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 arise naturally, 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 rely 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

$$x(yz) = (xy)(yz), \quad (CD)$$

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 \( \langle \{ g_\alpha \mid \alpha \in A \} \ ; \ R_{CD} \rangle \), where \( A \) 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 \( g_\alpha \)'s, and let \( sh_1 \) be the endomorphism of \( G \) that maps \( g_\alpha \) to \( g_{1 \alpha} \) for every \( \alpha \). Then the operation \( \ast \) defined on \( G \) by

\[
a \ast b = a \cdot sh_1(b) \cdot g_b \cdot sh_1(b^{-1})
\]

induces a well defined operation on the homogeneous set \( G_0 \backslash G \); the latter operation satisfies Identity (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 \( G_{CD} \) associated with Identity (CD), and we establish a list of relations holding in \( G_{CD} \) 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 \( 1 \leq n \leq \infty \), 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 \( (t_0, t_1, t_2), (t_0 \cdot t_1, t_1 \cdot t_2) \). 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 \( x_2 \ x_1 \ x_3 \). We use finite sequences of 0’s and 1’s as addresses for the nodes in such trees, starting with an empty address \( \emptyset \) 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 \( \alpha \)-subterm of \( t \) for \( \alpha \) 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 \( t = t_0 t_1 \).

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

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

Definition. The geometry monoid \( G_{CD} \) of Identity (CD) is defined to be the monoid generated by all partial operators \( CD_\alpha \) and \( CD_\alpha^{-1} \) using composition; the submonoid of \( G_{CD} \) generated by the operators \( CD_\alpha \) alone is denoted by \( G_{CD}^+ \).
By construction of the congruence $=_{CD}$, we have:

**Proposition 1.1.** For all terms $t, t'$ in $T_\infty$, the following are equivalent:

(i) The terms $t, t'$ are CD-equivalent, i.e., $t =_{CD} t'$ holds;

(ii) Some element of $G_{CD}$ maps $t$ to $t'$.

By definition, every element in $G_{CD}$ is a finite product of operators $CD_\alpha$ and $CD_\gamma^{-1}$. Such a product can be specified by a word over the alphabet $A \cup A^{-1}$, where $A^{-1}$ consists of a formal inverse $\alpha^{-1}$ for each address $\alpha$. To this end, we define $CD_{\alpha^{-1}} = CD_\alpha^{-1}$, and $CD_u = CD_\gamma \cdot CD_u$—as the elements of $G_{CD}$ 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 $A^*$ for the set of all words on $A$, i.e., the free monoid generated by $A$, and $(A \cup A^{-1})^*$ for the set of all words on $A \cup A^{-1}$. We use $\varepsilon$ for the empty word, and define $CD_\varepsilon$ to be the identity mapping on $T_\infty$.

The operators $CD_\alpha$ can be described using term unification techniques. Let us say that a term $t$ in $T_\infty$ 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 $A \cup A^{-1}$, either the operator $CD_w$ is empty, or there exists a unique pair of CD-equivalent canonical terms $(t'_w, t^u_w)$ such that $CD_w$ maps $t$ to $t'$ if and only if the pair $(t', t')$ is an instance of the pair $(t, t')$.

(ii) For every word $u$ on $A$, the operator $CD_u$ is nonempty, and the term $t'_u$ is injective.

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

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

$$
\gamma 0\alpha \cdot \gamma 1/\beta , \gamma 1\beta \cdot \gamma 0\alpha \quad \text{(type 0)}
$$

$$
\gamma 0\alpha \cdot \gamma , \gamma \cdot \gamma 0\alpha \quad \text{(type 10)}
$$

$$
\gamma 10\alpha \cdot \gamma , \gamma \cdot \gamma 01\alpha \cdot \gamma 10\alpha \quad \text{(type 10)}
$$

$$
\gamma 11\alpha \cdot \gamma , \gamma \cdot \gamma 11\alpha \quad \text{(type 11)}
$$

$$
\gamma 1 \cdot \gamma , \gamma 0 \cdot \gamma , \gamma 1 \cdot \gamma \quad \text{(type 1)}
$$

Then we have $CD_w = CD_{w'}$ for every CD-relation $(w, w')$.

**Proof.** Type $\perp$ relations are trivial. For types 0, 10, and 11, we observe that, when $CD_\gamma$ maps $t$ to $t'$, then the $\gamma 0\alpha$-subterm of $t$ (if it exists) is copied to the $\gamma 0\alpha$-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 $CD_{\phi \cdot 0}$ and $CD_{\phi \cdot 1}$ 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 $A^*$ generated by all CD-relations. Then, for all words $u$, $u'$ on $A$, $u \equiv^+ u'$ implies $CD_u = CD_{u'}$.

(ii) Define $M_{CD} = A^*/\equiv^+$. 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 $\alpha$, the operator $CD_{\alpha, \alpha^{-1}}$ is the identity mapping of its domain only, and the latter is a proper subset of $T_{\alpha}$. 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 $(A \cup A^{-1})^*$ generated by all CD-relations together with all pairs $(\alpha, \alpha^{-1}, \varepsilon)$ and $(\alpha^{-1}, \alpha, \varepsilon)$ with $\alpha \in A$. The group $(A \cup A^{-1})^*/\equiv$ is denoted by $G_{CD}$; for $\alpha \in A$, the element of $G_{CD}$ represented by $\alpha$ is denoted $g_\alpha$.

All subsequent results originate in the specific properties of the group $G_{CD}$, which themselves come from geometric properties of $(C,D)$. 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 $\alpha^{-1}$ 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 redressing.

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

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

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

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

Then $\equiv^+$ is the congruence on $A^*$ 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 $\alpha$, $\beta$, hence $\alpha^{-1} \beta \equiv f(\alpha, \beta) f(\beta, \alpha)^{-1}$. Let us say that a word $w$ on $A \cup A^{-1}$ redresses 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, $w$ redressing to $w'$ implies $w \equiv w'$.

The words that are terminal for word redressing are those words of the form $uw^{-1}$, where $u$ and $v$ are words on $A$. It is easy to show that every word $w$ on $A \cup A^{-1}$ redresses to at
most one word of the form $uv^{-1}$ with $u, v \in A^*$. 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 $A$, we define $u \backslash v = N(u^{-1}v)$, when the latter exists.

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

**Lemma 2.1.** Assume that $u, v$ are words on $A$ 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 redressing is *complete* when the converse implication holds, i.e., when word redressing always detects positive word equivalence. This need not be the case, but we have the following effective sufficient conditions:

**Proposition 2.2.** [7] Let $A$ be a nonempty alphabet. 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 $v : A^* \to \mathbb{N}$ such that $v(uv) = v(u)f(x, y)v) = v(yf(y, x)v)$ and $v(xu) > v(u)$ hold for all $x, y$ in $A$, and all $u, v$ in $A^*$;

(ii) For all $x, y, z$ in $A$, the word

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

exists and it is empty.

Then word redressing 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 lem.

**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 $CD_h$ increases the size of the terms. We put

$$v(u) = \text{size}(t_u^r) - \text{size}(t_u^l),$$

where $t_u^r$ and $t_u^l$ are the canonical terms involved in Proposition 1.2. By construction, $u \equiv^+ u'$ implies $CD_u = CD_{u'}$, so $v(u)$ depends of the $\equiv^*$-class of $u$ only. Assume $\alpha \in A$, and $u \in A^*$. By definition, we have $t_{\alpha \cdot u}^r = ((t_{\alpha \cdot u}^r)\alpha)u$, hence $(t_{\alpha \cdot u}^r)\alpha = h(t_u^r)$ and $t_{\alpha \cdot u}^a = h(t_u^a)$ for some substitution $h$. We deduce

$$v(\alpha \cdot u) = \text{size}(t_{\alpha \cdot u}^r) - \text{size}(t_{\alpha \cdot u}^l) = \text{size}(t_{\alpha \cdot u}^r) - \text{size}((t_{\alpha \cdot u}^l)\alpha) + \text{size}((t_{\alpha \cdot u}^r)\alpha) - \text{size}(t_{\alpha \cdot u}^l)$$

$$= \text{size}(h(t_u^r)) - \text{size}(h(t_u^l)) + \text{size}((t_{\alpha \cdot u}^l)\alpha) - \text{size}(t_{\alpha \cdot u}^r)$$

$$> \text{size}(h(t_u^r)) - \text{size}(h(t_u^l)) \geq \text{size}(t_u^r) - \text{size}(t_u^l) = v(u).$$

So the mapping $\nu$ 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 \( \alpha, \beta, \gamma \). However, almost all cases are automatically satisfied, as explained in [5]. Because \( \phi, 1, 0 \) 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

\[
\begin{align*}
(\phi\backslash 1)\backslash (\phi\backslash 11) &= (1 \cdot \phi)\backslash \phi = 11 \cdot 1 \cdot \phi, & (1 \cdot \phi)\backslash (11 \cdot 1) &= (\phi \cdot 0)\backslash (11 \cdot 1) = 11 \cdot 1 \cdot \phi, \\
\phi\backslash 11 &= 11 - 1, & 11\backslash \phi &= \phi, \\
\phi\backslash 1 &= 1 - \phi, & 11\backslash 1 &= 1 - 10, & \phi\backslash 11 &= \phi.
\end{align*}
\]

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

Applying Proposition 2.2, we deduce:

**Proposition 2.5.** Word redressing 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 redressing 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 \( \Delta_n \), that is a common multiple of all generators. Here the monoid \( M_{CD} \) is not of finite type, but we can introduce some elements \( \Delta_t \) indexed by terms which are local counterparts to the braids \( \Delta_n \). The intuition for constructing the element \( \Delta_t \) comes from the action of \( M_{CD} \) on terms.

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

**Definition.** For \( \alpha \in A \), we put \( \alpha^{(p)} = \varepsilon \) for \( p \leq 0 \), and \( \alpha^{(p)} = \alpha^{1^{p-1}} \cdot \alpha^{1} \cdot \alpha \) 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 \( A \cup A^{-1} \) and \( \alpha \) an address, we write \( \alpha w \) 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 \( n \), \( \alpha w \) has length \( n \), while \( \alpha \cdot w \) has length \( n + 1 \).

**Definition.** For \( t \) 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 \( \Delta_t \) makes sense as, by construction, \( \text{size}(s_i) < \text{size}(t) \) always holds. We begin with auxiliary results.
Lemma 2.6. For \(0 \leq p \leq r - 2\), \(0 \leq q \leq r - 1\), and for every word \(u\) on \(A\), we have
\[
\begin{align*}
1^p \cdot \phi^{(r)} &\equiv+ \phi^{(r)} \cdot 01^p \cdot 101^{p-1} \cdot \ldots \cdot 1^0 \cdot 0 \quad (2.1) \\
1^q u \cdot \phi^{(r)} &\equiv+ \phi^{(r)} \cdot 01^q u \cdot 101^{q-1}0u \cdot \ldots \cdot 1^00u, \quad (2.2) \\
1^r u \cdot \phi^{(r)} &\equiv+ \phi^{(r)} \cdot 01^r u \cdot \ldots \cdot 1^{r-1}01u \cdot 1^0u. \quad (2.3) \\
\phi^{(q)} \cdot \phi^{(r)} &\equiv+ \phi^{(r)} \cdot 0^{(q)} \cdot 10^{(q-1)} \cdot \ldots \cdot 1^{q-1}0. \quad (2.4)
\end{align*}
\]

Proof. We prove (2.1) using induction on \(p\). For \(p = 0\) and \(r \geq 2\), 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)
\[
\begin{align*}
1^p \cdot \phi^{(r)} = 11^p \cdot 1^{(r-1)} \cdot \phi \equiv+ 1^{(r-1)} \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^00 \cdot \phi & \quad \text{by ind. hyp.} \\
\equiv+ 1^{(r-1)} \cdot 101^{p-1} \cdot \phi \cdot 1101^{p-2} \cdot \ldots \cdot 1^00 & \quad (11) \\
\equiv+ 1^{(r-1)} \cdot \phi \cdot 01^p \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^00 & \quad (10) \\
= \phi^{(r)} \cdot \phi \cdot 01^p \cdot 101^{p-1} \cdot 1101^{p-2} \cdot \ldots \cdot 1^00.
\end{align*}
\]

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
\[
\begin{align*}
1^q u \cdot \phi^{(r)} = 11^q \cdot 1^{(r-1)} \cdot \phi \\
\equiv+ 1^{(r-1)} \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^000u \cdot \phi & \quad \text{by ind. hyp.} \\
\equiv+ 1^{(r-1)} \cdot 101^{q-1}0u \cdot \phi \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^000u & \quad (11) \\
\equiv+ 1^{(r-1)} \cdot \phi \cdot 01^q0u \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^000u & \quad (10) \\
= \phi^{(r)} \cdot 01^q0u \cdot 101^{q-1}0u \cdot 1101^{q-2}0u \cdot \ldots \cdot 1^000u.
\end{align*}
\]

We prove (2.3) using induction on \(r \geq 0\). For \(r = 0\), (2.3) is an equality; for \(r > 0\), we find
\[
\begin{align*}
1^r u \cdot \phi^{(r)} = 11^r \cdot 1^{(r-1)} \cdot \phi \\
\equiv+ 1^{(r-1)} \cdot 101^{r-1}u \cdot 1101^{r-2}u \cdot \ldots \cdot 1^r \cdot 01u \cdot 1^0u \cdot \phi & \quad \text{by ind. hyp.} \\
\equiv+ 1^{(r-1)} \cdot 101^{r-1}u \cdot \phi \cdot 1101^{r-2}u \cdot \ldots \cdot 1^r \cdot 01u \cdot 1^0u & \quad (11) \\
\equiv+ 1^{(r-1)} \cdot \phi \cdot 01^r u \cdot 101^{r-1}u \cdot 1101^{r-2}u \cdot \ldots \cdot 1^r \cdot 01u \cdot 1^0u & \quad (10) \\
= \phi^{(r)} \cdot 01^r u \cdot 101^{r-1}u \cdot \ldots \cdot 1^r \cdot 01u \cdot 1^0u.
\end{align*}
\]

Finally, (2.4) follows from applying (2.1) to \(\phi\), 1, \ldots, 1^{q-1} \) respectively, and gathering the factors using (\(\bot\))-relations.

Lemma 2.7. Assume \(t = t_0 \cdot \ldots \cdot \ldots (t_{k-1} \cdot t_k) \ldots \)) \(\text{Let} \ t'_i = t_i \cdot (t_{i+1} \cdot \ldots (t_{i-1} \cdot t_k) \ldots) \text{for} \ i \leq k. \) \(\text{Then there exists a word} \ u \) on \(A\) satisfying
\[
\Delta_i \equiv+ \phi^{(k)} \cdot 0 \Delta'_i \cdot 10 \Delta'_i \cdot \ldots \cdot 1^k 0 \Delta'_i \cdot 1^{k+1} \Delta_i \cdot u. \quad (2.5)
\]
Proof. We use induction on the size of $t$. Let $h = \text{ht}_q(t)$. The result is trivial if $t$ is a variable, and, more generally, for $k = h - 1$: indeed, in this case, $\Delta_t$ is empty, and the right hand expression in (2.5) with $u = \varepsilon$ is the definition of $\Delta_t$. Assume now $0 \leq k \leq h - 2$. Write $t = t_0(t_1(\ldots (t_{h-1}x)\ldots))$ with $x$ a variable. Then we have $t_* = t_{k+1}(\ldots (t_{h-1}x)\ldots)$. Let $s_i = t_*^i(\ldots (t_{h-2}\cdot t_{h-1})\ldots)$ 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 $s_i = t_*^i(\ldots (t_{k+1}(\ldots (t_{h-1}x)\ldots))$ and size($s_i$) < size($t$) for $i < k$, so, by induction hypothesis, there exists a word $u_i$ on $A$ satisfying
\[
\Delta_{s_i} = \phi^{(k-i)} \cdot 0 \Delta_{t_*^i} \cdot \ldots \cdot 1^{k-i} 0 \Delta_{t_*^i} \cdot 1^{k-i+1} \Delta_{s_{k+1}} \cdot u_i.
\]
Injecting these values in $\Delta_t$, and using $(\perp)$-relations to push the factors $1^i \phi^{(k-i)}$ to the left and the factors $1^i u_i$ and $1^i 0^j \Delta_{t_*^i}$ to the right, we obtain
\[
\Delta_t \equiv^{+} \phi^{(h-1)} \cdot 0^{(k)} \cdot 10^{(k-1)} \cdot \ldots \cdot 1^{k-1} \cdot 0^{(1)} \cdot 00 \Delta_{t_*^0} \cdot 010 \Delta_{t_*^1} \cdot 100 \Delta_{t_*^1} \cdot 0110 \Delta_{t_*^2} \cdot \ldots \cdot 10^1 \Delta_{t_*^k} \cdot \ldots \cdot 1^k \cdot 0 \Delta_{s_{k+1}} \cdot 1^k \cdot 0 \Delta_{s_{k+1}} \cdot 10 \Delta_{s_{k+1}} \cdot 0 \Delta_{s_{k+1}} \cdot 0 u_0 \cdot 10 u_1 \cdot \ldots \cdot 1^k \cdot 0 u_k.
\]
Applying (2.4) with $r = h - 1$ and $q = k$, then (2.2) with $r = h - 1$, $q = 0$, $u = \Delta_{t_*^0}$, then $q = 1$, $u = \Delta_{t_*^1}$, \ldots, $q = k$, $u = \Delta_{t_*^k}$ successively, and, finally, (2.3) with $r = k + 1$ and $u = \Delta_{s_{k+1}}$, we deduce
\[
\Delta_t \equiv^{+} \phi^{(k)} \cdot 0 \Delta_{t_*^0} \cdot 10 \Delta_{t_*^1} \cdot \ldots \cdot 1^k 0 \Delta_{t_*^k} \cdot \phi^{(k+1)} \cdot (1+1) \cdot 1^{h-k-2} \cdot 1^{k+1} 0 \Delta_{s_{k+1}} \cdot \phi^{(k+1)} \\
\equiv^{+} \phi^{(k)} \cdot 0 \Delta_{t_*^0} \cdot 10 \Delta_{t_*^1} \cdot \ldots \cdot 1^k 0 \Delta_{t_*^k} \cdot \phi^{(k+1)} \cdot 1^{k+1} 0 \Delta_{s_{k+1}} \cdot \phi^{(k+1)} \cdot 0 u_0 \cdot \ldots \cdot 1^k 0 u_k \tag{11}
\]
\[
= \phi^{(k)} \cdot 0 \Delta_{t_*^0} \cdot 10 \Delta_{t_*^1} \cdot \ldots \cdot 1^k 0 \Delta_{t_*^k} \cdot 1^k \cdot 0 \Delta_{s_{k+1}} \cdot \phi^{(k+1)} \cdot 0 u_0 \cdot \ldots \cdot 1^k 0 u_k.
\]

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

**Proof.** We use induction on the length of $\alpha$ as a word on $\{0,1\}$. Assume first $\alpha = \phi$. The hypothesis that $(t)\phi$ is defined implies $\text{ht}_q(t) \geq 2$. Hence $t$ can be expressed as $t = t_0(t_1 t_*)$. Applying Lemma 2.7 with $k = 2$, we obtain
\[
\Delta_t \equiv^{+} \phi \cdot 0 \Delta_{t_*^0} \cdot 10 \Delta_{t_*^1} \cdot 11 \Delta_{t_*^1} \cdot u
\]
which begins with $\alpha$ 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 $t = t_0 t_\beta$, with $(t_0)\beta$ defined. Applying Lemma 2.7 with $k = 1$, we obtain $u$ satisfying $\Delta_t \equiv^{+} 0 \Delta_{t_0} \cdot 1 \Delta_{t_\beta} \cdot u$, and, applying the induction hypothesis, we obtain $v$ satisfying $\Delta_{t_0} \equiv^{+} \beta \cdot v$. We deduce
\[
\Delta_t \equiv^{+} 0 \Delta_{t_0} \cdot 1 \Delta_{t_\beta} \cdot u \equiv^{+} 0 \beta \cdot 0 v \cdot 1 \Delta_{t_*} \cdot u = \alpha \cdot 0 v \cdot 1 \Delta_{t_*} \cdot u,
\]
which begins with $\alpha$ 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 $A$ and $(t)u$ is defined, say $t' = (t)u$. Then we have $u \cdot \Delta t' \equiv^* \Delta (t')u'$ for some word $u'$ on $A$.

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 $\alpha$. We prove the result using induction on the size of $t$. Let $h = t_0 u(t)$, $t = t_0 (t_1, \ldots, (t_{h-1}, x), \ldots)$, and $(t)\phi^{(h-1)} = s_0 (s_1, \ldots, (s_{h-1}, x), \ldots)$. Assume $t' = (t)\alpha$. We write similarly $t' = t'_0 (t'_1, \ldots, (t'_{h-1}, x), \ldots)$, and $(t')\phi^{(h-1)} = s'_0 (s'_1, \ldots, (s'_{h-1}, x), \ldots)$. We distinguish four cases according to $\alpha$.

Assume first $\alpha = 1^p0$ with $0 \leq p \leq h - 3$. Then we have $t'_i = t_t$ for $i \neq p$, and $t'_{p} = t'_p t'_{p+1}$. A direct computation gives $s'_i = (s_i)1^{p-1}$ for $i \leq p$, and $s'_i = s_i$ for $i > p$. For $i \leq p$, the induction hypothesis gives a word $u'_i$ on $A$ satisfying $1^{p-i} \cdot \Delta s'_i \equiv^* \Delta s_i \cdot u'_i$. We obtain

$$\alpha \cdot \Delta t' = 1^p \cdot \phi^{(h-1)} \cdot 1^p s_0 \cdot 1^p s_1 \cdot \ldots \cdot 1^{h-2} 0 \Delta s_{h-1} \equiv^* 1^p \cdot \phi^{(h-1)} \cdot 1^p s_0 \cdot 1^p s_1 \cdot \ldots \cdot 1^{h-1} 0 \Delta s_{h-1}$$

by (2.1) and the induction hypothesis.

Assume now $\alpha = 1^{h-1}$ and $s_h = (t_{h-1}, x)$, but, for $i < h$, we have $s'_i = t'_0 (t_1, \ldots, (t_{h-2}, t_{h-1}), t_h, \ldots)$, 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 $A$ satisfying

$$\Delta t' \equiv^* 1^{h-2} \cdot 0 \Delta s_0 \cdot 0 \Delta s_1 \cdot \ldots \cdot 1^{h-2} 0 \Delta s_{h-2} \cdot 1^{h-1} 1 \Delta t_{h-1} \cdot x \cdot u'.$$

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

$$\alpha \cdot \Delta t' \equiv^* 1^{h-2} \cdot 0 \Delta s_0 \cdot 1^{h-2} 0 \Delta s_{h-2} \cdot 1^{h-1} 0 \Delta s_{h-1} \cdot u' \equiv^* \Delta t \cdot u'.$$

Assume now $\alpha = 1^p0\beta$ with $0 \leq p \leq h - 2$. With the same notations, we have $t'_i = t_t$ for $i \neq p$, and $t'_{p} = (t_p)\beta$. We deduce $s'_i = (s_i)1^{p-1}0\beta$ for $i \leq p$, and $s'_i = s_i$ for $i > p$. For $i \leq p$, the induction hypothesis gives a word $u'_i$ on $A$ satisfying $1^{p-i}0\beta \cdot \Delta s'_i \equiv^* \Delta \cdot u'_i$, and we find

$$\alpha \cdot \Delta t' = 1^p 0 \beta \cdot \phi^{(h-1)} \cdot 0 \Delta s_0 \cdot \ldots \cdot 1^{p-1} 0 \Delta s_{p} \cdot \ldots \cdot 1^{h-1} 0 \Delta s_{h-1} \equiv^* 1^p 0 \beta \cdot \phi^{(h-1)} \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{p-1} 0 \beta \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{h-1} 0 \beta \cdot \Delta s_{h-1} \equiv^* 1^p 0 \beta \cdot \phi^{(h-1)} \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{p-1} 0 \beta \cdot 1^p 0 \beta \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{h-1} 0 \beta \cdot \Delta s_{h-1} \equiv^* \phi^{(h-1)} \cdot 0 \Delta s_0 \cdot 0 \Delta s_1 \cdot \ldots \cdot 1^p 0 \beta \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{h-1} 0 \beta \cdot \Delta s_{h-1} \equiv^* \phi^{(h-1)} \cdot 0 \Delta s_0 \cdot 0 \Delta s_1 \cdot \ldots \cdot 1^p 0 \beta \cdot 1^p 0 \beta \cdot \ldots \cdot 1^{h-1} 0 \beta \cdot \Delta s_{h-1}$$

by (2.2) and the induction hypothesis.

Finally, for $\alpha = 1^{h-1}0\beta$, we have $t'_i = t_t$ 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 $n \geq 2$. Write $u = u_1 \cdot u_2$ with $\lg(u_1), \lg(u_2) < n$. Applying the induction hypothesis to $u_1$ and $u_2$, we find words $u'_1, u'_2$ satisfying

$$u \cdot \Delta t' = u_1 \cdot u_2 \cdot \Delta (t)u_1 \cdot u_2 \equiv^* u_1 \cdot \Delta (t)u_1 \cdot u'_2 \equiv^* \Delta t \cdot u'_1 \cdot u'_2.$$

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

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 $\alpha$ 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 $u'' \cdot v'' \equiv^{+} \Delta_{t'} \cdot \Delta_{\partial t} \ldots \cdot \Delta_{\partial^{n-2} t}$, 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

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

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

Proof. Assume that $u$, $v$ are words on $A$. By Proposition 1.2, the terms $t^u_n$ and $t^v_n$ are injective, which implies that some substitute of $t^u_n$ is a substitute of $t^v_n$. 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

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

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 redressing in $A^*$, we deduce from the general results of [7, Chap.II]:

Proposition 2.12. (i) Word redressing in $(A \cup A^{-1})^*$ is convergent, i.e., for every word $w$ on $A \cup A^{-1}$, the words $N(w)$ and $D(w)$ exist.  
(ii) For all words $w$, $w'$ on $A \cup A^{-1}$, $w \equiv w'$ holds if and only if we have

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

for some words $v$, $v'$ on $A$.

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

Proof. Assume that $u$, $u'$ are words on $A$. By Proposition 2.5, $u \equiv^{+} u'$ holds if and only if redressing $u^{-1} u'$ ends with an empty word. As we know now that redressing $u^{-1} u'$ 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 $A$. 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 $\partial t$: Lemma 2.9 implies that the operator $\partial$ is increasing with respect to $CD$-expansions, i.e., that $\partial t'$ is a $CD$-expansion of $\partial t$ 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 \((S, \ast)\): 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 \( G_{CD} \) and its abstract version \( G_{\mathbb{CD}} \), 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 \( G_{\mathbb{CD}} \), or, equivalently, a distinguished word on \( A \cup A^{-1} \). 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

\[
x^{[p+1]} \equiv_{CD} t \cdot x^{[p]}.
\]

**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

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

It follows from Proposition 1.1 that, for every term \( t \) and for every \( p \) large enough, some operator in \( G_{CD} \) 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 \( \chi_t \) of \( t \) is the word defined by \( \chi_x = \varepsilon \) and

\[
\chi_t = \chi_{t_0} \cdot \text{sh}_1(\chi_{t_1}) \cdot \phi \cdot \text{sh}_1(\chi_{t_1})^{-1} \quad \text{for } t = t_0 \cdot t_1.
\]

**Proposition 3.2.** For every \( t \) in \( T_1 \), \( CD_{\chi_t} \) 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, \( CD_{\chi_{t_0}} \) maps \( x^{[p+1]} \) to \( t_0 \cdot x^{[p]} \), and \( CD_{\chi_{t_1}} \) maps \( x^{[p]} \) to \( t_1 \cdot x^{[p-1]} \). Hence \( CD_{\chi_{t_0}} \) maps \( t_0 \cdot x^{[p]} \) to \( t_0 \cdot (t_1 \cdot x^{[p-1]}) \), and, similarly, \( CD_{\chi_{t_1}} \) maps \( t \cdot (t_1 \cdot x^{[p-1]}) \) to \( t \cdot x^{[p]} \). By composing, we obtain

\[
x^{[p+1]} \xrightarrow{\chi_{t_0}} t_0 \cdot x^{[p]} \xrightarrow{1_{t_0}} t_0 \cdot (t_1 \cdot x^{[p-1]}) \xrightarrow{\phi} (t_0 \cdot t_1) \cdot (t_1 \cdot x^{[p-1]}) \xrightarrow{1} (t_0 \cdot t_1) \cdot x^{[p-1]} \xrightarrow{\chi_{t_1}} t \cdot x^{[p]}.
\]

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

**Definition.** For \( u, v \) words on \( A \cup A^{-1} \), we define

\[
u * v = u \cdot 1_{v} \cdot \phi \cdot 1_{v}^{-1},
\]

and we also use * for the induced binary operation on \( G_{\mathbb{CD}} \).
With this notation, \( \chi \) is the homomorphism of \( T_1 \) into \(((A \cup A^{-1})^*, \ast)\) that maps \( x \) to \( \varepsilon \). Our plan is to start from operation \( \ast \) on \( \mathsf{G}_{\mathsf{CD}} \) 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 \( \mathsf{CD} \)-equivalent terms, their blueprints \( \chi_t \) and \( \chi_{t'} \) need not be \( \equiv \)-equivalent, but some operator \( \mathsf{CD}_w \) maps \( t \) to \( t' \), and, therefore, \( \mathsf{CD}_w \) maps \( t \cdot x[p] \) to \( t' \cdot x[p] \) for every \( p \). Hence, both \( \mathsf{CD}_{\chi_t \cdot 0w} \) and \( \mathsf{CD}_{\chi_{t'} \cdot 0w} \) are \( \mathsf{CD} \)-equivalent terms, their blueprints \( \equiv \) 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 \( \alpha \). Then, the result follows from:

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

\[
(u \ast v) \ast (v \ast w) \equiv (u \ast (v \ast w)) \cdot 0
\]

(3.4)

\[
(u \cdot 0w) \ast v \equiv (u \ast v) \cdot 00w
\]

(3.5)

\[
u \ast (v \cdot 0w) \equiv (u \ast v) \cdot 01w
\]

(3.6)

**Proof.** Applying the definition of \( \ast \) and \( \mathsf{CD} \)-relations, we find

\[
(u \ast v) \ast (v \ast w) = u \cdot 1v \cdot \phi \cdot 1v^{-1} \cdot 1v \cdot 11w \cdot 1 \cdot 11w^{-1} \cdot 11w \cdot 1^{-1} \cdot 11w^{-1} \cdot 1v^{-1}
\]

\[
\equiv u \cdot 1v \cdot 11w \cdot 1 \cdot \phi \cdot 1^{-1} \cdot 11w^{-1} \cdot 1v^{-1}
\]

(11)

\[
\equiv u \cdot 1v \cdot 11w \cdot 1 \cdot \phi \cdot 0 \cdot 1^{-1} \cdot 11w^{-1} \cdot 1v^{-1}
\]

(1)

\[
\equiv u \cdot 1v \cdot 11w \cdot 1 \cdot \phi \cdot 1^{-1} \cdot 11w^{-1} \cdot 1v^{-1} \cdot 0
\]

(\( \bot \))

\[
\equiv u \cdot 1v \cdot 11w \cdot 1 \cdot 11w^{-1} \cdot 11w \cdot 1^{-1} \cdot 11w^{-1} \cdot 1v^{-1} \cdot 0
\]

(11)

\[
= (u \ast (v \ast w)) \cdot 0.
\]

\[
(u \cdot 0w) \ast v = u \cdot 0w \cdot 1v \cdot \phi \cdot 1v^{-1} \equiv u \cdot 1v \cdot 0w \cdot \phi \cdot 1v^{-1}
\]

(\( \bot \))

\[
\equiv u \cdot 1v \cdot \phi \cdot 00w \cdot 1v^{-1}
\]

(0)

\[
\equiv u \cdot 1v \cdot \phi \cdot 1v^{-1} \cdot 00w = (u \ast v) \cdot 00w
\]

(\( \bot \))

\[
u \ast (v \cdot 0w) = u \ast (1v \cdot 10w \cdot \phi \cdot 10w^{-1} \cdot 1v^{-1}
\]

\[
\equiv u \cdot 1v \cdot \phi \cdot 01w \cdot 10w \cdot 10w^{-1} \cdot 1v^{-1}
\]

(10)

\[
\equiv u \cdot 1v \cdot \phi \cdot 01w \cdot 1v^{-1}
\]

\[
\equiv u \cdot 1v \cdot \phi \cdot 1v^{-1} \cdot 01w = (u \ast v) \cdot 01w
\]

\[
\end{align*}

}\[
\end{align*}

\[
\end{align*}

\[
\end{align*}

\[
\end{align*}

\[
\end{align*}

\[
\end{align*}

Formula (3.4) tells us how to obtain a binary operation satisfying \((CD)\) from \( \ast \) on \( \mathsf{G}_{\mathsf{CD}} \): 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 \( \gamma \), let \( \mathsf{sh}_\gamma \) denote the endomorphism of \( \mathsf{G}_{\mathsf{CD}} \) induced by the address shift \( \alpha \mapsto \gamma \alpha \). Then the operation \( \ast \) defined on \( \mathsf{G}_{\mathsf{CD}} \) by

\[
a \ast b = a \cdot \mathsf{sh}_1(b) \cdot g_\phi \cdot \mathsf{sh}_1(b^{-1})
\]

induces a well defined operation on the coset set \( \mathsf{sh}_0(\mathsf{G}_{\mathsf{CD}}) \setminus \mathsf{G}_{\mathsf{CD}} \), 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 \( G_{CD} \).

Assume that \( w \) and \( w' \) are words on \( A \cup A^{-1} \) and both \( \text{CD}_w \) and \( \text{CD}_{w'} \) 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 \( \gamma \) 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 \( A \), as all intermediate words in a sequence of elementary transformations from \( \gamma u \) to \( \gamma u' \) witnessing \( \gamma u \equiv \gamma u' \) must be of the form \( \gamma v \). 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 \( \chi_t^* = \chi_t^* \cdot 1 \chi_t^* \) 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 \( \alpha \). We use induction on the length of \( \alpha \) as a word on \( \{0, 1\} \). Assume first \( \alpha = \phi \).
As \( (t)\phi \) exists, we can write \( t = t_0 \cdot (t_1 \cdot t_2) \), and we have then \( t' = (t_0 \cdot t_1) \cdot (t_1 \cdot t_2) \). We find

\[
\chi_{t'}^* = \chi_{t_0 \cdot t_1}^* \cdot 1 \chi_{t_1}^* \cdot 11 \chi_{t_2}^* = \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \cdot \phi_1^{-1} \cdot 1 \chi_{t_1}^* \cdot 11 \chi_{t_2}^* \\
\equiv \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \cdot \phi_1^{-1} \cdot 11 \chi_{t_1}^* \equiv \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \cdot 11 \chi_{t_1}^* \cdot \phi = \chi_t^* \cdot \phi.
\]

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

\[
\chi_{t'}^* = \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \equiv \chi_{t_0}^* \cdot 0 \beta \equiv \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \cdot 0 \beta = \chi_t^* \cdot \alpha.
\]

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

\[
\chi_{t'}^* = \chi_{t_0}^* \cdot 1 \chi_{t_1}^* \equiv \chi_{t_0}^* \cdot (1 \chi_{t_1}^* \cdot \beta) = \chi_t^* \cdot \alpha.
\]

**Lemma 3.7.** Assume that \( w \) is a word on \( A \cup A^{-1} \), \( w \) redresses 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 \( \alpha^{-1} \beta \) is replaced with the corresponding factor \( f_{CD}(\alpha, \beta) \cdot f_{CD}(\beta, \alpha) \). Then we consider each possible CD-relation. The details are easy.

**Proposition 3.8.** Assume that \( w, w' \) are words on \( A \cup A^{-1} \), and the domains of \( \text{CD}_w \) and \( \text{CD}_{w'} \) 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 \( A \), \( \text{CD}_w = \text{CD}_{w'} \) is equivalent to \( w \equiv w' \), so \( G_{CD}^+ \) is isomorphic to the submonoid \( G_{CD}^+ \) of \( G_{CD} \) generated by the elements \( g_o \).
Proof. Assume that both \( \text{CD}_w \) and \( \text{CD}_{w'} \) map \( t \) to \( t' \). By Lemma 3.6, we have
\[
\chi_t^* \cdot w \equiv \chi_t^* \cdot w' ,
\]
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 \( A \) satisfying \( N(w) \equiv N(w') \equiv v^{-1}D(w)^{-1} \), and we find
\[
(t)w = (t)N(w)D(w)^{-1} = (t)N(w)v^{-1}D(w)^{-1} = (t)N(w')v'^{-1}D(w')^{-1} = (t)N(w')D(w')^{-1} = (t)w'.
\]
If, in addition, \( w \) and \( w' \) are words on \( A \), then the terms \( t_w \) and \( t_{w'} \) are injective, and the basic properties of term unification imply that the domains of \( \text{CD}_w \) and \( \text{CD}_{w'} \) are never disjoint: the previous results apply, so \( w \equiv w' \) implies that \( \text{CD}_w \) and \( \text{CD}_{w'} \) agree on every term on which they are both defined. To conclude that \( \text{CD}_w \) and \( \text{CD}_{w'} \) coincide, we resort to the results of [7, Chapter VII], which apply mutatis mutandis.

Corollary 3.9. The word problem of the group \( G_{\text{CD}} \) is decidable.

Proof. Assume that \( w \) is a word on \( A \cup A^{-1} \). 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 \( CD_{N(w)} \) and \( CD_{D(w)} \). 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 \( G_{\text{CD}} \) belongs to the subgroup \( \text{sh}_0(G_{\text{CD}}) \). At this point, we do not know that the previous implication is an equivalence, and we have no effective criterion for recognizing elements of \( \text{sh}_0(G_{\text{CD}}) \). The last ingredient needed in our construction is a preorder on \( G_{\text{CD}} \) enabling us to prove that a given element of \( G_{\text{CD}} \) does not belong to \( \text{sh}_0(G_{\text{CD}}) \). Once again, the considered property of \( G_{\text{CD}} \) 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 \( \text{left}(t) \) the left subterm of \( t \). The precise statement is as follows:

Lemma 4.1. Define \( \text{dil} : \mathbb{N} \times A^* \rightarrow \mathbb{N} \) inductively by
\[
\text{dil}(i, \varepsilon) = i, \quad \text{dil}(i, \alpha) = \begin{cases} 
i + 1 & \text{for } \alpha = 1^p \text{ with } p < i, \\ i & \text{otherwise}, \end{cases} \quad \text{dil}(i, u \cdot v) = \text{dil}(\text{dil}(i, u), v).
\]

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

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

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

Proof. Consider all basic CD-relations successively.

\[14\]
When we consider an word \( w \) on \( A \cup A^{-1} \), the integers \( \text{dil}(i, w) \) 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 \( w, w' \in (A \cup A^{-1})^* \) and \( w \equiv w' \). Then \( \text{dil}(1, D(w)) = \text{dil}(1, N(w)) \) (resp. \( <, > \)) is equivalent to \( \text{dil}(1, D(w')) = \text{dil}(1, N(w')) \) (resp. \( <, > \)).

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

\[
\text{dil}(\text{dil}(1, D(w)), v) = \text{dil}(1, D(w)v) = \text{dil}(1, D(w')v') = \text{dil}(\text{dil}(1, D(w')), v'),
\]

\[
\text{dil}(\text{dil}(1, N(w)), v) = \text{dil}(1, N(w)v) = \text{dil}(1, N(w')v') = \text{dil}(\text{dil}(1, N(w')), v').
\]

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

**Proposition 4.4.** Assume that \( t, t' \) are terms in \( T \). Then the following are equivalent:

1. The terms \( t \) and \( t' \) are CD-equivalent;
2. We have \( \text{dil}(1, D(\chi_t^{-1} \chi_{t'})) = \text{dil}(1, N(\chi_t^{-1} \chi_{t'})) \).

**Proof.** Let \( w = \chi_t^{-1} \chi_{t'} \). 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 \( \text{dil}(1, 0u) = 1 \) for every word \( u \) on \( A \). Hence we have \( \text{dil}(1, D(0w_0)) = \text{dil}(1, N(0w_0)) = 1 \), which, by Lemma 4.3, implies \( \text{dil}(1, D(w)) = \text{dil}(1, N(w)) \).

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 \( \text{dil}(1, D(w)) \) and \( \text{dil}(1, N(w)) \). By Lemma 4.1, left \( ^k \) \( t_0 \) is a CD-expansion both of \( \text{left}(t \cdot x^{[p]}) \), i.e., of \( t \), and of \( \text{left}(t' \cdot x^{[p]}) \), i.e., of \( t' \). It follows that \( t \) and \( t' \) are CD-equivalent, since they admit a common CD-expansion. \( \blacksquare \)

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

**Proof.** The integers \( \text{dil}(1, N(\chi_t^{-1} \chi_{t'})) \) and \( \text{dil}(1, D(\chi_t^{-1} \chi_{t'})) \) are effectively computable. \( \blacksquare \)

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 \( A \cup A^{-1} \), let us say that \( w \) belongs to \( P_+ \) (resp. \( P_0 \)) if \( \text{dil}(1, D(w)) < \text{dil}(1, N(w)) \) 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

\[
\text{dil}(1, D(w_1w_2)) = \text{dil}(1, D(w_2) \backslash (N(w_2) \backslash D(w_1)))
\]

\[
= \text{dil}(\text{dil}(1, D(w_2)), N(w_2) \backslash D(w_1))
\]

\[
< \text{dil}(\text{dil}(1, N(w_2)), N(w_2) \backslash D(w_1))
\]

\[
= \text{dil}(1, N(w_2) \backslash (N(w_2) \backslash D(w_1)))
\]

\[
= \text{dil}(1, D(w_1) \backslash N(w_2))
\]

\[
= \text{dil}(\text{dil}(1, D(w_1)), N(w_2))
\]

\[
< \text{dil}(\text{dil}(1, N(w_1)), D(w_1) \backslash N(w_2))
\]

\[
= \text{dil}(1, N(w_1) \backslash (D(w_1) \backslash N(w_2))) = \text{dil}(1, N(w_1w_2)),
\]
so we have $P_+P_+ \subseteq P_+$, and, by a similar argument, $P_0P_+ \subseteq P_+$, and $P_+P_0 \subseteq P_+$.

Assume now that $t$ is a proper iterated left subterm of $t'$: this means that we have $t' = ((\ldots(t_{-1})(t_{-2})\ldots)t_k$ for some terms $t_1, \ldots, t_k$, which, by definition, gives a decomposition of the form

$$\chi_{u} = \chi_{t_1} \cdot 1w_0 \cdot \phi \cdot 1w_1 \cdot \ldots \cdot 1w_{k-1} \cdot \phi \cdot 1w_k.$$

For each $i$, the word $1w_i$ belongs to $P_0$, while $\phi$ belongs to $P_+$, since we have $\text{dil}(1,D(\phi)) = \text{dil}(1,\varepsilon) = 1$ and $\text{dil}(1,N(\phi)) = \text{dil}(1,\phi) = 2$. By the above computations, we deduce $\chi_{t_1}^{-1} \chi_{u} \in P_+$, while, by Proposition 4.4, $t = \text{cd} t'$ is equivalent to $\chi_{t}^{-1} \chi_{u} \in P_0$.

(ii) Assume that $t$, $t'$ are distinct terms with the same skeleton. Assume that some variable $x$ occurs at $\alpha$ in $t$, while $x'$ occurs at $\alpha$ 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 $\alpha$ has the form $0^1j$, 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 $\text{left}^k(t'') = \text{cd} \text{left}^k(t)$ and $\text{left}^k(t'') = \text{cd} \text{left}^k(t')$ for some $k$, $k'$. As the rightmost variables in $\text{left}^i(t)$ and $\text{left}^i(t')$ are distinct, and the rightmost variable is preserved under CD-equivalence, we deduce $k \neq k'$. Assume for instance $k > k'$. Then $\text{left}^k(t'')$ is a proper iterated subterm of $\text{left}^k(t'')$, hence of $t_0$, where $t_0$ is the term obtained from $\text{left}^k(t'')$ by replacing the final variable $x'$ by $x$. Now $t_0$ is CD-equivalent to the term obtained from $\text{left}^i(t')$ by replacing the final variable with $x$, and the latter term is $\text{left}^i(t)$. So $t_0$ is CD-equivalent to its proper iterated subterm $\text{left}^{k-k'}(t_0)$, contradicting (i).

\textbf{Proposition 4.7.} The word problem of Identity (CD) is decidable, with a primitive recursive complexity.

\textbf{Proof.} Assume that $t$, $t'$ are terms in $T_{\infty}$. 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 $t = \text{cd} t'$ as follows. First, we test $t_1 = \text{cd} t_1'$ using Proposition 4.4. If $t_1 = \text{cd} t_1'$ fails, so does $t = \text{cd} t'$. Otherwise, $t_1$ and $t_1'$ admit a common CD-expansion, namely $(t_1)u = (t_1')u'$, with $u = N(\chi_{t_1}^{-1} \chi_{u}')$ and $u' = D(\chi_{t_1}^{-1} \chi_{u'})$. Then we compare $(t)u$ and $(t')u'$: these terms exist, as, for $u$ in $A^*$, $(t)u$ 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 $t = \text{cd} t'$, while, by Lemma 4.6(ii), $(t)u \neq (t')u'$ implies $(t)u \neq \text{cd} (t')u'$, hence $t \neq \text{cd} t'$.

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 $\varepsilon^{2^n} x^{[\varepsilon]}$, 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 $a \subset b$, 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).

\textbf{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.

\textbf{Proof.} As $\subset$ is transitive by definition, the point is to prove that $\subset$ is irreflexive, which follows from Lemma 4.6(i): indeed, assume that $a$ is the class of the term $t$; then $a \subset a$ 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 $a$, $a' \subset S$ holds. Let $t$, $t'$ be one variable terms representing $a$ and $a'$ respectively. Let $w = \chi_{t}^{-1} \chi_{u}$. Let $t_0 = (t \cdot x^{[\varepsilon]} \cdot N(w))$, $k = \text{dil}(1, N(w))$, and $k' = \text{dil}(1, D(w))$. As in the proof of Proposition 4.4, we see that $\text{left}^k(t_0)$ is a CD-expansion of $t$, while $\text{left}^{k'}(t_0)$ is a CD-expansion of $t'$, and, therefore, $\text{left}^k(t_0)$
represents a and left $k'(t_0)$ represents $a'$. For $k = k'$, we obtain $a = a'$. For $k > k'$, the term left $k'(t_0)$ is a proper iterated left subterm of left $k'(t_0)$, and we deduce $a \subset a'$. Similarly $k < k'$ implies $a' \subset a$.  

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 $\pi$ 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 $a \subset a'$ or $a' \subset a$ holds. As $\subset$ is definable from the binary operation, $\pi$ preserves $\subset$, so $\pi(a) \subset \pi(a')$ or $\pi(a') \subset \pi(a)$ holds in $S$. If left division in $S$ has no cycle, both imply $\pi(a) \neq \pi(a')$, $\pi$ is injective, and $S$ is isomorphic to $F$, hence free. ■

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

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

The remaining question is whether the latter binary operation is trivial or not: when collapsing all generators $g_{\text{sh}_0}$ in $G$, we could have collapsed everything and obtained a trivial quotient. Actually, we have not:

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

*Proof.* Assume that $a_0G_0, \ldots, a_kG_0$ are cosets in $G_0 \setminus G$ 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 $(a_i * x_i) \, \text{sh}_0(y_i) = a_{i+1}$ in $G$ for some $y_i$. By using the definition of $*$ and gathering the equalities, we obtain in $G$ an equality of the form

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

For $k \geq 1$, (4.1) shows that $a^{-1}_1 a_k$ can be represented by a word containing $k$ letters $\phi$, and no letter $\phi^{-1}$, 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 $a^{-1}_0 a_k \in G_0$. 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 $(G_0 \setminus G, *)$. Proposition 4.9 then implies that every monogenic subsystem of $(G_0 \setminus G, *)$ 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 $\subset$ on free CD-systems of rank 1 as follows: for $t, t'$ in $T_1$, $\overline{t} \subset \overline{t'}$ holds in $T_1/\equiv_{\text{co}}$ if and only if $\overline{t} \prec \overline{t'}$ holds in $G$, where $\overline{t}$ denotes the $\equiv_{\text{co}}$-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 $\overline{G_0}$ of $G$ generated by $G_0$, we still obtain an operation satisfying $(CD)$ on the quotient-group $G/\overline{G_0}$—but the latter quotient is trivial: for every address $\gamma$, the CD-relation $g_\gamma g_{\gamma-1} g_\gamma = g_{\gamma-1} g_\gamma g_0$ in $G$ implies $g_\gamma g_{\gamma-1} g_\gamma g_0 g_\gamma = g_{\gamma-1} g_\gamma g_\gamma$, hence $g_\gamma = 1$, in $G/\overline{G_0}$, and $\overline{G_0}$ 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 \(G' / \hat{G}'_0\), where \(\hat{G}'_0\) is the normal subgroup of \(G'\) generated by \(G'_0\); now \(G' / \hat{G}'_0\) turns out to be Artin’s braid group \(B_\infty\), 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 redressing, 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 Thompson’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 10-1 (2000) 173–190.
[7] —, Braids and Self-Distributivity, Progress in Math. vol. 192, Birkhäuser, (2000).
[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.