15-354: Computational Discrete Math K. Sutner

Solutions Assignment 7

Solution: Determinization of Büchi Automata

Part A: Regular Expression

In terms of counting letters the language can be described as

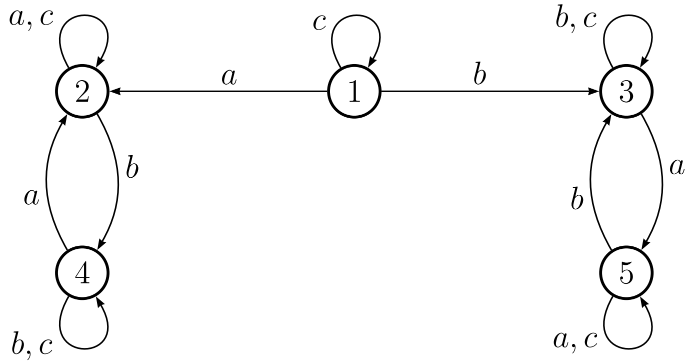
$$(\#_a \geq 1 \wedge \#_b < \infty) \vee (\#_b \geq 1 \wedge \#_a < \infty)$$

This translates into the following regular expression:

$$(a+b+c)^*(a(a+c)^\omega + b(b+c)^\omega)$$

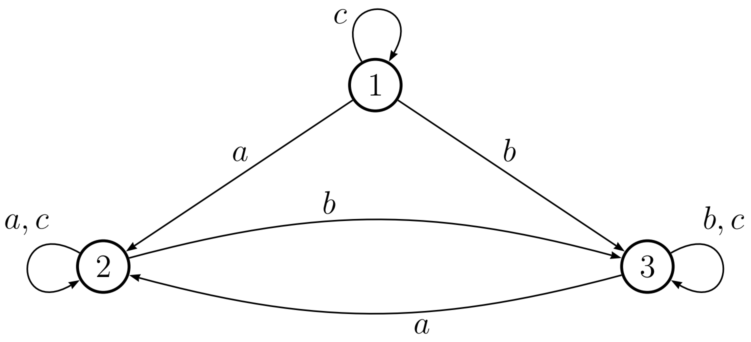
Part B: Safra

The Safra automaton has 5 states (using the version that updates state sets before branching; the other version produces 7 states):



The Rabin pairs are $(1,4,5;2,3)$ and $(1,2,3;4,5)$.

Note that there is a high degree of symmetry in this automaton. In fact, we can simplify the machine a bit by merging states in the component on the left with corresponding states in the component or the right.

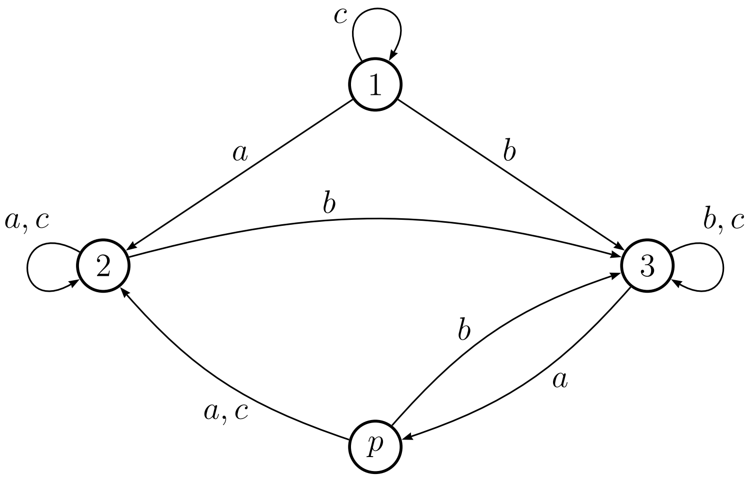


The new Rabin pairs are $(1, 2; 3)$ and $(1, 3; 2)$.

Part C: Complement Büchi

For complementation note that the Muller table for the machine from the last section is $\{2\}$, $\{3\}$. For the complement the table, after some cleanup based on the structure of strongly connected components of the machine, we get $\{1\}$, $\{2, 3\}$.

Unfortunately, this does not directly translate into a Büchi automaton. In the interesting case, we need to touch both 2 and 3 infinitely often. To enforce this via a Büchi acceptance condition we need to rewire the 2-point strongly connected component. Here is the modified automaton:



Note that the resulting Büchi automaton is still deterministic; the set of final states is $\{1, p\}$, corresponding to the two components that make up the complement of the language: $c^{\omega} \cup ((a + b + c)^{\star} a (a + b + c)^{\star} b)^{\omega}$ Or, in terms of counting:

$$(\#_a = 0 \wedge \#_b = 0) \vee (\#_a = \infty \wedge \#_b = \infty)$$

Solution: Floyd goes Algebraic

Part A: Idempotents

Consider the set of all powers $A = \{\, a^i \mid i \geq 0 \,\}$ Here we tacitly assume that the semigroup is actually a monoid and that $a^0 = 1$ is the identity element. If the semigroup has no identity we simply adjoin one.

We are looking for a power a^r, $r > 0$, of a with the property $a^{2r} = a^r$. But this is the same situation as in Floyd's cycle detection algorithm: one particle moves down the lasso at speed 2, the other at speed 1. When they meet we have the desired idempotent.

Part B: Exponents

We need to determine $r \geq 1$ minimal such that $a^{2r} = a^r$. Let $r = t + e$ where $t = t(a)$ and $0 \leq e < p = p(a)$. Floyd's algorithm finds the minimal e such that

$$(2e + t) \bmod p = e.$$

It is easy to see that the solution has the form

$$e = -t \bmod p$$

so that $r = t + (-t \bmod p)$. Note that we assume $0 \leq x \bmod p < p$; some implementations of the mod function may return negative values.

Part C: Plot

The periods p for which the Floyd time is equal to t clearly must be divisors of t. For $p \geq t$ we obtain the rightmost line with slope 1. The next line to the left has slope 2, and so forth.

Part D: Group

Let $G = \{\, a^{t+i} \mid 0 \leq i < p \,\}$ be the collection of powers of a that lie on the loop. Consider the map $f : \mathbb{Z}_p \to G$, $f(i) = a^{r+i}$. f is well-defined and bijective since p is the period of a.

We claim that f is a semigroup homomorphism. To see this compute

$$f(i+j) = a^{r+i+j} = a^r a^{i+j} = a^{2r} a^{i+j} = a^{2r+i+j} = a^{r+i} a^{r+j} = f(i)f(j).$$

So f is a semigroup isomorphism. Since $\mathbb{Z}_p$ is actually a group we're done.