Identités de matrices triangulaires booléennes

Mikhail V. Volkov [1]

Résumé : on fournit une caractérisation combinatoire des identités vérifiées dans le semi-anneau de toutes les matrices triangulaires supérieures $n \times n$ et on applique cette caractérisation à la complexité calculatoire de la vérification des identités, dans les théories équationnelles d'axiomatisabilité finie, et pour les descriptions de certaines classes de langages reconnaissables.

Introduction

Une matrice *booléenne* est une matrice dont les éléments sont seulement des 0 et des 1. L'addition et la multiplication de telles matrices s'effectuent comme habituellement, excepté que l'addition et la multiplication des éléments sont définies par $x+y := \max\{x,y\}$ et $x \cdot y := \min\{x,y\}$. (Ici et ci-dessous, le signe $:=$ représente l'égalité par définition ; ainsi, $A := B$ signifie que A est défini comme B). Pour tout n, l'ensemble de toutes les matrices booléennes $n \times n$ forme un semi-anneau idempotent additivement selon l'addition et la multiplication matricielle. Ici, un *semi-anneau additivement idempotent* (ai-semi-anneau, pour abréger) est une algèbre $(S,+,\cdot)$ avec addition $+$ et multiplication $\cdot$ binaires, telles que $(S,+)$ est un semi-groupe commutatif et idempotent, $(S,\cdot)$ est un semi-groupe, et la multiplication est distributive sur l'addition à droite et à gauche.

Une matrice booléenne $\left(\alpha_{ij}\right)_{n\times n}$ est dite *triangulaire supérieure* si $\alpha_{ij} = 0$ pour tout $1 \le j < i \le n$. L'ensemble T_n de toutes les matrices booléennes $n \times n$ triangulaires supérieures est fermé selon l'addition et la multiplication matricielles de telle façon qu'il forme un sous-semi-anneau de l'ai-semi-anneau de toutes les matrices booléennes $n \times n$. Notre but est de caractériser les identités de semi-anneau de l'ai-semi-anneau $(T_n,+,\cdot)$. Comme conséquence, on obtiendra une caractérisation des identités de semi-groupe du semi-groupe $(T_n,\cdot)$.

Notre caractérisation des identités de $(T_n,+,\cdot)$ et $(T_n,\cdot)$ est présentée dans la Sect. 2 ; les preuves utilisent seulement les notions détaillées dans la Sect. 1 et la règle de multiplication pour les matrices $n \times n$:

$$\left(\alpha_{ij}\right)_{n\times n} \cdot \left(\beta_{ij}\right)_{n\times n} := \left(\sum_{k=1}^{n} \alpha_{ik}\beta_{kj}\right)_{n\times n}.$$

La Section 3 contient des applications de nos principaux résultats. Les applications traitent l'étude de la complexité calculatoire de la vérification des identités, l'axiomatisabilité finie des théories d'égalité, et les descriptions algébriques de certaines classes de langages reconnaissables. Alors que les Sects. 1 et 2 sont vraiment autonomes, comprendre le matériau de la Sect. 3 nécessite un certain bagage fourni au début des sous-sections.

1. Institut des Sciences naturelles et des mathématiques, Université fédérale de l'Oural 620000 Ekaterinburg, Russie
Traduction : Denise Vella-Chemla, mars 2025.

1 Préliminaires

Pour énoncer nos résultats, nous avons besoin de plusieurs concepts algébriques et combinatoires. La plupart sont standard, mais certains sont moins connus ou même nouveaux. Nous fournissons une introduction autonome pour le confort du lecteur. En faisant cela, nous définissons également nos notations.

1.1 Mots et sous-mots

Un *mot* (d'un *semi-groupe*) est une séquence finie de symboles, appelées *variables*. Parfois, on emploiera l'expression *mot vide*, pour définir la chaîne vide. À chaque fois que les mots considérés peuvent être vides, on le dira toujours explicitement.

On dénotera les mots par des caractères minuscules gras. Si $\mathbf{w} = w_1 \cdots w_k$, où $w_1, \ldots, w_k$ sont des variables, avec éventuellement des répétitions, alors l'ensemble $\{w_1, \ldots, w_k\}$ est dénoté par $\mathrm{alph}(\mathbf{w})$ et appelé l'*alphabet* de $\mathbf{w}$ et le nombre k est dénoté par $|\mathbf{w}|$ et appelé la *longueur* de $\mathbf{w}$. Si $\mathbf{w}$ est vide, alors on définit $\mathrm{alph}(\mathbf{w}) := \varnothing$ et $|\mathbf{w}| := 0$.

Les mots sont multipliés par concaténation : étant donnés deux mots $\mathbf{w} = w_1 \cdots w_k$ et $\mathbf{w}' = w'_1 \cdots w'_\ell$, leur produit est défini comme $\mathbf{w}\mathbf{w}' := w_1 \cdots w_k w'_1 \cdots w'_\ell$. Clairement, la concaténation est associative, donc on n'a pas besoin de parenthèses quand on écrit des produits de plusieurs mots. Si $\mathbf{w}$ est n'importe quel mot et si $\mathbf{w}'$ est vide, alors $\mathbf{w}\mathbf{w}' := \mathbf{w}$ et $\mathbf{w}'\mathbf{w} := \mathbf{w}$. Si $\mathbf{w} = \mathbf{pfs}$ pour les mots $\mathbf{p}$, $\mathbf{f}$ et $\mathbf{s}$ (dont l'un ou l'autre peut être vide), on dit que $\mathbf{p}$ est un *préfixe*, $\mathbf{f}$ est un *facteur*, et $\mathbf{s}$ est un *suffixe* du mot $\mathbf{w}$.

Soient $\mathbf{u} = u_1 \cdots u_k$ et $\mathbf{v}$ des mots. On dit que $\mathbf{u}$ *apparaît comme sous-mot dans* $\mathbf{v}$ s'il existe des mots $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{v}_{k+1}$ (dont certains peuvent être vides) tels que

$$\mathbf{v} = \mathbf{v}_1 u_1 \mathbf{v}_2 \cdots \mathbf{v}_k u_k \mathbf{v}_{k+1}. \tag{1}$$

Ainsi, $\mathbf{u}$ comme séquence de variables est une sous-séquence dans $\mathbf{v}$. On fait référence à n'importe quelle décomposition de la forme (1) comme à une *occurrence* de $\mathbf{u}$ comme sous-mot dans $\mathbf{v}$. On dit que $\mathbf{u}$ apparaît dans un mot $\mathbf{v}$ *avec des sauts* $G_1, G_2, \ldots, G_{k+1}$ s'il y a une occurrence (1) de $\mathbf{u}$ comme sous-mot dans $\mathbf{v}$ telle que $\mathrm{alph}(\mathbf{v}_\ell) = G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$.

Les trois occurrences du mot x comme sous-mot dans x^2yx sont :

$$x^2yx = \begin{cases} \underline{x} \cdot xyx, & \text{avec les sauts } \varnothing, \{x,y\}; \\ x \cdot \underline{x} \cdot yx, & \text{avec les sauts } \{x\}, \{x,y\}; \\ x^2y \cdot \underline{x}, & \text{avec les sauts } \{x,y\}, \varnothing. \end{cases}$$

Les trois occurrences du mot xy comme sous-mot dans x^2yx sont :

$$x^2yx = \begin{cases} \underline{x} \cdot x \cdot \underline{y} \cdot x, & \text{avec les sauts } \varnothing, \{x\}, \{x\}; \\ x \cdot \underline{xy} \cdot x, & \text{avec les sauts } \{x\}, \varnothing, \{x\}. \end{cases}$$

On adopte la convention que le mot vide est sous-mot de tout mot d'une manière unique avec comme saut $G_1 := \mathrm{alph}(\mathbf{v})$.

1.2 Identités de semi-groupe et inégalités

Soit $\mathbf{w} = w_1 \cdots w_k$ un mot et $(S,\cdot)$ un semi-groupe. Une *substitution* est n'importe quelle application $\varphi\colon \operatorname{alph}(\mathbf{w}) \to S$. La *valeur* de $\mathbf{w}$ selon φ est l'élément $\mathbf{w}\varphi \in S$ défini comme $\mathbf{w}\varphi := w_1\varphi \cdots w_k\varphi$.

Une *identité* (*de semi-groupe*) est une expression formelle de la forme $\mathbf{w} \approx \mathbf{w}'$ où $\mathbf{w}$ et $\mathbf{w}'$ sont des mots. Un semi-groupe $(S,\cdot)$ *satisfait* $\mathbf{w} \approx \mathbf{w}'$ (ou $\mathbf{w} \approx \mathbf{w}'$ *est vérifié* dans $(S,\cdot)$) si $\mathbf{w}\varphi = \mathbf{w}'\varphi$ pour toute substitution $\varphi\colon \operatorname{alph}(\mathbf{w}) \cup \operatorname{alph}(\mathbf{w}') \to S$. C'est-à-dire que chaque substitution d'éléments de S pour les variables apparaissant dans les mots $\mathbf{w}$ ou $\mathbf{w}'$ renvoie des valeurs égales pour ces mots.

Un *semi-groupe ordonné* est une structure $(S,\cdot,\leq)$ telle que $(S,\cdot)$ est un semi-groupe, $(S,\leq)$ est un ensemble ordonné et l'ordre est compatible avec la multiplication au sens où $a \leq b$ implique $ca \leq cb$ et $ac \leq bc$ pour tout $a,b,c \in S$. Une *inégalité* (*de semi-groupe*) est une expression formelle de la forme $\mathbf{w} \preccurlyeq \mathbf{w}'$ où $\mathbf{w}$ et $\mathbf{w}'$ sont des mots. On fait référence à $\mathbf{w}$ et $\mathbf{w}'$ comme au côté bas et, respectivement au côté haut de l'inégalité $\mathbf{w} \preccurlyeq \mathbf{w}'$. Un semi-groupe ordonné $(S,\cdot,\leq)$ *satisfait* $\mathbf{w} \preccurlyeq \mathbf{w}'$ (ou $\mathbf{w} \preccurlyeq \mathbf{w}'$ *est vérifié* dans $(S,\cdot,\leq)$) si pour toute substitution $\varphi\colon \operatorname{alph}(\mathbf{w}) \cup \operatorname{alph}(\mathbf{w}') \to S$, on a $\mathbf{w}\varphi \leq \mathbf{w}'\varphi$. De façon évidente, une identité $\mathbf{w} \approx \mathbf{w}'$ est vérifiée dans un semi-groupe ordonné $(S,\cdot,\leq)$ si et seulement si $(S,\cdot,\leq)$ satisfait à la fois les inégalités $\mathbf{w} \preccurlyeq \mathbf{w}'$ et $\mathbf{w}' \preccurlyeq \mathbf{w}$.

1.3 Identités de semi-anneau et inégalités

La plupart des notions ci-dessus s'étendent naturellement aux ai-semi-anneaux. Un *polynôme* (de *semi-anneau*) est un ensemble fini de mots d'un semi-groupe ; on suppose les polynômes non vides. On dénote les polynômes par des lettres en majuscule grasses et on les écrit comme sommes formelles de leurs éléments. Ainsi, $\mathbf{W} = \mathbf{w}_1 + \cdots + \mathbf{w}_p$ ne signifie rien mais $\mathbf{W} = \{\mathbf{w}_1, \ldots, \mathbf{w}_p\}$; en particulier, l'ordre sur les sommants n'a pas d'importance.

Pour un polynôme $\mathbf{W} = \mathbf{w}_1 + \cdots + \mathbf{w}_p$, on pose $\operatorname{alph}(\mathbf{W}) := \cup_{i=1}^{p} \operatorname{alph}(\mathbf{w}_i)$. De plus, on dit qu'un mot $\mathbf{u}$ de longueur k *apparaît dans* $\mathbf{W}$ *avec des sauts* $G_1, G_2, \ldots, G_{k+1}$ si $\mathbf{u}$ apparaît avec des sauts $G_1, G_2, \ldots, G_{k+1}$ dans certains des mots $\mathbf{w}_i$, $i = 1, \ldots, p$.

Si $\mathbf{W} = \mathbf{w}_1 + \cdots + \mathbf{w}_p$ est un polynôme, $(S,+,\cdot)$ est un ai-semi-anneau, et $\varphi\colon \operatorname{alph}(\mathbf{W}) \to S$ est n'importe quelle substitution, alors la *valeur* $\mathbf{W}\varphi$ de $\mathbf{W}$ selon φ est définie comme $\sum_{i=1}^{p} \mathbf{w}_i\varphi$. Comme le semi-groupe $(S,+)$ est commutatif et idempotent, la valeur $\mathbf{W}\varphi$ est bien définie parce que l'élément $\sum_{i=1}^{p} \mathbf{w}_i\varphi \in S$ ne dépend pas de la façon dont $\mathbf{W}$ est représenté comme une somme de mots.

Une *identité* (*de semi-anneau*) est une expression formelle de la forme $\mathbf{W} \approx \mathbf{W}'$ où $\mathbf{W}$ et $\mathbf{W}'$ sont des polynômes. Un ai-semi-anneau $(S,+,\cdot)$ *satisfait* $\mathbf{W} \approx \mathbf{W}'$ (ou $\mathbf{W} \approx \mathbf{W}'$ *est vérifié* dans $(S,+,\cdot)$) si $\mathbf{W}\varphi = \mathbf{W}'\varphi$ pour toute substitution $\varphi\colon \operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}') \to S$.

Étant donné un semi-groupe commutatif et idempotent $(S,+)$, on sait que la relation binaire $\leq$ définie pour $a,b \in S$ par

$$a \leq b \text{ si et seulement si } a + b = b \tag{2}$$

est un ordre (et il est facile de le voir) sur S compatible avec l'addition. Si $(S,+,\cdot)$ est un ai-semi-anneau, la distributivité de la multiplication sur l'addition à gauche et à droite implique directement que l'ordre

(2) est aussi compatible avec la multiplication. Quand on parle d'un ordre sur un ai-semi-anneau, on veut toujours parler de l'ordre (2).

Une *inégalité* (de *semi-anneau*) est une expression formelle de la forme $\mathbf{W} \preccurlyeq \mathbf{W}'$ où $\mathbf{W}$ et $\mathbf{W}'$ sont des polynômes appelés le côté bas, respectivement le côté haut, de l'inégalité. Un ai-semi-anneau $(S,+,\cdot)$ *satisfait* $\mathbf{W} \preccurlyeq \mathbf{W}'$ (ou $\mathbf{W} \preccurlyeq \mathbf{W}'$ *est vérifiée* dans $(S,+,\cdot)$) si pour toute substitution $\varphi\colon \operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}') \to S$, on a $\mathbf{W}\varphi \leq \mathbf{W}'\varphi$. De façon évidente, une identité $\mathbf{W} \approx \mathbf{W}'$ est vérifiée dans un ai-semi-anneau si et seulement si le ai-semi-anneau satisfait à la fois l'inégalité $\mathbf{W} \preccurlyeq \mathbf{W}'$ et l'inégalité opposée $\mathbf{W}' \preccurlyeq \mathbf{W}$.

2 Caractériser les inégalités et les identités dans $(T_n,+,\cdot)$ et $(T_n,\cdot)$

Théorème 2.1. *Le ai-semi-anneau* [*semi-groupe ordonné*] *de toutes les matrices triangulaires supérieures booléennes $n \times n$ satisfait une inégalité de semi-anneau* [*respectivement de semi-groupe*] *si et seulement si tout mot de longueur $k < n$ qui apparaît du côté gauche de l'inégalité avec des sauts $G_1, G_2, \ldots, G_{k+1}$ apparaît du côté droit de l'inégalité avec des sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1,2,\ldots,k+1$.*

Démonstration. Les inégalités de semi-groupe sont des instances particulières de celles de semi-anneau, donc nous ne considèrerons que ce dernier cas dans la preuve.

Condition nécessaire. Prenons une inégalité $\mathbf{W} \preccurlyeq \mathbf{W}'$ vérifiée dans le ai-semi-anneau $(T_n,+,\cdot)$ de toutes les matrices triangulaires supérieures booléennes $n \times n$ et considérons un mot quelconque $\mathbf{u}$ de longueur $k < n$ qui apparaît dans $\mathbf{W}$ avec certains sauts $G_1, G_2, \ldots, G_{k+1}$. Cela signifie que $\mathbf{u}$ apparaît avec ces sauts dans un certain sommant du polynôme $\mathbf{W}$. On fixe un tel sommant $\mathbf{w}$ et une occurrence de $\mathbf{u}$ dans le mot $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_{k+1}$.

On souhaite définir une substitution spécifique $\operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}') \to T_n$, pour laquelle on a besoin de notations. Notons e_{ij} la $(i,j)^{\text{ieme}}$ *unité matricielle*, i.e., la matrice $n \times n$ avec un 1 en position (i,j) et un 0 partout ailleurs. La *matrice zéro*, i.e. la matrice $n \times n$ avec des 0 dans toutes les positions sera notée simplement 0 mais cela ne devrait pas porter à confusion. Si le mot $\mathbf{u}$ est non vide, on dénote par u_ℓ sa ℓ^{me} variable à partir de la gauche, de telle façon que $\mathbf{u} = u_1 \cdots u_k$. Maintenant définissons une substitution $\varphi\colon \operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}') \to T_n$ comme suit :

$$x\varphi := \begin{cases} \sum_{x \in G_\ell} e_{\ell\ell} + \sum_{x=u_\ell} e_{\ell\ell+1} & \text{si } x \in \operatorname{alph}(\mathbf{w}), \\ 0 & \text{si } x \in (\operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}')) \setminus \operatorname{alph}(\mathbf{w}). \end{cases} \tag{3}$$

Pour une variable $x \in \operatorname{alph}(\mathbf{w})$, la règle (3) revient à dire que la matrice $x\varphi$ a des 1 dans la diagonale principale et dans la sur-diagonale seulement, l'entrée de la sur-diagonale $(x\varphi)_{\ell\ell+1}$ étant égale à 1 si et seulement si x apparaît dans la ℓ^{ieme} position à partir de la position à l'extrême gauche du mot $\mathbf{u}$ alors que l'élément diagonal $(x\varphi)_{\ell\ell}$ est égal à 1 si et seulement si x apparaît dans le saut G_ℓ de l'occurrence choisie de $\mathbf{u}$ dans $\mathbf{w}$. Par exemple, si $k = 3$ et $n = 4$, disons, et si x apparaît dans le mot $\mathbf{w}$ comme cela est montré par les flèches dans le schéma suivant :

$$\mathbf{w} = \overset{x}{\downarrow}\mathbf{w}_1\, u_1 \mathbf{w}_2\, \overset{x}{\downarrow} u_2\, \mathbf{w}_3\, \overset{x}{\downarrow} u_3 \overset{x}{\downarrow} \mathbf{w}_3,$$

alors

$$x\varphi = e_{11} + e_{23} + e_{34} + e_{44} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Écrivons le mot $\mathbf{w}$ comme un produit de variables, $\mathbf{w} = w_1 \cdots w_m$, et posons $w_s\varphi = \left(\alpha_{ij}^{(s)}\right)_{n\times n}$ pour chaque $s = 1, \ldots, m$. Puisque toutes les matrices $\left(\alpha_{ij}^{(s)}\right)_{n\times n}$ sont des matrices triangulaires supérieures, on obtient le développement suivant de l'entrée de la matrice $\mathbf{w}\varphi$ dans la position $(1, k+1)$:

$$\left(\mathbf{w}\varphi\right)_{1\,k+1} = \sum_{1\le j_1\le\cdots\le j_{m-1}\le k+1} \alpha_{1j_1}^{(1)}\alpha_{j_1j_2}^{(2)}\cdots\alpha_{j_{m-1}k+1}^{(m)}. \tag{4}$$

Si $k = 0$ (c'est-à-dire si le mot $\mathbf{u}$ est vide), alors, la somme du côté droit de (4) se réduit au produit $\alpha_{11}^{(1)}\alpha_{11}^{(2)}\cdots\alpha_{11}^{(m)}$. Par la règle (3), $x\varphi = e_{11}$ pour tout $x \in G_1 = \mathrm{alph}(\mathbf{w})$, par conséquent $\alpha_{11}^{(s)} = 1$ pour tout $s = 1, \ldots, m$. Donc, $\left(\mathbf{w}\varphi\right)_{11} = \alpha_{11}^{(1)}\alpha_{11}^{(2)}\cdots\alpha_{11}^{(m)} = 1$.

Maintenant supposons $k > 0$. Puisque $\mathbf{u} = u_1 \cdots u_k$ apparaît dans $\mathbf{w}$ avec des sauts $G_1, G_2, \ldots, G_{k+1}$, il existe une séquence $1 \le s_1 < \cdots < s_k \le m$ telle que $u_\ell = w_{s_\ell}$ pour tout $\ell = 1, \ldots, k$, et de plus, si on pose $s_0 := 0$ et $s_{k+1} := m+1$, alors $\mathrm{alph}(w_{s_{\ell-1}+1}\cdots w_{s_\ell-1}) = G_\ell$ pour tout $\ell = 1, \ldots, k+1$. Alors la règle (3) implique que tous les facteurs dans le produit

$$\alpha_{11}^{(1)}\cdots\alpha_{11}^{(s_1-1)}\alpha_{12}^{(s_1)}\alpha_{22}^{(s_1+1)}\cdots\alpha_{22}^{(s_2-1)}\alpha_{23}^{(s_2)}\cdots\alpha_{kk}^{(s_{k-1}+1)}\cdots\alpha_{kk}^{(s_k-1)}\alpha_{kk+1}^{(s_k)}\alpha_{k+1k+1}^{(s_k+1)}\cdots\alpha_{k+1k+1}^{(m)}$$

sont égaux à 1, par conséquent, le produit lui-même est égal à 1 ainsi que la somme du côté droit de (4) dont ce produit est l'un des sommants. Donc, $\left(\mathbf{w}\varphi\right)_{1\,k+1} = 1$, et par conséquent, $\left(\mathbf{W}\varphi\right)_{1\,k+1} = 1$ puisque la matrice $\mathbf{w}\varphi$ est l'un des sommants de la matrice $\mathbf{W}\varphi$.

Puisque l'inégalité $\mathbf{W} \preccurlyeq \mathbf{W}'$ est vérifiée dans le ai-semi-anneau $(T_n, +, \cdot)$, on a $\mathbf{W}\varphi \le \mathbf{W}'\varphi$. La signification de l'ordre pour les matrices booléennes est assez transparent : $A \le B$ si et seulement si la matrice B a des 1 dans toutes les positions dans lesquelles la matrice A a des 1. On conclut que $\left(\mathbf{W}'\varphi\right)_{1\,k+1} = 1$, par conséquent $\left(\mathbf{w}'\varphi\right)_{1\,k+1} = 1$ pour un certain sommant $\mathbf{w}'$ du polynôme $\mathbf{W}'$.

Écrivons le mot $\mathbf{w}'$ comme un produit de variables, $\mathbf{w}' = w'_1 \cdots w'_{m'}$, et posons $w'_t\varphi = \left(\beta_{ij}^{(t)}\right)_{n\times n}$ pour tout $t = 1, \ldots, m'$. L'entrée de la matrice $\mathbf{w}'\varphi$ dans la position $(1, k+1)$ exprime que :

$$\left(\mathbf{w}'\varphi\right)_{1\,k+1} = \sum_{1\le j_1\le\cdots\le j_{m'-1}\le k+1} \beta_{1j_1}^{(1)}\beta_{j_1j_2}^{(2)}\cdots\beta_{j_{m'-1}\,k+1}^{(m')}.$$

Pour que cette somme soit égale à 1, il doit y avoir un sommant égal à 1. Considérons certains indices $j_1, \ldots, j_{m'-1}$ tels que

$$\beta_{1j_1}^{(1)}\beta_{j_1j_2}^{(2)}\cdots\beta_{j_{m'-1}\,k+1}^{(m')} = 1. \tag{5}$$

Par la règle (3), $x\varphi = 0$ pour tout $x \in \mathrm{alph}(\mathbf{W}) \setminus \mathrm{alph}(\mathbf{w})$, alors qu'à partir de (5), on voit que $x\varphi \ne 0$ pour tout $x \in \mathrm{alph}(\mathbf{w}')$. On conclut que $\mathrm{alph}(\mathbf{w}') \subseteq \mathrm{alph}(\mathbf{w})$. Ceci prouve notre assertion pour le cas où $\mathbf{u}$ est vide : en effet, par la convention que nous avons adoptée, le mot vide apparaît comme sous-mot dans $\mathbf{w}$ avec le saut $G_1 = \mathrm{alph}(\mathbf{w})$ et dans $\mathbf{w}'$ avec le saut $G'_1 = \mathrm{alph}(\mathbf{w}')$ donc $G'_1 \subseteq G_1$ comme souhaité.

Alors, supposons $k > 0$. Comme les matrices de la forme $x\varphi$ peuvent avoir des 1 dans la diagonale principale et dans la sur-diagonale seulement, $\beta_{ij}^{(t)} = 0$ à chaque fois que $j \neq i, i+1$. Par conséquent, pour que l'égalité (5) soit vérifiée, toutes les inégalités strictes dans la séquence $j_0 := 1 \leq j_1 \leq \cdots \leq j_{m'-1} \leq k+1 =: j_{m'}$ doivent être de la forme $j_r < j_{r+1} = j_r + 1$. Pour monter de $j_0 = 1$ à $j_{m'} = k+1$, on a besoin d'exactement k étapes de j_r à $j_{r+1} = j_r + 1$. Pour $\ell = 1, \ldots, k$, soit t_ℓ la position de la ℓ^{ieme} à partir de la gauche d'une telle étape. On voit que le produit $\beta_{1j_1}^{(1)} \beta_{j_1 j_2}^{(2)} \cdots \beta_{j_{m'-1} k+1}^{(m')}$ doit avoir la forme

$$\beta_{11}^{(1)} \cdots \beta_{11}^{(t_1-1)} \beta_{12}^{(t_1)} \beta_{22}^{(t_1+1)} \cdots \beta_{22}^{(t_2-1)} \beta_{23}^{(t_2)} \cdots \beta_{kk}^{(t_{k-1}+1)} \cdots \beta_{kk}^{(t_k-1)} \beta_{kk+1}^{(t_k)} \beta_{k+1k+1}^{(t_k+1)} \cdots \beta_{k+1k+1}^{(m')},$$

avec tous les facteurs égaux à 1. Par la règle (3), l'égalité $\beta_{\ell\ell+1}^{(t_\ell)} = 1$ est seulement possible si $w'_{t_\ell} = u_\ell$. Cela fixe une occurrence du mot $\mathbf{u} = u_1 \cdots u_k$ comme sous-mot du mot $\mathbf{w}'$. Pour des raisons pratiques de notation, posons $t_0 := 0$ et $t_{k+1} := m'+1$. Maintenant pour chaque $\ell = 1, \ldots, k+1$, considérons le segment $\beta_{\ell\ell}^{(t_{\ell-1}+1)} \cdots \beta_{\ell\ell}^{(t_\ell-1)}$ du produit (2), c'est-à-dire, le ℓ^{ieme} à partir du segment gauche maximal de (2) dont les entrées proviennent des diagonales principales des matrices $w'_t\varphi$. Le segment $\beta_{\ell\ell}^{(t_{\ell-1}+1)} \cdots \beta_{\ell\ell}^{(t_\ell-1)}$ correspond au facteur $w'_{t_{\ell-1}+1} \cdots w'_{t_\ell-1}$ du mot $\mathbf{w}'$. Si $G'_\ell := \operatorname{alph}(w'_{t_{\ell-1}+1} \cdots w'_{t_\ell-1})$, alors les ensembles $G'_1, G'_2, \ldots, G'_{k+1}$ constituent des sauts correspondant à l'occurrence de $\mathbf{u}$ dans $\mathbf{w}'$ que l'on a juste fixée. On a $\beta_{\ell\ell}^{(t)} = 1$ pour tout $t_{\ell-1} < t < t_\ell$ mais par la règle (3), ceci est seulement possible si toutes les variables $w'_{t_{\ell-1}+1}, \ldots, w'_{t_\ell-1}$ appartiennent à l'ensemble G_ℓ. Par conséquent, $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, \ldots, k+1$.

Condition suffisante. Prenons deux polynômes $\mathbf{W}$ et $\mathbf{W}'$ avec la propriété que tout mot de longueur $k < n$ qui apparaît dans $\mathbf{W}$ avec des sauts $G_1, G_2, \ldots, G_{k+1}$ apparaît dans $\mathbf{W}'$ avec des sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$. On a pour objectif de montrer que les ai-semi-anneaux $(T_n, +, \cdot)$ de toutes les matrices booléennes triangulaires supérieures $n \times n$ satisfont l'inégalité $\mathbf{W} \preccurlyeq \mathbf{W}'$, c'est-à-dire, $\mathbf{W}\varphi \leq \mathbf{W}'\varphi$ pour une substitution arbitraire $\varphi\colon \operatorname{alph}(\mathbf{W}) \cup \operatorname{alph}(\mathbf{W}') \to T_n$. Selon la signification de l'ordre (2) pour les matrices booléennes, on a besoin de montrer que $\big(\mathbf{W}'\varphi\big)_{pq} = 1$ à chaque fois que $\big(\mathbf{W}\varphi\big)_{pq} = 1$.

Fixons une paire d'indices (p, q) tels que $\big(\mathbf{W}\varphi\big)_{pq} = 1$. Il doit y avoir un sommant $\mathbf{w}$ du polynôme $\mathbf{W}$ tel que $\big(\mathbf{w}\varphi\big)_{pq} = 1$; on fixe un tel sommant. La matrice $\mathbf{w}\varphi$ est une matrice triangulaire supérieure, donc on a $p \leq q$.

Considérons d'abord le cas où $q = p$. Écrivons le mot $\mathbf{w}$ comme un produit de variables, $\mathbf{w} = w_1 \cdots w_m$, et posons $w_s\varphi = \big(\alpha_{ij}^{(s)}\big)_{n\times n}$ pour chaque $s = 1, \ldots, m$. Clairement, pour chaque $p = 1, \ldots, n$,

$$\big(\mathbf{w}\varphi\big)_{pp} = \prod_{1 \leq s \leq m} \alpha_{pp}^{(s)},$$

et par conséquent, $\big(\mathbf{w}\varphi\big)_{pp} = 1$ implique $\big(x\varphi\big)_{pp} = 1$ pour chaque variable $x \in \operatorname{alph}(\mathbf{w})$. Par notre convention, le mot vide apparaît comme sous-mot dans $\mathbf{w}$ avec saut $G_1 = \operatorname{alph}(\mathbf{w})$. Alors il doit apparaître dans un certain sommant $\mathbf{w}'$ du polynôme $\mathbf{W}'$ avec saut $G'_1 = \operatorname{alph}(\mathbf{w}')$ tel que $G'_1 \subseteq G_1$. Par conséquent $\operatorname{alph}(\mathbf{w}') \subseteq \operatorname{alph}(\mathbf{w})$, ce qui assure que $\big(\mathbf{w}'\varphi\big)_{pp} = 1$.

Ainsi, on peut supposer que $p < q$ pour le reste de la démonstration. Alors

$$\big(\mathbf{w}\varphi\big)_{pq} = \sum_{p \leq j_1 \leq \cdots \leq j_{m-1} \leq q} \alpha_{p j_1}^{(1)} \alpha_{j_1 j_2}^{(2)} \cdots \alpha_{j_{m-1} q}^{(m)},$$

et puisque la somme du côté droit est égale à 1, il en est de même de l'un de ses sommants. Définissons le produit $\alpha^{(1)}_{p\,j_1}\alpha^{(2)}_{j_1\,j_2}\cdots\alpha^{(m)}_{j_{m-1}\,q}$ comme étant l'un de ces sommants. Pour que la notation soit pratique, posons $j_0 := p$ et $j_m := q$. Puisque $p < q$, parmi les inégalités $j_0 \le j_1 \le \cdots \le j_{m-1} \le j_m$, certaines doivent être des inégalités strictes. Soient $j_{s_1-1} < j_{s_1}$, $j_{s_2-1} < j_{s_2}$, …, $j_{s_k-1} < j_{s_k}$ toutes les inégalités strictes et appelons $d_\ell := j_{s_\ell} - j_{s_\ell-1}$ pour chacune d'entre elles avec $\ell = 1,\ldots,k$. Alors le produit choisi peut s'écrire

$$\alpha^{(1)}_{p\,p}\cdots\alpha^{(s_1-1)}_{p\,p}\alpha^{(s_1)}_{p\;p+d_1}\alpha^{(s_1+1)}_{p+d_1\,p+d_1}\cdots\alpha^{(s_2-1)}_{p+d_1\,p+d_1}\alpha^{(s_2)}_{p+d_1\,p+d_1+d_2}\cdots$$
$$\alpha^{(s_{k-1}+1)}_{q-d_k\,q-d_k}\cdots\alpha^{(s_{k-1}-1)}_{q-d_k\,q-d_k}\alpha^{(s_k)}_{q-d_k\;q}\alpha^{(s_k+1)}_{q\,q}\cdots\alpha^{(m)}_{q\,q}.$$

Puisque le produit est égal à 1, il en est de même de l'un de ses facteurs. En particulier,

$$\alpha^{(s_1)}_{p\;p+d_1} = \alpha^{(s_2)}_{p+d_1\,p+d_1+d_2} = \cdots = \alpha^{(s_k)}_{q-d_k\;q} = 1. \tag{6}$$

Considérons le sous-mot $\mathbf{u} := w_{s_1}w_{s_2}\cdots w_{s_k}$ du mot $\mathbf{w}$. La longueur k de $\mathbf{u}$ est strictement inférieure à n ; en effet,

$$\begin{aligned}
k &= \sum_{1\le\ell\le k} 1 \le \sum_{1\le\ell\le k} d_\ell && \text{(puisque } d_\ell \ge 1 \text{ pour tout } \ell\text{)}\\
&= \sum_{1\le\ell\le k} (j_{s_\ell} - j_{s_\ell-1}) && \text{(par la définition de } d_\ell\text{)}\\
&= \sum_{1\le s\le m} (j_s - j_{s-1}) && \text{(on a ajouté des sommants nuls pour obtenir une somme télescopique)}\\
&= j_m - j_0 = q - p \le n-1.
\end{aligned}$$

Le mot $\mathbf{u}$ apparaît dans $\mathbf{w}$ avec les sauts $G_\ell := \mathrm{alph}(\prod_{s_{\ell-1}<s<s_\ell} w_s)$, où $\ell = 1,2,\ldots,k+1$ et on définit $s_0 := 0$ et $s_{k+1} := m+1$ de telle façon que pour $\ell = 1$ et $\ell = m+1$, l'expression $\prod_{s_{\ell-1}<s<s_\ell} w_s$ représente le préfixe $w_1\cdots w_{s_1-1}$ et, respectivement, le suffixe $w_{s_k+1}\cdots w_m$ du mot $\mathbf{w}$. Par la condition, $\mathbf{u}$ doit apparaître dans un certain sommant du polynôme $\mathbf{W}'$ avec les sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tel que $G'_\ell \subseteq G_\ell$ pour chaque $\ell = 1,2,\ldots,k+1$. Par abus de notation, on désigne ce sommant par $\mathbf{w}'$ même s'il ne doit pas être le même que celui utilisé dans l'analyse ci-dessus du cas où $q = p$.

Fixons une occurrence de $\mathbf{u}$ comme sous-mot dans $\mathbf{w}'$ avec $G'_1, G'_2, \ldots, G'_{k+1}$. Écrivons le mot $\mathbf{w}'$ comme un produit de variables, $\mathbf{w}' = w'_1\cdots w'_{m'}$, et appelons $t_1, t_2, \ldots, t_k$ les positions correspondant à l'occurrence choisi de $\mathbf{u}$ dans $\mathbf{w}'$. Cela signifie que, d'abord, $w'_{t_\ell} = w_{s_\ell}$ pour tout $\ell = 1,2,\ldots,k$, et deuxièmement, $G'_\ell := \mathrm{alph}(\prod_{t_{\ell-1}<t<t_\ell} w'_t) \subseteq G_\ell$, où $\ell = 1,2,\ldots,k+1$ et, similairement à ci-dessus, on pose $t_0 := 0$ et $t_{k+1} := m'+1$ pour rendre compte de tous les sauts dans une expression uniforme, incluant les extrêmes G'_1 et G'_{k+1}. Dans le schéma ci-dessous, les mots $\mathbf{w}$ et $\mathbf{w}'$ sont alignés sur leur sous-mot commun $\mathbf{u}$, avec les deux séquences de sauts explicitement écrites.

$$\begin{array}{ccccccccccccc}
\overbrace{w_1\cdots w_{s_1-1}}^{G_1=\mathrm{alph}(w_1\cdots w_{s_1-1})} & \cdot & w_{s_1} & \cdot & \overbrace{w_{s_1+1}\cdots w_{s_2-1}}^{G_2=\mathrm{alph}(w_{s_1+1}\cdots w_{s_2-1})} & \cdot & w_{s_2} & \ldots & w_{s_k} & \cdot & \overbrace{w_{s_k+1}\cdots w_m}^{G_{k+1}=\mathrm{alph}(w_{s_k+1}\cdots w_m)} \\
 & & \| & & & & \| & \ldots & \| & & \\
\underbrace{w'_1\cdots w'_{t_1-1}}_{G'_1=\mathrm{alph}(w'_1\cdots w'_{t_1-1})} & \cdot & w'_{t_1} & \cdot & \underbrace{w'_{t_1+1}\cdots w'_{t_2-1}}_{G'_2=\mathrm{alph}(w'_{t_1+1}\cdots w'_{t_2-1})} & \cdot & w'_{t_2} & \ldots & w'_{t_k} & \cdot & \underbrace{w'_{t_k+1}\cdots w'_{m'}}_{G'_{k+1}=\mathrm{alph}(w'_{t_k+1}\cdots w'_{m'})}
\end{array}$$

Soit $w'_t\varphi = \left(\beta_{ij}^{(t)}\right)_{n\times n}$ pour tout $t = 1,\ldots,m'$ et considérons le produit

$$\beta_{pp}^{(1)}\cdots\beta_{pp}^{(t_1-1)}\beta_{p\,p+d_1}^{(t_1)}\beta_{p+d_1\,p+d_1}^{(t_1+1)}\cdots\beta_{p+d_1\,p+d_1}^{(t_2-1)}\beta_{p+d_1\,p+d_1+d_2}^{(t_2)}\cdots$$

$$\beta_{q-d_k\,q-d_k}^{(t_{k-1}+1)}\cdots\beta_{q-d_k\,q-d_k}^{(t_{k-1}-1)}\beta_{q-d_k\,q}^{(t_k)}\beta_{qq}^{(t_k+1)}\cdots\beta_{qq}^{(m')},$$

qui apparaît comme l'un des sommants dans le développement de $\left(\mathbf{w}'\varphi\right)_{pq}$ via les éléments des matrices $\left(\beta_{ij}^{(t)}\right)_{n\times n}$, $t = 1,\ldots,m'$. On a pour objectif de montrer que le produit (2) est égal à 1, ce qui amènera l'égalité $\left(\mathbf{w}'\varphi\right)_{pq} = 1$.

Les égalités $w'_{t_\ell} = w_{s_\ell}$ impliquent les égalités matricielles $\left(\beta_{ij}^{(t_\ell)}\right)_{n\times n} = \left(\alpha_{ij}^{(s_\ell)}\right)_{n\times n}$ pour chaque $\ell = 1,2,\ldots,k$. Par conséquent, de (6), on obtient

$$\beta_{p\,p+d_1}^{(t_1)} = \beta_{p+d_1\,p+d_1+d_2}^{(t_2)} = \cdots = \beta_{q-d_k\,q}^{(t_k)} = 1,$$

c'est-à-dire que tous les facteurs du produit (2) qui ne sont pas sur les diagonales principales des matrices impliquées dans le produit sont égaux à 1. Il reste à comprendre pourquoi les facteurs des diagonales principales sont aussi égaux à 1.

Du fait que le produit (2) est égal à 1, on conclut que si x est une variable de saut G_ℓ, alors $\left(x\varphi\right)_{j\,j} = 1$ pour tout $j_{s_{\ell-1}} \le j \le j_{s_\ell-1}$ et $\ell = 1,2,\ldots,k+1$ (rappelons-nous que nous avons posé $s_0 = 0$ et $s_{k+1} = m+1$ alors que $j_0 = p$ et $j_m = q$ de telle façon que $j_{s_0} = j_0 = p$ et $j_{s_{k+1}-1} = j_m = q$). Puisque $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1,2,\ldots,k+1$ et $G'_\ell = \mathrm{alph}(\prod_{t_{\ell-1}<t<t_\ell} w'_t)$, on voit que chaque variable w'_t avec $t_{\ell-1} < t < t_\ell$ appartient à G_ℓ. Donc $\left(w'_t\varphi\right)_{j\,j} = \beta_{j\,j}^{t} = 1$ pour tout $t_{\ell-1} < t < t_\ell$ et $j_{t_{\ell-1}} \le j \le j_{t_\ell-1}$. Dans la notation utilisée dans (2), cela signifie que $\beta_{pp}^{(t)} = 1$ pour $t = 1,\ldots,t_1-1$, $\beta_{p+d_1\,p+d_1}^{(t)} = 1$ pour $t = t_1+1,\ldots,t_2-1$, …, $\beta_{qq}^{(t)} = 1$ pour $t = t_k+1,\ldots,m'$. Par conséquent, tous les facteurs dans le produit (2) sont égaux à 1 alors que $\left(\mathbf{w}'\varphi\right)_{pq} = 1$. Cela implique que $\left(\mathbf{W}'\varphi\right)_{pq} = 1$ comme souhaité. □

Une caractérisation des identités vérifiées dans les ai-semi-anneaux $(T_n,+,\cdot)$ ou le semi-groupe $(T_n,\cdot)$ en découle immédiatement.

Corollaire 2.2. *Les ai-semi-anneaux* [*semi-groupes*] *de toutes les matrices booléennes triangulaires supérieures $n\times n$ satisfont une identité de semi-anneau* [*respectivement, de semi-groupe*] *si et seulement si tout mot de longueur $k < n$ qui apparaît d'un côté de l'identité avec les sauts $G_1,G_2,\ldots,G_{k+1}$ apparaît de l'autre côté de l'identité avec les sauts $G'_1,G'_2,\ldots,G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1,2,\ldots,k+1$.*

Remarque : alors que les inclusions entre les sauts semblent concorder pour les inégalités caractérisantes de $(T_n,+,\cdot)$ et $(T_n,\cdot)$, on aurait pu s'attendre à ce que les identités $(T_n,+,\cdot)$ et $(T_n,\cdot)$ n'aient pas pu être caractérisées en fonction des égalités entre les sauts plutôt qu'entre les inclusions. Cela n'est pas le cas, comme nous allons le montrer maintenant. Nous nous restreignons aux identités de semi-groupes pour des raisons de simplicité mais la situation avec les semi-anneaux est la même.

Le corollaire 2.2 implique facilement que toute identité $\mathbf{w} \eqsim \mathbf{w}'$ vérifiée dans le semi-groupe de toutes les matrices triangulaires supérieures booléennes $n\times n$ satisfait la condition suivante $\exists\mathrm{EG}_n$ (existence de sauts identiques) :

$\exists\mathrm{EG}_n$: tout sous-mot commun de $\mathbf{w}$ et $\mathbf{w}'$ de longueur $k < n$ apparaît dans $\mathbf{w}$ et $\mathbf{w}'$ avec les mêmes sauts.

En effet, soit un mot $\mathbf{u}$ de longueur $k < n$ apparaissant dans $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_{k+1}$. Alors, par le corollaire 2.2, $\mathbf{u}$ doit apparaître dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$. Si l'une quelconque des inclusions $G'_\ell \subseteq G_\ell$ est une inclusion stricte, on applique le corollaire de cette occurrence de $\mathbf{u}$ dans $\mathbf{w}'$ et on obtient l'occurrence de $\mathbf{u}$ dans $\mathbf{w}$ avec $G''_1, G''_2, \ldots, G''_{k+1}$ tels que $G''_\ell \subseteq G'_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$, et etc. Puisque tous les sauts sont des ensembles finis, ce "processus" de "laçage de chaussures" s'arrête finalement sur certaines occurrences de $\mathbf{u}$ dans $\mathbf{w}$ et $\mathbf{w}'$ ayant les mêmes sauts.

Pourtant, la condition $\exists\mathrm{EG}_n$ n'est pas suffisante pour qu'une identité soit vérifiée dans le semi-groupe $(T_n, \cdot)$. Par exemple, l'identité $xyx^2yx \doteq xyxyx$ échoue dans $(T_3, \cdot)$ puisque, par la substitution

$$x \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

la valeur du mot xyx^2yx est la matrice $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ alors que la valeur du mot $xyxyx$ est la matrice $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. En même temps, une inspection directe montre que l'identité satisfait la condition $\exists\mathrm{EG}_3$.

D'un autre côté, par le Corollaire 2.2, la condition suivante $\forall\mathrm{EG}_n$ (tous les sauts sont égaux) est suffisante pour qu'une identité $\mathbf{w} \doteq \mathbf{w}'$ soit vérifiée dans $(T_n, \cdot)$:

$\forall\mathrm{EG}_n$: pour toute occurrence d'un sous-mot de longueur $k < n$ dans l'un des mots $\mathbf{w}$ et $\mathbf{w}'$, il existe une occurrence du sous-mot d'un autre mot avec les mêmes sauts.

Pourtant, la condition $\forall\mathrm{EG}_n$ n'est pas nécessaire. Par exemple, on voit facilement que l'identité $x^2yx \doteq xyx$ est vérifiée dans le semi-groupe $(T_2, \cdot)$ et en même temps, le mot x de longueur 1 apparaît avec les sauts $\{x\}, \{x, y\}$ dans le mot $x^2yx = x \cdot \underline{x} \cdot yx$, mais non pas dans le mot xyx. Ainsi, $\forall\mathrm{EG}_2$ échoue pour cette identité.

On a pour objectif de légèrement modifier le critère du théorème 2.1 pour les inégalités de semi-groupes. Pour cela, on a besoin de deux lemmes.

Lemme 2.3. *Soit k un entier positif et $\mathbf{w}$ un mot de longueur au moins égale à k. Supposons qu'un mot $\mathbf{w}'$ soit tel que tout mot de longueur k qui apparaît dans $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_{k+1}$ apparaisse également dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$. Alors, tout mot de longueur $k-1$ qui apparaît dans $\mathbf{w}$ avec les sauts $H_1, H_2, \ldots, H_k$ apparaît dans $\mathbf{w}'$ avec les sauts $H'_1, H'_2, \ldots, H'_k$ tels que $H'_j \subseteq H_j$ pour tout $j = 1, 2, \ldots, k$.*

Démonstration. Soit $\mathbf{u} = u_1 \cdots u_{k-1}$ apparaissant comme sous-mot dans $\mathbf{w}$ avec les sauts $H_1, H_2, \ldots, H_k$. Cela signifie qu'il existe des mots $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$ (certains d'entre eux pouvant être vides) tels que

$$\mathbf{w} = \mathbf{w}_1 u_1 \mathbf{w}_2 \cdots u_{k-1} \mathbf{w}_k$$

et $H_i = \mathrm{alph}(\mathbf{w}_i)$ pour tout $i = 1, 2, \ldots, k$. Comme $|\mathbf{w}| \geq k$, au moins l'un des sauts $H_1, H_2, \ldots, H_k$ est non vide. Fixons un indice i tel que le saut H_i est non vide et choisissons une variable arbitraire $t \in H_i$. Alors le mot $\mathbf{w}_i$ peut se décomposer en $\mathbf{w}_i = \mathbf{y}t\mathbf{z}$ pour certains mots (possiblement vides) $\mathbf{y}$ et $\mathbf{z}$. Le mot

$$\mathbf{v} := \begin{cases} tu_1 \cdots u_{k-1} & \text{si } i = 1, \\ u_1 \cdots u_{i-1} t u_i \cdots u_{k-1} & \text{si } 1 < i < k, \\ u_1 \cdots u_{k-1} t & \text{si } i = k \end{cases}$$

est de longueur k et apparaît comme sous-mot dans le mot $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_{k+1}$, où pour chaque $\ell = 1, 2, \ldots, k+1$,

$$G_\ell = \begin{cases} H_\ell & \text{si } \ell < i, \\ \mathrm{alph}(\mathbf{y}) & \text{si } \ell = i, \\ \mathrm{alph}(\mathbf{z}) & \text{si } \ell = i+1, \\ H_{\ell-1} & \text{si } \ell > i+1. \end{cases}$$

La ligne du haut du schéma ci-dessous montre les occurrences de $\mathbf{u}$ et $\mathbf{v}$ dans le mot $\mathbf{w}$ et les sauts correspondant à ces occurrences dans le cas où $1 < i < k$. Dans ce schéma, un symbole placé au-dessus ou au-dessous dénote l'alphabet du mot surmonté ou souligné d'une accolade.

$$\begin{array}{rccccccccccccccc} \mathbf{w} = & \overbrace{\underbrace{\mathbf{w}_1}_{G_1}}^{H_1} & \cdot & u_1 & \ldots & u_{i-1} & \cdot & \overbrace{\underbrace{\mathbf{y}}_{G_i} \cdot t \cdot \underbrace{\mathbf{z}}_{G_{i+1}}}^{H_i} & \cdot & u_i & \ldots & u_k & \cdot & \overbrace{\underbrace{\mathbf{w}_k}_{G_{k+1}}}^{H_k} \\ & \cup\mid & & & \ldots & & & \cup\mid \quad \cup\mid & & & \ldots & & & \cup\mid \\ \mathbf{w}' = & \overbrace{\underbrace{\mathbf{w}'_1}_{H'_1}}^{G'_1} & \cdot & u_1 & \ldots & u_{i-1} & \cdot & \underbrace{\overbrace{\mathbf{y}'}^{G'_i} \cdot t \cdot \overbrace{\mathbf{z}'}^{G'_{i+1}}}_{H'_i} & \cdot & u_i & \ldots & u_k & \cdot & \underbrace{\overbrace{\mathbf{w}'_k}^{G'_{k+1}}}_{H'_k} \end{array}$$

Par la condition du lemme, le mot $\mathbf{v}$ apparaît comme sous-mot dans le mot $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$.

L'occurrence de $\mathbf{v}$ dans $\mathbf{w}'$ entraîne une occurrence de $\mathbf{u}$ dans $\mathbf{w}'$ avec les sauts $H'_1, H'_2, \ldots, H'_k$, où pour chaque $j = 1, 2, \ldots, k$,

$$H'_j = \begin{cases} G'_j & \text{si } j < i, \\ G'_i \cup \{t\} \cup G'_{i+1} & \text{si } j = i, \\ G'_{j+1} & \text{si } j > i. \end{cases}$$

Pour le cas $1 < i < k$, les occurrences de $\mathbf{u}$ et $\mathbf{v}$ dans le mot $\mathbf{w}'$ et les sauts correspondant à ces occurrences sont montrées dans la ligne du bas du schéma ci-dessus. Clairement, les inclusions $G'_\ell \subseteq G_\ell$ pour $\ell = 1, 2, \ldots, k+1$ impliquent les inclusions $H'_j \subseteq H_j$ pour $j = 1, 2, \ldots, k$. □

Un mot $\mathbf{w}$ est *minimal* [*maximal*] pour un semi-groupe ordonné $(S, \cdot, \leq)$ si le seul mot $\mathbf{w}'$ tel que $(S, \cdot, \leq)$ satisfait l'inégalité $\mathbf{w}' \preccurlyeq \mathbf{w}$ [respectivement, $\mathbf{w} \preccurlyeq \mathbf{w}'$] est le mot $\mathbf{w}$ lui-même.

Lemme 2.4. *Les mots de longueur inférieure à n sont maximaux pour le semi-groupe ordonné* $(T_n, \cdot, \leq)$.

Démonstration. Prenons n'importe quel mot $\mathbf{w} = w_1 \cdots w_k$ avec $k < n$, et supposons qu'un mot $\mathbf{w}'$ est tel que l'inégalité $\mathbf{w} \preccurlyeq \mathbf{w}'$ est vérifiée dans $(T_n, \cdot, \leq)$. Le mot $\mathbf{w}$ apparaît comme sous-mot de lui-même avec tous les sauts $G_1, G_2, \ldots, G_{k+1}$ vides. Par le théorème 2.1, $\mathbf{w}$ doit apparaître comme sous-mot dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_{k+1}$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, k+1$. Puisque G_ℓ est vide, il en est de même de G'_ℓ. Ainsi, il y a une occurrence de $w_1 \cdots w_k$ comme sous-mot dans $\mathbf{w}'$ dans laquelle rien ne précède w_1, rien ne suit w_k, et rien n'apparaît entre w_i et w_{i+1} pour tout $i = 1, 2, \ldots, k-1$. Ceci est seulement possible si $\mathbf{w}' = w_1 \cdots w_k$. □

Théorème 2.5. *Le semi-groupe ordonné de toutes les matrices booléennes triangulaires supérieures $n \times n$ satisfait une inégalité $\mathbf{w} \preccurlyeq \mathbf{w}'$ si et seulement si $\mathbf{w} = \mathbf{w}'$ ou $|\mathbf{w}| \geq n$ et tout mot de longueur $n-1$ qui apparaît dans $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_n$ apparaît dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_n$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, n$.*

Démonstration. Condition nécessaire. Supposons que $\mathbf{w} \neq \mathbf{w}'$. Alors le lemme 2.4 assure que $|\mathbf{w}| \geq n$. Le fait que tout mot de longueur $n-1$ apparaissant dans $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_n$ apparaisse dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_n$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, n$ est un cas particulier de la condition établie dans le théorème 2.1.

Condition suffisante. Si $\mathbf{w} = \mathbf{w}'$, il n'y a rien à démontrer. Ainsi, supposons que $|\mathbf{w}| \geq n$ et que tout mot de longueur $n-1$ qui arrive dans $\mathbf{w}$ avec les sauts $G_1, G_2, \ldots, G_n$ apparaisse dans $\mathbf{w}'$ avec les sauts $G'_1, G'_2, \ldots, G'_n$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, n$. En appliquant le lemme 2.3 pour $k = n-1, n-2, \ldots, 1$ dans les suites, on obtient que tout mot de longueur $k < n$ apparaissant dans $\mathbf{w}$ avec les sauts $H_1, H_2, \ldots, H_{k+1}$ apparaît également dans $\mathbf{w}'$ avec les sauts $H'_1, H'_2, \ldots, H'_{k+1}$ de telle façon que $H'_j \subseteq H_j$ pour tout $j = 1, 2, \ldots, k+1$. Alors l'inégalité $\mathbf{w} \preccurlyeq \mathbf{w}'$ est vérifiée dans $(T_n, \cdot, \leq)$ par le théorème 2.1. □

Une caractérisation des identités qui sont vérifiées dans le semi-groupe $(T_n, \cdot)$ est immédiate.

Corollaire 2.6. *Le semi-groupe de toutes les matrices booléennes triangulaires supérieures $n \times n$ satisfait une identité $\mathbf{w} \doteq \mathbf{w}'$ si et seulement si soit $\mathbf{w} = \mathbf{w}'$ soit $|\mathbf{w}| \geq n$ et tout mot de longueur $n-1$ qui apparaît dans l'un des mots $\mathbf{w}$ et $\mathbf{w}'$ avec les sauts $G_1, G_2, \ldots, G_n$ apparaît dans l'autre mot avec les sauts $G'_1, G'_2, \ldots, G'_n$ tels que $G'_\ell \subseteq G_\ell$ pour tout $\ell = 1, 2, \ldots, n$.*

3 Applications

3.1 Complexité et vérification des identités

Ici, on suppose la familiarité des lecteurs et lectrices avec quelques notions de base de complexité calculatoire ; ces notions peuvent être retrouvées, par exemple, dans les premiers chapitres du livre de Papadimitriou [19].

Étant donné un semi-groupe $(S, \cdot)$, son *problème de vérification d'identité*[2] CHECK-ID$(S, \cdot)$ est le problème de décision suivant. L'instance de CHECK-ID$(S, \cdot)$ est une identité de semi-groupe $\mathbf{w} \doteq \mathbf{w}'$. La réponse à cette instance est "OUI" à chaque fois que l'indentité $\mathbf{w} \doteq \mathbf{w}'$ est vérifiée dans $(S, \cdot)$; sinon, la réponse est "NON".

On souligne le fait qu'ici le semi-groupe $(S, \cdot)$ est fixé et que c'est l'identité $\mathbf{w} \doteq \mathbf{w}'$ qui sert d'entrée de telle façon que la complexité en temps et espace de CHECK-ID$(S, \cdot)$ est mesurée en fonction de la taille de l'identité, c'est-à-dire dans $|\mathbf{w}\mathbf{w}'|$. Étudier la complexité calculatoire de la vérification des identités dans les semi-groupes a été proposé par Mark Sapir [16, Problème 2.4].

Pour un semi-groupe fini $(S, \cdot)$, le problème CHECK-ID$(S, \cdot)$ appartient à la classe de complexité coNP. En effet, si une identité $\mathbf{w} \doteq \mathbf{w}'$ échoue dans $(S, \cdot)$ et si les mots $\mathbf{w}$, $\mathbf{w}'$ font intervenir m variables au total,

2. également appelé le "*problème de l'équivalence de termes*" dans la littérature.

alors un algorithme non déterministe devine un m-uplet d'éléments en S témoins d'échec et il vérifie alors ce qu'il a deviné en calculant les valeurs des mots $\mathbf{w}$ et $\mathbf{w}'$ selon la substitution qui envoie les variables dans $\mathrm{alph}(\mathbf{w}) \cup \mathrm{alph}(\mathbf{w}')$ sur les entrées du m-uplet deviné. Si l'on suppose que la multiplication dans $(S, \cdot)$ est effectuée en une unité de temps, l'algorithme prend un temps linéaire en $|\mathbf{w}\mathbf{w}'|$.

Il y a de nombreux exemples de semi-groupes finis (et même de groupes finis) dont le problème de vérification d'identité est coNP-complet. On renvoie les lecteurs à [1] et aux références qui se trouvent dans ce livre pour des exemples particuliers et une discussion générale du point de vue de la complexité de la vérification des identités dans les semi-groupes finis. Ici, nous mentionnons seulement que ce problème de la vérification d'identité pour le semi-groupe de **toutes** les matrices booléennes $n \times n$ est coNP-complet à chaque fois que $n \geq 5$. Cela ne semble pas avoir été explicitement démontré dans la littérature, mais c'est une conséquence immédiate des deux faits suivants :

— si un semi-groupe fini possède un sous-groupe non résoluble, alors la vérification d'identité dans le semi-groupe est coNP-complète [1, Corollaire 1] ;
— pour tout $n \geq 5$, le semi-groupe de toutes les matrices booléennes $n \times n$ a un sous-groupe non résoluble, notamment le sous-groupe constitué de toutes les matrices $n \times n$ de permutation.

Par contraste, le corollaire 2.6 amène au résultat suivant :

Proposition 3.1. *Pour tout n, il existe un algorithme en temps polynomial qui décide si une identité est vérifiée dans le semi-groupe de toutes les matrices booléennes triangulaires supérieures $n \times n$.*

Démonstration. Prenons une identité arbitraire $\mathbf{w} \doteq \mathbf{w}'$ et posons $m := |\mathbf{w}\mathbf{w}'|$. Pour fixer une occurrence d'un sous-mot de longueur $n-1$ dans un mot, on doit choisir $n-1$ positions dans le mot. Par conséquent, le nombre de toutes les occurrences possibles de sous-mots de longueur $n-1$ dans chacun des mots $\mathbf{w}$ et $\mathbf{w}'$ est au plus $\binom{m-1}{n-1}$. Pour chaque occurrence, une étude de $\mathbf{w}$ et $\mathbf{w}'$ suffit à calculer les sauts correspondant. Ainsi, en temps $\leq 2(m-1)\binom{m-1}{n-1}$, qui est polynomial en m, on peut constituer deux listes contenant tous les sous-mots de longueur $n-1$ apparaissant dans $\mathbf{w}$ et $\mathbf{w}'$ avec des sauts pour chaque occurrence. En comparant les listes pour $\mathbf{w}$ et $\mathbf{w}'$, on peut vérifier la condition du corollaire 2.6, et par conséquent, on peut vérifier si l'identité $\mathbf{w} \doteq \mathbf{w}'$ est vérifiée dans le semi-groupe $(T_n, \cdot)$ en temps polynomial en m. □

Pour placer la proposition 3.1 dans un contexte plus large, mentionnons un résultat analogue pour les semi-groupes des matrices triangulaires supérieures tropicales $n \times n$. Le ai-semi-anneau *tropical* est constitué des nombres réels augmentés du symbole $-\infty$ équipé des opérations $a \oplus b := \max\{a, b\}$ et $a \otimes b := a + b$, pour lequel $-\infty$ joue le rôle de zéro : $a \oplus -\infty = -\infty \oplus a = a$ et $a \otimes -\infty = -\infty \otimes a = -\infty$. Une matrice carrée sur le ai-semi-anneau tropical est considérée comme étant *triangulaire supérieure* si ses éléments sous la diagonale principale sont tous égaux à $-\infty$. Le problème de la vérification de l'identité pour le semi-groupe des matrices tropicales triangulaires supérieures $n \times n$ a été intensivement étudié dans [5, 14] et il a été prouvé que ce problème est décidable en temps polynomial. Comparé à notre algorithme pour CHECK-ID$(T_n, \cdot)$, les algorithmes développés dans [5, 14] sont plus lourds et leur implémentation en temps polynomial dépend cruellement de l'existence d'un algorithme en temps polynomial pour la programmation linéaire (sur les réels). À nouveau, la logique sous-jacente est la même et l'utilisation de la triangularité dans notre algorithme et dans les algorithmes dans [5, 14] est assez similaire.

Ce que nous venons de dire ne devrait pas être compris comme le fait d'affirmer que les semi-groupes constitués de matrices triangulaires supérieures admettent toujours des algorithmes en temps polynomial pour vérifier les identités. Pour montrer que ça n'est pas le cas, on exhibe un sous-semi-groupe $(C_4, \cdot)$

de $(T_4,\cdot)$ avec une vérification d'identité coNP-complète. L'ensemble C_4 comprend les neuf matrices suivantes :

$$e=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\qquad a=\begin{pmatrix}1&1&0&0\\0&0&0&1\\0&0&0&0\\0&0&0&1\end{pmatrix},\qquad b=\begin{pmatrix}1&0&1&0\\0&0&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix},$$

$$a^2=\begin{pmatrix}1&1&0&1\\0&0&0&1\\0&0&0&0\\0&0&0&1\end{pmatrix},\qquad ab=\begin{pmatrix}1&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&1\end{pmatrix},\qquad ba=\begin{pmatrix}1&1&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix},$$

$$b^2=\begin{pmatrix}1&0&1&1\\0&0&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix},\qquad a^2b=\begin{pmatrix}1&0&1&1\\0&0&0&1\\0&0&0&0\\0&0&0&1\end{pmatrix},\qquad ba^2=\begin{pmatrix}1&1&0&1\\0&0&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix}.$$

On enregistre quelques propriétés de $(C_4,\cdot)$. Elles peuvent toutes être vérifiées par calcul direct.

1° Les égalités $aba=a$ et $bab=b$ sont vérifiées.

2° Excepté pour a et b, toutes les matrices $c\in C_4$ sont *idempotentes*, c'est-à-dire qu'elles satisfont $c^2=c$.

3° Pour tout $c\in C_4$, son carré c^2 est idempotent.

4° Tout produit de matrices idempotentes de C_4 est idempotent.

5° L'ensemble $I:=\{a^2,b^2,a^2b,ba^2\}$ de toutes les matrices ayant un 1 en position $(1,4)$ est un *idéal* dans $(C_4,\cdot)$, c'est-à-dire que $cd,dc\in I$ pour tout $c\in C_4$ et $d\in I$.

Proposition 3.2. *Le problème* CHECK-ID$(C_4,\cdot)$ *est* coNP*-complet.*

Démonstration. Comme mentionné au début de la section 3.1, le problème CHECK-ID$(S,\cdot)$ appartient à la classe coNP pour tout semi-groupe fini $(S,\cdot)$. Par conséquent, il suffit de montrer que le problème CHECK-ID$(C_4,\cdot)$ est coNP-difficile. Pour cela, on construit une réduction en temps polynomial de la négation de CHECK-ID$(C_4,\cdot)$ à partir du problème de l'ENSEMBLE INTERSECTANT dont il est connu qu'il est NP-complet [15, Théorème principal, item 15].

Une instance du problème de l'ENSEMBLE INTERSECTANT est une famille $\{U_i : i=1,\dots,q\}$ de sous-ensembles d'un ensemble fini $S=\{s_j : j=1,\dots,r\}$, et la question de savoir s'il existe un *ensemble intersectant* $H\subseteq S$ tel que $|H\cap U_i|=1$ pour tout $i=1,\dots,q$. On va construire des mots $\mathbf{w}$ et $\mathbf{w}'$ tels que : 1) $|\mathbf{w}\mathbf{w}'|$ est bornée supérieurement par un polynôme en r et q, et 2) l'identité $\mathbf{w}\mathrel{\widehat{=}}\mathbf{w}'$ échoue dans le semi-groupe $(C_4,\cdot)$ si et seulement si un ensemble intersectant pour la famille $\{U_i\}$ existe.

On introduit $2r+1$ variables : deux variables x_j et y_j pour chaque $j=1,\dots,r$ et une variable supplémentaire z. Pour chaque $j=1,\dots,r$, appelons $\mathbf{v}_j:=(x_jy_jzy_jx_jz)^2$. De plus, pour chaque $i=1,\dots,q$, si $U_i=\{s_{j_1},\dots,s_{j_p}\}$ où $p=|U_i|\le r$, alors on définit $\mathbf{u}_i:=(x_{j_1}\cdots x_{j_p}z)^2$. Finalement, définissons

$$\mathbf{w}:=z\mathbf{u}_1\cdots\mathbf{u}_q\mathbf{v}_1\cdots\mathbf{v}_r\ \text{ et }\ \mathbf{w}':=\mathbf{w}^2.$$

Puisque $|\mathbf{v}_j| = 12$ pour tout $j = 1,\dots,r$ et $|\mathbf{u}_i| \le 2(r+1)$ pour tout $i = 1,\dots,q$, on conclut que $|\mathbf{w}\mathbf{w}'| \le 3(1+2(r+1)q+12r)$, donc l'assertion 1) est établie.

Pour la partie "si" de l'assertion 2), soit H un ensemble intersectant pour la famille $\{U_i : i = 1,\dots,q\}$. Définissons une substitution $\varphi\colon \{x_1,y_1,\dots,x_r,y_r,z\} \to C_4$ comme suit :

$$x_j\varphi := \begin{cases} b & \text{si } s_j \in H, \\ e & \text{si } s_j \notin H; \end{cases} \qquad y_j\varphi := \begin{cases} e & \text{si } s_j \in H, \\ b & \text{si } s_j \notin H; \end{cases} \qquad z\varphi := a.$$

On calcule directement que $\mathbf{v}_j\varphi = (ba)^4$ pour tout $j = 1,\dots,r$. De plus, puisque $|H \cap U_i| = 1$ pour tout $i = 1,\dots,q$, on a $\mathbf{u}_i\varphi = (ba)^2$. Par la propriété 1°, on obtient $\mathbf{w}\varphi = a(ba)^{2q}(ba)^{4r} = a$. Par conséquent, la matrice $\mathbf{w}\varphi$ n'est pas idempotente et l'identité $\mathbf{w} \eqsim \mathbf{w}'$ échoue dans $(C_4,\cdot)$.

Pour la partie "et seulement si", supposons que $\mathbf{w} \eqsim \mathbf{w}'$ échoue dans le semi-groupe $(C_4,\cdot)$. Alors, il existe une substitution $\varphi\colon \{x_1,y_1,\dots,x_r,y_r,z\} \to C_4$ avec $\mathbf{w}\varphi \neq \mathbf{w}'\varphi$, ce qui signifie que la matrice $\mathbf{w}\varphi$ n'est pas idempotente. Par la construction, toutes les matrices $\mathbf{u}_i\varphi$ et $\mathbf{v}_j\varphi$ sont carrées et par conséquent, elles sont idempotentes (propriété 3°). Puisque n'importe quel produit de matrices idempotentes de C_4 est idempotent (propriété 4°), pour que $\mathbf{w}\varphi$ ne soit pas idempotent, il faut que la matrice $z\varphi$ ne soit pas idempotente. Par la propriété 2°, cela signifie soit que $z\varphi = a$ soit que $z\varphi = b$. Considérons le cas $z\varphi = a$; l'autre cas est complètement analogue.

Toutes les matrices dans l'ensemble $I = \{a^2, b^2, a^2b, ba^2\}$ sont idempotentes alors que $\mathbf{w}\varphi$ ne l'est pas. Donc $\mathbf{w}\varphi \notin I$, et puisque I est un idéal (propriété 5°), aucun facteur de $\mathbf{w}\varphi$ ne peut appartenir à I. En particulier,

$$\mathbf{v}_j\varphi = \left((x_jy_jzy_jx_jz)^2\right)\varphi = \left((x_j\varphi)(y_j\varphi)a(y_j\varphi)(x_j\varphi)a\right)^2 \notin I, \tag{7}$$

pour tout $j = 1,\dots,r$. Pour que (7) soit vérifiée, l'une des matrices $x_j\varphi, y_j\varphi$ doit être b et l'autre doit être e. En effet, et l'une et l'autre de $x_j\varphi$ et $y_j\varphi$ doivent appartenir à $C_4 \setminus I = \{e,a,b,ab,ba\}$. Si $x_j\varphi$ ou $y_j\varphi$ appartient à $\{a,ab,ba\}$, alors a^2 apparaitrait comme un facteur dans $\left((x_j\varphi)(y_j\varphi)a(y_j\varphi)(x_j\varphi)a\right)^2$, ce qui contredirait (7). Donc $x_j\varphi, y_j\varphi \in \{b,e\}$ mais les matrices $x_j\varphi, y_j\varphi$ ne peuvent être égales car sinon soit a^2 soit b^2 apparaitrait comme un facteur dans $\left((x_j\varphi)(y_j\varphi)a(y_j\varphi)(x_j\varphi)a\right)^2$.

Ainsi, $x_j\varphi \in \{b,e\}$ pour tout j. Pour chaque $i = 1,\dots,q$, on a

$$\mathbf{u}_i\varphi = \left((x_{j_1}\cdots x_{j_p}z)^2\right)\varphi = \left((x_{j_1}\varphi)\cdots(x_{j_p}\varphi)a\right)^2 \notin I. \tag{8}$$

Si au moins deux des matrices $x_{j_k}\varphi$, $k = 1,\dots,p$, sont égales à b, alors b^2 apparaît comme un facteur de $\left((x_{j_1}\varphi)\cdots(x_{j_p}\varphi)a\right)^2$, et si $x_{j_k}\varphi = e$ pour tout $k = 1,\dots,p$, alors $\left((x_{j_1}\varphi)\cdots(x_{j_p}\varphi)a\right)^2 = a^2$. Les deux options contredisent (8). Par conséquent, (8) implique qu'exactement l'une des matrices $x_{j_k}\varphi$, $k = 1,\dots,p$, est égale à b. Donc, l'ensemble $H := \{s_j \in S : x_j\varphi = b\}$ a une intersection qui est un singleton avec chaque ensemble U_i, $i = 1,\dots,q$, donc H est un ensemble intersectant pour la famille $\{U_i\}$. □

Remarque 1. *Le semi-groupe $(C_4,\cdot)$ est lié de façon étroite au* semi-groupe de Brandt $(B_2^1,\cdot)$ *à 6 éléments, qui est, pour reprendre la citation de [13], "peut-être le signe avant-coureur le plus omniprésent du comportement complexe dans tous les semi-groupes finis". Ici B_2^1 représente l'ensemble contenant les six matrices 2×2 suivantes :*

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

et $\cdot$ est la multiplication matricielle habituelle. On voit facilement que l'application $C_4 \to B_2^1$ définie par

$$e \mapsto \begin{pmatrix}1&0\\0&1\end{pmatrix}, ab \mapsto \begin{pmatrix}1&0\\0&0\end{pmatrix}, a \mapsto \begin{pmatrix}0&1\\0&0\end{pmatrix}, b \mapsto \begin{pmatrix}0&0\\1&0\end{pmatrix}, ba \mapsto \begin{pmatrix}0&0\\0&1\end{pmatrix},$$
$$a^2, b^2, a^2b, ba^2 \mapsto \begin{pmatrix}0&0\\0&0\end{pmatrix}$$

est un homomorphisme de semi-groupes, et cet homomorphisme induit un isomorphisme entre le quotient de Rees de $(C_4,\cdot)$ sur l'idéal $\{a^2,b^2,a^2b,ba^2\}$ et $(B_2^1,\cdot)$.

Il a été démontré par Seif [25] et, indépendamment par Klíma [17] que le semi-groupe $(B_2^1,\cdot)$ a une vérification d'identité qui est coNP*-complète. Les arguments de Klíma viennent de $(C_4,\cdot)$ avec des ajustements minimaux. À nouveau, pour faciliter la lecture, on a fourni la proposition 3.2 avec une preuve complète. On réduit à partir d'un problème* NP*-complet autre que celui utilisé par Klíma, mais on réutilise la construction de Klíma des mots du semi-groupe employés dans la réduction.*

Étudier la complexité du problème de la vérification d'identité est aussi intéressant pour les algèbres autres que les semi-groupes. Dans le contexte du présent article, il semble naturel de regarder la classe des ai-semi-anneaux finis. En général, si $(S,+,\cdot)$ est un ai-semi-anneau fini et s'il existe un algorithme en temps polynomial pour vérifier les identités dans le semi-groupe $(S,\cdot)$, le problème CHECK-ID$(S,+,\cdot)$ peut s'avérer être coNP-complet. (L'exemple le plus simple d'une telle situation est fourni par le treillis distributif à deux éléments ; voir [2]). Pourtant, les identités de semi-anneaux des matrices triangulaires booléennes $n \times n$ peuvent être aussi facilement vérifiées que celles des semi-groupes :

Proposition 3.3. *Pour tout n, il existe un algorithme en temps polynomial qui décide si une identité est vérifiée dans le semi-anneau de toutes les matrices booléennes triangulaires supérieures $n \times n$.*

Démonstration. La preuve de la proposition 3.1 fonctionne, en faisant référence au corollaire 2.2 plutôt qu'à 2.6. □

3.2 Le problème de la base finie

Ici on utilise quelques concepts de la logique des équations et de l'algèbre universelle ; on fournit les définitions nécessaires.

La *variété* définie par un ensemble Σ d'identités est la classe de toutes les algèbres satisfaisant toute identité appartenant à Σ. Un variété est *de base finie* [*de base non finie*] si elle peut (respectivement ne peut pas) être définie par un ensemble fini d'identités. Étant donnée une algèbre $\mathscr{A}$, la variété définie par l'ensemble de toutes les identités satisfaites par $\mathscr{A}$ est appelée la *variété engendrée par* $\mathscr{A}$ et on la dénote var$\mathscr{A}$. On dit que $\mathscr{A}$ est de base finie ou de base non finie s'il en est ainsi de la variété var$\mathscr{A}$. Le *problème de la base finie* pour une classe d'algèbres concerne la question de la classification des algèbres de cette classe selon le fait qu'elles soient de base finie ou de base non finie. Pour les classes des semi-groupes finis et des semi-anneaux finis, le problème de la base finie a été intensivement étudié depuis les années 1960 et, respectivement, depuis les années 2000. On peut se référer à [9] et à [12] comme des exemples

récents d'avancées dans ces domaines.

Une variété est dite *localement finie* si chacun de ses éléments finiment générés est fini. Une algèbre finie $\mathscr{A}$ est dite *de base non finie de façon inhérente* si $\mathscr{A}$ n'est contenue dans aucune variété localement finie de base finie. Il est notoire que la variété engendrée par une algèbre finie est localement finie (voir, par exemple [3, théorème II.10.16]). Par conséquent, une algèbre finie $\mathscr{A}$ est de base non finie à chaque fois que la variété var $\mathscr{A}$ contient une algèbre de base non finie de façon inhérente. En particulier, une algèbre de base non finie de façon inhérente est de base non finie.

Un mot $\mathbf{w}$ est dit être un *isoterme* pour un semi-groupe $(S,\cdot)$ si le seul mot $\mathbf{w}'$ tel que $(S,\cdot)$ satisfait l'identité $\mathbf{w} \doteq \mathbf{w}'$ est le mot $\mathbf{w}$ lui-même. Observons que si un mot $\mathbf{w}$ est minimal ou maximal pour un semi-groupe ordonné $(S,\cdot,\leq)$, alors $\mathbf{w}$ est un isoterme pour le semi-groupe $(S,\cdot)$.

Rappelons une caractérisation combinatoire des semi-groupes de base non finie de manière inhérente due à Mark Sapir [24]. Elle utilise la séquence $\{Z_m\}_{m=1,2,\ldots}$ des *mots de Zimin* définis inductivement par $Z_1 := x_1$, $Z_{m+1} := Z_m x_{m+1} Z_m$ où les $x_1, x_2, \ldots, x_m, \ldots$ sont des variables distinctes.

Proposition 3.4 ([24, Proposition 7])**.** *Un semi-groupe fini $(S,\cdot)$ est de base non finie de manière inhérente si et seulement si tous les mots de Zimin sont des isotermes pour $(S,\cdot)$.*

Notre description des inégalités du semi-groupe ordonné $(T_n,\cdot,\leq)$ nous permet d'établir la propriété suivante des mots de Zimin.

Proposition 3.5. *Les mots de Zimin sont minimaux pour le semi-groupe ordonné $(T_n,\cdot,\leq)$ si $n \geq 3$.*

Démonstration. Clairement, l'application $T_{n-1} \to T_n$ qui envoie chaque matrice $A \in T_{n-1}$ vers la matrice $n \times n$

$$\begin{pmatrix} & & & 0 \\ & A & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

est un plongement de semi-groupes ordonnés. Par conséquent, il suffit de montrer que tout mot de Zimin Z_m est minimal pour $(T_3,\cdot,\leq)$.

On procède à une induction sur m. Quand $m = 1$, on a $Z_1 = x_1$. Si pour un certain mot $\mathbf{w}$, l'inégalité $\mathbf{w} \preccurlyeq x_1$ est vérifiée dans $(T_3,\cdot,\leq)$, alors par le théorème 2.5, soit $\mathbf{w} = x_1$ soit $|\mathbf{w}| \geq 3$ et tout mot de longueur 2 qui apparaît dans $\mathbf{w}$ doit apparaître dans x_1. Le dernier cas est impossible de façon évidente.

Maintenant supposons que $m > 1$ et que le mot de Zimin Z_{m-1} est minimal pour $(T_3,\cdot,\leq)$. Considérons le mot de Zimin Z_m et appelons $\mathbf{w}$ n'importe quel mot tel que l'inégalité $\mathbf{w} \preccurlyeq Z_m$ est vérifiée dans $(T_3,\cdot,\leq)$. En substituant la matrice identité pour la variable x_1 dans l'inégalité, on obtient que $(T_3,\cdot,\leq)$ satisfait l'inégalité $\mathbf{w}' \preccurlyeq Z'_m$ où les mots $\mathbf{w}'$ et Z'_n sont obtenus à partir de $\mathbf{w}$ et, respectivement Z_m, en enlevant toutes les occurrences de x_1. Le mot Z'_m n'est rien d'autre que le mot de Zimin Z_{m-1} avec l'indice de chaque variable augmenté de 1. Par l'hypothèse d'induction, on a $\mathbf{w}' = Z'_m$. Puisque le mot $\mathbf{w}$ devient Z'_m après avoir enlevé toutes les occurrences de x_1, on conclut que

$$\mathbf{w} = x_1^{\varepsilon_1} x_2 x_1^{\varepsilon_2} x_3 x_1^{\varepsilon_3} x_2 x_1^{\varepsilon_4} x_4 \cdots x_3 x_1^{\varepsilon_{2^m-1}} x_2 x_1^{\varepsilon_{2^m}},$$

où ε_i, $i = 1, 2, \ldots, 2^m$, sont les nombres non négatifs. (Si $\varepsilon_i = 0$, $x_1^{\varepsilon_i}$ dénote le mot vide). Ainsi, le mot $\mathbf{w}$ est obtenu à partir de Z_m en substituant le facteur $x_1^{\varepsilon_i}$ au i^{ieme} facteur à partir de l'occurrence sur la gauche de la variable x_1.

Si $\varepsilon_i > 1$ pour un certain $i = 1, 2, \ldots, 2^m$, alors le mot x_1^2 de longueur 2 apparaît dans $\mathbf{w}$ avec les sauts G_1, G_2, G_3 tels que $G_2 = \varnothing$. Puisque l'inégalité $\mathbf{w} \preccurlyeq Z_m$ est vérifiée dans $(T_3, \cdot, \leq)$, le théorème 2.5 assure que le mot x_1^2 apparaît dans Z_m avec les sauts G_1', G_2', G_3' tels que $G_\ell' \subseteq G_\ell$ pour tout $\ell = 1, 2, 3$. Alors $G_2' = \varnothing$, ce qui devrait signifier que x_1^2 est comme un facteur de Z_m mais par la construction des mots de Zimin, dans toute paire d'occurrences de la variable x_1 dans Z_m, les deux éléments de la paire sont séparés par une autre variable. Ainsi, l'option $\varepsilon_i > 1$ est exclue.

Si $\varepsilon_i = 0$ pour un certain $i = 2, \ldots, 2^m - 1$, alors pour un certain x_j et x_k avec $j, k > 1$, le mot $x_j x_k$ de longueur 2 apparaît dans $\mathbf{w}$ avec les sauts G_1, G_2, G_3 tels que $G_2 = \varnothing$. Comme dans le paragraphe précédent, on conclut que $x_j x_k$ doit apparaître dans Z_m avec les sauts G_1', G_2', G_3' tels que le saut "intérieur" G_2' est vide. Cela devrait signifier que $x_j x_k$ est un facteur de Z_m mais dans Z_m, la variable x_1 apparaît entre toutes deux occurrences des variables d'indices supérieurs à 1.

Si $\varepsilon_1 = 0$, le mot $x_2 x_1$ de longueur 2 apparaît dans $\mathbf{w}$ avec les sauts G_1, G_2, G_3 tels que $G_1 = \varnothing$. Alors il doit apparaître dans Z_m avec les sauts G_1', G_2', G_3' tels que $G_1' = \varnothing$, devrait signifier que Z_m commence par x_2 alors qu'il commence par x_1. Un argument symétrique exclut la possibilité $\varepsilon_{2^m} = 0$.

On a montré que $\varepsilon_i = 1$ pour chaque $i = 1, 2, \ldots, 2^m$, et par conséquent que $\mathbf{w} = Z_m$. □

La proposition 3.5 implique que tous les mots de Zimin sont des isotermes pour le semi-groupe $(T_n, \cdot)$ si $n \geq 3$. Combiner cette observation avec la proposition 3.4 amène le corollaire suivant :

Corollaire 3.6. *Pour tout $n \geq 3$, le semi-groupe de toutes les matrices booléennes triangulaires supérieures $n \times n$ est de base non finie de manière inhérente.*

Alors que la proposition 3.5 semble nouvelle, le corollaire 3.6 est connu. Pour $n > 3$, le résultat a été obtenu dans [27], et le cas $n = 3$ a été réglé dans [18]. Et [27] et [18] ont utilisé une approche sémantique qui ne nécessitait pas de caractériser les identités de $(T_n, \cdot)$.

Par souci de complétude, mentionnons que le semi-groupe $(T_2, \cdot)$ est de base finie ; une base explicite finie pour les identités de $(T_2, \cdot)$ peut être trouvée dans [18, Théorème 3.5].

Qu'est-ce qui peut être dit à propos du problème de la base finie pour le ai-semi-anneau $(T_n, +, \cdot)$? Un analogue pour le semi-anneau (partiel) de la Proposition 3.4 a été trouvé par Dolinka [6].

Proposition 3.7 ([6, Théorème B])**.** *Un ai-semi-anneau fini $(S, +, \cdot)$ avec 0 est de base non finie de façon inhérente si chaque mot de Zimin est à la fois minimal et maximal pour $(S, +, \cdot)$.*

À cause de la proposition 3.5, on aurait pu espérer appliquer la proposition 3.7 à l'ai-semi-anneau $(T_n, +, \cdot)$ avec $n \geq 3$ en montrant que tous les mots de Zimin sont maximaux pour le semi-groupe ordonné $(T_n, \cdot, \leq)$ avec $n \geq 3$. Pourtant, en réalité, pour chaque n, il existe un mot de Zimin qui n'est pas maximal pour

$(T_n, \cdot, \leq)$. Par exemple, en utilisant le théorème 2.5, il est facile de vérifier que l'inégalité stricte $Z_3 \prec x_1x_2x_1^2x_3x_1x_2x_1$ est vérifiée dans le semi-groupe ordonné $(T_3, \cdot, \leq)$.

Puisque la proposition 3.7 (différemment de la proposition 3.4) est seulement une condition suffisante pour être de base non finie de manière inhérente, le fait que les mots de Zimin, en général, ne soient pas maximaux pour $(T_n, \cdot, \leq)$ n'exclut pas la possibilité que les ai-semi-anneaux $(T_n, +, \cdot)$ soient de base non finie de manière inhérente pour un n suffisamment grand. Habituellement, on sait seulement que les ai-semi-anneaux $(T_n, +, \cdot)$ avec $n \geq 3$ sont de base non finie. C'est un résultat récent du à Sergey Gusev et à l'auteur [10] qui a été trouvé par une approche sémantique.

Comme dans la sous-section 3.1, on souhaite mettre les résultats dont il vient d'être question dans un contexte plus large. Pour cela, reportons l'état de l'art du problème de la base finie pour d'autres semi-groupes de matrices triangulaires. Dans le cas tropical, on sait que le semi-groupe de toutes les matrices triangulaires supérieures tropicales $n \times n$ est de base non finie pour $n = 2$ [4] et $n = 3$ [11] alors que pour $n \geq 4$, le problème reste ouvert. La situation actuelle avec le semi-groupe $(T_n(q), \cdot)$ de toutes les matrices triangulaires supérieures $n \times n$ sur un corps fini à q éléments est à l'opposé dans un certain sens. Dans [26], il a été démontré que le semi-groupe $(T_n(q), \cdot)$ est de base non finie de façon inhérente si et seulement si $q > 2$ et $n \geq 4$, et dans [9], on a démontré que le semi-groupe $(T_n(2), \cdot)$ avec $n \geq 4$ est de base non finie. Le problème de la base finie pour les semi-groupes $(T_2(q), \cdot)$ et $(T_3(q), \cdot)$ reste ouvert avec la seule exception du semi-groupe $(T_2(2), \cdot)$ pour les identités duquel une base explicite finie a été trouvée dans [28, Théorème 3.1].

3.3 Connexions avec la théorie des langages formels

Un *monoïde* est un semi-groupe possédant un élément identité. Tous les semi-groupes de matrices considérés ci-dessus étaient en fait des monoïdes puisque chacun d'entre eux contenait la matrice identité de la taille appropriée. La *pseudo-variété* engendrée par un ensemble de monoïdes finis est la plus petit classe de monoïdes finis contenant l'ensemble et fermée en prenant les images homéomorphes, les sous-monoïdes et les produits directs finis. Les pseudo-variétés des monoïdes finis sont activement étudiées à cause de leurs connexions étroites avec certaines classes de langages reconnaissables via la correspondance de Eilenberg ([7], voir également [20]). On sait que la pseudo-variété engendrée par un monoïde fini unique est *équationnelle* [8], c'est-à-dire qu'elle est constituée de tous les monoïdes finis satisfaisant un certain système d'identités. En d'autres termes, une pseudo-variété équationnelle n'est rien d'autre que l'ensemble de tous les éléments finis d'une variété monoïde.

Soit Σ un ensemble fini de variables. Dénotons par Σ^* l'ensemble de tous les mots dont les variables viennent de Σ, y compris le mot vide. Selon la concaténation, $(\Sigma^*, \cdot)$ est un monoïde, avec le mot vide servant d'élément identité. Un *langage sur* Σ est n'importe quel sous-ensemble de Σ^*. Par une *combinaison booléenne* d'une famille $\{L_i\}$ de langages sur Σ, on entend tout langage qui peut être produit à partir des L_i par des applications répétées d'opérations de la théorie des ensembles telles que l'union ou l'intersection de deux ensembles et en prenant le complémentaire d'un ensemble. Pour deux langages $L, K \subseteq \Sigma^*$ et une variable $a \in \Sigma$, on écrit LaK pour le langage $\{\mathbf{u}a\mathbf{v} : \mathbf{u} \in L, \mathbf{v} \in K\}$.

Un langage $L \subseteq \Sigma^*$ est *reconnu* par un monoïde fini $(M, \cdot)$ s'il existe un homomorphisme de monoïdes

$\varphi\colon \Sigma^* \to M$ tel qu'un mot $\mathbf{w}$ est dans L si et seulement si $\mathbf{w}\varphi = \mathbf{w}'\varphi$ pour un certain mot $\mathbf{w}' \in L$. Un langage est dit *reconnaissable* s'il est reconnu par un certain monoïde fini.

Soit $\mathbb{T}$ la pseudo-variété des monoïdes finis engendrés par tous les monoïdes des matrices booléennes triangulaires supérieures $n \times n$, $n = 1, 2, \ldots$. Pin et Straubing [22] ont trouvé la caractérisation combinatoire suivante des langages reconnus par les monoïdes dans $\mathbb{T}$.

Proposition 3.8 ([22, Théorème 2])**.** *Un langage L sur Σ est reconnu par un monoïde dans la pseudo-variété $\mathbb{T}$ si et seulement si L est une combinaison booléenne de langages de la forme*

$$\Sigma_1^* a_1 \Sigma_2^* \cdots a_k \Sigma_{k+1}^*$$

où $k \geq 1$, $a_1, \ldots, a_k \in \Sigma$ et $\Sigma_1, \Sigma_2, \ldots, \Sigma_{k+1}$ sont des sous-ensembles (possiblement vides) de Σ.

Pour tout $n = 1, 2, \ldots$, appelons $\mathbb{T}_n$ la pseudo-variété des monoïdes finis engendrés par le monoïde $(T_n, \cdot)$. Le coorollaire 2.2 implique aisément une proposition similaire à la proposition 3.8 de caractérisation des langages reconnus par des monoïdes dans $\mathbb{T}_n$.

Proposition 3.9. *Un langage L sur Σ est reconnu par un monoïde dans la pseudo-variété $\mathbb{T}_n$ si et seulement si L est une combinaison booléenne de langages de la forme*

$$\Sigma_1^* a_1 \Sigma_2^* \cdots a_k \Sigma_{k+1}^*$$

où $1 \leq k < n$, $a_1, \ldots, a_k \in \Sigma$ et $\Sigma_1, \Sigma_2, \ldots, \Sigma_{k+1}$ sont des sous-ensembles (possiblement vides) de Σ.

De la définition d'une pseudo-variété, on voit directement que $\mathbb{T} = \bigcup_n \mathbb{T}_n$. Par conséquent, on peut voir la Proposition 3.9 comme une restriction du résultat souligné par Pin et Straubing, et de plus, la Proposition 3.8 est une conséquence immédiate de la Proposition 3.9. Pourtant, il est bon de dire que nos arguments dans la preuve du Corollaire 2.2 proviennent de [22].

Plusieurs auteurs ont modifié la correspondance d'Eilenberg entre les classes de langages reconnaissables et les pseudo-variétés des monoïdes finis en relâchant les conditions imposées sur les classes de langages tout en enrichissant les monoïdes par des relations et/ou des opérations supplémentaires. En particulier, Pin [21] et Polák [23] ont développé des correspondances de type Eilenberg avec des monoïdes ordonnés, respectivement, des ai-semi-anneaux du côté algébrique. Utiliser le théorème 2.1 et le corollaire 2.2 permet de caractériser les langages reconnus par des monoïdes ordonnés et des ai-semi-anneaux à partir des pseudo-variétés des monoïdes ordonnés et des ai-semi-anneaux engendrés par le monoïde ordonné $(T_n, \cdot, \leq)$ et, respectivement, le ai-semi-anneau $(T_n, +, \cdot)$ pour tout $n = 1, 2, \ldots$. Les caractérisations sont similaires à celles de la Proposition 3.9 donc nous omettons leurs formulations.

Références

[1] Almeida, J., Volkov, M.V., Goldberg, S.V. Complexity of the identity checking problem for finite semigroups. Zap. Nauchn. Sem. POMI **358**, 5–22 (2008) [Russian ; Engl. translation J. Math. Sci. **158**(5), 605–614 (2009)]

[2] Bloniarz, P.A., Hunt III, H.B., Rosenkrantz, D.J. : Algebraic structures with hard equivalence and minimization problems. J. Assoc. Comput. Mach. **31**, 879–904 (1984)

[3] Burris, S., Sankappanavar, H.P. : A Course in Universal Algebra. Springer, Berlin, Heidelberg, New York (1981)

[4] Chen, Y.Z., Hu, X., Luo, Y.F., Sapir, O. : The finite basis problem for the monoid of two-by-two upper triangular tropical matrices. Bull. Aust. Math. Soc. **94**, 54–64 (2016)

[5] Daviaud, L., Johnson, M., Kambites, M. : Identities in upper triangular tropical matrix semigroups and the bicyclic monoid. J. Algebra **501**, 503–525 (2018)

[6] Dolinka, I. : A class of inherently nonfinitely based semirings. Algebra Universalis **60**, 19–35 (2009)

[7] Eilenberg, S. : Automata, Languages and Machines, Vol. B. Academic Press, New York (1976)

[8] Eilenberg, S., Schützenberger, M.P. : On pseudovarieties. Adv. Math. **19**, 413–418 (1976)

[9] Gusev, S.V., Sapir, O.B., Volkov, M.V. : Strongly nonfinitely based monoids. J. Combinatorial Algebra **9** (2025)

[10] Gusev, S.V., Volkov, M.V. : The finite basis problem for semirings of triangular Boolean matrtices. In preparation.

[11] Han, B.B., Zhang, W.T., Luo, Y.F. : Equational theories of upper triangular tropical matrix semigroups. Algebra Universalis **82**, article no. 44 (2021)

[12] Jackson, M., Ren, M., Zhao, X.Z. : Nonfinitely based ai-semirings with finitely based semigroup reducts. J. Algebra **611**, 211–245 (2022)

[13] Jackson, M., Zhang, W.T. : From A to B to Z. Semigroup Forum **103**, 165–190 (2021)

[14] Johnson, M., Tran, N.M. : Geometry and algorithms for upper triangular tropical matrix identities. J. Algebra **530**, 470–507 (2019)

[15] Karp, R.M. : Reducibilty among combinatorial problems. In : Miller, R.E., Thatcher, J.W., Bohlinger, J.D. (eds.), Complexity of Computer Computations, pp. 85–103. Springer, Boston (1972)

[16] Kharlampovich, O.G., Sapir, M.V. : Algorithmic problems in varieties. Int. J. Algebra Comput. **5**(4-5), 379–602 (1995)

[17] Klíma, O. : Complexity issues of checking identities in finite monoids. Semigroup Forum **79**, 435–444 (2009)

[18] Li, J.R., Luo, Y.F. : On the finite basis problem for the monoids of triangular boolean matrices. Algebra Universalis **65**, 353–362 (2011)

[19] Papadimitriou, C.H. : Computational Complexity. Addison-Wesley, Reading, MA (1994)

[20] Pin, J.-É. : Variétés de Langages Formels. Masson, Paris (1984) [French ; Engl. translation : Varieties of Formal Languages. North Oxford Academic, London (1986) and Plenum, New York (1986)]

[21] Pin, J.-É. : A variety theorem without complementation. Izv. Vyssh. Uchebn. Zav. Mat. 1, 80–90 (1995) [Russian ; Engl. translation Russian Math. (Iz. VUZ) **39**(1), 74–83 (1995)]

[22] Pin, J.-É., Straubing, H. : Monoids of upper triangular matrices. In : Pollák, Gy., Schwarz, Št., Steinfeld, O. (eds), Semigroups. Structure and Universal Algebraic Problems. Colloquia Mathematica Societatis János Bolyai, vol. 39, pp. 259–272. North-Holland, Amsterdam (1985)

[23] Polák, L. : Syntactic semiring of a language. In : Sgall, J., Pultr, A., Kolman, P. (eds.), Mathematical Foundations of Computer Science 2001. MFCS 2001. Lecture Notes in Computer Science, vol. 2136, pp. 611–620. Springer, Berlin, Heidelberg (2001)

[24] Sapir, M.V. : Problems of Burnside type and the finite basis property in varieties of semigroups. Izv. Akad. Nauk SSSR, Ser. Mat. **51**, 319–340 (1987) [Russian ; Engl. translation Math. USSR–Izv. **30**, 295–314 (1988)]

[25] Seif, S. : The Perkins semigroup has co-NP-complete term-equivalence problem. Int. J. Algebra Comput. **15**(2), 317–326 (2005)

[26] Volkov, M.V., Goldberg, I.A. : Identities of semigroups of triangular matrices over finite fields. Mat. Zametki **73**(4), 502–510 (2003) [Russian ; Engl. translation Math. Notes **73**(4), 474–481 (2003)]

[27] Volkov, M.V., Goldberg, I.A. : The finite basis problems for monoids of triangular boolean matrices. In : Algebraic Systems, Formal Languages, and Conventional and Unconventional Computation Theory. RIMS Kokyuroku, vol. 1366, pp. 205–214. Kyoto University, Kyoto (2004)

[28] Zhang, W.T., Li, J.R., Luo, Y.F. : On the variety generated by the monoid of triangular 2×2 matrices over a two-element field. Bull. Aust. Math. Soc. **86**(1), 64–77 (2012)