State complexity of the multiples of the Thue-Morse set

Émilie Charlier, Célia Cisternino, Adeline Massuir

March 9, 2019

Abstract

The Thue-Morse set is the set of those nonnegative integers whose binary expansions have an even number of 1. We obtain an exact formula for the state complexity of the multiplication by a constant of the Thue-Morse set $\mathcal{T}$ with respect with any base b which is a power of 2. Our proof is constructive and we are able to explicitely provide the minimal automaton of the language of all 2^p-expansions of the set of integers $m\mathcal{T}$ for any positive integers m and p.

1 Introduction

This papers is a contribution to the study of recognizable sets of integers. Many descriptions of such sets were given by various authors. Among them, we point [3, 5, 6]. A complete description of the minimal automaton recognizing $m\mathbb{N}$ in any given base b was given in [1]. Strucural properties of minimal automata recognizing $m\mathbb{N}$ are known in various non-standard numeration systems as well [4]. A deep knowledge of the structures of such automata is important. For example, they can be fruitfully used to obtain efficient decision procedures of periodicty problems [2, 8]. In the present work, we propose ourselves to initiate a study of the state complexity of the multiplication by a constant of recognizable subsets X of $\mathbb{N}$. In doing so, we aim at generalizing the previous framework concerning the case $X = \mathbb{N}$ only. Our study starts with the well-known Thue-Morse set $\mathcal{T}$ consisting of the natural numbers whose base 2-expansions contain an even number of occurrences of the digit 1. Our goal here is to provide a complete characterization of the minimal automata recognizing the sets $m\mathcal{T}$ for any multiple m and any base b which is a power of 2.

2 Basics

In this text, we use the usual definitions and notation (alphabet, letter, word, language, free monoid, automaton, etc.) of formal language theory; for example, see [7, 9].

Nevertheless, let us give a few definitions and properties that will be central in this work. The empty word is denoted by ε. For a finite word w, $|w|$ designates its length and $|w|_a$ the number of occurrences of the letter a in w. A *regular language* is a language which is accepted by a finite automaton. For $L \subseteq A^*$ and $w \in A^*$, the *(left) quotient* of L by w is the language

$$w^{-1}L = \{u \in A^* \colon wu \in L\}.$$

As is well known, a language L over an alphabet A is regular if and only if is has finitely many quotients, that is, the set of languages

$$\{w^{-1}L \colon w \in A^*\}$$

is finite. The *state complexity* of a regular language is the number of its quotients: $\mathrm{Card}(\{w^{-1}L\colon w \in A^*\})$. It corresponds to the number of states of its minimal automaton. The following characterization of minimal automata will be used several times in this work: a deterministic finite automaton (or DFA for short) is minimal if and only if it is complete, reduced and accessible. A DFA is said to be *complete* if the transition function is total (i.e. from every state start transitions labeled with all possible letters), *reduced* if languages accepted from distinct states are distinct and *accessible* if every state can be reached from the initial state. The language accepted from a state q is denoted by L_q. Thus, the language accepted by a DFA is the language accepted from its initial state (we always consider automata having a single initial state).

In what follows we will need a notion that is somewhat stronger than that of reduced DFAs. We say that a DFA has *disjoint states* if the languages accepted from distinct states are disjoint: for distinct states p and q, we have $L_p \cap L_q = \emptyset$. A state q is said to be *coaccessible* if $L_q \neq \emptyset$ and, by extension, an automaton is *coaccessible* if all its states are coaccessible. Thus, any coaccessible DFA having disjoint states is reduced.

Now, let us give some background on numeration systems. Let $b \in \mathbb{N}_{\geq 2}$. We define A_b to be the aphabet $\{\mathtt{0}, \ldots, \mathtt{b{-}1}\}$. Elements of A_b are called *digits*. The number b is called the *base* of the numeration. In what follows we will make no distinction between a digit $\mathtt{c}$ in A_b and its *value* c in $[\![0, b{-}1]\!]$. Otherwise stated, we identify the alphabet A_b and the interval of integers $[\![0, b{-}1]\!]$. Note that here and throughout the text, we use the notation $[\![m, n]\!]$ to designate the interval of integers $\{m, m{+}1, \ldots, n\}$. The *b-expansion* of a positive integer n, which is denoted by $\mathrm{rep}_b(n)$, is the finite word $c_{\ell-1} \cdots c_0$ over A_b defined by

$$n = \sum_{j=0}^{\ell-1} c_j b^j, \quad c_{\ell-1} \neq 0.$$

The *b-expansion* of 0 is the empty word: $\mathrm{rep}_b(0) = \varepsilon$. Conversely, for a word $w = c_{\ell-1} \cdots c_0$ over A_b, we write $\mathrm{val}_b(w) = \sum_{j=0}^{\ell-1} c_j b^j$. Thus we have $\mathrm{rep}_b\colon \mathbb{N} \to A_b^*$ and $\mathrm{val}_b\colon A_b^* \to \mathbb{N}$. Clearly, the function $\mathrm{val}_b \circ \mathrm{rep}_b$ is the identity from $\mathbb{N}$ to $\mathbb{N}$. Moreover, for any $w \in A_b^*$, the words $\mathrm{rep}_b(\mathrm{val}_b(w))$ and w only differ by the potential leading zeroes in w. Also note that for all subsets X of $\mathbb{N}$, we have $\mathrm{val}_b^{-1}(X) = 0^*\mathrm{rep}_b(X)$. A subset X of $\mathbb{N}$ is said to be *b-recognizable* if the language $\mathrm{rep}_b(X)$ is regular. In what follows, we will always consider automata accepting $\mathrm{val}_b^{-1}(X)$ instead of $\mathrm{rep}_b(X)$. The *state complexity* of a b-recognizable subset X of $\mathbb{N}$ *with respect to the base b* is the state compexity of the language $\mathrm{val}_b^{-1}(X)$.

We will need to represent not only natural numbers, but also pairs of natural numbers. If $u = u_1 \cdots u_n \in A^*$ and $v = v_1 \cdots v_n \in B^*$ are words of the same length n, then we use the notation (u, v) to designate the word $(u_1, v_1) \cdots (u_n, v_n)$ of length n over the alphabet $A \times B$:

$$(u, v) = (u_1, v_1) \cdots (u_n, v_n) \in (A \times B)^*.$$

For $(m, n) \in \mathbb{N}^2$, we write

$$\mathrm{rep}_b(m, n) = (0^{\ell - |\mathrm{rep}_b(m)|}\mathrm{rep}_b(m), 0^{\ell - |\mathrm{rep}_b(n)|}\mathrm{rep}_b(n))$$

where $\ell = \max\{|\mathrm{rep}_b(m)|, |\mathrm{rep}_b(n)|\}$. Otherwise stated, we add leading zeroes to the shortest expansion (if any) in order to obtain two words of the same length. Finally, for a subset X of $\mathbb{N}^2$, we write

$$\mathrm{val}_b^{-1}(X) = (0, 0)^*\mathrm{rep}_b(X).$$

3 Method

The Thue-Morse set, which we denote by $\mathcal{T}$, is the set of all natural numbers whose base-2 expansions contain an even number of occurrences of the digit 1:

$$\mathcal{T} = \{n \in \mathbb{N} \colon |\text{rep}_2(n)|_1 \in 2\mathbb{N}\}.$$

The Thue-Morse set $\mathcal{T}$ is 2-recognizable since the language $\text{val}_2^{-1}(\mathcal{T})$ is accepted by the automaton depicted in Figure 1. More precisely, the Thue-Morse set $\mathcal{T}$ is 2^p-recognizable

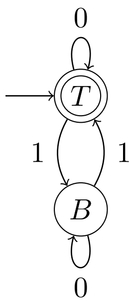

Figure 1: The Thue-Morse set is 2-recognizable.

for all $p \in \mathbb{N}_{\geq 1}$ and is not b-recognizable for any other base b. This is a consequence of the famous theorem of Cobham.

Two positive integers are said to be *multiplicatively independent* if their only common integer power is 1.

Theorem 1 ([5]).

- *Let b, b' be two multiplicatively independent bases. Then a subset of $\mathbb{N}$ is both b-recognizable and b'-recognizable if and only if it is a finite union of arithmetic progressions.*
- *Let b, b' be two multiplicatively dependent bases. Then a subset of $\mathbb{N}$ is b-recognizable if and only if it is b'-recognizable.*

In the case of the Thue-Morse set, it is easily seen that, for each $p \in \mathbb{N}_{\geq 1}$, the language $\text{val}_{2^p}^{-1}(\mathcal{T})$ is accepted by the DFA $(\{T, B\}, T, T, A_{2^p}, \delta)$ where for all $X \in \{T, B\}$ and all $a \in A_{2^p}$,

$$\delta(X, a) = \begin{cases} X & \text{if } a \in \mathcal{T} \\ \overline{X} & \text{else} \end{cases}$$

where $\overline{T} = B$ and $\overline{B} = T$. For example this automaton is depicted in Figure 2 for $p = 2$.

In order to avoid a systematic case separation, we introduce the following notation: for $X \in \{T, B\}$ and $n \in \mathbb{N}$, we define

$$X_n = \begin{cases} X & \text{if } n \in \mathcal{T} \\ \overline{X} & \text{else.} \end{cases}$$

With this notation, we can simply rewrite the definition of the transition function δ as $\delta(X, a) = X_a$.

The following proposition is well known; for example see [3].

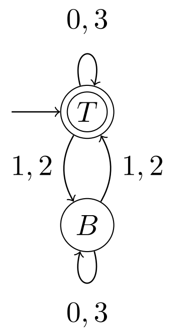

Figure 2: The Thue-Morse set is 4-recognizable.

Proposition 2. *Let $b \in \mathbb{N}_{\geq 2}$ and $m \in \mathbb{N}$. If X is b-recognizable, then so is mX. Otherwise stated, multiplication by a constant preserves b-recognizability.*

In particular, for any $m \in \mathbb{N}$ and $p \in \mathbb{N}_{\geq 1}$, the set $m\mathcal{T}$ is 2^p-recognizable. The aim of this work is to show the following result.

Theorem 3. *Let $m \in \mathbb{N}$ and $p \in \mathbb{N}_{\geq 1}$. Then the state complexity of $m\mathcal{T}$ with respect to the base 2^p is equal to*

$$2k + \left\lceil \frac{z}{p} \right\rceil$$

if $m = k2^z$ with k odd.

Our proof of Theorem 3 is constructive. In order to describe the minimal DFA of $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$, we will successively contruct several automata. First, we build a DFA $\mathcal{A}_{\mathcal{T},2^p}$ accepting the language

$$\mathrm{val}_{2^p}^{-1}(\mathcal{T} \times \mathbb{N}).$$

Then we build a DFA $\mathcal{A}_{m,b}$ accepting the language

$$\mathrm{val}_b^{-1}\big(\{(n, mn) \colon n \in \mathbb{N}\}\big).$$

Note that we do the latter step for any integer base b and not only for powers of 2. Next, we consider the product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. This DFA accepts the language

$$\mathrm{val}_{2^p}^{-1}\big(\{(t, mt) \colon t \in \mathcal{T}\}\big).$$

Finally, a finite automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ accepting $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$ is obtained by projecting the label of each transition in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ onto its second component. At each step of our construction, we check that the automaton under consideration is minimal (and hence deterministic) and the ultimate step precisely consists in a minimization procedure.

From now on, we fix $m \in \mathbb{N}$ and $p \in \mathbb{N}_{\geq 1}$. We also let z and k be the unique integers such that $m = k2^z$ with k odd.

4 The automaton $\mathcal{A}_{\mathcal{T},2^p}$

In this section, we build and study a DFA $\mathcal{A}_{\mathcal{T},2^p}$ accepting the language $\mathrm{val}_{2^p}^{-1}(\mathcal{T} \times \mathbb{N})$. This DFA is a modified version of the automaton accepting $\mathrm{val}_{2^p}^{-1}(\mathcal{T})$ defined in the previous section. Namely, we replace each transition labeled by $a \in A_{2^p}$ by 2^p copies of itself labeled by (a, b), for each $b \in A_{2^p}$. Formally,

$$\mathcal{A}_{\mathcal{T},2^p} = (\{T, B\}, T, T, A_{2^p} \times A_{2^p}, \delta_{\mathcal{T},2^p})$$

where, for all $X \in \{T, B\}$ and all $a, b \in A_{2^p}$, we have $\delta_{\mathcal{T},2^p}(X, (a, b)) = X_a$. For example, the automata $\mathcal{A}_{\mathcal{T},2}$ and $\mathcal{A}_{\mathcal{T},4}$ are depicted in Figure 3.

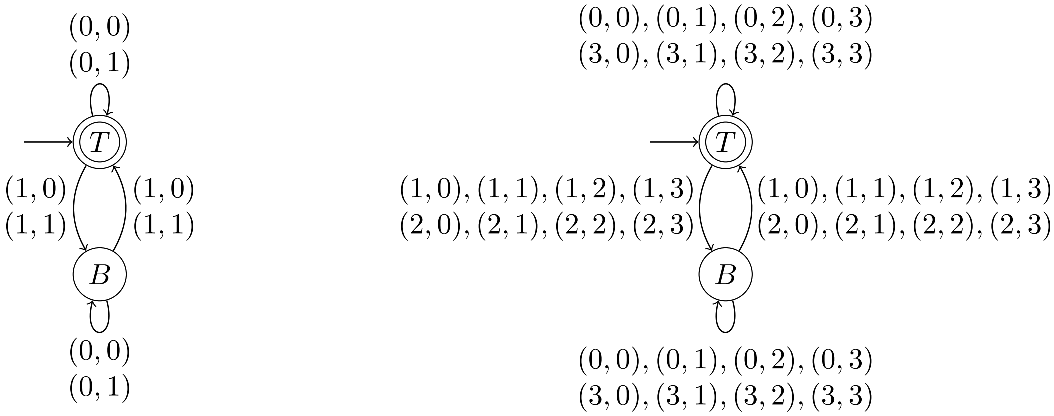

Figure 3: The automata $\mathcal{A}_{\mathcal{T},2}$ (left) and $\mathcal{A}_{\mathcal{T},4}$ (right).

Now we prove some properties of the automaton $\mathcal{A}_{\mathcal{T},2^p}$ that will be useful for our concerns.

Lemma 4. *The automaton $\mathcal{A}_{\mathcal{T},2^p}$ is complete, accessible, coaccessible and has disjoint states. In particular, it is the minimal automaton of* $\text{val}_{2^p}^{-1}(\mathcal{T} \times \mathbb{N})$.

Proof. These properties are all straightforward verifications. □

Lemma 5. *Let $u, v \in A_{2^p}^*$. Then* $\text{val}_{2^p}(uv) \in \mathcal{T}$ *if and only if, either* $\text{val}_{2^p}(u) \in \mathcal{T}$ *and* $\text{val}_{2^p}(v) \in \mathcal{T}$*, or* $\text{val}_{2^p}(u) \notin \mathcal{T}$ *and* $\text{val}_{2^p}(v) \notin \mathcal{T}$.

Proof. Let $\tau \colon A_{2^p}^* \to A_{2^p}^*$ be the p-uniform morphim defined by $\tau(a) = 0^{p-|\text{rep}_2(a)|}\text{rep}_2(a)$ for each $a \in A_{2^p}$. Then, for all $w \in A_{2^p}^*$, we have $\text{val}_{2^p}(w) = \text{val}_2(\tau(w))$. Therefore, $\text{val}_{2^p}(w) \in \mathcal{T}$ if and only if $|\tau(w)|_1 \in 2\mathbb{N}$. Since τ is a morphism, we have $|\tau(uv)|_1 = |\tau(u)|_1 + |\tau(v)|_1$. Hence $|\tau(uv)|_1$ is even if and only if $|\tau(u)|_1$ and $|\tau(v)|_1$ are both even or both odd. □

Lemma 6. *For all $X \in \{T, B\}$ and $(u, v) \in (A_{2^p} \times A_{2^p})^*$, we have*

$$\delta_{\mathcal{T},2^p}(X, (u, v)) = X_{\text{val}_{2^p}(u)}.$$

Proof. We do the proof by induction on $|(u, v)|$. The case $|(u, v)| = 0$ is trivial. The case $|(u, v)| = 1$ holds by definition of $\mathcal{A}_{\mathcal{T},2^p}$. Now let $X \in \{T, B\}$ and let $(ua, vb) \in (A_{2^p} \times A_{2^p})^*$ with $a, b \in A_{2^p}$. We suppose that the result is satisfied for (u, v) and we show that it is also true for (ua, vb). Let $Y = \delta_{\mathcal{T},2^p}(X, (u, v))$. By induction hypothesis, we have $Y = X_{\mathrm{val}_{2^p}(u)}$. Thus we obtain

$$\delta_{\mathcal{T},2^p}(X, (ua, vb)) = \delta_{\mathcal{T},2^p}(Y, (a, b)) = Y_a = (X_{\mathrm{val}_{2^p}(u)})_a = X_{\mathrm{val}_{2^p}(ua)}.$$

where we have used Lemma 5 for the last step. □

5 The automaton $\mathcal{A}_{m,b}$

In this section, we consider an arbitrary integer base b. Let

$$\mathcal{A}_{m,b} = ([\![0, m-1]\!], 0, 0, A_b \times A_b, \delta_{m,b})$$

where the (partial) transition function $\delta_{m,b}$ is defined as follows: for $i, j \in [\![0, m-1]\!]$ and $d, e \in A_b$, we set

$$\delta_{m,b}(i, (d, e)) = j \iff bi + e = md + j.$$

The DFA $\mathcal{A}_{m,b}$ accepts the language $\mathrm{val}_b^{-1}\big(\{(n, mn) : n \in \mathbb{N}\}\big)$. We refer the interested reader to [10]. For example, the automaton $\mathcal{A}_{6,4}$ is depicted in Figure 4.

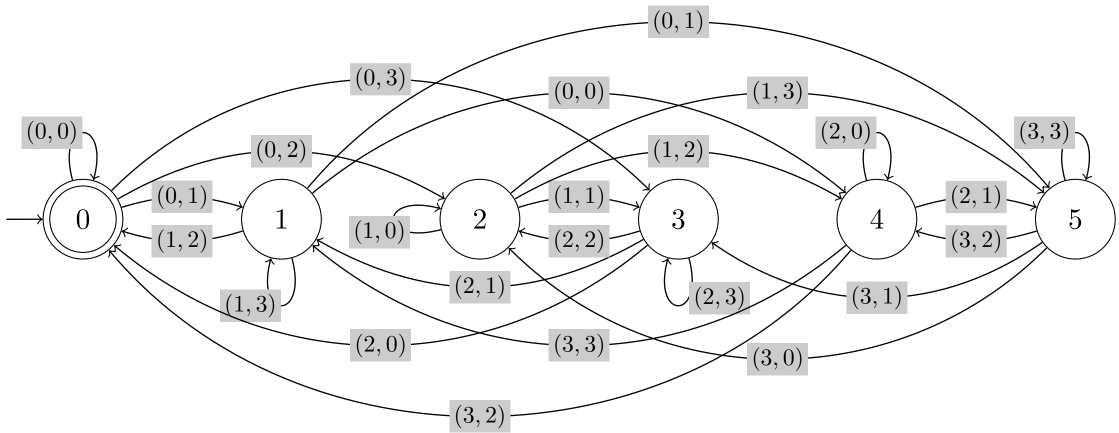

Figure 4: The automaton $\mathcal{A}_{6,4}$ accepts the language $\mathrm{val}_4^{-1}\big(\{(n, 6n) : n \in \mathbb{N}\}\big)$.

Note that the automaton $\mathcal{A}_{m,b}$ is not complete (see Remark 7). Also note that there is always a loop labeled by $(0, 0)$ on the initial state 0.

Remark 7. For each $i \in [\![0, m-1]\!]$ et $e \in A_b$, there exist unique $d \in A_b$ and $j \in [\![0, m-1]\!]$ such that $\delta_{m,b}(i, (d, e)) = j$. Indeed, d and j are unique since they are the quotient and remainder of the Euclidean division of $bi + e$ by m. We still have to check that $d < b$. We have

$$bi + e = md + j \iff d = \frac{bi + e - j}{m}.$$

Since $i \le m-1$, $j \ge 0$ and $e < b$, we have

$$\frac{bi+e-j}{m} \le \frac{b(m-1)+e}{m} = b - \frac{b-e}{m} < b.$$

Lemma 8. *For $i, j \in [\![0, m-1]\!]$ and $(u, v) \in (A_b \times A_b)^*$, we have*

$$\delta_{m,b}(i, (u, v)) = j \iff b^{|(u,v)|}\, i + \mathrm{val}_b(v) = m\, \mathrm{val}_b(u) + j.$$

Proof. We do the proof by induction on $n = |(u, v)|$. If n is equal to 0 or 1, the result is clear. Now let $i, j \in [\![0, m-1]\!]$ and let $(du, ev) \in (A_b \times A_b)^*$ with $d, e \in A_b$ and $|(u, v)| = n$. We suppose that the result is satisfied for (u, v) and we show that is also true for (du, ev). We use the notation $\mathrm{DIV}(x, y)$ and $\mathrm{MOD}(x, y)$ to designate the quotient and the remainder of the Euclidean division of x by y (thus, we have $\mathrm{DIV}(x, y) = \lfloor \frac{x}{y} \rfloor$). By definition of the transition function, we have

$$\delta_{m,b}(i, (du, ev)) = j \iff d = \mathrm{DIV}(bi + e, m) \ \text{ and } \ \delta_{m,b}(\mathrm{MOD}(bi + e, m), (u, v)) = j.$$

By using the induction hypothesis, we have

$$\begin{aligned} \delta_{m,b}(bi + e - md), (u, v)) = j &\iff b^n\,(bi + e - md) + \mathrm{val}_b(v) = m\, \mathrm{val}_b(u) + j \\ &\iff b^{n+1}\, i + \mathrm{val}_b(ev) = m\, \mathrm{val}_b(du) + j. \end{aligned}$$

To be able to conclude the proof, we still have to show that

$$b^{n+1}\, i + \mathrm{val}_b(ev) = m\, \mathrm{val}_b(du) + j \tag{1}$$

implies

$$d = \mathrm{DIV}(bi + e, m).$$

Thus, suppose that (1) is true. Then

$$b^{n+1}\, i + b^n e + \mathrm{val}_b(v) = m(b^n d + \mathrm{val}_b(u)) + j.$$

Since $\mathrm{val}_b(u)$ and $\mathrm{val}_b(v)$ are less than b^n, $d \ge 0$, $j < m$ and $b^n d + \mathrm{val}_b(u) \ge 0$, we obtain

$$\begin{aligned} d &= \mathrm{DIV}(b^n d + \mathrm{val}_b(u), b^n) \\ &= \mathrm{DIV}(\mathrm{DIV}(b^{n+1}\, i + b^n e + \mathrm{val}_b(v), m), b^n) \\ &= \mathrm{DIV}(\mathrm{DIV}(b^{n+1}\, i + b^n e + \mathrm{val}_b(v), b^n), m) \\ &= \mathrm{DIV}(b\, i + e, m) \end{aligned}$$

as desired. □

Remark 9. It is easily checked that Remark 7 extends from letters to words: for each $i \in [\![0, m-1]\!]$ and $v \in A_b^*$, there exist unique $u \in A_b^*$ and $j \in [\![0, m-1]\!]$ such that $\delta_{m,b}(i, (u, v)) = j$. In particular, the word u must have the same length as the word v, and hence $\mathrm{val}_b(u) < b^{|v|}$.

Let us describe a few properties of the automaton $\mathcal{A}_{m,b}$.

Proposition 10. *The automaton $\mathcal{A}_{m,b}$ is accessible, coaccessible and has disjoint states.*

Proof. For each $i \in [\![0, m-1]\!]$, we have $\delta_{m,b}(0, \mathrm{rep}_b(0, i)) = i$ from Lemma 8. Therefore $\mathcal{A}_{m,b}$ is accessible. It is a little trickier to find a word (u, v) that leads from i to 0. The reason is that there is a length constraint to respect: we must find words $u, v \in A_b^*$ of the same length n such that $b^n i + \mathrm{val}_b(v) = m \,\mathrm{val}_b(u)$. Equivalently, we have to find $n \in \mathbb{N}$ and $d, e \in [\![0, b^n - 1]\!]$ such that $b^n i + e = md$.

We claim that for all $n \in \mathbb{N}$ and $i \in [\![0, m-1]\!]$, there exists such d and e if and only if the following two inequalities hold

$$\left\lceil \frac{b^n i}{m} \right\rceil - \frac{b^n}{m} < \frac{b^n i}{m} \leq b^n - 1. \tag{2}$$

First, suppose that $d, e \in [\![0, b^n - 1]\!]$ are such that $b^n i + e = md$. Then $\frac{b^n i}{m} = d - \frac{e}{m} \leq d \leq b^n - 1$. Moreover $\frac{b^n i}{m} \leq d = \frac{b^n i + e}{m} < \frac{b^n (i+1)}{m}$. Since d is an integer, we get that $\lceil \frac{b^n i}{m} \rceil < \frac{b^n(i+1)}{m}$. Conversely, suppose that the two inequalities (2) hold. Let $d = \lceil \frac{b^n i}{m} \rceil$ and $e = md - b^n i$. It suffices to show that $d, e \in [\![0, b^n - 1]\!]$. Clearly $d, e \in \mathbb{N}$. From the inequality on the right, we get $d \leq b^n - 1$ and from that on the left, we get $e = md - b^n i < b^n(i+1) - b^n i = b^n$. This proves the claim.

For a given $i \in [\![0, m-1]\!]$, the inequalities (2) may not be satisfied for small n but it is easily checked that they are both satisfied for all n large enough. Therefore, the claim implies that $\mathcal{A}_{m,b}$ is coaccessible.

Finally, let $i, j \in [\![0, m-1]\!]$ and let $(u, v) \in L_i \cap L_j$. By Lemma 8, we have

$$b^{|(u,v)|} i + \mathrm{val}_b(v) = m \,\mathrm{val}_b(u) \quad \text{and} \quad b^{|(u,v)|} j + \mathrm{val}_b(v) = m \,\mathrm{val}_b(u),$$

which implies that $i = j$. We have thus obtained that $i \neq j \implies L_i \cap L_j = \emptyset$, i.e. that $\mathcal{A}_{m,b}$ has disjoint states. □

In a reduced DFA, there can be at most one non co-accessible state. Thus, we deduce from Proposition 10 that $\mathcal{A}_{m,b}$ is indeed the *trim minimal* automaton of the language $\mathrm{val}_b^{-1}(\{(n, mn) : n \in \mathbb{N}\})$, that is the automaton obtained by removing the only non co-accessible state from its minimal automaton.

6 The projected automaton $\Pi(\mathcal{A}_{m,b})$

In this section, we study the automaton obtained by projecting the label of each transition of $\mathcal{A}_{m,b}$ onto its second component. We denote by $\Pi(\mathcal{A}_{m,b})$ the automaton obtained thanks to this projection. For example, the automaton $\Pi(\mathcal{A}_{6,4})$ is depicted in Figure 5.

Remark 11. The automaton $\Pi(\mathcal{A}_{m,b})$ corresponds to the automaton that is commonly built for accepting the language $\mathrm{val}_b^{-1}(m\mathbb{N})$. For each $i, j \in [\![0, m-1]\!]$, there is a transition labeled by $e \in A_b$ from the state i to the state j if and only if $j = bi + e \bmod m$.

Corollary 12. *The automaton $\Pi(\mathcal{A}_{m,b})$ is complete, accessible and coaccessible.*

Proof. The accessibility and coaccessibility of the automaton $\Pi(\mathcal{A}_{m,b})$ are straightforward consequences of Proposition 10. The fact that it is complete comes from Remark 11: for every state $i \in [\![0, m-1]\!]$ and every digit $e \in A_b$, there is a transition labeled by e from i to the state $bi + e \bmod m$. □

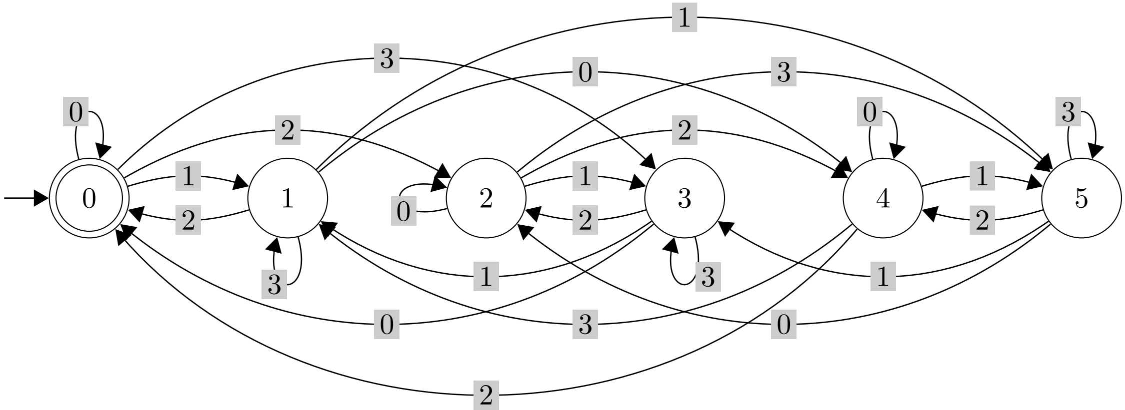

Figure 5: The projected automaton $\Pi(\mathcal{A}_{6,4})$.

The automaton $\Pi(\mathcal{A}_{m,b})$ is not minimal: it is minimal if and only if m and b are coprime; see for example [1]. In fact, whenever m and b are coprime, we have a stronger property than minimality as shown in the following proposition. This result will be useful in our future considerations.

Proposition 13. *If m and b are coprime, then the automaton $\Pi(\mathcal{A}_{m,b})$ has disjoint states, and hence it is the minimal automaton of $\mathrm{val}_b^{-1}(m\mathbb{N})$.*

Proof. Let $i, j \in [\![0, m-1]\!]$ and let $v \in A_b^*$ be a word accepted from both i and j in $\Pi(\mathcal{A}_{m,b})$. By Remark 9, there exist unique words u and u' of the same length as v such that (u, v) and (u', v) are accepted from i and j in $\mathcal{A}_{m,b}$ respectively. By Lemma 8, it is equivalent to say that

$$b^{|v|}i + \mathrm{val}_b(v) = m\,\mathrm{val}_b(u) \quad \text{and} \quad b^{|v|}j + \mathrm{val}_b(v) = m\,\mathrm{val}_b(u').$$

Thus, we have

$$b^{|v|}i - m\,\mathrm{val}_b(u) = b^{|v|}j - m\,\mathrm{val}_b(u'). \tag{3}$$

Therefore $m\,\mathrm{val}_b(u) \equiv m\,\mathrm{val}_b(u') \pmod{b^{|v|}}$. By using the hypothesis of coprimality of m and b, we obtain that $\mathrm{val}_b(u) \equiv \mathrm{val}_b(u') \pmod{b^{|v|}}$. Since $\mathrm{val}_b(u)$ and $\mathrm{val}_b(u')$ are both less than $b^{|v|}$, we obtain the equality $\mathrm{val}_b(u) = \mathrm{val}_b(u')$. Finally, we get from (3) that $i = j$, which proves that $\Pi(\mathcal{A}_{m,b})$ has disjoint states. □

To end this section, we prove some useful properties of the automaton $\Pi(\mathcal{A}_{m,b})$ under the more restrictive hypotheses of this work: $b = 2^p$ and $m = k2^z$ with k odd.

Lemma 14. *If $k > 1$ and $n = |\mathrm{rep}_{2^p}\big((k-1)2^z\big)|$, then $pn \geq z$.*

Proof. Then

$$n = \lfloor \log_{2^p}(k-1)2^z) \rfloor + 1 = \left\lfloor \log_{2^p}((k-1) + \frac{z}{p} \right\rfloor + 1 \geq \left\lfloor \frac{z}{p} \right\rfloor + 1 \geq \left\lceil \frac{z}{p} \right\rceil.$$

Thus $pn \geq p\lceil \frac{z}{p} \rceil \geq z$. □

For $k > 1$ and $n = |\mathrm{rep}_{2^p}\big((k{-}1)2^z\big)|$, we let σ be the permutation of the integers in $[\![0, k{-}1]\!]$ defined by $\sigma(j) = -j2^{pn-z} \bmod k$. Further, we define

$$w_j = 0^{n-|\mathrm{rep}_{2^p}(\sigma(j)2^z)|}\mathrm{rep}_{2^p}(\sigma(j)2^z)$$

for each $j \in [\![0, k{-}1]\!]$. Note that the words w_j are well defined since, by the choice of n, we have $\sigma(j)2^z \leq (k{-}1)2^z < b^n$ for every $j \in [\![0, k{-}1]\!]$.

Proposition 15. *Suppose that $k > 1$ and let $j, j' \in [\![0, k{-}1]\!]$. Then the word w_j is accepted from j' in the automaton $\Pi(\mathcal{A}_{m,2^p})$ if and only if $j = j'$.*

Proof. Let $n = |\mathrm{rep}_{2^p}\big((k{-}1)2^z\big)|$. Then $|w_j| = n$ for all $j \in [\![0, k{-}1]\!]$ and from Lemma 14, we know that $pn \geq z$. the result follows from the following computations:

$$\begin{aligned}
j'2^{p|w_j|} + \mathrm{val}_b(w_j) \equiv 0 \pmod{m} &\iff j'2^{pn} + \sigma(j)2^z \equiv 0 \pmod{k2^z}\\
&\iff j'2^{pn-z} + \sigma(j) \equiv 0 \pmod{k}\\
&\iff j'2^{pn-z} - j2^{pn-z} \equiv \quad \pmod{k}\\
&\iff j \equiv j' \pmod{k}\\
&\iff j = j'.
\end{aligned}$$

□

Proposition 16. *Suppose that $k > 1$ and let $j, j' \in [\![0, k{-}1]\!]$. Then the word $w_j\mathrm{rep}_{2^p}(m)$ is accepted from j' in the automaton $\Pi(\mathcal{A}_{m,2^p})$ if and only if $j = j'$.*

Proof. Let $n = |\mathrm{rep}_{2^p}\big((k{-}1)2^z\big)|$, let $L = |\mathrm{rep}_{2^p}(m)|$ and, for each $j \in [\![0, k{-}1]\!]$, let $x_j = w_j\mathrm{rep}_{2^p}(m)$. From Lemma 14, we know that $pn \geq z$. Therefore, we have

$$\begin{aligned}
j'2^{p|x_j|} + \mathrm{val}_b(x_j) \equiv 0 \pmod{m} &\iff j'2^{p(n+L)} + \mathrm{val}_b(w_j)2^{pL} \equiv 0 \pmod{m}\\
&\iff j'2^{p(n+L)} + \sigma(j)2^{z+pL} \equiv 0 \pmod{k2^z}\\
&\iff j'2^{p(n+L)-z} + \sigma(j)2^{pL} \equiv 0 \pmod{k}\\
&\iff j'2^{pn-z} - j2^{pn-z} \equiv \quad \pmod{k}\\
&\iff j \equiv j' \pmod{k}\\
&\iff j = j'
\end{aligned}$$

and the result follows. □

7 The product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$

In this section, we study the product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. Since the states of $\mathcal{A}_{m,2^p}$ are numbered from 0 to $m{-}1$ and those of $\mathcal{A}_{\mathcal{T},2^p}$ are T and B, we denote the states of the product automaton by

$$(0, T), \ldots, (m{-}1, T) \text{ and } (0, B), \ldots, (m{-}1, B),$$

or, when there is no ambiguity, simply by

$$0T, \ldots, (m{-}1)T \text{ and } 0B, \ldots, (m{-}1)B.$$

The transitions of $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ are defined as follows. For $i, j \in [\![0, m-1]\!]$, $X, Y \in \{T, B\}$ and $d, e \in A_{2^p}$, there is a transition labeled by (d, e) from the state (i, X) to the state (j, Y) if and only if

$$2^p i + e = md + j \quad \text{and} \quad Y = X_d.$$

We denote by $\delta_\times$ the (partial) transition function of this product automaton. The state $(0, T)$ is both initial and final, and there is no other final state.

Lemma 17. *For all $i, j \in [\![0, m-1]\!]$, $X, Y \in \{T, B\}$ and $(u, v) \in (A_{2^p} \times A_{2^p})^*$, we have $\delta_\times((i, X), (u, v)) = (j, Y)$ if and only if*

$$2^{p\,|(u,v)|}\, i + \mathrm{val}_{2^p}(v) = m\, \mathrm{val}_{2^p}(u) + j \quad \text{and} \quad Y = X_{\mathrm{val}_{2^p}(u)}.$$

Proof. It suffices to combine Lemmas 6 and 8. □

In Figure 6, we have depicted the automaton $\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4}$, as well as the automata $\mathcal{A}_{6,4}$ and $\mathcal{A}_{\mathcal{T},4}$, which we have placed in such a way that the labels of the product automata can be easily deduced. We have drawn a full cycle in purple. It is of course not the only such cycle. This shows that the automaton $\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4}$ is accessible and coaccessible. It will be true in general for the product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. We give a proof of this fact below.

Corollary 18. *The word $\mathrm{rep}_{2^p}(1, m)$ is accepted from the state $(0, B)$ in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. In particular, the state $(0, B)$ is coaccessible in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$.*

Proof. This follows from Lemma 17. □

Lemma 19. *For each $i \in \{0, \ldots, m-1\}$, the states (i, T) et (i, B) of the automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ are disjoint.*

Proof. This comes from the fact that $\mathcal{A}_{\mathcal{T},2^p}$ has disjoint states. □

Lemma 20. *For distinct $i, j \in [\![0, m-1]\!]$ and for $X, Y \in \{T, B\}$, the states (i, X) et (j, Y) are disjoint in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$.*

Proof. Let $i, j \in [\![0, m-1]\!]$ and $X, Y \in \{T, B\}$. Suppose that there exists a word $(u, v) \in (A_{2^p} \times A_{2^p})^*$ which is accepted from both (i, X) and (j, Y) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. Then (u, v) is accepted from both i and j in $\mathcal{A}_{m,2^p}$. Since the automaton $\mathcal{A}_{m,2^p}$ has disjoint states by Proposition 10, this implies that $i = j$. □

We are now ready to establish the main properties of the product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$.

Proposition 21. *The automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ is complete, accessible, coaccessible and has disjoint states. In particular, it is the minimal automaton of $\mathrm{val}_{2^p}^{-1}(\{(t, mt) \colon t \in \mathcal{T}\})$.*

Proof. By construction of the product automaton and since

$$\{(n, mn) \colon n \in \mathbb{N}\} \cap \big(\mathcal{T} \times \mathbb{N}\big) = \{(t, mt) \colon t \in \mathcal{T}\},$$

we get that the product automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ accepts the language

$$\mathrm{val}_{2^p}^{-1}(\{(t, mt) \colon t \in \mathcal{T}\}).$$

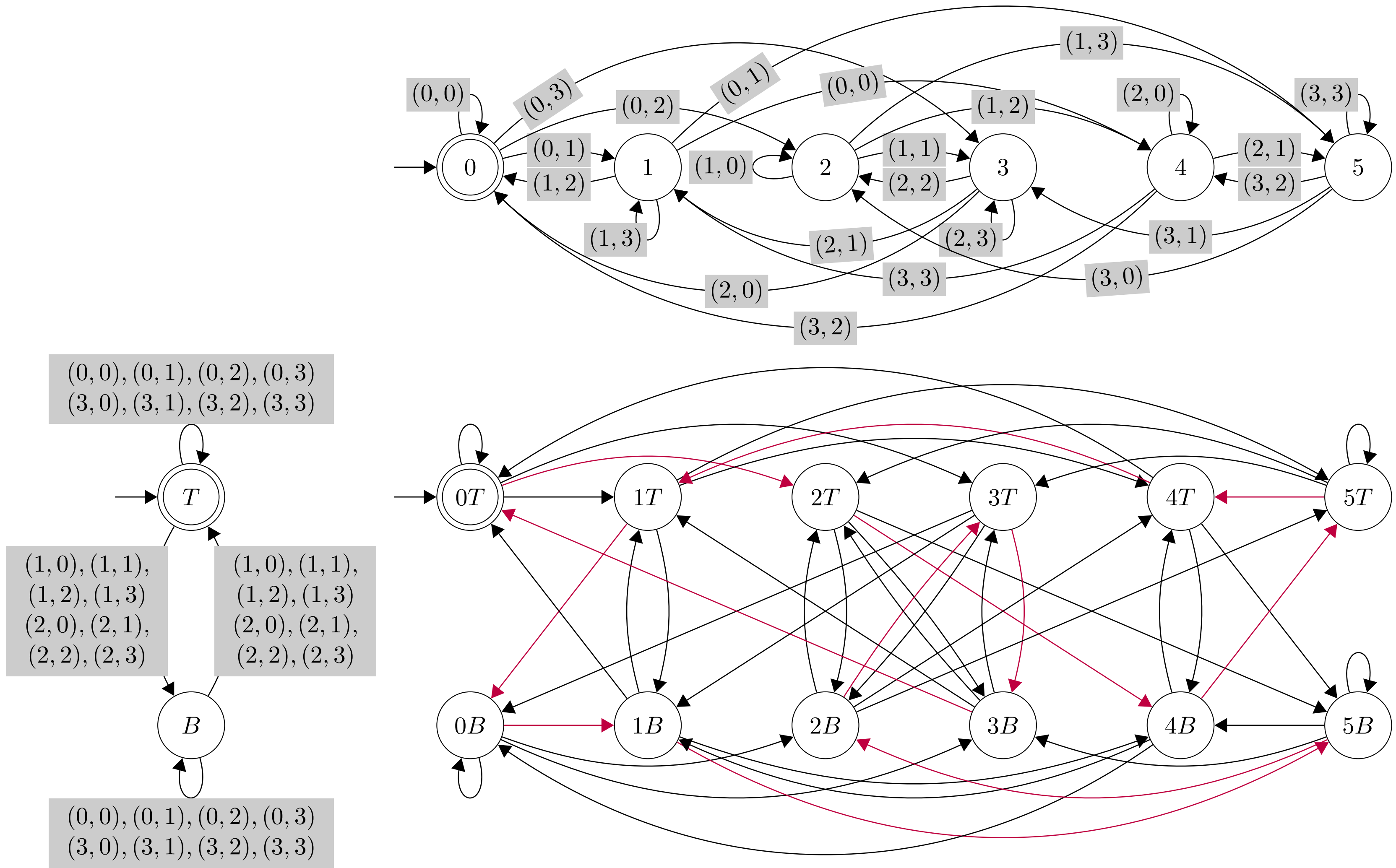

Figure 6: The product automaton $\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4}$

By Lemma 17, we can check that for every $i \in [\![0, m-1]\!]$, the states (i, T) and (i, B) are accessible thanks to the word $\mathrm{rep}_{2^p}(0, i)$ and $\mathrm{rep}_{2^p}(1, m+i)$ respectively. Hence, $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ is accessible. To show the coaccessibility, we now fix some $i \in [\![0, m-1]\!]$ and $X \in \{T, B\}$. By Proposition 10, we already know that the automaton $\mathcal{A}_{m,2^p}$ is coaccessible. Therefore, we can find $(u, v) \in (A_{2^p} \times A_{2^p})^*$ such that there is a path labeled by (u, v) from i to 0 in $\mathcal{A}_{m,2^p}$. Thus, by reading (u, v) from the state (i, X) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$, we reach either the state $(0, T)$ or the state $(0, B)$. If we reach $(0, T)$, then the state (i, X) is coaccessible. If we reach $(0, B)$ instead, then we may apply Corollary 18 in order to obtain that (i, X) is coaccessible as well. Finally, in order to see that $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ has disjoint states, it suffices to combine Lemmas 19 and 20. □

8 The projection $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ of the product automaton

The aim of this section is to provide a DFA accepting the language $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$. This automaton is denoted by $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ and is defined from the automaton $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ by only considering the second component of each label. Formally, the states of $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ are

$$(0, T), \ldots, (m-1, T) \text{ and } (0, B), \ldots, (m-1, B),$$

the state $(0, T)$ is both initial and final and no other state is final, and the transitions are defined as follows. For $i, j \in [\![0, m-1]\!]$, $X, Y \in \{T, B\}$ and $e \in A_{2^p}$, there is a transition labeled by e from the state (i, X) to the state (j, Y) if and only if there exists $d \in A_{2^p}$ such that

$$2^p i + e = md + j \quad \text{and} \quad Y = X_d.$$

Example 22. The automata $\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4}$ and $\Pi(\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4})$ are depicted in Figures 6 and 7 respectively. In Figure 7, all edges labeled by 0 (1, 2 and 3 respectively) are represented in black (blue, red and green respectively).

Lemma 23. *For every $i \in [\![0, m-1]\!]$, the states (i, T) and (i, B) are disjoint in the projected automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.*

Proof. Let $i \in [\![0, m-1]\!]$. It follows from Remark 7 and the definitions of the transition functions of $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ and $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ that if a word v over A_{2^p} is accepted from both (i, T) and (i, B) in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, then there exists a unique word u over A_{2^p} of length $|v|$ such that the word (u, v) is accepted from both (i, T) and (i, B) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. The conclusion then follows from Lemma 19. □

Proposition 24. *The automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$*

- *accepts* $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$
- *is deterministic*
- *is complete*
- *is accessible*
- *is coaccessible*

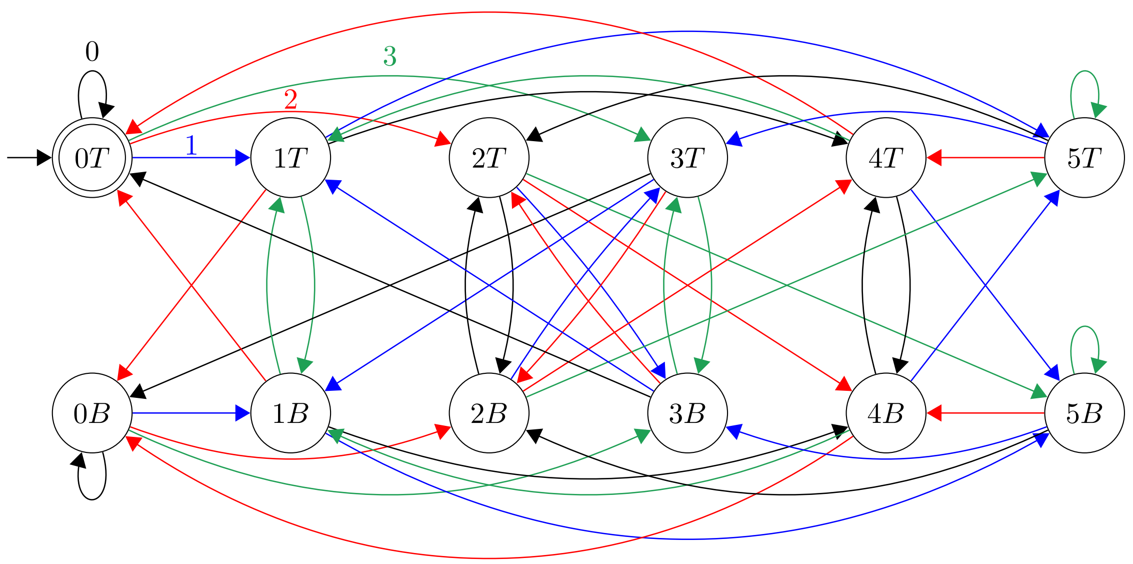

Figure 7: The projected automaton $\Pi(\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4})$.

- *has disjoint states if m is odd*
- *is minimal if m is odd.*

Proof. By construction, $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ accepts $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$; see Section 3. The fact that this automaton is deterministic and complete follows from Remark 7. It is accessible and coaccessible because so is $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. Now we turn to the last two items. If a word v over A_{2^p} is accepted from some state (i, X) in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, then there exists a word u over A_{2^p} of length $|v|$ such that the word (u, v) is accepted from (i, X) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. We deduce that (u, v) is accepted from the state i in $\mathcal{A}_{m,2^p}$ and in turn, that v is accepted from the state i in $\Pi(\mathcal{A}_{m,2^p})$. Therefore, and by combining Proposition 13 and Lemma 23, we obtain that if m is odd then the automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ has disjoint states. It directly follows that $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ is minimal if m is odd. □

Corollary 25. *If m is odd, then the state complexity of $m\mathcal{T}$ with respect to the base 2^p is $2m$.*

Note that Corollary 25 and Theorem 3 are consistent in the case where m is odd, i.e. where $z = 0$. However, we will see in the next section that the DFA $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ is never minimal for even m because it contains several states accepting the same language.

9 Minimization of $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$

We start by defining some classes of states of $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$. Our aim is twofold. First, we will prove that those subsets consist in *indistinguishable* states, i.e. accepting the same language. Second, we will show that states belonging to different such subsets are *distinguishable*, i.e. accepts different languages. Otherwise stated, these classes correspond to the left quotients $w^{-1}L$ where w is any word over the alphabet A_{2^p} and $L = \mathrm{rep}_{2^p}(m\mathcal{T})$.

Definition 26. For $(j, X) \in \big([\![1, k{-}1]\!] \times \{T, B\}\big) \cup \{(0, B)\}$, we define

$$[(j, X)] = \{(j + k\ell, X_\ell) \colon 0 \le \ell \le 2^z{-}1\}$$

and $[(0, T)] = \{(0, T)\}$. We say that $[(j, X)]$ is the *class* of the state (j, X).

Remark 27. Note that the classes $[(j, X)]$ are pairwise disjoint: $[(j, X)] \cap [(j', X')] = \emptyset$ if $(j, X) \neq (j', X')$. If m is odd, i.e. if $z = 0$, then all these classes are reduced to a single state. If m is a power of 2, i.e. if $k = 1$, then there is no class of the form $[(j, X)]$ with $j \geq 1$.

Definition 28. For $\alpha \in [\![0, z{-}1]\!]$, we define a *pre-class* C_α of size 2^α:

$$C_\alpha = [(k2^{z-\alpha-1}, B)] = \{(k2^{z-\alpha-1} + k2^{z-\alpha}\ell, B_\ell) \colon \ell \in [\![0, 2^\alpha{-}1]\!]\}.$$

Then, for $\beta \in [\![0, \lceil \frac{z}{p} \rceil{-}2]\!]$, we define a *class* Γ_β as follows:

$$\Gamma_\beta = \bigcup_{\alpha=\beta p}^{\beta p+p-1} C_\alpha.$$

In addition, we set

$$\Gamma_{\lceil \frac{z}{p} \rceil - 1} = \bigcup_{\alpha=\left(\lceil \frac{z}{p} \rceil - 1\right)p}^{z-1} C_\alpha.$$

Remark 29. Note that the classes Γ_β are pairwise disjoint. If m is odd, i.e. if $z = 0$, then there is no such class Γ_β.

Remark 30. If a class $[(j, X)]$ or Γ_β exists, then it is nonempty. Moreover, the classes Γ_β together with the class $[(0, T)]$ form a partition of $\{(k\ell, T_\ell) \colon \ell \in [\![0, 2^z{-}1]\!]$. Therefore, the classes $[(j, X)]$ and Γ_β form a partition of the set of states of $\Pi\,(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Example 31. For $m = 24$ and $p = 2$, the classes defined above are

$$\begin{aligned}
[(0,T)] &= \{(0,T)\} \\
[(1,T)] &= \{(1,T),(4,B),(7,B),(10,T),(13,B),(16,T),(19,T),(22,B)\} \\
[(2,T)] &= \{(2,T),(5,B),(8,B),(11,T),(14,B),(17,T),(20,T),(23,B)\} \\
[(0,B)] &= \{(0,B),(3,T),(6,T),(9,B),(12,T),(15,B),(18,B),(21,T)\} \\
[(1,B)] &= \{(1,B),(4,T),(7,T),(10,B),(13,T),(16,B),(19,B),(22,T)\} \\
[(2,B)] &= \{(2,B),(5,T),(8,T),(11,B),(14,T),(17,B),(20,B),(23,T)\} \\
\Gamma_0 = C_0 \cup C_1 &= \{(12,B)\} \cup \{(6,B),(18,T)\} = \{(6,B),(12,B),(18,T)\} \\
\Gamma_1 = C_2 &= \{(3,B),(9,T),(15,T),(21,B)\}.
\end{aligned}$$

In Figure 8, the states of the automaton $\Pi\,(\mathcal{A}_{24,4} \times \mathcal{A}_{\mathcal{T},4})$ are colored with respect to these classes.

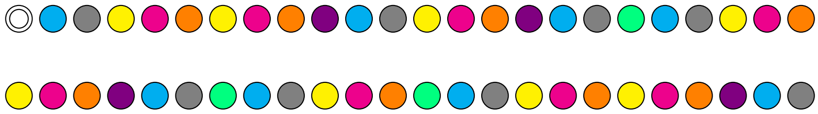

Figure 8: The classes of the projected automaton $\Pi(\mathcal{A}_{24,4} \times \mathcal{A}_{\mathcal{T},4})$.

9.1 States of the same class are indistinguishable

In order to prove that two states (j, X) and (j', X') of the automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ are indistinguishable, we have to prove that $L_{(j,X)} = L_{(j',X')}$. The general procedure that we use for proving that $L_{(j,X)} \subseteq L_{(j',X')}$ goes as follows. Let $v \in L_{(j,X)}$ and let $n = |v|$. Then we know that there exists a word u over A_{2^p} of length $|v|$ such that (u, v) is accepted from the state (j, X) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ (before the projection). If $d = \mathrm{val}_{2^p}(u)$ and $e = \mathrm{val}_{2^p}(v)$, then, in view of Lemma 17, we must have

$$2^{p|v|}j + e = md \quad \text{and} \quad X_d = T$$

(since the only final state of $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ is $(0, T)$). Moreover, since $n = |v|$, we have $d, e \in [\![0, 2^{pn}-1]\!]$. Now, in order to prove that $v \in L_{(j',X')}$, we have to find a word u' over A_{2^p} of length n such that (u', v) is accepted from (j', X') in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. But then, we necessarily have that

$$\mathrm{val}_{2^p}(u') = \frac{2^{p|v|}j' + e}{m}.$$

Let thus $d' = \frac{2^{p|v|}j+e}{m}$. We obtain that $v \in L_{(j',X')}$ if and only if $d' \in [\![0, 2^{pn}-1]\!]$ and $X'_{d'} = T$. Indeed, in this case, $|\mathrm{rep}_{2^p}(d')| \leq n$ and thus, we can take the word $u' = 0^{n-|\mathrm{rep}_{2^p}(d')|}\mathrm{rep}_{2^p}(d')$.

First, we show that two states of the same class of the form $[(j, X)]$ are indistinguishable.

Proposition 32. *Let $j \in [\![1, k-1]\!]$, $X \in \{T, B\}$ and $\ell \in [\![0, 2^z-1]\!]$. We have*

$$L_{(j,X)} = L_{(j+k\ell, X_\ell)}$$

in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proof. Let $v \in A^*_{2^p}$, $n = |v|$, $e = \mathrm{val}_{2^p}(v)$, $d = \frac{2^{pn}j+e}{m}$ and $d' = \frac{2^{pn}(j+k\ell)+e}{m}$. We have to prove that $d \in [\![0, 2^{pn}-1]\!]$ and $X_d = T$ if and only if $d' \in [\![0, 2^{pn}-1]\!]$ and $(X_\ell)_{d'} = T$.

Since $1 \leq j < k$ and $0 \leq e < 2^{pn}$, we have

$$0 < d = \frac{2^{pn}j + e}{m} < \frac{2^{pn}k}{m} = 2^{pn-z}. \tag{4}$$

Since $d' = d + \frac{2^{pn}k\ell}{m} = d + 2^{pn-z}\ell$, it follows from (4) that if d and d' are both integers, then we must have

$$\mathrm{rep}_2(d') = \mathrm{rep}_2(\ell)0^{pn-z-|\mathrm{rep}_2(d)|}\mathrm{rep}_2(d).$$

Therefore, $d \in \mathcal{T}$ if and only if either $\ell \in \mathcal{T}$ and $d' \in \mathcal{T}$, or $\ell \notin \mathcal{T}$ and $d' \notin \mathcal{T}$, and hence $X_d = (X_\ell)_{d'}$.

Now, suppose that $d \in [\![0, 2^{pn}-1]\!]$ and $X_d = T$. It follows from (4) that $pn > z$, for otherwise we would have $0 < d < 1$, which is not possible since d is an integer. Therefore, we get that $d' = d + 2^{pn-z}\ell$ is a positive integer. We also get from (4) that

$$d' = d + 2^{pn-z}\ell < 2^{pn-z}(\ell + 1) \leq 2^{pn}.$$

Consequently, $d' \in [\![0, 2^{pn}-1]\!]$ and $(X_\ell)_{d'} = T$.

Conversely, suppose that $d' \in [\![0, 2^{pn}-1]\!]$ and $(X_\ell)_{d'} = T$. In view of (4) and since $d = d' - 2^{pn-z}\ell$, in order to obtain that $d \in [\![0, 2^{pn}-1]\!]$, it is enough to show that $pn > z$. Proceed by contradiction and suppose that $pn \leq z$. Let $q = \left\lfloor \frac{\ell}{2^{z-pn}} \right\rfloor$. On the one hand, since $j \geq 1$ and $e \geq 0$, we obtain

$$d' = \frac{2^{pn}(j + k\ell) + e}{m} > \frac{2^{pn}k\ell}{m} = \frac{\ell}{2^{z-pn}} \geq q.$$

On the other hand, since $\ell \leq (q+1)2^{z-pn}-1$, $e < 2^{pn}$ and $j \leq k-1$, we obtain

$$d' < \frac{2^{pn}(j + k(q+1)2^{z-pn} - k) + 2^{pn}}{m} = q + 1 + 2^{pn}\frac{j - k + 1}{m} \leq q + 1.$$

This is not possible since d' is an integer, and hence $pn > z$. Consequently, $d \in [\![0, 2^{pn}-1]\!]$ and $X_d = T$ as desired. $\square$

Proposition 33. *Let $\ell \in [\![1, 2^z-1]\!]$. We have*

$$L_{(0,B)} = L_{(k\ell, B_\ell)}$$

in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proof. Let $v \in A_{2^p}^*$, $n = |v|$, $e = \mathrm{val}_{2^p}(v)$, $d = \frac{e}{m}$ and $d' = \frac{2^{pn}k\ell + e}{m}$. We have to prove that we have $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$ if and only if $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$.

Since $0 \leq e < 2^{pn}$, we have

$$0 \leq d = \frac{e}{m} < \frac{2^{pn}}{m} = \frac{2^{pn-z}}{k}. \tag{5}$$

Since $k \geq 1$, it follows that $d < 2^{pn-z}$ and we get that $B_d = (B_\ell)_{d'}$ as in the proof of Proposition 32, provided that both d and d' are integers.

Now, suppose that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$, that is, that d is an integer and that $d \notin \mathcal{T}$. If $pn \leq z$ then we get from (5) that $0 \leq d < 1$. But since d is an integer, this implies that $d = 0$, which is impossible because $d \notin \mathcal{T}$. Thus, $pn > z$ and $d' = d + \ell 2^{pn-z}$ is a nonnegative integer. Moreover, we have

$$d' = d + \ell 2^{pn-z} < \frac{2^{pn-z}}{k} + (2^z-1)2^{pn-z} = 2^{pn} + 2^{pn-z}\left(\frac{1}{k} - 1\right) \leq 2^{pn}.$$

Hence $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$.

Conversely, suppose that $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$. In particular, we have $d' \in \mathcal{T} \iff \ell \notin \mathcal{T}$. From (5), we know that $0 \leq d < 2^{pn}$. We claim that $pn > z$. Proceed by contradiction and suppose that $pn \leq z$. Let $q = \left\lfloor \frac{\ell}{2^{z-pn}} \right\rfloor$. Then, on the one hand, we have

$$d' = \frac{2^{pn}k\ell + e}{m} \geq \frac{\ell}{2^{z-pn}} \geq q.$$

On the other hand, since $\ell \leq (q+1)2^{z-pn}-1$ and $e < 2^{pn}$, we obtain

$$md' = 2^{pn}k\ell + e < 2^{pn}k((q+1)2^{z-pn}-1) + 2^{pn} = m(q+1) - 2^{pn}(k-1) \leq m(q+1),$$

and hence $d' < q + 1$. Since d' is an integer, we get that $d' = q$, $e = 0$ and $\ell = 2^{z-pn}d'$. But then we would have

$$\mathrm{rep}_2(\ell) = \mathrm{rep}_2(d')0^{z-pn},$$

contradicting that $d' \in \mathcal{T} \iff \ell \notin \mathcal{T}$. Thus $pn > z$ and $d = d' - \ell 2^{pn-z}$ is an integer. Altogether, we get that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$. $\square$

Corollary 34. *For each* $(j, X) \in \big([\![1, k-1]\!] \times \{T, B\}\big) \cup \{(0, B)\}$*, all states of the class* $[(j, X)]$ *are indistinguishable in* $\Pi\,(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Now, we show that two states of the same class of the form Γ_β are indistinguishable.

Proposition 35. *Suppose that* $z \geq 1$ *and let* $\alpha \in [\![0, z-1]\!]$ *and* $\ell \in [\![1, 2^\alpha-1]\!]$*. We have*

$$L_{(k2^{z-\alpha-1},B)} = L_{(k2^{z-\alpha-1}+k2^{z-\alpha}\ell,B_\ell)}$$

in $\Pi\,(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proof. Let $v \in A_{2^p}^*$, $n = |v|$, $e = \mathrm{val}_{2^p}(v)$, $d = \frac{2^{pn}k2^{z-\alpha-1}+e}{m}$ and $d' = \frac{2^{pn}(k2^{z-\alpha-1}+k2^{z-\alpha}\ell)+e}{m}$. We have to show that we have $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$ if and only if $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$.

Using that $k \geq 1$, $e < 2^{pn}$ and $\alpha < z$, we get

$$0 < d = \frac{k2^{pn+z-\alpha-1} + e}{m} < 2^{pn-\alpha-1} + \frac{2^{pn-z}}{k} \leq 2^{pn-\alpha-1} + 2^{pn-z} \leq 2^{pn-\alpha}. \tag{6}$$

Since $d' = d + \frac{k2^{pn+z-\alpha}\ell}{m} = d + 2^{pn-\alpha}\ell$, we obtain that if both d and d' are integers then

$$\mathrm{rep}_2(d') = \mathrm{rep}_2(\ell)0^{pn-\alpha-|\mathrm{rep}_2(d)|}\mathrm{rep}_2(d),$$

and hence $B_d = (B_\ell)_{d'}$.

Now, suppose that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$. Then, we get from (6) that $pn > \alpha$ and $d' = d + 2^{pn-\alpha}\ell$ is a nonnegative integer. Moreover, $d' < 2^{pn-\alpha}(\ell + 1) \leq 2^{pn}$. Therefore $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$.

Conversely, suppose that $d' \in [\![0, 2^{pn}-1]\!]$ and $(B_\ell)_{d'} = T$. In particular, we have that $d' \in \mathcal{T} \iff \ell \notin \mathcal{T}$. From (6), we know that $0 \leq d < 2^{pn}$. We claim that $pn > \alpha$. Proceed by contradiction and suppose that $pn \leq \alpha$. Let $q = \mathrm{DIV}(\ell, 2^{\alpha-pn})$. Then, on the one hand, we have

$$d' = d + \frac{\ell}{2^{\alpha-pn}} \geq q.$$

On the other hand, since $\ell \leq (q + 1)2^{\alpha-pn}-1$, $e < 2^{pn}$, $k \geq 1$ and $\alpha < z$, we successively obtain that

$$\begin{aligned} md' &< 2^{pn}(k2^{z-\alpha-1} + k2^{z-\alpha}((q + 1)2^{\alpha-pn}-1)) + 2^{pn} \\ &= m(q + 1) + 2^{pn}(k2^{z-\alpha-1} - k2^{z-\alpha} + 1) \\ &= m(q + 1) + 2^{pn}(1 - k2^{z-\alpha-1}) \\ &\leq m(q + 1). \end{aligned}$$

We obtain that $q \leq d' < (q + 1)$, hence $d' = q$ and $\ell = 2^{\alpha-pn}d'$, contradicting that $d' \in \mathcal{T} \iff \ell \notin \mathcal{T}$. Thus, we have that $pn > \alpha$ and $d = d' - 2^{pn-\alpha}\ell$ is an integer. It follows that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$. □

Corollary 36. *For all* $\alpha \in [\![0, z-1]\!]$*, all states of the pre-class* C_α *are indistinguishable in* $\Pi\,(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proposition 37. *Suppose that* $z \geq 1$ *and let* $\beta \in [\![0, \lceil \frac{z}{p} \rceil-2]\!]$ *and* $c \in [\![1, p-1]\!]$*. Then*

$$L_{(k2^{z-\beta p-1},B)} = L_{(k2^{z-(\beta p+c)-1},B)}$$

in $\Pi\,(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proof. Let $v \in A_{2^p}^*$, $n = |v|$, $e = \text{val}_{2^p}(v)$, $d = \frac{2^{pn}k2^{z-\beta p-1}+e}{m}$ and $d' = \frac{2^{pn}k2^{z-(\beta p+c)-1}+e}{m}$. We have to show that we have $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$ if and only if $d' \in [\![0, 2^{pn}-1]\!]$ and $B_{d'} = T$.

We have $d = 2^{pn-\beta p-1} + \frac{e}{m}$ and $d' = 2^{pn-\beta p-c-1} + \frac{e}{m}$. Since $z > (\beta+1)p$ and $p \geq c+1$, we have

$$\frac{e}{m} < 2^{pn-z} < 2^{pn-(\beta+1)p} \leq 2^{pn-\beta p-c-1}.$$

Thus, if both d and d' are integers and if m divides e then we obtain that

$$\text{rep}_2(d) = 10^{pn-\beta p-1-|\text{rep}_2(\frac{e}{m})|}\text{rep}_2\left(\frac{e}{m}\right)$$

and

$$\text{rep}_2(d') = 10^{pn-\beta p-c-1-|\text{rep}_2(\frac{e}{m})|}\text{rep}_2\left(\frac{e}{m}\right).$$

In this case, we have that $d \in \mathcal{T} \iff d' \in \mathcal{T}$, hence $B_d = B_{d'}$.

Now, suppose that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$. Since $k \geq 1$ and $d = d' + 2^{pn-\beta p-1}(1 - 2^{-c})$, we obtain that $0 < d' < d < 2^{pn}$. We claim that $pn \geq \beta p + c + 1$. Proceed by contradiction and suppose that $pn < \beta p + c + 1$. Then, since $c+1 \leq p$ and $\beta \leq \lceil \frac{z}{p} \rceil - 2$, we obtain that $pn \leq \beta p < z - p$. Therefore, we have

$$d = 2^{pn-\beta p-1} + \frac{e}{m} < \frac{1}{2} + \frac{2^{pn-z}}{k} < 1$$

contradicting that d is a positive integer. Thus $pn \geq \beta p + c + 1$, and hence both d' and $\frac{e}{m}$ are integers. Therefore, we obtain that $d' \in [\![0, 2^{pn}-1]\!]$ and $B_{d'} = T$.

Conversely, suppose that $d' \in [\![0, 2^{pn}-1]\!]$ and $B_{d'} = T$. Using that $z \geq 1$, we obtain

$$0 \leq d = 2^{pn-\beta p-1} + \frac{e}{m} < 2^{pn-\beta p-1} + 2^{pn-z} \leq 2^{pn}.$$

We claim that $pn \geq \beta p+c+1$. Proceed by contradiction and suppose that $pn < \beta p+c+1$. Since $c + 1 \leq p$, we obtain that $n \leq \beta$ and

$$d' = 2^{pn-\beta p-c-1} + \frac{e}{m} < 2^{-c-1} + 2^{pn-z} \leq \frac{1}{2} + 2^{\beta p-z} < \frac{1}{2} + 2^{-p} < 1$$

contradicting that d' is a positive integer. Thus $d = d' - 2^{pn-\beta p-1}(1 - 2^{-c})$ is an integer, and consequently, so is $\frac{e}{m}$. Therefore, we obtain that $d \in [\![0, 2^{pn}-1]\!]$ and $B_d = T$. □

Corollary 38. *For all $\beta \in [\![0, \lceil \frac{z}{p} \rceil - 2]\!]$, all states of the class Γ_β are indistinguishable in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.*

Proposition 39. *Suppose that $z \geq 1$ and let $\beta = \lceil \frac{z}{p} \rceil - 1$ and $c \in [\![1, z-\beta p-1]\!]$. We have*

$$L_{(k2^{z-\beta p-1},B)} = L_{(k2^{z-(\beta p+c)-1},B)}$$

in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$.

Proof. The proof is a straightforward adaptation of that of Proposition 37. □

Corollary 40. *In $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, all states of $\Gamma_{\lceil \frac{z}{p} \rceil - 1}$ are indistinguishable.*

9.2 States of different classes are distinguishable

In this section, we show that, in the projected automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, states from different classes $[(j,X)]$ or Γ_β are pairwise distinguishable, that is, for any two such states, there exists a word which is accepted from exactly one of them.

Proposition 41. *Let $\beta \in [\![0, \lceil \frac{z}{p} \rceil - 1]\!]$. In $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, the word $0^{\beta+1}$ is accepted from all states of Γ_β.*

Proof. From Corollaries 38 et 40, it suffices to show that $0^{\beta+1}$ is accepted from the state $(k2^{z-\beta p-1}, B)$. Let

$$d = \frac{2^{p(\beta+1)} k 2^{z-\beta p-1}}{m}.$$

We have to show that $d \in \{0, \ldots, 2^{p(\beta+1)}\} \setminus \mathcal{T}$. It is immediate since $d = 2^{p-1}$. □

Proposition 42. *Let $\beta, \gamma \in [\![0, \lceil \frac{z}{p} \rceil - 1]\!]$ such that $\gamma > \beta$. In $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, the word $0^{\beta+1}$ is not accepted from any state of Γ_γ.*

Proof. From Corollaries 38 et 40, it suffices to show that $0^{\beta+1}$ is not accepted from the state $(k2^{z-\gamma p-1}, B)$. Suppose to the contrary that $0^{\beta+1}$ is accepted from $(k2^{z-\gamma p-1}, B)$. Then

$$\frac{2^{p(\beta+1)} k 2^{z-\gamma p-1}}{m} = 2^{p(\beta-\gamma+1)-1}$$

must be an integer, and hence $p(\beta - \gamma + 1) \geq 1$, contradicting that $\gamma > \beta$. The conclusion follows. □

Proposition 43. *Let $(j,X) \in ([\![1, k-1]\!] \times \{T, B\}) \cup \{(0,B)\}$ and $\beta \in [\![0, \lceil \frac{z}{p} \rceil - 1]\!]$. In $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, the word $0^{\beta+1}$ is not accepted from any state of $[(j,X)]$.*

Proof. Since there is a loop labeled by 0 on the state $(0,T)$ and in view of Corollary 34, it suffices to show that the word $0^{\lceil z/p \rceil}$ is not accepted from the state (j,X). If $0^{\lceil z/p \rceil}$ were accepted from the state (j,X), then we would get that

$$d = \frac{2^{p\lceil \frac{z}{p} \rceil} j}{m} = \frac{2^{\lceil \frac{z}{p} \rceil - z} j}{k}$$

is an integer and that $X_d = T$. If $j \neq 0$, then d cannot be an integer since k is odd and $0 < j < k$. If $j = 0$, then we get that d must belong to $\mathcal{T}$, which is not possible either since in this case we have $d = 0$. Hence the conclusion. □

Proposition 44. *Suppose that $k > 1$ and let $(j,X), (j',X') \in ([\![1, k-1]\!] \times \{T, B\}) \cup \{(0,B)\}$ be distinct. In $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, the states (j,X) and (j',X') are distinguishable.*

Proof. First, suppose that $j = j'$. Then $X \neq X'$ by hypothesis and the states (j,X) and (j,X') are disjoint by Lemma 23. Since $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ is coaccessible by Proposition 24, we obtain that the states (j,X) and (j,X') are distinguishable.

Now suppose that $j \neq j'$. By Proposition 15, the word w_j is accepted from j in the automaton $\Pi(\mathcal{A}_{m,2^p})$ but is not accepted from j'. Then, there exists a word u of length $|w_j|$ such that (u, w_j) is accepted from j in the automaton $\mathcal{A}_{m,2^p}$ but is not accepted from j'. Then, this word (u, w_j) is accepted either from (j,T) or from (j,B) in the automaton

$\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$ but is not accepted neither from (j',T) nor from (j',B). Now, two cases are possible.

First, suppose that (u,w_j) is accepted from (j,X) in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. Then, in the projection $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, the word w_j is accepted from (j,X) but not from (j',X'). Thus, the word w_j distinguishes the states (j,X) and (j',X').

Second, suppose that (u,w_j) is accepted from $(j,\overline{X})$ in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. Then there is a path labeled by (u,w_j) from (j,X) to $(0,B)$ in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$. By Corollary 18, in $\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p}$, the word $\mathrm{rep}_{2^p}(1,m)$ is accepted from $(0,B)$, and hence the word $(u,w_j)\mathrm{rep}_{2^p}(1,m) = (u0^{|\mathrm{rep}_{2^p}(m)|-1}1, w_j\mathrm{rep}_{2^p}(m))$ is accepted from (j,X). Therefore the word $w_j\mathrm{rep}_{2^p}(m)$ is accepted from the state (j,X) in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$. Besides, the word $w_j\mathrm{rep}_{2^p}(m)$ cannot be accepted from (j',X') in $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ for otherwise it would also be accepted from j' in $\Pi(\mathcal{A}_{m,2^p})$, which is impossible by Proposition 16. Thus, the word $w_j\mathrm{rep}_{2^p}(m)$ distinguishes the states (j,X) and (j',X'). □

Corollary 45. *In the automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, two states belonging to different classes are distinguished.*

9.3 The minimal automaton of $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$.

We are ready to construct the minimal automaton of $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$. Since the states of $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ that belong to the same class $[(j,X)]$ or Γ_β are indistinguishable, they can be glued together in order to define a new automaton $\mathcal{M}_{m,\mathcal{T},2^p}$ that still accepts the same language. Formally, the alphabet of $\mathcal{M}_{m,\mathcal{T},2^p}$ is A_{2^p}. Its states are the classes $[(j,X)]$ for $j \in [\![0,k-1]\!]$ and the classes Γ_β for $\beta \in [\![0,\lceil \frac{z}{p} \rceil - 1]\!]$. The class $[(0,T)]$ is the initial state and the only final state. The transitions of $\mathcal{M}_{m,\mathcal{T},2^p}$ are defined as follows: there is a transition labeled by a letter a in A_{2^p} from a class J_1 to a class J_2 if and only if there exists $j_1 \in J_1$ and $j_2 \in J_2$ such that, in the automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$, there is a transition labeled by a from the state j_1 to the state j_2.

Example 46. In Figure 9, the classes of $\Pi(\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4})$ are colored in white, blue, grey, yellow, fushia, orange and purple. Figure 10 depicts the minimal automaton $\mathcal{M}_{6,\mathcal{T},4}$ of $\mathrm{val}_4^{-1}(6\mathcal{T})$, where states corresponding to the same color are glued together to form a single state.

Theorem 47. *Let p and m be positive integers. The automaton $\mathcal{M}_{m,\mathcal{T},2^p}$ is the minimal automaton of the language $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$.*

Proof. By construction, the language accepted by $\mathcal{M}_{m,\mathcal{T},2^p}$ is $\mathrm{val}_{2^p}^{-1}(m\mathcal{T})$. In order to see that $\mathcal{M}_{m,\mathcal{T},2^p}$ is minimal, it suffices to prove that it is complete, reduced and accessible. The fact that $\mathcal{M}_{m,\mathcal{T},2^p}$ is reduced follows from the results of Sections 9.1 and 9.2. We know from From Proposition 24 that the automaton $\Pi(\mathcal{A}_{m,2^p} \times \mathcal{A}_{\mathcal{T},2^p})$ is complete and accessible, which in turn implies that $\mathcal{M}_{m,\mathcal{T},2^p}$ is complete and accessible as well. □

Note that Proposition 24 and Theorem 47 are consistent in the case where m is odd, i.e. where $z = 0$.

We are now ready to prove Theorem 3.

Proof of Theorem 3. In view of Theorem 47, it suffices to count the number of states of $\mathcal{M}_{m,\mathcal{T},2^p}$. By definition, it has $2(k-1)+2 = 2k$ states of the form $[(j,X)]$ and $\lceil \frac{z}{p} \rceil$ states of the form Γ_β. □

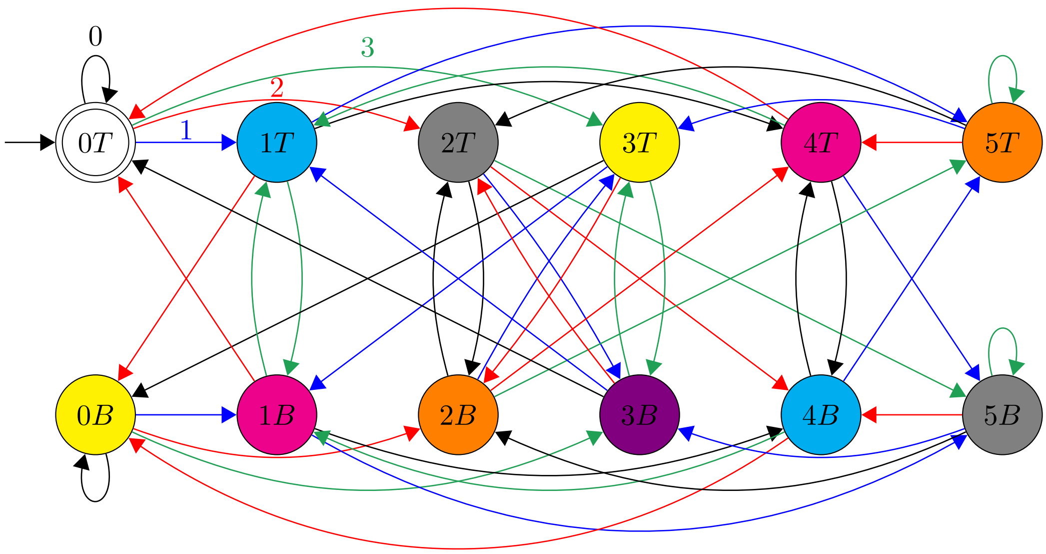

Figure 9: The classes of the automaton of $\Pi\left(\mathcal{A}_{6,4} \times \mathcal{A}_{\mathcal{T},4}\right)$.

Example 48. The minimal automaton of the language $\text{rep}_4(6\mathcal{T})$ has 7 states. We can indeed compute that $2 \cdot 3 + \lceil \frac{1}{2} \rceil = 7$.

References

[1] B. Alexeev. Minimal DFA for testing divisibility. *J. Comput. System Sci.*, 69(2):235–243, 2004.

[2] B. Boigelot, I. Mainz, V. Marsault, and M. Rigo. An efficient algorithm to decide periodicity of b-recognisable sets using MSDF convention. In *44th International Colloquium on Automata, Languages, and Programming*, volume 80 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 118, 14. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017.

[3] V. Bruyère, G. Hansel, C. Michaux, and R. Villemaire. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc. Simon Stevin*, 1(2):191–238, 1994. Journées Montoises (Mons, 1992).

[4] E. Charlier, N. Rampersad, M. Rigo, and L. Waxweiler. The minimal automaton recognizing $m\mathbb{N}$ in a linear numeration system. *Integers*, 11B:Paper No. A4, 24, 2011.

[5] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory*, 3:186–192, 1969.

[6] S. Eilenberg. *Automata, languages, and machines. Vol. A.* Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58.

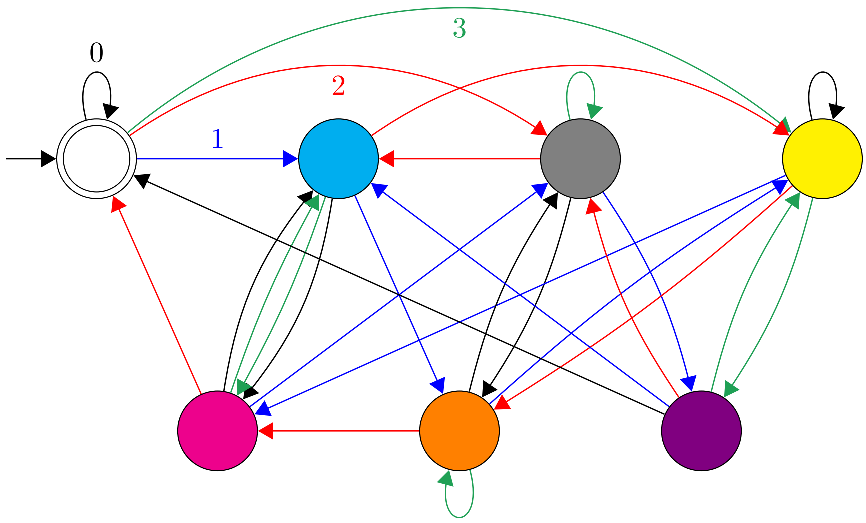

Figure 10: The minimal automaton $\mathcal{M}_{6,\mathcal{T},4}$ of $\mathrm{rep}_4(6\mathcal{T})$.

[7] M. Lothaire. *Combinatorics on words*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1997.

[8] V. Marsault and J. Sakarovitch. Ultimate periodicity of b-recognisable sets: a quasi-linear procedure. In *Developments in language theory*, volume 7907 of *Lecture Notes in Comput. Sci.*, pages 362–373. Springer, Heidelberg, 2013.

[9] J. Sakarovitch. *Elements of automata theory*. Cambridge University Press, Cambridge, 2009. Translated from the 2003 French original by Reuben Thomas.

[10] L. Waxweiler. *Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini*. PhD thesis, University of Liège, Belgium, 2009.