Internship report

Towards automating proofs in commutative semi-rings

06/09/2016

IANNETTA Paul

How to prove automatically, the following theorem.

Associtativity of the `plus` operator

$$\forall (x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

What do we need?

How to prove automatically, the following theorem.

Associtativity of the `plus` operator

$$\forall (x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

What do we need?

1. A way to express mathematical statements ;

How to prove automatically, the following theorem.

Associtativity of the `plus` operator

$$\forall (x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

What do we need?

1. A way to express mathematical statements ;
2. An automated proof scheme.

How to prove automatically, the following theorem.

Associtativity of the `plus` operator

$$\forall(x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

What do we need?

1. A way to express mathematical statements ;
   - By using *Terms*.
2. An automated proof scheme.

How to prove automatically, the following theorem.

Associtativity of the `plus` operator

$$\forall(x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

What do we need?

1. A way to express mathematical statements ;
   - By using *Terms*.
2. An automated proof scheme.
   - By using *rewriting induction*.

Let $\mathcal{F}$ be a set and $\mathtt{ar} : \mathcal{F} \longrightarrow \mathbb{N}$.

skip

Signature and Carrier of an Algebra

The tuple $(\mathcal{F}, \mathtt{ar})$ is called signature.
$\mathcal{F}$ is the carrier (set) associated to the signature $(\mathcal{F}, \mathtt{ar})$.

An element $e \in \mathcal{F}$ is said to be either:

- a *constant* if $\mathtt{ar}(e) = 0$;
- a *function* whose arity is $\mathtt{ar}(e)$.

Set of functions of arity k

$$\mathcal{F}_k = \{ \ f \in \mathcal{F} \mid \mathtt{ar}(f) = k \ \}$$

Let $\mathcal{F}$ and $\mathcal{V}$ be two *disjoint* sets and $\mathtt{ar} : \mathcal{F} \longrightarrow \mathbb{N}$.
Let's consider the signature $(\mathcal{F}, \mathtt{ar})$.

Term

The set of terms $\mathcal{T}(\mathcal{F}, \mathcal{V})$ is the least set closed under:

(i) All variables are terms ;

(ii) All constants are terms ;

(iii) $\forall (x_1, \ldots, x_n) \in \mathcal{T}(\mathcal{F}, \mathcal{V})^n, f \in \mathcal{F}_n, f(x_1, \cdots, x_n)$ are terms.

Let $\mathcal{F}$ and $\mathcal{V}$ be two *disjoint* sets and $\mathtt{ar} : \mathcal{F} \longrightarrow \mathbb{N}$.
Let's consider the signature $(\mathcal{F}, \mathtt{ar})$.

Term

The set of terms $\mathcal{T}(\mathcal{F}, \mathcal{V})$ is the least set closed under:

(i) All variables are terms ;

(ii) All constants are terms ;

(iii) $\forall (x_1, \ldots, x_n) \in \mathcal{T}(\mathcal{F}, \mathcal{V})^n, f \in \mathcal{F}_n, f(x_1, \cdots, x_n)$ are terms.

Point

How to define our arithmetical statements?
What is $\mathcal{F}$? What is $\mathtt{ar}$?

Substitution

A substitution is a partial function from the set of variables $\mathcal{V}$ to the set of terms $\mathcal{T}(\mathcal{F},\mathcal{V})$. By abuse we call the extended function to terms a substitution. For a substitution σ and a term t, $t\sigma$ is called an *instance* of t.

Substitution

A substitution is a partial function from the set of variables $\mathcal{V}$ to the set of terms $\mathcal{T}(\mathcal{F},\mathcal{V})$. By abuse we call the extended function to terms a substitution. For a substitution σ and a term t, $t\sigma$ is called an *instance* of t.

Unification

Let $\{(s_i, t_i)\}_{i \in I}$ be a set of equalities and $I \subseteq \mathbb{N}$.
Unification is the fact of finding a substitution σ such that $\forall i \in I, s_i\sigma \equiv t_i\sigma$ (In the best case, σ is an idempotent mgu).

? Check Point

- Can we unify $x + (y + z) \equiv x' + (y' + (z' + w'))$?

Rewrite Rule

A rewrite rule is a tuple of term (ℓ, r) written $\ell \to r$
That means that $\ell\sigma \to r\sigma$.

Rewrite Rule

A rewrite rule is a tuple of term (ℓ, r) written $\ell \to r$
That means that $\ell\sigma \to r\sigma$.

Term Rewriting System

A term rewriting system (TRS) is a set of rewrite rules.

Rewrite Rule

A rewrite rule is a tuple of term (ℓ, r) written $\ell \to r$
That means that $\ell\sigma \to r\sigma$.

Term Rewriting System

A term rewriting system (TRS) is a set of rewrite rules.

Point

We can now define a TRS that encompasses basic arithmetic.

Rewrite Rule

A rewrite rule is a tuple of term (ℓ, r) written $\ell \to r$
That means that $\ell\sigma \to r\sigma$.

Term Rewriting System

A term rewriting system (TRS) is a set of rewrite rules.

Point

We can now define a TRS that encompasses basic arithmetic.

TRS for basic arithmetic

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

Constructor symbols and Defined symbols

Let's consider an arbitrary term-rewriting system $\mathcal{T}$.

- **Defined symbols** are the set of symbols appearing at the root position of the left hand sides of the rules.
- **Constructor symbols** are the symbols that are not defined symbols.

Constructor symbols and Defined symbols

Let's consider an arbitrary term-rewriting system $\mathcal{T}$.

- **Defined symbols** are the set of symbols appearing at the root position of the left hand sides of the rules.
- **Constructor symbols** are the symbols that are not defined symbols.

TRS for basic arithmetic

$$\mathcal{R}_+ : \begin{cases} x + 0 \rightarrow x \\ x + s(y) \rightarrow s(x + y) \end{cases}$$

Basic terms and Ground terms

- A basic term is a term made up entirely of constructor symbols save for the root symbol (which is a defined symbol).
- A ground term is a term with no variables.

Basic terms and Ground terms

- A basic term is a term made up entirely of constructor symbols save for the root symbol (which is a defined symbol).
- A ground term is a term with no variables.

Examples of ground basic terms

- $s(0) + s(0)$;

Basic terms and Ground terms

- A basic term is a term made up entirely of constructor symbols save for the root symbol (which is a defined symbol).
- A ground term is a term with no variables.

Examples of ground basic terms

- $s(0) + s(0)$;
- $0 + s(s(0))$;

Basic terms and Ground terms

- A basic term is a term made up entirely of constructor symbols save for the root symbol (which is a defined symbol).
- A ground term is a term with no variables.

Examples of ground basic terms

- $s(0) + s(0)$;
- $0 + s(s(0))$;
- $s^m(0) + s^n(0), \forall (m, n) \in \mathbb{N}^2$.

Sufficiently-completeness

A rewriting-system $\mathcal{T}$ is said to be sufficiently complete if all ground basic terms can be reduced to constructor terms.

Sufficiently-completeness

A rewriting-system $\mathcal{T}$ is said to be sufficiently complete if all ground basic terms can be reduced to constructor terms.

The following TRS is sufficient complete

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$s^m(0) + s^n(0) \to^*_{\mathcal{R}_+} s^{m+n}(0), \forall (m, n) \in \mathbb{N}^2.$

Inductive property

A property $\mathcal{P}(t_1, \ldots, t_n)$ on terms is an inductive property if $\mathcal{P}(t_1\sigma, \ldots, t_n\sigma)$ holds for all *ground* substitution σ wherein $t_1, \ldots, t_n$ are all instanciated to ground terms.

Semantic equality on terms

Let $\mathcal{R}$ be a TRS.
$\mathcal{R} \vdash s = t$ *if and only if* $s\sigma = t\sigma$ for all ground substitution σ whose domain encompass the variables appearing both in s and t.

Inference Rules for Rewriting Induction

Expand:

$$\frac{\langle E \cup \mathrm{Expd}_u(s,t), H \cup \{s \to t\}\rangle}{\langle E \cup \{s = t\}, H\rangle}, u \in \mathcal{B}(s), s > t$$

Simplify:

$$\frac{\langle \{E \cup \{s' = t\}, H\}\rangle}{\langle E \cup \{s = t\}, H\rangle} s \to_{R \cup H} s'$$

Delete:

$$\frac{\langle \{E, H\}\rangle}{\langle \{E \cup \{s = s\}, H\}\rangle}$$

$$\mathrm{Expd}_u(s,t) = \{C[r]\sigma = t\sigma \mid s \equiv C[u], \sigma = \mathrm{mgu}(u,l), l \to r \in \mathcal{R}, l \in \mathcal{B}(s)\}$$

$$(E,H) \rightsquigarrow_i (E' H') \text{ if } \frac{\langle E', H'\rangle}{\langle E, H\rangle} \text{ with } i \in \{e, s, d\}$$

Theorem

For a *sufficiently-complete* and *terminating* $\mathrm{TRS}\ \mathcal{R}$, if $\langle \{s = t\}, \emptyset \rangle \ \rightsquigarrow^*_{e,s,d}\ \langle \emptyset, H \rangle$ then $\mathcal{R} \vdash s = t$.

Associtativity of the `plus` operator

$$\forall (x, y, z) \in \mathbb{N}^3, (x + y) + z = x + (y + z)$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$$\langle \{x + (y + z) = (x + y) + z\}, \emptyset \rangle$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x + y) \end{cases}$$

$$\langle \{x + (y + z) = (x + y) + z\}, \emptyset \rangle$$
$$\rightsquigarrow_e \langle \{x + (y_1 + 0) = x + y_1 ; x + (y_1 + s(z_1)) = s((x + y_1) + z_1)\},$$
$$\{x + (y + z) \to (x + y) + z\} \rangle$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x+y) \end{cases}$$

$$\begin{aligned}
& \langle \{x + (y+z) = (x+y) + z\}, \emptyset \rangle \\
\rightsquigarrow_e & \langle \{x + (y_1 + 0) = x + y_1 ; x + (y_1 + s(z_1)) = s((x + y_1) + z_1)\}, \\
& \{x + (y+z) \to (x+y) + z\} \rangle \\
\rightsquigarrow_s^* & \langle \{x + y_1 = x + y_1 ; x + s(y_1 + z_1) = s((x + y_1) + z_1)\}, \\
& \{x + (y+z) \to (x+y) + z\} \rangle
\end{aligned}$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \rightarrow x \\ x + s(y) \rightarrow s(x+y) \end{cases}$$

$$\begin{aligned}
& \langle \{x + (y+z) = (x+y)+z\}, \emptyset \rangle \\
\rightsquigarrow_e & \langle \{x + (y_1 + 0) = x + y_1 ; x + (y_1 + s(z_1)) = s((x+y_1)+z_1)\}, \\
& \{x + (y+z) \rightarrow (x+y)+z\} \rangle \\
\rightsquigarrow_s^* & \langle \{x + y_1 = x + y_1 ; x + s(y_1 + z_1) = s((x+y_1)+z_1)\}, \\
& \{x + (y+z) \rightarrow (x+y)+z\} \rangle \\
\rightsquigarrow_s^* & \langle \{x + y_1 = x + y_1 ; s(x + (y_1 + z_1)) = s((x+y_1)+z_1)\}, \\
& \{x + (y+z) \rightarrow (x+y)+z\} \rangle
\end{aligned}$$

The underlying TRS

$$\mathcal{R}_+ : \begin{cases} x + 0 \to x \\ x + s(y) \to s(x+y) \end{cases}$$

$$\begin{aligned}
&\langle \{x + (y+z) = (x+y)+z\}, \emptyset\rangle \\
\rightsquigarrow_e &\langle \{x + (y_1 + 0) = (x+y_1); x + (y_1 + s(z_1)) = s((x+y_1)+z_1)\}, \\
&\{x + (y+z) \to (x+y)+z\}\rangle \\
\rightsquigarrow_s^* &\langle \{x + y_1 = (x+y_1); x + s(y_1+z_1) = s((x+y_1)+z_1)\}, \\
&\{x + (y+z) \to (x+y)+z\}\rangle \\
\rightsquigarrow_s^* &\langle \{x + y_1 = (x+y_1); s(x + (y_1+z_1)) = s((x+y_1)+z_1)\}, \\
&\{x + (y+z) \to (x+y)+z\}\rangle \\
\rightsquigarrow_d^* &\langle \emptyset, \{x + (y+z) \to (x+y)+z\}\rangle
\end{aligned}$$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$
- **A**: $(x \star y) \star z = x \star (y \star z)$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$
- **A**: $(x \star y) \star z = x \star (y \star z)$
- **N**: $x \star n = x$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$
- **A**: $(x \star y) \star z = x \star (y \star z)$
- **N**: $x \star n = x$
- **D**: $x \cdot (y \star z) = x \cdot y \star x \cdot y$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$
- **A**: $(x \star y) \star z = x \star (y \star z)$
- **N**: $x \star n = x$
- **D**: $x \cdot (y \star z) = x \cdot y \star x \cdot y$
- **E**: $x \cdot e = x$

Semi-ring

A semi-ring $(\mathcal{A}, \star, \cdot)$ is a triple where $\mathcal{A}$ is a *set*, and $\star$ and $\cdot$ are two internal operations.

Properties of $\star$ and $\cdot$

$\exists n, \exists e, \forall (x, y, z) \in \mathcal{A}^3.$

- **C**: $x \star y = y \star x$
- **A**: $(x \star y) \star z = x \star (y \star z)$
- **N**: $x \star n = x$
- **D**: $x \cdot (y \star z) = x \cdot y \star x \cdot y$
- **E**: $x \cdot e = x$
- **C**: $x \cdot y = y \cdot x$

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

How to prove equality ?

1. Expand (distributivity) to normal forms;

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

How to prove equality ?

1. Expand (distributivity) to normal forms;
2. Kill off inverses ($\star$) by swapping sides ;

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

How to prove equality ?

1. Expand (distributivity) to normal forms;
2. Kill off inverses ($\star$) by swapping sides ;
3. Sort (commutativity + associativity) ;

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

How to prove equality ?

1. Expand (distributivity) to normal forms;
2. Kill off inverses ($\star$) by swapping sides ;
3. Sort (commutativity + associativity) ;
4. Compare terms by terms.

Well-ordered commutative semi-ring

A *well-ordered* semi-ring is a tuple $(\mathcal{A}, \preceq)$ where $\mathcal{A}$ is a semi-ring and $\preceq$ is an order on $\mathcal{A}$.

How to prove equality ?

1. Expand (distributivity) to normal forms;
2. Kill off inverses ($\star$) by swapping sides ;
3. Sort (commutativity + associativity) ;
4. Compare terms by terms.

Note

Deciding equality on terms in a semi-ring is equivalent to deciding the equality of two sortable-lists.

Vadja's Equality

$\forall(n, i, j) \in \mathbb{N}^3, \mathcal{F}_{n+i}\mathcal{F}_{n+j} - \mathcal{F}_n\mathcal{F}_{n+i+j} = (-1)^n\mathcal{F}_i\mathcal{F}_j$

Vadja's Equality

$\forall (n, i, j) \in \mathbb{N}^3, \mathcal{F}_{n+i}\mathcal{F}_{n+j} - \mathcal{F}_n\mathcal{F}_{n+i+j} = (-1)^n\mathcal{F}_i\mathcal{F}_j$

The special case

$n \leftarrow 2n$, $i \leftarrow n$, $j \leftarrow 1$:
$\forall n \in \mathbb{N}, \mathcal{F}_{3n}\mathcal{F}_{2n+1} = \mathcal{F}_{2n}\mathcal{F}_{3n+1} + \mathcal{F}_n$

Attention

We should keep the axioms of the well ordered semi-ring structure and the rules for the Fibonacci numbers apart.

The TRS

$$\mathcal{F}(m+2) \to \mathcal{F}(m+1) + \mathcal{F}(m)$$

Attention

We should keep the axioms of the well ordered semi-ring structure and the rules for the Fibonacci numbers apart.

The TRS

$$\mathcal{F}(m+2) \to \mathcal{F}(m+1) + \mathcal{F}(m)$$

Expand!

$$\begin{aligned} & \langle \{\mathcal{F}_{3n}\mathcal{F}_{2n+1} = \mathcal{F}_{2n}\mathcal{F}_{3n+1} + \mathcal{F}_n\}, \emptyset \rangle \\ \rightsquigarrow_e & \langle \{\mathcal{F}_{3n+6}\mathcal{F}_{2n+5} = (\mathcal{F}_{2n+3} + \mathcal{F}_{2n+2})(\mathcal{F}_{3n+6} + \mathcal{F}_{3n+5}) + (\mathcal{F}_{n+1} + \mathcal{F}_n)\} \\ & \{\mathcal{F}_{2n}\mathcal{F}_{3n+1} + \mathcal{F}_n \to \mathcal{F}_{3n}\mathcal{F}_{2n+1}\}\rangle \end{aligned}$$

At

We sh [illegible] he axioms of the well orde [illegible] ing structure and th [illegible] r the Fibonacci nu [illegible] art.

The TRS

$\mathcal{F}(m+2) \to \mathcal{F}(m+1) +$ [illegible]

Expand!

$\langle\{\mathcal{F}_{3n}\mathcal{F}_{2}$ [illegible] $_{3n+1} + \mathcal{F}_n\}, \emptyset\rangle$

$\rightsquigarrow_e \langle\{\mathcal{F}$ [illegible] $(\mathcal{F}_{2n+3} + \mathcal{F}_{2n+2})(\mathcal{F}_{3n+6} + \mathcal{F}_{3n+5}) +$ [illegible] $)\}$

[illegible] $+ \mathcal{F}_n \to \mathcal{F}_{3n}\mathcal{F}_{2n+1}\}\rangle$

Attention

That would be a good point if we could expand $\mathcal{F}_{n+1}$ w.r.t. the second induction hypothesis we should have.

The TRS

$$\begin{aligned}
\mathcal{F}(m+2) &\rightarrow \mathcal{F}(m+1) + \mathcal{F}(m) \\
\mathcal{F}(m+1) &\rightarrow \mathcal{F}(m) + \mathcal{F}(m-1) \\
\mathcal{F}(m) &\rightarrow \mathcal{F}(m-1) + \mathcal{F}(m-2)
\end{aligned}$$

Attention

That would be a good point if we could expand $\mathcal{F}_{n+1}$ w.r.t. the second induction hypothesis we should have.

The TRS

$$\begin{aligned}\mathcal{F}(m+2) &\rightarrow \mathcal{F}(m+1)+\mathcal{F}(m)\\ \mathcal{F}(m+1) &\rightarrow \mathcal{F}(m)+\mathcal{F}(m-1)\\ \mathcal{F}(m) &\rightarrow \mathcal{F}(m-1)+\mathcal{F}(m-2)\end{aligned}$$

$$\begin{aligned}&\langle\{\mathcal{F}_{3n}\mathcal{F}_{2n+1} = \mathcal{F}_{2n}\mathcal{F}_{3n+1}+\mathcal{F}_n\},\emptyset\rangle\\ \rightsquigarrow_e&\langle\{\mathcal{F}_{3n+6}\mathcal{F}_{2n+5} = (\mathcal{F}_{2n+3}+\mathcal{F}_{2n+2})(\mathcal{F}_{3n+6}+\mathcal{F}_{3n+5})+\\ &(\mathcal{F}_{3n+3}\mathcal{F}_{2n+3}-\mathcal{F}_{3n+4}\mathcal{F}_{2n+2}+\mathcal{F}_n)\}\\ &\{\mathcal{F}_{2n}\mathcal{F}_{3n+1}+\mathcal{F}_n \rightarrow \mathcal{F}_{3n}\mathcal{F}_{2n+1}\}\rangle\end{aligned}$$

But I still have some problems ...

But I still have some problems ...

- Indexes should never contain minus sign

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use
  - We should handle minus signs as long as they do not conflict

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use
  - We should handle minus signs as long as they do not conflict
- We should find both induction hypothesis

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use
  - We should handle minus signs as long as they do not conflict
- We should find both induction hypothesis
  - As of now, It is not done

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use
  - We should handle minus signs as long as they do not conflict
- We should find both induction hypothesis
  - As of now, It is not done
  - Once it is done we could find the final property to prove ...

But I still have some problems ...

- Indexes should never contain minus sign
  - We should be wary of which rule to use
  - We should handle minus signs as long as they do not conflict
- We should find both induction hypothesis
  - As of now, It is not done
  - Once it is done we could find the final property to prove ...
  - ...And apply well-ordered semi-rings properties.

Conclusion

- I presented rewriting induction (Reddy 1990) ;

Conclusion

- I presented rewriting induction (Reddy 1990) ;
- How to appy it in the context of well-ordered semi-rings.

Thank you for your attention

Question time