Unary self-verifying symmetric difference automata

Laurette Marais, Lynette van Zijl

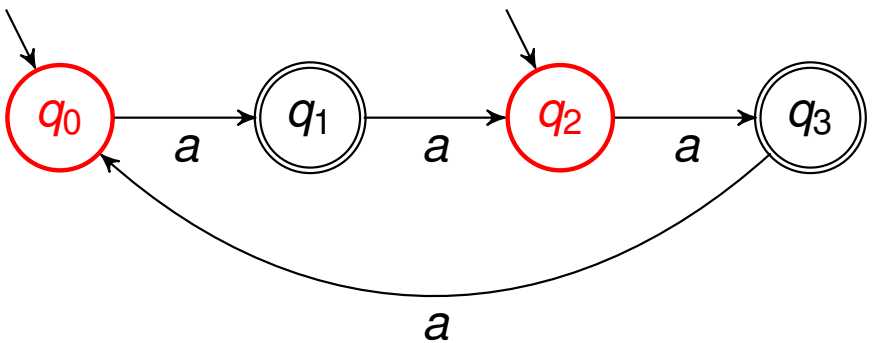
Computer Science
Stellenbosch University

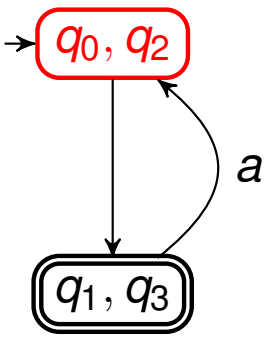
July 2016

Self-verifying NFA

Self-verifying NFA

- Final states are accepting or rejecting: $F = F^a \cup F^r$
- Rejection is different from failure to accept
- Every path with same label leads to same acceptance/rejection result

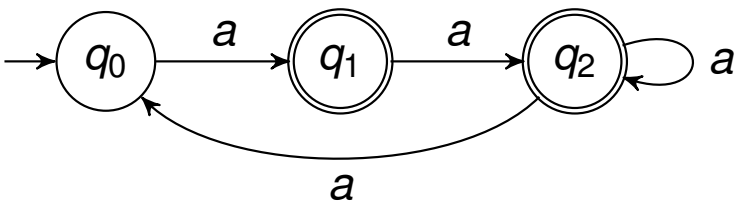


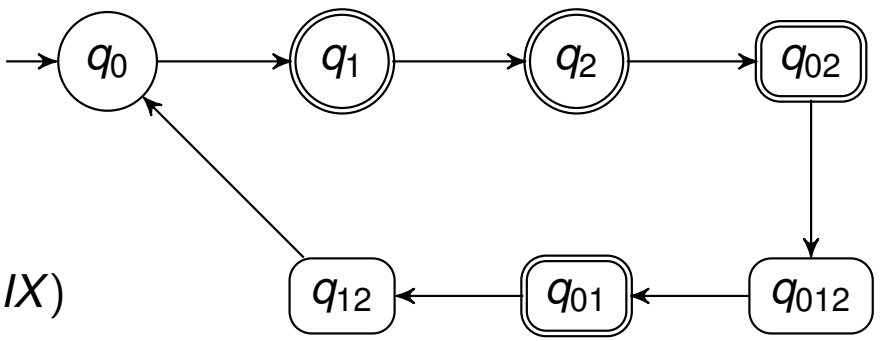


Symmetric difference NFA (XNFA)

Symmetric difference NFA (XNFA)

- Linear machine; LFSR; weighted automaton
- Parity machine: acceptance on an odd number of accept states





$$M = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$c(X) = \det(M - IX)$$

$$c(X) = X^3 + X^2 + 1$$

Self-verifying XNFA

Definition

A self-verifying symmetric difference finite automaton (SV-XNFA) is a 6-tuple $N = (Q, \Sigma, \delta, Q_0, F^a, F^r)$, where Q, Σ, δ and Q_0 are defined as for XNFA, and F^a and F^r are defined as for SV-XNFA. That is, each state in the SV-XDFA equivalent to N must contain an odd number of states from either F^a or F^r, but not both.

.

- Unary SV-XNFA
- Existence, descriptional complexity

Analysis

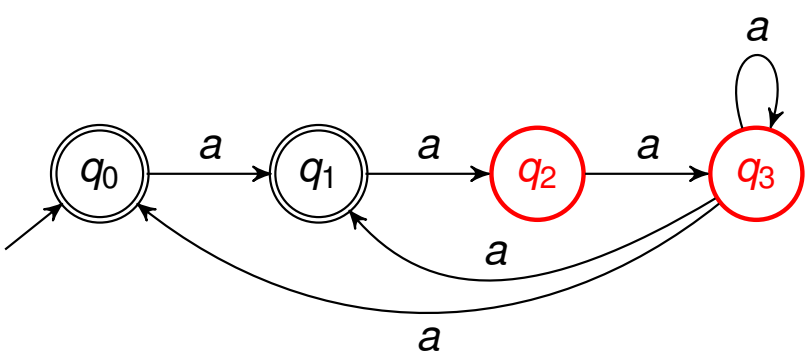
Analysis

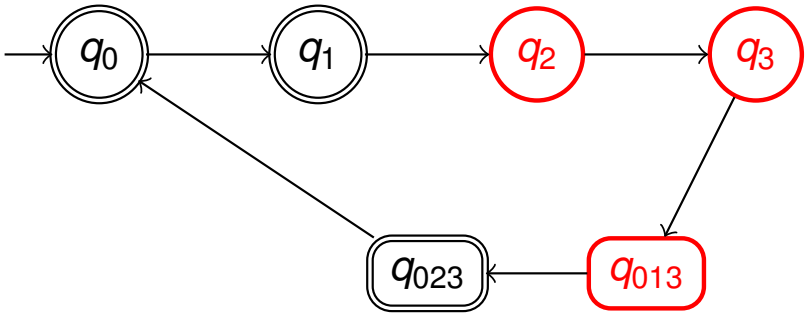
- Unary XNFA cycle structure – polynomial in Galois field GF(2)
- Are there polynomials that guarantee existence (or not) of non-trivial SV assignments?
- There is no n-state SV-XNFA such that its characteristic polynomial is primitive and irreducible
- Therefore, no n-state SV-XNFA such that equivalent DFA has $2^n - 1$ states

Analysis

Theorem

Let $c(X) = X^n + X^{n-1} + X + 1$, with companion matrix M, and let N be an XNFA with transition matrix M and $Q_0 = \{q_0\}$. Then N has an interesting SV-assignment, and the equivalent minimal DFA forms a cycle of length $2n - 2$.





Family of languages

Theorem

For any integer $n \geq 2$, let $\mathcal{L}_n = a^{(2n-2)i+j}$, for $i \geq 0$ and $0 \leq j < n-1$, and $\mathcal{L}_n^c = a^{(2n-2)i+j}$, for $i \geq 0$ and $n-1 \leq j < 2n-2$. Then there exists a pair of SV-XNFA with n states and the same transition graph that accept $\mathcal{L}_n$ and $\mathcal{L}_n^c$ respectively. Moreover, these languages each require an SV-XDFA with $2n-2$ states.

Descriptional complexity (unary)

Known

$2^n - 1$ upper bound, not tight

Our result

For any $n \geq 2$, there is an interesting SV-XNFA N whose equivalent minimal N_D has $2^{n-1} - 1$ states.

- $c(X) = (X + 1)\phi(X)$, with $\phi(X)$ primitive

Descriptional complexity (unary)

Lemma

Let $c(X) = (X+1)\phi(X)$ be a polynomial of degree n with non-singular companion matrix M, and let N be an XNFA with transition matrix M and $Q_0 = \{q_0\}$. Then the equivalent XDFA N_D has the following properties:

1. $[q_0], [q_1], \ldots, [q_{n-1}] \in Q_D$
2. $|Q_D| > n$
3. $|d|$ is odd for $d \in Q_D$

Descriptional complexity (unary)

Proof

- $X+1$ factor of $c(X)$ therefore 1 is root of $c(X)$
- $c(X) = X^n + \ldots + 1$ has even number of terms, and hence $\delta(q_{n-1}, a) = \{q_c | c \in C\} = Q_c$ where $|C|$ is odd.
- Let $P = \{q_{i_0}, q_{i_1}, ..., q_{i_k}\} \subseteq Q$ with $|P|$ odd. If $i_j < n-1$ for all $0 \leq j \leq k$, then $\delta(P, a) = \{q_{i_0+1}, q_{i_1+1}, ..., q_{i_k+1}\}$, and so $|\delta(P, a)|$ must be odd as well.
- But what if $q_{n-1} \in P$? Assume that $q_{n-1} = q_{i_k}$. Let $P' = \{q_{i_0+1}, q_{i_1+1}, ..., q_{i_k}\}$, so $|P'| = |P| - 1$ and therefore even. Then $\delta(P, a) = P' \oplus Q_c$. Let $m = |P' \cap Q_c|$. Then $|\delta(P, a)| = |P'| + |Q_c| - 2m$. Since $|P'|$ is even, $|Q_c|$ is odd and $2m$ is even, it follows that $|\delta(P, a)|$ is odd.

Descriptional complexity (unary)

Lemma

Let $c(X) = (X + 1)\phi(X)$ be a polynomial of degree n with non-singular companion matrix M. Then there is an XNFA N with transition matrix M and $Q = \{q_0\}$ for which there is an interesting SV-assignment.

Proof

Any choice of F^a and F^r so that $F^a \cup F^r = Q$ and $F^a \cap F^r = \emptyset$

Descriptional complexity (unary)

Lemma

Let $c(X) = (X + 1)\phi(X)$ be a polynomial of degree n with non-singular companion matrix M and where $\phi(X)$ is a primitive polynomial. Let N be an XNFA with transition matrix M and $Q_0 = \{q_0\}$, then N_D forms a cycle of length $2^{n-1} - 1$.

Descriptional complexity (unary)

Proof

Factors $X + 1$ and $\phi(X)$ each induce a single cycle of length $2^m - 1$ with $m = 1$ and $m = n - 1$ respectively. Hence, the possible cycle lengths are

$$\gcd(1, 2^{n-1} - 1) \text{ cycle(s) of length } \operatorname{lcm}(1, 2^{n-1} - 1)$$

Descriptional complexity (unary)

Theorem

For any $n \geq 2$, there is a language $\mathcal{L}_n$ so that some n-state SV-XNFA accepts $\mathcal{L}_n$ and the minimal SV-XDFA that accepts $\mathcal{L}_n$ has $2^{n-1} - 1$ states.

Descriptional complexity (unary)

Proof

- $F^a = \{q_0\}$ and $F^r = Q \setminus F^a$. Then $\mathcal{L} = a^{(2^{n-1}-1)i+j}$ for $i \geq 0$ and $j \in \{0, n\}$, since $q_0 \in \delta(q_0, a^n)$ and $q_0 \notin \delta(q_0, a^m)$ for $m < n$.
- If $\exists\ N'_D$ with $< 2^{n-1} - 1$ states, then there must be some $d_j \neq \{q_0\} \in Q_D$ such that $q_0 \in d_j$, $q_0 \in \delta(d_j, a^n)$ and there is no $m < n$ so that $q_0 \in \delta(d_j, a^m)$.
- Let d_k be any state in N_D such that $d_k \neq \{q_0\}$. Let $max(d_k)$ be the largest subscript of any SV-XNFA state in d_k. Then $max(d_k) > 0$. Let $m = n - max(d_k)$, so $m < n$, then $q_0 \in \delta(d_k, a^m)$. That is, for any d_k there is an $m < n$ so that $q_0 \in \delta(d_k, a^m)$.
- Thus no N'_D with $< 2^{n-1} - 1$ states that accepts $\mathcal{L}$.

Questions?