

# Canonical Reduction Systems in Symbolic Mathematics

Franz Winkler

RISC

Research Institute for Symbolic Computation  
Johannes Kepler University Linz, Austria

# 1. Introduction

The biological theory of evolution knows many instances of similar solutions having been developed for similar problem; examples are the wings of insects, birds, and bats, or the different realizations of light sensitive organs such as eyes.

The same phenomenon can be observed in the development of the sciences, and also in particular in mathematics.

Many algorithmic methods in different fields of mathematics, e.g. linear algebra, commutative algebra, or logic, can be seen as constructing canonical systems for deciding membership problems. Important examples are

Gauss' elimination method for linear systems,

Euclid's algorithm for computing GCDs,

Buchberger's algorithm for constructing Gröbner bases,

the Knuth-Bendix procedure for equational theories.

Here we explain the basic concept of a canonical systems and investigate the close connections between these algorithms.

Canonical reduction systems are supposed to solve the following kind of problem:

- we are given a mathematical structure  $\mathcal{S}$  and a congruence relation  $\cong$  on  $\mathcal{S}$ , (i.e.  $\cong \subseteq \mathcal{S}^2$ ) given by a finite set of generators  $G$  (i.e.  $\cong = \cong_G$ )
- for any given  $s, t \in \mathcal{S}$ , we want to decide whether  $s \cong_G t$
- this should be achieved by a general algorithm depending only on  $\mathcal{S}$ , and **not** on the particular congruence  $\cong_G$  or its set of generators  $G$

In order to solve such decision problems we introduce a reduction relation

$$\longrightarrow_G \subseteq \mathcal{S} \times \mathcal{S}$$

with the properties

- $\longrightarrow_G$  is terminating or Noetherian, i.e. every reduction chain is finite
- $\cong_G = \longleftarrow_G^*$ , i.e. the symmetric reflexive transitive closure of  $\longrightarrow_G$  is equal to the congruence generated by  $G$

if in addition to being Noetherian the reduction relation is also Church-Rosser, then we can solve our initial problem systematically

the reduction relation  $\longrightarrow_G$  is Church-Rosser iff connectednes w.r.t. " $\longleftarrow_G$ ", i.e.

$$a \longleftarrow_G^* b ,$$

implies the existence of a common successor, i.e.

$$\exists c : a \longrightarrow_G^* c \text{ and } b \longrightarrow_G^* c .$$

in particular this means that two irreducible elements  $a, b$  are congruent if and only if they are syntactically equal.

in order to decide whether

$$a \cong_G b$$

under the conditions of Noetherianity and Church-Rosserness of  $\longrightarrow_G$  we do the following:

- reduce  $a$  and  $b$  to (any) irreducible  $a'$  and  $b'$  s.t.

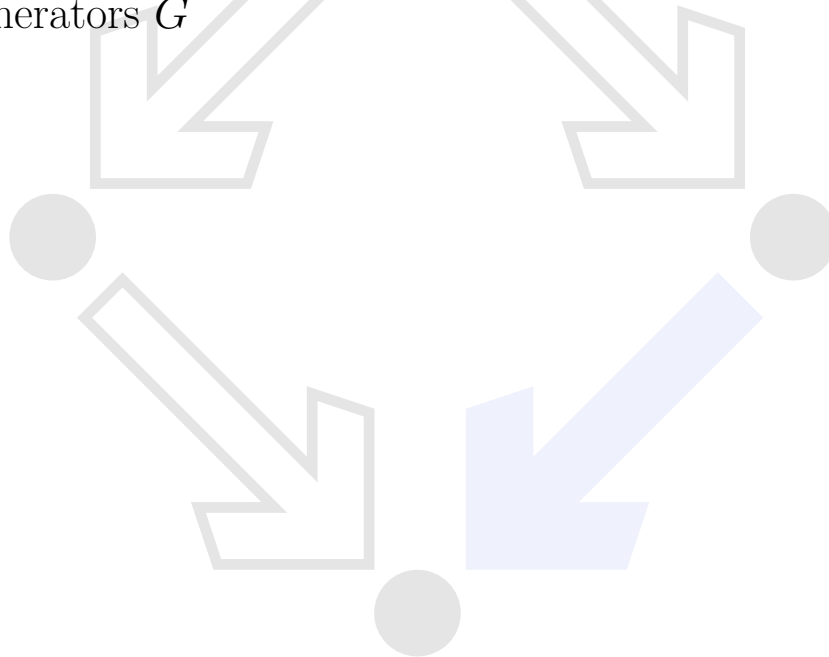
$$\begin{aligned} a &= a_0 \longrightarrow_G a_1 \longrightarrow_G \cdots \longrightarrow_G a_m = a', \\ b &= b_0 \longrightarrow_G b_1 \longrightarrow_G \cdots \longrightarrow_G b_n = b' \end{aligned}$$

observe that because of Noetherianity these reduction chains have to be finite

- check whether  $a' = b'$ ;  
if so  $a \cong_G b$ , otherwise not

but of course in general our set of generators  $G$  will not have this nice Church-Rosser property

the goal now is to transform  $G$  into an equivalent set of generators  $\hat{G}$





## 2. Gauss Elimination

the setting:

- vector space  $V = K^n$  over field  $K$
- generating elements  $B$  for a subvector space  $W = \text{span}(B)$
- equivalence relation  $v \cong_W w \iff v - w \in W$

the problem:

- for  $v \in V$
- decide: “ $v \cong_W 0$ ”, i.e. “ $v \in \text{span}(B) = W$ ” ?

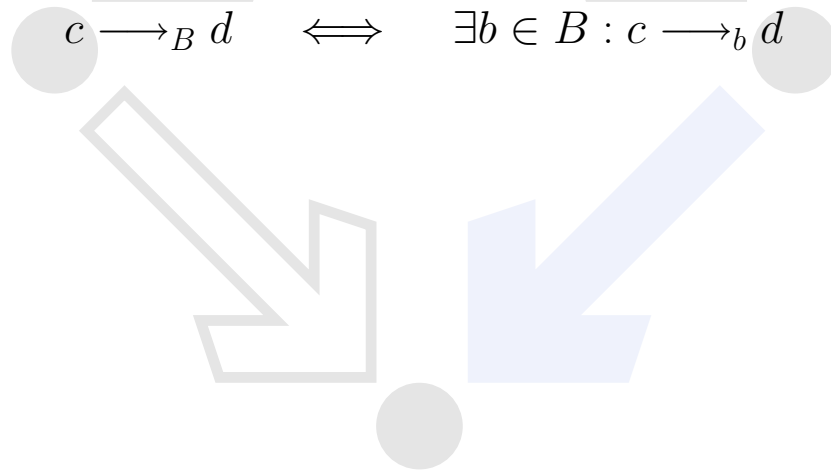
define a reduction relation  $\longrightarrow_B$ :

for vector  $b = (0, \dots, 0, b_i, \dots, b_n)$  with  $b_i \neq 0$  we say  $\text{lead}(b) = i$ ;

$$c = (c_1, \dots, c_i \neq 0, \dots, c_n) \longrightarrow_b c - \frac{c_i}{b_i} \cdot b$$

and

$$c \longrightarrow_B d \iff \exists b \in B : c \longrightarrow_b d$$



clearly  $\longrightarrow_B$  has the following properties:

- $\longrightarrow_B$  is terminating
- if  $c \longrightarrow_B d$  then  $c - d \in \text{span}(B) = W$

but  $\longrightarrow_B$  in general is **not** Church-Rosser:

let

$$B = \{\underbrace{(1, 0, 0)}_{b_1}, \underbrace{(1, 1, 1)}_{b_2}\}$$

then

$$\begin{aligned} (1, 2, 2) &\longrightarrow_{b_1} (0, 2, 2) \\ (1, 2, 2) &\longrightarrow_{b_2} (0, 1, 1) \end{aligned}$$

both results are irreducible,

they are congruent,

but they have no common successor

So what do we do in order to create a situation where we have a CR reduction system?

Well, we transform the Matrix

$$B = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix}$$

to row echelon form; i.e. we look at situations, where the component of a vector, or for this matter a unit vector

$$e_i = (0, \dots, 0, \underbrace{1}_{i\text{-th pos}}, 0, \dots, 0) ,$$

can be reduced by 2 different generators  $b_j$  and  $b_k$

$$\text{lead}(b_j) = i = \text{lead}(b_k) .$$

$$\begin{array}{ccc} & e_i & \\ \downarrow & & \downarrow \\ e_i - b_j & & e_i - b_k \end{array}$$

These reduction results are congruent w.r.t.  $\cong_W$ , so their difference  $b_{m+1} := b_j - b_k$  is in  $W$ ; if  $b_{m+1} = 0$ , then there was no divergence anyway; otherwise we add  $b_{m+1}$  to the set of generators  $B$ , thereby enforcing this particular divergence of reduction to converge:

$$\begin{array}{l} \text{either} \quad e_i - b_j \xrightarrow{b_{m+1}} e_i - b_k \\ \text{or} \quad \quad e_i - b_k \xrightarrow{b_{m+1}} e_i - b_j \end{array}$$

observe that this represents exactly a step in the formation of the row echelon form of the matrix  $B$

this process terminates and yields a set of generators  $\hat{B}$   
s.t.

- $\longleftrightarrow_B^* = \cong_W = \longleftrightarrow_{\hat{B}}^*$
- $\longrightarrow_{\hat{B}}$  is both Noetherian and CR

So we can decide the membership problem for  $W$  by reduction w.r.t.  $\hat{B}$

if in the end we interreduce the elements in  $\hat{B}$ , we basically get the Hermite matrix associated to  $B$

for our example above this means the following:

$$\begin{array}{rcl} B \rightarrow & b_1 = & (1, 0, 0) \\ & b_2 = & (1, 1, 1) \\ & \text{---} & \text{---} \\ & b_3 = & (0, 1, 1) \end{array} \rightarrow \hat{B}$$

now  $\hat{B}$  spans the same vector space  $W$ , and we can use the reduction w.r.t.  $\hat{B}$  to decide membership in  $W$ :

$$\begin{array}{rcl} (1, 2, 2) & \xrightarrow{b_1} & (0, 2, 2) & \xrightarrow{b_3} & (0, 0, 0) \\ & \xrightarrow{b_2} & (0, 1, 1) & \xrightarrow{b_3} & (0, 0, 0) \end{array}$$

So  $(1, 2, 2) \in W$ .

### 3. Euclid's algorithm for GCDs

the setting:

- $K[x]$ , the ring of polynomials over a field  $K$
- $F = \{f_1(x), f_2(x)\} \subset K[x]$   
generating an ideal  $I = \langle F \rangle$  in  $K[x]$
- equivalence relation  $g \equiv_I h \iff g - h \in I$

the problem:

- for  $g \in K[x]$
- decide: “ $g \equiv_i 0$ ”, i.e. “ $g \in \langle F \rangle = I$ ” ?



define a reduction relation  $\longrightarrow_F$ :

for polynomial  $f(x) = f_n x^n + \cdots + f_1 x + f_0$  with  $f_n \neq 0$

we say  $\text{lead}(f) = \text{deg}(f) = n$ ;

$$c(x) = c_m x^m + \cdots + \underbrace{c_i}_{\neq 0} x^i + \cdots + c_0$$

$\longrightarrow_f$

$$c(x) - \frac{c_i}{f_n} x^{i-n} f(x), \quad \text{if } i \geq n$$

and

$$c \longrightarrow_F d \iff \exists f \in F : c \longrightarrow_f d$$

clearly  $\longrightarrow_F$  has the following properties:

- $\longrightarrow_F$  is terminating
- if  $c \longrightarrow_F d$  then  $c - d \in \langle F \rangle = I$

but  $\longrightarrow_F$  in general is **not** Church-Rosser:

let

$$F = \left\{ \underbrace{x^5 + x^4 + x^3 - x^2 - x - 1}_{f_1}, \underbrace{x^4 + x^2 + 1}_{f_2} \right\}$$

then

$$\begin{array}{l} x^5 - x^2 \xrightarrow{f_1} -x^4 - x^3 + x + 1 \xrightarrow{f_2} -x^3 + x^2 + x + 2 \\ x^5 - x^2 \xrightarrow{f_2} -x^3 - x^2 - x \end{array}$$

both results are irreducible,

they are congruent,

but they have no common successor

So what do we make the reduction CR? Well, we consider (smallest) situations in which a term  $x^i$  can be reduced by two different polynomials; i.e. we compute a remainder sequence starting with  $f_1, f_2$ :

$$\begin{array}{r}
 F = \begin{array}{l} f_1 \\ f_2 \\ \hline \end{array} \\
 f_3 \quad := \text{rem}(f_1, f_2) \\
 \vdots \\
 f_k \quad (\neq 0) \\
 f_{k+1} \quad (= 0) \quad \hat{F} = \{f_1, f_2, \dots, f_k\}
 \end{array}$$

then  $f_k$  will be the greatest common divisor (gcd) of  $f_1$  and  $f_2$ , and

$$g \in \langle F \rangle \iff f_k | h \iff h \xrightarrow{\hat{F}} 0$$

in terms of the algorithmic scheme of reduction and completion we can view this process in the following way:

- we look at terms  $x^i$  which can be reduced w.r.t. two different generators  $f_j, f_k$
- this means that  $i \geq \deg(f_j), \deg(f_k)$
- the smallest such situation occurs when  $i = \max(\deg(f_j), \deg(f_k))$ , and all the other cases are instantiations of such basic situations

(assuming w.l.o.g. leading coefficients to be 1)

$$x^i = \max(\text{lead}(f_j), \text{lead}(f_k))$$

$$\begin{array}{ccc} & \downarrow & \downarrow \\ x^i - f_j & & x^i - f_k \end{array}$$

These reduction results are congruent w.r.t.  $\equiv_I$ , so their difference  $f_{m+1} := f_j - f_k$  is in  $I$ ; if  $f_{m+1} = 0$ , then there was no divergence anyway; otherwise we add  $f_{m+1}$  to the set of generators  $F$ , thereby enforcing this particular divergence of reduction to converge:

$$\begin{array}{l} \text{either} \quad x^i - f_j \xrightarrow{f_{m+1}} x^i - f_k \\ \text{or} \quad \quad \quad x^i - f_k \xrightarrow{f_{m+1}} x^i - f_j \end{array}$$

observe that this represents exactly a step in the formation of the remainder sequence (in fact one step in the division of  $f_j$  by  $f_k$  or vice versa)

this process terminates and yields a set of generators  $\hat{F}$   
s.t.

- $\longleftarrow_F^* = \equiv_I = \longleftarrow_{\hat{F}}^*$
- $\longrightarrow_{\hat{F}}$  is both Noetherian and CR

So we can decide the membership problem for  $I$  by reduction w.r.t.  $\hat{F}$

if in the end we interreduce the elements in  $\hat{F}$ , we simply get only the gcd in the generating set  $\hat{F}$

for our example above this means the following:

$$\begin{array}{rcl}
 F \rightarrow f_1 = & x^5 + x^4 + x^3 - x^2 - x - 1 & \\
 f_2 = & x^4 + x^2 + 1 & \\
 \text{---} & \text{---} & \\
 f_3 = & x^4 - x^2 - 2x - 1 = & f_1 - x \cdot f_2 \\
 f_4 = & x^2 + x + 1 = & \frac{1}{2}(f_2 - f_3) \\
 f_5 = & 0 = & f_3 - (x^2 - x - 1)f_4 \\
 & & \rightarrow \hat{F}
 \end{array}$$

now  $\hat{F}$  generates the same ideal  $I$ , and we can use the reduction w.r.t.  $\hat{F}$  to decide membership in  $I$ :

$$\begin{array}{rcl}
 x^5 - x^2 & \xrightarrow{f_1} & -x^4 - x^3 + x + 1 \xrightarrow{f_2} -x^3 + x^2 + x + 2 \\
 & \xrightarrow{f_4} & 2x^2 + 2x + 2 \xrightarrow{f_4} 0 \\
 x^5 - x^2 & \xrightarrow{f_2} & -x^3 - x^2 - x \xrightarrow{f_4} 0
 \end{array}$$

So  $x^5 - x^2 \in I$ .

### 3. Gröbner Bases algorithm for polynomial rings

the setting:

- $K[x_1, \dots, x_n]$ , the ring of multivariate polynomials over a field  $K$
- $F = \{f_1, \dots, f_m\} \subset K[x_1, \dots, x_n]$  generating an ideal  $I = \langle F \rangle$  in  $K[x_1, \dots, x_n]$
- equivalence relation  $g \equiv_I h \iff g - h \in I$

the problem:

- for  $g \in K[x_1, \dots, x_n]$
- decide: “ $g \equiv_I 0$ ”, i.e. “ $g \in \langle F \rangle = I$ ” ?



define a reduction relation  $\longrightarrow_F$ :

first define a linear ordering  $<$  on the terms/power products in the variables  $x_1, \dots, x_n$  respecting the multiplicative structure of this set of terms, called an **admissible ordering**; i.e.

- $1 = x^{(0, \dots, 0)} \leq s$  for every term  $s$
- if  $s \leq t$  and  $u$  any term, then  $s \cdot u \leq t \cdot u$

examples of such admissible ordering are

lexicographic orderings,  
graduated lexicographic orderings,  
and many others ...

so every non-zero polynomial  $f$  has a well-defined

**leading term**  $\text{lead}(f)$  and a  
non-zero **leading coefficient**  $\text{lc}(f)$ .

By  $\text{le}(f)$  we denote the exponent (vector) of  $\text{lead}(f)$ .

for polynomial  $g = \dots + g_e x^{e=(e_1, \dots, e_n)} + \dots$  with  $g_e \neq 0$

$$g \xrightarrow{f} g - \frac{g_e}{\text{lc}(f)} x^{e-\text{le}(f)} f(x),$$

if  $e - \text{le}(f) \in \mathbb{N}^n$

and

$$g \xrightarrow{F} h \iff \exists f \in F : g \xrightarrow{f} h$$



then  $\longrightarrow_F$  has the following properties:

- $\longrightarrow_F$  is terminating
- if  $g \longrightarrow_F h$  then  $g - h \in \langle F \rangle = I$

but  $\longrightarrow_F$  in general is **not** Church-Rosser:

let

$$F = \left\{ \underbrace{x^2y^2 + y - 1}_{f_1}, \underbrace{x^2y + x}_{f_2} \right\}$$

then

$$\begin{array}{l} x^2y^2 \longrightarrow_{f_1} -y + 1 \\ x^2y^2 \longrightarrow_{f_2} -xy \end{array}$$

both results are irreducible,

they are congruent,

but they have no common successor

So what do we do in order to create a situation where we have a CR reduction system?

Well, as in the previous cases (Gauss elimination, Euclidean algorithm) we investigate the “smallest” situations in which something can be reduced in essentially 2 different ways

- we look at terms  $x^e$  which can be reduced w.r.t. two different generators  $f_j, f_k$
- this means that  $\text{lead}(f_j)|x^e$  and also  $\text{lead}(f_k)|x^e$
- the (finitely many) smallest such situations occur when

$$x^e = \text{lcm}(\text{lead}(f_j), \text{lead}(f_k))$$

(least common multiple), and all the other cases are instantiations of such basic situations

(assuming w.l.o.g. leading coefficients to be 1)

$$x^i = \max(\text{lead}(f_j), \text{lead}(f_k))$$

$$\begin{array}{ccc} & \downarrow & \downarrow \\ x^i - f_j & & x^i - f_k \end{array}$$

These reduction results are congruent w.r.t.  $\equiv_I$ , so their difference  $f_{m+1} = f_j - f_k$  is in  $I$ . If  $f_{m+1} = 0$ , then there was no divergence anyway; otherwise we add  $f_{m+1}$  to the set of generators  $F$ , thereby enforcing this particular divergence of reduction to converge:

$$\begin{array}{l} \text{either} \quad x^i - f_j \xrightarrow{f_{m+1}} x^i - f_k \\ \text{or} \quad \quad \quad x^i - f_k \xrightarrow{f_{m+1}} x^i - f_j \end{array}$$

observe that this represents exactly a step in the formation of the remainder sequence (in fact one step in the division of  $f_j$  by  $f_k$  or vice versa)

this process terminates and yields a set of generators  $\hat{F}$   
s.t.

- $\longleftarrow^*_F = \equiv_I = \longleftarrow^*_{\hat{F}}$
- $\longrightarrow_{\hat{F}}$  is both Noetherian and CR

So we can decide the membership problem for  $I$  by reduction w.r.t.  $\hat{F}$

If in the end we interreduce the elements in  $\hat{F}$ , we get a minimal Gröbner basis for the ideal  $I$ .

for our example above this means the following:

$$\begin{aligned}
 F \rightarrow f_1 &= x^2y^2 + y - 1 \\
 f_2 &= x^2y + x \\
 &\text{-----} \\
 f_3 &= -xy + y - 1 = f_1 - y \cdot f_2 \\
 f_4 &= y - 1 = f_2 + (x + 1)f_3 \\
 f_5 &= -x = f_3 + (x - 1)f_4 \\
 &\rightarrow \hat{F}
 \end{aligned}$$

now  $\hat{F}$  generates the same ideal  $I$ , and we can use the reduction w.r.t.  $\hat{F}$  to decide membership in  $I$ :

$$\begin{array}{rclcl}
 x^2y^2 & \longrightarrow_{f_1} & -y + 1 & \longrightarrow_{f_4} & 0 \\
 x^2y^2 & \longrightarrow_{f_2} & -xy & \longrightarrow_{f_5} & 0
 \end{array}$$

So  $x^2y^2 \in I$ .

## 4. Knuth-Bendix algorithm for 1st order equ.theories

the setting:

- a term algebra  $\mathcal{T}(\Sigma, V)$  over a signature  $\Sigma$  and variables  $V$
- $E = \{s_i = t_i \mid i \in I\}$  a set of equations over  $\mathcal{T}$  generating an equational theory  $=_E$
- equivalence relation  $s \equiv_E t \iff s = t \in =_E$

the problem:

- for  $s, t \in \mathcal{T}(\Sigma, V)$
- decide: “ $s =_E t$ ” ?



define a reduction relation on  $\mathcal{T}(\Sigma, V)$  by orienting the equations

$$e_i : s_i = t_i$$

in one of the ways (according to a reduction ordering)

$$r_i : s_i \longrightarrow t_i \quad \text{or} \quad t_i \longrightarrow s_i$$

(w.l.o.g. assume  $r_i : s_i \longrightarrow t_i$ .)

This leads to a so-called “rewrite rule system (RRS)”

$$R = \{r_i \mid i \in I\}$$

The reduction  $\longrightarrow_R$  works in the following way: if there is a substitution  $\sigma$  such that  $\sigma(s_i) = u$ , then any term containing  $u$  as a subterm can be reduced to the corresponding term, where  $u$  is replaced by  $\sigma(t_i)$ :

$$u \longrightarrow_R v \iff \exists p, i, \sigma : u|_p = \sigma(s_i), \text{ and} \\ v = u[p \leftarrow \sigma(t_i)] .$$

In general the termination property is undecidable for rewrite rule systems. But there are several sufficient conditions; e.g.  $s_i > t_i$  w.r.t. a reduction ordering. For the following let us assume that the rules can be ordered w.r.t. such a reduction ordering.

then  $\longrightarrow_R$  has the following properties:

- $\longrightarrow_R$  is terminating (if, e.g., the rules are ordered w.r.t. a reduction ordering)
- $\longleftarrow_R^* = =_E$

but  $\longrightarrow_R$  in general is **not** Church-Rosser:



let  $G$  consist of the axioms of group theory

$$G = \left\{ \begin{array}{l} (1) \ 1 \cdot x = x, \\ (2) \ x^{-1} \cdot x = 1, \\ (3) \ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}$$

which are oriented (lexicographic path ordering with  $^{-1} > \cdot > 1$ ) to give the rewrite rule system

$$R = \left\{ \begin{array}{l} (1) \ 1 \cdot x \longrightarrow x, \\ (2) \ x^{-1} \cdot x \longrightarrow 1, \\ (3) \ (x \cdot y) \cdot z \longrightarrow x \cdot (y \cdot z) \end{array} \right\}$$

then

$$x^{-1} \cdot (x \cdot y) \xleftarrow{(3)} (x^{-1} \cdot x) \cdot y \xrightarrow{(2)} 1 \cdot y \xrightarrow{(1)} y$$

both results are irreducible,

they are congruent modulo  $=_E$ ,

but they have no common successor

So again the goal is to transform the RRS  $R$  into an equivalent  $\hat{R}$

$$\longleftrightarrow_R^* = \longleftrightarrow_{\hat{R}}^*$$

which has the Church-Rosser property

As in the previous cases (Gauss elimination, Euclidean algorithm, Gröbner bases) we investigate “smallest” situations in which a term can be reduced in essentially 2 different ways

- we look at terms which can be reduced w.r.t. two different rules  $r_i : s_i \longrightarrow t_i$ ,  $r_j : s_j \longrightarrow t_j$
- this means that there is a most general unifier (substitution)  $\sigma$  s.t.

$$\sigma(s_j) = \sigma(s_i)|_p$$

for some position  $p$

if

$$\sigma(s_i)|_p = \sigma(s_j)$$

then

$$\sigma(s_i) = u$$

↓

$$\sigma(t_i)$$

↓

$$\sigma(s_i)[p \leftarrow \sigma(t_j)]$$

these reduction results are obviously equal modulo  $=_E$ ;  
so are normal forms  $v_1, v_2$  to which they can be reduced.  
If  $v_1 \neq v_2$ , then we try to orient them into a new rule  
which will not violate the termination property

if this process terminates and yields a set of rules  $\hat{R}$  then

- $\longleftrightarrow_R^* = =_E = \longleftrightarrow_{\hat{R}}^*$
- $\longrightarrow_{\hat{R}}$  is both Noetherian and CR

So we can decide the equality modulo  $E$  by reduction w.r.t.  $\hat{R}$

in the end we can interreduce the elements in  $\hat{R}$  and so get a minimal set of rewrite rules for  $=_E$

for the example of group theory this means that because of

$$x^{-1} \cdot (x \cdot y) \xleftarrow{(3)} (x^{-1} \cdot x) \cdot y \xrightarrow{(2)} 1 \cdot y \xrightarrow{(1)} y$$

we add the new rule

$$(4) \quad x^{-1} \cdot (x \cdot y) \longrightarrow y$$





for the case of group theory this process (Knuth-Bendix) actually terminates and yields the following minimal rewrite rule system:

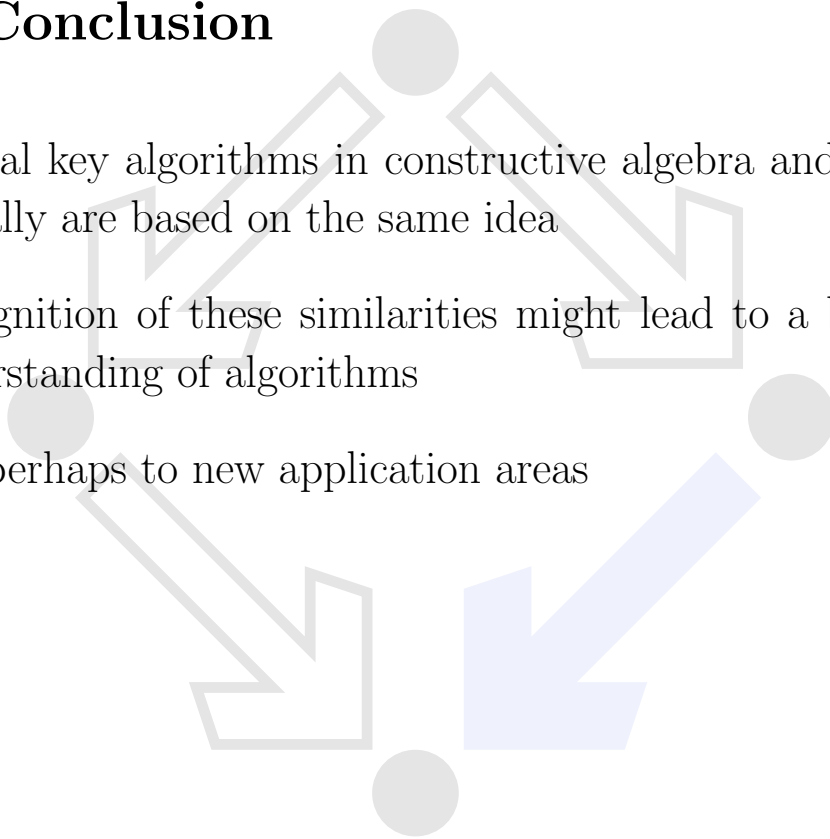
- (1)  $1 \cdot x \longrightarrow x,$
- (2)  $x^{-1} \cdot x \longrightarrow 1,$
- (3)  $(x \cdot y) \cdot z \longrightarrow x \cdot (y \cdot z),$
- (4)  $x^{-1} \cdot (x \cdot y) \longrightarrow y,$
- (5)  $x \cdot 1 \longrightarrow x,$
- (6)  $1^{-1} \longrightarrow 1,$
- (7)  $(x^{-1})^{-1} \longrightarrow x,$
- (8)  $x \cdot x^{-1} \longrightarrow 1,$
- (9)  $x \cdot (x^{-1} \cdot y) \longrightarrow y,$
- (10)  $(x \cdot y)^{-1} \longrightarrow y^{-1} \cdot x^{-1}.$

## 5. Conclusion

Several key algorithms in constructive algebra and logic actually are based on the same idea

Recognition of these similarities might lead to a better understanding of algorithms

and perhaps to new application areas





**Thank you !**