This part focus on **Operational Semantics**
of formal calculi (and programming languages)
Topics

• Tools to study the operational properties of a system:
  ➢ Rewrite Theory (rewriting=abstract form of program execution)

• Induction and Co-induction proof principles.

• Linear Logic and Proof-Nets.

• Bridging between lambda-calculus and functional programming.
  ➢ Call-by-Value and Call-by Name, weak and lazy calculi.
  ➢ Big-Step and Small-Step operational semantics.
  ➢ Observational equivalence

• Reasoning on programs equivalence:
  ➢ Bisimulation and coinductive methods.

• Beyond pure functional:
  ➢ Probabilistic programming and Bayesian Inference:
    Probabilistic lambda calculi, Bayesian proof-nets
Resources

• **Reference Books:**
  
  ➢ *R. AMADIO: Operational methods in semantics*  
  (available on HAL https://hal.archives-ouvertes.fr/cel-01422101v1).
  
  ➢ *D. SANGIORGI: Introduction to Bisimulation and Coinduction*  
  (Cambridge University Press, 2011)

• **Lecture Notes**  
  (by Middeldorp, Laurent, Ong)

Please send me an email (with LMFI in the subject) to have the lecture notes on Rewriting Theory
Operational semantics
of formal calculi and programming languages

Rewriting theory

- Rewriting = abstract form of program execution
- Paradigmatic example: λ-calculus
  (functional programming language, in its essence)
A colony of chameleons includes 20 red, 18 blue, and 16 green individuals. Whenever two chameleons of different color meet, each changes to the third color. Some time passes during which no chameleons are born or die nor do any enter or leave the colony. Is it possible that at the end of this period, all 54 chameleons are the same color?
Example (Group Theory)

**signature**
- e (constant)
- \(-\) (unary, postfix)
- \(\cdot\) (binary, infix)

**equations**
- \(e \cdot x \approx x\)
- \(x^- \cdot x \approx e\)
- \((x \cdot y) \cdot z \approx x \cdot (y \cdot z)\)

**theorems**
- \(e^- \approx_\mathcal{E} e\)
- \((x \cdot y)^- \approx_\mathcal{E} y^- \cdot x^-\)

**rewrite rules**
- \(e \cdot x \rightarrow x\)
- \(x \cdot e \rightarrow x\)
- \(x^- \cdot x \rightarrow e\)
- \(x \cdot x^- \rightarrow e\)
- \((x \cdot y) \cdot z \rightarrow x \cdot (y \cdot z)\)
- \(x^{-\cdot} \rightarrow x\)
- \(e^- \rightarrow e\)
- \((x \cdot y)^- \rightarrow y^- \cdot x^-\)
- \(x^- \cdot (x \cdot y) \rightarrow y\)
- \(x \cdot (x^- \cdot y) \rightarrow y\)

1. \(s \approx t\) is valid in \(\mathcal{E}\) (\(s \approx_\mathcal{E} t\)) if and only if \(s\) and \(t\) have same \(\mathcal{R}\)-normal form
2. \(\mathcal{R}\) admits no infinite computations

\(1 \& 2 \implies \mathcal{E}\) has decidable validity problem
Example (Combinatory Logic)

signature  
S  K  I  (constants)  ·  (application, binary, infix)

terms  
S  ((K · I) · I) · S  (x · z) · (y · z)

rewrite rules  
I · x → x
(K · x) · y → x
((S · x) · y) · z → (x · z) · (y · z)

rewriting  
((S · K) · K) · x → (K · x) · (K · x)
          → x

inventor  
Moses Schönfinkel (1924)
Example (Lambda Calculus)

signature \( \lambda \) (binds variables) \( \cdot \) (application, binary, infix)

terms \( M ::= x \mid (\lambda x. M) \mid (M \cdot M) \)

\( \alpha \) conversion \( \lambda x. x \cdot y \equiv_{\alpha} \lambda z. z \cdot y \)

\( \beta \) reduction \( (\lambda x. M) \cdot N \rightarrow_{\beta} M[x := N] \)

\( \) replace free occurrences of \( x \) in \( M \) by \( N \)
\( \) (and avoid variable capturing)

rewriting \( (\lambda x. x \cdot x) \cdot (\lambda x. x \cdot x) \rightarrow (\lambda x. x \cdot x) \cdot (\lambda x. x \cdot x) \)

inventor Alonzo Church (1932)

both Combinatory Logic and Lambda Calculus are Turing-complete
Rewrite Theory provides a powerful set of tools to study computational and operational properties of a system: normalization, termination, confluence, uniqueness of normal forms.

Tools to study and compare strategies:

- Is there a strategy guaranteed to lead to normal form, if any (normalizing strat.)?

Abstract Rewrite Systems (ARS) capture the common substratum of rewrite theory (independently from the particular structure of terms) - can be used in the study of any calculus or programming language.
Abstract Rewriting: motivations

**concrete** rewrite formalisms / concrete operational semantics:

- $\lambda$-calculus
- *Quantum/ probabilistic/ non-deterministic/............* $\lambda$-calculus
- Proof-nets / graph rewriting
- Sequent calculus and cut-elimination
- string rewriting
- term rewriting

**abstract** rewriting

- **independent from** structure of objects that are rewritten
- **uniform** presentation of properties and proofs
Abstract Rewriting

Basic language
**Definition 1.1.1.** An *abstract rewrite system* (ARS for short) is a pair $\mathcal{A} = \langle A, \rightarrow \rangle$ consisting of a set $A$ and a binary relation $\rightarrow$ on $A$. Instead of $(a, b) \in \rightarrow$ we write $a \rightarrow b$ and we say that $a \rightarrow b$ is a *rewrite step*.

- A (finite) *rewrite sequence* is a non-empty sequence $(a_0, \ldots, a_n)$ of elements in $A$ such that $a_i \rightarrow a_{i+1}$

  We write $a_0 \rightarrow^n a_n$ or simply $a_0 \rightarrow^* a_n$

- **rewrite sequence**
  - finite $\quad a \rightarrow e \rightarrow b \rightarrow c \rightarrow f$
  - empty $\quad a$
  - infinite $\quad a \rightarrow e \rightarrow b \rightarrow a \rightarrow e \rightarrow b \rightarrow \cdots$
\[ s \leftrightarrow_R t \iff s \rightarrow_R t \text{ or } t \rightarrow_R s \]
\[ s \leftrightarrow^*_R t \iff s = s_0 \leftrightarrow_R s_1 \leftrightarrow_R \ldots \leftrightarrow_R s_n = t \text{ for } n \geq 0 \]

• \leftrightarrow \quad \text{symmetric closure of } \rightarrow

• \leftrightarrow^* \quad \text{conversion} \quad \text{(equivalence relation generated by } \rightarrow) \quad **

• \rightarrow^+ \quad \text{transitive closure of } \rightarrow

• \rightarrow= \quad \text{reflexive closure of } \rightarrow

is relation composition: \[ R \cdot S = \{ (a, c) \mid a \ R \ b \text{ and } b \ S \ c \} \]
We denote $\rightarrow^*$ (resp. $\rightarrow^=$) the transitive-reflexive (resp. reflexive) closure of $\rightarrow$.

If $\rightarrow_1, \rightarrow_2$ are binary relations on $A$ then $\rightarrow_1 \cdot \rightarrow_2$ denotes their composition, i.e. $t \rightarrow_1 \cdot \rightarrow_2 s$ iff there exists $u \in A$ such that $t \rightarrow_1 u \rightarrow_2 s$.

We write $(A, \{\rightarrow_1, \rightarrow_2\})$ to denote the ARS $(A, \rightarrow)$ where $\rightarrow = \rightarrow_1 \cup \rightarrow_2$. 
The transitive-reflexive closure of a relation is a closure operator, \textit{i.e.} satisfies
\[
\rightarrow \subseteq \rightarrow^*, \quad (\rightarrow^*)^* = \rightarrow^*, \quad \rightarrow_1 \subseteq \rightarrow_2 \text{ implies } \rightarrow_1^* \subseteq \rightarrow_2^*
\]

As a consequence
\[
(\rightarrow_1 \cup \rightarrow_2)^* = (\rightarrow_1^* \cup \rightarrow_2^*)^*.
\]
**Terminology**

- if $x \rightarrow^* y$ then $x$ rewrites to $y$ and $y$ is **reduct** of $x$
- if $x \rightarrow^* z \leftarrow y$ then $z$ is **common reduct** of $x$ and $y$
- if $x \leftrightarrow^* y$ then $x$ and $y$ are **convertible**

**Example**

```
  a ← b → c → d
   ↑    ↓    ↓
e ← f ↓ e ↓ f ↓ d
   ↓    ↓        not g ↓ d
   ↓    ↓
g      g ← d
```
- $a \rightarrow^* f$
- $e \downarrow f$, $f \downarrow d$, not $g \downarrow d$
- $g \leftrightarrow^* d$
Definition 1.1.11. Let $\mathcal{A} = \langle A, \rightarrow \rangle$ be an ARS. An element $a \in A$ is reducible if there exists an element $b \in A$ with $a \rightarrow b$. A normal form is an element that is not reducible. The set of normal forms of $\mathcal{A}$ is denoted by $\text{NF}(\mathcal{A})$ or $\text{NF}(\rightarrow)$ when $A$ can be inferred from the context. An element $a \in A$ has a normal form if $a \rightarrow^* b$ for some normal form $b$. In that case we write $a \rightarrow^! b$.

Element a has normal forms? How many normal forms has this ARS?

ARS $\mathcal{A} = \langle A, \rightarrow \rangle$

- d is normal form
- $\text{NF}(\mathcal{A}) = \{ d, g \}$
- $b \rightarrow^! g$
- **SN**  strong normalization  termination
  - no infinite rewrite sequences

- **WN**  (weak) normalization
  - every element has at least one normal form
  - $\forall a \\exists b \ a \rightarrow^1 b$

- **UN**  unique normal forms
  - no element has more than one normal form
  - $\forall a, b, c$  if $a \rightarrow^1 b$ and $a \rightarrow^1 c$ then $b = c$
**Termination**

**Definition 1.2.1.** Let $\mathcal{A} = \langle A, \to \rangle$ be an ARS. An element $a \in A$ is called *terminating* or *strongly normalizing* (SN) if there are no infinite rewrite sequences starting at $a$. The ARS $\mathcal{A}$ is terminating or strongly normalizing if all its elements are terminating. An element $a \in A$ has *unique normal forms* (UN) if it does not have different normal forms ($\forall b, c \in A$ if $a \to^1 b$ and $a \to^1 c$ then $b = c$). The ARS $\mathcal{A}$ has unique normal forms if all its elements have unique normal forms.

An element $a$ is *weakly normalizing* (WN) (or simply normalizing) if it has a normal form.

- a is WN? SN?
- c is WN? SN?
- a or c has UN?
- The nf are convertible?
Given

\[ R = \left\{ \begin{array}{ccc} f(x, x) & \rightarrow & c \\ a & \rightarrow & b \\ f(x, b) & \rightarrow & d \end{array} \right\} \]

*f(a, a)* has normal form?
Can you produce two different nf?

We can compute from the same term *f(a, a)* two different normal-forms *c* and *d* different meaning for for equivalent terms
Same meaning for *equivalent* terms
**Confluence**

**Definition 1.2.3.** Let $\mathcal{A} = \langle A, \rightarrow \rangle$ be an ARS. An element $a \in A$ is confluent if for all elements $b, c \in A$ with $b \overset{*}{\leftarrow} a \overset{*}{\rightarrow} c$ we have $b \downarrow c$. The ARS $\mathcal{A}$ is confluent if all its elements are confluent.

Every confluent ARS has unique normal forms.
1. Is $a$ confluent?
2. Is $f$ confluent?

3. Can you add a single arrow so that the resulting ARS has unique normal forms without being confluent?
**Definition 1.2.3.** Let $A = \langle A, \rightarrow \rangle$ be an ARS. An element $a \in A$ is confluent if for all elements $b, c \in A$ with $b \xleftarrow{*} a \xrightarrow{*} c$ we have $b \downarrow c$. The ARS $A$ is confluent if all its elements are confluent.

\[
\begin{array}{c}
\text{An ARS } A = \langle A, \rightarrow \rangle \text{ is confluent if and only if } \leftrightarrow^* \subseteq \downarrow.
\end{array}
\]
**Definition 1.2.10.** An ARS $A = \langle A, \rightarrow \rangle$ has unique normal forms with respect to conversion (UNC) if different normal forms are not convertible ($\forall a, b \in \text{NF}(A)$ if $a \leftrightarrow^* b$ then $a = b$).

In an ARS with the property UNC every equivalence class of convertible elements contains at most one normal form.

Q: are UN and UNC equivalent?
Global vs Local
A property of term $t$ is *local* if it is quantified over only *one-step reductions* from $t$; it is *global* if it is quantified over all *rewrite sequences* from $t$.

**Locally confluent (WCR)**

**Strongly confluent**

**Diamond**

---

**confluence** Let $A = \langle A, \rightarrow \rangle$ be an ARS. An element $a \in A$ is *confluent* if for all elements $b, c \in A$ with $b \xleftarrow{*} a \rightarrow{*} c$ we have $b \Downarrow c$. The ARS $A$ is confluent if all its elements are confluent.

**Global property:**
Confluence

A property of term $t$ is *local* if it is quantified over only *one-step reductions* from $t$; it is *global* if it is quantified over all *rewrite sequences* from $t$.

<table>
<thead>
<tr>
<th>Locally confluent (WCR)</th>
<th>Strongly confluent</th>
<th>Diamond</th>
</tr>
</thead>
</table>

**Local confluence**  
Let $\mathcal{A} = \langle A, \rightarrow \rangle$ be an ARS. An element $a \in A$ is *locally confluent* for all elements $b, c \in A$ with $b \leftarrow a \rightarrow c$ we have $b \downarrow c$. The ARS $\mathcal{A}$ is confluent if all its elements are confluent.

An ARS $\mathcal{A} = \langle A, \rightarrow \rangle$ has the *diamond property* ($\Diamond$) if $\leftarrow \cdot \rightarrow \subseteq \rightarrow \cdot \leftarrow$
• diamond property

• \( \leftrightarrow \cdot \rightarrow \subseteq \rightarrow \cdot \leftarrow \)

• \( \forall a, b, c \)

\[ \exists d \]

• every ARS with diamond property is conflu ent
An ARS \( \mathcal{A} = \langle A, \rightarrow \rangle \) is \textit{strongly confluent} (SCR) if \( \leftarrow \cdot \rightarrow \subseteq \rightarrow^* \cdot \leftarrow \), see Figure.

\( a \) Show that every strongly confluent ARS is confluent.

\( b \) Does the converse also hold?

\( c \) Show that an ARS \( \mathcal{A} = \langle A, \rightarrow \rangle \) is confluent if and only if \( \leftarrow^* \cdot \rightarrow \subseteq \rightarrow^* \cdot \leftarrow^* \)
Which is true?

1. SN => WN
2. WN => SN
3. Confluence => UN
4. UN => Confluence
5. Confluence => Local confluence
6. Local confluence => Confluence
7. WN & UN => Confluence
8. WN & Local Conf. => Confluence
9. SN & Local Conf. => Confluence
WN vs SN

\[ R = \begin{cases} 
  f(a) & \rightarrow & c \\
  f(x) & \rightarrow & f(a) 
\end{cases} \]

The system is weakly normalising but not strongly normalising:

Can you find an infinite reduction sequence?

\[ f(b) \rightarrow f(a) \rightarrow c \]

\[ f(b) \rightarrow f(a) \rightarrow f(a) \ldots \]
1. SN $\Rightarrow$ WN
2. WN $\Rightarrow$ SN

3. Confluence $\Rightarrow$ UN
4. UN $\Rightarrow$ Confluence

5. Confluence $\Rightarrow$ Local confluence
6. Local confluence $\Rightarrow$ Confluence

7. WN & UN $\Rightarrow$ Confluence
8. WN & Local Conf. $\Rightarrow$ Confluence
9. SN & Local Conf. $\Rightarrow$ Confluence

Newman’s Lemma
Lemma

\[ \text{WN} \& \text{UN} \implies \text{CR} \]

Proof

- \( \text{WN} \implies \exists n_1, n_2: b_1 \rightarrow^{!} n_1 \text{ and } b_2 \rightarrow^{!} n_2 \)

- \( \text{UN} \implies n_1 = n_2 \implies b_1 \downarrow b_2 \)
Newman’s Lemma. *Every terminating and locally confluent ARS is confluent.*

By well-founded induction
Définition : [Relation bien fondée] Une relation d’ordre $\geqslant E \times E$ est bien fondée si il n’existe pas de suite infinie d’éléments de $E$ décroissante par rapport à $>$. 

Theorem : [Principe d’induction bien fondée] Soient donnés un ensemble $E$ quelconque, un ordre strict $<$ sur $E$ (dont $\mathcal{M}$ est son ensemble d’éléments minimaux), et une propriété $P$ sur $E$.

Si

1. pour tout élément minimal $m \in \mathcal{M}$ on a $P(m)$
2. le fait que $P(k)$ soit vérifiée pour tout élément $k < x$ implique $P(x)$

alors

pour tout $x \in E$ on a $P(x)$
Newman’s Lemma. *Every terminating and locally confluent ARS is confluent.*

\[ \text{Diagram:} \]

1. **WCR**
2. Induction hypothesis \((a \rightarrow b_1 \implies b_1 \text{ is CR})\)
3. Induction hypothesis \((a \rightarrow c_1 \implies c_1 \text{ is CR})\)
EX Say which properties hold

1. Confluent
2. Locally confluent
3. Normalizing (weakly normalizing, WN)
4. Terminating (strongly normalizing, SN)
Newman’s Lemma. Every terminating and locally confluent ARS is confluent.

A second Proof.

Let $\mathcal{A} = \langle A, \rightarrow \rangle$ terminating and locally confluent. It suffices to show that every element has unique normal forms.

- Suppose $B = \{ a \in A \mid \neg UN(a) \} \neq \emptyset$.
- Let $b \in B$ be minimal element (with respect to $\rightarrow$).
- $b \xrightarrow{\dagger} n_1$ and $b \xrightarrow{\dagger} n_2$ with $n_1 \neq n_2$.

➤ Conclude by showing that it is impossible (absurd).
Recap basics

- An abstract rewriting system (ARS) is a pair \((\mathcal{A}, \rightarrow)\) consisting of a set \(\mathcal{A}\) and a binary relation \(\rightarrow\) on \(\mathcal{A}\) whose pairs are written \(t \rightarrow s\) and called steps.

- We denote \(\rightarrow^*\) (resp. \(\rightarrow^=\)) the transitive-reflexive (resp. reflexive) closure of \(\rightarrow\). We write \(t \leftarrow u\) if \(u \rightarrow t\).

- If \(\rightarrow_1, \rightarrow_2\) are binary relations on \(\mathcal{A}\) then \(\rightarrow_1 \cdot \rightarrow_2\) denotes their composition, i.e. \(t \rightarrow_1 \cdot \rightarrow_2 s\) if there exists \(u \in \mathcal{A}\) such that \(t \rightarrow_1 u \rightarrow_2 s\).

- We write \((\mathcal{A},\{\rightarrow_1, \rightarrow_2\})\) to denote the compound system \((\mathcal{A}, \rightarrow)\) where \(\rightarrow = \rightarrow_1 \cup \rightarrow_2\).

- A \(\rightarrow\)-sequence (or reduction sequence) from \(t\) is a (possibly infinite) sequence \(t, t_1, t_2, \ldots\) such that \(t_i \rightarrow t_{i+1}\).

  - \(t \rightarrow^* s\) indicates that there is a finite sequence from \(t\) to \(s\).
  - A \(\rightarrow\)-sequence from \(t\) is maximal if it is either infinite or ends in a \(\rightarrow\)-nf.
The heart of confluence is a diamond

Prop. DIAMOND implies CONFLUENCE

Can rarely be used directly:
Most relations of interest do not satisfy it

Lemma (Characterize Confluence). \( \rightarrow \) is confluent if and only if there exists a relation \( \Rightarrow \) such that

1. \( \Rightarrow^* = \rightarrow^* \),
2. \( \Rightarrow \) is diamond.
Closure

$\rightarrow_R$ is the reflexive, transitive closure of $\rightarrow_R$:

1. $M \rightarrow_R N \Rightarrow M \rightarrow_R N$,
2. $M \rightarrow_R M$,
3. $M \rightarrow_R N, N \rightarrow_R L \Rightarrow M \rightarrow_R L$.

The transitive-reflexive closure of a relation is a closure operator, i.e.
satisfies

$\rightarrow \subseteq \rightarrow^*$, \hspace{1cm} (\rightarrow^*)^* = \rightarrow^*$, \hspace{1cm} $\rightarrow_1 \subseteq \rightarrow_2$ implies $\rightarrow_1^* \subseteq \rightarrow_2^*$

As a consequence

$(\rightarrow_1 \cup \rightarrow_2)^* = (\rightarrow_1^* \cup \rightarrow_2^*)^*$. 
Commutation. Two relations $\rightarrow_1$ and $\rightarrow_2$ on $A$ commute if

$\leftarrow_1^* \cdot \rightarrow_2^* \subseteq \rightarrow_2^* \cdot \leftarrow_1^*$.

Confluence. A relation $\rightarrow$ on $A$ is confluent if it commutes with itself.
Lemma (Hindley-Rosen)

If two relations $\rightarrow_1$ and $\rightarrow_2$ are confluent and commute with each other, then $\rightarrow_1 \cup \rightarrow_2$ is confluent.
An effective usable technique

Lemma (Hindley-Rosen)

If two relations $\rightarrow_1$ and $\rightarrow_2$ are confluent and commute with each other, then

$\rightarrow_1 \cup \rightarrow_2$ is confluent.

Global condition (all sequences)

Local condition (one-step test)

Lemma (Hindley’s local test)

Strong commutation $\leftarrow_1 \cdot \rightarrow_2 \subseteq \rightarrow_2^* \cdot \leftarrow_1^*$ implies commutation.
Lemma (Hindley-Rosen)

If two relations $\rightarrow_1$ and $\rightarrow_2$ are confluent and commute with each other, then

$\rightarrow_1 \cup \rightarrow_2$ is confluent.

Global condition (all sequences)

Local condition (one-step test)

$\leftarrow_1 \cdot \rightarrow_2 \subseteq \rightarrow_2^* \cdot \leftarrow_1 =$

(Strong Commutation)

Lemma (Local test). Strong commutation implies commutation.
Strategies
and subreductions