Identités de semi-anneaux de semi-groupes de relations réflexives et matrices booléennes triangulaires supérieures

S. V. Gusev

Résumé : On montre que les semi-anneaux suivants satisfont les mêmes identités : le semi-anneau $\mathcal{R}_n$ de toutes les relations binaires sur un ensemble à n éléments, le semi-anneau $\mathcal{U}_n$ de toutes les matrices triangulaires supérieures $n \times n$ sur un semi-anneau booléen, le semi-anneau $\mathcal{C}_n$ des transformations extensives et préservant tous les ordres d'une chaîne à n éléments. Au vu du résultat de Klíma et Polák, qui énonce que $\mathcal{C}_n$ a une base finie d'identités pour tout n, cela implique que les identités de $\mathcal{R}_n$ et $\mathcal{U}_n$ admettent également une base finie.

Un semi-anneau additivement idempotent (ai-semi-anneau, pour abréger) est une algèbre $\mathcal{S} = (S, +, .)$ de type (2,2) telle que la réduction additive $(S, +)$ est un semi-anneau (c'est-à-dire est un semi-groupe idempotent commutatif), la réduction multiplicative $(S, .)$ est un semi-groupe et la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire que $\mathcal{S}$ satisfait les identités $x(y+z) \approx xy+xz$ et $(y + z)x \approx yx + zx$.

L'ensemble de toutes les relations réflexives binaires sur un ensemble à n éléments forme un ai-semi-anneau selon l'union et la multiplication au sens de la théorie des ensembles. On peut penser convenablement à ce ai-semi-anneau comme à un sous-semi-anneau du ai-semi-anneau de toutes les matrices $n \times n$ (avec les multiplication et addition usuelles des matrices) sur le semi-anneau booléen $\mathcal{B} = \langle \{0, 1\}; +, .\rangle$ avec les opérations définies par les règles

$$0.0 = 0.1 = 1.0 = 0 + 0 = 0, \qquad 1.1 = 1 + 0 = 0 + 1 = 1 + 1 = 1.$$

Notamment, il peut être identifié avec le sous-semi-anneau contenant les matrices dont tous les éléments diagonaux sont égaux à 1. Dénotons ce semi-anneau par $\mathcal{R}_n = \langle R_n; +, .\rangle$. Dénotons par $\mathcal{U}_n = \langle U_n; +, .\rangle$ le sous-semi-anneau de $\mathcal{R}_n$ contenant les matrices triangulaires supérieures, c'est-à-dire les matrices (α_{ij}) avec $\alpha_{ij} = 0$ pour $j < i$.

Une transformation α d'un ensemble partiellement ordonné $\langle Q; \leq\rangle$ est dite préserver l'ordre si $q \leq q'$ implique $q.\alpha \leq q'.\alpha$ pour tous $q, q' \in Q$, et extensive si $q \leq q.\alpha$ pour tout $q \in Q$. On dit qu'un ai-semi-anneau $\langle S; +, .\rangle$ est un semi-anneau jointure de transformations extensives préservant l'ordre d'un semi-anneau-jointure $\langle Q; \leq\rangle$ si $\langle S; .\rangle$ est un semi-groupe des transformations préservant l'ordre et extensives de $\langle Q; \leq\rangle$ et $q.(\alpha + \beta) = \sup(q.\alpha, q.\beta)$ pour tous $\alpha, \beta \in S$ et $q \in Q$. Par exemple, l'ensemble de toutes les transformations extensives et préservant l'ordre d'une chaîne à n éléments forme un semi-anneau jointure. Dénotons ce semi-anneau par $\mathcal{C}_n = \langle C_n; +, .\rangle$.

En [2], Volkov montre que les monoïdes $\langle R_n; .\rangle, \langle U_n; .\rangle$ et $\langle C_n; .\rangle$ satisfont les mêmes identités et que ces identités admettent une base finie si et seulement si $n \leq 4$. Par contraste, par le résultat de Klíma et Polák [1], le ai-semi-anneau $\mathcal{C}_n$ a une base finie d'identités pour chaque n. Dans la note présente, on prouve le théorème suivant :

Théorème 1. *Pour tout n, les trois ai-semi-anneaux $\mathcal{U}_n, \mathcal{R}_n$ et $\mathcal{C}_n$ satisfont les mêmes identités et ces identités admettent une base finie.*

Traduction en français de https://arxiv.org/pdf/2301.11863, Denise Vella-Chemla, mars 2025.

Pour prouver le théorème 1, on a besoin de quelques définitions, notations et résultats auxiliaires. Si u, v sont des mots sur un même alphabet Σ, on dit que u est un sous-mot de v à chaque fois qu'il existe des mots $u_1, ..., u_n, v_0, v_1, ..., v_{n-1}, v_n \in \Sigma^*$ tels que

$$u = u_1 \dots u_n \qquad \text{et} \qquad v = v_0 u_1 v_1 \dots v_{n-1} u_n v_n \ ;$$

en d'autres termes, cela signifie qu'on peut extraire u traité comme une séquence de lettres de la séquence v. Soit $s_k(w)$ dénotant l'ensemble de tous les sous-mots de w de longueur $\leq k$. Rappelons qu'une identité de semi-anneau sur un alphabet Σ, ou disons une identité, est une paire $(u_1 + \ldots + u_\ell, v_1 + ... + v_r)$, où $u_1, \ldots, u_\ell, v_0, ..., v_r \in \Sigma^+$, habituellement écrite comme

$$u_1 + \ldots + u_\ell \approx v_1 + \ldots + v_r. \tag{1}$$

On dénote par J_k l'ensemble de toutes les identités (1) avec $\bigcup_{i=1}^{l} s_k(u_i) = \bigcup_{i=1}^{r} s_k(v_i)$. Pour un ai-semi-anneau $\mathcal{S}$, on dénote par $\mathrm{Id}(\mathcal{S})$ l'ensemble de toutes les identités de $\mathcal{S}$.

Proposition 1. *Soit $\mathcal{S} = \langle S; +, . \rangle$ un semi-anneau jointure de transformations préservant l'ordre et extensives d'un semi-treillis jointure $\langle Q; \leq \rangle$. Si $k+1$ est la longueur de la plus longue chaîne dans $\langle Q; \leq \rangle$, alors $\mathcal{S}$ satisfait toute identité dans J_k.*

Preuve. Prenons n'importe quelle identité (1) dans J_k et soit Σ l'alphabet des mots $u_1, ..., u_\ell$ et $v_1, ..., v_r$. On doit montrer que pour toute substitution $\varphi : \Sigma \to S$, on obtient $(u_1 + \ldots + u_\ell)\varphi = (v_1 + \ldots + v_r)\varphi$ ou, de façon équivalente, $q.(u_1 + \ldots + u_\ell)\varphi = q.(v_1 + \ldots + v_r)\varphi$ pour tout $q \in Q$.

Ainsi, fixons une substitution arbitraire $\varphi : \Sigma \to S$ et un élément arbitraire $q_0 \in Q$. Par symétrie, il suffit de vérifier que

$$q_0.(u_1 + \ldots + u_\ell)\varphi \leq q_0.(v_1 + \ldots + v_r)\varphi.$$

Si $q_0.u_i\varphi = q_0$ pour tout $i = 1, ..., \ell$, alors

$$q_0.(u_1 + \ldots + u_\ell)\varphi = q_0 \leq q_0.(v_1 + \ldots + v_r)\varphi$$

parce que la transformation $(v_1 + \ldots + v_r)\varphi$ est extensive. Supposons maintenant que l'ensemble $\{i_1, ..., i_p\} = \{i \mid 1 \leq i \leq \ell, q_0.u_i\varphi > q_0\}$ n'est pas vide. Pour tout $i = i_1, ..., i_p$, dénotons par u_{i1} le plus long préfixe du mot u_i tel que $q_0.u_{i1}\varphi = q_0$ et soit $x_{i1} \in \Sigma$ la lettre qui suit u_{i1} dans u_i de telle façon que $u_i = u_{i1}x_{i1}w_{i1}$ pour un certain $w_{i1} \in \Sigma^*$. Alors

$$q_{i1} = q_0.(u_{i1}x_{i1})\varphi = q_0.u_{i1}\varphi x_{i1}\varphi = q_0.x_{i1}\varphi \geq q_0 \tag{2}$$

parce que la transformation $x_{i1}\varphi$ est extensive, et par le choix du préfixe u_{i1}, l'inégalité $q_1 \geq q_0$ est en fait une inégalité stricte. Maintenant dénotons par u_{i2} le plus long préfixe du mot w_{i1} tel que $q_{i1}.u_{i2}\varphi = q_{i1}$ et soit $x_{i2} \in \Sigma$ la lettre qui suit u_{i2} dans w_{i1} de telle façon que $u_i = u_{i1}x_{i1}u_{i2}x_{i2}w_{i2}$ pour un certain $w_{i2} \in \Sigma^*$. Alors

$$q_{i2} = q_{i1}.(u_{i2}x_{i2})\varphi = q_{i1}.u_{i2}\varphi x_{i2}\varphi = q_{i1}.x_{i2}\varphi > q_{i1} \tag{3}$$

et en substituant les expressions pour q_{i1} à partir de (2) dans les expressions pour q_{i2} dans (3), on obtient également

$$q_{i2} = q_0.(u_{i1}x_{i1}u_{i2}x_{i2})\varphi = q_0.(x_{i1}x_{12})\varphi.$$

En continuant ce processus, on aboutit finalement à la décomposition

$$u_i = u_{i1}x_{i1}u_{i2}x_{i2}\dots x_{im_i}u_{m_i+1} \tag{4}$$

telle que $q_0.u_i\varphi = q_0.(x_{i1}\dots x_{im_i})\varphi$ et

$$q_{i_i} > q_{i,m_i-1} > \dots > q_{i_1} > q_0$$

où $q_{ij} = q_0.(x_{i1}\dots x_{ij})$ pour $j = 1, 2, ..., m_i$. Puisque la plus longue chaîne dans $\langle Q; \leq\rangle$ a $k+1$ éléments, on conclut que $m_i \leq k$. Comme l'identité (1) est obtenue à partir de J_k, le mot $x_{i1}\dots x_{im_i}$ étant au vu de (4) un sous-mot de longueur $\leq k$ du mot u_i, doit être un sous-mot d'un mot dans $\{v_1, ..., v_r\}$. Ainsi, il existe un $r_i \in \{1, ..., r\}$ tel que

$$v_{r_i} = v_{i1}x_{i1}v_{i2}x_{i2}\dots x_{im_i}v_{i,m_i+1}$$

pour certains mots $v_{i1}, ..., v_{i,m_i+1} \in \Sigma^*$. En utilisant le fait que les transformations dans $\mathcal{S}$ sont extensives et préservent l'ordre, on obtient finalement que

$$q_0.v_{r_i}\varphi \geq q_0.(x_1x_2\dots x_m)\varphi = q_0.u_i\varphi,$$

$i = i_1, ..., i_p$. Puisque $\mathcal{S}$ est un semi-anneau jointure de transformations préservant l'ordre et extensives de $\langle Q; \leq\rangle$, il en découle que

$$\begin{aligned} q_0.(u_1 + \dots + u_\ell)\varphi &= q_0.(u_{i_1} + \dots + u_{i_p})\varphi \\ &\leq q_0.(v_{r_{i_1}} + ... + v_{r_{i_p}})\varphi \\ &\leq q_0.(v_1 + \dots + v_r)\varphi \end{aligned}$$

comme souhaité. □

Corollaire 1. $J_k \subseteq \mathrm{Id}(\mathcal{R}_{k+1})$.

Preuve. Soit $Q = \mathcal{B}^{(k+1)}\backslash\{(0, ..., 0)\}$ l'ensemble de tous les $(k+1)$-vecteurs non nuls sur le semi-anneau booléen $\mathcal{B} = \langle\{0, 1\}; +, .\rangle$. On équipe l'ensemble Q de l'ordre composante à composante $\leq$ induit par l'ordre standard $0 < 1$ dans $\mathcal{B}$. Alors $\langle Q, \leq\rangle$ devient un semi-treillis jointure dans lequel la chaîne la plus longue est de longueur $k+1$. Le semi-groupe $\langle R_{k+1}; .\rangle$ agit sur l'ensemble Q par la multiplication matricielle habituelle sur la droite : si $q = (q_i) \in Q$ et $\alpha = (\alpha_{ij}) \in R_{k+1}$ alors

$$q.\alpha = \left(\sum_{i=1}^{k+1} q_i\alpha_{i1}, ..., \sum_{i=1}^{k+1} q_i\alpha_{ik+1}\right).$$

Comme noté en [2], ceci est une représentation fidèle sur le semi-groupe par transformations extensives et préservant l'ordre de $\langle Q, \leq \rangle$. De plus, pour tout $q = (q_i) \in Q$ et $\alpha = (\alpha_{ij}), \beta = (\beta_{ij}) \in R_{k+1}$, on a :

$$
\begin{aligned}
q.(\alpha+\beta) &= \left(\sum_{i=1}^{k+1} q_i(\alpha_{i1}+\beta_{i1}), ..., \sum_{i=1}^{k+1} q_i(\alpha_{ik+1}+\beta_{ik+1}) \right) \\
&= \left(\sum_{i=1}^{k+1} q_i\alpha_{i1} + \sum_{i=1}^{k+1} q_i\beta_{i1}, ..., \sum_{i=1}^{k+1} q_i\alpha_{ik+1} + \sum_{i=1}^{k+1} q_i\beta_{ik+1} \right) \\
&= \left(\max\left(\sum_{i=1}^{k+1} q_i\alpha_{i1}, \sum_{i=1}^{k+1} q_i\beta_{i1} \right), \ldots, \max\left(\sum_{i=1}^{k+1} q_i\alpha_{ik+1}, \sum_{i=1}^{k+1} q_i\beta_{ik+1} \right) \right) \\
&= sup(q.\alpha, q.\beta).
\end{aligned}
$$

Maintenant la proposition (1) s'applique. □

Preuve du théorème 1. Les ai-semi-anneaux $\mathcal{U}_1, \mathcal{R}_1$ et $\mathcal{C}_1$ sont triviaux et admettent ainsi une base finie d'identités. Dénotons par $\mathcal{S}_{k+1} = \langle S_{k+1}; +, . \rangle$, le sous-semi-anneau de $\mathcal{U}_{k+1}$ contenant toutes les matrices triangulaires en escalier, i.e. les matrices (α_{ij}) satisfaisant la condition : si $\alpha_{ij} = 1, i < j$, alors

$$\alpha_{ii} = \alpha_{ii} + 1 = \ldots = \alpha_{ij} = \alpha_{i+1j} = \ldots = \alpha_{jj} = 1.$$

Il est remarqué en [1 Section 5], que le monoïde $\langle S_{k+1}; . \rangle$ est isomorphe au monoïde $\langle C_{k+1}; . \rangle$. En fait, on voit facilement que le ai-semi-anneau $\mathcal{S}_{k+1}$ est isomorphe à $\mathcal{C}_{k+1}$. De plus, il est démontré dans [1 Sections 4.1 et 5] que $\mathrm{Id}(\mathcal{S}_{k+1}) = J_k$ et que le ai-semi-anneau $\mathcal{S}_{k+1}$ est de base finie par l'identité

$$x_1 \ldots x_{k+1} \approx \sum_{i=1}^{k+1} x_1 \ldots x_{i-1} x_{i+1} \ldots x_{k+1},$$

Puisque $J_k = \mathrm{Id}(\mathcal{C}_{k+1}) = \mathrm{Id}(\mathcal{S}_{k+1}) \supseteq \mathrm{Id}(\mathcal{U}_{k+1}) \supseteq \mathrm{Id}(\mathcal{R}_{k+1})$, ces faits et le corollaire 1 impliquent que les ai-semi-anneaux $\mathcal{U}_{k+1}, \mathcal{R}_{k+1}$ et $\mathcal{C}_{k+1}$ satisfont les mêmes identités et ces identités admettent une base finie. Le théorème 1 est ainsi prouvé. □

Références

[1] O. Klíma, L. Polák, Hierarchies of piecewise testable languages, Int. J. Found. Comput. Sci. 21 (2010), 517-533.

[2] M. V. Volkov, Reflexive relations, extensive transformations and piecewise testable languages of a given height, Int. J. Algebra Comput. 14 (2004) 817-827.