3. Reduction relations

This material is taken from the book

> F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer-Verlag Wien New York, 1996.

Many of the properties that are important for Gröbner bases can be developed in the frame of binary relations on arbitrary sets, so-called reduction relations (compare G. Huet,"Confluent reductions: abstract properties and applications to term rewriting systems", *J.ACM* 27, pp. 797–821, 1980). The theory of reduction relations forms a common basis for the theory of Gröbner bases, word problems in finitely presented groups, term rewriting systems, and lambda calculus.

Definition 3.1. Let M be a set and $\longrightarrow$ a binary relation on M, i.e. $\longrightarrow \subseteq M \times M$. We call $\longrightarrow$ a *reduction relation* on M. Instead of $(a,b) \in \longrightarrow$ we usually write $a \longrightarrow b$ and say that *a reduces to b*.
Given reduction relations $\longrightarrow$ and $\longrightarrow'$ on M, we define operations on $M \times M$ for constructing new reduction relations.

- $\longrightarrow \circ \longrightarrow'$ (or just $\longrightarrow\longrightarrow'$), the *composition* of $\longrightarrow$ and $\longrightarrow'$, is the reduction relation defined as $a \longrightarrow\longrightarrow' b$ iff there exists a $c \in M$ such that $a \longrightarrow c \longrightarrow' b$;
- $\longrightarrow^{-1}$ (or just $\longleftarrow$), the *inverse relation* of $\longrightarrow$, is the reduction relation defined as $a \longleftarrow b$ iff $b \longrightarrow a$;
- $\longrightarrow_{\mathrm{sym}}$ (or just $\longleftrightarrow$), the *symmetric closure* of $\longrightarrow$, is the reduction relation defined as $\longrightarrow \cup \longleftarrow$, i.e. $a \longleftrightarrow b$ iff $a \longrightarrow b$ or $a \longleftarrow b$;
- $\longrightarrow^i$, the *i-th power* of $\longrightarrow$, is the reduction relation defined inductively for $i \in \mathbb{N}_0$ as
  $\longrightarrow^0 :=$ id (identity relation on M), i.e $a \longrightarrow^0 b$ iff $a = b$, and
  $\longrightarrow^i := \longrightarrow\longrightarrow^{i-1}$ for $i \geq 1$.
  So $a \longrightarrow^i b$ if and only if there exist $c_0, \ldots, c_i$ such that $a = c_0 \longrightarrow c_1 \longrightarrow \ldots \longrightarrow c_i = b$. In this case we say that *a reduces to b in i steps*;
- $\longrightarrow^+ := \bigcup_{i=1}^{\infty} \longrightarrow^i$, the *transitive closure* of $\longrightarrow$;
- $\longrightarrow^* := \bigcup_{i=0}^{\infty} \longrightarrow^i$, the *reflexive–transitive closure* of $\longrightarrow$;
- $\longleftrightarrow^*$ is the *reflexive–transitive–symmetric closure* of $\longrightarrow$. □

In the sequel we will always assume that the set M is recursively enumerable and the reduction relation $\longrightarrow$ is recursive, i.e. for given $x, y \in M$ we can decide whether $x \longrightarrow y$.

$\longleftrightarrow^*$ is an equivalence relation on M and $M_{/\longleftrightarrow^*}$ is the set of equivalence classes modulo $\longleftrightarrow^*$. One of the main problems in connection with reduction relations is to decide $\longleftrightarrow^*$, i.e. to determine for $a, b \in M$ whether $a \longleftrightarrow^* b$; or, in other words, whether a and b belong to the same equivalence class. We call this problem the *equivalence problem* for the reduction relation $\longrightarrow$.

Example 3.1. (a) One well known version of the equivalence problem is the word problem for groups. A *free presentation* of a group is a set X of *generators* together with a set R of words (strings) in the generators, called *relators*. Words are formed by concatenating symbols x or x^{-1} for $x \in X$. Such a presentation is usually written as $\langle X|R\rangle$ and it denotes the group $F(X)$ modulo $\langle R\rangle$, $F(X)_{/\langle R\rangle}$, where $F(X)$ is the free group generated by X and

$\langle R \rangle$ is the smallest normal subgroup of $F(X)$ which contains R. In more concrete terms, we think of $\langle X|R \rangle$ as the group obtained from $F(X)$ by forcing all words in R to be equal to the identity together with all consequences of these equations.

For example, consider the group

$$G = \langle\ \{a, b\} \mid \{a^2, b^2, aba^{-1}b^{-1}\}\ \rangle.$$

The first relator tells us that we can replace a^m by 1 if m is even and by a if m is odd. Similarly for powers of b. The third relator tells us that a and b commute so that we can collect all powers of a and then all powers of b in a word. Thus, every element of G is equal to one of

$$1, a, b, ab$$

and it can be shown that these are distinct.

The *word problem for freely presented groups* is:
given: a presentation $\langle X|R \rangle$ and words $u, v \in F(X)$,
decide: $u \stackrel{?}{=} v$ in $\langle X|R \rangle$.

Actually this definition looks as though the problem were about the presentation of the group rather than the group itself. But, in fact, if we insist that the presentations considered must be effectively given, i.e. both X and R are recursively enumerable, then the decidability is independent of the presentation. It is not very hard to show that the problem is undecidable in general. It is much harder to show that the same is true even if we consider only finite presentations, i.e. both X and R are finite sets.

(b) Another example is from polynomial ideal theory and it will lead us to the introduction of Gröbner bases. Consider the polynomial ring $K[x_1, \ldots, x_n]$, K a field, and let $I = \langle p_1, \ldots, p_m \rangle$ be the ideal generated by $p_1, \ldots, p_m$ in $K[x_1, \ldots, x_n]$. The *main problem in polynomial ideal theory* according to van der Waerden is:
given: generators $p_1, \ldots, p_m$ for an ideal I in $K[x_1, \ldots, x_n]$, and
polynomials $f, g \in K[x_1, \ldots, x_n]$,
decide: whether $f \equiv g \pmod{I}$, or equivalently, whether f and g represent the same element of the factor ring $K[x_1, \ldots, x_n]_{/I}$.
Later we will introduce a reduction relation $\longrightarrow$ such that $\longleftrightarrow^* = \equiv_I$, so again the problem is to decide the equivalence problem of a reduction relation. □

Let us introduce some more useful notations for abbreviating our arguments about reduction relations.

Definition 3.2.

- $x \longrightarrow$ means x is *reducible*, i.e. $x \longrightarrow y$ for some y;
- $\underline{x}\!\!\not\longrightarrow$ means x is *irreducible* or *in normal form* w.r.t. $\longrightarrow$. We omit mentioning the reduction relation if it is clear from the context;
- $x \downarrow y$ means that x and y have a *common successor*, i.e. $x \longrightarrow z \longleftarrow y$ for some z;
- $x \uparrow y$ means that x and y have a *common predecessor*, i.e. $x \longleftarrow z \longrightarrow y$ for some z;
- *x is a $\longrightarrow$–normal form* of y iff $y \longrightarrow^* \underline{x}$. □

In the sequel we will always assume that we can decide whether $x \in M$ is reducible and if so compute a y such that $x \longrightarrow y$. Based on these assumptions about the decidability of the reduction relation we will establish that the equivalence problem for $\longrightarrow$ can be decided

if $\longrightarrow$ has two basic properties, namely the Church–Rosser property and the termination property.

Definition 3.3. (a) $\longrightarrow$ is *Noetherian* or has the *termination property* iff every reduction sequence terminates, i.e. there is no infinite sequence $x_1, x_2, \ldots$ in M such that $x_1 \longrightarrow x_2 \longrightarrow \ldots$.
(b) $\longrightarrow$ is *Church–Rosser* or has the *Church–Rosser property* iff $a \longleftrightarrow^* b$ implies $a \downarrow_* b$. □

Whenever a set M is equipped with a Noetherian relation $\longrightarrow$ we can apply the *principle of Noetherian induction* for proving that a predicate P holds for all $x \in M$:

if for all $x \in M$
  [for all $y \in M$*:* $(x \longrightarrow y) \Longrightarrow P(y)] \Longrightarrow P(x)$
then
  for all $x \in M$*:* $P(x)$.

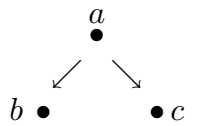
A correctness proof of this principle can be found in P.M. Cohn, *Algebra*, Wiley, New York, 1974.

Theorem 3.1. Let $\longrightarrow$ be Noetherian and Church–Rosser. Then the equivalence problem for $\longrightarrow$ is decidable.

Proof: Let $x, y \in M$. Let $\tilde{x}, \tilde{y}$ be normal forms of x, y, respectively (by Noetherianity every sequence of reductions leads to a normal form after finitely many steps). Obviously $x \longleftrightarrow^* y$ if and only if $\tilde{x} \longleftrightarrow^* \tilde{y}$. By the Church–Rosser property $\tilde{x} \longleftrightarrow^* \tilde{y}$ if and only if $\tilde{x} \downarrow_* \tilde{y}$. Since $\tilde{x}$ and $\tilde{y}$ are irreducible, $\tilde{x} \downarrow_* \tilde{y}$ if and only if $\tilde{x} = \tilde{y}$.
Summarizing we have $x \longleftrightarrow^* y$ if and only if $\tilde{x} = \tilde{y}$. □

Theorem 3.1 cannot be reversed, i.e. the equivalence problem for $\longrightarrow$ could be decidable although $\longrightarrow$ is not Noetherian or $\longrightarrow$ is not Church–Rosser.

Example 3.2. (a) Let $M = \mathbb{N}$ and $\longrightarrow = \{(n, n+1) | n \in \mathbb{N}\}$. Obviously the equivalence problem for $\longrightarrow$ is decidable, but $\longrightarrow$ is not Noetherian.
(b) Let $M = \{a, b, c\}$ and $\longrightarrow = \{(a, b), (a, c)\}$. So



Obviously the equivalence problem for $\longrightarrow$ is decidable, but $\longrightarrow$ is not Church–Rosser. □

So if $\longrightarrow$ is Noetherian and Church–Rosser then we have a *canonical simplifier* for $M_{/\longleftrightarrow^*}$, i.e. a function which for every equivalence class computes a unique representative in that equivalence class. For $x \in M$ any normal form of x can be taken as the simplified form of x, since all these normal forms are equal.

Example 3.3. (a) Let H be the commutative semigroup generated by a, b, c, f, s modulo the relations

$$as = c^2 s, \ bs = cs, \ s = f. \qquad (E)$$

Consider the reduction relation $\longrightarrow$ given by

$$s \longrightarrow f,\ cf \longrightarrow bf,\ b^2 f \longrightarrow af$$

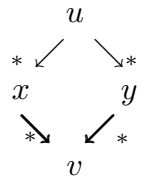
and if $u \longrightarrow v$ then $ut \longrightarrow vt$ for all words u, v, t.
$\longrightarrow$ is Church–Rosser and Noetherian and $\longleftrightarrow^* = =_{(E)}$. So, for example, we can discover that $a^3bcf^3 =_{(E)} a^2b^4fs^2$ by computing the normal forms of both words, which turn out to be equal.
(b) Let I be the ideal in $\mathbb{Q}[x, y]$ generated by

$$x^3 - x^2,\ x^2y - x^2.$$

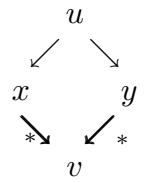
Let $\longrightarrow$ be defined on $\mathbb{Q}[x, y]$ in such a way that every occurrence of x^3 or x^2y can be replaced by x^2. Then $\longrightarrow$ is Church–Rosser and Noetherian. Thus, we can decide whether $f \equiv g \pmod I$ for arbitrary $f, g \in \mathbb{Q}[x, y]$, i.e. we can compute in $\mathbb{Q}[x, y]_{/I}$. □

Checking whether the Church–Rosser property and the Noetherian property are satisfied for a given reduction relation is not an easy task. Fortunately, in the situation of polynomial ideals Noetherianity is always satisfied as we will see later. Our goal now is to reduce the problem of checking the Church–Rosser property to checking simpler properties.

Definition 3.4. (a) $\longrightarrow$ is *confluent* iff $x \uparrow^* y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:



(b) $\longrightarrow$ is *locally confluent* iff $x \uparrow y$ implies $x \downarrow_* y$, or graphically every diamond of the following form can be completed:

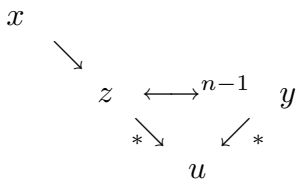


□

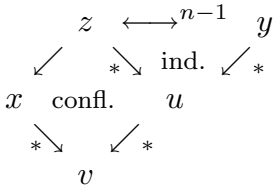
Theorem 3.2. (a) $\longrightarrow$ is Church–Rosser if and only if $\longrightarrow$ is confluent.
(b) (Newman Lemma) Let $\longrightarrow$ be Noetherian. Then $\longrightarrow$ is confluent if and only if $\longrightarrow$ is locally confluent.

Proof: (a) If $\longrightarrow$ is Church–Rosser then it is obviously confluent. So let us assume that $\longrightarrow$ is confluent. Suppose that $x \longleftrightarrow^* y$ in n steps, i.e. $x \longleftrightarrow^n y$. We use induction on n. The case $n = 0$ is immediate. For $n > 0$ there are two possible situations:

for some z. In the first case by the induction hypothesis there is a u such that



and in the second case by the induction hypothesis and by confluence there are u, v such that



In either case $x \downarrow_* y$.

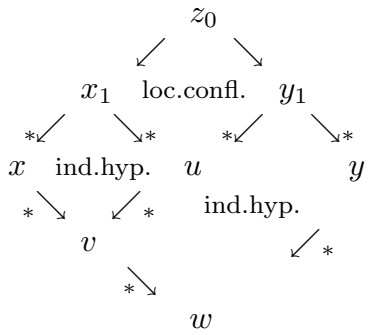
(b) Confluence obviously implies local confluence. So assume that $\longrightarrow$ is locally confluent. We use Noetherian induction on the Noetherian ordering $\longrightarrow$. The induction hypothesis is

"for all z with $z_0 \longrightarrow z$ and for all x', y' with $x' \longleftarrow^* z \longrightarrow^* y'$ we have $x' \downarrow_* y'$."

Now assume that $x \longleftarrow^* z_0 \longrightarrow^* y$. The cases $x = z_0, y = z_0$ are obvious. So consider

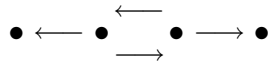
$$x \longleftarrow^* x_1 \longleftarrow z_0 \longrightarrow y_1 \longrightarrow^* y.$$

By local confluence and the induction hypothesis there are u, v, w such that



So $x \downarrow_* y$. □

If we drop the requirement of Noetherianity in Theorem 3.2(b) then the statement does not hold any more, as can be seen from the counterexample



Definition 3.5. Let $\longrightarrow$ be a reduction relation on the set M and $>$ a partial ordering on M. Let $x, y, z \in M$. x and y are *connected (w.r.t. $\longrightarrow$) below (w.r.t. $>$) z* iff there are $w_1, \ldots, w_n \in M$ such that $x = w_1 \longleftrightarrow \ldots \longleftrightarrow w_n = y$ and $w_i < z$ for all $1 \leq i \leq n$. We use the notation $x \longleftrightarrow^*_{(<z)} y$. □

Theorem 3.3. (Refined Newman Lemma) *Let $\longrightarrow$ be a reduction relation on M and $>$ a partial Noetherian ordering on M such that $\longrightarrow \subseteq >$. Then $\longrightarrow$ is confluent if and only if for all x, y, z in M:*

$$x \longleftarrow z \longrightarrow y \quad \textit{implies} \quad x \longleftrightarrow^*_{(<z)} y.$$

Proof: Confluence obviously implies connectedness. So now let us assume that the connectedness property holds. We use Noetherian induction on $>$ with the induction hypothesis

$$\text{for all } \tilde{x}, \tilde{y}, \tilde{z}\text{: if } \tilde{z} < z \text{ and } \tilde{x} \longleftarrow^* \tilde{z} \longrightarrow^* \tilde{y} \text{ then } \tilde{x} \downarrow_* \tilde{y}. \qquad \text{(IH 1)}$$

Now consider the situation $x \longleftarrow^* z \longrightarrow^* y$. If $x = z$ or $y = z$ then we are done. Otherwise we have

$$x \longleftarrow^* x_1 \longleftarrow z \longrightarrow y_1 \longrightarrow^* y.$$

By the assumption of connectedness there are $u_1, \ldots, u_n < z$ such that

$$x_1 = u_1 \longleftrightarrow \ldots \longleftrightarrow u_n = y_1.$$

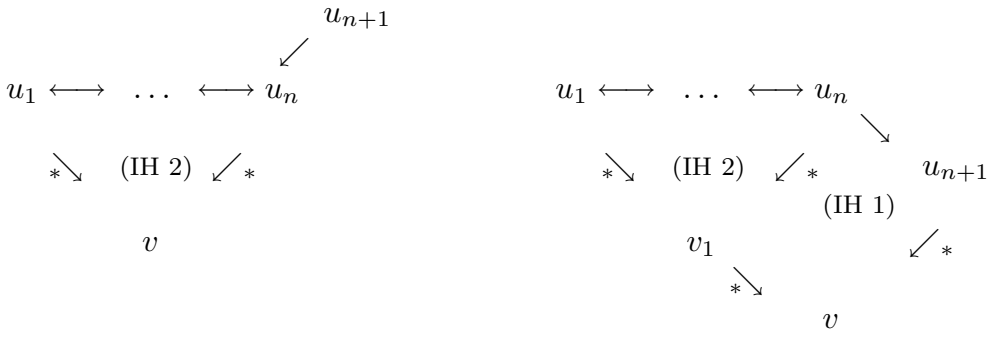
We use induction on n to show that for all n and all $u_1, \ldots, u_n \in M$:

$$\text{if } u_1 \longleftrightarrow \ldots \longleftrightarrow u_n \text{ and } u_i < z \text{ for all } 1 \leq i \leq n, \text{ then } u_1 \downarrow_* u_n. \qquad (3.1)$$

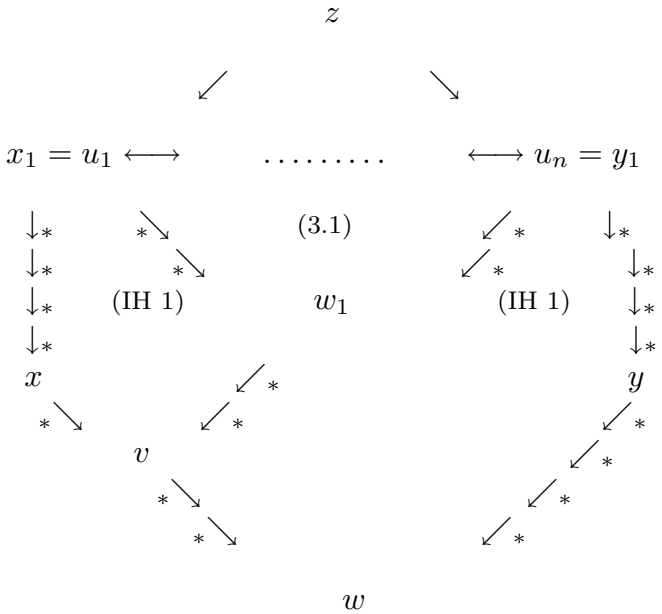
The case $n = 1$ is clear. So we formulate induction hypothesis 2:

$$(3.1) \text{ holds for some fixed } n. \qquad \text{(IH 2)}$$

For the induction step let $u_1, \ldots, u_{n+1} \in M$ such that $u_i < z$ for $1 \leq i \leq n+1$ and $u_1 \longleftrightarrow \ldots \longleftrightarrow u_{n+1}$. We distinguish two cases in which the existence of a common successor v to u_1 and u_{n+1} can be shown by the following diagrams:



This proves (3.1). The proof of the theorem can now be completed by the diagram



□

Exercises

3.1. If the reduction relation $\longrightarrow$ on the set M is Noetherian, does that mean that $R(x) = \{y \mid x \longrightarrow y\}$ is finite for every x?

3.2. Give another example of a locally confluent reduction relation which is not confluent.