Minimal DFA for Symmetric Difference NFA*

Brink van der Merwe[1], Hellis Tamm[2], and Lynette van Zijl[1]

[1] Department of Computer Science
Stellenbosch University, Private Bag X1, 7602 Matieland, South Africa
abvdm@cs.sun.ac.za,lvzijl@sun.ac.za
[2] Institute of Cybernetics, Tallinn University of Technology,
Akadeemia tee 21, 12618 Tallinn, Estonia
hellis@cs.ioc.ee

Abstract. Recently, a characterization of the class of nondeterministic finite automata (NFAs) for which determinization results in a minimal deterministic finite automaton (DFA), was given in [2]. We present a similar result for the case of symmetric difference NFAs. Also, we show that determinization of any minimal symmetric difference NFA produces a minimal DFA.

1 Introduction

Regular languages, and more specifically compact representations of regular languages, are important in many areas in computer science. The state minimization of deterministic finite automata (DFAs) is well-known [1, 8], but the state minimization of nondeterministic finite automata (NFAs) is more complicated [9, 10]. Symmetric difference NFAs ($\oplus$-NFAs) are of interest for their ability to succinctly describe regular languages [16].

In practical applications, it is often required to find the DFA equivalent to a given NFA (that is, to determinize the NFA). This is accomplished by the so-called subset construction, employing the union set operation for NFAs and the symmetric difference set operation for $\oplus$-NFAs. It is however quite possible that the equivalent DFA may have exponentially more states than the NFA or $\oplus$-NFA, and would need further minimization to reduce its number of states. It is therefore a notable advantage to be able to test in advance whether the determinization of a given NFA or $\oplus$-NFA would result in a minimal DFA. This issue was investigated by Brzozowski and Tamm [2] for the case of NFAs. They introduced so-called atoms of a regular language as non-empty intersections of uncomplemented or complemented left quotients of the language, and atomic NFAs in which the right language of every state is a union of atoms. It was shown in [2] that determinization of an NFA results in a minimal DFA if and only if the reverse of the given NFA is atomic.

* This research was supported by the National Research Foundation of South Africa, by the ERDF funded Estonian Center of Excellence in Computer Science, EXCS, by the Estonian Science Foundation grant 7520, and by the Estonian Ministry of Education and Research target-financed research theme no. 0140007s12.

In this work we show that the same characterization of when determinization leads to a minimal DFA, holds in the case of $\oplus$-NFAs. Also, we show that it is sufficient to require that a $\oplus$-NFA be minimal in order to obtain a minimal DFA by determinization.

The layout of the article is as follows. In Section 2 we define $\oplus$-NFAs and give some basic examples. Some properties of minimal $\oplus$-NFAs, that are used to obtain one of our main results, are given in Section 3. In Section 4, the notions of atomic and $\oplus$-atomic $\oplus$-NFAs are introduced. The main results, specifying conditions to obtain a minimal DFA on determinizing a $\oplus$-NFA, are presented in Section 5, followed by conclusions in Section 6.

2 Symmetric Difference NFA Definitions

$\oplus$-NFAs are typically defined by using the symmetric difference set operation, in contrast to the union set operation as in the case of NFAs. We give this definition, in order to be consistent with previous literature, but also equivalently consider $\oplus$-NFAs as weighted automata over the semiring $\mathbb{Z}_2$ (the Galois field with two elements).

We begin this section by recalling the definitions for a semiring and for weighted automata.

Definition 1. *(from [6], [7]) A tuple* $(S, \oplus, \otimes, \bar{0}, \bar{1})$ *is a* semiring *if* $(S, \oplus, \bar{0})$ *is a commutative monoid with identity element* $\bar{0}$*,* $(S, \otimes, \bar{1})$ *is a monoid with identity element* $\bar{1}$*,* $\otimes$ *distributes over* $\oplus$*, and* $\bar{0}$ *is an annihilator for* $\otimes$*: for all* $a \in S$*,* $a \otimes \bar{0} = \bar{0} \otimes a = \bar{0}$*.*

Example 1.

a) The *Boolean* semiring is the two element semiring over `true` (`true` being $\bar{1}$) and `false` (`false` being $\bar{0}$) using `and` as $\otimes$ and `or` as $\oplus$.
b) The *symmetric difference* semiring ($\mathbb{Z}_2$), is obtained by replacing `or` with `exclusive or` in the definition of the Boolean semiring.
c) The *tropical* semiring is the semiring $(\mathbb{N} \cup \{+\infty\}, min, +, +\infty, 0)$, also known as the min-plus semiring, with *min* and $+$ extended to $\mathbb{N} \cup \{+\infty\}$ in the natural way ($\mathbb{N}$ denotes the natural numbers, including 0).

Definition 2. *(from [6], [7]) A* weighted automaton *(without ε-transitions) over a semiring* $(S, \oplus, \otimes, \bar{0}, \bar{1})$ *is a 5-tuple* $\mathcal{A} = (Q, \Sigma, \delta, I, F)$*, where* Q *is a finite set of states,* Σ *is the finite input alphabet,* $\delta : \Sigma \to S^{Q \times Q}$ *the transition function,* $I : Q \to S$ *an initial weight function and* $F : Q \to S$ *the final weight function.*

Note that $\delta(a)$ is a $Q \times Q$-matrix whose (p, q)-*th* entry $\delta(a)_{p,q} \in S$ indicates the weight of the transition from p to q on the symbol a.

Let $\mathcal{A}$ be a weighted automaton over the semiring $(S, \oplus, \otimes, \bar{0}, \bar{1})$. A path in $\mathcal{A}$ is an alternating sequence $P = q_0 a_1 q_1 \ldots q_{n-1} a_n q_n \in Q(\Sigma Q)^*$. Its *run weight* is the product $rw(P) = I(q_0) \otimes \delta(a_1)_{q_0,q_1} \otimes \delta(a_2)_{q_1,q_2} \otimes \ldots \otimes \delta(a_n)_{q_{n-1},q_n} \otimes F(q_n)$.

The label of path $P = q_0a_1q_1 \dots q_{n-1}a_nq_n$, denoted by $label(P)$, is the word $a_1 \dots a_n \in \Sigma^*$. The *behaviour* of a weighted automaton $\mathcal{A}$ is the function $\|\mathcal{A}\| : \Sigma^* \to S$ defined by $\|\mathcal{A}\|(w) = \oplus_{label(P)=w} rw(P)$. One can easily verify that $\|\mathcal{A}\|(a_1 \dots a_n) = I\delta(a_1) \dots \delta(a_n)F^{\mathrm{T}}$, with usual matrix multiplication, considering I and F as row vectors and denoting by F^{T} the column vector obtained by transposing F.

Note that the Boolean semiring and $\mathbb{Z}_2$ are the only semirings with two elements. In the case of two element semirings, we can interpret weights as acceptance and rejection (words with weight 1 are accepted). Also, weighted automata over the Boolean semiring and over $\mathbb{Z}_2$ accept the same class of languages, namely, the regular languages.

$\oplus$-NFAs are in fact precisely weighted automata over $\mathbb{Z}_2$, but in order to stay consistent with previous work on the topic, we next give the standard definition for $\oplus$-NFAs.

Definition 3. *A $\oplus$-NFA $\mathcal{N}$ is a 5-tuple $(Q, \Sigma, \delta, I, F)$, where Q is the finite non-empty set of states, Σ is the finite non-empty input alphabet, $I \subseteq Q$ is the set of initial states, $F \subseteq Q$ is the set of final states and δ is the transition function such that $\delta : Q \times \Sigma \to 2^Q$.* □

The transition function δ can be extended to $\delta : 2^Q \times \Sigma \to 2^Q$ by defining

$$\delta(P, a) = \bigoplus_{q \in P} \delta(q, a)$$

for any $a \in \Sigma$ and $P \in 2^Q$. We define $\delta^* : 2^Q \times \Sigma^* \to 2^Q$ by $\delta^*(P, \epsilon) = P$ and $\delta^*(P, aw) = \delta^*(\delta(P, a), w)$ for any $a \in \Sigma$, $w \in \Sigma^*$ and $P \in 2^Q$. We will denote δ^* also by δ.

Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ be a $\oplus$-NFA and let w be a word in Σ^*. Then $\mathcal{N}$ *accepts* w if and only if $|F \cap \delta(I, w)| \bmod 2 \neq 0$. In other words, a $\oplus$-NFA accepts a word w by parity – if there is an odd number of accepting paths for w in the execution tree, then w is accepted; else it is rejected. Note that acceptance for $\oplus$-NFAs is in accordance with how acceptance is defined for weighted automata. The *language accepted* by $\mathcal{N}$, indicated by $L(\mathcal{N})$, is the set of all words accepted by $\mathcal{N}$. Given any two subsets of states $G, H \subseteq Q$ of $\mathcal{N}$, we define the *language from G to H* as the set of words $L_{G,H}(\mathcal{N}) = \{w \in \Sigma^* \mid |H \cap \delta(G, w)| \bmod 2 \neq 0\}$. If $G = \{q\}$, we will use the notation $L_{q,H}$, and similarly if H (or both G and H) consists of a single state. Then the *left language* of a state q of $\mathcal{N}$ is $L_{I,q}(\mathcal{N})$, and the *right language* of q is $L_{q,F}(\mathcal{N})$. Note that $L(\mathcal{N}) = L_{I,F}(\mathcal{N})$. Two $\oplus$-NFAs are *equivalent* if they accept the same language. A $\oplus$-NFA is *minimal* if it has the minimum number of states among all equivalent $\oplus$-NFAs.

By determinizing $\mathcal{N}$, we get a complete DFA $\mathcal{N}^{\mathbb{D}}$, which is defined as follows:

Definition 4. *Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ be a $\oplus$-NFA. Then the complete DFA $\mathcal{N}^{\mathbb{D}} = (Q^D, \Sigma, \delta^D, q_0, F^D)$, obtained by determinizing $\mathcal{N}$, is defined as follows:*

- $Q^D = \{\delta(I, w) \mid w \in \Sigma^*\}$;

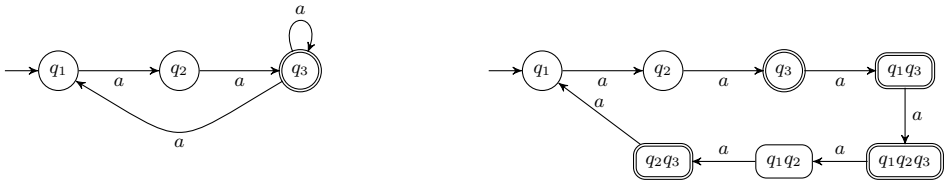

Fig. 1. The $\oplus$-NFA and corresponding DFA for Example 2.

- *for* $J \in Q^D \subseteq 2^Q$*, and* $a \in \Sigma$*,* $\delta^D(J, a) = \oplus_{q \in J} \delta(q, a)$*, with* $\delta^D(\emptyset, a) = \emptyset$ *for all* $a \in \Sigma$*, if* $\emptyset \in Q^D$*;*
- *the start state* q_0 *of* $\mathcal{N}^{\mathbb{D}}$ *is the set* I*;*
- *the set of final states* F^D *of* $\mathcal{N}^{\mathbb{D}}$ *is* $\{K \in Q^D \mid |K \cap F| \bmod 2 \neq 0\}$.

It was shown in [15] that $\mathcal{N}^{\mathbb{D}}$ is indeed equivalent to $\mathcal{N}$.

Example 2. Let $\mathcal{N} = (\{q_1, q_2, q_3\}, \{a\}, \delta, \{q_1\}, \{q_3\})$ be a $\oplus$-NFA where δ is given by $\delta(q_1) = \{q_2\}, \delta(q_2) = \{q_3\}$, and $\delta(q_3) = \{q_1, q_3\}$.

Figure 1 shows a graphical representation of $\mathcal{N}$; note that there is no visual difference from a traditional NFA. To find the DFA $\mathcal{N}^{\mathbb{D}}$ equivalent to $\mathcal{N}$, we apply the subset construction using the symmetric difference operation instead of union. The transition function $\delta^{\mathbb{D}}$ of $\mathcal{N}^{\mathbb{D}}$ is given by

$$\begin{array}{llll} \{q_1\} & \to^{\delta^{\mathbb{D}}} \{q_2\} & \to^{\delta^{\mathbb{D}}} \{q_3\} & \to^{\delta^{\mathbb{D}}} \{q_1, q_3\} \to^{\delta^{\mathbb{D}}} \\ \{q_1, q_2, q_3\} & \to^{\delta^{\mathbb{D}}} \{q_1, q_2\} & \to^{\delta^{\mathbb{D}}} \{q_2, q_3\} & \to^{\delta^{\mathbb{D}}} \{q_1\} \quad , \end{array}$$

and the final states by $\{\{q_3\}, \{q_1, q_3\}, \{q_1, q_2, q_3\}, \{q_2, q_3\}\}$.

As is the case for weighted automata in general, one can encode the transition table of a unary $\oplus$-NFA $\mathcal{N}$ as a binary matrix $m(\delta(a))$:

$$m(\delta(a))_{ij} = \begin{cases} 1 \text{ if } q_j \in \delta(q_i, a) \\ 0 \text{ otherwise,} \end{cases}$$

and successive matrix multiplications in the Galois field $\mathbb{Z}_2$ reflect the subset construction on $\mathcal{N}$.

We call $m(\delta(a))$ the *characteristic matrix* of $\mathcal{N}$, and $c(x) = \det(m(\delta(a)) - x\mathbf{I})$, where $\mathbf{I}$ is the identity matrix of the appropriate size, is known as its characteristic polynomial.

Similarly, we can encode any set of states $B \subseteq Q$ as an n-entry row vector $v(B)$ by defining

$$v(B)_i = \begin{cases} 1 \text{ if } q_i \in B \\ 0 \text{ otherwise .} \end{cases}$$

We place an arbitrary but fixed order on the elements of Q. We refer to $v(B)$ as the *vector encoding* of B, and to B as the *set encoding* of $v(B)$. Note that $v(B_1) + v(B_2) = v(B_1 \oplus B_2)$.

The matrix product $v(I)m(\delta(a))$ encodes the states reachable from the initial states after reading one letter, $v(I)m(\delta(a))^2$ encodes the states reachable after two letters, and in general $v(I)m(\delta(a))^k$ encodes the states reachable after k letters. Standard linear algebra shows the following:

$$\mathcal{N} \text{ accepts } a^k \text{ if and only if } v(I)m(\delta(a))^k v(F)^{\mathrm{T}} = 1,$$

where $v(F)^{\mathrm{T}}$ denotes the transpose of the row vector $v(F)$. In the general case where we consider also non-unary symmetric difference automata, one can associate a matrix $m(\delta(a))$ to each symbol $a \in \Sigma$. Then a word $w = a_1 \dots a_k$, with $a_i \in \Sigma$, is accepted if and only if:

$$v(I)m(\delta(a_1)) \dots m(\delta(a_k))v(F)^{\mathrm{T}} = 1.$$

Note that if $\mathcal{N}$ is an n-state $\oplus$-NFA with initial vector $v(I)$, final vector $v(F)$ and transition matrices $m(\delta(a))$, and A is a $n \times n$ non-singular matrix with inverse A^{-1}, then the $\oplus$-NFA $\mathcal{N}_A$ with initial vector $v(I)A$, final vector $A^{-1}v(F)$ and transition matrices $A^{-1}m(\delta(a))A$, accepts the same language as $\mathcal{N}$, since:

$$\begin{aligned} &v(I)m(\delta(a_1)) \dots m(\delta(a_k))v(F)^{\mathrm{T}} \\ =\, &v(I)AA^{-1}m(\delta(a_1))A \dots A^{-1}m(\delta(a_k))AA^{-1}v(F)^{\mathrm{T}}. \end{aligned}$$

It is shown in [17] that if $\mathcal{N}$ and $\mathcal{N}'$ are minimal $\oplus$-NFAs for the same language L, then we can find a non-singular matrix A such that $\mathcal{N}' = \mathcal{N}_A$. We will refer to the process of changing from $\mathcal{N}$ to $\mathcal{N}_A$ as making a change of basis by using A.

Definition 5. *The* mirror image *or* reverse *of a string $w = a_1 \dots a_n$ is the string $w^R = a_n \dots a_1$. The reverse L^R of a language L is defined to be $\{w^R \mid w \in L\}$.*

Given a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$, its *reverse* is $\mathcal{N}^{\mathbb{R}} = (Q, \Sigma, \delta^{\mathbb{R}}, F, I)$, where $q \in \delta^{\mathbb{R}}(p, a)$ if and only if $p \in \delta(q, a)$. In terms of vectors and matrices, the initial and final vectors are exchanged, and the transpose (that is, exchanging rows and columns) of the transition matrices of $\mathcal{N}$ is taken, in order to obtain the initial and final vectors and transition matrices of $\mathcal{N}^{\mathbb{R}}$. Note that

$$v(I)m(\delta(a_1)) \dots m(\delta(a_k))v(F)^{\mathrm{T}} = v(F)m(\delta(a_k))^{\mathrm{T}} \dots m(\delta(a_1))^{\mathrm{T}}v(I)^{\mathrm{T}} .$$

Thus $L(\mathcal{N}^{\mathbb{R}}) = (L(\mathcal{N}))^R$.

Example 3. Consider the $\oplus$-NFA $\mathcal{N}$ in Example 2. Its characteristic matrix is

$$m(\delta(a)) = \begin{bmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,1 \end{bmatrix}$$

and its characteristic polynomial is $c(x) = x^3 + x^2 + 1$. Interested readers may note that $c(x)$ is a primitive polynomial in $\mathbb{Z}_2$. The fact that $c(x)$ is primitive implies that we obtain $2^3 - 1 = 7$ states when determinizing the given $\oplus$-NFA

$\mathcal{N}$ (see [16]). It can be shown that $\mathcal{N}$ is minimal, and that $\mathcal{N}^{\mathbb{D}}$ is a minimal DFA ([16]), which is always the case when determinizing a minimal $\oplus$-NFA, as we will show later in Theorem 4. If we encode the start state as a row vector $v(I)$, with only the first component of $v(I)$ equal to one, and compute $v(I)m(\delta(a))^k$, we end up with the k-th entry in the on-the-fly subset construction on $\mathcal{N}$. For example, with the start state q_1 encoded as $v(I) = [\,1\ 0\ 0\,]$, we see that

$$m(\delta(a))^4 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

and hence $v(I)m(\delta(a))^4$ is given by $[\,1\ 1\ 1\,]$. This corresponds to the state $\{q_1, q_2, q_3\}$, which is reached after four applications of the subset construction on $\mathcal{N}$. Similarly, $v(I)m(\delta(a))^6$ is given by $[\,0\ 1\ 1\,]$, which corresponds to $\{q_2, q_3\}$.

In [15] we formally showed that the state behaviour of a unary $\oplus$-NFA is the same as that of a linear feedback shift register (LFSR). The similarity is intuitively straightforward, as an LFSR is a linear machine over $\mathbb{Z}_2$, and we can encode a unary $\oplus$-NFA as a linear machine over $\mathbb{Z}_2$ as shown above. This correspondence means that we can exploit the literature on LFSRs to analyse the behaviour of unary $\oplus$-NFAs, and in particular their cyclic behaviour (see, for example, [5] or [13]). For $\oplus$-NFAs in general (whether unary or non-unary), standard techniques in linear algebra are often used. For example, to obtain a more convenient form of transition matrices, a change of basis can be performed [14].

3 Properties of Minimal $\oplus$-NFAs

In this section we study properties of minimal $\oplus$-NFAs, which are used to obtain one of our main results that determinization of a minimal $\oplus$-NFA leads to a minimal DFA.

Proposition 1. *A $\oplus$-NFA $\mathcal{N}$ is minimal if and only if $\mathcal{N}^{\mathbb{R}}$ is minimal.*

Proof. Suppose $\mathcal{N}$ is a minimal $\oplus$-NFA. Then $\mathcal{N}^{\mathbb{R}}$ is obtained from $\mathcal{N}$ by interchanging the initial and the final states and by taking the transpose of the transition matrices for each letter in Σ. If $\mathcal{N}^{\mathbb{R}}$ is not minimal, we can rewrite its transition matrices with fewer rows and columns to obtain $\mathcal{N}'$, where $\mathcal{N}'$ accepts the same language as $\mathcal{N}^{\mathbb{R}}$. If we now reverse $\mathcal{N}'$ by transposing its transition matrices, we obtain a $\oplus$-NFA which accepts $(L(\mathcal{N}^{\mathbb{R}}))^R$, that is, $L(\mathcal{N})$. This is a contradiction, as $\mathcal{N}$ is minimal. The converse holds by the same argument. □

For a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$, the *kernel* of $\mathcal{N}$ is defined as the set of subsets $I' \subseteq Q$, such that if we obtain $\mathcal{N}'$ from $\mathcal{N}$ by replacing I with I', then $L(\mathcal{N}') = \emptyset$.

Definition 6. *The* kernel $K(\mathcal{N})$ *of a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ is the set* $\{I' \subseteq Q \mid L_{I',F}(\mathcal{N}) = \emptyset\}$.

Note that we always have $\emptyset \in K(\mathcal{N})$.

The *range* of a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ is defined as the linear subspace of 2^Q generated by subsets of the form $\delta(I, w)$.

Definition 7. *The* range $R(\mathcal{N})$ *of a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ is the set of subsets of Q of the form $\delta(I, w_1) \oplus \ldots \oplus \delta(I, w_k)$, with $w_1, \ldots, w_k \in \Sigma^*$, $k \geq 0$, where we assume that for $k = 0$ we obtain the empty set.*

A $\oplus$-NFA is trim if there are no states that are unreachable from start states. Instead of also removing states from which final states can not be reached, as in the case of trim (union) NFAs, we rather consider these as states that should be trimmed from $\mathcal{N}^{\mathbb{R}}$.

Definition 8. *A $\oplus$-NFA $\mathcal{N}$ is* trim *if $R(\mathcal{N}) = 2^Q$.*

Let $\mathcal{N}$ be the single state $\oplus$-NFA with no transitions, and with the single state not an initial or a final state. Then $\mathcal{N}$ is a minimal $\oplus$-NFA for $\emptyset$, but $R(\mathcal{N}) = \{\emptyset\}$. For the remainder of this paper, we either have to assume that the minimal $\oplus$-NFA for the empty language is the empty $\oplus$-NFA, or we should exclude the empty language from our discussions. To avoid technical complications, we thus do not consider the empty language in the remainder of this paper.

Next we show that $\oplus$-NFAs can be trimmed by making a change of basis.

Proposition 2. *Let $\mathcal{N}$ be a $\oplus$-NFA. Then there is a change of basis from $\mathcal{N}$ to $\mathcal{N}_A$, such that the $\oplus$-NFA obtained from $\mathcal{N}_A$ by removing all unreachable states from the initial states (in the usual graph theoretic sense), is trim.*

Proof. Assume that $\mathcal{N} = (Q, \Sigma, \delta, I, F)$. The proposition follows from the following standard fact from linear algebra. Let V be a k-dimensional linear subspace of the n-dimensional vector space $\mathbb{Z}_2^n$. Then there exists a $n \times n$ non-singular matrix A over $\mathbb{Z}_2$, such that $\{vA \mid v \in V\}$ is equal to $\{(v_1, \ldots, v_k, 0, \ldots, 0) \in (\mathbb{Z}_2)^n \mid v_i \in \mathbb{Z}_2\}$. Thus we can find a non-singular matrix A such that the vectors $v(I)m(\delta(a_1)) \ldots m(\delta(a_l))A$, for all $w = a_1 \ldots a_l \in \Sigma^*$, which is also equal to $v(I)AA^{-1}m(\delta(a_1)) \ldots AA^{-1}m(\delta(a_l))A$, generate (by using $\oplus$) precisely all 2^k vectors with all components from the $(k+1)$-th component onwards being zero. Thus by removing states $q_{k+1}, \ldots, q_n$ from $\mathcal{N}_A$, we obtain a trim $\oplus$-NFA. □

Proposition 3. *Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$. Then $K(\mathcal{N}) = \{\emptyset\}$ if and only if $R(\mathcal{N}^{\mathbb{R}}) = 2^Q$.*

Proof. Assume that $K(\mathcal{N}) \neq \{\emptyset\}$ and let $\emptyset \neq J \in K(\mathcal{N})$. Then from the definition of $K(\mathcal{N})$ we have that $L_{J,F}(\mathcal{N}) = \emptyset$, and thus $L_{F,J}(\mathcal{N}^{\mathbb{R}}) = \emptyset$. But note that $L_{F,J}(\mathcal{N}^{\mathbb{R}}) = \emptyset$ implies that $R(\mathcal{N}^{\mathbb{R}}) \neq 2^Q$. The converse can be proved in a similar way. □

Theorem 1. *Assume that the $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ is minimal. Then $K(\mathcal{N}) = \{\emptyset\}$, $K(\mathcal{N}^{\mathbb{R}}) = \{\emptyset\}$, $R(\mathcal{N}) = 2^Q$ and $R(\mathcal{N}^{\mathbb{R}}) = 2^Q$.*

Proof. Follows from Propositions 1, 2 and 3. □

Remark 1. It can be shown that if $K(\mathcal{N}) = \{\emptyset\}$ and $K(\mathcal{N}^{\mathbb{R}}) = \{\emptyset\}$ (or if $K(\mathcal{N}) = \{\emptyset\}$ and $R(\mathcal{N}) = 2^Q$), then $\mathcal{N}$ is minimal, but this result is not required in the remainder of this paper.

Definition 9. *Let L be a (regular) language. The* left quotient*, or simply* quotient*, of L by a word $w \in \Sigma^*$ is the language $w^{-1}L = \{x \in \Sigma^* \mid wx \in L\}$.*

Note that, if $\mathcal{D}$ is a minimal DFA accepting L, then the right language of every state of $\mathcal{D}$ is some quotient of L.

Similar to residual NFAs (as introduced in [4]), we define residual $\oplus$-NFAs. We will see in the next two sections of the paper that the more general class of automata, where the right languages of $\oplus$-NFAs are the symmetric difference of quotients, is in fact the more interesting class of $\oplus$-NFAs in our case.

Definition 10. *A* residual $\oplus$-NFA *($\oplus$-RFSA) is a $\oplus$-NFA $\mathcal{N} = (Q, \Sigma, \delta, I, F)$, such that for all $q \in Q$ there exists $w_q \in \Sigma^*$ with $L_{q,F}(\mathcal{N}) = w_q^{-1}L$.*

The $\oplus$-NFA given in Example 2 is a $\oplus$-RFSA, since by reading ε, a and aa, each of the three states are reached respectively.

Theorem 2. *For any regular language L, there exists a minimal $\oplus$-NFA $\mathcal{N}$, which is also a $\oplus$-RFSA, with $L(\mathcal{N}) = L$.*

Proof. Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ be a minimal $\oplus$-NFA accepting L, with $Q = \{q_1, \ldots, q_n\}$. Since $\mathcal{N}$ is minimal, it is implied by Theorem 1 that $R(\mathcal{N}) = 2^Q$. Thus we can find words $w_1, \ldots, w_n$ so that $\delta(I, w_1), \ldots, \delta(I, w_n)$ are linearly independent. We can now make a change of basis on $\mathcal{N}$ to obtain an equivalent minimal $\oplus$-NFA $\mathcal{N}' = (Q', \Sigma, \delta', I', F')$, with $Q' = \{q'_1, \ldots, q'_n\}$ and $\delta'(I', w_i) = \{q'_i\}$ for $1 \leq i \leq n$. In fact, it is fairly straightforward to verify that the matrix B, with $B = A^{-1}$, where A is a matrix with rows given by vectors $v(\delta(I, w_1)), \ldots, v(\delta(I, w_n))$, will provide the change of basis with the appropriate properties, since $v(\delta(I, w_i))B$, which is the vector of states in $\mathcal{N}'$ reached after reading w_i, is a vector with a 1 in the ith position and zeros in all other positions. Thus $\mathcal{N}'$ is residual. □

Example 4. In Figure 2(a) we give an example of a $\oplus$-NFA $\mathcal{N}$, with the states $Q = \{q_1, q_2, q_3, q_4, q_5\}$, and the initial states $I = \{q_1, q_5\}$. Note that $\mathcal{N}^{\mathbb{D}}$, given in Figure 2(b), is not minimal. Also, $K(\mathcal{N}) = \{\emptyset, \{q_2, q_4\}\}$, and $R(\mathcal{N})$ is the symmetric difference (or union) of any subset of the set $\{\{q_1, q_5\}, \{q_2\}, \{q_3\}, \{q_4\}\}$, and therefore properly contained in 2^Q. Thus, $\mathcal{N}$ is not minimal, and it is easy to see that $L(\mathcal{N})$ can be recognized by a three state minimal $\oplus$-NFA. If we use the 5×5 non-singular matrix $A = [a_{ij}]$ with $a_{ii} = 1$ for $i = 1, \ldots, 5$, $a_{15} = 1$, and $a_{ij} = 0$ at all other positions (i.e. A has ones on the diagonal and in the fifth column of the first row, but zeros elsewhere), then we obtain the $\oplus$-NFA $\mathcal{N}_A$ in Figure 2(c), which can be trimmed by removing state q_5.

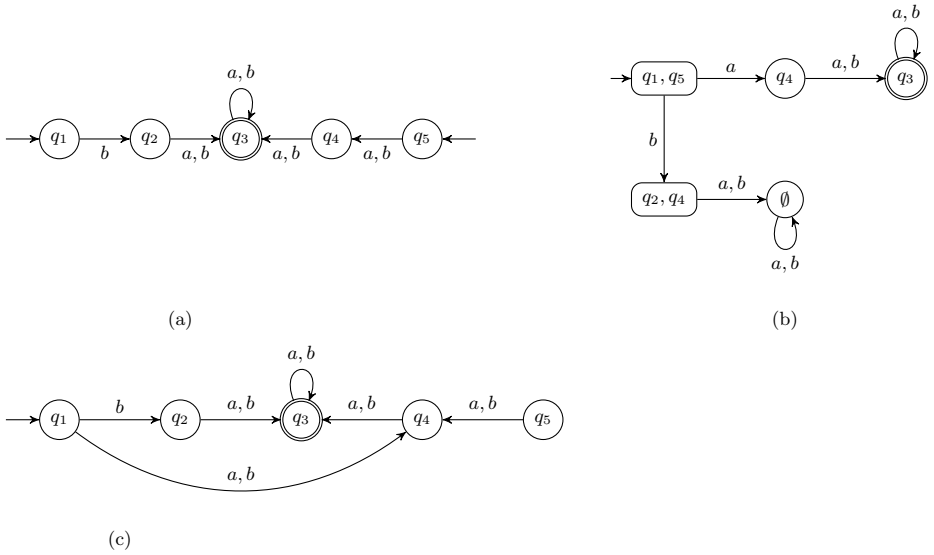

Fig. 2. (a) $\mathcal{N}$, (b) $\mathcal{N}^{\mathbb{D}}$, and (c) $\mathcal{N}_A$ for Example 4

4 Atomic and $\oplus$-Atomic $\oplus$-NFAs

Atoms of regular languages were recently introduced in [2].

Definition 11. *Let L be a regular language and let $L_1, \ldots, L_n$ be the quotients of L. An* atom *of L is any non-empty language of the form $\widetilde{L_1} \cap \cdots \cap \widetilde{L_n}$, where $\widetilde{L_i}$ is either L_i or $\overline{L_i}$, and $\overline{L_i}$ is the complement of L_i with respect to Σ^** [3].

A language has at most 2^n atoms. It is easy to see from the definition of an atom that any two atoms are disjoint from each other, and every quotient is a union of atoms.

Definition 12. *Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ be a $\oplus$-NFA. We say that $\mathcal{N}$ is* atomic *if for every state $q \in Q$, the right language $L_{q,F}(\mathcal{N})$ of q is a union of some atoms (or the empty set). Similarly, $\mathcal{N}$ is* $\oplus$-atomic *if for every state $q \in Q$, the right language $L_{q,F}(\mathcal{N})$ of q is a symmetric difference of some quotients of $L(\mathcal{N})$ (or the empty set).*

Example 5. In Figure 3, the minimal DFA $\mathcal{D}$ and a $\oplus$-NFA $\mathcal{N}$ accepting the language $L = (a+b)a^*$ are shown. The quotients of L are $L_1 = (a+b)a^*$, $L_2 = a^*$, $L_3 = \emptyset$. The atoms of L are $A_1 = L_1 \cap L_2 \cap \overline{L_3} = aa^*$, $A_2 = \overline{L_1} \cap L_2 \cap \overline{L_3} = \{\epsilon\}$, $A_3 = L_1 \cap \overline{L_2} \cap \overline{L_3} = ba^*$, $A_4 = \overline{L_1} \cap \overline{L_2} \cap \overline{L_3} = (a+b)^*(a+b)ba^*$. By

[3] The definition in [2] does not consider $\overline{L_1} \cap \overline{L_2} \cap \cdots \cap \overline{L_n}$ to be an atom. In [3], the definition of an atom was changed to read as presented here.

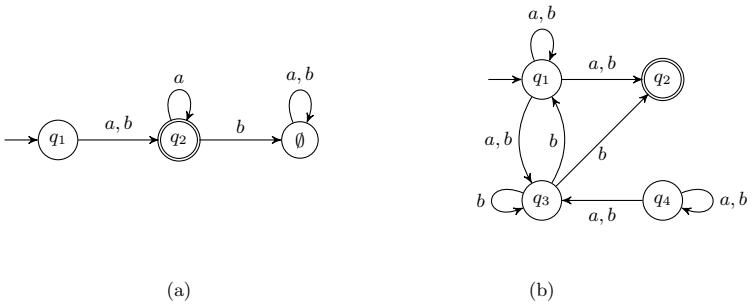

Fig. 3. (a) minimal DFA $\mathcal{D}$, (b) $\oplus$-NFA $\mathcal{N}$ for Example 5

determinization it can be verified that the right languages of the states of $\mathcal{N}$ are as follows: $A_1 \cup A_3$ for q_1 (note that $A_1 \cup A_3 = L_1$), A_2 for q_2, A_3 for q_3, and A_4 for q_4. Thus $\mathcal{N}$ is atomic, but not $\oplus$-atomic, since none of A_2, A_3 or A_4 can be expressed as a symmetric difference of any combination of quotients.

Proposition 4. *Let $\mathcal{N}$ be a $\oplus$-NFA. If $\mathcal{N}$ is $\oplus$-atomic, then $\mathcal{N}$ is also atomic.*

Proof. From the definition of an atom it follows that a quotient of a language L is a (disjoint) union of atoms of L. It thus follows that the symmetric difference of quotients is a union of atoms. Thus if a $\oplus$-NFA is $\oplus$-atomic, it is also atomic. □

Proposition 5. *A minimal $\oplus$-NFA is $\oplus$-atomic.*

Proof. From [17] we have that if $\mathcal{N}$ and $\mathcal{N}'$ are minimal $\oplus$-NFAs with $L(\mathcal{N}) = L(\mathcal{N}')$, then we can obtain $\mathcal{N}'$ from $\mathcal{N}$ by making a change of basis. Also, by Theorem 2, there exists a minimal $\oplus$-NFA $\mathcal{N}$ for any language L, that is also a $\oplus$-RFSA. The result now follows from the observation that if $\mathcal{N}_A$ is obtained from $\mathcal{N}$ by a change of basis by using the non-singular matrix A, then the right language of a state of $\mathcal{N}_A$ is the symmetric difference of the right languages of some of the states of $\mathcal{N}$. To see this, note that from the equation

$$\begin{aligned} &A^{-1}m(\delta(a_1))\dots m(\delta(a_k))v(F)^{\mathrm{T}} \\ =\,&A^{-1}m(\delta(a_1))A\dots A^{-1}m(\delta(a_k))AA^{-1}v(F)^{\mathrm{T}}, \end{aligned}$$

it follows that if we take the symmetric difference of the right languages of states of $\mathcal{N}$ corresponding to the positions of the ith row of A^{-1} having 1's, then we obtain the right language of the ith state of $\mathcal{N}_A$. □

5 Getting a Minimal DFA by Determinization

Let L be a regular language. Let the set of atoms of the reverse language L^R be $B = \{B_1, \dots, B_r\}$. The results in [2] and [3] imply the following proposition:

Proposition 6. *Let $\mathcal{D} = (Q, \Sigma, \delta, q_0, F)$ be the complete minimal DFA accepting L. Then there is a one-to-one correspondence between the sets Q and B, mapping a state $q \in Q$ to some atom B_i so that $L_{q_0,q}(\mathcal{D}) = B_i^R$ holds.*

Corollary 1. *Let $\mathcal{D} = (Q, \Sigma, \delta, q_0, F)$ be any DFA accepting L. Then for every state $q \in Q$ there is some $i \in \{1, \ldots, r\}$, such that $L_{q_0,q}(\mathcal{D}) \subseteq B_i^R$ holds.*

The following theorem is similar to the result obtained in [2] for (union) NFAs. Also, the proof we present here for $\oplus$-NFAs is essentially the same as it was for NFAs in [2].

Theorem 3. *For any $\oplus$-NFA $\mathcal{N}$, $\mathcal{N}^{\mathbb{D}}$ is minimal if and only if $\mathcal{N}^{\mathbb{R}}$ is atomic.*

Proof. Let $\mathcal{N} = (Q, \Sigma, \delta, I, F)$ be a $\oplus$-NFA and assume that $\mathcal{N}^{\mathbb{D}}$ is minimal, but suppose that $\mathcal{N}^{\mathbb{R}}$ is not atomic. Then there is a state q of $\mathcal{N}^{\mathbb{R}}$ that is not a union of atoms. That is, there is a word $u \in L_{q,I}(\mathcal{N}^{\mathbb{R}})$ such that $u \in B_i$ for some $i \in \{1, \ldots, r\}$, but for some other word $v \in B_i$, $v \notin L_{q,I}(\mathcal{N}^{\mathbb{R}})$. It is implied that $u^R \in L_{I,q}(\mathcal{N})$ and $v^R \notin L_{I,q}(\mathcal{N})$. Since we assumed that $\mathcal{N}^{\mathbb{D}}$ is a minimal DFA, by Proposition 6 there is a state s of $\mathcal{N}^{\mathbb{D}}$ such that $L_{I,s}(\mathcal{N}^{\mathbb{D}}) = B_i^R$. It is implied that $u^R, v^R \in L_{I,s}(\mathcal{N}^{\mathbb{D}})$. Since we had $u^R \in L_{I,q}(\mathcal{N})$, we get that $q \in s$. On the other hand, because $v^R \notin L_{I,q}(\mathcal{N})$ holds, we get $q \notin s$, a contradiction.

Conversely, assume that $\mathcal{N}^{\mathbb{R}}$ is atomic. Then for every state q of $\mathcal{N}^{\mathbb{R}}$, there is a set $H_q \subseteq \{1, \ldots, r\}$ such that $L_{q,I}(\mathcal{N}^{\mathbb{R}}) = \bigcup_{i \in H_q} B_i$. This implies $L_{I,q}(\mathcal{N}) = \bigcup_{i \in H_q} B_i^R$ for every state q of $\mathcal{N}$. Consider any state s of the DFA $\mathcal{N}^{\mathbb{D}}$. Then for any word u, $u \in L_{I,s}(\mathcal{N}^{\mathbb{D}})$ if and only if $u \in L_{I,q}(\mathcal{N})$ for every $q \in s$, and $u \notin L_{I,q'}(\mathcal{N})$ for any $q' \notin s$. That is, $L_{I,s}(\mathcal{N}^{\mathbb{D}}) = (\bigcap_{q \in s} \bigcup_{i \in H_q} B_i^R) \setminus (\bigcup_{q' \notin s} \bigcup_{i \in H_{q'}} B_i^R)$. On the other hand, by Corollary 1, $L_{I,s}(\mathcal{N}^{\mathbb{D}}) \subseteq B_k^R$ for some atom B_k. Since atoms are disjoint, any boolean combination of sets B_i^R cannot be a proper subset of any B_k^R. Thus, $L_{I,s}(\mathcal{N}^{\mathbb{D}}) = B_k^R$. If we suppose that $\mathcal{N}^{\mathbb{D}}$ is not minimal, then there are some states s' and s'' of $\mathcal{N}^{\mathbb{D}}$, and a state t of the corresponding minimal DFA, such that s', s'' and t have the same right language. Then it is easy to see by Proposition 6 that there is some B_i, such that $L_{I,s'}(\mathcal{N}^{\mathbb{D}}) \subset B_i^R$ and $L_{I,s''}(\mathcal{N}^{\mathbb{D}}) \subset B_i^R$, a contradiction. □

Theorem 4. *If $\mathcal{N}$ is a minimal $\oplus$-NFA, then $\mathcal{N}^{\mathbb{D}}$ is a minimal DFA.*

Proof. The result follows from Propositions 1, 4, 5 and Theorem 3. □

6 Conclusions and Future Work

In this paper and in [2] the problem of when determinization of a weighted automaton leads to minimal DFA was considered, for the case where the weights are taken from the Boolean semiring and from the semiring $\mathbb{Z}_2$. We would also like to consider this problem for weighted automata over other semirings, keeping in mind that determinization is not always possible for arbitrary weighted automata (see [11], [12]).

Acknowledgment We thank Jaco Geldenhuys for helpful discussions.

References

1. Brzozowski, J.: Canonical regular expressions and minimal state graphs for definite events. In: Proceedings of the Symposium on the Mathematical Theory of Automata. MRI Symposia Series, Polytechnic Press of Polytechnic Institute of Brooklyn (1963) 529–561
2. Brzozowski, J., Tamm, H.: Theory of átomata. In Mauri, G., Leporati, A., eds.: Proceedings of the 15th International Conference on Developments in Language Theory (DLT). Volume 6795 of Lecture Notes in Computer Science, Springer (2011) 105–117
3. Brzozowski, J., Tamm, H.: Quotient complexities of atoms of regular languages. In: Proceedings of the 16th International Conference on Developments in Language Theory (DLT). Lecture Notes in Computer Science, Springer (August 2012)
4. Denis, F., Lemay, A., Terlutte, A.: Residual finite state automata. In Ferreira, A., Reichel, H., eds.: STACS 2001, 18th Annual Symposium on Theoretical Aspects of Computer Science, Dresden, Germany, February 15-17, 2001, Proceedings. Volume 2010 of Lecture Notes in Computer Science, Springer (2001) 144–157
5. Dornhoff, L., Hohn, F.: Applied Modern Algebra. Macmillan Publishing Company (1978)
6. Droste, M., Kuich, W., Vogler, H.: Handbook of Weighted Automata. 1st edn. Springer Publishing Company, Incorporated (2009)
7. Droste, M., Rahonis, G.: Weighted automata and weighted logics on infinite words. In Ibarra, O.H., Dang, Z., eds.: Developments in Language Theory. Volume 4036 of Lecture Notes in Computer Science, Springer (2006) 49–58
8. Hopcroft, J., Ullman, J.: Introduction to Automata Theory, Languages and Computation. Addison Wesley (1979)
9. Ilie, L., Navarro, G., Yu, S.: On NFA reductions. Lecture Notes in Computer Science **3113** 112–124
10. Jiang, T., Ravikumar, B.: Minimal NFA problems are hard. SIAM Journal on Computing **22**(6) (December 1993) 1117–1141
11. Kirsten, D., Mäurer, I.: On the determinization of weighted automata. Journal of Automata, Languages and Combinatorics **10**(2/3) (2005) 287–312
12. Mohri, M.: Finite-state transducers in language and speech processing. Computational Linguistics **23**(2) (June 1997) 269–311
13. Stone, H.: Discrete Mathematical Structures. Science Research Associates (1973)
14. Van der Merwe, A., Van Zijl, L., Geldenhuys, J.: Ambiguity of unary symmetric difference NFAs. In: Proceedings of the International Colloquium on Theoretical Aspects of Computing. Volume 6916 of Lecture Notes in Computer Science, Springer (September 2011) 256–266
15. Van Zijl, L.: Generalized Nondeterminism and the Succinct Representation of Regular Languages. PhD thesis, Stellenbosch University (November 1997)
16. Van Zijl, L.: On binary symmetric difference NFAs and succinct representations of regular languages. Theoretical Computer Science **328**(1) (November 2004) 161–170
17. Vuillemin, J., Gama, N.: Compact normal form for regular languages as xor automata. In: Proceedings of the 14th International Conference on Implementation and Application of Automata. CIAA '09, Berlin, Heidelberg, Springer-Verlag (2009) 24–33