Unary Self-verifying Symmetric Difference Automata

Laurette Marais, Lynette Van Zijl

Unary Self-Verifying Symmetric Difference Automata

Laurette Marais[1,2] and Lynette van Zijl[1]

[1] Department of Computer Science, Stellenbosch University, South Africa
[2] Meraka Institute, CSIR, South Africa

Abstract. We investigate self-verifying nondeterministic finite automata, in the case of unary symmetric difference nondeterministic finite automata (SV-XNFA). We show that there is a family of languages $\mathcal{L}_{n\geq 2}$ which can always be represented non-trivially by unary SV-XNFA. We also consider the descriptional complexity of unary SV-XNFA, giving an upper and lower bound for state complexity.

1 Introduction

Any nondeterministic finite automaton (NFA) has an equivalent deterministic finite automaton (DFA) which can by found by applying the subset construction [1]. This subset construction uses the union set operation. Symmetric difference NFA (XNFA), on the other hand, employ the symmetric difference set operation [2] during the determinisation process with the subset construction. XNFA may also be considered as a special case of weighted automata over GF(2) [3]. XNFA, even in the unary case, are interesting because of the different descriptional complexity when compared to traditional NFA. For example, an n-state unary XNFA may have an equivalent minimal DFA with $2^n - 1$ states, whereas the bound is $e^{\Theta\sqrt{n\ \ln n}}$ in the case of NFA [2]. In this work, we consider self-verification for XNFA.

Self-verifying NFA (SV-NFA) [4–6] are automata with two kinds of final states, namely, accept states and reject states. Each path in the automaton may reach either an "Accept", "Reject" or "I do not know" state. Once a path has been found that either accepts or rejects, it is guaranteed that no other path with the same label will reach the opposite answer. Furthermore, every word is guaranteed one path that reaches either an accept or a reject state. Consequently, unlike with NFA, rejection is the result of reaching a reject state, and not the result of a failure to reach an accept state.

Assent and Seibert [4] showed that any n-state SV-NFA has an equivalent DFA with $O(2^n/\sqrt{n})$ states. Jirásková and Pighizzini [6] improved their result, and showed a tight upper bound $h(n)$, where $h(n)$ grows like $3^{\frac{n}{3}}$, for an SV-NFA with a binary alphabet. In the unary case, it was shown that the upper bound of $e^{\Theta\sqrt{n\ \ln n}}$ is not tight for unary SV-NFA.

In this article, we define self-verifying XNFA (SV-XNFA), and consider the case of unary SV-XNFA. We show the existence of a family of languages accepted

by unary SV-XNFA, and point out some conditions for the existence of n-state unary SV-XNFA. We also give an upper bound and lower bound for the state complexity.

2 Preliminaries

An NFA N is a five-tuple $N = (Q, \Sigma, \delta, Q_0, F)$, where Q is a finite set of states, Σ is a finite alphabet, $\delta : Q \times \Sigma \to 2^Q$ is a transition function (here, 2^Q indicates the power set of Q), $Q_0 \subseteq Q$ is a set of initial states, and $F \subseteq Q$ is the set of final (acceptance) states. The transition function δ can be extended to strings in the Kleene closure Σ^* of the alphabet:

$$\delta'(q, w_0 w_1 \dots w_k) = \delta(\delta(\dots \delta(q, w_0), w_1), \dots, w_k) \ .$$

For convenience, we write $\delta(q, w)$ to mean $\delta'(q, w)$.

An NFA N is said to accept a string $w \in \Sigma^*$ if $q_0 \in Q_0$ and $\delta(q_0, w) \in F$, and the set of all strings (also called words) accepted by N is the language $\mathcal{L}(N)$ accepted by N. Any NFA has an equivalent DFA which accepts the same language. The DFA equivalent to a given NFA can be found by the subset construction [1]. In essence, the subset construction keeps track of all the states that the NFA may be in at the same time, and forms the states of the equivalent DFA by grouping of the states of the DFA. In short,

$$\delta(A, \sigma) = \bigcup_{q \in A} \delta(q, \sigma)$$

for any $A \subseteq Q$ and $\sigma \in \Sigma$.

An XNFA $M = (Q, \Sigma, \delta, Q_0, F)$ is defined similarly to an NFA, with the difference that the XNFA accepts a string $w \in \Sigma^*$ if $q_0 \in Q_0$, and $|\delta(q_0, w) \cap F|$ is odd. This acceptance condition reflects the parity nature of the XNFA, so that a string is accepted when there is an odd number of paths which lead to final states [7]. This definition of acceptance ensures that an XNFA can be seen as a special case of a weighted automaton [3]. When the subset construction is applied to find the DFA equivalent to the XNFA, the symmetric difference (in the set theoretic sense) is used to reflect the parity of the paths. That is,

$$\delta(A, \sigma) = \bigoplus_{q \in A} \delta(q, \sigma)$$

for any $A \subseteq Q$ and $\sigma \in \Sigma$.

For clarity, the DFA equivalent to an XNFA N is termed an XDFA and denoted with N_D (with corresponding Q_D, δ_D etc).

It was shown (amongst others) in [2, 7] that XNFA can be investigated by considering them as linear machines over the Galois field GF(2). We also use that approach in this work. Consider the transition table of a unary XNFA $N = (Q, \Sigma, \delta, Q_0, F)$, where each row represents a mapping from a state $q \in Q$ to a set of states $P \in 2^Q$. Then P can be written as a vector with a one in

position i if $q_i \in P$, and a zero in position i if $q_i \notin P$. Hence, the transition table can be represented as a matrix of zeroes and ones (see Example 1). This is known as the characteristic or transition matrix of the XNFA.

Initial and final states can be represented by vectors, and appropriate vector and matrix multiplications over GF(2) represent the behaviour of the XNFA[3]. For more detail, see for example [3]. For the purposes of this work, we consider only unary XNFA with one alphabet symbol. In general, for larger alphabets, there is a matrix associated with each alphabet symbol.

Let M be the characteristic matrix of N. The characteristic polynomial $c(X)$ of M is given by $\det(M - IX)$, and $c(X)$ is said to be the characteristic polynomial of N.

Note that the characteristic matrix of an XNFA does not contain information about the choice of initial and final states, so in fact any such matrix represents a set of XNFA sharing a transition graph but differing in choice of initial and final states. A characteristic polynomial is associated with the matrix, but many matrices may share the same polynomial, so a polynomial over GF(2) represents a set of characteristic matrices. A useful result from linear field theory [8] states that any monic polynomial $c(X) = X^n + c^{n-1}X^{n-1} + \ldots c_2X^2 + c_1X + c_0$ over GF(2) has a so-called companion matrix (also called a normal form matrix) M of the form

$$M = \begin{bmatrix} 0 & 0 \ldots & 0 & c_0 \\ 1 & 0 \ldots & 0 & c_1 \\ 0 & 1 \ldots & 0 & c_2 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 \ldots & 1 & c_{n-1} \end{bmatrix} .$$

Thus, given a polynomial over GF(2), it is possible to construct its companion matrix directly, and then construct an XNFA from the companion matrix. Such an XNFA will have the transition function $\delta(q_i, a) = q_{i+1}$ for $0 \leq i < n-1$, and $q_j \in \delta(q_{n-1}, a)$ for all j such that $c_j \neq 0$.

Finally, each $c(X)$ over GF(2) is associated with a certain cycle structure. Specifically, given a unary XNFA N, the properties of its characteristic polynomial $c(X)$ allow conclusions about the possible length of the cycle of states of the equivalent XDFA N_D (see for example [2, 8, 9]).

Theorem 1. *[8] Let $c(X)$ be a polynomial of degree n over GF(2) that does not have X as a factor.*

- *If $c(X)$ is a primitive irreducible polynomial over GF(2), then $c(X)$ has a single cycle of length $2^n - 1$.*
- *If $c(X)$ is an irreducible but not primitive polynomial over GF(2), then $c(X)$ has $(2^n - 1)/b$ cycles of length b, where b is a factor of $2^n - 1$.*
- *If $c(X)$ is a reducible polynomial over GF(2), consider its factors. For each cycle of length k_i induced by factor $\phi_i(X)$ and for each cycle of length k_j induced by factor $\phi_j(X)$, $c(X)$ has $gcd(k_i, k_j)$ cycles of length $lcm(k_i, k_j)$.*

[3] In GF(2), $1 + 1 = 0$.

The choice of initial states for N determines which cycle in the cycle structure of $c(X)$ represents the equivalent XDFA N_D. We give an example of an XNFA to illustrate the discussion above.

Example 1. Let N be an XNFA where $Q = \{q_0, q_1, q_2, q_3\}$, $\Sigma = \{a\}$, $Q_0 = \{q_0\}$, $F = \{q_1, q_3\}$ and δ is defined in Table 1 (start states are indicated by $\rightarrow$, and final states by $\leftarrow$). This corresponds to the matrix M below and characteristic polynomial $c(X) = X^4 + X^3 + X + 1$.

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

Table 1. Transition function of N

	δ	a
$\rightarrow$	q_0	q_1
$\leftarrow$	q_1	q_2
	q_2	q_3
$\leftarrow$	q_3	q_0, q_1, q_3

Table 2. Transition function of N_D

	δ_D	a
$\rightarrow$	$[q_0]$	$[q_1]$
$\leftarrow$	$[q_1]$	$[q_2]$
	$[q_2]$	$[q_3]$
$\leftarrow$	$[q_3]$	$[q_0, q_1, q_3]$
	$[q_0, q_1, q_3]$	$[q_0, q_2, q_3]$
$\leftarrow$	$[q_0, q_2, q_3]$	$[q_0]$

The transition function δ_D of the equivalent XDFA N_D is shown in Table 2 and N_D is shown in Fig. 1. Note that $[q_0, q_1, q_3] \notin F_D$, since it contains an even number of states from F.

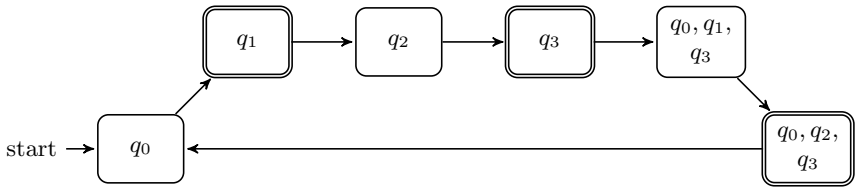

Fig. 1. Example 1: N_D

□

We now recap the definition of SV-NFA:

Definition 1. *[4, 6] A self-verifying nondeterministic finite automaton (SV-NFA) 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 standard NFA. Here, $F^a \subseteq Q$ and $F^r \subseteq Q$ are the sets of accept and*

reject states, respectively. The remaining states, that is, the states belonging to $Q \setminus (F^a \cup F^r)$*, are called neutral states. For each input string* w *in* Σ^**, it is required that there exists at least one path ending in either an accept or a reject state; that is,* $\delta(q_0, w) \cap (F^a \cup F^r) \neq \emptyset$ *for any* $q_0 \in Q_0$*, and there are no strings* w *such that both* $\delta(q_0, w) \cap F^a$ *and* $\delta(q_1, w) \cap F^r$ *for any* $q_0, q_1 \in Q_0$ *are nonempty.*

Unlike an NFA, an SV-NFA leads to an explicit answer state for any string $w \in \Sigma^*$. Hence, its equivalent DFA must do so too. The path for each w in a DFA is unique, so each state in the DFA is an accept or reject state. Hence, for any DFA state d, there is some SV-NFA state $q_r \in d$ such that $q_r \in F^a$ so that $d \in F^a_D$ or $q_r \in F^r$ so that $d \in F^r_D$. Since each state in the DFA is a subset of states of the SV-NFA, accept and reject states cannot occur together in a DFA state. That is, if d is a DFA state, then for any $p, q \in d$, if $p \in F^a$ then $q \notin F^r$ and vice versa.

Combining the notions of SV-NFA and XNFA, we now define SV-XNFA.

Definition 2. *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.*

Note that the acceptance condition for SV-XNFA (or the SV condition) implies that if a state in the SV-XDFA of an SV-XNFA N contains an odd number of states from F^a, it may also contain an even number of states from F^r, and so belongs to F^a_D, and vice versa. Parity is not applied to neutral states, so that any state in the XDFA may contain any number of neutral states from N.

The choice of F^a and F^r for a given SV-XNFA N is called an *SV-assignment* of N. An SV-assignment where either F^a or F^r is empty, is called a *trivial SV-assignment*. Otherwise, if both F^a and F^r are nonempty, the SV-assignment is non-trivial.

Definition 3. *Let* N *be an XNFA. A non-trivial SV-assignment for* N *such that* $\mathcal{L}(N) \neq \emptyset$ *and* $\mathcal{L}(N) \neq \Sigma^*$*, is called an interesting SV-assignment. An SV-XNFA with an interesting SV-assignment is called an interesting SV-XNFA.*

Example 2. Let N be an XNFA where $Q = \{q_0, q_1, q_2, q_3, q_4\}$, $\Sigma = \{a\}$, $Q_0 = \{q_0, q_1\}$ and δ is defined in Table 3.

The transition function δ_D of the equivalent XDFA is shown in Table 4. Then $F^a = \{q_2, q_4\}$ and $F^r = \{q_0\}$ is an interesting SV-assignment. The resulting SV-XDFA N_D is shown in Fig. 2. We see that $F^a_D = \{[q_1, q_2], [q_2, q_3], [q_3, q_4], [q_1, q_4]\}$, since these states each contain one state from F^a. Similarly, it holds that $F^r_D = \{[q_0, q_1], [q_0, q_1, q_2, q_4], [q_0, q_3]\}$, since each state contains q_0. Note that $[q_0, q_1, q_2, q_4]$ contains even number of states from F^a. □

We now investigate when interesting SV-assignments are possible for unary XNFA.

Table 3. Transition function of N

	δ	a
$_r\rightleftarrows$	q_0	q_1
$\rightarrow$	q_1	q_2
$_a\leftarrow$	q_2	q_3
	q_3	q_4
$_a\leftarrow$	q_4	q_0, q_1, q_2

Table 4. Transition function of N_D

	δ_D	a
$_r\rightleftarrows$	$[q_0, q_1]$	$[q_1, q_2]$
$_a\leftarrow$	$[q_1, q_2]$	$[q_2, q_3]$
$_a\leftarrow$	$[q_2, q_3]$	$[q_3, q_4]$
$_a\leftarrow$	$[q_3, q_4]$	$[q_0, q_1, q_2, q_4]$
$_r\leftarrow$	$[q_0, q_1, q_2, q_4]$	$[q_0, q_3]$
$_r\leftarrow$	$[q_0, q_3]$	$[q_1, q_4]$
$_a\leftarrow$	$[q_1, q_4]$	$[q_0, q_1]$

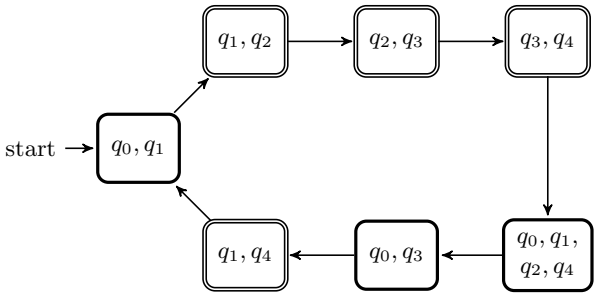

Fig. 2. Example 2: N_D

3 Unary SV-XNFA

Consider any unary XNFA N and its corresponding transition matrix M over GF(2). Then M can be either singular, or non-singular. If M is singular, it is known [8] that the XDFA N_D equivalent to N forms a state graph with a transient head followed by a cycle. If M is non-singular, then N_D forms a cycle. In the rest of this article, we only consider unary XNFA whose transition matrices are non-singular. By Lemma 1 below, this means we only consider polynomials over GF(2) that do not have X as a factor.

Noting the correspondence between a given XNFA, its matrix representation over GF(2), and the corresponding characteristic polynomial $c(X)$, we investigate whether there are properties of polynomials that guarantee the existence or non-existence of SV-assignments for XNFA with certain characteristic polynomials. We are specifically interested in finding properties that will guarantee the existence of SV-XNFA with n states that accept languages that require $n_D > n$ states in the equivalent SV-XDFA. This implies that we focus on interesting SV-assignments when determining the existence of SV-XNFA for certain polynomials.

Lemma 1. *The companion matrix of a polynomial over GF(2) is singular if and only if X is a factor of the polynomial.*

Proof. Let $c(X)$ be some polynomial over GF(2) of degree n. If and only if X is a factor of $c(X)$, then the coefficient of X^0 is zero, and so in the companion matrix, $M_{0,n-1} = 0$. Then $det(M) = 0$, which implies that M is singular [9].

□

Theorem 2. *There is no n-state SV-XNFA such that its characteristic polynomial is primitive and irreducible.*

Proof. Let $N = (Q, \Sigma, \delta, Q_0, F)$ be an n-state unary XNFA with characteristic polynomial $c(X)$. If $c(X)$ is primitive and irreducible, then the XDFA N_D forms a cycle of length $2^n - 1$. Each state in the cycle is a non-empty subset of Q. If there are $2^n - 1$ states, then every non-empty subset of Q is a state in the XDFA, including the state consisting of all the states in Q.

Since each $q \in Q$ appears as a state in the cycle, each q must either be an accept or reject state. There are two cases to consider. If n is even, then the state consisting of all the states in Q contains either an even number of accept states and an even number of reject states, or an odd number of accept states and an odd number of reject states. In either case the SV condition is violated, since each SV-XDFA state must contain an odd number of either F^a or F^r, but not both.

On the other hand, if n is odd, then – in order for the state consisting of all the states in Q to be either accepting or rejecting – some $A \subset Q$ where $|A|$ is odd must contain, say, the accepting states, while $Q \setminus A$ contains the rejecting states and $|Q \setminus A|$ is even. But the XDFA also contains a state consisting of $Q \setminus A$, that is a state consisting entirely of an even number of reject states. Hence if n is odd, this necessarily results in a neutral state in the XDFA, which again violates the SV condition. Therefore, no SV-XNFA is possible.

□

Note that Theorem 2 excludes all SV-assignments for primitive polynomials, including trivial or uninteresting SV-assignments. On the other hand, we now prove that for a certain family of polynomials, interesting SV-assignments are always possible.

Theorem 3. *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 XDFA N_D forms a cycle of length $2n - 2$.*

Proof. The transition function of N is given in Table 5. Since $\delta(q_i, a) = q_{i+1}$ for all $i < n - 1$, the XDFA N_D contains the states $[q_0], [q_1], ..., [q_{n-1}]$ in its cycle. Also, $\delta(q_{n-1}, a) = \{q_0, q_1, q_{n-1}\}$. Now, $\delta(\{q_0, q_i, q_{n-1}\}, a) = \{q_0, q_{i+1}, q_{n-1}\}$ for $1 \leq i \leq n - 3$, since $\delta(\{q_0, q_i, q_{n-1}\}, a) = \{q_1\} \oplus \{q_{i+1}\} \oplus \{q_0, q_1, q_{n-1}\} = \{q_0, q_{i+1}, q_{n-1}\}$, as $q_{i+1} \neq q_{n-1}$ for $1 \leq i \leq n-3$. However, $\delta(\{q_0, q_{n-2}, q_{n-1}\}, a) = \{q_1\} \oplus \{q_{n-2+1}\} \oplus \{q_0, q_1, q_{n-1}\} = \{q_0\}$. Therefore, N_D contains $[q_0], [q_1], ..., [q_{n-1}]$ and $[q_0, q_i, q_{n-1}]$ for $1 \leq i \leq n - 2$, and hence has $n + n - 2 = 2n - 2$ states.

Now, since every state in N_D has odd size, any choice of F^a and F^r so that $F^a \cup F^r = Q$ and $F^a \cap F^r = \emptyset$ with F^a and F^r non-empty will guarantee that

Table 5. Transition function of N with $c(X) = X^n + X^{n-1} + X + 1$

δ	a
q_0	q_1
q_1	q_2
$\vdots$	$\vdots$
q_{n-2}	q_{n-1}
q_{n-1}	q_0, q_1, q_{n-1}

each state in the XDFA contains an odd number of states from either F^a or F^r and zero or an even number of states from the other, and hence will be a non-trivial SV-assignment. Since $[q_0], [q_1], ..., [q_{n-1}] \in Q_D$, it will also necessarily be an interesting SV-assignment.

□

3.1 Languages for unary SV-XNFA

Given the existence of SV-XNFA for certain $c(X)$ as shown above, we may now consider whether there is a family of languages $\mathcal{L}_{n\geq 2}$ such that each $\mathcal{L}_i$ may be represented by an SV-XNFA in a non-trivial way. That is, we consider whether there are languages that may be represented by SV-XNFA with n states that require $n_D > n$ states in their equivalent SV-XDFA. The next theorem presents such a language family.

Theorem 4. *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.*

Proof. Using the construction given in the proof of Theorem 3, we construct N with n states so that N_D has $2n-2$ states. The states in the SV-XDFA are given in Figure 3.

Then $F^a = \{q_i | 0 \leq i \leq n-2\}$ and $F^r = \{q_{n-1}\}$ is an interesting SV-assignment. Consequently, $d_0, d_1, ..., d_{n-2} \in F_D^a$ and $d_{n-1}, d_n, ..., d_{2n-3} \in F_D^r$, so the language accepted by N is $\mathcal{L}_n = a^{(2n-2)i+j}$, for $i \geq 0$ and $0 \leq j < n-1$. Since this pattern of $n-1$ accept states followed by $n-1$ reject states requires $2n-2$ states, N_D is the minimal SV-XDFA that accepts $\mathcal{L}_n$.

Also, $F^r = \{q_i | 0 \leq i \leq n-2\}$ and $F^a = \{q_{n-1}\}$ is an interesting SV-assignment that would cause $d_0, d_1, ..., d_{n-2} \in F_D^r$ and $d_{n-1}, d_n, ..., d_{2n-3} \in F_D^a$ so that N accepts $\mathcal{L}_n^c = a^{(2n-2)i+j}$, for $i > 0$ and $n-1 \leq j < 2n-2$. Similarly as for $\mathcal{L}_n$, $2n-2$ states are required to accept $\mathcal{L}_n^c$.

This leads to a pair of SV-XNFA with n states and the same transition graphs that accept $\mathcal{L}_n$ and $\mathcal{L}_n^c$ respectively, while in the deterministic case, an SV-XDFA with at least $2n-2$ states is required.

$$
\begin{aligned}
d_0 &= [q_0] \\
d_1 &= [q_1] \\
&\vdots \\
d_{n-2} &= [q_{n-2}] \\
d_{n-1} &= [q_{n-1}] \\
d_n &= [q_0, q_1, q_{n-1}] \\
d_{n+1} &= [q_0, q_2, q_{n-1}] \\
&\vdots \\
d_{2n-3} &= [q_0, q_{n-2}, q_{n-1}]
\end{aligned}
$$

Fig. 3. Theorem 4: states in the SV-XDFA

□

The ability of self-verifying automata to represent complementary pairs of languages using the same transition graph is discussed in [10].

3.2 Descriptional complexity of unary SV-XNFA

We now turn to the question of state complexity for SV-XNFA. By Theorem 1, the maximum cycle length for any $c(X)$ of degree n is $2^n - 1$, and therefore this is an upper bound for the number of states in the equivalent XDFA of any XNFA with n states. However, it is not a tight upper bound for SV-XNFA, because this cycle length is only achieved if $c(X)$ is primitive and from Theorem 2 it is clear such XDFA cannot have SV-assignments. Instead, we show in this section that for certain $c(X)$ of degree n, there exist SV-XNFA with characteristic polynomial $c(X)$ for which the equivalent SV-XDFA have at least $2^{n-1} - 1$ states, and that for any $n \geq 2$, there is a language $\mathcal{L}_n$ that can be represented by an n-state SV-XNFA while requiring an $(2^{n-1} - 1)$-state SV-XDFA.

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

Proof. Since $X + 1$ is a factor, 1 is a root of the polynomial, and so $c(X)$ must have an even number of terms, including X^0. The companion matrix M of $c(X)$ is

$$M = \begin{bmatrix} 0\,0 & 0 & \cdots & 0\,0 & c_0 \\ 1\,0 & 0 & \cdots & 0\,0 & c_1 \\ 0\,1 & 0 & \cdots & 0\,0 & c_2 \\ \vdots & \ddots & & \vdots & \\ \vdots & & \ddots & \vdots & \\ 0\,0 & 0 & \cdots & 1\,0 & c_{n-2} \\ 0\,0 & 0 & \cdots & 0\,1 & c_{n-1} \end{bmatrix}.$$

The last column contains an odd number of 1's, representing an odd number of transitions from state q_{n-1}. That is, $\delta(q_{n-1}, a) = \{q_c | c \in C\} = Q_c$ where $|C|$ is odd.

Since $\delta(q_i, a) = q_{i+1}$ for all $i < n-1$, N_D contains the states $[q_0], [q_1], ..., [q_{n-1}]$, as well as $[Q_c]$, and therefore forms a cycle with at least $n+1$ states. These states all have odd size, so it only remains to show that all other states in the cycle must have odd size as well.

Let $P = \{q_{i_0}, q_{i_1}, ..., q_{i_k}\} \subseteq Q$ where k is even and so $|P|$ is odd. Then 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. However, suppose $q_{n-1} \in P$. We may 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.

Therefore, any state with odd size in N_D transitions to a state with odd size, and so all the states in the XDFA cycle have odd size.

□

Theorem 5. *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. From Lemma 2 it follows that the XNFA N whose transition matrix is the companion matrix of $c(X)$ has a cycle with length greater than n in which each state has odd size. Furthermore, $[q_0], [q_1], ..., [q_{n-1}]$ are all states in Q_D, so $q_0, q_1, ..., q_{n-1}$ must all be in either F^a or F^r.

Therefore, any choice of F^a and F^r so that $F^a \cup F^r = Q$ and $F^a \cap F^r = \emptyset$ with F^a and F^r non-empty will guarantee that each state in the XDFA contains an odd number of states from either F^a or F^r and zero or an even number of states from the other, and hence will be an interesting SV-assignment.

□

Lemma 3. *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 $2^{n-1} - 1$.*

Proof. We calculate the number and lengths of all cycles for $c(X)$. By Theorem 1, factors $X+1$ and $\phi(X)$ each induce a single cycle of length $2^m - 1$ with $m = 1$

and $m = n - 1$ respectively, as well as a single cycle each of length 1, which is the so-called empty cycle ε. Therefore $c(X)$ has the following cycles:

- ε_{X+1} and $X + 1$: $gcd(1, 1)$ cycle(s) of length $lcm(1, 1)$
- $\varepsilon_{\phi(X)}$ and $X + 1$: $gcd(1, 1)$ cycle(s) of length $lcm(1, 1)$
- ε_{X+1} and $\phi(X)$: $gcd(1, 2^{n-1} - 1)$ cycle(s) of length $lcm(1, 2^{n-1} - 1)$
- $\varepsilon_{\phi(X)}$ and $\phi(X)$: $gcd(1, 2^{n-1} - 1)$ cycle(s) of length $lcm(1, 2^{n-1} - 1)$

Therefore, $c(X)$ has two cycles of length 1, one of which is $\varepsilon_{c(X)}$, and two cycles of length $2^{n-1} - 1$. By Lemma 2, N_D must be a cycle with length greater than n, so it must have length $2^{n-1} - 1$.

□

Theorem 6. *For any $n \geq 2$, there is an interesting SV-XNFA N whose equivalent N_D has $2^{n-1} - 1$ states.*

Proof. Let $c(X) = (X + 1)\phi(X)$ be a polynomial of degree n, where $\phi(X)$ is a primitive polynomial, and let M be its non-singular companion matrix. Let N be an XNFA with transition matrix M and let $Q_0 = \{q_0\}$. By Theorem 5, N has an interesting SV-assignment, and by Lemma 3, the equivalent N_D has $2^{n-1} - 1$ states.

□

The following theorem shows that, for any $n \geq 2$, there exists an n-state SV-XNFA that accepts a language requiring at least $2^{n-1} - 1$ states in an equivalent SV-XDFA.

Theorem 7. *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.*

Proof. Let $c(X) = (X + 1)\phi(X)$ where $\phi(X)$ is a primitive polynomial and let $c(X)$ have degree n. We construct an SV-XNFA N with n states whose equivalent N_D has $2^{n-1} - 1$ states as in Theorem 6, and let $F^a = \{q_0\}$ and $F^r = Q \setminus F^a$. Then $\mathcal{L} = a^{(2^{n-1}-1)i+j}$ for $i \geq 0$ and $j \in J$, where J is some set of integers. Now, from the transition matrix of N it follows that $0, n \in J$, while $1, 2, ..., n - 1 \notin J$, since $q_0 \in \delta(q_0, a^n)$ and $q_0 \notin \delta(q_0, a^m)$ for $m < n$.

If there is an N'_D with fewer than $2^{n-1} - 1$ states that accepts $\mathcal{L}$, 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 from the transition matrix of N it follows that $q_0 \in \delta(d_k, a^m)$. That is, for any d_k there is an $m < n$ so that $q_0 \in \delta(d_k, a^m)$.

Therefore, there is no N'_D with fewer than $2^{n-1} - 1$ states that accepts $\mathcal{L}$.

□

This gives a lower bound of $2^{n-1} - 1$ for the state complexity of unary SV-XNFA.

4 Conclusion

We introduced the notion of unary self-verifying symmetric difference automata, and showed that for certain polynomials, interesting SV-XNFA exist. We also showed that for primitive polynomials, no SV-assignments for unary XNFA are possible. This provides an upper bound of $2^n - 1$ on the state complexity of unary SV-XNFA that is known not to be tight. Furthermore, we demonstrated that $2^{n-1} - 1$ is a lower bound for unary SV-XNFA.

Directions for future work include determining a tight bound, as well as providing a more detailed exposition of the properties of polynomials over GF(2) that lead to SV-assignments, and especially interesting SV-assignments. Also, further consideration may be given to the question of which languages can be represented succinctly by SV-XNFA.

References

1. Hopcroft, J.E., Ullman, J.D.: Introduction to automata theory, languages, and computation. 1st edn. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (1990)
2. Van Zijl, L.: Generalized nondeterminism and the succinct representation of regular languages. PhD thesis, University of Stellenbosch (1997) Available at `http://www.cs.sun.ac.za/~lvzijl/publications/boek.ps.gz`.
3. Van der Merwe, B., Tamm, H., Van Zijl, L.: Minimal DFA for symmetric difference NFA. In: Descriptional Complexity of Formal Systems: 14th International Workshop, DCFS 2012, Braga, Portugal, July 23-25, 2012. Proceedings. Springer Berlin Heidelberg, Berlin, Heidelberg (2012) 307–318
4. Assent, I., Seibert, S.: An upper bound for transforming self-verifying automata into deterministic ones. RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications **41**(3) (2007) 261–265
5. Hromkovič, J., Schnitger, G.: On the power of Las Vegas II. Two-way finite automata. In: Automata, Languages and Programming: 26th International Colloquium, ICALP'99 Prague, Czech Republic, July 11–15, 1999 Proceedings. Springer Berlin Heidelberg, Berlin, Heidelberg (1999) 433–442
6. Jirásková, G., Pighizzini, G.: Optimal simulation of self-verifying automata by deterministic automata. Information and Computation **209**(3) (2011) 528 – 535 Special Issue: 3rd International Conference on Language and Automata Theory and Applications (LATA 2009).
7. Vuillemin, J., Gama, N.: Compact normal form for regular languages as XOR automata. In: Implementation and Application of Automata: 14th International Conference, CIAA 2009, Sydney, Australia, July 14-17, 2009. Proceedings. Springer Berlin Heidelberg, Berlin, Heidelberg (2009) 24–33
8. Stone, H.S.: Discrete mathematical structures and their applications. Science Research Associates Chicago (1973)
9. Dornhoff, L.L., Hohn, F.E.: Applied modern algebra. Macmillan Publishing Co., Inc., Collier Macmillan Publishers (1978)
10. Geffert, V., Pighizzini, G.: Pairs of complementary unary languages with "balanced" nondeterministic automata. Algorithmica **63**(3) (2010) 571–587