counting of sequences interesting, so I will give you a very famous problem that is easy to state and that no one has solved.

The Excluded Volume Problem

On a rectangular grid with origin O, you are allowed to take a walk starting at O and finishing at O. A *walk* is a sequence of steps, each of unit length, in the directions *east*, *north*, *west* or *south*. The condition is that the walk is not allowed to cross itself, and the problem is to find a formula for the number of walks with n steps.

Its origin

The problem comes from the physical sciences and concerns chemical compounds called polymers (plastic is an example). The chemical diagrams for polymers are long and stringy. It is a law of physics that no site in space can be occupied twice: once an infinitesimal *volume* in space is occupied, it is *excluded* from further occupancy. The number is needed for the determination of the energy function. This perplexing problem is called the Excluded Volume Problem, and there is a Noble Prize awaiting the person who can solve it.

The corresponding sequence problem

This problem can be encoded as a sequence as follows. Let E, N, W and S denote the four types of step. Then a sequence in the alphabet $\{E, N, W, S\}$ defines a walk, starting by convention from O. For example, $SWNE$ is a walk around the boundary of a unit square in a clockwise direction, with O at the northeast corner. Since a walk starts and finishes at the same point, $\#N$'s $=$ $\#S$'s, and $\#W$'s $= \#E$'s. Since a walk is not permitted to cross itself, $SWNE$, $ENWS$, $NEESWSW$, among others, are forbidden as subsequences. Thus the Excluded Volume Problem can be viewed as a question of counting sequences that possess none of the forbidden subsequences.

Best known results

The best known result so far is an approximate one that takes account of all forbidden subsequences up to a particular length. The idea is that the longer forbidden subsequences rule out, relatively, fewer and fewer sequences. The result was obtained quite recently by a colleague, Doron Zeilberger, and his doctoral student, who used a theorem that Ian Goulden and I obtained many years ago in an entirely different connexion.

1.2 Sequences as encoding devices for combinatorial structures

It has been seen how sequences can be used to encode the Excluded Volume Problem. This is not an exceptional case. There are many instances where sequences play this role.

An applied problem

For example, I have included a problem that happened to be sent to me from one of the computer research organisations. It is a question that comes from the optimization of a computer code for a filing system, and involves the determination of the probability that a particular branch of the code will be executed. It appears as Problem 8.

General theory

Part of combinatorics concerns itself with counting the number of sequences that satisfy various conditions. Even quite mild conditions can produce questions that are very hard indeed. In this talk I am going to explore what can be done when the conditions use only the relationship between adjacent symbols. The Excluded Volume Problem is in this class, so this class is a significant one.

1.3 Noncommutativity, rings, homomorphisms

First of all, do not be intimidated by these terms. You are already familiar with operations that do *not commute*. For example, "add 1 and multiply by 2" is not the same as "multiply by 2 and add 1." "Putting on hiking boots and then walking twenty miles" is very different from "walking twenty miles and then putting on hiking boots" (pachyderms excluded).

You already have some experience with *rings* without realising it, because the rules (we call them *axioms*) for a ring list the permissible operations, such as multiplying out brackets and collecting terms, in High School algebra.

Homomorphisms will be new to you, but they are functions, and they allow you to do legally what you have always be tempted to do with functions, which is to assume that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$. Not all functions are homomorphisms. For example, $\sin(x + y) \neq \sin(x) + \sin(y)$ and $\sin(xy) \neq \sin(x)\sin(y)$; $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$, although $\sqrt{xy} = \sqrt{x}\sqrt{y}$. Far from being difficult, homomorphisms put one into that blissful world where everything begins to simplify.

Ideas

I am going to use no operations more complex than $+$ (addition) and $\cdot$ (multiplication), but the multiplication is to be *noncommutative* (so $ab \neq ba$). Moreover, these operations will be used in a fairly sophisticated way. The variables are to be a and b (we call them *indeterminates*) and all of our expressions will be formed from these. They will be polynomials and infinite series.

There will be familiar rules that specify the operations that are legal on expressions. These you have seen before, but I am going to be careful about expressing them in detail. The object produced by these rules is a *noncommutative ring.*

In addition, I am going to use three very carefully designed functions, one (δ) for deleting unwanted information, another (ϕ) for recording counting information, and a third (θ) for pulling out a particular class of sequences (called *permutations*) that are of special interest. Each of these functions turn out to be a *homomorphism.* These functions act on rings.

These, then, are the names of the tools to be used.

What I do

Perhaps I should let you know a little of what I do. My research deals with discrete structure and its analysis through combinatorial means and through algebraic and analytic techniques, with applications to a variety of questions in topology, the theory of functions and to mathematical physics. Such things are only seen at the university level.

1.4 Problems

It is useful to have a collection of problems to work on and to assist in the explanation of the ideas. These are Problems 1 to 9, and they are solved in the Notes. At the end of the Notes are some questions for you to work on yourselves. They can all be solved by the theory explained here.

1.5 Review of some familiar results

I am going to assume that you are familiar with the binomial theorem, the solution of linear equations by Crámer's Rule, multiplication of small matrices, the expansions of series such as e^x and $(1-x)^{-1}$, and elementary properties of determinants.

Chapter 2

Noncommutation

2.1 Problem 1

Find the number c_2 of $\{0,1\}$-sequences of length 2.

The usual solution

The set of $\{0,1\}$-sequences of length 2 is $\{00, 01, 10, 11\}$, so $c_n = 4$.

Encoding the sequences

I am going to look at this problem in greater detail to squeeze some more general ideas out of it. The first idea is to represent this set in a more convenient way by using the translation

$$0 \leftrightarrow \mathsf{a}, \quad 1 \leftrightarrow \mathsf{b}.$$

Then this set becomes $\{\mathsf{aa}, \mathsf{ab}, \mathsf{ba}, \mathsf{bb}\}$ and, encoded as polynomial, this becomes

$$\mathsf{a}^2 + \mathsf{ab} + \mathsf{ba} + \mathsf{b}^2.$$

Clearly, we require that a and b do not commute, for otherwise $\mathsf{ab} = \mathsf{ba}$ so the sequences 01 and 10 would be indistinguishable, and this would defeat our purpose. In other words, the algebraic statement that a and b to not commute is a direct consequence of the combinatorial statement that you cannot interchange different symbols in a sequence without changing the sequence into a different one.

Deleting unwanted information

The second idea is to use the substitution function δ such that

$$\mathsf{a} \mapsto 1, \quad \mathsf{b} \mapsto 1.$$

Then

$$\begin{aligned}\delta\left(\mathsf{a}^2+\mathsf{ab}+\mathsf{ba}+\mathsf{b}^2\right) &= \delta(\mathsf{a}^2)+\delta(\mathsf{ab})+\delta(\mathsf{ba})+\delta(\mathsf{b}^2)\\ &= \delta(\mathsf{a})\delta(\mathsf{a})+\delta(\mathsf{a})\delta(\mathsf{b})+\delta(\mathsf{b})\delta(\mathsf{a})+\delta(\mathsf{b})\delta(\mathsf{b})\\ &= 1^2+1^2+1^2+1^2\\ &= 4.\end{aligned}$$

This explains why the function δ has been introduced in the first place. It preserves the relevant information (the number of sequences), and deletes the rest (what the sequences actually were).

δ as a homomorphism for deleting sequences

Let us formally record the three very convenient properties that the substitution function δ has. For any polynomials f and g in the a's and b's

$$\left.\begin{aligned}\delta(\mathsf{f}+\mathsf{g}) &= \delta(\mathsf{f})+\delta(\mathsf{g}) && \text{(additivity property)},\\ \delta(\mathsf{fg}) &= \delta(\mathsf{f})\,\delta(\mathsf{g}) && \text{(multiplicative property)},\\ \delta(1) &= 1.\end{aligned}\right\}$$

The first states that δ can be applied to each sequence in a set. The second states that it can be done symbol by symbol. This is what I meant in the Introduction by saying that we will use functions that preserve counting information and that also behave *nicely* with respect to addition and multiplication. In general, a function that satisfies the above three conditions is called a *homomorphism*, and δ is a concrete example of such a function. We have just made use of the first two of these properties in the above example.

The solution

Observe that

$$\begin{aligned}\mathsf{a}^2+\mathsf{ab}+\mathsf{ba}+\mathsf{b}^2 &= \left(\mathsf{a}^2+\mathsf{ab}\right)+\left(\mathsf{ba}+\mathsf{b}^2\right)=\mathsf{a}\left(\mathsf{a}+\mathsf{b}\right)+\mathsf{b}\left(\mathsf{a}+\mathsf{b}\right)\\ &= \left(\mathsf{a}+\mathsf{b}\right)^2.\end{aligned}$$

In this simplification, only standard properties of expanding brackets has been used, although care has been taken with noncommutativity.

The solution to the problem is therefore

$$\begin{aligned}c_2 &= \delta\left((\mathsf{a}+\mathsf{b})^2\right) \quad \text{(encoding the problem)}\\ &= (\delta(\mathsf{a})+\delta(\mathsf{b}))^2 \quad (\delta \text{ is a homomorphism})\\ &= (1+1)^2 \quad (\text{definition of } \delta)\\ &= 4.\end{aligned}$$

Constructing as opposed to listing the elements of a set

The usual solution made use of a listing of the elements of the set one by one. In general, however, we have to assume that the sets are too complicated for this to be feasible, so it is necessary immediately to move away from listing. Instead, we consider an algorithm of constructing all of the elements in a set, and then attempt to turn this algorithm into a mathematical expression.

The algorithm and the corresponding mathematical expression ought to be clear in this case. In a $\{0,1\}$-sequence of length 2, the first symbol is 0 or 1, symbolised by $\mathsf{a}+\mathsf{b}$, and the second symbol is 0 or 1, symbolised by a second $\mathsf{a}+\mathsf{b}$. Combining these choices serially we have

$$(\mathsf{a}+\mathsf{b})^2$$

as the mathematical expression corresponding to this algorithm for constructing $\{0,1\}$-sequences. In other words, we could have written down this expression straightaway, without listing the sequences in the set.

2.2 Problem 2

Find the number c_n of $\{0,1\}$-sequences of length n.

The usual solution

You will all know that the answer to this problem is 2^n.

The solution

The mathematical expression that corresponds to the construction of the set of all sequences of length n is $(\mathsf{a}+\mathsf{b})^n$. We can use the above approach, and assert that

$$\begin{aligned}
c_n &= \delta\left((\mathsf{a}+\mathsf{b})^n\right) \quad \text{(encoding the problem)}\\
&= (\delta(\mathsf{a})+\delta(\mathsf{b}))^n \quad (\delta \text{ is a homomorphism})\\
&= (1+1)^n \quad (\text{definition of } \delta)\\
&= 2^n.
\end{aligned}$$

Moreover, explicit listing of the elements of the set has been avoided.

2.3 Problem 3

Find the number $c_{2,k}$ of $\{0,1\}$-sequences of length 2 with k 1's.

The usual solution

There are 2 positions in a sequence of length 2, and k of the are to be occupied by 1's, and the rest by 0's, so

$$c_{2,k} = \binom{2}{k}.$$

ϕ as a homomorphism for recording counting information

I am going to look at this problem in a different way to discover another homomorphism, and to show how to prove that it is indeed a homomorphism.

We can use the above approach by designing a function ϕ that works on a product t of a's and b's to record the number of 1's. The function must be

$$\phi(\mathsf{t}) = u^{\#_{\mathsf{b}}(\mathsf{t})}\mathsf{t},$$

where $\#_{\mathsf{b}}(\mathsf{t})$ is the number of occurrences of b in t. We call t a *term*. Let $\{\mathsf{t}_0, \mathsf{t}_1, \mathsf{t}_2, \ldots\}$ be the set of all terms formed from a's and b's, with $\mathsf{t}_0 = 1$. If you wish, suppose that the terms have been indexed in lexicographic (dictionary) order. A *series* in a and b has the form

$$\mathsf{f} = \alpha_0 1 + \alpha_1\mathsf{t}_1 + \alpha_2\mathsf{t}_2 + \cdots,$$

where the α_i's are rational numbers. We *define* ϕ to apply term by term to such series, so

$$\phi(\mathsf{f}) = \alpha_0\phi(1) + \alpha_1\phi(\mathsf{t}_1) + \alpha_2\phi(\mathsf{t}_2) + \cdots.$$

Algebraists express this by saying that ϕ is *extended linearly.* It follows that if g is another series, then

$$\phi(\mathsf{f}+\mathsf{g}) = \phi(\mathsf{f}) + \phi(\mathsf{g}).$$

This additive property, as we have seen, is part of the definition of ϕ, so it is not something to be proved.

Proving the multiplicative property for ϕ

A proof of the multiplicative property is, however, needed. If t and t' are terms then it is simple combinatorial property of $\#_{\mathsf{b}}$ that

$$\#_{\mathsf{b}}(\mathsf{t}\mathsf{t}') = \#_{\mathsf{b}}(\mathsf{t}) + \#_{\mathsf{b}}(\mathsf{t}').$$

Then

$$\phi(\mathsf{t}\mathsf{t}') = u^{\#_{\mathsf{b}}(\mathsf{t}\mathsf{t}')}\mathsf{t}\mathsf{t}' = u^{\#_{\mathsf{b}}(\mathsf{t})+\#_{\mathsf{b}}(\mathsf{t}')}\mathsf{t}\mathsf{t}' = \left(u^{\#_{\mathsf{b}}(\mathsf{t})}\mathsf{t}\right)\left(u^{\#_{\mathsf{b}}(\mathsf{t}')}\mathsf{t}'\right) = \phi(\mathsf{t})\phi(\mathsf{t}').$$

This can be extended from terms to series as follows. Let g be the series $\mathsf{g} = \sum_{i\geq 0}\beta_i\mathsf{t}_i$. Then

$$\mathsf{f}\mathsf{g} = \left(\sum_{i\geq 0}\alpha_i\mathsf{t}_i\right)\left(\sum_{j\geq 0}\beta_j\mathsf{t}_j\right) = \sum_{i,j\geq 0}\alpha_i\beta_j\mathsf{t}_i\mathsf{t}_j,$$

so

$$\begin{aligned}
\phi(\mathsf{fg}) &= \phi\left(\sum_{i,j\geq 0}\alpha_i\beta_j\mathsf{t}_i\mathsf{t}_j\right)\\
&= \sum_{i,j\geq 0}\alpha_i\beta_j\phi(\mathsf{t}_i\mathsf{t}_j) \quad \text{(definition of } \phi)\\
&= \sum_{i,j\geq 0}\alpha_i\beta_j\phi(\mathsf{t}_i)\phi(\mathsf{t}_j) \quad \text{(proved above)}\\
&= \left(\sum_{i\geq 0}\alpha_i\phi(\mathsf{t}_i)\right)\left(\sum_{j\geq 0}\beta_j\phi(\mathsf{t}_j)\right)\\
&= \phi(\mathsf{f})\phi(\mathsf{g}) \quad \text{(definition of } \phi).
\end{aligned}$$

Summarising these properties, we have

$$\left.\begin{aligned}
\phi(\mathsf{f}+\mathsf{g}) &= \phi(\mathsf{f})+\phi(\mathsf{g}),\\
\phi(\mathsf{fg}) &= \phi(\mathsf{f})\,\phi(\mathsf{g}),\\
\phi(1) &= 1.
\end{aligned}\right\}$$

Thus we conclude that ϕ is a *homomorphism*.

The solution

If f is a series in u and x, let $[x^2u^k]f$ denote the coefficient of u^kx^n in f.

Let δ be the substitution function defined by $\delta(\mathsf{a}) = x$ and $\delta(\mathsf{b}) = x$. Then δ is a homomorphism. Moreover, it records the number of a's and b's in terms, and so records the *length* of the corresponding $\{0,1\}$-sequence.

The set of all $\{0,1\}$-sequences of length 2 is encoded as $(\mathsf{a}+\mathsf{b})^2$. Now apply ϕ to record the number of 1's, to get

$$\begin{aligned}
c_{2,k} &= \left[x^2u^k\right]\,\delta\phi\left((\mathsf{a}+\mathsf{b})^2\right) \quad \text{(encoding the problem)}\\
&= \left[x^2u^k\right]\,\delta\left((\mathsf{a}+u\mathsf{b})^2\right) \quad (\phi \text{ is a homomorphism})\\
&= \left[x^2u^k\right]\,(x+ux)^2 \quad (\delta \text{ is a homomorphism})\\
&= \left[x^2u^k\right]\,x^2\,(1+u)^2\\
&= \left[u^k\right]\,(1+u)^2\\
&= \binom{2}{k} \quad \text{(binomial theorem)}.
\end{aligned}$$

The series $x^2(1+u)^2$ is called the *generating series* for the problem.

This has been a long proof, but it has accomplished more than just the solution of this simple problem. It has given the standard way in which the multiplicative property needed for a homomorphism is actually proved. We will use this technique several times.

2.4 Problem 4

Find the number $c_{n,k}$ of $\{0,1\}$-sequences of length n with k 1's. Again, this is an easy problem. The answer is

$$\begin{aligned}
c_{n,k} &= \left[x^n u^k\right] \delta\phi\left((\mathsf{a}+\mathsf{b})^n\right) \quad \text{(encoding the problem)} \\
&= \left[x^n u^k\right] \delta\left((\mathsf{a}+u\mathsf{b})^n\right) \quad \text{(ϕ is a homomorphism)} \\
&= \left[x^n u^k\right] (x+ux)^n \quad \text{(δ is a homomorphism)} \\
&= \left[u^k\right] (1+u)^n \\
&= \binom{n}{k} \quad \text{(binomial theorem).}
\end{aligned}$$

2.5 Problem 5

Find the number $c_{n,0}$ of $\{0,1\}$-sequences of length n with no 1's.

The answer is obviously 1. However, the point to observe here is that setting $u=0$ obtains the information we desire. To see this, think about the action of ϕ. If a sequence has a 1, then a b occurs, and therefore a factor of u against the corresponding term in the encoding. Setting $u=0$ eradicates this term from the encoding. This is the same as applying $[u^0]$ to get the coefficient of u^0. Therefore,

$$\begin{aligned}
c_{n,0} &= \left[x^2 u^0\right] \delta\phi\left((\mathsf{a}+\mathsf{b})^n\right) \quad \text{(encoding the problem)} \\
&= \left[x^n u^0\right] \delta\left((\mathsf{a}+u\mathsf{b})^n\right) \quad \text{(ϕ is a homomorphism)} \\
&= \left[x^n\right] x^n \quad \text{(δ is a homomorphism)} \\
&= 1.
\end{aligned}$$

2.6 Summary

You have now seen the how the method of noncommutative algebra works. The set of sequences to be counted is encoded as a series in the indeterminates a and b. A function ϕ is designed to encode the counting information, and we establish that this function is a homomorphism. A typical proof for establishing this has been given in detail. A second function δ is designed to retain the counting information and to delete the indeterminates a and b. This gives a power series from which the answer is obtained by the extraction of a coefficient.

Both ϕ and δ vary from context to context, but I will use the same symbol for each problem, for simplicity of notation.

Chapter 3

Rings

Before advancing to some problems which really exercise these powerful ideas properly, we must get a firmer view of what sets the homomorphisms actually act on.

The axioms for a noncommutative ring

Look at the following list of rules carefully. They contain all of the operations that you are used to using in simplifying algebraic expressions. However, they have been presented in a systematic way, as a set of mutually consistent axioms. The only exception to the rules you use is that here multiplication is not commutative.

A *noncommutative ring* is a set R equipped with two operations $+$ (called *addition*) and $\cdot$ (called *multiplication*) such that

1. If $a, b \in \mathsf{R}$ then $a + b \in \mathsf{R}$ (closure with respect to $+$):
   (a) $a + b = b + a$ for all $a, b \in \mathsf{R}$ (commutativity),
   (b) $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathsf{R}$ (associativity),
   (c) There is an element $0 \in \mathsf{R}$ such that $a + 0 = a$ for all $a \in \mathsf{R}$ (neutral element for addition),
   (d) Given $a \in \mathsf{R}$, there is a $b \in \mathsf{R}$ such that $a + b = 0$ (negative).
2. If $a, b \in \mathsf{R}$ then $a \cdot b \in \mathsf{R}$ (closure with respect to $\cdot$):
   (a)
   (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathsf{R}$ (associativity),
   (c) There is an element $1 \in \mathsf{R}$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathsf{R}$ (neutral element for multiplication),
3. For all $a, b, c \in \mathsf{R}$:
   (a) $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributivity on the left),

(b) $(b+c)\cdot a = b\cdot a + c\cdot a$ (distributivity on the right).

It is a convenience to denote $a\cdot b$ by ab, and this will be done from now onwards.

Axioms for a commutative ring

For a commutative ring, insert the axiom

$$a\cdot b = b\cdot a \quad \text{for all } a, b \in \mathsf{R} \text{ (commutativity).}$$

as axiom (2a) in the above list.

Examples

The set of integers is a commutative ring; so is the set Q of rational numbers. The set of all $n\times n$ matrices with real elements is a noncommutative ring.

3.1 The formal power series ring $\mathsf{Q}[[x]]$

As an example, consider the ring of formal power series.

Definition

Let

$$\mathsf{Q}[[x]] = \left\{\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots : \alpha_0, \alpha_1, \alpha_2, \ldots \in \mathsf{Q}\right\}.$$

The *addition* is usual sum of series. The *multiplication* is commutative, and is the usual one for multiplying series together. It is a straightforward matter to check that these standard ways of adding and multiplying series satisfy the axioms for a *commutative* ring.

The *square brackets* in $\mathsf{Q}[[x]]$ indicate that the multiplication is commutative. *Angle brackets* will be used to indicate that the multiplication is noncommutative.

Power series and functions

From the definition, two power series are equal if and only if they have the same coefficients, term by term. However, the test for equality of functions is entirely different. You have to show that they can be evaluated on the given set, and evaluate to equal values at all point of the set. Thus, the power series we deal with are different from functions although, superficially, they appear to be the same.

3.2 The ring $\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$

There is a second ring that we use. Consider the following fundamental set. Let $\{\mathsf{t}_0, \mathsf{t}_1, \mathsf{t}_2, \ldots\}$ be the set of all distinct (finite) terms that can be made out of a's and b's. For example, $\mathsf{a}^2\mathsf{b}^3\mathsf{a}^5\mathsf{b}$ is in this set. Let

$$\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle = \{\alpha_0 1 + \alpha_1 \mathsf{t}_1 + \alpha_2 \mathsf{t}_2 + \cdots : \alpha_0, \alpha_1, \alpha_2, \ldots \in \mathsf{Q}\}.$$

This is the set of all series in the indeterminates a and b with coefficients that are rational numbers, and therefore in Q. For example,

$$\mathsf{f} = 1 + \mathsf{ab} + \frac{1}{2!}(\mathsf{ab})^2 + \frac{1}{3!}(\mathsf{ab})^3 + \cdots \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle.$$

Similarly,

$$\mathsf{g} = 1 + \frac{1}{2}\mathsf{a} + \frac{2}{3}e^u(\mathsf{ab})^2 + (2 + 5u^2)\mathsf{a}^3\mathsf{b}^3 + \cdots \in \mathsf{Q}[[u]]\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle.$$

The coefficients of this series are in $\mathsf{Q}[[u]]$ and, as observed above, this is the ring of all formal power series in u with coefficients in Q. As a final example,

$$(\mathsf{a} + \mathsf{b})^n \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle,$$

where n is a nonnegative integer.

Addition and *multiplication* are defined as usual for series, although the multiplication is noncommutative. The 0 and the 1 are the familiar ones, and it is easy to see that $\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$ is a noncommutative ring by checking each of the axioms. Similarly, $\mathsf{Q}[[u]]\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$ is a ring. These are the two in which we will be doing a good deal of the algebraic computations. Indeed, the latter was used in the earlier problems without attention being drawn to it.

Inverses

Let $\mathsf{f} \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$, and suppose there are $\mathsf{g}_1, \mathsf{g}_2 \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$ such that $\mathsf{f}\mathsf{g}_1 = 1$, and $\mathsf{g}_2\mathsf{f} = 1$. Then

$$\mathsf{g}_1 = 1\mathsf{g}_1 = (\mathsf{g}_2\mathsf{f})\mathsf{g}_1 = \mathsf{g}_2(\mathsf{f}\mathsf{g}_1) = \mathsf{g}_2 1 = \mathsf{g}_2,$$

by associativity of multiplication (one of the ring axioms). Thus $\mathsf{g}_1 = \mathsf{g}_2$, and we call g_1 *an* inverse of f. We ought to check that if f has an inverse, then it is unique. For this purpose, let f be invertible, and suppose that g and h are inverses of f. Then

$$\mathsf{g} = \mathsf{g}1 = \mathsf{g}(\mathsf{fh}) = (\mathsf{gf})\mathsf{h} = 1\mathsf{h} = \mathsf{h},$$

by associativity of multiplication. Thus, if f is invertible, it has a unique inverse. The inverse is denoted by

$$\mathsf{f}^{-1}.$$

Finding an inverse

We wish to find the inverse of $1-\mathsf{a}$, if it exists. Suppose the inverse exists. Then, since it is to be in $\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$, suppose it has the form $\alpha_0 1 + \alpha_1 \mathsf{a} + \alpha_2 \mathsf{a}^2 + \cdots \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$. Then, from the definition of the inverse,

$$(1-\mathsf{a})\left(\alpha_0 1 + \alpha_1 \mathsf{t}_1 + \alpha_2 \mathsf{t}_2 + \cdots\right) = 1,$$

so

$$\alpha_0 1 + (\alpha_1 - \alpha_0)\mathsf{a} + (\alpha_2 - \alpha_1)\mathsf{a}^2 + (\alpha_3 - \alpha_2)\mathsf{a}^3 + \cdots = 1.$$

Equating terms on the left hand and right hand side,

$$\alpha_0 = 1, \alpha_1 - \alpha_0 = 0, \alpha_2 - \alpha_1 = 0, \alpha_3 - \alpha_2 = 0, \ldots$$

so $1 = \alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = \ldots$, whence

$$(1-\mathsf{a})^{-1} = 1 + \mathsf{a} + \mathsf{a}^2 + \mathsf{a}^3 + \cdots.$$

Again, this is familiar to you as the sum of a geometric series.

Encoding the set of all $\{0,1\}$-sequences

In a similar way,

$$(1-\mathsf{a}-\mathsf{b})^{-1} = 1 + (\mathsf{a}+\mathsf{b}) + (\mathsf{a}+\mathsf{b})^2 + (\mathsf{a}+\mathsf{b})^3 + \cdots.$$

You will recognise the right hand side, since $(\mathsf{a}+\mathsf{b})^n$ is the encoding of the set of all $\{0,1\}$-sequences of length n. The right hand side is therefore the encoding of the *set of all* $\{0,1\}$*-sequences*. The left hand side gives another expression for the same series, and will be used extensively.

A property of the inverse

Finally, we need a way of constructing the inverse of a product of invertible elements. Suppose c and d are invertible. Then I claim that

$$(\mathsf{cd})^{-1} = \mathsf{d}^{-1}\mathsf{c}^{-1}.$$

To see this, consider

$$(\mathsf{cd})\left(\mathsf{d}^{-1}\mathsf{c}^{-1}\right) = \mathsf{c}\left(\mathsf{dd}^{-1}\right)\mathsf{c}^{-1} = \mathsf{c}1\mathsf{c}^{-1} = \mathsf{cc}^{-1} = 1,$$

by associativity and the property of the neutral element 1. This establishes the claim.

If you have done some work with matrices, you will recognise that this also works in their case. This should not surprise you now, since $n \times n$ matrices form a ring under matrix addition and matrix multiplication. Moreover, not all such matrices have inverses, but the ones that do have a unique inverse.

3.3 The general approach

It is now possible to be more specific about the general approach. In the previous problems, we started off with a $\{0,1\}$-sequence question, encoded it in the ring $\mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle$, acted on it with a carefully designed ϕ to preserve counting information, acted on this with a carefully designed δ which deleted the encoding of the sequences, to end up in the power series ring $\mathsf{Q}[[u,x]]$, in which we used theorems such as the binomial theorem to compute the information that we want.

The chain of transformations for Problem 4

It is a good idea to summarise each of the main steps in the solution of a problem. This can be done by listing the functions and the sets they acted upon, and the effect they had. Two lines are needed, the first to list the sets in order and the functions that act between them, and the second to list the effects of the functions. For this purpose, let $\mathcal{S}$ be a subset of the set of all $\{0,1\}$-sequences, and let $\mathcal{B}_n$ be the set of all $\{0,1\}$-sequences of length n. Then, for Problem 4,

$$\begin{array}{ccccccccc} \mathcal{S} & \longrightarrow & \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle & \xrightarrow{\phi} & \mathsf{Q}[[u]]\,\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle & \xrightarrow{\delta} & \mathsf{Q}[[u,x]] & \xrightarrow{[u^k x^n]} & \mathsf{Q}, \\ \mathcal{B}_n & \longmapsto & (\mathsf{a}+\mathsf{b})^n & \stackrel{\phi}{\longmapsto} & (\mathsf{a}+u\mathsf{b})^n & \stackrel{\delta}{\longmapsto} & (1+u)^n x^n & \stackrel{[u^k x^n]}{\longmapsto} & \binom{n}{k}. \end{array}$$

Now is the time to check that you agree that this is what was done and that you understand what it means. It is pretty straightforward as you read along the two lines.

Partial homomorphisms

However, life is not always this simple, and sequence problems become more complicated because the ϕ that is appropriate for a problem may fail to be a homomorphism. It may behave well on certain kinds of expressions and not on others. Such a homomorphism is called a *partial homomorphism*, and we need to be able to work with it.

It is rather like the *Tower of Hanoi Puzzle*, where an ordered stack of discs is to be moved from one position to another, with order preserved. One solution is the obvious one: simply move the stack bodily. However, this solution is not available because there is a condition that a disc may not be put on top of a smaller one, and no more that three piles are allowed during the process. Inspite of the condition, the problem can be solved.

The rest of the Notes involve the use of partial homomorphisms and how one can work with them.

Chapter 4

Using the ring $\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$

The three problems of this chapter require the development of some more mathematical technique to accompany the new ideas and to allow algebraic computations to be made.

4.1 Problem 6

Find the number $c_{n,k}$ of $\{0,1\}$-sequences with k occurrences of the subsequence 000. Take care here: 0000 has two occurrences of the subsequence 000. They are indicated in $0\underline{000}$ and $\underline{000}0$.

The usual solution

There is not one.

The solution

The set of all $\{0,1\}$-sequences is encoded as $(1-\mathsf{a}-\mathsf{b})^{-1}$. We now need to preserve information about the number of occurrences of 000.

The functions ϕ and δ

I am going to be a little more formal about the definition of ϕ, since we now have the rings at our disposal. Let

$$\phi\colon \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \longrightarrow \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \colon \mathsf{t} \longmapsto u^{\#_{\mathsf{aaa}}}\mathsf{t},$$

and define ϕ to act term by term. Let

$$\delta\colon \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \longrightarrow \mathsf{Q}[[u, x]]$$

such that $\delta(\mathsf{a}) = \delta(\mathsf{b}) = x$, as a substitution. Then

$$c_{n,k} = \left[u^k x^n\right]\, \delta\mathsf{F},$$

where

$$\mathsf{F} = \phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right).$$

Properties of ϕ and δ

To apply ϕ and δ, we need to look for their homomorphic properties. δ is easy; we have seen it before and it is a homomorphism.

ϕ, on the other hand, is more complicated. First, note that, for $\mathsf{f}, \mathsf{g} \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle$ so, since ϕ acts term by term, $\phi(\mathsf{f}+\mathsf{g}) = \phi(\mathsf{f}) + \phi(\mathsf{g})$, by definition. For multiplication of the terms t and t', observe the simple combinatorial property

$$\#_{\mathsf{aaa}}(\mathsf{tbt}') = \#_{\mathsf{aaa}}(\mathsf{t}) + \#_{\mathsf{aaa}}(\mathsf{t}')$$

of $\#_{\mathsf{aaa}}$. Then

$$\begin{aligned}
\phi(\mathsf{tbt}') &= u^{\#_{\mathsf{aaa}}(\mathsf{tbt}')}\mathsf{tbt}' \quad \text{(definition of } \phi) \\
&= u^{\#_{\mathsf{aaa}}(\mathsf{t})+\#_{\mathsf{aaa}}(\mathsf{t}')}\mathsf{tbt}' \quad \text{(the above relationship)} \\
&= \left(u^{\#_{\mathsf{aaa}}(\mathsf{t})}\mathsf{t}\right)\mathsf{b}\left(u^{\#_{\mathsf{aaa}}(\mathsf{t}')}\mathsf{t}'\right) \\
&= \phi(\mathsf{t})\mathsf{b}\phi(\mathsf{t}') \quad \text{(definition of } \phi)
\end{aligned}$$

Thus $\phi(\mathsf{tbt}') = \phi(\mathsf{t})\mathsf{b}\phi(\mathsf{t}')$, so $\phi(\mathsf{fbg}) = \phi(\mathsf{f})\mathsf{b}\phi(\mathsf{g})$. This proof is very similar indeed to one that appeared in connexion with Problem 3. Summarising these properties of ϕ, we have

$$\left.\begin{aligned}
\phi(\mathsf{f}+\mathsf{g}) &= \phi(\mathsf{f}) + \phi(\mathsf{g}), \\
\phi(\mathsf{fbg}) &= \phi(\mathsf{f})\mathsf{b}\phi(\mathsf{g}), \\
\phi(1) &= 1.
\end{aligned}\right\}$$

The multiplicative property is almost the one we want that would make ϕ into a homomorphism. However, it does not quite make it because of the required occurrence of the b, so we call ϕ a *partial homomorphism.*

Working with partial homomorphisms

Having a *partial homomorphism* as opposed to a *full* homomorphism means that there is a lot of extra work to be done. We must manipulate $(1-\mathsf{a}-\mathsf{b})^{-1}$ into a form such that we can actually apply the above two rules. In particular, we must trap a sequence of a's between two b's, and we therefore need to think about how this can be done. It is this that makes this problem considerably harder than the previous ones, although the overall strategy is the same.

A combinatorial-algebraic expansion

To apply ϕ, we make a subtle observation. First,

$$1-\mathsf{a}-\mathsf{b} = (1-\mathsf{a})\left(1-(1-\mathsf{a})^{-1}\mathsf{b}\right).$$

Check it by multiplying it out, using distributivity. Then, by properties of the inverse,

$$(1-\mathsf{a}-\mathsf{b})^{-1} = \left(1-(1-\mathsf{a})^{-1}\mathsf{b}\right)^{-1}(1-\mathsf{a})^{-1}.$$

This has achieved the objective of trapping a sequence of a's between two b's, so we can use the properties of ϕ. The sequences of a's are trapped because the right hand side is equal to

$$(1-\mathsf{a})^{-1} + (1-\mathsf{a})^{-1}\mathsf{b}(1-\mathsf{a})^{-1} + \left((1-\mathsf{a})^{-1}\mathsf{b}\right)^2(1-\mathsf{a})^{-1} + \cdots.$$

Applying ϕ as a partial homomorphism

We can now calculate as follows.

$$\begin{aligned} \delta\mathsf{F} &= \delta\left(\left(1-\left(\phi\left((1-\mathsf{a})^{-1}\right)\right)\mathsf{b}\right)^{-1}\phi\left((1-\mathsf{a})^{-1}\right)\right) \\ &\quad (\phi \text{ is a partial homomorphism}) \\ &= \left(1-x\delta\phi\left((1-\mathsf{a})^{-1}\right)\right)^{-1}\delta\phi\left((1-\mathsf{a})^{-1}\right) \\ &\quad (\delta \text{ is a homomorphism}). \end{aligned}$$

But

$$\begin{aligned} \delta\phi\left((1-\mathsf{a})^{-1}\right) &= \delta\phi\left(1+\mathsf{a}+\mathsf{a}^2+\mathsf{a}^3+\mathsf{a}^4+\cdots\right) \\ &= \delta\left(1+\mathsf{a}+\mathsf{a}^2+u\mathsf{a}^3+u^2\mathsf{a}^4+\cdots\right) \\ &= \delta\left(\left(1+(1-u)(\mathsf{a}+\mathsf{a}^2)\right)(1-u\mathsf{a})^{-1}\right) \\ &= \left(1+(1-u)(x+x^2)\right)(1-ux)^{-1}. \end{aligned}$$

Then, substituting this into the previous expression, and simplifying, we have

$$\delta\mathsf{F} = \frac{1+(1-u)(x+x^2)}{1-(1+u)x-(1-u)(x^2+x^3)}.$$

Then

$$c_{n,k} = \left[u^k x^n\right]\frac{1+(1-u)(x+x^2)}{1-(1+u)x-(1-u)(x^2+x^3)}.$$

Generating series

The series on the right hand side is called a *generating series*, a term introduced in connexion with Problem 3. There are several techniques for obtaining a formula for the coefficient of the general term in the expansion of this series in the ring $\mathsf{Q}[[u,x]]$. You may have encountered *Taylor's Theorem* or the *Binomial Series Theorem*. Slight adaptations of these can be proved in the ring, and can therefore be used. *Recurrence equations* can also be use for fast computations.

This is a technical side of the subject that I do not wish to get into. For us, a problem will be regarded as solved once the generating series has been determined.

Symbolic computation with Maple

The generating series for $c_{n,k}$ can be expanded readily and the first few terms are

$$1 + 2x + 4x^2 + (7+u)x^3 + (13+2u+u^2)x^4 + (24+5u+2u^2+u^3)x^5 \\ +(44+12u+5u^2+2u^3+u^4)x^6 + \cdots.$$

Then $c_{6,2} = 5$, so there are 5 sequences of length 6 with exactly 2 occurrences of the subsequence 000. These are $\{000011, 100001, 110000, 000010, 010000\}$.

I did this computation with the aid of a system called Maple that carries out operations symbolically on mathematical expressions, as distinct from number crunching. It was designed by some members of the Computer Science Department at the University of Waterloo. For mathematicians, it is like an electron microscope. If you know where to look in a complex mathematical situation, but you do not know what is happening there, this device allows one to catch a glimpse of what is there, and this is often enough to lead the way to a clearer understanding of difficult mathematical situations.

Notice that, when $u = 1$, the generating series becomes

$$\frac{1}{1-2x},$$

as, indeed, it should. This is because setting $u = 1$ means that an occurrence of the subsequence 000 is no longer being recorded, so the whole question then reverts to an earlier one of counting the number of $\{0,1\}$-sequences of length n.

The chain of transformations for this problem

The expressions are now too large to fit across the page, so they have to be split. Let $\mathcal{S}$ be the set of all $\{0,1\}$-sequences. Then the chain of transformations is

$$\mathcal{S} \longrightarrow \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \xrightarrow{\phi} \mathsf{Q}[[u]]\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \xrightarrow{\delta} \mathsf{Q}[[u,x]] \xrightarrow{[u^kx^n]} \mathsf{Q},$$

where

$$\begin{aligned} \mathcal{S} &\longmapsto (1-\mathsf{a}-\mathsf{b})^{-1} \\ &\overset{\phi}{\longmapsto} \left(1-\left(\phi\left((1-\mathsf{a})^{-1}\right)\right)\mathsf{b}\right)^{-1}\phi\left((1-\mathsf{a})^{-1}\right) \\ &\overset{\delta}{\longmapsto} \frac{1+(1-u)(x+x^2)}{1-(1+u)x-(1-u)(x^2+x^3)} \\ &\overset{[u^kx^n]}{\longrightarrow} c_{n,k}. \end{aligned}$$

4.2 Problem 7

Find the number d_n of $\{0,1\}$-sequences of length n with no occurrences of the subsequence 01110.

The usual solution

There is not one.

Connexion with the Excluded Volume Problem

This is an example of a *forbidden subsequence* problem, and so has the essential characteristic of the Excluded Volume Problem. However, in the Excluded Volume Problem, the alphabet is larger and there is more than one forbidden subsequence.

The solution

We start with a bigger problem of finding the number $c_{n,k}$ of $\{0,1\}$-sequences of length n with k occurrences of the subsequence 01110. Then $d_n = c_{n,0}$.

The functions ϕ and δ

Let

$$\phi\colon \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle \longrightarrow \mathsf{Q}[[u]]\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle\colon \mathsf{t} \longmapsto u^{\#_{\mathsf{abbba}}}\mathsf{t},$$

and define ϕ to act term by term. Let

$$\delta\colon \mathsf{Q}[[u]]\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle \longrightarrow \mathsf{Q}[[u,x]]$$

such that $\delta(\mathsf{a}) = \delta(\mathsf{b}) = x$, as a substitution. Then

$$c_{n,k} = \left[u^k x^n\right] \delta\mathsf{F},$$

where

$$\mathsf{F} = \phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right).$$

Properties of ϕ and δ

To apply ϕ and δ, we need to look for their homomorphic properties. δ is easy; we have seen it before and it is a homomorphism.

ϕ, on the other hand, is more complicated. First, note that, for all $\mathsf{f},\mathsf{g} \in \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle$, we have $\phi(\mathsf{f}+\mathsf{g}) = \phi(\mathsf{f}) + \phi(\mathsf{g})$. For multiplication, observe the simple combinatorial property of $\#_{\mathsf{abbba}}$ that, for $i \geq 0$,

$$\#_{\mathsf{abbba}}\left(\mathsf{tab}^i\mathsf{at}'\right) = \begin{cases} \#_{\mathsf{abbba}}\left(\mathsf{ta}\right) + 1 + \#_{\mathsf{abbba}}\left(\mathsf{at}'\right) & \text{if} \quad i=3, \\ \#_{\mathsf{abbba}}\left(\mathsf{ta}\right) + 0 + \#_{\mathsf{abbba}}\left(\mathsf{at}'\right) & \text{if} \quad i\neq 3, \end{cases}$$

so

$$\phi\left(\mathsf{tab}^i\mathsf{at}'\right) = \begin{cases} \phi\left(\mathsf{ta}\right) u\mathsf{b}^i \phi\left(\mathsf{at}'\right) & \text{if} \quad i=3, \\ \phi\left(\mathsf{ta}\right) \mathsf{b}^i \phi\left(\mathsf{at}'\right) & \text{if} \quad i\neq 3. \end{cases}$$

Summing over i we have,

$$\begin{aligned} \phi\left(\mathsf{ta}(1-\mathsf{b})^{-1}\mathsf{at}'\right) &= \phi\left(\mathsf{ta}(1+\mathsf{b}+\mathsf{b}^2+\mathsf{b}^3+\mathsf{b}^4+\cdots)\mathsf{at}'\right) \\ &= \phi(\mathsf{ta})\left(1+\mathsf{b}+\mathsf{b}^2+u\mathsf{b}^3+\mathsf{b}^4+\cdots\right)\phi(\mathsf{at}') \\ &= \phi(\mathsf{ta})\left((1-\mathsf{b})^{-1}+(u-1)\mathsf{b}^3\right)\phi(\mathsf{at}'). \end{aligned}$$

so $\phi\left(\mathsf{fa}(1-\mathsf{b})^{-1}\mathsf{ag}\right) = \phi(\mathsf{fa})\left((1-\mathsf{b})^{-1} + (u-1)\mathsf{b}^3\right)\phi(\mathsf{ag})$, for all $\mathsf{f}, \mathsf{g} \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b} \rangle\rangle$. Summarising these properties we have

$$\left.\begin{array}{rcl} \phi(\mathsf{f}+\mathsf{g}) & = & \phi(\mathsf{f}) + \phi(\mathsf{g}), \\ \phi\left(\mathsf{fa}(1-\mathsf{b})^{-1}\mathsf{ag}\right) & = & \phi(\mathsf{fa})\left((1-\mathsf{b})^{-1} + (u-1)\mathsf{b}^3\right)\phi(\mathsf{ag}), \\ \phi(1) & = & 1. \end{array}\right\}$$

Then ϕ is a partial homomorphism. It also suggests a strategy for solving the problem. We have to trap a sequence of b's between two a's. This will need a set of carefully chosen algebraic manipulations.

A combinatorial-algebraic expansion

To apply ϕ, we make the following observation.

$$1-\mathsf{a}-\mathsf{b} = (1-\mathsf{b}) - \mathsf{a} = (1-\mathsf{b})\left(1-(1-\mathsf{b})^{-1}\mathsf{a}\right).$$

This is equivalent to the combinatorial-algebraic expansion for Problem 6.

Applying ϕ as a partial homomorphism

Then

$$\begin{array}{rcl} (1-\mathsf{a}-\mathsf{b})^{-1} & = & \left(1-(1-\mathsf{b})^{-1}\mathsf{a}\right)^{-1}(1-\mathsf{b})^{-1} \\ & & \text{(property of the inverse)} \\ & = & \left(1+(1-\mathsf{b})^{-1}\mathsf{a}\left(1-(1-\mathsf{b})^{-1}\mathsf{a}\right)^{-1}\right)(1-\mathsf{b})^{-1} \\ & & \text{(since } (1-\mathsf{x})^{-1} = 1+\mathsf{x}(1-\mathsf{x})^{-1}\text{)} \\ & = & (1-\mathsf{b})^{-1} + (1-\mathsf{b})^{-1}\mathsf{a}\left(1-(1-\mathsf{b})^{-1}\mathsf{a}\right)^{-1}(1-\mathsf{b})^{-1}. \end{array}$$

We have now succeeded in trapping a sequence of b's between a pair of a's, so ϕ can now be applied.

$$\begin{array}{rcl} \mathsf{F} & = & \phi\left((1-\mathsf{b})^{-1}\right) \\ & & +\phi\left((1-\mathsf{b})^{-1}\mathsf{a}\right)\left(1-\left((1-\mathsf{b})^{-1}+(u-1)\mathsf{b}^3\right)\mathsf{a}\right)^{-1}\phi\left((1-\mathsf{b})^{-1}\right) \\ & & \text{(since } \phi \text{ is a partial homomorphism)} \\ & = & (1-\mathsf{b})^{-1} + (1-\mathsf{b})^{-1}\mathsf{a}\left(1-\left((1-\mathsf{b})^{-1}+(u-1)\mathsf{b}^3\right)\mathsf{a}\right)^{-1}(1-\mathsf{b})^{-1}, \end{array}$$

since, from the definition of ϕ,

$$\begin{array}{rcl} \phi\left((1-\mathsf{b})^{-1}\right) & = & (1-\mathsf{b})^{-1}, \\ \phi\left((1-\mathsf{b})^{-1}\mathsf{a}\right) & = & (1-\mathsf{b})^{-1}\mathsf{a}. \end{array}$$

The next step is to apply δ, which is easily done.

$$\delta\mathsf{F} = (1-x)^{-1} + x(1-x)^{-1}\left(1-\left((1-x)^{-1}+(u-1)x^3\right)x\right)^{-1}(1-x)^{-1}$$

so

$$c_{n,k} = \left[u^k x^n\right]\frac{1-(u-1)x^4}{1-2x-(u-1)(1-x)x^4}.$$

Symbolic computations with Maple

The first few terms of this generating series are

$$1 + 2x + 4x^2 + 8x^3 + 16x^4 + (3 + u)x^5 + (60 + 4u)x^6 + (116 + 12u)x^7$$
$$+(224 + 32u)x^8 + (433 + 78u + u^2)x^9 + (837 + 182u + 5u^2)x^{10} + \cdots.$$

For example, $c_{5,2} = 5$, so there are 5 $\{0,1\}$-sequences of length 10 with exactly 2 occurrences of the subsequence 01110. These are

$$\{0111011100, 0111011101, 0011101110, 1011101110, 0111001110\}.$$

Solution of the problem

In fact, the problem asked for the number of $\{0,1\}$-sequences with *no* occurrences of the subsequence 01110. This is easily achieved by setting $u = 0$ in the generating series to get

$$d_n = [x^n]\,\frac{1 + x^4}{1 - 2x + (1 - x)x^4}.$$

The first few terms of the series are

$$1 + 2\,x + 4\,x^2 + 8\,x^3 + 16\,x^4 + 31\,x^5 + 60\,x^6 + 116\,x^7 + 224\,x^8 + 433\,x^9$$
$$+837\,x^{10} + 1618\,x^{11} + 3128\,x^{12} + 6047\,x^{13} + 11690\,x^{14} + 22599\,x^{15}$$
$$+43688\,x^{16} + 84457\,x^{17} + 163271\,x^{18} + 315633\,x^{19} + \cdots.$$

Thus, for example, $d_{18} = 163271$, so there are 163271 $\{0,1\}$-sequences of length 18 with no occurrences of the sequence 01110.

The chain of transformations for this problem

The expressions are also too large to fit across the page, so again they have to be split. Let $\mathcal{B}$ be the set of all $\{0,1\}$-sequences. Then

$$\mathcal{S} \longrightarrow \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle \xrightarrow{\phi} \mathsf{Q}[[u]]\,\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle \xrightarrow{\delta} \mathsf{Q}[[u,x]] \xrightarrow{[u^k x^n]} \mathsf{Q},$$

where

$$\begin{aligned}
\mathcal{B} &\longmapsto (1 - \mathsf{a} - \mathsf{b})^{-1}\\
&\overset{\phi}{\longmapsto} (1-\mathsf{b})^{-1} + (1-\mathsf{b})^{-1}\mathsf{a}\left(1 - \left((1-\mathsf{b})^{-1} + (u-1)\mathsf{b}^3\right)\mathsf{a}\right)^{-1}(1-\mathsf{b})^{-1}\\
&\overset{\delta}{\longmapsto} \frac{1 - (u-1)x^4}{1 - 2x - (u-1)(1-x)x^4}\\
&\overset{[u^0x^n]}{\longrightarrow} d_n.
\end{aligned}$$

4.3 Problem 8

Find the probability $\mathsf{prob}(p,q,r)$ that a sequence with p 1's, q 2's and r 3's has at least one occurrence of the subsequence 12.

Origin of the problem

The problem was sent to me on the Internet by someone in a large computer corporation who was writing the code for implementing a filing system. The system was to take advantage of the history of earlier transactions as a guide to the distribution of the activity on the file. Thus, certain parts of the code that were going to be executed with high probability were to be optimised to cut down running time. The problem was to determine, at run time, the probability that a particular branch of the code would be taken.

The probability

Let $c_k(p,q,r)$ be the number of sequences with p 1's, q 2's and r 3's and with k occurrences of the subsequence 12, and let

$$c(p,q,r) = \sum_{k\geq 0} c_k(p,q,r).$$

Then

$$\mathsf{prob}(p,q,r) = 1 - \frac{c_0(p,q,r)}{c(p,q,r)}.$$

This has reduced the problem to a counting question for sequences, and we must determine $c_k(p,q,r)$.

Three functions ϕ, δ, and L_α.

Let $1 \leftrightarrow \mathsf{a}$, $2 \leftrightarrow \mathsf{b}$, and $3 \leftrightarrow \mathsf{c}$. Then the encoding of the set of all sequences in the alphabet $\{1,2,3\}$ is $(1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}$. We determine $c_k(p,q,r)$ as the consequence of a computation in $\mathsf{Q}\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle$. This time three mappings are required.

The first mapping, ϕ, records the number of occurrences of 12 in the sequences. Let t be an arbitrary term in $\mathsf{a},\mathsf{b},\mathsf{c}$, and let ϕ be the function

$$\phi\colon \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle \longrightarrow \mathsf{Q}[[u]]\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle\colon \mathsf{t} \longmapsto u^{\#_{\mathsf{ab}}(\mathsf{t})}\mathsf{t},$$

extended linearly to $\mathsf{Q}\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle$, where $\#_{\mathsf{ab}}(\mathsf{t})$ denotes the number of occurrences of ab in t.

The second function, δ, records the number of occurrences of $1,2$ and 3 in a sequence. Let x,y,z be commutative indeterminates. Let

$$\delta\colon \mathsf{Q}[[u]]\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle \longrightarrow \mathsf{Q}[[u,x,y,z]]$$

such that $\mathsf{a} \mapsto x$, $\mathsf{b} \mapsto y$, and $\mathsf{c} \mapsto z$.

Let $[x^p y^q z^r]f$ denote the coefficient of $x^p y^q z^r$ in $f \in \mathsf{Q}[[u,x,y,z]]$. Then

$$\sum_{k\geq 0} c_k(p,q,r)u^k = [x^p y^q z^r]\delta\phi\left((1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}\right).$$

The third function is the evaluation function

$$L_\alpha\colon \mathsf{Q}[[u,x,y,z]] \longrightarrow \mathsf{Q}[[x,y,z]]\colon f(u,x,y,z) \longmapsto f(\alpha,x,y,z),$$

where $\alpha \in \mathsf{Q}$.

The probability

Then, combining these functions, we have

$$\begin{aligned} c_0(p,q,r) &= [x^p y^q z^r] L_0\, \delta\phi\left((1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}\right), \\ c(p,q,r) &= [x^p y^q z^r] L_1\, \delta\phi\left((1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}\right), \end{aligned}$$

completing the identification of $\mathsf{prob}(p,q,r)$ as a computation in $\mathsf{Q}\langle\langle \mathsf{a},\mathsf{b},\mathsf{c}\rangle\rangle$.

Properties of ϕ, δ and L_α

To apply the function $L_\alpha\delta\phi$ to $(1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}$, we look for the homomorphic properties of ϕ, δ and L_α. This is now a familiar step.

δ is easy; we have seen it before and it is a homomorphism.

For ϕ, note that, for all $\mathsf{f},\mathsf{g} \in \mathsf{Q}\langle\langle \mathsf{a},\mathsf{b}\rangle\rangle$, we have $\phi(\mathsf{f}+\mathsf{g}) = \phi(\mathsf{f}) + \phi(\mathsf{g})$. For multiplication, observe the simple combinatorial property of $\#_{\mathsf{ab}}$ that note that if t and t' are terms in $\mathsf{a},\mathsf{b},\mathsf{c}$ then $\#_{\mathsf{ab}}(\mathsf{tbt}') = \#_{\mathsf{ab}}(\mathsf{tb}) + \#_{\mathsf{ab}}(\mathsf{t}')$, so

$$\phi(\mathsf{tbt}') = \phi(\mathsf{tb})\phi(\mathsf{t}').$$

Extending this from terms to series, by the process which is now familiar, we have $\phi(\mathsf{fbg}) = \phi(\mathsf{fb})\phi(\mathsf{g})$.

Summarising these properties,

$$\left.\begin{aligned} \phi(\mathsf{f}+\mathsf{g}) &= \phi(\mathsf{f}) + \phi(\mathsf{g}), \\ \phi(\mathsf{fbg}) &= \phi(\mathsf{fb})\phi(\mathsf{g}), \\ \phi(1) &= 1. \end{aligned}\right\}$$

Thus ϕ is a *partial homomorphism.*

Finally, L_α is clearly a homomorphism, since it is a substitution function.

Applying ϕ as a partial homomorphism

$$\begin{aligned} \phi\left((1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}\right) &= \phi\left(\left(1-(1-\mathsf{a}-\mathsf{b})^{-1}\mathsf{c}\right)^{-1}(1-\mathsf{a}-\mathsf{b})^{-1}\right) \\ &= \left(1-\phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right)\mathsf{c}\right)^{-1}\phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right). \end{aligned}$$

Moreover,

$$\begin{aligned} \phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right) &= \phi\left(\left(1-(1-\mathsf{a})^{-1}\mathsf{b}\right)^{-1}(1-\mathsf{a})^{-1}\right) \\ &= \left(1-\phi\left((1-\mathsf{a})^{-1}\right)\mathsf{b}\right)^{-1}\phi\left((1-\mathsf{a})^{-1}\right) \\ &= \left(1-\mathsf{a}-(1-\mathsf{a})\phi((1-\mathsf{a})^{-1}\mathsf{b})\right)^{-1}. \end{aligned}$$

But the action of ϕ can now be computed as follows.

$$\begin{aligned} \phi\left((1-\mathsf{a})^{-1}\mathsf{b}\right) &= \phi\left(\mathsf{b}+\mathsf{ab}+\mathsf{a}^2\mathsf{b}+\mathsf{a}^3\mathsf{b}+\cdots\right) \\ &= \mathsf{b}+u\mathsf{ab}+u\mathsf{a}^2\mathsf{b}+u\mathsf{a}^3\mathsf{b}+\cdots \\ &= \left(1+u\mathsf{a}(1-\mathsf{a})^{-1}\right)\mathsf{b}, \end{aligned}$$

and $\phi\left((1-\mathsf{a})^{-1}\right) = (1-\mathsf{a})^{-1}$. Working back through the substitutions we have

$$\begin{aligned}
\phi\left((1-\mathsf{a}-\mathsf{b})^{-1}\right) &= \left(1-\mathsf{a}-(1-\mathsf{a})\left(1+u\mathsf{a}(1-\mathsf{a})^{-1}\right)\mathsf{b}\right)^{-1}\\
&= (1-\mathsf{a}-\mathsf{b}+(1-u)\mathsf{ab})^{-1}
\end{aligned}$$

so

$$\begin{aligned}
\phi(1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1} &= (1-\mathsf{a}-\mathsf{b}-\mathsf{c}+(1-u)\mathsf{ab})^{-1}\\
&= ((1-\mathsf{a})(1-\mathsf{b})-\mathsf{c}-u\mathsf{ab})^{-1}.
\end{aligned}$$

Applying δ and L_α as homomorphisms

Then

$$\delta\phi\left((1-\mathsf{a}-\mathsf{b}-\mathsf{c})^{-1}\right) = ((1-x)(1-y)-z-uxy)^{-1},$$

so

$$\begin{aligned}
c_0(p,q,r) &= [x^py^qz^r]L_0\left(((1-x)(1-y)-z-uxy)^{-1}\right)\\
&= [x^py^qz^r]\,((1-x)(1-y)-z)^{-1}\\
&= [x^py^qz^r]\,(1-x)^{-1}(1-y)^{-1}\left(1-z(1-x)^{-1}(1-y)^{-1}\right)^{-1}\\
&= [x^py^q]\,(1-x)^{-(r+1)}(1-y)^{-(r+1)}\\
&= \binom{p+r}{p}\binom{q+r}{q} \quad \text{(Binomial Series Theorem)}
\end{aligned}$$

and

$$\begin{aligned}
c(p,q,r) &= [x^py^qz^r]L_1\left(((1-x)(1-y)-z-uxy)^{-1}\right)\\
&= [x^py^qz^r]\,(1-x-y-z)^{-1}\\
&= \frac{(p+q+r)!}{p!q!r!} \quad \text{(Binomial Series Theorem).}
\end{aligned}$$

The solution

We can now complete the solution of the problem.

$$\begin{aligned}
\mathsf{prob}(p,q,r) &= 1-\frac{c_0(p,q,r)}{c(p,q,r)}\\
&= 1-\binom{p+r}{p}\binom{q+r}{q}\frac{p!q!r!}{(p+q+r)!}.
\end{aligned}$$

Thus

$$\mathsf{prob}(p,q,r) = 1-\frac{\binom{p+q+2r}{r}}{\binom{p+q+r}{p+r}}.$$

This is the final result.

Coefficient extraction and the Binomial Series Theorem

I have used a small amount of technical results for extracting coefficients for series. The theorem used is the Binomial Series Theorem, which states that, if u and x are indeterminates, then

$$(1+x)^u = \sum_{i \geq 0} \binom{u}{i} x^i,$$

where

$$\binom{u}{i} = \frac{1}{i!}(u)(u-1)\cdots(u-i+1).$$

This evaluates to the the binomial coefficient for nonnegative integers, but it gives meaning to the binomial coefficient $\binom{n}{i}$ when n is *not* and integer. For example, $\binom{\pi}{2} = \pi(\pi-1)/2$.

Chapter 5

Conditions on adjacent symbols

You have now seen a powerful theory that can be brought to bear on $\{0,1\}$-sequence questions. What is more remarkable is that it can be extended to additional types of conditions and to arbitrarily large alphabets $\{1,2,\ldots\}$. There is a particular type of sequence that is of interest: a permutation. A *permutation* on the alphabet $\{1,\ldots,n\}$ is a sequence such that each symbol occurs one and only once. For example, the permutations on $\{1,2,3,4\}$ are

$$1234, 1324, 2143, 2413, 3421, \ldots.$$

A *pattern* can be associated with a sequence (or permutation) as follows. Let a stand for the relation $<$ and b stand for the relation $\geq$. Now fill in the relation between successive elements in the permutations to get

$$1\,\mathsf{a}\,2\,\mathsf{a}\,3\,\mathsf{a}\,4, 1\,\mathsf{a}\,3\,\mathsf{b}\,2\,\mathsf{a}\,4, 2\,\mathsf{b}\,1\,\mathsf{a}\,4\,\mathsf{b}\,2, 2\,\mathsf{a}\,4\,\mathsf{b}\,1\,\mathsf{a}\,3, 3\,\mathsf{a}\,4\,\mathsf{b}\,2\,\mathsf{b}\,1, \cdots,$$

and then drop the symbols of the alphabet to obtain

$$\mathsf{aaa}, \mathsf{aba}, \mathsf{bab}, \mathsf{aba}, \mathsf{abb}, \ldots.$$

These are said to be the *patterns* of the corresponding sequences. For example, the pattern of 1234 is a^3 and the pattern of 1324 and 2413 is aba.

Permutations with pattern $(\mathsf{ab})^m$ or $(\mathsf{ab})^m\mathsf{a}$ are called *alternating permutations.* For example, the set of all alternating permutations of length 4 is $\{1324, 1423, 2314, 2413, 2412\}$, so there are 5 of them. The first few terms of $\sec(x)$ are

$$\sec(x) = 1 + 1\frac{x^2}{2!} + 5\frac{x^4}{4!} + 61\frac{x^6}{6!} + 1385\frac{x^8}{8!} + \cdots,$$

and

$$4!\,[x^4]\,\sec(x) = 5.$$

I am going to prove this in general.

5.1 Problem 9

Find the number c_{2n} of alternating permutations of length $2n$.

The functions ϕ and δ

Let $\mathsf{x}_1, \mathsf{x}_2, \ldots$ be noncommuting indeterminates (previously we had just two, namely a and b). Let

$$1 \leftrightarrow \mathsf{x}_1, 2 \leftrightarrow \mathsf{x}_2, 3 \leftrightarrow \mathsf{x}_3, \cdots.$$

Thus $521153 \leftrightarrow \mathsf{x}_5\mathsf{x}_2\mathsf{x}_1^2\mathsf{x}_5\mathsf{x}_3$, and the sequence has pattern $\mathsf{b}^3\mathsf{ab}$. Let

$$\phi(\mathsf{t}) = \text{sum of the encodings of all sequences with pattern } \mathsf{t}.$$

Then

$$\phi\colon \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}\rangle\rangle \longrightarrow \mathsf{Q}\langle\langle \mathsf{x}_1, \mathsf{x}_2 \ldots\rangle\rangle.$$

For example,

$$\phi(\mathsf{a}^2) = \mathsf{x}_1\mathsf{x}_2\mathsf{x}_3 + \mathsf{x}_1\mathsf{x}_2\mathsf{x}_4 + \cdots + \mathsf{x}_1\mathsf{x}_3\mathsf{x}_4 + \mathsf{x}_1\mathsf{x}_3\mathsf{x}_5 + \cdots + \mathsf{x}_2\mathsf{x}_3\mathsf{x}_4 + \mathsf{x}_2\mathsf{x}_3\mathsf{x}_5 + \cdots + \cdots.$$

Moreover, each pattern appears once only in the series $(1 - \mathsf{a} - \mathsf{b})^{-1}$ that was so important in the earlier chapters.

Let $x_1, x_2, \ldots$ be commuting indeterminates. Let

$$\delta\colon \mathsf{Q}\langle\langle \mathsf{x}_1, \mathsf{x}_2 \ldots\rangle\rangle \longrightarrow \mathsf{Q}[[x_1, x_2, \ldots]]$$

such that $\delta(\mathsf{x}_1) = x_1$, $\delta(\mathsf{x}_2) = x_2, \ldots$ as a substitution.

Encoding the problem

The set of all alternating patterns for sequences of even length is $(1 - \mathsf{ab})^{-1}\mathsf{a}$, so the answer to the problem is

$$c_{2n} = [x_1 \cdots x_n]\ \delta\mathsf{F},$$

where

$$\mathsf{F} = \phi\left((1 - \mathsf{ab})^{-1}\mathsf{a}\right),$$

since the coefficient operator ensures that each of $1, \ldots, n$ occurs once and only once.

Properties of ϕ and δ

The task before us is quite clear in view of the work on the previous problems. It is necessary to find homomorphic properties of both ϕ and δ. Of these, δ is again easy: it is a homomorphism.

For ϕ we do not have to work very hard. Let $\diamond$ denote the full relation, the union of $<$ and $\geq$, so $\diamond$ corresponds to the application of no conditions. Let w be an indeterminate that corresponds to $\diamond$. Thus

$$\mathsf{a} + \mathsf{b} = \mathsf{w}.$$

Although w represents no conditions at all, it is a very useful object, and we now work in the noncommutative ring $\mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}, \mathsf{w}\rangle\rangle$.

First, note that $\phi(\mathsf{f} + \mathsf{g}) = \phi(\mathsf{f}) + \phi(\mathsf{g})$, for all $\mathsf{f}, \mathsf{g} \in \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}, \mathsf{w}\rangle\rangle$. For multiplication, we have $\phi(\mathsf{twt}') = \phi(\mathsf{t})\phi(\mathsf{t}')$, where t and t' are terms, because w imposes no conditions at all. Then, extending this from terms to series we have $\phi(\mathsf{fwg}) = \phi(\mathsf{f})\phi(\mathsf{g})$. Summarising these properties, we have

$$\left.\begin{array}{rcl} \phi(\mathsf{f} + \mathsf{g}) & = & \phi(\mathsf{f}) + \phi(\mathsf{g}), \\ \phi(\mathsf{fwg}) & = & \phi(\mathsf{f})\phi(\mathsf{g}), \\ \phi(1) & = & 1. \end{array}\right\}$$

Then ϕ is a *partial homomorphism*, and indicates that our strategy ought to be to introduce w in a systematic way so that advantage can be taken of the partial homomorphism.

Two combinatorial-algebraic expansions

We use two subtle observation that at first sight are trivial. The first is

$$1 - \mathsf{ab} = 1 - \mathsf{a}(\mathsf{w} - \mathsf{a}) = 1 + \mathsf{a}^2 - \mathsf{aw}.$$

The second, that follows from this, is

$$\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{a} = \left(1 + \mathsf{a}^2\right)^{-1} \left(1 + \mathsf{a}^2 - \mathsf{aw}\right) (1 - \mathsf{ab})^{-1} \mathsf{a}.$$

Applying ϕ as a partial homomorphism

Combining these two gives

$$\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{a} = (1 - \mathsf{ab})^{-1} \mathsf{a} - \left(1 + \mathsf{a}^2\right)^{-1} \mathsf{aw} \, (1 - \mathsf{ab})^{-1} \mathsf{a}.$$

Now apply ϕ to obtain

$$\begin{array}{rcl} \phi\left(\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{a}\right) & = & \phi\left((1 - \mathsf{ab})^{-1} \mathsf{a} - \left(1 + \mathsf{a}^2\right)^{-1} \mathsf{aw} \, (1 - \mathsf{ab})^{-1} \mathsf{a}\right) \\ & = & \phi\left((1 - \mathsf{ab})^{-1} \mathsf{a}\right) - \phi\left(\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{aw} \, (1 - \mathsf{ab})^{-1} \mathsf{a}\right) \\ & & \text{(additive property of } \phi\text{)} \\ & = & \phi\left((1 - \mathsf{ab})^{-1} \mathsf{a}\right) - \phi\left(\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{a}\right) \phi\left((1 - \mathsf{ab})^{-1} \mathsf{a}\right) \\ & & \text{(multiplicative property of } \phi\text{)} \\ & = & \left(1 - \phi\left(\left(1 + \mathsf{a}^2\right)^{-1} \mathsf{a}\right)\right) \phi\left((1 - \mathsf{ab})^{-1} \mathsf{a}\right) \end{array}$$

so

$$\mathsf{F} = \left(1 - \phi\left(\left(1+\mathsf{a}^2\right)^{-1}\mathsf{a}\right)\right)^{-1}\phi\left(\left(1+\mathsf{a}^2\right)^{-1}\mathsf{a}\right)$$

and, tidying this up by adding 1 to both sides,

$$1 + \mathsf{F} = \left(1 - \phi\left(\left(1+\mathsf{a}^2\right)^{-1}\mathsf{a}\right)\right)^{-1}.$$

Now apply δ, giving

$$1 + \delta\mathsf{F} = \left(1 - \delta\phi\left(\left(1+\mathsf{a}^2\right)^{-1}\mathsf{a}\right)\right)^{-1},$$

since δ is a homomorphism. But

$$\begin{aligned} \delta\phi\left((1+\mathsf{a}^2)^{-1}\mathsf{a}\right) &= \delta\phi\left(\mathsf{a} - \mathsf{a}^3 + \mathsf{a}^5 - \mathsf{a}^7 + \cdots\right) \\ &= \delta\phi(\mathsf{a}) - \delta\phi(\mathsf{a}^3) + \delta\phi(\mathsf{a}^5) - \delta\phi(\mathsf{a}^7) + \cdots. \end{aligned}$$

To simplify this, let

$$\delta\phi(\mathsf{a}^{k-1}) = \gamma_k,$$

where γ_k is a series in the commuting indeterminates $x_1, x_2, \ldots$. The suffix for γ is k since the sequences with pattern a^{k-1} have length k, not $k-1$. Then

$$1 - \delta\phi\left(\left(1+\mathsf{a}^2\right)^{-1}\mathsf{a}\right) = 1 - \gamma_2 + \gamma_4 - \cdots,$$

so

$$c_{2n} = [x_1 \cdots x_{2n}]\left(1 - \gamma_2 + \gamma_4 - \cdots\right)^{-1}.$$

Computing the γ_i's

The answer has been left in terms of γ_k. However, this can be worked out easily since, from the definition, it is the generating series for all sequences of length k whose symbols are in strictly increasing order. For example,

$$\begin{aligned} \gamma_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_1x_3x_4 + x_1x_3x_5 + \cdots \\ &\quad + x_2x_3x_4 + x_2x_3x_5 + \cdots \\ &= [t^3]\prod_{i\geq 1}(1 + tx_i), \end{aligned}$$

where $\prod_{i\geq 1}(1+tx_i)$ denotes the product of the terms $1 + tx_i$ for all integer values of i greater than or equal to 1. In general, clearly

$$\gamma_k = [t^k]\prod_{i\geq 1}(1 + tx_i).$$

Indeterminates

The final task in the solution of this problem is to find the coefficient, and for this we need to know some properties of the γ_k's. The key observation is that we can set

$$x_1^2 = x_2^2 = \cdots = 0.$$

Be careful about this. It does *not* mean that $x_1 = x_2 = \cdots = 0$. This is because the x_i's are indeterminates. They could be integers, in which case they would be zero. However, they could also be 2×2 square matrices, in which case they need not be zero. For example,

$$x_1^2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0, \quad x_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0.$$

Thus $x_1^2 = 0$ and $x_1 \neq 0$.

If $xy = 0$ but $x, y \neq 0$ then x and y are called *zero divisors*. We cannot *assume* that $x_1, x_2, \ldots$ have *no* zero divisors. This is what we mean by saying that $x_1, x_2, \ldots$ are *indeterminates*: we can make no assumptions about them, except that $x_i^k x_i = x_i^{k+1}$ if $k \geq 0$, and $x_i^0 = 1$.

We are now going to work in the ring $\mathsf{Q}[[x_1, x_2, \ldots]]$ with the conditions $x_1^2 = 0$, $x_2^2 = 0, \ldots$. This is in fact another ring, called a *quotient ring* and is denoted by $\mathsf{Q}[[x_1, x_2, \ldots]]/(x_1^2 = 0, x_2^2 = 0, \ldots)$, but I am going to develop this a little further.

The homomorphism θ

Then, *computing within this quotient ring* we have

$$\begin{aligned}
\gamma_k &= [t^k] \prod_{i \geq 1} (1 + t x_i) \\
&= [t^k] \prod_{i \geq 1} e^{t x_i} \\
&\quad (e^x = 1 + x \text{ inside this quotient ring!}) \\
&= [t^k]\, e^{t(x_1 + x_2 + \cdots)} \\
&= [t^k]\, e^{t\gamma_1} \quad (\text{definition of } \gamma_1) \\
&= \frac{\gamma_1^k}{k!}.
\end{aligned}$$

Now some magic happens. Let θ denote the function

$$\theta(\gamma_k) = \frac{x^k}{k!}.$$

Then θ is a substitution function, and is therefore a homomorphism. We have the following remarkable result about it.

Lemma 5.1 *Let f be a series in $\gamma_1, \gamma_2, \ldots$. Then*

$$[x_1 \cdots x_n]\, f = n!\,[x^n]\,\theta f.$$

Proof: $[x_1 \cdots x_n] f = ([x_1 \cdots x_n]\gamma_1^n)\;[x^n]\theta f = n![x^n]\theta f.$ $\quad|$

The solution

We can now complete the solution of the problem.

$$\begin{aligned}
c_{2n} &= [x_1 \cdots x_{2n}]\,(1 - \gamma_2 + \gamma_4 - \cdots)^{-1} \\
&= (2n)!\,\left[x^{2n}\right]\,\theta\,(1 - \gamma_2 + \gamma_4 - \cdots)^{-1} \quad \text{(from the above Lemma)} \\
&= (2n)!\,\left[x^{2n}\right]\,\left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots\right)^{-1} \quad \text{(from the above Lemma)} \\
&= (2n)!\,\left[x^{2n}\right]\,\sec(x).
\end{aligned}$$

Thus, the answer to this problem is

$$c_{2n} = (2n)!\,\left[x^{2n}\right]\sec(x).$$

The chain of transformations

The steps in the solution of the above problem are summarised below in a very useful diagram. We used a to stand for $<$ and b to stand for $\geq$, and noted that $\mathsf{a} + \mathsf{b} = \mathsf{w}$ where w stands for the imposition of *no* conditions. Thus we worked in the ring $\mathsf{R} = \mathsf{Q}\langle\langle \mathsf{a}, \mathsf{b}, \mathsf{w}\rangle\rangle/(\mathsf{a} + \mathsf{b} = \mathsf{w})$.

We started with an encoding of the *pattern* of the alternating sequences. This was transformed by ϕ that fills in the symbols of the sequences that satisfy the pattern. The result was transformed by δ which retained information about which symbols occurred, but forgot the order of the appearance in the sequences. Finally, the result of this was transformed by θ, which picked out all of the sequences that had one copy of each symbol in $\{1, \ldots, n\}$, for some n. These are the permutations. Thus the chain of transformations is:

$$\begin{array}{ccccccc}
\mathsf{R} & \xrightarrow{\phi} & \mathsf{Q}\langle\langle \mathsf{x}_1, \ldots\rangle\rangle & \xrightarrow{\delta} & \mathsf{Q}[[x_1, \ldots]] & \xrightarrow{\theta} & \mathsf{Q}[[x]], \\
(1 - \mathsf{ab})^{-1}\mathsf{a} & \xmapsto{\phi} & \left(1 - \phi\left((1 + \mathsf{a}^2)^{-1}\mathsf{a}\right)\right)^{-1} & \xmapsto{\delta} & \frac{1}{1 - \gamma_2 + \gamma_4 - \cdots} & \xmapsto{\theta} & \sec(x),
\end{array}$$

where $\mathsf{g} = \left(1 - \phi\left((1 + \mathsf{a}^2)^{-1}\mathsf{a}\right)\right)^{-1}$. The first line of the diagram specifies the sets to which these expressions belong, as they are successively transformed.

As before, in the earlier Problems, each transformation achieves a combinatorial goal, although the details behind it are algebraic. This diagram, when it is read correctly, therefore indicates the connexion between the combinatorial and algebraic ideas.

5.2 Problem 10

Let $\mathbf{A}_n$ denote the $n \times n$ matrix whose (i,j)-element is $\binom{2j}{2i-2}$, with the convention that if $j > i$ then $\binom{i}{j} = 0$. Then

$$[x^{2n}] \sec(x) = \frac{1}{(2n)!} \det \mathbf{A}_n$$

Numerical computation

Let $n = 3$. Then

$$\det \mathbf{A}_3 = \begin{vmatrix} \binom{2}{0} & \binom{4}{0} & \binom{6}{0} \\ \binom{2}{2} & \binom{4}{2} & \binom{6}{2} \\ \binom{2}{4} & \binom{4}{4} & \binom{6}{4} \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 6 & 15 \\ 0 & 1 & 15 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & 5 & 14 \\ 0 & 1 & 15 \end{vmatrix} = 61,$$

by subtracting column 1 from columns 2 and 3. Thus

$$[x^6]\ \sec(x) = \frac{61}{6!},$$

in agreement with the expansion that was given earlier for $\sec(x)$.

The solution

This problem does not seem to be a combinatorial one; it looks more like a problem from calculus. However, combinatorial techniques can be used to solve it.

I am going to do this for $n = 3$, and will leave you to edit the proof so that it is general. Consider the set of all alternating permutations of length 6. Then we have seen that there are $6![x^6]\ \sec(x)$ of them. But these can be counted in another way. Their pattern is $(\mathsf{ab})^2\mathsf{a}$, so the number of permutations with this pattern is $[x_1 \cdots x_6]\, \delta\phi((\mathsf{ab})^2\mathsf{a})$, where ϕ is defined in Problem 9. Thus

$$6!\ [x^6]\ \sec(x) = [x_1 \cdots x_6]\ \delta\phi\left((\mathsf{ab})^2\mathsf{a}\right).$$

We now determine the right hand side but another subtle expansion that makes use of the properties of ϕ as a partial homomorphism. This expansion is obtained by the repeated application of the first of the two *combinatorial-algebraic expansions* for Problem 9.

$$\begin{aligned}
\phi(\mathsf{ababa}) &= \phi(\mathsf{aba(w-a)a}) \quad \text{(1st. application of } \mathsf{b} = \mathsf{w} - \mathsf{a}\text{)} \\
&= \phi(\mathsf{abawa}) - \phi(\mathsf{abaaa}) \quad \text{(additive property of } \phi\text{)} \\
&= \phi(\mathsf{aba})\,\phi(\mathsf{a}) - \phi\left(\mathsf{aba}^3\right) \quad \text{(multiplicative property of } \phi\text{)} \\
&= \phi(\mathsf{aba})\,\phi(\mathsf{a}) - \phi\left(\mathsf{a(w-a)a}^3\right) \quad \text{(2nd. application of } \mathsf{b} = \mathsf{w} - \mathsf{a}\text{)} \\
&= \phi(\mathsf{aba})\,\phi(\mathsf{a}) - \phi(\mathsf{a})\,\phi\left(\mathsf{a}^3\right) - \phi\left(\mathsf{a}^5\right) \quad \text{(both properties of } \phi\text{)}
\end{aligned}$$

so $\phi\left(\mathsf{ababa}\right)-\phi\left(\mathsf{aba}\right)\phi\left(\mathsf{a}\right)+\phi\left(\mathsf{a}\right)\phi\left(\mathsf{a}^3\right)=\phi\left(\mathsf{a}^5\right)$. Similarly,

$$\begin{aligned}\phi\left(\mathsf{aba}\right) &= \phi\left(\mathsf{a}(\mathsf{w}-\mathsf{a})\mathsf{a}\right) \quad \text{(1st. application of } \mathsf{b}=\mathsf{w}-\mathsf{a}) \\ &= \phi\left(\mathsf{a}\right)\phi\left(\mathsf{a}\right)-\phi\left(\mathsf{a}^3\right), \quad \text{(both properties of } \phi)\end{aligned}$$

so $\phi\left(\mathsf{aba}\right)-\phi\left(\mathsf{a}\right)\phi\left(\mathsf{a}\right)=\phi\left(\mathsf{a}^3\right)$. Collecting these equations we have

$$\left.\begin{aligned}\phi\left(\mathsf{ababa}\right)-\phi\left(\mathsf{aba}\right)\phi\left(\mathsf{a}\right)+\phi\left(\mathsf{a}\right)\phi\left(\mathsf{a}^3\right) &= \phi\left(\mathsf{a}^5\right), \\ \phi\left(\mathsf{aba}\right)-\phi\left(\mathsf{a}\right)\phi\left(\mathsf{a}\right) &= \phi\left(\mathsf{a}^3\right), \\ \phi\left(\mathsf{a}\right) &= \phi\left(\mathsf{a}\right),\end{aligned}\right\}$$

where the last equation is a triviality. In matrix form, this system of linear equations is

$$\begin{bmatrix} 1 & -\phi\left(\mathsf{a}\right) & \phi\left(\mathsf{a}^3\right) \\ 0 & 1 & -\phi\left(\mathsf{a}\right) \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \phi\left(\mathsf{ababa}\right) \\ \phi\left(\mathsf{aba}\right) \\ \phi\left(\mathsf{a}\right) \end{bmatrix}=\begin{bmatrix} \phi\left(\mathsf{a}^5\right) \\ -\phi\left(\mathsf{a}^3\right) \\ \phi\left(\mathsf{a}\right) \end{bmatrix},$$

where $\phi\left(\mathsf{ababa}\right)$, $\phi\left(\mathsf{aba}\right)$ and $\phi\left(\mathsf{a}\right)$ are to be regarded as the unknowns, for this purpose. Note that the coefficient matrix is upper triangular with no zeros on the diagonal, so the matrix is invertible and the system has a unique solution. Now apply the homomorphism δ to give

$$\begin{bmatrix} 1 & -\delta\phi\left(\mathsf{a}\right) & \delta\phi\left(\mathsf{a}^3\right) \\ 0 & 1 & -\delta\phi\left(\mathsf{a}\right) \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \delta\phi\left(\mathsf{ababa}\right) \\ \delta\phi\left(\mathsf{aba}\right) \\ \delta\phi\left(\mathsf{a}\right) \end{bmatrix}=\begin{bmatrix} \delta\phi\left(\mathsf{a}^5\right) \\ -\delta\phi\left(\mathsf{a}^3\right) \\ \delta\phi\left(\mathsf{a}\right) \end{bmatrix}.$$

This is because matrix multiplication consists simply of additions and multiplications, operations that are preserved by the homomorphism. But $\delta\phi(\mathsf{a}^k)=\gamma_{k+1}$, by definition, so

$$\begin{bmatrix} 1 & -\gamma_2 & \gamma_4 \\ 0 & 1 & -\gamma_2 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \delta\phi\left(\mathsf{ababa}\right) \\ \delta\phi\left(\mathsf{aba}\right) \\ \delta\phi\left(\mathsf{a}\right) \end{bmatrix}=\begin{bmatrix} \gamma_6 \\ -\gamma_4 \\ \gamma_2 \end{bmatrix}.$$

The unknown that we want is $\delta\phi\left(\mathsf{ababa}\right)$. The elements of the matrix and vectors commute since they involve only commuting indeterminates $x_1, x_2, \ldots$, so the determinant is defined. This is a technical fact about determinants and noncommutation: determinants are only defined in a *commutative ring.* Then, by Crámer's Rule, noting that the determinant of the coefficient matrix is 1, we have

$$\delta\phi\left(\mathsf{ababa}\right)=\begin{vmatrix} \gamma_6 & -\gamma_2 & \gamma_4 \\ -\gamma_4 & 1 & -\gamma_2 \\ \gamma_2 & 0 & 1 \end{vmatrix}=\begin{vmatrix} \gamma_2 & \gamma_4 & \gamma_6 \\ 1 & \gamma_2 & \gamma_4 \\ 0 & 1 & \gamma_2 \end{vmatrix}$$

by switching columns and removing factors of -1 from rows and columns. Thus,

$$[x_1\cdots x_6]\,\delta\phi(\mathsf{ababa}) = 6!\left[x^6\right]\theta\begin{vmatrix} \gamma_2 & \gamma_4 & \gamma_6 \\ 1 & \gamma_2 & \gamma_4 \\ 0 & 1 & \gamma_2 \end{vmatrix} \quad \text{(by the Lemma)}$$

$$
\begin{aligned}
&= 6!\,[x^6]\begin{vmatrix} \theta(\gamma_2) & \theta(\gamma_4) & \theta(\gamma_6) \\ \theta(1) & \theta(\gamma_2) & \theta(\gamma_4) \\ 0 & \theta(1) & \theta(\gamma_2) \end{vmatrix} \\
&\qquad \text{(since } \theta \text{ is a homomorphism)} \\
&= 6!\,[x^6]\begin{vmatrix} \frac{x^2}{2!} & \frac{x^4}{4!} & \frac{x^6}{6!} \\ 1 & \frac{x^2}{2!} & \frac{x^4}{4!} \\ 0 & 1 & \frac{x^2}{2!} \end{vmatrix} = 6!\begin{vmatrix} \frac{1}{2!} & \frac{1}{4!} & \frac{1}{6!} \\ 1 & \frac{1}{2!} & \frac{1}{4!} \\ 0 & 1 & \frac{1}{2!} \end{vmatrix} \\
&= \begin{vmatrix} \binom{2}{0} & \binom{4}{0} & \binom{6}{0} \\ \binom{2}{2} & \binom{4}{2} & \binom{6}{2} \\ \binom{2}{4} & \binom{4}{4} & \binom{6}{4} \end{vmatrix},
\end{aligned}
$$

by elementary properties of the determinant. In the application of θ we have used the fact that the determinant involves only addition and multiplication, and these are preserved by θ since, as we have proved, θ is a homomorphism.

Thus we have

$$
[x^6]\sec(x) = \frac{1}{6!}\begin{vmatrix} \binom{2}{0} & \binom{4}{0} & \binom{6}{0} \\ \binom{2}{2} & \binom{4}{2} & \binom{6}{2} \\ \binom{2}{4} & \binom{4}{4} & \binom{6}{4} \end{vmatrix},
$$

which completes the solution.

5.3 Summary and closing comments

I have introduced you so some very powerful methods for examining sequences. Although little more than addition and multiplication have been used, the ideas have been subtle. We have used the notion of a noncommutative ring to hold the encodings of the sequences. We have used functions to retain counting information and to destroy all other information. We have studied the homomorphic properties of these functions. Finally, we have extended these ideas to more general sequences and more general conditions.

Of course, more can be done and there are further generalisations. For example, the theory can be extended to give a theorem for counting sequences that have no forbidden subsequences. This has been used to obtain the best known approximation to the answer to the Excluded Volume Problem.

Perhaps you are surprised that I have not given you any theorems. There are theorems, and these are proved by the theory that I have developed for you. One of them is in the set of Problems.

This completes my brief introduction for you to the connexion between non-commutation and combinatorics. Even in this very brief glimpse, you have before you evidence that some very elegant ideas can greatly simplify very hard problems.

Chapter 6

Problems to work on

Below are a variety of questions on sequences. They are of varying difficulty, but they can all be done with the material that I have presented here, and with some of the intuition that I have tried to give.

1. (a) Let a and b be noncommuting indeterminates. Prove that

$$(1-\mathsf{a}-\mathsf{b})^{-1} = (1-\mathsf{b})^{-1}\left(1-(1-\mathsf{a})^{-1}\mathsf{ab}(1-\mathsf{b})^{-1}\right)^{-1}(1-\mathsf{a})^{-1}.$$

   (b) Hence, or otherwise, use this *combinatorial-algebraic expansion* to find the generating series for number of $\{0,1\}$-sequences of length n with p occurrences of the subsequence 00 and q occurrences of the subsequence 111.

2. Find the generating series for the number of $\{0,1\}$-sequences of length n such that every subsequence of 0's of length at least 3 is followed by a subsequence of 1's of length at least 3.

3. Prove that the number of alternating permutations of length $2n+1$ is

$$(2n+1)!\left[x^{2n+1}\right]\tan(x).$$

4. Express $\left[x^{2n+1}\right]\tan(x)$ as the determinant of a matrix involving binomial coefficients.

5. Consider a sequence in the alphabet $\{1,2,\ldots\}$. A *maximal strictly increasing* subsequence, is a subsequence that is strictly increasing and cannot be made longer by the adjoining of adjacent symbols. For example, the maximal strictly increasing subsequences of the sequence 1566278952, listed in the order in which they appear are 156, 6, 2789, 5, and 2. These have lengths $3,1,4,1,2$ respectively. Note that they factorise the sequence into $156|6|2789|5|2$. Let the indeterminate f_i record the occurrence of a maximal increasing subsequence of length i.

Let $f = 1 + f_1 x + f_2 x^2 + \cdots$ and let $f^{-1} = 1 + g_1 x + g_2 x^2 + \cdots$. By considering the expansion

$$(1 - \mathsf{a} - \mathsf{b})^{-1} = \left(1 - (1-\mathsf{a})^{-1}\mathsf{b}\right)(1-\mathsf{a})^{-1},$$

or otherwise, prove that the generating series that counts sequences with respect to the lengths of their maximal strictly increasing subsequences is

$$(1 + g_1\gamma_1 + g_2\gamma_2 + \cdots)^{-1}.$$

This is called the *Maximal Decomposition Theorem.*

6. Use the Maximal Decomposition Theorem to solve the alternating permutation problem for permutations of even length.

7. A *strict increase* in a sequence is a subsequence ij with $i < j$. Prove that the number of permutations of length n with k strict increases is

$$n!\left[u^k x^n\right] \frac{u-1}{u - e^{(u-1)x}}.$$

8. A *strict maximum* in a sequence is an element j of a subsequence ijk such that $i < j$ and $j \geq k$. Let a stand for $<$ and b stand for $\geq$.

   (a) Prove that
   $$\left(1 - \mathsf{a}^2 - \mathsf{b}^2 - \mathsf{ba}\right)^{-1}$$
   generates all patterns of sequences of odd length which do not have a strict maximum in a even numbered position.

   (b) Prove that the number of such permutations of odd length n is
   $$n!\,[x^n]\,\frac{\tanh x}{1 - x\tanh x},$$
   where *tanh* is the hyperbolic tangent function.

9. Let a stand for 0 and b stand for 1.

   (a) Prove that
   $$\left(1 - u\mathsf{a} - \left(1 + (1-u)(\mathsf{a}+\mathsf{a}^2)\right)\mathsf{b}\right)^{-1}\left(1 + (1-u)(\mathsf{a}+\mathsf{a}^2)\right)$$
   is the series that encodes the set of all $\{0,1\}$-sequences in its terms, each term corresponding to a sequence, and that the coefficient of each term is a power of u, where the power is the number of occurrences of 000 as a subsequence of the corresponding sequence.

   (b) Prove that this sequence can be rewritten as
   $$\left(1 - (1-\mathsf{a}-\mathsf{b})^{-1}\left(1 - v\left(\mathsf{a}+\mathsf{a}^2\right)\right)^{-1} v\mathsf{a}^3\right)^{-1}(1-\mathsf{a}-\mathsf{b})^{-1},$$
   where $v = u - 1$.

(c) Now regard v as an indeterminate, and forget that it is equal to $u-1$. Give a sequence problem, involving 000 as a subsequence, to which this is the solution, and explain the role of the constituents $(1-\mathsf{a}-\mathsf{b})^{-1}$ and $\left(1-v\left(\mathsf{a}+\mathsf{a}^2\right)\right)^{-1} v\mathsf{a}^3$. For example, $(1-\mathsf{a}-\mathsf{b})^{-1}$ encodes all $\{0,1\}$-sequences, but how does this relate to $\left(1-v\left(\mathsf{a}+\mathsf{a}^2\right)\right)^{-1}$, and to $v\mathsf{a}^3$ and to occurrences of 000 as a subsequence?

(d) If you can answer the previous part, does your answer suggest how to exclude both 000 and 01110. Explain. (This is moving slightly closer towards the Excluded Volume Problem.)

10. Let ij a subsequence of a sequence in the alphabet $\{1, 2, \ldots\}$. Then ij is called a *strict increase* if $i < j$, a *level* if $i = j$, and a *strict decrease* if $i > j$. Let $\mathsf{u}, \mathsf{s}, \mathsf{d}$, respectively, stand for these. Explain how to use this theory to count sequences with respect to the number of strict increases, levels, and strict decreases. Start by finding an algebraic relationship between $\mathsf{s}, \mathsf{u}, \mathsf{d}$ and then indicate how to use it.