1. Dihedral Recognizer (30)

Background

Consider the dihedral group D_4 with generators a and b where $a^2 = b^4 = 1$ and $ba = a^3 b$. The group has 8 elements and can be written as $\{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$. Here a corresponds to a rotation by 90 degrees, and b is the reflection along the horizontal axis.

If we think of a and b as symbols over the two-letter alphabet $\Sigma = \{a, b\}$, so that words over this alphabet naturally correspond to group elements. More precisely, there is an evaluation map $\eta : \Sigma^\star \to D_4$ which turns out to be a monoid homomorphism.

Task

A. Explain the group elements $\{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$ geometrically.

B. Show that η really is an epimorphism.

C. Construct a DFA that recognizes the kernel $K \subseteq \Sigma^\star$ of this homomorphism (all words that map to 1). Your machine should have 8 states.

D. Determine the cardinality of $K \cap \Sigma^n$.

2. Invertible Transducer (30)

Background

Recall the three word maps defined in class: $\alpha, \beta, \gamma : \mathbf{2}^\star \to \mathbf{2}^\star$ by $\alpha(\varepsilon) = \beta(\varepsilon) = \gamma(\varepsilon) = \varepsilon$ and

$$\begin{aligned}
\alpha(0x) &= 1\,\gamma(x) \\
\alpha(1x) &= 0\,\beta(x) \\
\beta(sx) &= s\,\alpha(x) \\
\gamma(sx) &= s\,\beta(x)
\end{aligned}$$

Concretely, here is the result of applying α repeatedly to 11000010.

1	1	0	0	0	0	1	0
0	1	1	0	0	1	1	0
1	1	1	1	0	1	0	0
0	1	0	1	1	1	0	1
1	1	0	0	1	0	0	0
0	1	1	0	1	1	0	0
1	1	1	1	1	1	1	0

Let S be the collection of all transductions $\mathbf{2}^\star \to \mathbf{2}^\star$ that can be obtained from the given three by composition. So S is a semigroup under composition (in other words, we consider arbitrary products of the three generators, but we will not allow the empty product, which would trivially produce the identity and we would have a monoid).

Task

A. Construct an alphabetic transducer that defines these three maps.

B. Explain why the maps α, β and γ are all injective.

C. Show that this semigroup is commutative.

D. Show that $\alpha\alpha\beta\beta\gamma = I$. Conclude that S is actually a group and in fact a homomorphic image of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

Comment

For part (A), one transducer is enough, you can just move the initial state around.

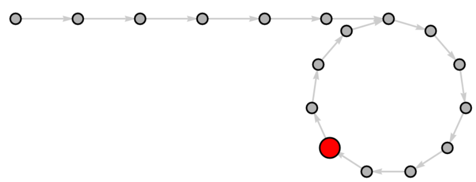
One can show that S is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, but that is rather difficult.

3. Floyd goes Algebraic (40)

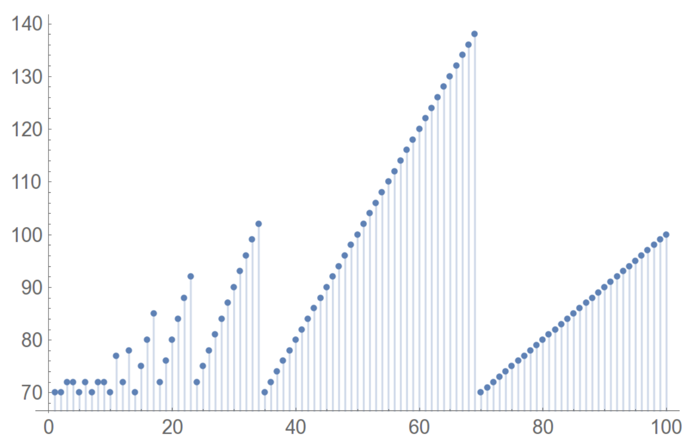
Background

One of the most elementary results about finite semigroups is that every element in the semigroup has an idempotent power. Recall that x is idempotent if $x^2 = x$. Then the claim is that for S any finite semigroup and $a \in S$, there exists some integer $r \geq 1$ such that a^r is idempotent.

Ignoring algebraic aspects for a moment, note that the powers of a (the points a^i, $i \geq 1$) must form a lasso since S is finite. Hence we can associate a with a transient $t = t(a) \geq 0$ and a period $p = p(a) \geq 1$.



We can think of the powers of a as the orbit of a under the map $x \mapsto ax$, so we can apply Floyd's trick to find a point on the loop (the big, red dot above). Let's call the time when the algorithm finds this point the Floyd time $\tau(t, p)$, an integer in the range 0 to $t + p - 1$. The next picture shows the Floyd times for $t = 70$ and $p = 1, \ldots, 100$.



Inquisitive minds will wonder if there is any connection between the Floyd time and the idempotent from above.

Here is an example: the function $a : [13] \to [13]$ defined by $a = [2, 3, 4, 5, 6, 7, 8, 8, 10, 9, 12, 13, 11]$ produces a lasso with transient and period both 6 and $a^{12} = [8, 8, 8, 8, 8, 8, 8, 8, 9, 10, 11, 12, 13]$ is the required idempotent.

Task

A. Prove the claim about idempotents in finite semigroups. Hint: think about the Floyd time.

B. Show that there is exactly one idempotent among the powers of a.

C. Give a simple description of the Floyd time $\tau(t, p)$ in terms of the transient t and period p.

D. Explain the plot of the Floyd times above.

E. Show that the powers of a that lie on the loop form a group with the idempotent as identity.