MATHEMATICAL MAGIC VIA DE BRUIJN SEQUENCES II

JEREMY BOOHER

1. Warmup

(1) How many sequences of 0's and 1's of length 3 are there?

(2) Can you find a sequence of 0's and 1's such that when you arrange them around a circle, each sequence of 0's and 1's of length 3 appears exactly once? How long must such a sequence be?

(3) (Digression) How many such sequences are there?

Date: September 21, 2024.

2. de Bruijn Sequences

Definition 2.1. A binary *de Bruijn sequence* of order n is a sequence of 0's and 1's such that when arranged around a circle every length-n sequence of 0's and 1's appears exactly once.

Variants: having order n is sometimes called having "window n". Do you see why? You can also use more symbols than just 0's and 1's, in which case the sequence is no longer binary.

Definition 2.2. An *linear feedback shift register* is a sequence where the next term in the sequence is given by a linear function of previous terms in the sequence.

The ones we will consider consist of sequences whose terms are either 0 and 1, and arithmetic is done modulo two. (The name comes from computer science: these computations are very easy to do on a computer or using circuits.)

(4) Consider the linear feedback shift register given by $a_n = a_{n-2} + a_{n-3} \mod 2$, and starting with 001. What sequence does it produce, and how long does it take until it returns to its initial state?

(5) Consider the linear feedback shift register given by $a_n = a_{n-3} + a_{n-5} \mod 2$, and starting with 00001. What sequence does it produce, and how long does it take until it returns to its initial state?

(6) What connections do you see between the sequences produced by these linear feedback shift registers and de Bruijn sequences?

3. Polynomials Modulo Polynomials

Now we work with polynomials modulo 2 and modulo a polynomial $f(x)$. Here is an example.

Example 3.1. $(x^2 + x + 1) + (x^3 + x) \equiv x^3 + x^2 + 1 \mod (2, x^5 + x^2 + 1)$ since we treat the coefficients of the polynomials as being integers modulo 2. Furthermore,

$$x^3(x^2 + 1) \equiv x^5 + x^3 \equiv (x^2 + 1) + x^3 \equiv x^3 + x^2 + 1 \mod (2, x^5 + x^2 + 1).$$

The second step uses that $x^5 + x^2 + 1 \equiv 0 \mod (2, x^5 + x^2 + 1)$, or equivalently $x^5 \equiv x^2 + 1 \mod (2, x^5 + x^2 + 1)$ as $1 \equiv -1 \mod 2$.

(7) Find the powers of x modulo $(2, x^3 + x + 1)$.

(8) Find the powers of x modulo $(2, x^5 + x^2 + 1)$.

(9) Obtain a sequence of numbers by looking at the coefficient of x^2 in (7) (resp. x^4 in (8)). What is the connection with the linear feedback shift registers we previously looked at? Why do we essentially get de Bruijn sequences?

4. Conclusion

(10) Can you explain the magic trick using de Bruijn sequences? Can you perform the trick yourself?
(11) Try to construct a de Bruijn sequences by working modulo $(2, x^3 + x)$. What goes wrong? What was special about $(2, x^3 + x + 1)$ in (7)?
(12) Construct a binary de Bruijn sequence of order 4.
(13) Is there a binary de Bruijn sequence of order n for all positive integers n?
(14) How might de Bruijn sequnces help a robot navigate in a lab?
(15) Can you construct de Bruijn sequences using three or more symbols, like $\{0, 1, 2\}$?

If you want to see more mathematical magic tricks, I recommend "Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks" by Persi Diaconis and Ron Graham.