Open Problem: Decidability of Divisibility in Automata

Jeffrey Shallit
School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@cs.uwaterloo.ca
http://www.cs.uwaterloo.ca/~shallit

The model

- $\Sigma_k = \{0, 1, \ldots, k-1\}$
- Numbers are represented in base k
- Numbers represented by words in Σ_k^*
- Canonical representation of n is $(n)_k$, without leading zeroes
- If $w \in \Sigma_k^*$ then $[w]_k$ is the integer represented by w
- E.g., 3526 is represented by the string 3526

Representing pairs

- Representations of pairs of integers are words over the alphabet $\Sigma_k \times \Sigma_k$
- For example, if $w = [3,0][5,0][2,4][6,1]$ then $[w]_{10} = $ `(3526,41)`.
- Canonical representations lack leading $[0,0]$'s

An open question

Question: Given an automaton M accepting the base-k representations of a set of pairs $S \subseteq \mathbb{N}^2$, is there a pair $(p, q) \in S$ such that $p \mid q$?

What's known

- Tarski: the first-order theory of $(\mathbb{N}, +, |)$ is undecidable. (Idea: use $|$ to implement multiplication.)
- Decidable: given an automaton M accepting the base-k representations of a set of pairs $S \subseteq \mathbb{N}^2$, does $p \mid q$ for all $(p, q) \in S$?
  - The condition $p \mid q$ for all $(p, q) \in S$ is very strong, and forces p to be in an easily describable set

A related question

- Suppose M is an automaton with n states and
- Suppose it accepts the base-k representations of a set $S \subseteq \mathbb{N} \times \mathbb{N}$ of pairs (p, q) such that $p \mid q$ for at least one pair
- How large can the smallest q be, in terms of n?
- A simple argument shows q can be doubly-exponential:
  - Choose a prime p such that 2 is a primitive root, modulo p and $S = (p, 2^n - 1)$ for $n \geq 1$. It is easy to build a DFA of $\log_2 p + O(1)$ states accepting $(S)_2$, but the smallest pair (p, q) where $p \mid q$ has $q = 2^{p-1} - 1$, and hence is doubly exponentially large in n.

Even worse examples

- Take $(p, q) = (2^j + s, 2^i + r)$ where $i \geq i_0$, $j \geq j_0$.
- Example: for $(r, s) = (55, 113)$ the smallest solution is $(i, j) = (685, 11)$.
- The least $i \geq 6$ such that there exists $j \geq 6$ with $2^j + 57 \mid 2^i + 55$ seems to be $i = 5230932780542371665$, $j = 70$.