Notes on Transducer Orbit Checking

Evan Bergeron

March 18, 2016

A Necassary Condition

Let f be the function produced by A_2^3. Let $y \in f^*(x)$. Let c be a sequence where c_i is the number of times x_i is flipped on the way to y. Then we claim that

$$\begin{aligned} c_i &= \lfloor (c_{i-3}/2) \rfloor + (c_{i-3} \mod 2) \cdot (1 - x_{i-3}) \\ &+ \lfloor (c_{i-2}/2) \rfloor + (c_{i-2} \mod 2) \cdot x_{i-2} \end{aligned}$$

where c_0 is the index of y in $f^*(x)$, c_1 is 0, and c_2 is $\lfloor c_0/2 \rfloor$.

x_0 is flipped upon every invocation of f. x_1 is never flipped. x_2 is flipped roughly every other time x_0 is flipped. That is, it's flipped every time x_0 changes from a 1 to a 0. Without loss, we may assume $x_0 = 0$. Thus, $c_2 = \lfloor c_0/2 \rfloor$ (it's not flipped the first time, but then is flipped every other time afterward).

Consider some application of f. c_i is flipped iff c_{i-2} is flipped from a 1 to a 0 or c_{i-3} is flipped from a 0 to a 1. If c_{i-2} and c_{i-3} are even, then this is precisely every other flip. If either c_{i-2} or c_{i-3} is odd, then c_i is dependent on both c_{i-2} and c_{i-3} as well as the initial conditions in x. We add one depending on whether or not the first flip of c_{i-2}, c_{i-3} causes c_i to flip as well.

A Sufficient Condition

Let p be a sequence where $p_i = c_i \mod 2$ for all i. Then if $x \oplus y$ looks like some p, then $y \in f^*(x)$. That is, if you fix your initial conditions and the above recurrence holds through $x \oplus y$, then $y \in f^*(x)$.

That being said, we necassarily don't know c_0.

A_2^3 Orbit Checking is in NP

Our verifier takes in two strings x, y, and an index i. This index is the position of y in x's orbit. WLOG, suppose $x_0 = 1$. We first set $c_0 = i$, $c_1 = 0$, and

$c_2 = \lfloor c_0/2 \rfloor$. We then calculate c_i and check that $c_i \mod 2 = x_i \oplus y_i$ for all i.

The certificate is poly length with respect to x and y, as the orbit of y has length at most 2^n (so the length of an index is at most n).

A Rephrasing of the Problem

In orbit iff there is a t such that $y = f^t(x)$. Suffices to find this t.

Derivatives

Notation incoming.

A_2^3 Orbit Checking is in P

The algo in question.

The A_2^3 Orbit Relation is Rational

This is hard - need to write that vector reduction thing.

A New Class of Transducers - 1-Toggle-1-Split

1-Tog-1-Split Orbit Checking in P?

1-Tog-1-Split Orbit Relation Rational?

1-Tog Orbit Relation Rational?

TODO: Automate making the orbit automaton?