Vesa Halava | Tero Harju | Tomi Kärki

Defect theorems with compatibility relations

Turku Centre for Computer Science

TUCS Technical Report
No 778, August 2006

Defect theorems with compatibility relations

Vesa Halava
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku FIN-20014 Turku, Finland
Supported by the Academy of Finland under grant 208414.
vehalava@utu.fi
Tero Harju
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku FIN-20014 Turku, Finland
harju@utu.fi
Tomi Kärki
Department of Mathematics and
TUCS - Turku Centre for Computer Science
University of Turku FIN-20014 Turku, Finland
topeka@utu.fi

TUCS Technical Report
No 778, August 2006

Abstract

We consider words together with a compatibility relation induced by a relation on letters. Unique factorization with respect to two arbitrary word relations R and S defines the (R, S)-freeness of the semigroup considered. We generalize the stability theorem of Schützenberger and Tilson's closure result for (R, S)-free semigroups. The inner and the outer (R, S)-unique factorization hull and the (R, S)-free hull of a set of words are introduced and we show how they can be computed. We prove that the (R, S)-unique factorization hulls possess a defect effect, which implies a variant of a cumulative defect theorem of word semigroups. In addition, a defect theorem of partial words is proved as a corollary.

Keywords: unique factorization, free semigroup, stability, compatibility relation, defect theorem, partial word

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Introduction

Let A be an alphabet. If a set of n words in a free semigroup A^+ generated by the letters of A satisfies a nontrivial relation then these words can be written as products of at most $n-1$ words. This basic result is called the *defect theorem* of words and it is used in many different connections [3, 13, 17, 18]. Actually, there exist several defect theorems depending on the restrictions that are put to the $n-1$ words [15]. A typical formulation of the defect effect is to say that the *rank* of the smallest free semigroup containing a set of words X is strictly smaller than the cardinality of X if and only if X is not a code. By rank we mean the cardinality of the base of the semigroup. The smallest free semigroup containing X is the *free hull* of X.

In this paper the above mentioned concepts are generalized with respect to *word relations*. These are reflexive and symmetric relations, which are induced by letter relations. They were introduced in [14] to generalize the notion of a *partial word* as presented by J. Berstel and L. Boasson in 1999 [1]. Since then combinatorics on partial words has been widely studied; see [4–12, 16]. Motivation for this research comes partly from the study of biological sequences such as DNA, RNA and proteins [6].

In [14] we defined codes with respect to two arbitrary word relations R and S. Such (R, S)-codes model the situation where some of the letters in a message are changed to related letters, but the message can still be decoded in a proper manner. Here we consider the free subsemigroups of A^+ generated by (R, S)-codes. Our aim is to examine defect effects of such semigroups. Basic definitions and results are shortly revisited in Section 2. The starting point of this work is the (R, S)-unique factorization of elements in a subsemigroup of A^+. Unique factorization and freeness with respect to word relations are defined in Section 3. Section 4 is devoted to characterizing these properties with stability conditions. A modified Schützenberger's criterium is proved. In Section 5 we show that under some restrictions there exists the smallest semigroup in A^+ where a set $X \subseteq A^+$ can be factorized (R, S)-uniquely. The inner and the outer (R, S)-unique factorization hulls are defined. The existence of these hulls is a consequence of a generalized Tilson's result. In addition, the result implies the existence of the (R, S)-free hull of X. Section 6 describes procedures for finding the hulls. Finally, we prove a defect effect concerning (R, S)-unique factorizations hulls in the last section. Moreover, a cumulative defect theorem of (R, S)-free hulls is proved as a corollary. Consequently, a defect theorem of partial words follows.

We end this section with some notation. The empty word is denoted by ε. The sets of all finite words and finite nonempty words over A are denoted by A^* and A^+, respectively. With the operation of catenation A^* is a free monoid and A^+ is a free semigroup generated by the letters of A. The *length* of a word w, denoted by $|w|$, is the total number of (occurrences of) letters in w. A word u is called a *prefix* (resp. a *suffix*) of a word v if there exists a word w such that $v = uw$ (resp. $v = wu$). A prefix (resp. a suffix) of v of length n is denoted by $\mathrm{pref}_n(v)$ (resp.

$\mathrm{suf}_n(v)$). For subsets $L, K \subseteq A^*$, we let

$$\begin{aligned} &LK = \{uv \mid u \in L, v \in K\}, \\ &L^{i+1} = L^i L, \\ &L^+ = \bigcup_{i \geq 1} L^i, \quad L^* = L^+ \cup \{\varepsilon\}. \end{aligned}$$

2 Word relations and relational codes

Let $R \subseteq X \times X$ be a relation on a set X. We often write $x\,R\,y$ instead of $(x, y) \in R$. Then R is a *compatibility relation* if it is both reflexive and symmetric, i.e., (i) $\forall x \in X : \; x\,R\,x$, and (ii) $\forall x, y \in X : \; x\,R\,y \implies y\,R\,x$. The *identity relation* on a set X is defined by

$$\iota_X = \{(x, x) \mid x \in X\}$$

and the *universal relation* on X is defined by

$$\Omega_X = \{(x, y) \mid x, y \in X\}.$$

Subscripts are often omitted when they are clear from the context. Clearly, both ι_X and Ω_X are compatibility relations on X.

A compatibility relation $R \subseteq A^+ \times A^+$ on the set of all words over an alphabet A will be called a *word relation* if it is induced by its restriction on the letters, i.e.,

$$a_1 \cdots a_m\,R\,b_1 \cdots b_n \quad \iff \quad m = n \text{ and } a_i\,R\,b_i \text{ for all } i = 1, 2, \ldots, m$$

whenever $a_1, \ldots, a_m, b_1, \ldots, b_n \in A$. Let S be a relation on A. By $\langle S \rangle$ we denote the compatibility relation *generated* by S, i.e., $\langle S \rangle$ is the reflexive and symmetric closure of the relation S. Sometimes we need to consider the restriction of a relation R on a subset X of A^+. We denote $R_X = R \cap (X \times X)$. Words u and v satisfying $u\,R\,v$ are said to be *compatible* or, more precisely, R*-compatible*. For example, in the binary alphabet $A = \{a, b\}$ the compatibility relation $R = \langle\{(a, b)\}\rangle = \{(a, a), (b, b), (a, b), (b, a)\}$ makes all words with equal length compatible with each other. In the ternary alphabet $\{a, b, c\}$ we have $abba\,R\,baab$ but, for instance, words abc and cac are not compatible.

Clearly a word relation R satisfies the following two conditions:

$$\begin{array}{lccc} \text{multiplicativity:} & u\,R\,v, u'\,R\,v' & \implies & uu'\,R\,vv', \\ \text{simplifiability:} & uu'\,R\,vv', |u| = |v| & \implies & u\,R\,v,\; u'Rv'. \end{array}$$

However, a word relation R does not need to be transitive. From now on the relations on words considered in this presentation are supposed to be word relations induced by some compatibility relation on letters.

Let 2^X denote the *power set* of X, that is, the family of all subsets of X including the empty set $\emptyset$ and X itself. For a word relation R on A^+, let the corresponding function $R\colon 2^{A^+} \to 2^{A^+}$ be defined by

$$R(X) = \{u \in A^+ \mid \exists\, x \in X : \, x\, R\, u\}.$$

If X contains only one word $w \in A^+$, we denote $R(X)$ shortly by $R(w)$. The function R is multiplicative in the following sense.

Lemma 1 ([14])**.** *Let R be a word relation on A^+. Then $R(X)R(Y) = R(XY)$ for all $X, Y \subseteq A^+$. Especially, $R(X)^+ = R(X^+)$ for all $X \subseteq A^+$.*

In [14] we considered relational codes. Let R and S be two word relations on the semigroup A^+. A subset $X \subseteq A^+$ is an (R, S)*-code* if for all $n, m \geq 1$ and for all $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$ we have

$$x_1 \cdots x_m\, R\, y_1 \cdots y_n \Rightarrow n = m \text{ and } x_i\, S\, y_i \text{ for } i = 1, 2, \ldots, m.$$

If S is the identity relation ι, then an (R, S)-code is called a *strong R-code*, or shortly just an *R-code*. A strong R-code is always a pairwise non compatible set, but the converse does not hold in general. An (R, R)-code is called a *weak R-code*. An (ι, ι)-code is simply called a *code*. The definition coincides with the original definition of a variable length code.

We note the following results proved in [14]. Suppose that R_1, R_2 and S are relations on A^+ satisfying $R_1 \subset R_2$. If X is an (R_2, S)-code, then X is an (R_1, S)-code. Similarly, consider the relations R, S_1 and S_2 satisfying $S_1 \subset S_2$. If X is an (R, S_1)-code, then X is an (R, S_2)-code. Note that (R, S)-codes are always (ι, ι)-codes, i.e., codes in the usual meaning.

Theorem 1 ([14])**.** *Every (R, S)-code X is a code.*

Moreover, we have the following characterization of (R, S)-codes.

Theorem 2 ([14])**.** *Let X be a subset of A^+. Then X is an (R, S)-code if and only if X is an (R, R)-code and $R_X \subseteq S_X$.*

3 Unique factorization and freeness

All elements in the semigroup X^+ generated by an (R, S)-code X have a "relationally unique" X-factorization. In the sequel we consider these unique factorizations more closely. Let $\mathfrak{S}$ be an arbitrary subsemigroup of A^+. A subset B of a semigroup $\mathfrak{S}$ such that $\mathfrak{S} = B^+$ is called a *generating set* of $\mathfrak{S}$. A generating set is called *minimal* if no proper subset of B is a generating set of $\mathfrak{S}$. Every $\mathfrak{S} \subseteq A^+$ has a unique minimal generating set. Namely, it is the set of *indecomposable elements* of $\mathfrak{S}$, i.e., $\mathfrak{S} \setminus \mathfrak{S}^2$. We call this set the *base* of $\mathfrak{S}$. The cardinality of the base is called the *rank* of $\mathfrak{S}$: $\mathrm{rank}(\mathfrak{S}) = |\mathfrak{S} \setminus \mathfrak{S}^2|$. Note that, for each subset $X \subseteq A^+$, the base of the semigroup X^+ is $X \setminus X^2$.

Let $\mathfrak{T}$ be a semigroup containing a semigroup $\mathfrak{S}$. Denote the base of $\mathfrak{T}$ by B. Since $\mathfrak{S} \subseteq \mathfrak{T} = B^+$, each $x \in \mathfrak{S}$ has at least one B-factorization: $x = x_1 \cdots x_m$ with $x_i \in B$ for $i = 1, 2, \ldots, m$. The element x is said to posses an (R, S)*-unique* B*-factorization in* $\mathfrak{S}$ if, for every compatible factorization $y = y_1 \cdots y_n \in \mathfrak{S}$ with $y_j \in B$ for all $j = 1, 2, \ldots, n$, the following condition holds:

$$x = x_1 \cdots x_m \, R \, y_1 \cdots y_n \Rightarrow n = m \text{ and } x_i \, S \, y_i \text{ for } i = 1, 2, \ldots, m. \qquad (*)$$

Note that if $R = S = \iota$ this definition coincides with the original definition of unique B-factorization. Moreover, we say that $x \in \mathfrak{S}$ possesses an (R, S)*-unique* B*-factorization in* $\mathfrak{T}$ if the condition $(*)$ holds also for every $y \in \mathfrak{T}$.

Next we define two extensions of the semigroup $\mathfrak{S}$ with respect to (R, S)-unique factorization. The semigroup $\mathfrak{T}$ containing $\mathfrak{S}$ is called an *inner* (R, S)*-unique factorization extension* of $\mathfrak{S}$ if every element of $\mathfrak{S}$ has an (R, S)-unique $\mathfrak{T} \setminus \mathfrak{T}^2$-factorization in $\mathfrak{S}$. In addition, the semigroup $\mathfrak{T}$ is called an *outer* (R, S)*-unique factorization extension* of $\mathfrak{S}$ if every element of $\mathfrak{S}$ has an (R, S)-unique $\mathfrak{T} \setminus \mathfrak{T}^2$-factorization in $\mathfrak{T}$. Hence, every outer (R, S)-unique factorization extension of $\mathfrak{S}$ is also inner (R, S)-unique factorization extension. In the sequel, if the type of the (R, S)-unique factorization extension is not specified, the statement is valid for both inner or outer extensions. For these extensions we use the abbreviation (R, S)*-ufe.*

In the above, the (R, S)-unique factorization extension $\mathfrak{T}$ is called a *strong* R*-unique factorization extension,* a *weak* R*-unique factorization extension* or a *unique factorization extension* if $S = \iota$, $R = S$ or $R = S = \iota$, respectively. The following three results describing the role of these special cases can be compared with Theorem 1 and Theorem 2.

Theorem 3. *Let* $\mathfrak{S}$ *be a subsemigroup of* A^+*. Every inner (resp. outer)* (R, S)*-ufe of* $\mathfrak{S}$ *is an inner (resp. outer)* (ι, ι)*-ufe of* $\mathfrak{S}$*.*

Proof. Let $\mathfrak{T}$ be an inner (R, S)-unique factorization extension of $\mathfrak{S}$ and let B be the base of $\mathfrak{T}$. Suppose that $x \in \mathfrak{S}$ has two B-factorizations: $x_1 \cdots x_m = x = y_1 \cdots y_n$, where $x_i, y_j \in B$ for all i and j. Since always $\iota \subseteq R$, we have $x_1 \cdots x_m \, R \, y_1 \cdots y_n$. By the assumption, it follows that $m = n$ and $x_i \, S \, y_i$. Especially, this means that $|x_i| = |y_i|$. Therefore, considering the two B-factorizations of x, we must have $x_i = y_i$. Thus $\mathfrak{T}$ is an inner (ι, ι)-unique factorization extension of $\mathfrak{S}$. The proof for the outer (R, S)-ufe is similar. □

For inner and outer (R, S)-unique factorization extensions we have characterizations in terms of weak R-unique factorization extensions with some additional conditions concerning the order of the word relations R and S.

Theorem 4. *Let* $\mathfrak{S}$ *be a subsemigroup of* A^+ *and let* $\mathfrak{T}$ *be a semigroup containing* $\mathfrak{S}$*. The semigroup* $\mathfrak{T}$ *is an inner* (R, S)*-ufe of* $\mathfrak{S}$ *if and only if* $\mathfrak{T}$ *is an inner* (R, R)*-ufe and* $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$*.*

Proof. Let $\mathfrak{T}$ be an inner (R, S)-unique factorization extension of $\mathfrak{S}$. Let B be the base of $\mathfrak{T}$. Let $x_1 \cdots x_m \in \mathfrak{S}$ and $y_1 \cdots y_n \in \mathfrak{S}$ satisfy $x_1 \cdots x_m \, R \, y_1 \cdots y_n$, where $x_i, y_j \in B$ for all i and j. By the assumption, it follows that $m = n$ and $x_i \, S \, y_i$. Especially, this means that $|x_i| = |y_i|$. By the simplifiability of word relations, $x_1 \cdots x_m \, R \, y_1 \cdots y_m$ implies $x_i \, R \, y_i$ for all $i = 1, 2, \ldots, m$. Hence, $\mathfrak{T}$ is an inner (R, R)-ufe of $\mathfrak{S}$. Clearly, $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$ for all (R, S)-unique factorization extensions of $\mathfrak{S}$.

Conversely, suppose that $\mathfrak{T}$ is an inner (R, R)-ufe of $\mathfrak{S}$, $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$ and B is the base of $\mathfrak{T}$. Let $x_1 \cdots x_m \in \mathfrak{S}$ and $y_1 \cdots y_n \in \mathfrak{S}$ satisfy $x_1 \cdots x_m \, R \, y_1 \cdots y_n$, where $x_i, y_j \in B$ for all i and j. Since $\mathfrak{T}$ is an inner (R, R)-ufe, it follows that $m = n$ and $x_i \, R \, y_i$. Especially this means that $|x_i| = |y_i|$. Since $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$, we have also $x_1 \cdots x_m \, S \, y_1 \cdots y_m$. By the simplifiability of word relations, it follows that $x_i \, S \, y_i$ for all $i = 1, 2, \ldots, m$. Hence, $\mathfrak{T}$ is an inner (R, S)-unique factorization extension of $\mathfrak{S}$. $\square$

For an outer (R, S)-ufe of $\mathfrak{S}$, the characterization takes the following form.

Theorem 5. *Let $\mathfrak{S}$ be a subsemigroup of A^+ and let $\mathfrak{T}$ be a semigroup containing $\mathfrak{S}$. The semigroup $\mathfrak{T}$ is an outer (R, S)-ufe of $\mathfrak{S}$ if and only if $\mathfrak{T}$ is an outer (R, R)-ufe and, for all $x \in \mathfrak{S}$, we have $R(x) \cap \mathfrak{T} \subseteq S(x) \cap \mathfrak{T}$.*

Proof. If $\mathfrak{T}$ is an outer (R, S)-unique factorization extension of $\mathfrak{S}$, then using the same kind of reasoning as in the previous proof, we see that $\mathfrak{T}$ is also an outer (R, R)-ufe and the condition $R(x) \cap \mathfrak{T} \subseteq S(x) \cap \mathfrak{T}$ is satisfied for all $x \in \mathfrak{S}$.

Conversely, suppose that $\mathfrak{T}$ is an outer (R, R)-ufe of $\mathfrak{S}$ and $R(x) \cap \mathfrak{T} \subseteq S(x) \cap \mathfrak{T}$ for all $x \in \mathfrak{S}$. Let B be the base of $\mathfrak{T}$. Assume that $x = x_1 \cdots x_m \in \mathfrak{S}$ and $y = y_1 \cdots y_n \in \mathfrak{T}$ satisfy $x_1 \cdots x_m R y_1 \cdots y_n$, where $x_i, y_j \in B$ for all i and j. Since $\mathfrak{T}$ is an outer (R, R)-ufe, it follows that $m = n$ and $x_i \, R \, y_i$. Especially this means that $|x_i| = |y_i|$. Since $y \in R(x) \cap \mathfrak{T}$, we also have $y \in S(x) \cap \mathfrak{T}$ by the assumption. In other words, $x \, S \, y$. By the simplifiability of word relations, it follows from $|x_i| = |y_i|$ that $x_i \, S \, y_i$ for all $i = 1, 2, \ldots, m$. Hence, $\mathfrak{T}$ is an outer (R, S)-unique factorization extension of $\mathfrak{S}$. $\square$

We define further that a semigroup which is its own (R, S)-unique factorization extension is called (R, S)*-free.* Note that the definitions of outer and inner extensions coincide in this case. *Strong R-freeness*, *weak R-freeness* and *freeness* of an (R, S)-free semigroup are defined similarly as above, i.e., $S = \iota$, $R = S$ or $R = S = \iota$, respectively. By using (R, S)-codes we have the following characterization of (R, S)-free semigroups.

Theorem 6. *Let $X \subseteq A^+$. Then the following conditions are equivalent.*

(i) *X is an (R, S)-code.*

(ii) *X^+ is (R, S)-free and X is its base.*

Proof. Suppose first that X is an (R,S)-code. By Theorem 1, X is a code and thus $X = X \backslash X^2$. Therefore X is the base of X^+. Consider now an element of X^+ with an X-factorization $x_1 \cdots x_m$. Since X is an (R,S)-code, the condition $(*)$ holds for all $y_1, \ldots, y_n \in X$. Thus X^+ is its own (R,S)-unique factorization extension and therefore it is (R,S)-free.

Conversely, suppose that X^+ is (R,S)-free and X is its base. Since X^+ is its own (R,S)-unique factorization extension with base X, then the condition $(*)$ holds for all $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$. Thus, X is an (R,S)-code. □

By the above theorem, it is clear the (ι,ι)-free semigroups are the free semigroups in the original meaning of freeness. Relational freeness of a semigroup of A^+ implies the following facts about the considered word relations.

Theorem 7. *Let $\mathfrak{S}$ be an (R,S)-free semigroup of A^+. The following conditions hold.*

(i) If $S \subseteq R$, then $R_{\mathfrak{S}} = S_{\mathfrak{S}}$.

(ii) If $R \cap S = \iota$, then $R_{\mathfrak{S}} = \iota_{\mathfrak{S}}$

Proof. Since $\mathfrak{S}$ is an (R,S)-free semigroup, every element of $\mathfrak{S}$ satisfies the condition $(*)$. Thus $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$. If $S \subseteq R$, then $S_{\mathfrak{S}} \subseteq R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$, i.e., $R_{\mathfrak{S}} = S_{\mathfrak{S}}$. Also if $R \cap S = \iota$, then $R_{\mathfrak{S}} = R_{\mathfrak{S}} \cap S_{\mathfrak{S}} = \iota$. □

The next theorem follows from the code characterization of (R,S)-free semigroups.

Theorem 8. *A semigroup $\mathfrak{S} \subseteq A^+$ is (R,S)-free if and only if $\mathfrak{S}$ is (R,R)-free and $R_B \subseteq S_B$ for the base B of $\mathfrak{S}$.*

Proof. Let B be the base of the semigroup $\mathfrak{S}$. By Theorem 6, $\mathfrak{S}$ is (R,S)-free if and only if B is an (R,S)-code. By Theorem 2, B is an (R,S)-code if and only if B is an (R,R)-code and $R_B \subseteq S_B$. Using again Theorem 6, this is true if and only if $\mathfrak{S} = B^+$ is (R,R)-free and $R_B \subseteq S_B$. □

We have also the following corollary.

Corollary 1. *The full semigroup A^+ for an alphabet A is (R,S)-free if and only if $R \subseteq S$.*

Proof. By the definition of a word relation, the semigroup A^+ is (R,R)-free with base A. Thus, by the previous theorem, A^+ is (R,S)-free if and only if $R_A \subseteq S_A$. □

Note that, for (R,S)-free semigroups, the characterizing condition on the order of the relations R and S can be easily expressed using the base of the semigroup. This is not the case for inner and outer (R,S)-unique factorization extensions of $\mathfrak{S}$. The condition $R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}$ for inner (R,S)-unique factorization extensions cannot be replaced by $R_B \subseteq S_B$, where B is the base of $\mathfrak{S}$. Consider the following example.

Example 1. Let $\mathfrak{S}$ be a semigroup with base $B = \{ab, a, c\}$. Define $R = \langle\{(b, c)\}\rangle$ and $S = \iota$. Clearly the semigroup with base $\{a, b, c\}$ is an inner (R, R)-ufe of $\mathfrak{S}$. Now $R_B \subseteq S_B$ is satisfied, since there are no R-compatible base elements in $\mathfrak{S}$. But there does not exist an inner (R, S)-ufe of $\mathfrak{S}$, since $ab\, R\, ac$, but $(ab, ac) \notin S$. Since an inner (R, S)-ufe is also an outer (R, S)-ufe, the base condition $R_B \subseteq S_B$ is not sufficient for outer (R, S)-unique factorization extensions either.

Moreover, let $B_{\mathfrak{S}}$ be the base of $\mathfrak{S}$ and assume that $\mathfrak{S} \subseteq \mathfrak{T}$. The following implications are valid in general:

$$(\forall\, x \in \mathfrak{S} : R(x) \cap \mathfrak{T} \subseteq S(x) \cap \mathfrak{T}) \implies R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}} \implies R_{B_{\mathfrak{S}}} \subseteq S_{B_{\mathfrak{S}}}.$$

Suppose now that $\mathfrak{S} = \mathfrak{T}$ and $\mathfrak{S}$ is (R, S)-free, in other words, it is an outer and an inner (R, S)-unique factorizations extensions of itself. Thus, for such $\mathfrak{S}$, the (R, R)-unique factorizations of its elements implies

$$R_{B_{\mathfrak{S}}} \subseteq S_{B_{\mathfrak{S}}} \Leftrightarrow R_{\mathfrak{S}} \subseteq S_{\mathfrak{S}}.$$

and, for all $x \in \mathfrak{S} = \mathfrak{T}$, it clearly holds $R(x) \cap \mathfrak{T} \subseteq S(x) \cap \mathfrak{T}$. Hence, the above mentioned implications are equivalences in this special case.

4 Stability

A semigroup $\mathfrak{T} \subseteq A^+$ is called *intrinsically* (R, S)*-stable* over a semigroup $\mathfrak{S}$ if $\mathfrak{S} \subseteq \mathfrak{T}$ and for all $u, v, w, u', v', w' \in A^+$ satisfying conditions

(i) $\quad u\, R\, u'$, $w\, R\, w'$ and $v\, R\, v'$,

(ii) $\quad uwv, u'w'v' \in \mathfrak{S}$ and $uw, v, u', w'v' \in \mathfrak{T}$,

we have $u, w \in \mathfrak{T}$ and $u\, S\, u'$. This situation is illustrated in Figure 1. Similarly, $\mathfrak{T}$ is called *extrinsically* (R, S)*-stable* over $\mathfrak{S}$ if condition (ii) above is replaced by

$(ii)'$ $\quad uwv \in \mathfrak{S}$ **or** $u'w'v' \in \mathfrak{S}$ and $uw, v, u', w'v' \in \mathfrak{T}$.

If a semigroup is (R, S)-stable over itself, we shortly call it (R, S)*-stable.* Note that in this case the definitions of intrinsic and extrinsic (R, S)-stability coincide. As above, we talk about *strong* and *weak* R*-stability* depending on whether $S = \iota$ or $S = R$. The definition of (R, S)-stable semigroups coincides with the original definition of *stable* word semigroups in the case $R = S = \iota$.

Next we prove, how stability and unique factorization are related to each other.

Theorem 9. *Let $\mathfrak{S}$ be a semigroup in A^+. A subsemigroup of A^+ is an inner (resp. outer) (R, S)-unique factorization extension of $\mathfrak{S}$ if and only if it is intrinsically (resp. extrinsically) (R, S)-stable over $\mathfrak{S}$.*

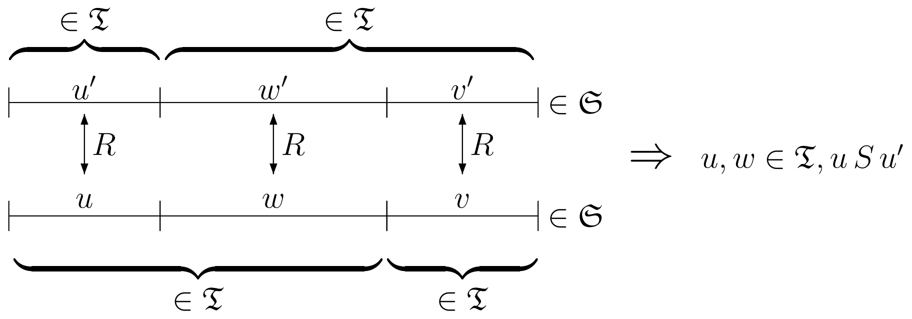

Figure 1: Illustration of (R, S)-stability of $\mathfrak{T}$ in $\mathfrak{S}$

Proof. Let us prove the theorem for inner extensions and intrinsic stability. The proof for the outer and extrinsic case is similar. Assume that $\mathfrak{S}$ is a subsemigroup of $\mathfrak{T}$. Let $\mathfrak{T}$ be intrinsically (R, S)-stable over $\mathfrak{S}$ and let B be the base of $\mathfrak{T}$. Suppose now that $\mathfrak{T}$ is not an inner (R, S)-unique factorization extension of $\mathfrak{S}$. Then there exist words $x_1, \ldots, x_m, y_1, \ldots, y_n \in B$ such that $x_1 \cdots x_m, y_1 \cdots y_n \in \mathfrak{S}$, $x_1 \cdots x_m \, R \, y_1 \cdots y_n$ and $(x_i, y_i) \in S$ for $i = 1, 2, \ldots, k-1 < \min\{m, n\}$, but $(x_k, y_k) \notin S$. We may now assume that $k \neq 1$, $k \neq m$ and $k \neq n$ by replacing the word $x_1 \cdots x_m$ with $x_1 \cdots x_m x_1 \cdots x_m x_1 \cdots x_m$ and the word $y_1 \cdots y_n$ with $x_1 \cdots x_m y_1 \cdots y_n x_1 \cdots x_m$. By the symmetry, we may further suppose that $|x_k| \leq |y_k|$.

Consider first the case $|x_k| = |y_k|$. Then $x_k \, R \, y_k$. Choose now

$$\left\{\begin{array}{lcl} u & = & x_1 \cdots x_k, \\ w & = & x_{k+1} \cdots x_m, \\ v & = & x_1 \cdots x_m, \end{array}\right. \quad \text{and} \quad \left\{\begin{array}{lcl} u' & = & y_1 \cdots y_k, \\ w' & = & y_{k+1} \cdots y_n, \\ v' & = & y_1 \cdots y_n. \end{array}\right.$$

Since these words in A^+ satisfy the conditions (i) and (ii) and $\mathfrak{T}$ is intrinsically (R, S)-stable, we have $x_1 \cdots x_k \, S \, y_1 \cdots y_k$. By the simplifiability of a word relation, we have $x_k \, S \, y_k$. A contradiction.

Hence, we must have $|x_k| < |y_k|$. Thus, we may write $y_k = y' y''$, where $y', y'' \in A^+$ and $|y'| = |x_k|$. Write also $x_{k+1} \cdots x_m = x'' x$, where $x'', x \in A^+$ and $|x''| = |y''|$. Note that the word x is not empty since $x \, R \, y_{k+1} \cdots y_n$. Let us now choose

$$\left\{\begin{array}{lcl} u & = & y_1 \cdots y_{k-1} y', \\ w & = & y'', \\ v & = & y_{k+1} \cdots y_n, \end{array}\right. \quad \text{and} \quad \left\{\begin{array}{lcl} u' & = & x_1 \cdots x_k, \\ w' & = & x'', \\ v' & = & x. \end{array}\right.$$

Since $|x_i| = |y_i|$ for $i = 1, 2, \ldots, k-1$, the conditions (i) and (ii) of the (R, S)-stability of $\mathfrak{T}$ over $\mathfrak{S}$ are satisfied. Since $\mathfrak{T}$ is intrinsically (R, S)-stable over $\mathfrak{S}$, we have $y_1 \cdots y_{k-1} y', y'' \in \mathfrak{T}$ and $y_1 \cdots y_{k-1} y' \, S \, x_1 \cdots x_k$. This in turn enables us to use the intrinsic (R,S)-stability over $\mathfrak{S}$ again. We choose

$$\left\{\begin{array}{lcl} u &=& y_1\cdots y_{k-1},\\ w &=& y',\\ v &=& y''y_{k+1}\cdots y_n,\end{array}\right. \qquad \text{and} \qquad \left\{\begin{array}{lcl} u' &=& x_1\cdots x_{k-1},\\ w' &=& x_k,\\ v' &=& x_{k+1}\cdots x_m,\end{array}\right.$$

and we get $y' \in \mathfrak{T}$. Now $y_k = y'y'' \in \mathfrak{T}^2$. This is impossible since y_1 is an element of the base $\mathfrak{T} \setminus \mathfrak{T}^2$. Hence, $\mathfrak{T}$ must be an (R,S)-unique factorization extension of $\mathfrak{S}$.

Conversely, let $\mathfrak{T}$ be an inner (R,S)-unique factorization extension of $\mathfrak{S}$ and let B be the base of $\mathfrak{T}$. Furthermore, assume that words $u,v,w,u',v',w' \in A^+$ satisfy the conditions (i) and (ii). Thus we may write $uw, v, u', w'v'$ as products of elements of the base B:

$$\begin{array}{rcl} uw &=& x_1\cdots x_k\\ v &=& v_1\cdots v_l\\ u' &=& u_1\cdots u_m\\ w'v' &=& y_1\cdots y_n\end{array}$$

Since $u\,R\,u'$, $w\,R\,w'$ and $v\,R\,v'$, we have by the multiplicativity of word relations that

$$x_1\cdots x_k v_1\cdots v_l\,R\,u_1\cdots u_m y_1\cdots y_n.$$

Since $\mathfrak{T}$ is an inner (R,S)-unique factorization extension of $\mathfrak{S}$ and $x_1\cdots x_k v_1\cdots v_l, u_1\cdots u_m y_1\cdots y_n \in \mathfrak{S}$, we conclude that $k+l = m+n$ and corresponding elements of the both sides are S-compatible and furthermore of the same length. Since $|u'| = |u| < |uw|$, we have

$$u' = u_1\cdots u_m\,S\,x_1\cdots x_m = u \quad \text{and} \quad w = x_{m+1}\cdots x_k \in B^+.$$

In other words, $u,w \in \mathfrak{T}$ and $u\,S\,u'$. Hence, $\mathfrak{T}$ is intrinsically (R,S)-stable over $\mathfrak{S}$. □

This result gives as an easy consequence the following theorem concerning (R,S)-stable and (R,S)-free semigroups. It is called here the generalized Schützenberger's criterium, for comparison see [2].

Corollary 2. (generalized Schützenberger's criterium) *A subsemigroup of A^+ is (R,S)-free if and only if it is (R,S)-stable.*

Proof. By the definition of (R,S)-freeness, (R,S)-free subsemigroup $\mathfrak{T}$ of A^+ is an (R,S)-unique factorization extension of itself. This is possible if and only if $\mathfrak{T}$ is (R,S)-stable (over itself) by the previous theorem. □

Note that the usual formulation of Schützenberger's criterium for semigroups follows easily by assigning $R = S = \iota$.

Corollary 3. *A subsemigroup of A^+ is free if and only if it is stable.*

5 Hulls

Using the stability results of the previous section it is easy to prove the following closure property of (R, S)-unique factorization extensions.

Theorem 10. *Let $\mathfrak{S}$ be a semigroup of A^+. Any intersection of inner (resp. outer) (R, S)-unique factorizations extensions of $\mathfrak{S}$ is an inner (resp. outer) (R, S)-unique factorization extension of $\mathfrak{S}$.*

Proof. We prove the theorem for inner extensions. The proof for outer extensions is similar. Let $\mathfrak{T}_i$ be an inner (R, S)-unique factorization extension of $\mathfrak{S}$ for each $i \in \mathcal{I}$. Set $\mathfrak{T} = \cap_{i\in\mathcal{I}}\mathfrak{T}_i$. Clearly $\mathfrak{T}$ is a semigroup as an intersection of semigroups. Moreover, it is nonempty, since the intersection contains $\mathfrak{S}$. Consider now words u, w, v, u', w', v' satisfying $u\,R\,u'$, $w\,R\,w'$ and $u\,R\,u'$. Assume that $uwv, u'w'v' \in \mathfrak{S}$ and $uw, v, u', w'v' \in \mathfrak{T}$. By the definition of $\mathfrak{T}$, this means that $uw, v, u', wv' \in \mathfrak{T}_i$ for all $i \in \mathcal{I}$. Since every $\mathfrak{T}_i$ is an inner (R, S)-unique factorization extension of $\mathfrak{S}$, every $\mathfrak{T}_i$ is intrinsically (R, S)-stable over $\mathfrak{S}$ by Theorem 9. Hence, we have $u, w \in \mathfrak{T}_i$ for all $i \in \mathcal{I}$ and $u\,S\,u'$. This means that $u, w \in \mathfrak{T}$ and $u\,S\,u'$, i.e., $\mathfrak{T}$ is intrinsically (R, S)-stable. Using Theorem 9 again, we conclude that $\mathfrak{T}$ is an inner (R, S)-unique factorization extension of $\mathfrak{S}$. $\square$

As a corollary of the previous theorem we get the following result concerning (R, S)-free semigroups. It is called here the generalized Tilson's result, for comparison see [19].

Corollary 4. (generalized Tilson's result) *Any nonempty intersection of (R, S)-free subsemigroups of A^+ is (R, S)-free.*

Proof. Let $\mathfrak{S}_i$ be an (R, S)-free subsemigroup of A^+ for each $i \in \mathcal{I}$. Suppose that the intersection $\mathfrak{S} = \cap_{i\in\mathcal{I}}\mathfrak{S}_i$ is nonempty. Clearly $\mathfrak{S}$ is a semigroup. By the definition of (R, S)-freeness, every $\mathfrak{S}_i$ is an (R, S)-unique factorization extension of itself. Thus, every $\mathfrak{S}_i$ is an (R, S)-unique factorization extension of $\mathfrak{S}$. By Theorem 10, $\mathfrak{S}$ is an (R, S)-unique factorization extension of itself and therefore (R, S)-free. $\square$

Note that the previous theorem could have been proved also using Corollary 2. In that case the proof is similar to the proof of Theorem 10. As a special case $R = S = \iota$ of Corollary 4 we have also proved the usual formulation of Tilson's result for words.

Corollary 5. *Any nonempty intersection of free subsemigroups of A^+ is free.*

Let X be an arbitrary subset of A^+. Consider now the following sets of (R, S)-unique factorization extensions of X^+:

$$\begin{aligned}
\mathcal{E}^i_{R,S}(X) &= \{\mathfrak{S} \mid \mathfrak{S} \text{ is an inner } (R, S)\text{-ufe of } X^+\},\\
\mathcal{E}^o_{R,S}(X) &= \{\mathfrak{S} \mid \mathfrak{S} \text{ is an outer } (R, S)\text{-ufe of } X^+\}.
\end{aligned}$$

First we note that if X is a generating set of a semigroup $\mathfrak{S}$, then $\mathcal{E}^i_{R,S}(\mathfrak{S}) = \mathcal{E}^i_{R,S}(X)$ and $\mathcal{E}^o_{R,S}(\mathfrak{S}) = \mathcal{E}^o_{R,S}(X)$. Secondly, note that these sets may be empty. This was already seen in Example 1. On the other hand, it follows from Theorem 10 that the set $\mathcal{E}^i_{R,S}(X)$ (resp. $\mathcal{E}^o_{R,S}(X)$) is closed under intersection. Thus, if $\mathcal{E}^i_{R,S}(X)$ is nonempty, there exists a semigroup

$$\mathfrak{E}^i_{R,S}(X) = \bigcap_{\mathfrak{S} \in \mathcal{E}^i_{R,S}(X)} \mathfrak{S},$$

which is the smallest inner (R, S)-unique factorization extension of X^+. It is called the *inner* (R, S)*-unique factorization hull* of X or, shortly, the *inner* (R, S)*-hull* of X. The similar result holds also for outer (R, S)-unique factorization extensions. We denote the *outer* (R, S)*-unique factorization hull* of X by $\mathfrak{E}^o_{R,S}(X)$ and call it shortly the *outer* (R, S)*-hull* of X. As noted above, the existence of these hulls depends on the relations R and S and the set X itself. By Corollary 1, the sets $\mathcal{E}^i_{R,S}(X)$ and $\mathcal{E}^o_{R,S}(X)$ are nonempty at least if $R \subseteq S$. Namely, in this case A^+ is an (R, S)-unique factorization extension of any of its subsemigroups. Thus we always have $\mathcal{E}^i_{R,R}(X) \neq \emptyset$ and $\mathcal{E}^o_{R,R}(X) \neq \emptyset$. For simplicity, we denote $\mathfrak{E}^i_{R,R}(X) = \mathfrak{E}^i_R(X)$ and $\mathfrak{E}^o_{R,R}(X) = \mathfrak{E}^o_R(X)$ in the sequel. These hulls are shortly called *weak inner and outer* R*-hulls* of X, respectively. Weak hulls play an important role among relational hulls as will be stated in the following theorem.

Theorem 11. *Let X be a subset of A^+. The inner (R, S)-hull of X exists if and only if $R_{X^+} \subseteq S_{X^+}$, in which case $\mathfrak{E}^i_{R,S}(X) = \mathfrak{E}^i_R(X)$.*

Proof. Since the inner (R, R)-hull of an arbitrary set $X \subseteq A^+$ always exists, the condition $R_{X^+} \subseteq S_{X^+}$ is necessary and sufficient for the existence of the (R, S)-hull by Theorem 4.

Suppose now that an inner (R, S)-hull of a set X exists. By Theorem 4, every inner (R, S)-ufe of X is a weak R-ufe of X. Thus, the smallest weak R-ufe of X is contained in the intersection of all inner (R, S)-unique factorization extensions of X. In other words, $\mathfrak{E}^i_R(X) \subseteq \mathfrak{E}^i_{R,S}(X)$. Suppose that $\mathfrak{E}^i_R(X) \neq \mathfrak{E}^i_{R,S}(X)$. Now the (R, R)-unique factorization extension $\mathfrak{E}^i_R(X)$ is not an (R, S)-unique factorization extension of X^+. Hence, there exist $x, y \in X^+$ such that $(x, y) \in R \setminus S$. This contradicts the above mentioned condition on the inclusion of the relations. Thus, we must have $\mathfrak{E}^i_R(X) = \mathfrak{E}^i_{R,S}(X)$ □

Using similar consideration we may also prove the corresponding result for outer (R, S)-hulls.

Theorem 12. *Let X be a subset of A^+. The outer (R, S)-hull of X exists if and only if, for all $x \in X^+$, we have $R(x) \cap \mathfrak{E}^o_R(X) \subseteq S(x) \cap \mathfrak{E}^o_R(X)$, in which case $\mathfrak{E}^o_{R,S}(X) = \mathfrak{E}^o_R(X)$.*

We also have similar results for (R,S)-free semigroups. If the set

$$\mathcal{F}_{R,S}(X) = \{\mathfrak{S} \mid X^+ \subseteq \mathfrak{S} \subseteq A^+, \mathfrak{S} \text{ is an } (R,S)\text{-free semigroup}\}.$$

is not empty, we define that the (R,S)*-free hull* of $X \subseteq A^+$ is

$$\mathfrak{F}_{R,S}(X) = \bigcap_{\mathfrak{S} \in \mathcal{F}_{R,S}(X)} \mathfrak{S}.$$

The existence of this smallest (R,S)-free semigroup containing X is based on the generalized Tilson's resuls (Corollary 4). Like above we use a shorter notation for weak R-free hulls, i.e. $\mathfrak{F}_{R,R}(X) = \mathfrak{F}_R(X)$. For all sets $X \subseteq A^+$, the weak R-free hull of X exists, since A^+ is always (R,R)-free. For (R,S)-free hulls we have a similar characterization as above.

Theorem 13. *Let X be a subset of A^+. Let B be the base of the semigroup $\mathfrak{F}_R(X)$. The (R,S)-free hull of X exists if and only if $R_B \subseteq S_B$, in which case $\mathfrak{F}_{R,S}(X) = \mathfrak{F}_R(X)$.*

The proof of this theorem is based on the characterization of (R,S)-free semigroups in Theorem 8 and on similar considerations as in the proof of Theorem 11.

Let X be an arbitrary subset of A^+. Clearly the outer (R,S)-hull of X is an inner (R,S)-ufe of X^+. Moreover, the (R,S)-free hull of X is an outer (R,S)-ufe of X^+. By the minimality of hulls, we therefore have

$$\mathfrak{E}^i_{R,S}(X) \subseteq \mathfrak{E}^o_{R,S}(X) \subseteq \mathfrak{F}_{R,S}(X). \tag{1}$$

Suppose further that Y is a set containing X. By the minimality of hulls, it is also clear that

$$\begin{aligned} \mathfrak{E}^i_{R,S}(X) &\subseteq \mathfrak{E}^i_{R,S}(Y), & (2)\\ \mathfrak{E}^o_{R,S}(X) &\subseteq \mathfrak{E}^o_{R,S}(Y), & (3)\\ \mathfrak{F}_{R,S}(X) &\subseteq \mathfrak{F}_{R,S}(Y). & (4) \end{aligned}$$

In the next section we will consider inclusion properties of hulls more precisely.

6 Procedures

Next we consider a method to find the hulls in practise. By the characterizations of the previous section, we can restrict our considerations to finding weak R-hulls. If the weak hulls are (R,S)-hulls, this can be verified algorithmically by considering the inclusion of the relations R and S; see Theorems 11-13.

Let X be a finite subset of A^+. In order to construct an inner (R,R)-unique factorization hull Y^+ of X, we must prevent "nontrivial" relations in X^+. For this purpose, we define that a pair of words $(u,v) \in Y \times Y$ is an *inner R-match for Y over X* if u and v begin a relation at the same position, i.e.,

$$\exists\, x', x'', y', y'' \in Y^* : x'ux'', y'vy'' \in X^+,\ x'ux''\, R\, y'vy'',\text{ and } |x'| = |y'|. \quad (5)$$

In the definition of an *outer R-match for Y over X* condition (5) is replaced by the weaker condition

$$\exists\, x', x'', y', y'' \in Y^* : x'ux'' \in X^+,\ x'ux''\, R\, y'vy'',\text{ and } |x'| = |y'|, \quad (6)$$

where only one of the words $x'ux''$ and $y'vy''$ must belong to X^+. An inner or an outer R-match is called *nontrivial* if $(u,v) \notin R$. Otherwise, the pair is called *trivial*. Let us denote the set of nontrivial inner (resp. outer) R-matches for Y over X by $C^i_{R,X}(Y)$ (resp. $C^o_{R,X}(Y)$). Using these sets we can characterize (R,R)-unique factorization extensions of X^+ in the following way.

Lemma 2. *Y^+ is an inner (resp. outer) (R,R)-ufe of X^+ if and only if $C^i_{R,X}(Y) = \emptyset$ (resp. $C^o_{R,X}(Y) = \emptyset$).*

Proof. We give a proof for the inner (R,R)-hulls. The proof for the outer (R,R)-hulls is similar. If Y^+ is an inner (R,R)-ufe of X, it is clear that $C^i_{R,X}(Y)$ must be empty. Conversely, suppose that $C^i_{R,X}(Y) = \emptyset$. Consider words $x_1, \ldots, x_m$, $y_1, \ldots, y_n \in Y$ such that $x_1 \cdots x_m\, R\, y_1 \cdots y_n$ and $x_1 \cdots x_m, y_1 \cdots y_n \in X^+$. Since $C^i_{R,X}(Y) = \emptyset$, we must have $x_1\, R\, y_1$. This implies that $|x_1| = |y_1|$. Thus also $x_2\, R\, y_2$, for otherwise, $C^i_{R,X}(Y) \neq \emptyset$. Now $|x_1x_2| = |y_1y_2|$. Continuing similarly, we see that $x_i\, R\, y_i$ for all $i = 1, 2, \ldots, \min\{m,n\}$. By R-compatibility, $|x_1 \cdots x_m| = |y_1 \cdots y_n|$, which implies that $n = m$. Hence, Y^+ is an inner (R,R)-ufe of X^+. □

For the next procedure we need one more definition. For a word $u \in Y$ we define a set $D^i_{R,X}(u,Y)$: A word v belongs to $D^i_{R,X}(u,Y)$ if and only if $v = u$ or for some positive integer n there exist words $u = u_0, u_1, \ldots, u_{n-1}, u_n = v \in Y$ such that for $j = 0, 1, \ldots, n-1$ the pair (u_i, u_{i+1}) is a trivial inner R-match for Y over X. If we require that (u_i, u_{i+1}) is only a trivial outer R-match, the corresponding set is denoted by $D^o_{R,X}(u,Y)$. Let us now define the following iterative procedure similar to the procedures introduced in [15].

Procedure 1 (Inner hull $P_i(X,R)$**).** Let the input be a finite set $X \subseteq A^+$ and a word relation R on A^+. Set $X_0 = X$, and iterate for $j \geq 0$:

1. Choose an inner match $(u,v) \in C^i_{R,X}(X_j)$ such that $u = u'u''$, where $|u'| = |v|$ and $u'' \in A^+$. If no such pair exists, then stop and return $P_i(X,R) = X_j$.
2. Set $R'(u) = \{\mathrm{pref}_{|u'|}(w) \mid w \in D^i_{R,X}(u, X_j)\}$ and set $R''(u) = \{\mathrm{suf}_{|u''|}(w) \mid w \in D^i_{R,X}(u, X_j)\}$.
3. Set $X_{j+1} = \big(X_j \setminus D^i_{R,X}(u, X_j)\big) \cup R'(u) \cup R''(u)$.

When a word $u = u'u'' \in X_j$ is replaced by two new words u' and u'' in X_{j+1}, this is called a *split* of u into u' and u''. Note that in each iteration step at least one of the words in X_j is split into two proper factors, since $\varepsilon \notin X_j$ for any $j \geq 0$. For a finite set of words there are only finitely many factors, and therefore the procedure must terminate. Next we prove that Procedure 1 computes the inner (R, R)-hull of X.

Theorem 14. *Let X be a finite subset of X^+. Then Procedure 1 with input X returns the base of the inner (R, R)-hull of X, i.e.,*

$$\mathfrak{E}^i_R(X) \setminus \mathfrak{E}^i_R(X)^2 = P_i(X, R).$$

Proof. As mentioned above the procedure P_i always terminates with finite input $X \subseteq A^+$. Suppose now that the procedure terminates after k iterations. Let us first show by induction that

$$X_j^+ \subseteq \mathfrak{E}^i_R(X)$$

for all $j = 0, 1, \ldots, k$. The case $j = 0$ is clear by the definition of $\mathfrak{E}^i_R(X)$. Suppose now that $X_j^+ \subseteq \mathfrak{E}^i_R(X)$ and $(u, v) \in C^i_{R,X}(X_j)$. We claim that

$$R'(u) \cup R''(u) \subseteq \mathfrak{E}^i_R(X).$$

Consider a word $w \in D^i_{R,X}(u, X_j)$. Assume first that $w = u$. We prove that u' and u'' belong to $\mathfrak{E}^i_R(X)$. Since u and v satisfy condition (5) and we have $x'u, x'', y'v, y'' \in X_j^+ \subseteq \mathfrak{E}^i_R(X)$ by our induction hypothesis, the intrinsic (R, R)-stability of $\mathfrak{E}^i_R(X)$ implies

$$x'u', u'' \in \mathfrak{E}^i_R(X).$$

Similarly, $x'u', u''x'', y', vy'' \in \mathfrak{E}^i_R(X)$ imply

$$x', u' \in \mathfrak{E}^i_R(X).$$

Suppose then that $w \in D^i_{R,X}(u, X_j) \setminus \{u\}$ and for some positive integer n there exist words $u = u_0, u_1, \ldots, u_{n-1}, u_n = w \in X_j$ such that u_i and u_{i+1} satisfy condition (5) and $u_i \, R \, u_{i+1}$ for all $i = 0, 1, \ldots, n-1$. Furthermore, assume that for $i = 0, 1, \ldots, n-1$ the words $u'_i = \mathrm{pref}_{|u'|}(u_i)$ and $u''_i = \mathrm{suf}_{|u''|}(u_i)$ belong to $\mathfrak{E}^i_R(X)$. We use the intrinsic (R, R)-stability of $\mathfrak{E}^i_R(X)$ like above. Since u_{n-1} and u_n satisfy condition (5) and $y'u_n$, y'', $x'u'_{n-1}$ and $u''_{n-1}x''$ belong to $\mathfrak{E}^i_R(X)$, we have $y'u'_n, u''_n \in \mathfrak{E}^i_R(X)$, where $u'_n = \mathrm{pref}_{|u'|}(u_n)$ and $u''_n = \mathrm{suf}_{|u''|}(u_n)$. Note that we used the fact that $|u_{n-1}| = |u_n|$. Moreover, since now the words $y'u'_n, u''_n y'', x', u_{n-1}x'' \in \mathfrak{E}^i_R(X)$, we have $u'_n \in \mathfrak{E}^i_R(X)$ again because of the intrinsic (R, R)-stability. Hence, we have proved that $R'(u) \cup R''(u) \subseteq \mathfrak{E}^i_R(X)$. Thus, we have modified X_j in such a way that we have added only elements which must belong to the inner (R, R)-hull of X and we have not deleted any essential elements. Namely, $X \subseteq X_j^+ \subseteq X_{j+1}^+$, since $D^i_{R,X}(u, X_j) \subseteq R'(u)R''(u)$. Therefore, $X_{j+1}^+ \subseteq \mathfrak{E}^i_R(X)$.

Since $C^i_{R,X}(X_k) = \emptyset$, the semigroup X_k^+ is an inner (R, R)-ufe of X^+ by Lemma 2. Hence $X \subseteq X_k^+ \subseteq \mathfrak{E}^i_R(X)$ and the minimality of the inner (R, R)-hull of X implies that $X_k^+ = \mathfrak{E}^i_R(X)$. Note that X_k consists only of the indecomposable elements in X_k^+. Namely, consider words $x, x', x'' \in X_k$ such that $x = x'x''$. Since every $x \in X_k$ is a factor of some word in X^+, we have $(x, x') \in C^i_{R,X}(X_k)$. This is impossible. Thus X_k is the (R, R)-base of $\mathfrak{E}^i_R(X)$. In other words, $\mathfrak{E}^i_R(X) \setminus \mathfrak{E}^i_R(X)^2 = X_k = P_i(X, R)$. ☐

The procedure for finding the base of the outer (R, R)-hull of X is very similar to Procedure 1. It is obtained by replacing $C^i_{R,X}(X_j)$ by $C^o_{R,X}(X_j)$ and $D^i_{R,X}(u, X_j)$ by $D^o_{R,X}(u, X_j)$. We denote this procedure for outer hulls by $P_o(X, R)$. Modifying slightly the previous proof, it is easy to see that $P_o(X, R)$ works.

We may use Procedure 1 also to obtain the (R, R)-free hull of X. Let us define that $(\mathfrak{E}^i_R)^0(X) = X$ and

$$(\mathfrak{E}^i_R)^j(X) = \mathfrak{E}^i_R((\mathfrak{E}^i_R)^{j-1}(X))$$

for all integers $j > 0$. The notation $(E^o_R)^j(X)$ is defined similarly. Now we have the following result.

Theorem 15. *Let X be a subset of A^+. Then for all $j \geq 0$ we have*

$$(\mathfrak{E}^i_R)^j(X) \subseteq (\mathfrak{E}^o_R)^j(X) \subseteq \mathfrak{F}_R(X).$$

Moreover, for finite X, there exists $k \geq 0$ such that $(\mathfrak{E}^i_R)^k(X) = (\mathfrak{E}^i_R)^{k+1}(X)$, in which case

$$(\mathfrak{E}^i_R)^k(X) = (\mathfrak{E}^i_R)^k(X) = \mathfrak{F}_R(X).$$

Proof. For $j = 0$, the claim $(\mathfrak{E}^i_R)^0(X) = (\mathfrak{E}^o_R)^0(X) = X \subseteq \mathfrak{F}_R(X)$ is clear. Suppose then that $(\mathfrak{E}^i_R)^j(X) \subseteq (\mathfrak{E}^o_R)^j(X) \subseteq \mathfrak{F}_R(X)$ for some integer j. Using properties $(1) - (3)$ of the previous section, we now have

$$(\mathfrak{E}^i_R)^{j+1}(X) \subseteq \mathfrak{E}^i_R((\mathfrak{E}^o_R)^j(X)) \subseteq (\mathfrak{E}^o_R)^{j+1}(X) \subseteq \mathfrak{E}^o_R(\mathfrak{F}_R(X)) \subseteq \mathfrak{F}_R(\mathfrak{F}_R(X)).$$

Since $\mathfrak{F}_R(X)$ is an (R, R)-unique factorization extension over itself, we have $\mathfrak{F}_R(\mathfrak{F}_R(X)) = \mathfrak{F}_R(X)$. Thus, the first claim is proved.

The second claim is based on the fact that the base of $\mathfrak{E}^i_R((\mathfrak{E}^i_R)^j(X))$ contains only factors of $(\mathfrak{E}^i_R)^j(X)$. For a finite set X, there exist only finitely many factors, and therefore we must have $(\mathfrak{E}^i_R)^{k+1}(X) = (\mathfrak{E}^i_R)^k(X)$ for some k. But this means that $(\mathfrak{E}^i_R)^k(X)$ is an inner (R, R)-ufe of itself. Thus, it is (R, R)-free. Since $(\mathfrak{E}^i_R)^k(X) \subseteq (\mathfrak{E}^o_R)^k(X) \subseteq \mathfrak{F}_R(X)$, we must have $(\mathfrak{E}^i_R)^k(X) = (\mathfrak{E}^o_R)^k(X) = \mathfrak{F}_R(X)$ by the minimality of the (R, R)-free hull $\mathfrak{F}_R(X)$. ☐

The previous theorem implies that we can use the following iterative procedure for finding the base of the weak R-free hull of X.

Procedure 2 (Free Hull $P_f(X,R)$)**.** Let the input be a finite set $X \subseteq A^+$ and a word relation R on A^+. Set $X_0 = X$, and iterate for $j \geq 0$:

1. Set $X_{j+1} = P_i(X_j, R)$.
2. If $X_j = X_{j+1}$, then stop and return $P_f(X,R) = X_j$.

Thus this procedure is based on iterative calculation of inner (R,R)-hulls. Note that by Theorem 15 we could as well use an algorithm which counts the outer (R,R)-hulls iteratively. Next we will give some examples of these hulls. In the first example the inner (R,R)-hull $\mathfrak{E}^i_R(X)$ is a proper subset of the outer (R,R)-hull of X. More precisely,

$$\mathfrak{E}^i_R(X) \subsetneq \mathfrak{E}^o_R(X) = \mathfrak{F}_R(X).$$

Example 2. Let us consider a set $X = \{a, ac, dd, ddb\} \subseteq \{a,b,c,d\}^+$ and a word relation $R = \langle\{(a,b),(b,c),(c,d)\}\rangle$. It is easy to see that

$$C^i_{R,X}(X) = C^o_{R,X}(X) = \{(dd, ddb)\},$$

because of the relation $dd \cdot a\, R\, ddb$. Other pairs of words in X do not satisfy condition (5). By Procedure 1, we therefore have $X_1 = \{a, ac, b, dd\}$ and furthermore $C^i_{R,X}(X_1) = \emptyset$. Thus, $X_1 = \mathfrak{E}^i_R(X) \setminus \mathfrak{E}^i_R(X)^2$. On the other hand,

$$C^o_{R,X}(X_1) = \{(a, ac), (b, ac)\},$$

since $a \cdot b\, R\, ac\, R\, b \cdot b$. Note that $ac \in X^+$, but ab and bb belong to $X_1^+ \setminus X^+$. By extrinsic (R,R)-stability, we define $X_2 = \{a,b,c,dd\}$. Then $C^o_{R,X}(X_2) = \{(c, dd)\}$ because of $c \cdot c\, R\, dd$ and $dd \in X^+$. Finally we get $X_3 = \{a,b,c,d\}$, which is the base of the weak outer R-hull of X. Moreover, X_3^+ is the weak R-free hull of X.

Next we show that also the outer (R,R)-hull $\mathfrak{E}^o_R(X)$ can be a proper subset of the (R,R)-free hull of X, i.e., $\mathfrak{E}^i_R(X) = \mathfrak{E}^o_R(X) \subsetneq \mathfrak{F}_R(X)$.

Example 3. Consider a set $X = \{eee, fffi, ggi, hh, i\} \subseteq \{e,f,g,h,i\}^+$ with a word relation $R = \langle\{(e,f),(f,g),(g,h)\}\rangle$. Using similar computations as in the previous example, we get sets X_j indicated in Table 1. The relation which effects a split of words in one step of the procedure is called a *split relation.* Words of X_j in relations of the last column are separated by dots. We make some comments about the calculations. First note that the third column is $C^i_{R,X_j}(X_j)$ instead of $C^i_{R,X}(X_j)$. If we consider the first two lines of Table 1, both R-compatible words of the split relation belong to X^+. This is not the case in $fff.gg\, R\, gg.fff$. Actually, we cannot build a split relation such that at least one of the R-compatible words in it belongs to X^+. Thus $C^i_{R,X}(X_2) = C^o_{R,X}(X_2) = \emptyset$ and therefore

$$\mathfrak{E}^i_R(X) \setminus \mathfrak{E}^i_R(X)^2 = \mathfrak{E}^o_R(X) \setminus \mathfrak{E}^o_R(X)^2 = X_2.$$

j	X_j	$C^i_{R,X_j}(X_j)$	split relation
0	$\{eee, fffi, ggi, hh, i\}$	$\{(eee, fffi), (ggi, hh)\}$	$eee.i\,R\,fffi$
1	$\{eee, fff, ggi, hh, i\}$	$\{(ggi, hh)\}$	$ggi\,R\,hh.i$
2	$\{eee, fff, gg, hh, i\}$	$\{(fff, gg)\}$	$fff.gg\,R\,gg.fff$
3	$\{e, ee, f, ff, gg, hh, i\}$	$\{(e, ee), (f, ff), (f, gg)\}$	$e.ee\,R\,ee.e$
4	$\{e, f, gg, hh, i\}$	$\{(f, gg)\}$	$gg.f.f.f\,R\,f.f.f.gg$
5	$\{e, f, g, h, i\}$	$\emptyset$	

Table 1: Calculations for the (R, R)-free hull of Example 3

On the other hand, for $j = 2, 3, 4$ the split relation is over X_2^+. This means that $X_5^+ = \mathfrak{E}^i_R(X_2) = \mathfrak{E}^o_R(X_2)$, since $C^i_{R,X_2}(X_5)$ is clearly empty. Since X_5 is an inner (R, R)-ufe of itself, it is (R, R)-free. Moreover, $(\mathfrak{E}^i_R)^2(X) = X_5^+ = (\mathfrak{E}^i_R)^3(X)$. Thus, by Theorem 15, we have

$$(\mathfrak{E}^i_R)^2(X) = (\mathfrak{E}^o_R)^2(X) = \mathfrak{F}_R(X).$$

We may now combine the previous two examples to verify that it is possible to have

$$\mathfrak{E}^i_R(X) \subsetneq \mathfrak{E}^o_R(X) \subsetneq \mathfrak{F}_R(X).$$

Example 4. Consider a set $X = \{a, ac, dd, ddb, eee, fffi, ggi, hh, i\}$ in a nine letter alphabet and define $R = \langle\{(a, b), (b, c), (c, d), (e, f), (f, g), (g, h)\}\rangle$. Since the alphabets and the relations in Examples 2 and 3 are independent, we may deduce from the previous calculations that

$$\begin{aligned}
\mathfrak{E}^i_R(X) \setminus \mathfrak{E}^i_R(X)^2 &= \{a, ac, b, dd, eee, fff, gg, hh, i\},\\
\mathfrak{E}^o_R(X) \setminus \mathfrak{E}^o_R(X)^2 &= \{a, b, c, d, eee, fff, gg, hh, i\},\\
\mathfrak{F}_R(X) \setminus \mathfrak{F}_R(X)^2 &= \{a, b, c, d, e, f, g, h, i\}.
\end{aligned}$$

Observe that iterating Procedure 1 with input X and R sufficiently many times we do not necessarily get the outer (R, R)-hull of X. More precisely, arbitrary iterations of inner and outer hulls may not be included in each other. Namely, in our example we have

$$(\mathfrak{E}^i_R)^2(X_j) \setminus \mathfrak{E}^o_R(X) \neq \emptyset \quad \text{and} \quad \mathfrak{E}^o_R(X) \setminus (\mathfrak{E}^i_R)^2(X_j) \neq \emptyset,$$

since the base of $(E^i_R)^2(X_j)$ is $\{a, ac, b, dd, e, f, g, h, i\}$. This is due to the fact that $C^i_{R,X_1}(X_2) = \emptyset$ in Example 2.

Finally we note that the presented procedures can be implemented by using generalized Spehner's graphs and automata theory; for Spehner's graphs, see [18].

7 Defect effect

The well know *defect theorem* of words says that if a set of n words satisfies a nontrivial relation, then these words can be expressed simultaneously as products of at most $n-1$ words. This is the so called *defect effect*. It can be formulated also in the following way.

Theorem 16. *Let $X \subseteq A^+$ be a finite set and let B be the base of the free hull of X. Then $|B| \leq |X|$, and the equality holds if and only if X is a code.*

For a short proof of the theorem and more on defect theorems of words, see [15].

We formulate now a defect effect with respect to a word relation R. Note that the original defect theorem does not hold in general and we need a new nontrivial formulation for the defect in the relational case. Let X be a finite subset of A^+. Let us consider a graph $G_R(X) = (V, E)$ defined as follows. The vertices are the words in X, and $(u, v) \in E$ if and only if $u\,R\,v$. We consider the connected components of G. Denote the transitive closure of R by R^+ as above. We note that the set of vertices in the connected component containing x is exactly $(R_X)^+(x)$. Denote the number of connected components of $G_R(X)$ by $c(X, R)$. The cardinalities of the original defect theorem are now replaced by the number of connected components and a defect theorem of inner (R, R)-hulls is given in the following way.

Theorem 17. *Let X be a finite subset of A^+ and let B be the base of the inner (R, R)-hull of X. Then $c(B, R) \leq c(X, R)$, and the equality holds if and only if X is an (R, R)-code.*

Proof. If X is an (R, R)-code, then X^+ is an inner (R, R)-ufe of itself and $B = X$ by Theorem 6. Thus the equality holds trivially. Suppose now that X is not an (R, R)-code. Hence there exist words $x_1, \ldots, x_m, y_1, \ldots, y_n \in X$ such that $x_1 \cdots x_m\,R\,y_1 \cdots y_n$ and, for some $t \in \{1, 2, \ldots, \min\{n, m\}\}$, we have $x_s\,R\,y_s$ for $s = 1, 2, \ldots, t-1$, but $(x_t, y_t) \notin R$. Thus, (x_t, y_t) is a nontrivial inner R-match and $C^i_{R,X}(X) \neq \emptyset$. Hence, $X^+ \neq \mathfrak{C}^i_R(X)$. By Theorem 14, Procedure 1 computes the base of the inner (R, R)-hull of X correctly. Let $k > 0$ be an integer such that X_k is the output of the procedure, i.e., $B = X_k$. We show that $c(X_k, R) < c(X, R)$. For simplicity, in this proof we denote $c_j = c(X_j, R)$. The vertex set of $G_R(X_j)$ is denoted by V_j and the set of edges is denoted by E_j.

First we prove that after each iteration step of the Procedure 1 the number of connected components of $G_R(X_j)$ cannot be greater than the number of the original connected components of $G_R(X)$. In other words,

$$c_j \leq c_0 \tag{7}$$

for any j satisfying $0 \leq j < k$. For this purpose, we divide the set of edges E_j into two parts. An edge (u, v) is called a *light edge* if $(u, v) \in E_j$ is a trivial inner R-match for X_j over X. Otherwise, the edge is called *heavy*. Let us denote the set of vertices in the connected component of X_j containing a vertex u by $C_j(u)$. If there exists a path from u to v using only light edges, we denote $u \to_{L_j} v$. We define also a partition of the vertices of $G_R(X_j)$ into *light components*

$$L_j(u) = \{v \in C_j(u) \mid u \to_{L_j} v\}.$$

Clearly, this is a refinement of the partition of vertices into connected components. We note that $L_j(u)$ coincides with the set $D^i_{R,X}(u, X_j)$ by the definition. Figure 2 illustrates the edges and components of the graph $G_R(X_j)$.

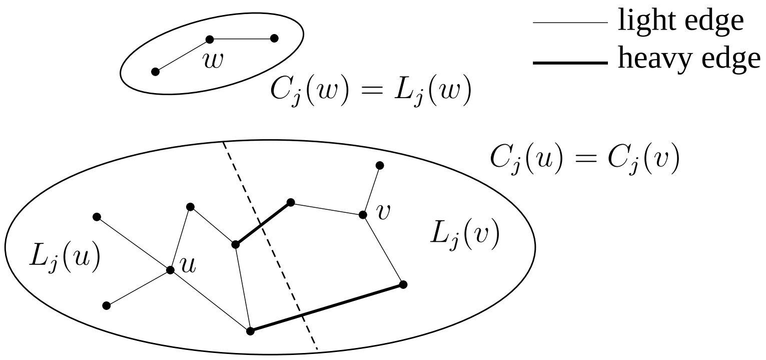

Figure 2: Components of the graph $G_R(X_j)$

We define further that in Procedure 1 a split of u into parts u' and u'' is a *good* split if and only if $L_j(u) = C_j(u)$. Otherwise, the split is called *bad.* Denote the set of connected components of $G_R(X_j)$ by $\mathcal{C}_j$. For a connected component $C \in \mathcal{C}_j$, let $l(C)$ be the number of light components in C, and set

$$l_j = \sum_{C \in \mathcal{C}_j} (l(C) - 1).$$

Instead of inequality (7) we will now prove by induction a stronger result

$$c_j + l_j \leq c_0, \tag{8}$$

where $0 \leq j < k$. Note that inequality (7) follows, since l_j must always be nonnegative by the definition.

Consider first the case $j = 0$. We clearly have $l_0 = 0$. Namely all the R-compatible words u and v of the vertex set V_0 belong to $X_0 = X$ and they form a trivial inner R-match for X_0 over X. Thus, there are no heavy edges in the graph $G_R(X)$ and therefore $l(C) = 1$ for all $C \in \mathcal{C}_0$. Hence, for $j = 0$, inequality (8) holds.

Suppose now that $c_j + l_j \leq c_0$. We will prove that $c_{j+1} + l_{j+1} \leq c_0$. By Procedure 1, we do not delete any edges of a light component except if the whole component is deleted. Hence, light components cannot split into smaller light components. Thus the only way to form connected components with $l(C) > 1$ is to connect disconnected light components to each other using only heavy edges. These heavy edges must appear after some splits. Next we consider all the different cases how this may happen.

Let us first consider good splits. Assume that $(u, v) \in C_i(X_j, R)$ and let $u = u'u''$, where $|u'| = |v|$ and $u'' \in A^+$ as in Procedure 1. When the word u splits, according to Procedure 1, the whole connected component $C_j(u) = L_j(u) = D^i_{R,X}(u, X_j)$ disappears and new vertices $R'(u)$ and $R''(u)$ are born. By the construction, we know that $R'(u) \subseteq C_{j+1}(u')$ and $R''(u) \subseteq C_{j+1}(u'')$. In addition, we have $u' \, R \, v$ and therefore $C_{j+1}(u') = C_{j+1}(v) \supseteq C_j(v) \cup R'(u)$. Thus, the new vertices $R'(u)$ are connected to an old component containing the vertex v. In sum, the components $C_j(u)$ and $C_j(v)$ are changed to components $C_{j+1}(u'')$ and $C_j(v)$. Therefore, the number of connected components cannot increase in a good split, i.e., $c_{j+1} \leq c_j$.

If $l_{j+1} = l_j$, our claim clearly holds. Assume now that $l_{j+1} > l_j$. This means that in the jth iteration step a good split of u induces heavy edges in $G_R(X_{j+1})$ in such a way that the number l_j increases. These edges are of the form (x, w), where either $x \in R'(u)$ or $x \in R''(u)$. Note that in order to increase the number l_j, the connected light components must be distinct, i.e., $w \notin L_{j+1}(x)$. We consider three cases:

$$(i)\ x \in R'(u), w \in C_j(v), \quad (ii)\ x \in R'(u), w \notin C_j(v), \quad (iii)\ x \in R''(u).$$

In the first case, we have $x \in R'(u)$. By Procedure 1, $x \rightarrow_{L_{j+1}} u'$ and $u' \in L_{j+1}(v)$. Thus $x \rightarrow_{L_{j+1}} v$ and $L_{j+1}(x) = L_{j+1}(v)$. Hence, if $w \in L_j(v)$, then $w \in L_{j+1}(x)$, which contradicts with our assumptions. On the other hand, if $L_j(w) \neq L_j(v)$ and $w \in C_j(v)$, this means that $L_j(w)$ is already a light component of $C_j(v)$ and the new heavy edge does not increase the number of light components in the connected component of v. This is impossible, since we assumed that the heavy edge (x, w) induces an increase in l_j.

In the second case, two distinct old components $C_j(v)$ and $C_j(w)$ are connected. Namely, $C_{j+1}(x) = C_{j+1}(u') \supseteq C_j(v)$ and $C_{j+1}(x) \supseteq C_j(w)$. Since $C_j(v) \neq C_j(w)$, we know that the number of connected components c_j is decreased by one whereas the number l_j is increased by one.

In the third case, we may assume that $x \notin R'(u)$. Otherwise, we are in case (i) or in case (ii). Thus the new heavy edge connects some old component $C_j(w)$ to the new component $C_{j+1}(u'') \supseteq L_{j+1}(x)$. Hence, we can make the same conclusion as in the previous case.

Note that in both possible cases (ii) and (iii) there may be more decrease in the number of connected components than it is described above, since also new light edges may appear. However, the number c_j decreases at least as much as the number l_j increases. Therefore, $c_{j+1} + l_{j+1} \leq c_j + l_j \leq c_0$ in a good split. Figure 3 illustrates a good split of u in $G_R(X_j)$.

For bad splits, the situation is more complicated. Suppose that the split of $u \in X_j$ is a bad split. In other words, suppose that $C_j(u)$ is partitioned into $n + 1$

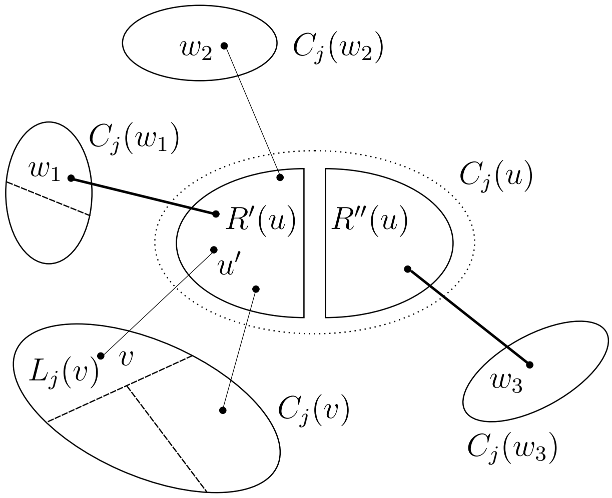

Figure 3: Good split of u in $G_R(X_j)$

light components

$$L_j(u_0), L_j(u_1), \ldots, L_j(u_n),$$

where $u_0 = u$. Now the whole component $C_j(u)$ does not disappear in the jth iteration step, since only the elements of $L_j(u)$ split. Depending on the heavy edges between the light components $L_j(u_1), L_j(u_2), \ldots, L_j(u_n)$, we get m new connected components, where $0 < m \leq n$. We may assume that these components are $C_{j+1}(u_1), C_{j+1}(u_2), \ldots, C_{j+1}(u_m)$. This means that $L_j(u)$ is connected via m heavy edges to light components $L_j(u_1), L_j(u_2), \ldots, L_j(u_m)$ and these light components $L_j(u_i)$ are pairwise disconnected. We have

$$l(C_j(u)) - 1 = n = \sum_{i=1}^{m} l(C_{j+1}(u_i)).$$

This implies that

$$\sum_{i=1}^{m} (l(C_{j+1}(u_i) - 1) = n - m.$$

and we obtain a decrease of size m in l_j. An example of a deletion of a light component $L_j(u)$ is given in Figure 4, where $n = 8$ and $m = 4$

Consider then the number of connected components. Because of the new edge (v, u') the components $C_j(v)$ and $C_j(u)$ are replaced by components $C_{j+1}(u_1)$, $C_{j+1}(u_2), \ldots, C_{j+1}(u_m)$, $C_{j+1}(v) = C_{j+1}(u')$ and $C_{j+1}(u'')$. In addition to the edge (v, u') there may be some other new edges reducing the number of connected components. If the split induces heavy edges which connect two disconnected old components, we have exactly the same cases $(i) - (iii)$ as in a good split. This is based on the fact that if (x, w) is a new heavy edge, then $w \notin \cup_i^m C_{j+1}(u_i)$. The length of words in these components $C_{j+1}(u_i)$ is namely greater than the length

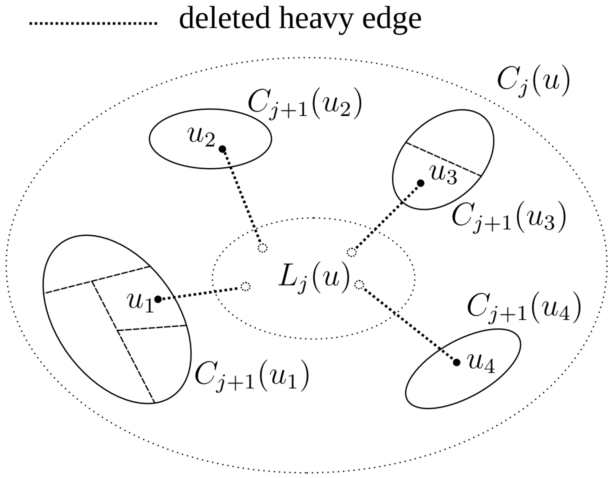

Figure 4: Deletion of $L_j(u)$.

of words in $R'(u)$ and $R''(u)$. Thus increase of size l in l_j induced by these new heavy edges makes a decrease of size l in the number of connected components c_j like in a good split. In other words,

$$c_{j+1} + l_{j+1} \leq (c_j + m - l) + (l_j - m + l) = c_j + l_j \leq c_0$$

and inequality (8) is proved. A bad split is illustrated in Figure 5.

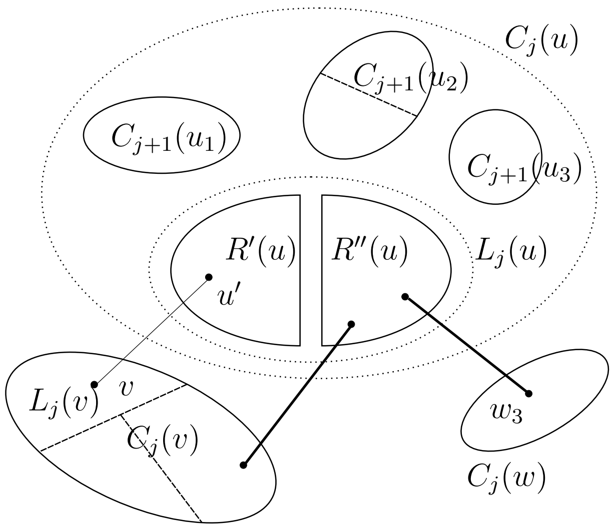

Figure 5: Bad split of u in $G_R(X_j)$.

Now it remains to show that in the last iteration round of the procedure the number of the components strictly decreases and we get $c_k < c_0$. Assume now that in Procedure 1 we choose $(u, v) \in C^i_{R,X}(X_{k-1})$, where $u = u'u''$, $|u'| = |v|$ and

$u'' \in A^+$. More precisely, suppose that there exist $x', x'', y', y'' \in X_{k-1}^*$ such that $x'ux'', y'vy'' \in X^+$, $x'ux'' \, R \, y'vy''$ and $|x'| = |y'|$. Denote $y'' = y_1 \cdots y_n$, where $y_i \in X_{k-1}$ for all $i = 1, 2, \ldots, n$. Suppose also that in addition to components $C_k(u')$ and $C_k(u'')$ there are m new connected components in $G_R(X_k)$. These new components are light components of $C_{k-1}(u)$. Note that $m \leq l_{k-1}$. We consider two cases.

Assume first that $u'' \, R \, y_1$. This means that $C_k(u'') = C_k(y_1)$. Since the new component $C_k(u'')$ is now connected to the old component $C_{k-1}(y_1)$, this causes a decrease by one to the number of connected components. Hence, by inequality (8), we have

$$c_k \leq c_{k-1} + m - 1 \leq c_{k-1} + l_{k-1} - 1 \leq c_0 - 1 < c_0 \tag{9}$$

and we get the desired defect effect.

Suppose next that $(u'', y_1) \notin R$. If $y_1 \notin L_{k-1}(u)$, then y_1 is not split in the final iteration step and $y_1 \in X_k$. Hence, the pair (u'', y_1) is a nontrivial inner R-match for X_k over X by the relation

$$x'u'u''x'' \, R \, y'vy_1 \cdots y_n,$$

where $|x'u| = |y'v|$. Therefore $C^i_{R,X}(X_k) \neq \emptyset$ and X_{j+1} is not the final outcome of the Procedure $P_i(X, R)$; a contradiction.

Thus, we must have $y_1 \in L_{k-1}(u)$. We may denote $y_1 = y_1'y_1''$, where $|y_1'| = |u'|$, $|y_1''| = |u''|$ and $y_1' \in L_k(u')$. If $(u'', y_1') \notin R$, then it is a nontrivial inner R-match for X_k over X by the relation

$$x'u'u''x'' \, R \, y'vy_1'y_1''y_2 \cdots y_n,$$

where $|x'u'| = |y'v|$. This is again impossible, since $C^i_{R,X}(X_k)$ must be empty. Thus $u'' \, R \, y_1'$ and (u'', y_1') is a trivial R-match. Hence,

$$u'' \to_{L_k} y_1' \to_{L_k} u' \to_{L_k} v.$$

Hence besides the new component $C_k(u')$ the component $C_k(u'')$ is connected to the old component $C_{k-1}(v)$, i.e., $C_k(u') = C_k(u'') = C_k(v)$, which causes a reduction in the number of connected components. We conclude that the equation (9) holds. This proves the defect effect for inner (R, R)-hulls. $\square$

As a corollary, we get the defect effect also for the inner (R, S)-hulls.

Corollary 6. *Suppose that $\mathfrak{E}^i_{R,S}(X)$ exists and let B be the base of the inner (R, S)-hull of X. Then $c(B, R) \leq c(X, R)$, and the equality holds if and only if X is an (R, S)-code.*

Proof. This follows from the previous theorem and Theorem 11. Namely, if B is the base of the (R, S)-free hull of X, then it is the base of the (R, R)-free hull and $c(B, R) \leq c(X, R)$. Like above the equality holds if and only if X is an (R, S)-code. $\square$

For the outer (R,S)-hull of X we have the same defect effect. This can be proved by modifying the two previous proofs by replacing inner objects, e.g., $\mathfrak{C}^i_R(X)$, $C^i_{R,X}(X)$ and $D^i_{R,X}(u,X)$ by outer objects, e.g., $\mathfrak{C}^o_R(X)$, $C^o_{R,X}(X)$ and $D^o_{R,X}(u,X)$.

Theorem 18. *Suppose that $\mathfrak{C}^o_{R,S}(X)$ exists and let B be the base of the outer (R,S)-hull of X. Then $c(B,R) \leq c(X,R)$, and the equality holds if and only if X is an (R,S)-code.*

Using Procedure 2 it is easy to see that the defect effect of inner (R,S)-hulls produces a cumulative defect effect for (R,S)-free hulls.

Corollary 7. *Suppose that $\mathfrak{F}_{R,S}(X)$ exists and let B be its base. Let k be the smallest index such that $(\mathfrak{C}^i_R)^{k+1}(X) = (\mathfrak{C}^i_R)^k(X)$. Then*

$$c(B,R) \leq c(X,R) - k.$$

Moreover, $c(B,R) = c(X,R)$ if and only if X is an (R,S)-code.

Proof. Suppose first that X is an (R,S)-code. Then by Theorem 6, X^+ is (R,S)-free and X is its base. Hence, $\mathfrak{F}_{R,S}(X) = X^+$ and the claim $c(B,R) = c(X,R)$ follows trivially. Since X^+ is (R,S)-free, $(\mathfrak{C}^i_R)(X) = X = (\mathfrak{C}^i_R)^0(X)$. Hence, $k = 0$ in this case.

Suppose then that X is not an (R,S)-code. Hence, by Theorem 6 and Theorem 13, $X^+ \neq \mathfrak{F}_{R,S}(X) = \mathfrak{F}_{R,R}(X)$. Thus the smallest k such that $(\mathfrak{C}^i_R)^{k+1}(X) = (\mathfrak{C}^i_R)^k(X)$ must be positive by Theorem 15. Since $\mathfrak{F}_{R,S}(X) = \mathfrak{F}_{R,R}(X)$, we must have $B = \mathfrak{F}_{R,R}(X) \setminus \mathfrak{F}_{R,R}(X)^2$. By our assumption, Procedure 2 stops after $k+1$ iterations. In other words, $P_f(X,R) = (\mathfrak{C}^i_{R,X})^k(X)$. In each of the first k iteration rounds, we have a defect effect by Theorem 17. Therefore $c(B,R) \leq c(X,R) - k$ and $c(B,R) \neq c(X,R)$, since $k > 0$. □

Finally, we consider an application of these defect theorems. Partial words can be seen as a special case of words with word relations. In [14] we proved that the compatibility relation $\uparrow$ of partial words is a word relation over the alphabet $A_\diamondsuit$ such that

$$R_\uparrow = \langle \{(\diamondsuit, a) \mid a \in A\} \rangle.$$

Thus the previous defect theorems imply a defect theorem on partial words; see [12]. Codes on partial words, i.e., *pcodes* were defined in [6]. Naturally, we say that a semigroup on partial words is *pfree* if and only if it is generated by a pcode. The *pfree hull* of a semigroup X of partial words is the smallest pfree semigroup containing X. Using our notation pcodes are $(R_\uparrow, \iota)$-codes over $A_\diamondsuit$ and pfree semigroups are $(R_\uparrow, \iota)$-free. The pfree hull of X is the $(R_\uparrow, \iota)$-free hull of X. Now we state:

Corollary 8. *Let X be a finite set of partial words, i.e., a set of words over the alphabet $A_\diamondsuit$. Suppose that the pfree hull of X exists and let B be its base. Then $|B| \leq |X|$, and the equality holds if and only if X is a pcode.*

Proof. As mentioned above the pfree hull is the $(R_\uparrow, \iota)$-free hull of X. Thus, by Corollary 7, we have $c(B, R_\uparrow) \leq c(X, R_\uparrow)$ and the equality holds if and only if X is an $(R_\uparrow, \iota)$-code. Since $\mathfrak{S} = B^+$ is an $(R_\uparrow, \iota)$-free semigroup, we have $(R_\uparrow)_\mathfrak{S} \subseteq \iota_\mathfrak{S}$. This means that all the connected components of $G_R(B)$ and $G_R(X)$ must consist of single elements. Thus $c(B, R_\uparrow) = |B|$ and $c(X, R_\uparrow) = |X|$. This implies our statement. $\square$

Of course, all the defect theorems on words with word relations could also be formulated for partial words. For example, we could get a cumulative defect effect by using inner $(R_\uparrow, \iota)$-hulls and the procedure $P_f(X, R_\uparrow)$.

References

[1] J. Berstel, L. Boasson, Partial words and a theorem of Fine and Wilf. Theoret. Comput. Sci. 218, 135–141, 1999.

[2] J. Berstel, D. Perrin, Theory of Codes. Academic press, New York, 1985.

[3] J. Berstel, D. Perrin, J.F. Perrot and A. Restivo, Sur le théorème du défaut. J. Algebra 60, 169–180, 1979.

[4] F. Blanchet-Sadri, A Periodicity Result of Partial Words with One Hole. Comput. Math. Appl. 46, 813–820, 2003.

[5] F. Blanchet-Sadri, Periodicity on partial words. Comput. Math. Appl. 47, 71–82, 2004.

[6] F. Blanchet-Sadri, Codes, orderings, and partial words. Theoret. Comput. Sci. 329, 177–202, 2004.

[7] F. Blanchet-Sadri, Primitive Partial Words. Discrete Appl. Math. 148, 195–213, 2005.

[8] F. Blanchet-Sadri, A. Chriscoe, Local periods and binary partial words: an algorithm. Theoret. Comput. Sci. 314, 189–216, 2004.

[9] F. Blanchet-Sadri, S. Duncan, Partial words and the critical factorization theorem. J. Combin. Theory, Ser. A 109, 221–245, 2005.

[10] F. Blanchet-Sadri, R.A. Hegstrom, Partial words and a theorem of Fine and Wilf revisited. Theoret. Comput. Sci. 270, 401–419, 2002.

[11] F. Blanchet-Sadri, D.K. Luhmann, Conjugacy on partial words. Theoret. Comput. Sci. 289, 297–312, 2002.

[12] F. Blanchet-Sadri, M. Moorefield, Pcodes of partial words. Manuscript, 2005.

[13] A. Ehrenfeucht, G. Rozenberg, Elementary homomorphisms and a solution of the D0L sequence equivalence problem. Theoret. Comput. Sci 7, 169–183, 1978.

[14] V. Halava, T. Harju and T. Kärki, Relational codes of words, TUCS Tech. Rep. 767, Turku Centre for Computer Science, Finland, 1–16, April 2006.

[15] T. Harju and J. Karhumäki, Many aspects of Defect Theorems. Theor. Comput. Sci. 324, 35–54, 2004.

[16] P. Leupold, Partial words for DNA coding. Lecture Notes in Comput. Sci. 3384, 224–234, 2005.

[17] M. Linna, On the decidability of the D0L prefix problem. Internat. J. Comput. Math. A6, 127-142, 1977.

[18] J.C. Spehner, Présentation et présentations simplifiables d'un monoïd simplifiable. Semigroup Forum 14, 295–329, 1977.

[19] B. Tilson, The intersection of free submonoids of free monoids is free. Semigroup forum 4, 345–350, 1972.

Turku Centre *for* Computer Science

Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
- Institute of Information Systems Sciences

ISBN 952-12-1763-4
ISSN 1239-1891