10.1. Xor Map (50)

Background

Suppose we have a ternary Boolean function $f : \mathbf{2}^3 \to \mathbf{2}$. We can extend f to a map F defined on bit sequences (say, of length at least 3 to avoid awkwardness) by setting

$$F(\boldsymbol{x})(i) = f(x_{i-1}, x_i, x_{i+1})$$

Here the indices are supposed to wrap around, so that x_1 is the right neighbor of x_n, and x_n the left neighbor of x_1. In other words, we think of x as a circular rather than linear sequence and apply f, in parallel, to all blocks of 3 consecutive bits. Note that this also works, without any wrap-around, for biinfinite sequences.

As it turns out, F is additive in the sense that

$$F(\boldsymbol{x} + \boldsymbol{y}) = F(\boldsymbol{x}) + F(\boldsymbol{y})$$

where + stands for bitwise exclusive or (or addition mod 2). If we iterate F on $\boldsymbol{x} \in \mathbf{2}^n$, the only a priori upper bound for the transients and periods is 2^n, but it turns out that for additive maps the transients are usually quite short, and the periods are typically also short. Here are the transient/period values for all one-point seed configurations up to size 40 for F. Take some time to study this table, a lot of information is hiding there.

n	t	p	n	t	p
1	–	–	21	1	63
2	–	–	22	1	62
3	1	1	23	1	2047
4	2	1	24	4	8
5	1	3	25	1	1023
6	1	2	26	1	126
7	1	7	27	1	511
8	4	1	28	2	28
9	1	7	29	1	16383
10	1	6	30	1	30
11	1	31	31	1	31
12	2	4	32	16	1
13	1	63	33	1	31
14	1	14	34	1	30
15	1	15	35	1	4095
16	8	1	36	2	28
17	1	15	37	1	87381
18	1	14	38	1	1022
19	1	511	39	1	4095
20	2	12	40	4	24

Here is the distribution of transient/period pairs for $n = 10$.

t/p	#	t/p	#
$(0, 1)$	1	$(1, 1)$	3
$(0, 3)$	15	$(1, 3)$	45
$(0, 6)$	240	$(1, 6)$	720

Needless to say, the tables were obtained by brute force computation.

Task

A. It is easy to check that f is additive. Verify that F is also additive.

B. Why is F never injective on $\mathbf{2}^n$?

C. In the example $n = 10$, the period of any configurations is a divisor of the period of the one-point seed configuration (6 in this case). Is this always the case? Why?

D. Explain the entries in the main table for $n = 2^k$. Describe all the orbits in this special case.

E. How about $n = 2^k \pm 1$ (this is a bit harder).

F. Now consider the biinfinite grid with the one-point seed configuration $\boldsymbol{x}$ defined by $x_0 = 1$, $x_i = 0$ otherwise. Find a reasonably simple description for the bit at time $t \geq 0$ in cell $k \in \mathbb{Z}$.

Comment

For the last part, you will undoubtedly run into binomial coefficients. You may find it useful to think about path counting in a rectangular grid (rotated appropriately so things match up properly with the grid of cells). Think about a single pebble in position $x = 0$ at time $t = 0$ that splits and moves one copy to the left, and one to right at time $t + 1$. Two copies in the same spot cancel out.

Extra Credit 1: Do the same for $f(x, y, z) = x + y + z$. This may seem like a minor modification, but things turn out to be considerably more complicated.

Extra Credit 2: Explain the rest of the table. One way to tackle this problem is to identify a configuration $(c_0, c_1, \ldots, c_{n-1})$ with the polynomial $\sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_2[x]$. The map F can then be expressed elegantly in terms of the quotient ring $\mathbb{F}_2[x]/(x^n + 1)$. Then use algebra.

Solution: Xor Map

Part A: Additive

Write $\beta(\boldsymbol{x}) = ((x_{-1}, x_1, x_2), (x_1, x_2, x_3), \ldots, (x_{-2}, x_{-1}, x_1))$ for the function that produces a list of overlapping blocks of length 3 from a given $x \in \mathbf{2}^n$ and write $\mathsf{map}(g, L)$ for the map that applies function g to each element in list L. Then by the additivity of f we have

$$\begin{aligned} F(\boldsymbol{x} + \boldsymbol{y}) &= \mathsf{map}(f, \beta(\boldsymbol{x} + \boldsymbol{y})) \\ &= \mathsf{map}(f, \beta(\boldsymbol{x}) + \beta(\boldsymbol{y})) \\ &= \mathsf{map}(f, \beta(\boldsymbol{x})) + \mathsf{map}(f, \beta(\boldsymbol{y})) \\ &= F(\boldsymbol{x}) + F(\boldsymbol{y}) \end{aligned}$$

Part B: Injective

Consider the configurations all-ones $\mathbf{1}$ and all-zeros $\mathbf{0}$. Then $F(\mathbf{0}) = \mathbf{0} = F(\mathbf{1})$ so that the global map is not injective. In fact, by additivity,

$$F(X) = F(X + \mathbf{1})$$

for any configuration X.

Part C: Periods

We claim that any configuration has period dividing the period of, say, $\boldsymbol{e}_1$ (which is the same for all unit vectors $\boldsymbol{e}_i$).

To see this consider more generally a map $g : A \to A$ and a point $a \in A$. If a has periods p and q under g where $p < q$ then clearly a also has period $q - p$: $g^p(a) = a = g^q(a)$. It follows that $\gcd(p, q)$ is also a period.

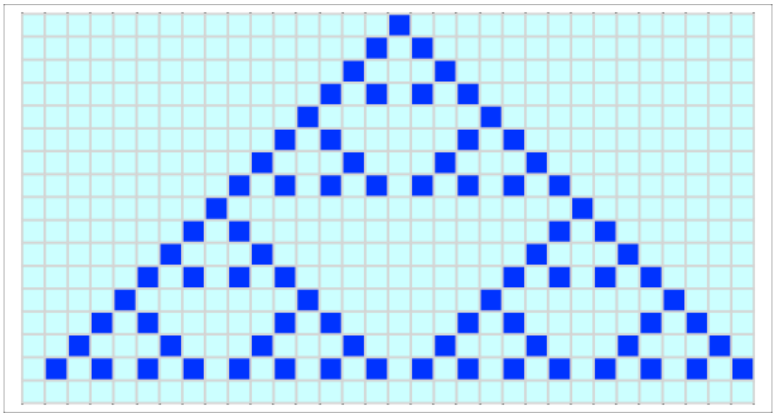
Now consider any configuration $\boldsymbol{x} \in \mathbf{2}^n$. We can write $\boldsymbol{x} = \sum_i x_i \boldsymbol{e}_i$ where $\boldsymbol{e}_i$. By additivity

$$F^t(\boldsymbol{x}) = \sum_i x_i F^t(\boldsymbol{e}_i)$$

Since the transient and period of all the $\boldsymbol{e}_i$ is the same it is clear that the period q of $\boldsymbol{x}$ cannot be any larger than p, the period of any unit vector. But if $q < p$ then we must have $q \mid p$ by the previous comment.

Part D: Powers of 2

For $n = 2^k$, $k > 1$, the table suggests that all configurations evolve to a fixed point after at most 2^{k-1} steps. To see why, it is best to draw a picture of an orbit. For $n = 32$ we get

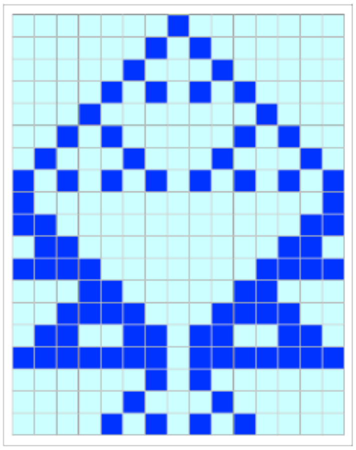


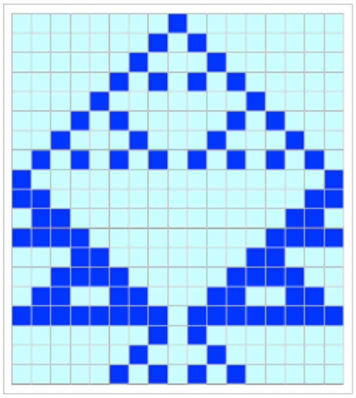
At time $t = 16$ we have reached the fixed point $\mathbf{0}$. Moreover, one can read off a geometric proof from this picture. By induction, we can show that for $t = 2^i - 1$, $i < k$, configuration $F^t(\boldsymbol{e}_1)$ consists of an alternating block $10101 \ldots 0101$ of length $2t + 1$, surrounded by $0's$. Hence, at the next step $t + 1$ we must have a configuration of two 1's, separated by $2t + 1$ many $0's$.

However, because of the periodic boundary conditions we reach $\mathbf{0}$ at time $n/2$.

Part E: Nearby

If you geometric intuition is excellent you may be able to deal with the $2^k \pm 1$ case by looking at the previous section–otherwise some more simulation is needed. Here is a typical orbit for $n = 15$: the transient is 1 and the period is 15. The same transient and period appear for $n' = 17$.





In general, we would expect transient 1 and period $2^k - 1$ for $n = 2^k \pm 1$.

For a proof, we can recycle the result from the last section to explain the "thick" part of the picture as a superposition of two adjacent unit vector orbits. As a consequence we obtain a configuration of the form $\mathbf{1} - \boldsymbol{e}_i$ at time $2^k - 1$. At the next step we obtain $\boldsymbol{e}_{i-1} + \boldsymbol{e}_{i+1}$ and have completed the first cycle.

Part F: Biinfinite

Count the number of ways a pebble could travel from cell 0 at time 0 to cell c at time $t \geq 0$ (where at each step the pebble either moves left or moves right by one place). If the number is odd then the state of the cell is 1, otherwise it is 0. This produces

$$\binom{t}{(c+t)/2} \bmod 2$$

whenever c and t have the same parity, and 0 otherwise.

By a famous theorem of Lucas one can determine if a binomial coefficient $\binom{a}{b}$ is odd by computing the binary expansions of a and b (pad b on the left by 0's): for every 1 in b there must be a corresponding 1 in a.

This can be used to derive part (D) in a purely algebraic fashion: **0** is reached before the boundary conditions make the binomial characterization useless (at least in its simple form).