STUDY OF AN IDENTITY

Patrick DEHORNOY

Abstract. We solve the word problem of the identity $x(yz) = (xy)(yz)$ by investigating a certain group describing the geometry of that identity. We also construct a concrete realization of the free system of rank 1 relative to the above identity.

Key words: word problem, free algebras, non-associative binary operation.

MSC 2000: 03D40, 08B20, 20N02.

When we are given an algebraic identity I (or a family of algebraic identities), two questions naturally arise, namely solving the word problem of I, *i.e.*, describing an algorithm recognizing whether two terms are forced to be equal by I, and constructing concrete realizations for the free systems in the equational variety defined by I—and, more generally, constructing concrete examples of systems satisfying I. Of course, answering such questions depends on the considered identity in an essential way, and it seems hopeless to find a uniform method that works for all identities, or, even, for a wide class.

Due to its connection with iterations of elementary embeddings in set theory [10] and with braid groups in low dimensional topology [1], [7], the left self-distributivity identity $x(yz) = (xy)(xz)$ has received some attention in the past decade, and, in particular, the above mentioned questions have been solved by introducing a specific monoid that captures some properties of this identity [4], [6], and which turns out to be connected with Artin's braid groups.

A similar geometry monoid can be associated with associativity [5]. In the latter case, the monoid is essentially R. Thompson's group F [2], and it is closely connected with the well known Mac Lane–Stasheff pentagon [11], [12]. Of course, solving the word problem and constructing realizations of free systems, *i.e.*, of free semigroups, is trivial here.

The geometry monoid exists for every identity, and, more generally, for every family of identities [3]. In the most general case, the monoid is a complicated object, of which we have no control, and it is presumably of little help for solving the word problem. Actually, most of the details in [4] may seem to relie on the specific properties of left self-distributivity, making it unclear that the method can be applied to other identities beyond the more or less trivial case of associativity.

The aim of this paper is to show that the above mentioned scheme does apply to other identities, yet the technical details heavily depend on the considered identity. Here, we shall consider

$$x(yz) = (xy)(yz), \tag{CD}$$

which can be called *central duplication* as it consists in duplicating the central factor y. Identity (CD) has probably never been investigated so far, and it has probably little interest in itself, but it should be clear that the subject of the paper is not really that particular identity, but rather the method we use for studying it, namely investigating the corresponding geometry monoid.

The results we prove are:

Proposition. *(i) The word problem of Identity (CD) is decidable, even primitive recursive.*

(ii) Let G be the group $\langle\{g_\alpha\,;\,\alpha\in\boldsymbol{A}\}\ ;\ R_{CD}\rangle$, where $\boldsymbol{A}$ is the set of all finite sequences of 0's and 1's, and R_{CD} is an effective list of relations given in Lemma 1.3 below; let G_0 be the subgroup of G generated by all $g_{0\alpha}$'s, and let sh_1 be the endomorphism of G that maps g_α to $g_{1\alpha}$ for every α. Then the operation $*$ defined on G by

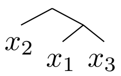
$$a*b=a\cdot\mathrm{sh}_1(b)\cdot g_\phi\cdot\mathrm{sh}_1(b^{-1})$$

induces a well defined operation on the homogeneous set $G_0\backslash G$; the latter operation satisfies Identiy (CD), and every monogenic subsystem of $G_0\backslash G$ is a free CD-system.

The paper is organized as follows. In Sec. 1, we introduce the geometry monoid $\mathcal{G}_{CD}$ associated with Identity (CD), and we establish a list of relations holding in $\mathcal{G}_{CD}$ called CD-relations. In Sec. 2, we study CD-relations from an algebraic point of view, and, in particular, we show that the group G_{CD} for which CD-relations make a presentation is a group of fractions. In Sec. 3, we introduce the blueprint of a term, which is our main tool for constructing a binary operation satisfying a prescribed identity, here (CD). Finally, in Sec. 4, we prove the decidability of the word problem of (CD) by using the blueprint to translate the abstract properties of terms into concrete properties in the group G_{CD}.

1. The geometry monoid

A set equipped with a binary operation satisfying Identity (CD) will be called a *CD-system.* We fix an infinite sequence of variables $x_1, x_2, \ldots$, and, for $1\le n\le\infty$, we use T_n for the set of all well formed terms constructed using $x_1,\ldots,x_n$ and a single binary operator. We define $=_{CD}$ to be the congruence relation on T_n generated by all pairs $(t_0{\cdot}(t_1{\cdot}t_2),(t_0{\cdot}t_1){\cdot}(t_1{\cdot}t_2))$. The quotient system $T_n/{=_{CD}}$ is the free CD-system of rank n based on $x_1,\ldots,x_n$.

In order to specify geometric features precisely, we associate with every term a finite binary tree whose leaves are labelled with variables: if t is the variable x, the tree associated with t consists of a single node labelled x, while, for $t=t_0{\cdot}t_1$, the tree associated with t has a root with two immediate successors, namely a left one which is (the tree associated with) t_0, and a right one which is (the tree associated with) t_1. For instance, the tree associated with $x_2{\cdot}(x_1{\cdot}x_3)$ is 

. We use finite sequences of 0's and 1's as addresses for the nodes in such trees, starting with an empty address ϕ for the root, and using 0 and 1 for going to the left and to the right respectively. In this way, for each term t, we can speak of the α-subterm of t for α a sufficiently short address: for instance, the 0-subterm (or left subterm) of t exists if and only if t is not a variable, and it is t_0 for $t=t_0t_1$.

Definition. For every address α in $\boldsymbol{A}$, we denote by CD_α the partial operator on T_∞ that maps every term t with a well defined α-subterm of the form $s_0{\cdot}(s_1{\cdot}s_2)$ to the term denoted $(t)\alpha$ obtained from t by replacing the α-subterm with $(s_0{\cdot}s_1){\cdot}(s_1{\cdot}s_2)$.

Thus, applying the operator CD_α means applying Identity (CD) in the expanding direction to the subterm with address α. Notice that, for every α, CD_α is an injective partial mapping on T_∞, and its inverse is the symmetric operator CD_α^{-1} corresponding to applying (CD) in the other direction.

Definition. The *geometry monoid* $\mathcal{G}_{CD}$ of Identity (CD) is defined to be the monoid generated by all partial operators CD_α and CD_α^{-1} using composition; the submonoid of $\mathcal{G}_{CD}$ generated by the operators CD_α alone is denoted by $\mathcal{G}_{CD}^+$.

By construction of the congruence $=_{CD}$, we have:

Proposition 1.1. *For all terms t, t' in T_∞, the following are equivalent:*
(i) The terms t, t' are CD-equivalent, i.e., $t =_{CD} t'$ holds;
(ii) Some element of $\mathcal{G}_{CD}$ maps t to t'.

By definition, every element in $\mathcal{G}_{CD}$ is a finite product of operators CD_α and CD_α^{-1}. Such a product can be specified by a word over the alphabet $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, where $\boldsymbol{A}^{-1}$ consists of of a formal inverse α^{-1} for each address α. To this end, we define $\mathrm{CD}_{\alpha^{-1}} = \mathrm{CD}_\alpha^{-1}$, and $\mathrm{CD}_{uv} = \mathrm{CD}_v \circ \mathrm{CD}_u$—as the elements of $\mathcal{G}_{CD}$ act on terms on the right, it is convenient to use reversed composition. Extending the previous notation, we write $t' = (t)w$ when t' is the image of t under CD_w. We use $\boldsymbol{A}^*$ for the set of all words on $\boldsymbol{A}$, *i.e.*, the free monoid generated by $\boldsymbol{A}$, and $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ for the set of all words on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$. We use ε for the empty word, and define CD_ε to be the identity mapping on T_∞.

The operators CD_w can be described using term unification techniques. Let us say that a term t in T_∞ is *canonical* if the variables of t make an initial segment of $(x_1, x_2, \ldots)$ when enumerated from left to right skipping repetitions; let us say that the pair of terms (t_0, t'_0) is an instance of the pair (t, t') if there exists a substitution h satisfying $t_0 = h(t)$ and $t'_0 = h(t')$; finally, let us say that a term t is *injective* if no variable occurs twice or more in t. *Mutatis mutandis*, the results of [7, Chap.VII] give:

Proposition 1.2. *(i) For every word w on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, either the operator CD_w is empty, or there exists a unique pair of CD-equivalent canonical terms (t_w^L, t_w^R) such that CD_w maps t to t' if and only if the pair (t, t') is an instance of (t_w^L, t_w^R).*
(ii) For every word u on $\boldsymbol{A}$, the operator CD_u is nonempty, and the term t_u^L is injective.

We look now for a presentation of the monoids $\mathcal{G}_{CD}$ and $\mathcal{G}_{CD}^+$. As in the case of left self-distributivity [7] and of associativity [5] , we consider relations in $\mathcal{G}_{CD}^+$ of the special type $\ldots \circ \mathrm{CD}_\alpha = \ldots \circ \mathrm{CD}_\beta$, *i.e.*, for each pair of distinct addresses (α, β), we look for possible finite sequences of addresses u, v satisfying $\mathrm{CD}_{\alpha \cdot u} = \mathrm{CD}_{\beta \cdot v}$.

Lemma 1.3. *Let us say that a pair of words on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$ is a CD-relation if it is of one of the following types:*

$$\begin{aligned} &\gamma 0\alpha \cdot \gamma 1\beta \ , \ \gamma 1\beta \cdot \gamma 0\alpha && \textit{(type } \perp\textit{)} \\ &\gamma 0\alpha \cdot \gamma \ , \ \gamma \cdot \gamma 00\alpha && \textit{(type 0)} \\ &\gamma 10\alpha \cdot \gamma \ , \ \gamma \cdot \gamma 01\alpha \cdot \gamma 10\alpha && \textit{(type 10)} \\ &\gamma 11\alpha \cdot \gamma \ , \ \gamma \cdot \gamma 11\alpha && \textit{(type 11)} \\ &\gamma 1 \cdot \gamma \cdot \gamma 0 \ , \ \gamma \cdot \gamma 1 \cdot \gamma && \textit{(type 1)} \end{aligned}$$

Then we have $\mathrm{CD}_w = \mathrm{CD}_{w'}$ for every CD-relation (w, w').

Proof. Type $\perp$ relations are trivial. For types 0, 10, and 11, we observe that, when CD_γ maps t to t', then the $\gamma 0\alpha$-subterm of t (if it exists) is copied to the $\gamma 00\alpha$-subterm of t', the $\gamma 11\alpha$-subterm is preserved, and the $\gamma 10\alpha$-subterm of t has two copies in t', at $\gamma 01\alpha$ and $\gamma 10\alpha$. The last relation is less obvious, and, in some sense, it is characteristic of the identity we consider. Verifying the relation amounts to verifying (for $\gamma = \phi$) that both $\mathrm{CD}_{1\cdot\phi\cdot 0}$ and $\mathrm{CD}_{\phi\cdot 1\cdot\phi}$ map $x_1{\cdot}(x_2{\cdot}(x_3{\cdot}x_4))$ to $((x_1{\cdot}x_2){\cdot}(x_2{\cdot}x_3)){\cdot}((x_2{\cdot}x_3){\cdot}(x_3{\cdot}x_4))$. ∎

At this point, we do not claim that CD-relations exhaust all possible relations in $\mathcal{G}_{CD}$, but we can state:

Corollary 1.4. *(i) Let $\equiv^+$ denote the congruence on $\boldsymbol{A}^*$ generated by all CD-relations. Then, for all words u, u' on $\boldsymbol{A}$, $u \equiv^+ u'$ implies $\mathrm{CD}_u = \mathrm{CD}_{u'}$.*

(ii) Define $M_{CD} = \boldsymbol{A}^*/{\equiv^+}$. Then $\mathcal{G}_{CD}^+$ is a quotient of M_{CD}.

2. The group G_{CD}

An unpleasant feature with the monoid $\mathcal{G}_{CD}$ is its consisting of partial operators only: for every address α, the operator $\mathrm{CD}_{\alpha\cdot\alpha^{-1}}$ is the identity mapping of its domain only, and the latter is a proper subset of T_∞. The existence of words w such that CD_w is empty makes it impossible to identify all such partial identity mappings—as is possible in the case of associativity, and, more generally, of every identity of which both sides are injective terms. To overcome the problem here, we introduce the group G_{CD} for which CD-relations form a presentation. The leading principle in the sequel is that G_{CD} should resemble $\mathcal{G}_{CD}$, and, in particular, every notion or result about $\mathcal{G}_{CD}$ established using its action on terms via Identity (CD) should admit a purely syntactic counterpart involving G_{CD}.

Definition. We denote by $\equiv$ the congruence on $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ generated by all CD-relations together with all pairs $(\alpha\cdot\alpha^{-1}, \varepsilon)$ and $(\alpha^{-1}\cdot\alpha, \varepsilon)$ with $\alpha \in \boldsymbol{A}$. The group $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*/{\equiv}$ is denoted by G_{CD}; for $\alpha \in \boldsymbol{A}$, the element of G_{CD} represented by α is denoted g_α.

All subsequent results originate in the specific properties of the group G_{CD}, which themselves come from geometric properties of (CD). The main technical point is that every element of G_{CD} can be expressed as a right fraction of the form ab^{-1}, where a and b admit expressions where no negative letter α^{-1} occurs. This follows from the existence of right lcm's in the monoid M_{CD}, which will be proved now using a uniform method called word reversing.

By definition, the CD-relations involved in the presentation of the monoid M_{CD} and of the group G_{CD} all are of the type

$$\alpha \cdot \ldots = \beta \cdot \ldots,$$

and, more precisely, for every pair of addresses (α, β), there exists exactly one CD-relation of this type. Let us define the mapping $f_{CD} : \boldsymbol{A} \times \boldsymbol{A} \to \boldsymbol{A}^*$ by

$$f_{CD}(\alpha,\beta) = \begin{cases} \varepsilon & \text{for } \alpha = \beta, \\ \alpha00\gamma & \text{for } \beta = \alpha0\gamma, \\ \alpha01\gamma\cdot\alpha10\gamma & \text{for } \beta = \alpha10\gamma, \\ \alpha1\cdot\alpha & \text{for } \beta = \alpha1, \\ \beta\cdot\beta0 & \text{for } \alpha = \beta1, \\ \beta & \text{in all other cases.} \end{cases}$$

Then $\equiv^+$ is the congruence on $\boldsymbol{A}^*$ generated by all pairs $(\alpha f_{CD}(\alpha,\beta), \beta f_{CD}(\beta,\alpha))$. A general study of those monoids and groups with a presentation associated with a mapping f as above can be developed along the lines of Garside's seminal paper [8]. Here we extract those results needed for our current approach. We refer to [7, Chap.II] for proofs.

By construction, we have $\alpha f(\alpha,\beta) \equiv \beta f(\beta,\alpha)$ for all α, β, hence $\alpha^{-1}\beta \equiv f(\alpha,\beta)f(\beta,\alpha)^{-1}$. Let us say that a word w on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$ is *reversible* to another word w' if w' is obtained from w by repeatedly replacing some factors $\alpha^{-1}\beta$ with the corresponding factors $f(\alpha,\beta)f(\beta,\alpha)^{-1}$. By construction, w being reversible to w' implies $w \equiv w'$.

The words that are terminal for word reversing are those words of the form uv^{-1}, where u and v are words on $\boldsymbol{A}$. It is easy to show that every word w on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$ is reversible to at most one word of the form uv^{-1} with u, $v \in \boldsymbol{A}^*$. When they exist, the latter words will be denoted $N(w)$ and $D(w)$ respectively: by definition, $w \equiv N(w)D(w)^{-1}$ holds, and we can think of $N(w)$ and $D(w)$ as the numerator and the denominator of w.

Definition. For u, v words on $\boldsymbol{A}$, we define $u\backslash v = N(u^{-1}v)$, when the latter exists.

The operation $\backslash$ is a partial binary operation on $\boldsymbol{A}^*$. By definition, we have $\alpha\backslash\beta = f(\alpha, \beta)$ when α, β are addresses: $\backslash$ is an extension of f to arbitrary positive words.

Lemma 2.1. *Assume that u, v are words on $\boldsymbol{A}$ and $u\backslash v$ exists. Then $v\backslash u$ exists as well, and we have $u(u\backslash v) \equiv^+ v(v\backslash u)$.*

In particular, $u\backslash v = v\backslash u = \varepsilon$ implies $u \equiv^+ v$. We say that word reversing is *complete* when the converse implication holds, *i.e.*, when word reversing always detects positive word equivalence. This need not be the case, but we have the following effective sufficient conditions:

Proposition 2.2. [7] *Assume that f is a mapping of $A \times A$ to A^* such that $f(x, x) = \varepsilon$ holds for every x, and f satisfies the following conditions:*
(i) There exists a mapping $\nu : A^* \to \mathbf{N}$ such that $\nu(uxf(x, y)v) = \nu(uyf(y, x)v)$ and $\nu(xu) > \nu(u)$ hold for all x, y in A, and all u, v in A^*;
(ii) For all x, y, z in A, the word

$$((x\backslash y)\backslash(x\backslash z))\backslash((y\backslash x)\backslash(y\backslash z))$$

exists and it is empty.
Then word reversing associated with f is complete, the monoid M associated with f admits left cancellation, and any two elements of M that admit a common right multiple admit a right lcm.

Lemma 2.3. *The mapping f_{CD} satisfies Condition (i) of Proposition* 2.2.

Proof. For t a term, define the size of t to be the number of occurrences of variables in t. We observe that each operator CD_α increases the size of the terms. We put

$$\nu(u) = \mathrm{size}(t_u^R) - \mathrm{size}(t_u^L),$$

where t_u^L and t_u^R are the canonical terms involved in Proposition 1.2. By construction, $u \equiv^+ u'$ implies $\mathrm{CD}_u = \mathrm{CD}_{u'}$, so $\nu(u)$ depends of the $\equiv^+$-class of u only. Assume $\alpha \in \boldsymbol{A}$, and $u \in \boldsymbol{A}^*$. By definition, we have $t_{\alpha\cdot u}^R = ((t_{\alpha\cdot u}^L)\alpha)u$, hence $(t_{\alpha\cdot u}^L)\alpha = h(t_u^L)$ and $t_{\alpha\cdot u}^R = h(t_u^R)$ for some substitution h. We deduce

$$\begin{aligned}\nu(\alpha\cdot u) = \mathrm{size}(t_{\alpha\cdot u}^R) - \mathrm{size}(t_{\alpha\cdot u}^L) &= \mathrm{size}(t_{\alpha\cdot u}^R) - \mathrm{size}((t_{\alpha\cdot u}^L)\alpha) + \mathrm{size}((t_{\alpha\cdot u}^L)\alpha) - \mathrm{size}(t_{\alpha\cdot u}^L)\\ &= \mathrm{size}(h(t_u^R)) - \mathrm{size}(h(t_u^L)) + \mathrm{size}((t_{\alpha\cdot u}^L)\alpha) - \mathrm{size}(t_{\alpha\cdot u}^L)\\ &> \mathrm{size}(h(t_u^R)) - \mathrm{size}(h(t_u^L)) \geq \mathrm{size}(t_u^R) - \mathrm{size}(t_u^L) = \nu(u).\end{aligned}$$

So the mapping ν satisfies the required conditions. ■

Lemma 2.4. *The mapping f_{CD} satisfies Condition (ii) of Proposition* 2.2.

Proof. A priori, a lot of cases have to be considered, according to all possible mutual positions of three addresses α, β, γ. However, almost all cases are automatically satisfied, as explained in [5]. Because ϕ, 1, and 0 are the only internal addresses in the two terms $x(yz)$, $(xy)(yz)$ involved in (CD), the only non-trivial cases here are the triples $(\phi, 1, 11)$, $(\phi, 0, 1)$, and their permuted images. In the first case, we find

$$\begin{cases} \phi\backslash 1 = 1{\cdot}\phi, \\ 1\backslash\phi = \phi{\cdot}0, \end{cases} \qquad \begin{cases} 1\backslash 11 = 11{\cdot}1, \\ 11\backslash 1 = 1{\cdot}10, \end{cases} \qquad \begin{cases} \phi\backslash 11 = \phi, \\ 11\backslash\phi = \phi, \end{cases}$$

$$(\phi\backslash 1)\backslash(\phi\backslash 11) = (1\cdot\phi)\backslash\phi = 11\cdot 1\cdot\phi, \qquad (1\cdot\phi)\backslash(1\cdot 11) = (\phi\cdot 0)\backslash(11\cdot 1) = 11\cdot 1\cdot\phi,$$
$$(\phi\backslash 11)\backslash(\phi\backslash 1) = 11\backslash(1\cdot\phi) = 1\cdot 10\cdot\phi\cdot 0, \qquad (11\cdot\phi)\backslash(11\cdot 1) = \phi\backslash(1\cdot 10) = 1\cdot\phi\cdot 01\cdot 0\cdot 10,$$
$$(1\backslash 11)\backslash(1\backslash\phi) = (11\cdot 1)\backslash(\phi\cdot 0) = \phi\cdot 0\cdot 00, \qquad (11\cdot 1)\backslash(11\cdot\phi) = (1\cdot 10)\backslash\phi = \phi\cdot 0\cdot 00,$$
$$(11\cdot 1\cdot\phi)\backslash(11\cdot 1\cdot\phi) = \varepsilon,$$
$$(1\cdot 10\cdot\phi\cdot 0)\backslash(1\cdot\phi\cdot 01\cdot 0\cdot 10) = (1\cdot\phi\cdot 01\cdot 0\cdot 10)\backslash(1\cdot 10\cdot\phi\cdot 0) = \varepsilon,$$
$$(\phi\cdot 0\cdot 00)\backslash(\phi\cdot 0\cdot 00) = \varepsilon.$$

The verifications are similar (and simpler) in the case of $(\phi, 0, 1)$. ■

Applying Proposition 2.2, we deduce:

Proposition 2.5. *Word reversing associated with f_{CD} is complete, the monoid M_{CD} admits left cancellation, and any two elements of M_{CD} that admit a common right multiple admit a right lcm.*

We prove now that word reversing always terminates, *i.e.*, equivalently, that any two elements of M_{CD} admit a common right multiple. The technique we use is reminiscent of Garside's proof that any two elements in a braid monoid B_n^+ admit a common right multiple resorting to a distinguished element Δ_n that is a common multiple of all generators. Here the monoid M_{CD} is not of finite type, but we can introduce some elements Δ_t indexed by terms which are local counterparts to the braids Δ_n. The intuition for constructing the element Δ_t comes from the action of M_{CD} on terms.

For t a term, we define the *right height* $\mathrm{ht}_R(t)$ of t to be the length of the rightmost branch in t viewed as a tree, *i.e.*, we put $\mathrm{ht}_R(t) = 0$ for t a variable, and $\mathrm{ht}_R(t_0{\cdot}t_1) = \mathrm{ht}_R(t_1) + 1$.

Definition. For $\alpha \in \boldsymbol{A}$, we put $\alpha^{(p)} = \varepsilon$ for $p \leq 0$, and $\alpha^{(p)} = \alpha 1^{p-1}{\cdot}\ldots{\cdot}\alpha 1{\cdot}\alpha$ for $p > 0$.

If t has right height h, then $(t)\phi^{(p)}$ is defined exactly for $p < h$. In this case, assuming $t = t_0{\cdot}(t_1{\cdot}(\ldots(t_{h-1}{\cdot}x)\ldots))$ with x a variable, we have $(t)\phi^{(p)} = s_0{\cdot}(s_1{\cdot}(\ldots(s_{h-1}{\cdot}x\ldots))$ with $s_i = t_i{\cdot}(t_{i+1}{\cdot}(\ldots(t_{p-1}{\cdot}t_p)\ldots))$ for $i \leq p-1$ and $s_i = t_i$ for $i \geq p$.

Notation. For w a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$ and α an address, we write αw for the word obtained from w by replacing each letter $\gamma^{\pm 1}$ with the letter $(\alpha\gamma)^{\pm 1}$—not to be confused with the word $\alpha{\cdot}w$: for w of length n, αw has length n, while $\alpha{\cdot}w$ has length $n+1$.

Definition. For t is a term of right height h, and $(t)\phi^{(h-1)} = s_0{\cdot}(s_1{\cdot}(\ldots(s_{h-1}{\cdot}x)\ldots))$, we put

$$\Delta_t = \phi^{(h-1)} \cdot 0\Delta_{s_0} \cdot 10\Delta_{s_1} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}}.$$

The inductive definition of the word Δ_t makes sense as, by construction, $\mathrm{size}(s_i) < \mathrm{size}(t)$ always holds. We begin with auxiliary results.

Lemma 2.6. *For $0 \le p \le r-2$, $0 \le q \le r-1$, and for every word u on $\boldsymbol{A}$, we have*

$$1^p \cdot \phi^{(r)} \equiv^+ \phi^{(r)} \cdot 01^p \cdot 101^{p-1} \cdot \ldots \cdot 1^p0 \tag{2.1}$$
$$1^q0u \cdot \phi^{(r)} \equiv^+ \phi^{(r)} \cdot 01^q0u \cdot 101^{q-1}0u \cdot \ldots \cdot 1^q00u, \tag{2.2}$$
$$1^r0u \cdot \phi^{(r)} \equiv^+ \phi^{(r)} \cdot 01^ru \cdot \ldots \cdot 1^{r-1}01u \cdot 1^r0u. \tag{2.3}$$
$$\phi^{(q)} \cdot \phi^{(r)} \equiv^+ \phi^{(r)} \cdot 0^{(q)} \cdot 10^{(q-1)} \cdot \ldots \cdot 1^{q-1}0. \tag{2.4}$$

Proof. We prove (2.1) using induction on p. For $p=0$ and $r \ge 2$, we have

$$\phi \cdot \phi^{(r)} = \phi \cdot 11^{(r-2)} \cdot 1 \cdot \phi \equiv^+ 11^{(r-2)} \cdot \phi \cdot 1 \cdot \phi \equiv^+ 11^{(r-2)} \cdot 1 \cdot \phi \cdot 0 = \phi^{(r)} \cdot 0.$$

For $p > 0$, observing that $u \equiv^+ u'$ implies $1u \equiv^+ 1u'$, we obtain (we mention the type of CD-relation used at each step)

$$\begin{aligned}
1^p \cdot \phi^{(r)} = 11^{p-1} \cdot 1^{(r-1)} \cdot \phi &\equiv^+ 1^{(r-1)} \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^p0 \cdot \phi && \text{by ind. hyp.}\\
&\equiv^+ 1^{(r-1)} \cdot 101^{p-1} \cdot \phi \cdot 1101^{p-2} \cdot \ldots \cdot 1^p0 && (11)\\
&\equiv^+ 1^{(r-1)} \cdot \phi \cdot 01^p \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^p0 && (10)\\
&= \phi^{(r)} \cdot \phi \cdot 01^p \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^p0.
\end{aligned}$$

We prove (2.2) using induction on q. For $q=0$ and $r > 0$, we have

$$0u \cdot \phi^{(r)} \equiv^+ 1^{(r-1)} \cdot 0u \cdot \phi \equiv^+ 1^{(r-1)} \cdot \phi \cdot 00u = \phi^{(r)} \cdot 00u.$$

For $q > 0$, applying the induction hypothesis to $1^{q-1}0u$ and $\phi^{(r-1)}$ and shifting all addresses by 1, we find

$$\begin{aligned}
1^q0u \cdot \phi^{(r)} &= 11^{q-1}0u \cdot 1^{(r-1)} \cdot \phi\\
&\equiv^+ 1^{(r-1)} \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^q00u \cdot \phi && \text{by ind. hyp.}\\
&\equiv^+ 1^{(r-1)} \cdot 101^{q-1}0u \cdot \phi \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^q00u && (11)\\
&\equiv^+ 1^{(r-1)} \cdot \phi \cdot 01^q0u \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^q00u && (10)\\
&= \phi^{(r)} \cdot 01^q0u \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^q00u.
\end{aligned}$$

We prove (2.3) using induction on $r \ge 0$. For $r=0$, (2.3) is an equality; for $r > 0$, we find

$$\begin{aligned}
1^r0u \cdot \phi^{(r)} &= 11^{r-1}0u \cdot 1^{(r-1)} \cdot \phi\\
&\equiv^+ 1^{(r-1)} \cdot 101^{r-1}u \cdot 1101^{r-2}u \cdot \ldots \cdot 1^{r-1}01u \cdot 1^r0u \cdot \phi && \text{by ind. hyp.}\\
&\equiv^+ 1^{(r-1)} \cdot 101^{r-1}u \cdot \phi \cdot 1101^{r-2}u \cdot \ldots \cdot 1^{r-1}01u \cdot 1^r0u && (11)\\
&\equiv^+ 1^{(r-1)} \cdot \phi \cdot 01^ru \cdot 101^{r-1}u \cdot \ldots \cdot 1^{r-1}01u \cdot 1^r0u && (10)\\
&= \phi^{(r)} \cdot 01^ru \cdot 101^{r-1}u \cdot \ldots \cdot 1^{r-1}01u \cdot 1^r0u.
\end{aligned}$$

Finally, (2.4) follows from applying (2.1) to ϕ, 1, …, 1^{q-1} respectively, and gathering the factors using $(\perp)$-relations. ■

Lemma 2.7. *Assume $t = t_0{\cdot}(t_1{\cdot}(\ldots(t_k{\cdot}t_*)\ldots))$. Let $t'_i = t_i{\cdot}(t_{i+1}{\cdot}(\ldots(t_{k-1}{\cdot}t_k)\ldots))$ for $i \le k$. Then there exists a word u on $\boldsymbol{A}$ satisfying*

$$\varDelta_t \equiv^+ \phi^{(k)} \cdot 0\varDelta_{t'_0} \cdot 10\varDelta_{t'_1} \cdot \ldots \cdot 1^k0\varDelta_{t'_k} \cdot 1^{k+1}\varDelta_{t_*} \cdot u. \tag{2.5}$$

Proof. We use induction on the size of t. Let $h = \mathrm{ht}_R(t)$. The result is trivial if t is a variable, and, more generally, for $k = h-1$: indeed, in this case, Δ_{t_*} is empty, and the right hand expression in (2.5) with $u = \varepsilon$ is the definition of Δ_t. Assume now $0 \le k \le h-2$. Write $t = t_0{\cdot}(t_1{\cdot}(\ldots(t_{h-1}{\cdot}x)\ldots))$ with x a variable. Then we have $t_* = t_{k+1}{\cdot}(\ldots{\cdot}(t_{h-1}{\cdot}x)\ldots)$. Let $s_i = t_i{\cdot}(t_{i+1}{\cdot}(\ldots(t_{h-2}{\cdot}t_{h-1})\ldots))$ for $i < h$. By definition, we have

$$\Delta_t = \phi^{(h-1)} \cdot 0\Delta_{s_0} \cdot 10\Delta_{s_1} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}},$$
$$1^k\Delta_{t_*} = (1^{k+1})^{(h-k-2)} \cdot 1^{k+1}0\Delta_{s_{k+1}} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}}.$$

By construction, we have $s_i = t_i{\cdot}(t_{i+1}{\cdot}(\ldots(t_k{\cdot}s_{k+1})\ldots))$ and $\mathrm{size}(s_i) < \mathrm{size}(t)$ for $i \le k$, so, by induction hypothesis, there exists a word u_i on $\boldsymbol{A}$ satisfying

$$\Delta_{s_i} \equiv^+ \phi^{(k-i)} \cdot 0\Delta_{t'_i} \cdot \ldots \cdot 1^{k-i}0\Delta_{t'_k} \cdot 1^{k-i+1}\Delta_{s_{k+1}} \cdot u_i.$$

Injecting these values in Δ_t, and using ($\perp$)-relations to push the factors $1^i0^{(k-i)}$ to the left and the factors 1^i0u_i and $1^i01^j0\Delta_{t'_j}$ to the right, we obtain

$$\begin{aligned}\Delta_t \equiv^+ &\phi^{(h-1)} \cdot 0^{(k)} \cdot 10^{(k-1)} \cdot \ldots \cdot 1^{k-1}0^{(1)} \cdot 00\Delta_{t'_0} \cdot 010\Delta_{t'_1} \cdot 100\Delta_{t'_1} \cdot 0110\Delta_{t'_2} \cdot \ldots \cdot 1100\Delta_{t'_2}\\ &\cdot \ldots \cdot 01^k0\Delta_{t'_k} \cdot \ldots \cdot 1^k00\Delta_{t'_k} \cdot 01^{k+1}\Delta_{s_{k+1}} \cdot \ldots \cdot 1^k01\Delta_{s_{k+1}} \cdot 1^{k+1}0\Delta_{s_{k+1}}\\ &\cdot 1^{k+2}0\Delta_{s_{k+2}} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}} \cdot 0u_0 \cdot 10u_1 \cdot \ldots \cdot 1^k0u_k.\end{aligned}$$

Applying (2.4) with $r = h-1$ and $q = k$, then (2.2) with $r = h-1$, $q = 0$, $u = \Delta_{t'_0}$, then $q = 1$, $u = \Delta_{t'_1}$, ..., $q = k$, $u = \Delta_{t'_k}$ successively, and, finally, (2.3) with $r = k+1$ and $u = \Delta_{s_{k+1}}$, we deduce

$$\begin{aligned}\Delta_t &\equiv^+ \phi^{(k)} \cdot 0\Delta_{t'_0} \cdot 10\Delta_{t'_1} \cdot \ldots \cdot 1^k0\Delta_{t'_k} \cdot (1^{k+1})^{(h-k-2)} \cdot 1^{k+1}0\Delta_{s_{k+1}} \cdot \phi^{(k+1)}\\ &\qquad\qquad \cdot 1^{k+2}0\Delta_{s_{k+2}} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}} \cdot 0u_0 \cdot \ldots \cdot 1^k0u_k\\ &\equiv^+ \phi^{(k)} \cdot 0\Delta_{t'_0} \cdot 10\Delta_{t'_1} \cdot \ldots \cdot 1^k0\Delta_{t'_k} \cdot (1^{k+1})^{(h-k-2)} \cdot 1^{k+1}0\Delta_{s_{k+1}}\\ &\qquad\qquad \cdot 1^{k+2}0\Delta_{s_{k+2}} \cdot \ldots \cdot 1^{h-1}0\Delta_{s_{h-1}} \cdot \phi^{(k+1)} \cdot 0u_0 \cdot \ldots \cdot 1^k0u_k \qquad (11)\\ &= \phi^{(k)} \cdot 0\Delta_{t'_0} \cdot 10\Delta_{t'_1} \cdot \ldots \cdot 1^k0\Delta_{t'_k} \cdot 1^{k+1}\Delta_{t_*} \cdot \phi^{(k+1)} \cdot 0u_0 \cdot \ldots \cdot 1^k0u_k\end{aligned}$$
∎

Lemma 2.8. *Assume that $(t)\alpha$ is defined. Then $\alpha{\cdot}v \equiv^+ \Delta_t$ holds for some word v on $\boldsymbol{A}$.*

Proof. We use induction on the length of α as a word on $\{0, 1\}$. Assume first $\alpha = \phi$. The hypothesis that $(t)\phi$ is defined implies $\mathrm{ht}_R(t) \ge 2$. Hence t can be expressed as $t = t_0(t_1t_*)$. Applying Lemma 2.7 with $k = 2$, we obtain

$$\Delta_t \equiv^+ \phi \cdot 0\Delta_{t_0t_1} \cdot 10\Delta_{t_1} \cdot 11\Delta_{t_*} \cdot u$$

which begins with α explicitly.

Assume now $\alpha = 0\beta$. The hypothesis that $(t)\alpha$ is defined implies that t is not a variable, so it can be written as $t = t_0t_*$, with $(t_0)\beta$ defined. Applying Lemma 2.7 with $k = 1$, we obtain u satisfying $\Delta_t \equiv^+ 0\Delta_{t_0}{\cdot}1\Delta_{t_*}{\cdot}u$, and, applying the induction hypothesis, we obtain v satisfying $\Delta_{t_0} \equiv^+ \beta{\cdot}v$. We deduce

$$\Delta_t \equiv^+ 0\Delta_{t_0} \cdot 1\Delta_{t_*} \cdot u \equiv^+ 0\beta \cdot 0v \cdot 1\Delta_{t_*} \cdot u = \alpha \cdot 0v \cdot 1\Delta_{t_*} \cdot u,$$

which begins with α explicitly. The argument is similar for $\alpha = 1\beta$, as $0\Delta_{t_0}$ and $1\Delta_{t_*}$ commute up to $\equiv^+$-equivalence. ∎

Lemma 2.9. *Assume that u is a word on $\boldsymbol{A}$ and $(t)u$ is defined, say $t' = (t)u$. Then we have $u{\cdot}\Delta_{t'} \equiv^+ \Delta_t{\cdot}u'$ for some word u' on $\boldsymbol{A}$.*

Proof. We prove using induction on n that, for every word u of length n, the result is true for every term t such that $(t)u$ exists. For $n = 0$, *i.e.*, for $u = \varepsilon$, the property is obvious. Assume $n = 1$. Then u consists of a single address, say α. We prove the result using induction on the size of t. Let $h = \mathrm{ht}_R(t)$, $t = t_0{\cdot}(t_1{\cdot}(\ldots(t_{h-1}{\cdot}x)\ldots))$, and $(t)\phi^{(h-1)} = s_0{\cdot}(s_1{\cdot}(\ldots(s_{h-1}{\cdot}x)\ldots))$. Assume $t' = (t)\alpha$. We write similarly $t' = t'_0{\cdot}(t'_1{\cdot}(\ldots(t'_{h-1}{\cdot}x)\ldots))$, and $(t')\phi^{(h-1)} = s'_0{\cdot}(s'_1{\cdot}(\ldots(s'_{h-1}{\cdot}x)\ldots))$. We distinguish four cases according to α.

Assume first $\alpha = 1^p$ with $0 \le p \le h-3$. Then we have $t'_i = t_i$ for $i \ne p$, and $t'_p = t_p{\cdot}t_{p+1}$. A direct computation gives $s'_i = (s_i)1^{p-i}$ for $i \le p$, and $s'_i = s_i$ for $i > p$. For $i \le p$, the induction hypothesis gives a word u'_i on $\boldsymbol{A}$ satisfying $1^{p-i}{\cdot}\Delta_{s'_i} \equiv^+ \Delta_{s_i}{\cdot}u'_i$. We obtain

$$\begin{aligned}
\alpha\cdot\Delta_{t'} &= 1^p\cdot\phi^{(h-1)}\cdot 0\Delta_{s'_0}\cdot 10\Delta_{s'_1}\cdot\ldots\cdot 1^{h-1}0\Delta_{s'_{h-1}} \\
&\equiv^+ \phi^{(h-1)}\cdot 01^p\cdot\ldots\cdot 1^p0\cdot 0\Delta_{s'_0}\cdot 10\Delta_{s'_1}\cdot\ldots\cdot 1^{h-1}0\Delta_{s'_{h-1}} && \text{by (2.1)}\\
&\equiv^+ \phi^{(h-1)}\cdot 01^p\cdot 0\Delta_{s'_0}\cdot\ldots\cdot 1^p0\cdot 1^p0\Delta_{s'_p}\cdot 1^{p+1}0\Delta_{s_{p+1}}\cdot\ldots\cdot 1^{h-1}0\Delta_{s_{h-1}} && (\perp)\\
&\equiv^+ \phi^{(h-1)}{\cdot}0\Delta_{s_0}{\cdot}0u'_0{\cdot}\ldots{\cdot}1^p0\Delta_{s_p}{\cdot}1^p0u'_p{\cdot}1^{p+1}0\Delta_{s_{p+1}}{\cdot}\ldots{\cdot}1^{h-1}0\Delta_{s_{h-1}} && \text{by ind. hyp.}\\
&\equiv^+ \phi^{(h-1)}{\cdot}0\Delta_{s_0}{\cdot}\ldots{\cdot}1^p0\Delta_{s_p}{\cdot}1^{p+1}0\Delta_{s_{p+1}}{\cdot}\ldots{\cdot}1^{h-1}0\Delta_{s_{h-1}}{\cdot}0u'_0{\cdot}\ldots{\cdot}1^p0u'_p && (\perp)\\
&= \Delta_t\cdot 0u'_0\cdot\ldots\cdot 1^p0u'_p
\end{aligned}$$

Assume now $\alpha = 1^{h-2}$. We still have $s'_{h-1} = s_{h-1} (= t_{h-1})$, but, for $i < h$, we have $s'_i = t_0{\cdot}(t_1{\cdot}(\ldots{\cdot}((t_{h-2}{\cdot}t_{h-1}){\cdot}t_{h-1})\ldots))$, which is not a CD-expansion of s_i. Applying Lemma 2.7 to t' with $k = h-2$ (this is the point), we obtain a word u' on $\boldsymbol{A}$ satisfying

$$\Delta_{t'} \equiv^+ \phi^{(h-2)}\cdot 0\Delta_{s_0}\cdot 10\Delta_{s_1}\cdot\ldots\cdot 1^{h-2}0\Delta_{s_{h-2}}\cdot 1^{h-1}\Delta_{t_{h-1}\cdot x}\cdot u'.$$

By definition, we have $\Delta_{t_{h-1}\cdot x} = 0\Delta_{t_{h-1}}$ and $s_{h-1} = t_{h-1}$, so we deduce

$$\alpha\cdot\Delta_{t'} \equiv^+ 1^{h-2}\cdot\phi^{(h-2)}\cdot 0\Delta_{s_0}\cdot 10\Delta_{s_1}\cdot\ldots\cdot 1^{h-2}0\Delta_{s_{h-2}}\cdot 1^{h-1}0\Delta_{s_{h-1}}\cdot u' = \Delta_t\cdot u'.$$

Assume now $\alpha = 1^p0\beta$ with $0 \le p \le h-2$. With the same notations, we have $t'_i = t_i$ for $i \ne p$, and $t'_p = (t_p)\beta$. We deduce $s'_i = (s_i)1^{p-i}0\beta$ for $i \le p$, $s'_i = s_i$ for $i > p$. For $i \le p$, the induction hypothesis gives a word u'_i satisfying $1^{p-i}0\beta{\cdot}\Delta_{s'_i} \equiv^+ \Delta_{s_i}{\cdot}u'_i$, and we find

$$\begin{aligned}
\alpha\cdot\Delta_{t'} &= 1^p0\beta\cdot\phi^{(h-1)}\cdot 0\Delta_{s'_0}\cdot\ldots\cdot 1^p0\Delta_{s'_p}\cdot\ldots\cdot 1^{h-1}0\Delta_{s'_{h-1}}\\
&\equiv^+ \phi^{(h-1)}\cdot 01^p0\beta\cdot\ldots\cdot 1^p00\beta\cdot 0\Delta_{s'_0}\cdot\ldots\cdot 1^p0\Delta_{s'_p}\cdot\ldots\cdot 1^{h-1}0\Delta_{s'_{h-1}} && \text{by (2.2)}\\
&\equiv^+ \phi^{(h-1)}\cdot 01^{p-1}0\beta\cdot 0\Delta_{s'_1}\cdot\ldots\cdot 1^p00\beta\cdot 1^p0\Delta_{s'_p}\cdot\ldots\cdot 1^{h-1}0\Delta_{s'_{h-1}} && (\perp)\\
&\equiv^+ \phi^{(h-1)}\cdot 0\Delta_{s_0}\cdot 0u'_0\cdot\ldots\cdot 1^p0\Delta_{s_p}\cdot 1^p0u'_p\cdot\ldots\cdot 1^{h-1}0\Delta_{s_{h-1}} && \text{by ind. hyp.}\\
&\equiv^+ \phi^{(h-1)}\cdot 0\Delta_{s_0}\cdot\ldots\cdot 1^p0\Delta_{s_p}\cdot\ldots\cdot 1^{h-1}0\Delta_{s_{h-1}}\cdot 0u'_0\cdot\ldots\cdot 1^p0u'_p && (\perp)\\
&= \Delta_t\cdot 0u'_0\cdot\ldots\cdot 1^p0u'_p.
\end{aligned}$$

Finally, for $\alpha = 1^{h-1}0\beta$, we have $t'_i = t_i$ for $i < h$ and $t'_{h-1} = (t_{h-1})\beta$, hence $s'_i = (s_i)1^{h-i}\beta$. The computation is similar to the previous one, using (2.3) instead of (2.2).

Assume now $n \ge 2$. Write $u = u_1{\cdot}u_2$ with $\mathrm{lg}(u_1), \mathrm{lg}(u_2) < n$. Applying the induction hypothesis to u_1 and u_2, we find words u'_1, u'_2 satisfying

$$u\cdot\Delta_{t'} = u_1\cdot u_2\cdot\Delta_{((t)u_1)u_2} \equiv^+ u_1\cdot\Delta_{(t)u_1}\cdot u'_2 \equiv^+ \Delta_t\cdot u'_1\cdot u'_2. \qquad \blacksquare$$

Definition. For t a term, we put $\partial t = (t)\Delta_t$—which makes sense, as an immediate induction shows that every term t lies in the domain of the operator CD_{Δ_t}.

Lemma 2.10. *Assume that u is a word of length n on $\boldsymbol{A}$, and $(t)u$ is defined. Then $u{\cdot}v \equiv^+ \Delta_t{\cdot}\Delta_{\partial t}{\cdot}\ldots{\cdot}\Delta_{\partial^{n-1}t}$ holds for some word v on $\boldsymbol{A}$.*

Proof. We use induction on n. For $n = 0$, *i.e.*, for $u = \varepsilon$, the result is obvious. For $n = 1$, the result is Lemma 2.8. Otherwise, write $u = u'{\cdot}\alpha$ with α an address, and let $t' = (t)u'$, which exists by hypothesis. By construction, we have $(t)u = (t')\alpha$, hence, by Lemma 2.8, we have $\alpha{\cdot}v' = \Delta_{t'}$ for some v'. By induction hypothesis, there exists u'' satisfying $u'{\cdot}u'' \equiv^+ \Delta_t\Delta_{\partial t}\ldots\Delta_{\partial^{n-2}t}$, hence $(t')u'' = \partial^{n-1}t$. Hence, by Lemma 2.9, we have $u''{\cdot}\Delta_{\partial^{n-1}t} = \Delta_{t'}{\cdot}v''$ for some v''. We find

$$u \cdot v' \cdot v'' \equiv^+ u' \cdot \Delta_{t'} \cdot v'' \equiv^+ u' \cdot u'' \cdot \Delta_{\partial^{n-1}t} \equiv^+ \Delta_t \cdot \ldots \cdot \Delta_{\partial^{n-2}t} \cdot \Delta_{\partial^{n-1}t}.$$ ■

Proposition 2.11. *Any two elements of M_{CD} admit a common right multiple.*

Proof. Assume that u, v are words on $\boldsymbol{A}$. By Proposition 1.2, the terms t_u^L and t_v^L are injective, which implies that some substitute of t_u^L is a substitute of t_v^L. Hence, some term t lies both in the domain of CD_u and CD_v. Letting n be the supremum of the lengths of u and v, we deduce from Lemma 2.10 the existence of two words u' , v' satisfying

$$u \cdot v' \equiv^+ v \cdot u' \equiv^+ \Delta_t \cdot \Delta_{\partial t} \cdot \ldots \cdot \Delta_{\partial^{n-1}t}.$$

The common class of $u{\cdot}v'$ and $v'{\cdot}u$ in M_{CD} is a common right multiple of the classes of u and v in M_{CD}. ■

Returning to word reversing in $\boldsymbol{A}^*$, we deduce from the general results of [7, Chap.II]:

Proposition 2.12. *(i) Word reversing in $(\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ is convergent, i.e., for every word w on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, the words $N(w)$ and $D(w)$ exist.*

(ii) For all words w, w' on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, $w \equiv w'$ holds if and only if we have

$$N(w) \cdot v \equiv^+ N(w') \cdot v', \qquad D(w) \cdot v \equiv^+ D(w') \cdot v' \tag{2.6}$$

for some words v, v' on $\boldsymbol{A}$.

Corollary 2.13. *The word problem of the monoid M_{CD} is decidable.*

Proof. Assume that u, u' are words on $\boldsymbol{A}$. By Proposition 2.5, $u \equiv^+ u'$ holds if and only if reversing $u^{-1}u'$ ends with an empty word. As we know now that reversing $u^{-1}u'$ comes to an end in a finite number of steps, this gives an effective decision method. ■

Let us come back to Identity (CD). For t, t' terms, let us say that t' is a *CD-expansion* of t if $t' = (t)u$ holds for some word u on $\boldsymbol{A}$. If t' is a CD-expansion of t, then t' and t are CD-equivalent, but the converse implication is not true: going to a CD-expansion means applying Identity (CD) in the expanding direction only. The above results imply strong properties for the terms ∂t: Lemma 2.9 implies that the operator ∂ is increasing with respect to CD-expansions, *i.e.*, that $\partial t'$ is a CD-expansion of ∂t whenever t' is a CD-expansion of t, and Lemma 2.10 implies that, for every term t, $\partial^n t$ is a CD-expansion of every CD-expansion of t obtained by applying (CD) n times at most. Finally, Proposition 2.11 implies the following confluence property:

Proposition 2.14. *Any two CD-equivalent terms admit a common CD-expansion.*

Proof. As CD-equivalence is the equivalence relation generated by the relation of being a CD-expansion, it suffices to prove that any two CD-expansions of a term t admit a common CD-expansion: this follows from Proposition 2.11 immediately. ■

Actually, Proposition 2.11 tells us a little more, namely that, for every term t, the term t' is CD-equivalent to t if and only if the term $\partial^n t$ is a CD-expansion of t for n large enough. Building on this remark, unique normal forms with respect to CD-equivalence can be constructed along the lines of [7, Chap.VI].

3. The blueprint of a term

Let us address the question of constructing a monogenic CD-system $(S, *)$: the question is to construct, for each term t in T_1, an interpretation of t in S in such a way that CD-equivalent terms receive the same interpretation. As the only specific algebraic systems available so far are the geometry monoid $\mathcal{G}_{CD}$ and its abstract version G_{CD}, we shall start from these structures: the core of the construction will consist in associating with every term t in T_1 a distinguished element in G_{CD}, or, equivalently, a distinguished word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$. This word arises as a natural translation for the following property:

Lemma 3.1. *Define $x^{[1]} = x$, and $x^{[p+1]} = x{\cdot}x^{[p]}$ for $p \geq 1$. Then, for every term t in T_1, and for p large enough, we have*

$$x^{[p+1]} =_{CD} t{\cdot}x^{[p]}. \tag{3.1}$$

Proof. We use induction on t. For $t = x$, (3.1) is an equality. Otherwise, assuming $t = t_0{\cdot}t_1$ and using the induction hypothesis, we obtain for p large enough

$$x^{[p+1]} =_{CD} t_0{\cdot}x^{[p]} =_{CD} t_0{\cdot}(t_1{\cdot}x^{[p-1]}) =_{CD} (t_0{\cdot}t_1){\cdot}(t_1{\cdot}x^{[p-1]}) =_{CD} (t_0{\cdot}t_1){\cdot}x^{[p]} = t{\cdot}x^{[p]}. \qquad \blacksquare$$

It follows from Proposition 1.1 that, for every term t and for every p large enough, some operator in $\mathcal{G}_{CD}$ maps $x^{[p+1]}$ to $t{\cdot}x^{[p]}$. It suffices to read the inductive proof of Lemma 3.1 to obtain an explicit description of the involved operator.

Definition. For t a term in T_1, the *blueprint* χ_t of t is the word defined by $\chi_x = \varepsilon$ and

$$\chi_t = \chi_{t_0} \cdot \mathrm{sh}_1(\chi_{t_1}) \cdot \phi \cdot \mathrm{sh}_1(\chi_{t_1}^{-1}) \qquad \text{for } t = t_0{\cdot}t_1. \tag{3.2}$$

Proposition 3.2. *For every t in T_1, CD_{χ_t} maps $x^{[p+1]}$ to $t{\cdot}x^{[p]}$ for p large enough.*

Proof. As for Lemma 3.1, we use induction on t. The result is true for $t = x$. Assume $t = t_0{\cdot}t_1$, and p large enough. By induction hypothesis, $\mathrm{CD}_{\chi_{t_0}}$ maps $x^{[p+1]}$ to $t_0{\cdot}x^{[p]}$, and $\mathrm{CD}_{\chi_{t_1}}$ maps $x^{[p]}$ to $t_1{\cdot}x^{[p-1]}$. Hence $\mathrm{CD}_{1\chi_{t_1}}$ maps $t_0{\cdot}x^{[p]}$ to $t_0{\cdot}(t_1{\cdot}x^{[p-1]})$, and, similarly, $\mathrm{CD}_{1\chi_{t_1}^{-1}}$ maps $t{\cdot}(t_1{\cdot}x^{[p-1]})$ to $t{\cdot}x^{[p]}$. By composing, we obtain

$$x^{[p+1]} \overset{\chi_{t_0}}{\mapsto} t_0{\cdot}x^{[p]} \overset{1\chi_{t_1}}{\mapsto} t_0{\cdot}(t_1{\cdot}x^{[p-1]}) \overset{\phi}{\mapsto} (t_0{\cdot}t_1){\cdot}(t_1{\cdot}x^{[p-1]}) = t{\cdot}(t_1{\cdot}x^{[p-1]} \overset{1\chi_{t_1}^{-1}}{\mapsto} t{\cdot}x^{[p]}. \qquad \blacksquare$$

The idea is to use the operator CD_{χ_t}, or, rather, the image of the word χ_t in the group G_{CD}, as the interpretation of the term t, which leads us to introduce the binary operation on G_{CD} such that the class of $\chi_{t_0{\cdot}t_1}$ is the product of the classes of χ_{t_0} and χ_{t_1}.

Definition. For u, v words on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, we define

$$u * v = u \cdot 1v \cdot \phi \cdot 1v^{-1}, \tag{3.3}$$

and we also use $*$ for the induced binary operation on G_{CD}.

With this notation, χ is the homomorphism of T_1 into $((\boldsymbol{A}\cup\boldsymbol{A}^{-1})^*, *)$ that maps x to ε. Our plan is to start from operation $*$ on G_{CD} to construct an operation satisfying Identity (CD). The point is that the latter operation does not satisfy Identity (CD), but the obstruction to its satisfying (CD) can be measured exactly. If t and t' are CD-equivalent terms, their blueprints χ_t and $\chi_{t'}$ need not be $\equiv$-equivalent, but some operator CD_w maps t to t', and, therefore, CD_{0w} maps $t{\cdot}x^{[p]}$ to $t'{\cdot}x^{[p]}$ for every p. Hence, both $\mathrm{CD}_{\chi_t\cdot 0w}$ and $\mathrm{CD}_{\chi_{t'}}$ map $x^{[p+1]}$ to $t'{\cdot}x^{[p]}$ for p large enough. If CD-relations axiomatize the relations in $\mathcal{G}_{CD}$ correctly, we can therefore expect the equivalence $\chi_t\cdot 0w \equiv \chi_{t'}$ to hold—which, if true, must be verifiable by a direct computation.

Lemma 3.3. *Assume $t' = (t)w$. Then we have $\chi_{t'} \equiv \chi_t{\cdot}0w$.*

For an induction on the length of w , it suffices to prove the result when w consists of a single address α. Then, the result follows from:

Lemma 3.4. *For all words u, v, w on $\boldsymbol{A}\cup\boldsymbol{A}^{-1}$, we have*

$$(u * v) * (v * w) \equiv (u * (v * w)) \cdot 0 \tag{3.4}$$

$$(u\cdot 0w) * v \equiv (u * v)\cdot 00w \tag{3.5}$$

$$u * (v\cdot 0w) \equiv (u * v)\cdot 01w \tag{3.6}$$

Proof. Applying the definition of $*$ and CD-relations, we find

$$\begin{aligned}
(u * v) * (v * w) &= u\cdot 1v\cdot \phi\cdot 1v^{-1}\cdot 1v\cdot 11w\cdot 1\cdot 11w^{-1}\cdot\phi\cdot 11w\cdot 1^{-1}\cdot 11w^{-1}\cdot 1v^{-1} \\
&\equiv u\cdot 1v\cdot 11w\cdot\phi\cdot 1\cdot\phi\cdot 1^{-1}\cdot 11w^{-1}\cdot 1v^{-1} && (11)\\
&\equiv u\cdot 1v\cdot 11w\cdot 1\cdot\phi\cdot 0\cdot 1^{-1}\cdot 11w^{-1}\cdot 1v^{-1} && (1)\\
&\equiv u\cdot 1v\cdot 11w\cdot 1\cdot\phi\cdot 1^{-1}\cdot 11w^{-1}\cdot 1v^{-1}\cdot 0 && (\perp)\\
&\equiv u\cdot 1v\cdot 11w\cdot 1\cdot 11w^{-1}\cdot\phi\cdot 11w\cdot 1^{-1}\cdot 11w^{-1}\cdot 1v^{-1}\cdot 0 && (11)\\
&= (u * (v * w))\cdot 0.\\
(u\cdot 0w) * v &= u\cdot 0w\cdot 1v\cdot\phi\cdot 1v^{-1} \equiv u\cdot 1v\cdot 0w\cdot\phi\cdot 1v^{-1} && (\perp)\\
&\equiv u\cdot 1v\cdot\phi\cdot 00w\cdot 1v^{-1} && (0)\\
&\equiv u\cdot 1v\cdot\phi\cdot 1v^{-1}\cdot 00w = (u * v)\cdot 00w && (\perp)\\
u * (v\cdot 0w) &= u\cdot 1v\cdot 10w\cdot\phi\cdot 10w^{-1}\cdot 1v^{-1}\\
&\equiv u\cdot 1v\cdot\phi\cdot 01w\cdot 10w\cdot 10w^{-1}\cdot 1v^{-1} && (10)\\
&\equiv u\cdot 1v\cdot\phi\cdot 01w\cdot 1v^{-1}\\
&\equiv u\cdot 1v\cdot\phi\cdot 1v^{-1}\cdot 01w = (u * v)\cdot 01w && \blacksquare
\end{aligned}$$

Formula (3.4) tells us how to obtain a binary operation satisfying (CD) from $*$ on G_{CD}: it suffices that we collapse g_0. Now (3.5) and (3.6) show that, in order to obtain a well defined induced operation, we have to collapse every generator $g_{0\alpha}$ as well. So we have:

Proposition 3.5. *For every address γ, let sh_γ denote the endomorphism of G_{CD} induced by the address shift $\alpha\mapsto\gamma\alpha$. Then the operation $*$ defined on G_{CD} by*

$$a * b = a\cdot \mathrm{sh}_1(b)\cdot g_\phi\cdot \mathrm{sh}_1(b^{-1})$$

induces a well defined operation on the coset set $\mathrm{sh}_0(G_{CD})\backslash G_{CD}$, and the latter operation satisfies Identity (CD).

We shall say more about the previous operation (and, in particular, prove that it is not trivial) in the next section. We conclude the current section with a complete description of the connection between the group G_{CD} and the geometry monoid $\mathcal{G}_{CD}$.

Assume that w and w' are words on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$ and both CD_w and $\mathrm{CD}_{w'}$ map the term t to the term t'. Then, by Lemma 3.3, we have

$$\chi_t \cdot 0w \equiv \chi_{t'} \equiv \chi_t \cdot 0w',$$

which implies $0w \equiv 0w'$. We observe that, if the address γ is a prefix of all addresses involved in the left term of a CD-relation, then the same holds for the right term, and *vice versa*. It follows that $\gamma u \equiv^+ \gamma u'$ implies $u \equiv^+ u'$ for all words u, u' on $\boldsymbol{A}$, as all intermediate words in a sequence of elementary transformations from γu to $\gamma u'$ witnessing $\gamma u \equiv^+ \gamma u'$ must be of the form γv. Now, arbitrary factors $\alpha{\cdot}\alpha^{-1}$ may appear in $\equiv$-equivalences, and the same argument does not apply to $\equiv$. It is actually true that $0w \equiv 0w'$ implies $w \equiv w'$, but the proof requires a number of auxiliary results. We can avoid the problem by resorting to an alternative blueprint.

Definition. For t in T_1, we define $\chi^*_t = \varepsilon$ for $t = x$, and $\chi^*_t = \chi_{t_0}{\cdot}1\chi^*_{t_1}$ for $t = t_0{\cdot}t_1$.

Lemma 3.6. *Assume $t' = (t)w$. Then we have $\chi^*_{t'} \equiv \chi^*_t{\cdot}w$.*

Proof. For an induction, it suffices to prove the result when w consists of a single positive address, say α. We use induction on the length of α as a word on $\{0, 1\}$. Assume first $\alpha = \phi$. As $(t)\phi$ exists, we can write $t = t_0{\cdot}(t_1{\cdot}t_*)$, and we have then $t' = (t_0{\cdot}t_1){\cdot}(t_1{\cdot}t_*)$. We find

$$\begin{aligned}\chi^*_{t'} = \chi_{t_0\cdot t_1} \cdot 1\chi_{t_1} \cdot 11\chi^*_{t_*} &= \chi_{t_0} \cdot 1\chi_{t_1} \cdot \phi \cdot 1\chi^{-1}_{t_1} \cdot 1\chi_{t_1} \cdot 11\chi^*_{t_*}\\ &\equiv \chi_{t_0} \cdot 1\chi_{t_1} \cdot \phi \cdot 11\chi^*_{t_*} \equiv \chi_{t_0} \cdot 1\chi_{t_1} \cdot 11\chi^*_{t_*} \cdot \phi = \chi^*_t \cdot \phi.\end{aligned}$$

Assume now $\alpha = 0\beta$. Write $t = t_0{\cdot}t_1$. Then we have $t' = t'_0{\cdot}t_1$ with $t'_0 = (t_0)\beta$. Applying Lemma 3.3, we find

$$\chi^*_{t'} = \chi_{t'_0} \cdot 1\chi^*_{t_1} \equiv \chi_{t_0} \cdot 0\beta \cdot 1\chi^*_{t_1} \equiv \chi_{t_0} \cdot 1\chi^*_{t_1} \cdot 0\beta = \chi^*_t \cdot \alpha.$$

Assume finally $\alpha = 1\beta$. We write $t = t_0{\cdot}t_1$ again. Then we have $t' = t_0{\cdot}t'_1$ with $t'_1 = (t_1)\beta$. Applying the induction hypothesis, we find

$$\chi^*_{t'} = \chi_{t_0} \cdot 1\chi^*_{t'_1} \equiv \chi_{t_0} \cdot 1\chi^*_{t_1} \cdot 1\beta = \chi^*_t \cdot \alpha. \qquad \blacksquare$$

Lemma 3.7. *Assume that w is a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, w is reversible to w', and $(t)w$ is defined. Then $(t)w'$ is defined as well.*

Proof. It suffices to consider the case where exactly one factor $\alpha^{-1}{\cdot}\beta$ is replaced with the corresponding factor $f_{CD}(\alpha, \beta){\cdot}f_{CD}(\beta, \alpha)^{-1}$. Then we consider each possible CD-relation. The details are easy. $\blacksquare$

Proposition 3.8. *Assume that w, w' are words on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, and the domains of CD_w and $\mathrm{CD}_{w'}$ are not disjoint. Then the following are equivalent:*
- *$(t)w = (t)w'$ holds for at least one term t;*
- *$(t)w = (t)w'$ holds for every term t such that $(t)w$ and $(t)w'$ exist;*
- *$w \equiv w'$ holds.*

If w and w' are words on $\boldsymbol{A}$, $\mathrm{CD}_w = \mathrm{CD}_{w'}$ is equivalent to $w \equiv w'$, so $\mathcal{G}^+_{CD}$ is isomorphic to the submonoid G^+_{CD} of G_{CD} generated by the elements g_α.

Proof. Assume that both CD_w and $\mathrm{CD}_{w'}$ map t to t'. By Lemma 3.6, we have

$$\chi_t^* \cdot w \equiv \chi_{t'}^* \equiv \chi_t^* \cdot w',$$

hence $w \equiv {\chi_t^*}^{-1} \cdot \chi_{t'}^* \equiv w'$.

Conversely, assume that $w \equiv w'$ holds, and both $(t)w$ and $(t)w'$ exist. By Lemma 3.7, $(t)N(w)D(w)^{-1}$ and $(t)N(w')D(w')^{-1}$ exist. By Proposition 2.12, there exists two words v, v' on $\boldsymbol{A}$ satisfying $N(w)\, v \equiv^+ N(w')\, v'$ and $D(w)\, v \equiv^+ D(w')\, v'$, and we find

$$\begin{aligned}(t)w = (t)N(w)\, D(w)^{-1} &= (t)N(w)\, v\, v^{-1}\, D(w)^{-1} \\ &= (t)N(w')\, v'\, {v'}^{-1}\, D(w')^{-1} = (t)N(w')\, D(w')^{-1} = (t)w'.\end{aligned}$$

If, in addition, w and w' are words on $\boldsymbol{A}$, then the terms t_w^L and $t_{w'}^L$ are injective, and the basic properties of term unification imply that the domains of CD_w and $\mathrm{CD}_{w'}$ are never disjoint: the previous results apply, so $w \equiv w'$ implies that CD_w and $\mathrm{CD}_{w'}$ agree on every term on which they are both defined. To conclude that CD_w and $\mathrm{CD}_{w'}$ coincide, we resort to the results of [7, Chapter VII], which apply *mutatis mutandis*. ∎

Corollary 3.9. *The word problem of the group G_{CD} is decidable.*

Proof. Assume that w is a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$. Then $w \equiv \varepsilon$ is equivalent to $N(w) \equiv D(w)$, hence, by the previous result, to $(t)N(w) = (t)D(w)$ for some/any term t in the intersection of the domains of $\mathrm{CD}_{N(w)}$ and $\mathrm{CD}_{D(w)}$. Such a term t can be computed effectively from w and w' using unification. ∎

4. Iterated left subterms

Let us consider the word problem of Identity (CD), *i.e.*, the problem of recognizing CD-equivalent terms. In the case of one variable terms, Lemma 3.3 tells us that $t =_{CD} t'$ implies that the class of $\chi_t^{-1} \cdot \chi_t$ in the group G_{CD} belongs to the subgroup $\mathrm{sh}_0(G_{CD})$. At this point, we do not know that the previous implication is an equivalence, and we have no effective criterion for recognizing elements of $\mathrm{sh}_0(G_{CD})$. The last ingredient needed in our construction is a preordering on G_{CD} enabling us to prove that a given element of G_{CD} does not belong to $\mathrm{sh}_0(G_{CD})$. Once again, the considered property of G_{CD} is the translation of some geometric feature involving Identity (CD), namely the action on iterated left subterms.

If t' is a CD-expansion of t, then some iterated left subterm of t' is a CD-expansion of the left subterm of t, as a trivial induction shows. For t a term that is not a variable, let us denote by $\mathrm{left}(t)$ the left subterm of t. The precise statement is as follows:

Lemma 4.1. *Define* $\mathrm{dil} : \mathbf{N} \times \boldsymbol{A}^* \to \mathbf{N}$ *inductively by*

$$\mathrm{dil}(i, \varepsilon) = i, \quad \mathrm{dil}(i, \alpha) = \begin{cases} i+1 & \text{for } \alpha = 1^p \text{ with } p < i, \\ i & \text{otherwise,} \end{cases}, \quad \mathrm{dil}(i, u \cdot v) = \mathrm{dil}(\mathrm{dil}(i, u), v).$$

Assume that u is a word on $\boldsymbol{A}$, and $t' = (t)u$ holds. Then, for every i such that $\mathrm{left}^i(t)$ exists, $\mathrm{left}^{\mathrm{dil}(i,u)}(t')$ is a CD-expansion of $\mathrm{left}^i(t)$.

The proof is an easy induction. If u and u' are $\equiv^+$-equivalent words on $\boldsymbol{A}$, the operators CD_u and $\mathrm{CD}_{u'}$ coincide, and we can therefore expect the mappings $\mathrm{dil}(\cdot, u)$ and $\mathrm{dil}(\cdot, u')$ to coincide as well. Once again, if true, this property must be easily verifiable.

Lemma 4.2. *Assume $u, u' \in \boldsymbol{A}^*$ and $u \equiv^+ u'$. Then we have $\mathrm{dil}(i, u) = \mathrm{dil}(i, u')$ for every i.*

Proof. Consider all basic CD-relations successively. ∎

When we consider an word w on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, the integers $\mathrm{dil}(i, w)$ are no longer defined, but we can consider the values associated with the numerator and the denominator of w. These values depend on w, but their relative position depends on the $\equiv$-class of w only:

Lemma 4.3. *Assume $w, w' \in (\boldsymbol{A} \cup \boldsymbol{A}^{-1})^*$ and $w \equiv w'$. Then $\mathrm{dil}(1, D(w)) = \mathrm{dil}(1, N(w))$ (resp. $<, >$) is equivalent to $\mathrm{dil}(1, D(w')) = \mathrm{dil}(1, N(w'))$ (resp. $<, >$).*

Proof. By Proposition 2.12, there exist words v, v' on $\boldsymbol{A}$ satisfying $N(w)\, v \equiv^+ N(w')\, v'$ and $D(w)\, v \equiv^+ D(w')\, v'$. Applying the definition of dil and Lemma 4.2, we find

$$\mathrm{dil}(\mathrm{dil}(1, D(w)), v) = \mathrm{dil}(1, D(w)v) = \mathrm{dil}(1, D(w')v') = \mathrm{dil}(\mathrm{dil}(1, D(w')), v'),$$
$$\mathrm{dil}(\mathrm{dil}(1, N(w)), v) = \mathrm{dil}(1, N(w)v) = \mathrm{dil}(1, N(w')v') = \mathrm{dil}(\mathrm{dil}(1, N(w')), v').$$

By construction, the mappings $\mathrm{dil}(\cdot, v)$ and $\mathrm{dil}(\cdot, v')$ are increasing, hence $\mathrm{dil}(1, D(w)) = \mathrm{dil}(1, N(w))$ is equivalent to $\mathrm{dil}(1, D(w')) = \mathrm{dil}(1, N(w'))$, and the same for $<$ and $>$. ∎

Proposition 4.4. *Assume that t, t' are terms in T_1. Then the following are equivalent:*
(i) The terms t and t' are CD-equivalent;
(ii) We have $\mathrm{dil}(1, D(\chi_t^{-1}{\cdot}\chi_{t'})) = \mathrm{dil}(1, N(\chi_t^{-1}{\cdot}\chi_{t'}))$.

Proof. Let $w = \chi_t^{-1}{\cdot}\chi_{t'}$. Assume (i). By Lemma 3.3, we have $w \equiv 0w_0$ for some word w_0. By construction, we have $D(0w_0) = 0D(w_0)$ and $N(0w_0) = 0N(w_0)$, and $\mathrm{dil}(1, 0u) = 1$ for every word u on $\boldsymbol{A}$. Hence we have $\mathrm{dil}(1, D(0w_0)) = \mathrm{dil}(1, N(0w_0)) = 1$, which, by Lemma 4.3, implies $\mathrm{dil}(1, D(w)) = \mathrm{dil}(1, N(w))$.

Assume now (ii). By Proposition 3.2 and Lemma 3.7, we have

$$(t{\cdot}x^{[p]})w = (t{\cdot}x^{[p]})N(w) \cdot D(w)^{-1} = t'{\cdot}x^{[p]}$$

for p large enough. Let $t_0 = (t{\cdot}x^{[p]})N(w)$. By construction, we have $t_0 = (t'{\cdot}x^{[p]})D(w)$. Let k be the common value of $\mathrm{dil}(1, D(w))$ and $\mathrm{dil}(1, N(w))$. By lemma 4.1, $\mathrm{left}^k(t_0)$ is a CD-expansion both of $\mathrm{left}(t{\cdot}x^{[p]})$, *i.e.*, of t, and of $\mathrm{left}(t'{\cdot}x^{[p]})$, *i.e.*, of t'. It follows that t and t' are CD-equivalent, since they admit a common CD-expansion. ∎

Corollary 4.5. *The word problem of Identity (CD) restricted to one variable terms is decidable.*

Proof. The integers $\mathrm{dil}(1, N(\chi_t^{-1}{\cdot}\chi_{t'}))$ and $\mathrm{dil}(1, D(\chi_t^{-1}{\cdot}\chi_{t'}))$ are effectively computable. ∎

Extending the solution of the word problem to the general case turns out to be easy.

Lemma 4.6. *(i) A term is never CD-equivalent to one of its proper iterated left subterms.*
(ii) Distinct terms with the same skeleton are never CD-equivalent.

Proof. (i) For w a word on $\boldsymbol{A} \cup \boldsymbol{A}^{-1}$, let us say that w belongs to P_+ (*resp.* P_0) if $\mathrm{dil}(1, D(w)) < \mathrm{dil}(1, N(w))$ holds (*resp.* $=$). By Lemma 4.3, the sets P_+ and P_0 is saturated under $\equiv$. Assume w_1, $w_2 \in P_+$. We find

$$\begin{aligned}
\mathrm{dil}(1, D(w_1w_2)) &= \mathrm{dil}(1, D(w_2)\,(N(w_2)\backslash D(w_1)))\\
&= \mathrm{dil}(\mathrm{dil}(1, D(w_2)), N(w_2)\backslash D(w_1))\\
&< \mathrm{dil}(\mathrm{dil}(1, N(w_2)), N(w_2)\backslash D(w_1))\\
&= \mathrm{dil}(1, N(w_2)\,(N(w_2)\backslash D(w_1)))\\
&= \mathrm{dil}(1, D(w_1)\,(D(w_1)\backslash N(w_2)))\\
&= \mathrm{dil}(\mathrm{dil}(1, D(w_1)), D(w_1)\backslash N(w_2))\\
&< \mathrm{dil}(\mathrm{dil}(1, N(w_1)), D(w_1)\backslash N(w_2))\\
&= \mathrm{dil}(1, N(w_1)\,(D(w_1)\backslash N(w_2))) = \mathrm{dil}(1, N(w_1w_2)),
\end{aligned}$$

so we have $P_+ \cdot P_+ \subseteq P_+$, and, by a similar argument, $P_0 \cdot P_+ \subseteq P_+$, and $P_+ \cdot P_0 \subseteq P_+$.

Assume now that t is a proper iterated left subterm of t': this means that we have $t' = ((\ldots(t \cdot t_1) \cdot t_2) \cdot \ldots) \cdot t_k$ for some terms $t_1, \ldots, t_k$, which, by definition, gives a decomposition of the form

$$\chi_{t'} = \chi_t \cdot 1w_0 \cdot \phi \cdot 1w_1 \cdot \ldots \cdot 1w_{k-1} \cdot \phi \cdot 1w_k.$$

For each i, the word $1w_i$ belongs to P_0, while ϕ belongs to P_+, since we have $\mathrm{dil}(1, D(\phi)) = \mathrm{dil}(1, \varepsilon) = 1$ and $\mathrm{dil}(1, N(\phi)) = \mathrm{dil}(1, \phi) = 2$. By the above computations, we deduce $\chi_t^{-1} \cdot \chi_{t'} \in P_+$, while, by Proposition 4.4, $t =_{CD} t'$ is equivalent to $\chi_t^{-1} \cdot \chi_{t'} \in P_0$.

(ii) Assume that t, t' are distinct terms with the same skeleton. Assume that some variable x occurs at α in t, while x' occurs at α in t'. We assume (x, x') to be the leftmost variable clash between t and t'. First, by replacing t and t' by some CD-expansion, we can assume that α has the form $0^i 1^j$, *i.e.*, the clash involves the rightmost variable in the p-th iterated left subterm of t and t'. Let t'' be a common CD-expansion for t and t'. By Lemma 4.1, we have $\mathrm{left}^k(t'') =_{CD} \mathrm{left}^i(t)$ and $\mathrm{left}^{k'}(t'') =_{CD} \mathrm{left}^i(t')$ for some k, k'. As the rightmost variables in $\mathrm{left}^i(t)$ and $\mathrm{left}^i(t')$ are distinct, and the righmost variable is preserved under CD-equivalence, we deduce $k \neq k'$. Assume for instance $k > k'$. Then $\mathrm{left}^k(t'')$ is a proper iterated subterm of $\mathrm{left}^{k'}(t'')$, hence of t_0, where t_0 is the term obtained from $\mathrm{left}^{k'}(t'')$ by replacing the final variable x' by x. Now t_0 is CD-equivalent to the term obtained from $\mathrm{left}^i(t')$ by replacing the final variable with x, and the latter term is $\mathrm{left}^i(t)$. So t_0 is CD-equivalent to its proper iterated subterm $\mathrm{left}^{k-k'}(t_0)$, contradicting (i). ∎

Proposition 4.7. *The word problem of Identity (CD) is decidable, with a primitive recursive complexity.*

Proof. Assume that t, t' are terms in T_∞. Let t_1 and t'_1 respectively be the terms in T_1 obtained by replacing every variable in t and t' with x_1. We can decide $t =_{CD} t'$ as follows. First, we test $t_1 =_{CD} t'_1$ using Proposition 4.4. If $t_1 =_{CD} t'_1$ fails, so does $t =_{CD} t'$. Otherwise, t_1 and t'_1 admit a common CD-expansion, namely $(t_1)u = (t'_1)u'$, with $u = N(\chi_{t_1}^{-1} \cdot \chi_{t'_1})$ and $u' = D(\chi_{t_1}^{-1} \cdot \chi_{t'_1})$. Then we compare $(t)u$ and $(t')u'$: these terms exist, as, for u in $\boldsymbol{A}^*$, $(t)u$ being defined only depends on the skeleton of t, and they have the same skeleton, namely the common skeleton of $(t_1)u$ and $(t'_1)u'$. Then $(t)u' = (t')u'$ implies $t =_{CD} t'$, while, by Lemma 4.6(ii), $(t)u \neq (t')u'$ implies $(t)u \neq_{CD} (t')u'$, hence $t \neq_{CD} t'$.

As for complexity, we observe that, if t and t' have size n at most, then the whole computation can be made using space resources not larger than the size of the term $\partial^{2^n} x^{[n]}$, and the latter is bounded above by a tower of exponentials of height 2^n. ∎

If S is an arbitrary binary system, we say that a is a left divisor of b if $b = ax$ holds for some x, and that a is an iterated left divisor of b, denoted $a \sqsubset b$, if we have $b = (\ldots(ax_1)\ldots)x_k$ for some $x_1, \ldots, x_k$ (the two notions coincide in the case of an associative operation only).

Proposition 4.8. *Assume that S is a free CD-system. Then iterated left division is a partial order on S. Moreover, if S has rank 1, this order is a linear order.*

Proof. As $\sqsubset$ is transitive by definition, the point is to prove that $\sqsubset$ is irreflexive, which follows from Lemma 4.6(i): indeed, assume that a is the class of the term t; then $a \sqsubset a$ is equivalent to the existence of a term t' such that t' is CD-equivalent to t and t is CD-equivalent to a proper iterated left subterm of t'.

Assume now that S is a free CD-system of rank 1, and a, $a' \in S$ holds. Let t, t' be one variable terms representing a and a' respectively. Let $w = \chi_t^{-1} \cdot \chi_{t'}$. Let $t_0 = (t \cdot x^{[p]})N(w)$, $k = \mathrm{dil}(1, N(w))$, and $k' = \mathrm{dil}(1, D(w))$. As in the proof of Proposition 4.4, we see that $\mathrm{left}^k(t_0)$ is a CD-expansion of t, while $\mathrm{left}^{k'}(t_0)$ is a CD-expansion of t', and, therefore,

$\mathrm{left}^k(t_0)$ represents a and $\mathrm{left}^{k'}(t_0)$ represents a'. For $k = k'$, we obtain $a = a'$. For $k > k'$, the term $\mathrm{left}^k(t_0)$ is a proper iterated left subterm of $\mathrm{left}^{k'}(t_0)$, and we deduce $a \sqsubset a'$. Similarly $k < k'$ implies $a' \sqsubset a$. ∎

An application of the previous results is the following criterion for recognizing free CD-systems, which is directly reminiscent of Laver's criterion for free LD-systems [10]:

Proposition 4.9. *A monogenic CD-system S is free if and only if left division has no cycle in S.*

Proof. By Proposition 4.8, the condition is necessary. Conversely, assume S to be generated by g. Let F be a free CD-system based on $\{x\}$, and let π be the canonical homomorphism of F onto S that maps x to g. Let a, a' distinct elements of F. By Proposition 4.8, either $a \sqsubset a'$ or $a' \sqsubset a$ holds. As $\sqsubset$ is definable from the binary operation, π preserves $\sqsubset$, so $\pi(a) \sqsubset \pi(a')$ or $\pi(a') \sqsubset \pi(a)$ holds in S. If left division in S has no cycle, both imply $\pi(a) \neq \pi(a')$, π is injective, and S is isomorphic to F, hence free. ∎

Let us come back to the CD-system $(\mathrm{sh}_0(G_{CD})\backslash G_{CD}, *)$ of Proposition 3.5. For simplicity, we write G for G_{CD} and G_0 for $\mathrm{sh}_0(G_{CD})$ in the sequel. The operation $*$ on $G_0\backslash G$ is defined by

$$aG_0 * bG_0 = a\,\mathrm{sh}_1(b)\,g_\phi, \mathrm{sh}_1(b^{-1})\,G_0.$$

The remaining question is whether the latter binary operation is trivial or not: when collapsing all generators $g_{0\alpha}$ in G, we could have collapsed everything and obtained a trivial quotient. Actually, we have not:

Proposition 4.10. *Every monogenic subsystem of $(G_0\backslash G, *)$ is free.*

Proof. Assume that a_0G_0, …, a_kG_0 are cosets in $G_0\backslash G$ and each factor divides the next one, *i.e.*, we have $a_iG_0 * x_iG_0 = a_{i+1}G_0$ for some x_i. This means that, for every i, we have $(a_i * x_i)\cdot\mathrm{sh}_0(y_i) = a_{i+1}$ in G for some y_i. By using the definition of $*$ and gathering the equalities, we obtain in G an equality of the form

$$a_k = a_0\,\mathrm{sh}_1(c_0)\,g_\phi\,\mathrm{sh}_1(c_1)\mathrm{sh}_0(c'_1)\,g_\phi\,\ldots\,g_\phi\,\mathrm{sh}_1(c_k)\mathrm{sh}_0(c'_k). \tag{4.1}$$

For $k \geq 1$, (4.1) shows that $a_1^{-1}a_k$ can be represented by a word containing k letters ϕ, and no letter ϕ^{-1}, hence a word in the set P_+ introduced in the proof of Lemma 4.6, and, therefore, not in P_0, as would be the case if we had $a_0^{-1}a_k \in G_0$. So we deduce $a_kG_0 \neq a_0G_0$, *i.e.*, $(a_0G_0, \ldots, a_kG_0)$ is not a cycle for left division in $(G_0\backslash G, *)$. Proposition 4.9 then implies that every mongenic subsystem of $(G_0\backslash G, *)$ is free. ∎

Remarks. (i) If, for a, b in G, we say that $a \prec b$ (*resp.* $a \simeq b$) holds if $a^{-1}b$ admits an expression in P_+ (*resp.* in P_0), then $\prec$ is a preorder on G, and $\simeq$ is the associated equivalence relation; both are invariant under left multiplication. The previous proof means that $a \prec a * b$ holds for all a, b in G, and the preorder $\prec$ is connected with the iterated left divisibility order $\sqsubset$ on free CD-systems of rank 1 as follows: for t, t' in T_1, $\overline{t} \sqsubset \overline{t'}$ holds in $T_1/{=_{CD}}$ if and only if $\overline{\chi_t} \prec \overline{\chi_{t'}}$ holds in G, where $\overline{t}$ denotes the $=_{CD}$-class of t, and $\overline{w}$ the $\equiv$-class of w.

(ii) If, instead of considering the cosets associated with the subgroup G_0, we consider the normal subgroup $\widehat{G_0}$ of G generated by G_0, we still obtain an operation satisfying (CD) on the quotient-group $G/\widehat{G_0}$—but the latter quotient is trivial: for every address γ, the CD-relation $g_\gamma\,g_{\gamma1}\,g_\gamma = g_{\gamma1}\,g_\gamma\,g_{\gamma0}$ in G implies $g_\gamma\,g_{\gamma1}\,g_\gamma = g_{\gamma1}\,g_\gamma$, hence $g_\gamma = 1$, in $G/\widehat{G_0}$, and

$\widehat{G_0}$ is all of G. This distinguishes (CD) from left self-distributivity (LD): in the latter case, we have a similar situation where a binary operation satisfying (LD) exists both on a coset set $G'_0\backslash G'$—where G' is a certain group connected with the geometry monoid of (LD)—and on the quotient group $G'/\widehat{G'_0}$, where $\widehat{G'_0}$ is the normal subgroup of G' generated by G'_0; now $G'/\widehat{G'_0}$ turns out to be Artin's braid group B_∞, and one can deduce a simplified solution for the word problem of (LD) by using this group and its representation in the automorphisms of a free group [9]. In the case of (CD), such an indirect approach is not possible.

The study of Identity (CD) can be continued along the lines developed for left self-distributivity in [7]. As natural examples are missing, going into details seems unnecessary. Let us only mention that the group G_{CD} is an orderable group, *i.e.*, it can be equipped with a linear ordering compatible with multiplication on both sides, and that one can construct realizations for the free CD-systems of any rank by extending the blueprints so as to generate arbitrary terms.

As it stands, the current analysis, which is reminiscent of Henkin's proof of Gödel's completeness theorem, relies on three ingredients, namely the completeness of the involved word reversing, its convergence, and the existence of a convenient blueprint. We conjecture that the first condition holds whenever the left term of the considered identity is injective, *i.e.*, no variable is repeated. For the other conditions, no general principle arises so far, but, in any case, the current scheme is not the only possible one for using the geometry monoid, and we hope for new applications of the latter in the future.

References

[1] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemporary Maths AMS **78** (1988) 45–117.

[2] J.W. Cannon, W.J. Floyd, & W.R. Parry, *Introductory notes on Richard Thompsons's groups*, Ens. Math. **42** (1996) 215–257.

[3] P. Dehornoy, *Structural monoids associated to equational varieties*, Proc. Amer. Math. Soc. **117-2** (1993) 293–304.

[4] —, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

[5] —, *The structure group for the associativity identity*, J. Pure Appl. Algebra **111** (1996) 59–82.

[6] —, *Construction of left distributive operations and charged braids*, Int. J. for Algebra & Computation, to appear.

[7] —, *Braids and Self-Distributivity*, Progress in Math. Series, Birkhäuser, to appear.

[8] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.

[9] D.M. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994) 104–112.

[10] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91-2** (1992) 209–231.

[11] S. Mac Lane, *Natural associativity and commutativity*, Rice Univ. Studies **49** (1963) 28–46

[12] J. Stasheff, *Homotopy associativity of H-spaces*, Trans. Amer. Math. Soc. **108** (1963) 275–292.

Mathématiques, laboratoire SDAD, ESA 6081 CNRS
Université Campus II, BP 5186, 14 032 Caen, France
dehornoy@math.unicaen.fr
http://www.math.unicaen.fr/~dehornoy/