A note on: A superpolynomial lower bound for the complementation problem of unambiguous fininte automata

Lorenzo Clemente,University of Warsaw, Poland

June 22, 2020

We build a UFA consisting of n disjoint simple cycles $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Cycle $\mathcal{C}_i$ has length m_i and is of the form $0 \to 1 \to \cdots \to (m_i - 1) \to 0$. In order to define the moduli m_i's, we need to construct a set P of small primes sufficiently close to each other.

Lemma 1. *For N large enough, there are N primes $P = \{p_1, \ldots, p_N\}$ s.t.*

1. *every prime p_i is at most $4N^2 \log N$, and*
2. *if $p_i > p_j$, then $\frac{p_i}{p_j} \leqslant 1 + \frac{1}{N}$.*

Let $b \in \mathbb{N}$ be a parameter and take $N = b^n$. The modulus $m_i = \prod P_i$ is the product of a subset P_i of P of cardinality $|P_i| = \frac{N}{b} = b^{n-1}$, defined as follows: The prime p_j is in P_i iff, by representing j in base b as $j = k_0 b^0 + \cdots + k_N b^N$, we have that the i-th digit $k_i \in \{0, \ldots, b-1\}$ is 0. Every two distinct moduli $m_i \neq m_j$ share $|P_i \cap P_j| = \frac{N}{b^2} = b^{n-2}$ common primes.

In order to ensure unambiguity, the languages of difference cycles must be disjoint. Ties are broken according to a *tournament* graph $G = (V, \to)$, with $V = \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$, that is, for every $i \neq j$, either $\mathcal{C}_i \to \mathcal{C}_j$ or $\mathcal{C}_j \to \mathcal{C}_i$, but not both. Accepting states of $\mathcal{C}_i$ are defined as follows: $r \in R_i \subseteq \{0, \ldots, m_i - 1\}$ iff 1) $r \neq 0$, 2) for every $p \in P_i$, either $r \equiv 0 \pmod p$ or $r \equiv i \pmod p$, and 3) for every j s.t. $\mathcal{C}_i \to \mathcal{C}_j$ there exists $q \in P_i \cap P_j$ s.t. $r \equiv i \pmod q$.

Lemma 2. *For every natural number $k \in \mathbb{N}$ there exists at most one i s.t. $k \mod m_i \in R_i$.*

Proof. Let $r := k \mod m_i \in R_i \cap R_j$. There exists $q \in P_i \cap P_j$ s.t. $r \equiv i \pmod q$. Since $q \mid m_j$, for every x, $r \equiv x \pmod{m_j}$ implies $r \equiv x \pmod q$, and thus neither $r \equiv 0 \pmod{m_j}$, nor $r \equiv j \pmod{m_j}$, and thus $r \notin R_j$. □

A set of vertices $U \subseteq V$ is an *inbound vertex cover* if for every other vertex $u \in V \backslash U$ there exists $v \in U$ s.t. $u \to v$. The *cover complexity* of G is the size of a minimal inbound vertex cover.

Lemma 3. *For every k there exists a tournament of cover complexity $\geqslant k$ of size $n = 3k^2 2^k$.*

Lemma 4. *Assume that the cover complexity of G is $\geqslant k$, and let $m \in \mathbb{N}$. If, for every l, i, $ml \mod m_i \notin R_i$, then m is divisible by at least $(1 - (1 - \frac{1}{b^2})^{\frac{k}{2}})N > 0.6N$ primes from P.*

Theorem 5. *For every d there exists a UFA $\mathcal{A}$ over a single letter alphabet s.t. every NFA recognising $\Sigma^* \setminus L(\mathcal{A})$ has size at least $|\mathcal{A}|^d$.*

Proof. Take $b = 2d$, the cover complexity to be $k = 2b^2$, and the number of disjoint cycles to be $n = 3k^2 2^k$. Recall that the number of primes is $N = b^n$. By Lemma 3, the cover complexity of G is $\geqslant k$. The size of $\mathcal{A}$ is $|\mathcal{A}| = O(n \cdot p_N^{\frac{N}{b}})$. TODO: p_N. Since $m = \prod P$ is not recognised by $\mathcal{A}$, $\mathcal{B}$ contains a cycle of length divisible by m. Moreover, for every $l \in \mathbb{N}$, also lm is not recognised by $\mathcal{A}$, which means that for every i, $lm \mod m_i \notin R_i$. By Lemma 4, m is divisible by at least $0.6N$ primes in P, and thus $\mathcal{B}$ has size at least $p_1^{0.6N}$. It is easy to check that $p_1^{0.6N} > |\mathcal{A}|^d$. □