Sorting $\rightsquigarrow$ braids $\rightsquigarrow$ self-distributivity $\rightsquigarrow$ substitution lemma of the λ-calculus $\rightsquigarrow$ multisets

Vincent van Oostrom

Theoretical Philosophy
Universiteit Utrecht
The Netherlands
supported by LIX

January 31, 2008

Sorting

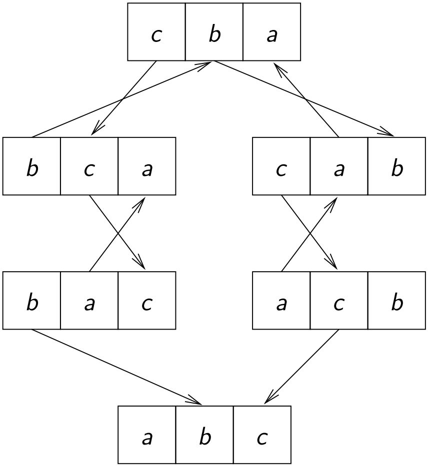
Braids

Self-distributivity

Substitution lemma of the λ-calculus

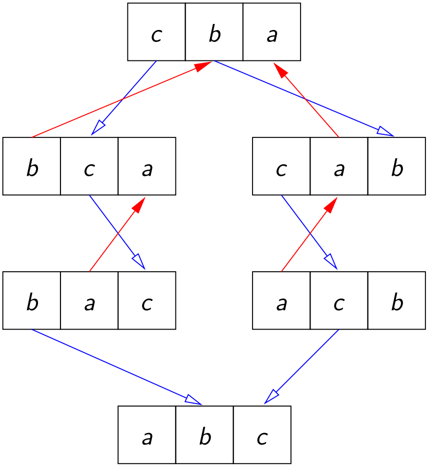
Multisets

sorting by swapping adjacent elements



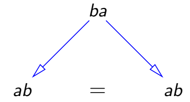
Reduction steps: arrows start at first element of swapped pair

sorting by swapping adjacent elements

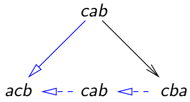


Reduction steps: inversions in blue, anti-inversions in red

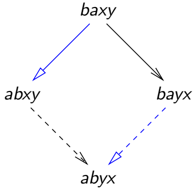
sorting local commutation diagrams



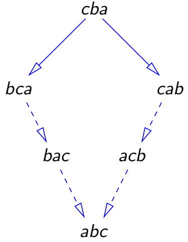
same



overlap



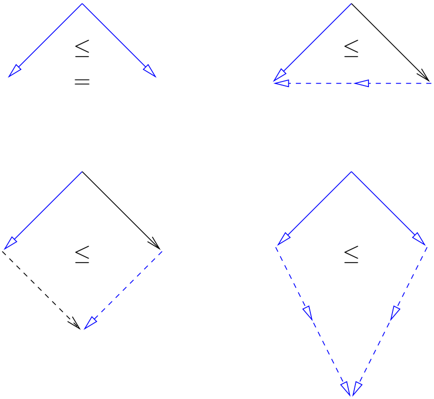
independent



self-overlap

Comparing inversions ($\swarrow$) to arbitrary reduction steps ($\searrow$)

sorting local commutation diagrams



Left path not longer than right path when closing diagram as $\searrow\swarrow$

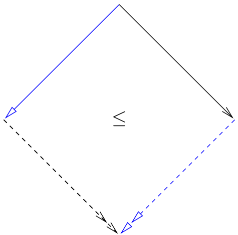
optimality of inversion sorting

Theorem

inversion sorting is optimal

Proof.

all local commutation diagrams of shape

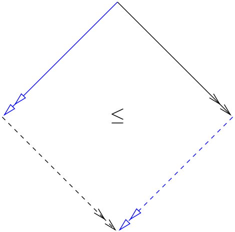


$\forall$ local peak $\exists$ valley s.t. left path not longer than right path □

optimality of inversion sorting

Theorem
inversion sorting is optimal

Proof.
all commutation diagrams of shape



$\forall$ peak $\exists$ valley s.t. left path not longer than right path $\square$

inversion local confluence diagrams

$$
\begin{tikzcd}
 & ba \arrow[dl] \arrow[dr] & \\
ab & = & ab
\end{tikzcd}
$$

same

$$
\begin{tikzcd}
 & baxy \arrow[dl] \arrow[dr] & \\
abxy \arrow[dr, dashed] & & bayx \arrow[dl, dashed] \\
 & abyx &
\end{tikzcd}
$$

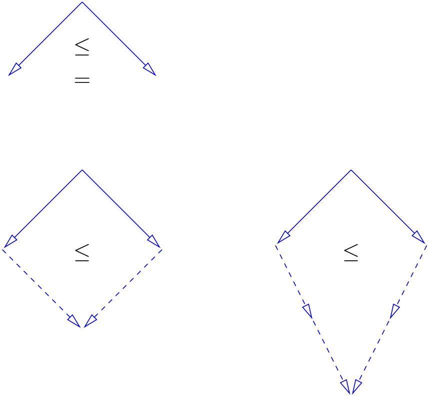
independent

$$
\begin{tikzcd}
 & cba \arrow[dl] \arrow[dr] & \\
bca \arrow[d, dashed] & & cab \arrow[d, dashed] \\
bac \arrow[dr, dashed] & & acb \arrow[dl, dashed] \\
 & abc &
\end{tikzcd}
$$

self-overlap

Comparing inversion to itself

inversion local confluence diagrams



Left path not longer than right path when closing diagram

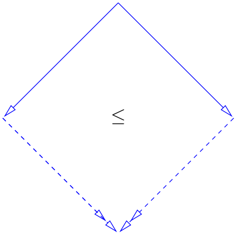
inversion sorting is $O(n^2)$

Theorem

inversion sorting is $O(n^2)$

Proof.

all sorting algorithms are $O(n^2)$ because some is (e.g. bubblesort):
all local confluence diagrams of shape



$\forall$ local peak $\exists$ valley s.t. left path not longer than right path $\square$

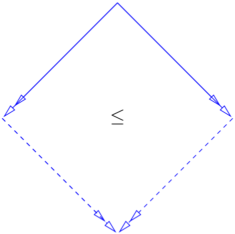
inversion sorting is $O(n^2)$

Theorem

inversion sorting is $O(n^2)$

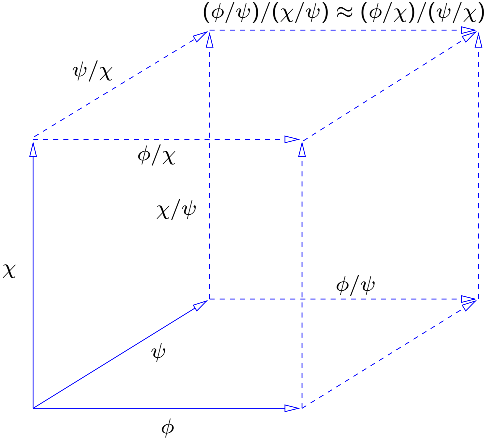
Proof.

all sorting algorithms are $O(n^2)$ because some is (e.g. bubblesort): all confluence diagrams of shape



$\forall$ peak $\exists$ valley s.t. left path not longer than right path $\square$

orthogonality of sorting



Orthogonal = to have a residual map (/) on steps

orthogonality of sorting

Definition (Residual system)

- 1 the empty step
- / the residual map from pairs of steps to steps
-

$$
\begin{array}{rcl}
\phi/\phi & \approx & 1 \\
\phi/1 & \approx & \phi \\
1/\phi & \approx & 1 \\
(\phi/\psi)/(\chi/\psi) & \approx & (\phi/\chi)/(\psi/\chi)
\end{array}
$$

orthogonality of sorting

Theorem

sorting gives a residual system

Proof.

step ϕ from list ℓ is multi-inversion: relation $\frown$ s.t. if $\widehat{ij}$

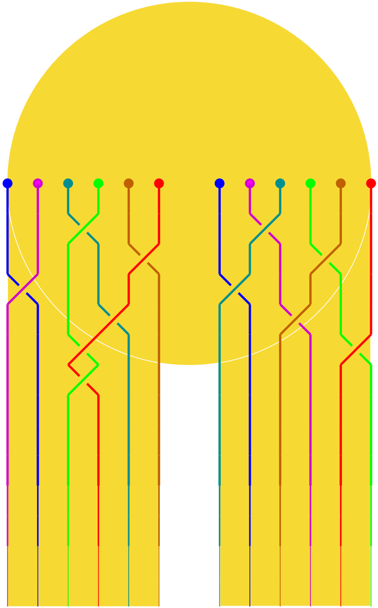
- out-of-order: $\ell = \ldots i \ldots j \ldots$ but $i > j$;
- transitive: if $\widehat{jk}$, then $\widehat{ik}$;
- scopic: if $\ell = \ldots i \ldots k \ldots j \ldots$, then either $\widehat{ik}$ or $\widehat{jk}$

define 1 to be the empty relation,
define ϕ/ψ as $(\phi \cup \psi)^+ - \psi$. $\square$

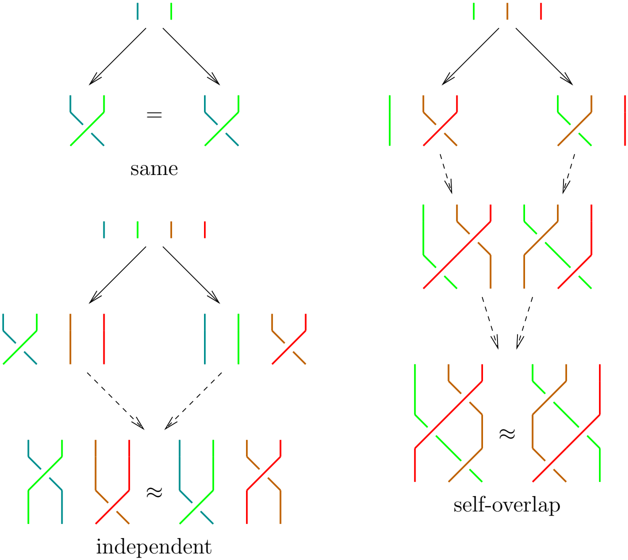
Example

$(cba \rightarrow_{\widehat{cb}a} bca)/(cba \rightarrow_{c\widehat{ba}} cab) = (cab \rightarrow_{\widehat{cab}} abc)$

braid problem

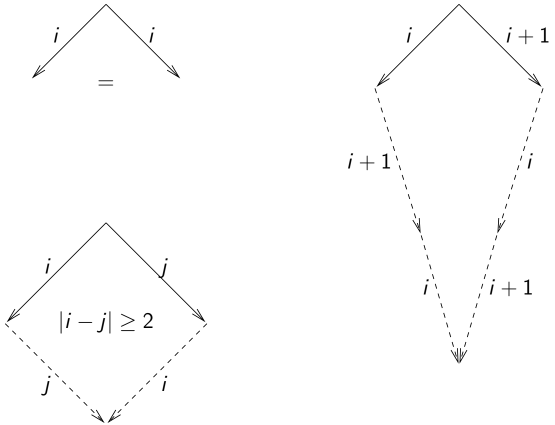


braid confluence diagrams



Reductions end in topologically equivalent (≈) braids

braid confluence diagrams



Reduction steps labelled by gap# of crossing
$ij \approx ji$ if $|i-j| \geq 2$ and $i(i+1)i \approx (i+1)i(i+1)$

sorting vs. braiding

- sorting is braiding without crossing strands (inverting) twice

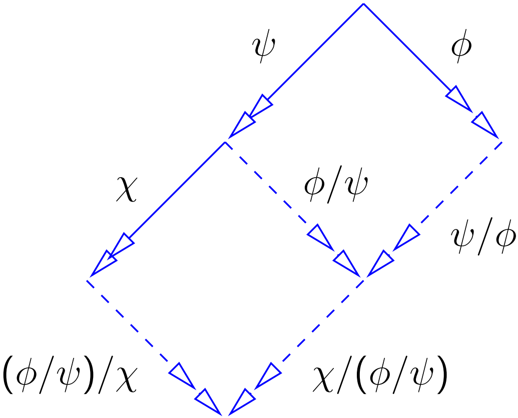
sorting vs. braiding

- sorting is braiding without crossing strands (inverting) twice
- model braids as 'repeated sorting'

sorting vs. braiding

- sorting is braiding without crossing strands (inverting) twice
- model braids as ‘repeated sorting’
- model braids as reduction sequences of multi-inversions

orthogonality of braids



$$\phi/(\psi \circ \chi) \approx (\phi/\psi)/\chi$$

$$(\psi \circ \chi)/\phi \approx (\psi/\phi) \circ (\chi/(\phi/\psi))$$

Orthogonal reduction sequences $=$ to have stepwise residuals

orthogonality of braids

Definition (Residual system with composition)

- 1 the empty reduction
- $/$ the residual map from pairs of reductions to reductions
- $\circ$ the composition map on composable reductions
- $$\begin{array}{rcl} \phi/\phi & \approx & 1 \\ \phi/1 & \approx & \phi \\ 1/\phi & \approx & 1 \\ (\phi/\psi)/(\chi/\psi) & \approx & (\phi/\chi)/(\psi/\chi) \\ 1 \circ 1 & \approx & 1 \\ \chi/(\phi \circ \psi) & \approx & (\chi/\phi)/\psi \\ (\phi \circ \psi)/\chi & \approx & (\phi/\chi) \circ (\psi/(\chi/\phi)) \end{array}$$

orthogonality of braids

Theorem

braiding gives a residual system with composition

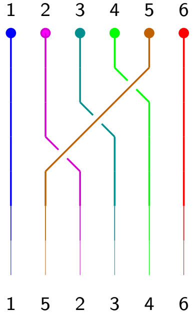
Proof.

- steps are sequences of multi-inversions
- without out-of-order restriction (omit but ...)
- define $\circ$ to be formal composition
- $/$ on sequences defined via composition laws

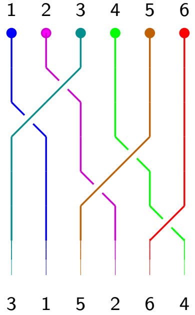
$\square$

orthogonality of braids

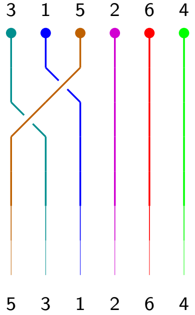
Example



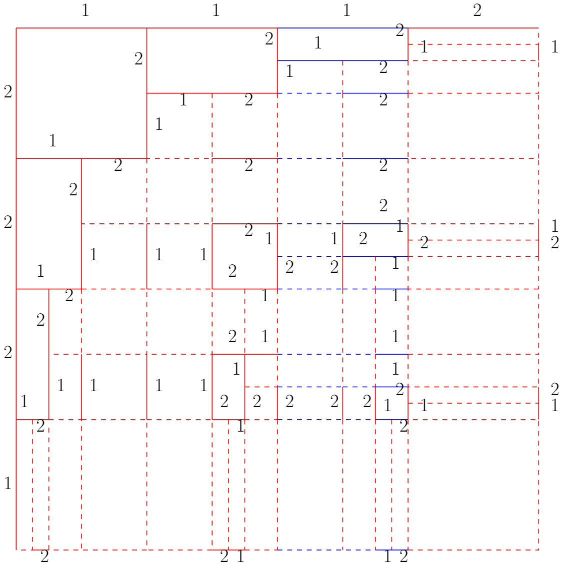
/



=



alternative route: braid completion



Adjoin 12 and 21 as atomic steps, and repeat (stops directly).

self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as first projection

self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

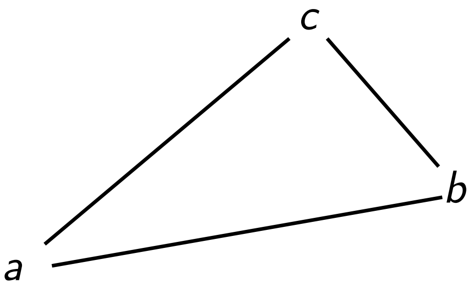
Interpret as an ACI-operation

$$\begin{aligned}
(x \cdot y) \cdot z &=_A x \cdot (y \cdot z) \\
&=_I x \cdot (y \cdot (z \cdot z)) \\
&=_A x \cdot ((y \cdot z) \cdot z) \\
&=_C x \cdot (z \cdot (y \cdot z)) \\
&=_A (x \cdot z) \cdot (y \cdot z)
\end{aligned}$$

Examples: disjunction/union, conjunction/intersection

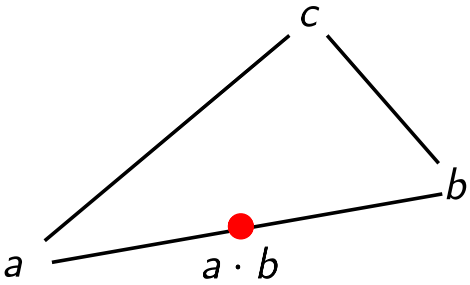
self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as 'middle'



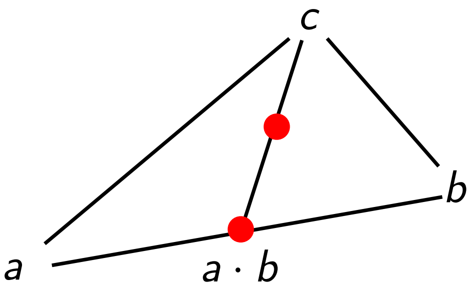
self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as ‘middle’



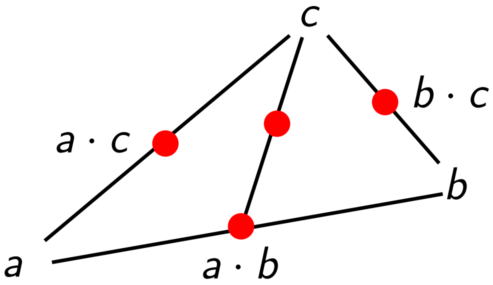
self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as ‘middle’



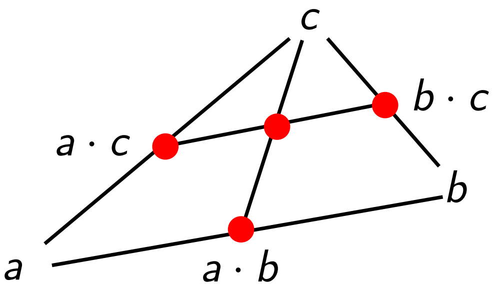
self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as 'middle'



self-distributivity: $(x \cdot y) \cdot z \approx (x \cdot z) \cdot (y \cdot z)$

Interpret as 'middle'



self-distributivity rule: $xyz \longrightarrow xz(yz)$ critical pair

- applicative notation: $\cdot$ infix, associating to left

self-distributivity rule: $xyz \longrightarrow xz(yz)$ critical pair

- applicative notation: $\cdot$ infix, associating to left
- as expansion rule better behaved than as reduction rule

self-distributivity rule: $xyz \to xz(yz)$ critical pair

- applicative notation: $\cdot$ infix, associating to left
- as expansion rule better behaved than as reduction rule
- a single critical pair:

$$
\begin{tikzcd}
 & wxyz \arrow[dl] \arrow[dr] & \\
wy(xy)z \arrow[d] & & wxz(yz) \arrow[d] \\
wyz(xyz) \arrow[d] & & wz(xz)(yz) \arrow[d] \\
wz(yz)(xyz) \arrow[rr] & & wz(yz)(xz(yz))
\end{tikzcd}
$$

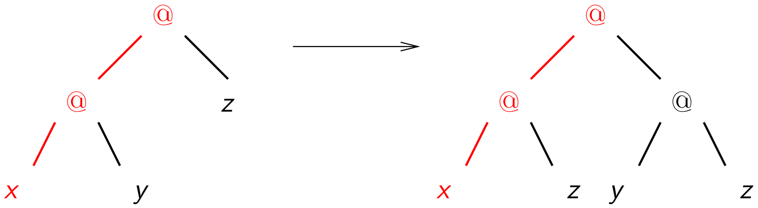
self-distributivity rule: $xyz \longrightarrow xz(yz)$ critical pair

- applicative notation: $\cdot$ infix, associating to left
- as expansion rule better behaved than as reduction rule
- a single critical pair:

$$
\begin{tikzcd}
 & wxyz \arrow[dl] \arrow[dr] & \\
wy(xy)z \arrow[d] & & wxz(yz) \arrow[d] \\
wyz(xyz) \arrow[d] & & wz(xz)(yz) \arrow[d] \\
wz(yz)(xyz) \arrow[rr] & & wz(yz)(xz(yz))
\end{tikzcd}
$$

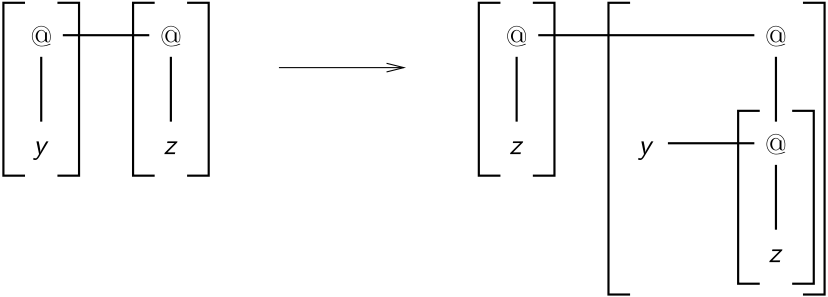
- w represents spine ...

Spine rectification



Spine is stable!

Spine rectification



If you don't have a spine, they can't break you

self-distributivity rule: $[y][z] \to [z][y[z]]$

- elements on spine juxtaposed

self-distributivity rule: $[y][z] \to [z][y[z]]$

- elements on spine juxtaposed
- rule to be applied modulo associativity

self-distributivity rule: $[y][z] \to [z][y[z]]$

- elements on spine juxtaposed
- rule to be applied modulo associativity
- the critical pair becomes:

$$\begin{tikzcd}
& {[x][y][z]} \arrow[dl] \arrow[dr] & \\
{[y][x[y]][z]} \arrow[d] & & {[x][z][y[z]]} \arrow[d] \\
{[y][z][x[y][z]]} \arrow[d] & & {[z][x[z]][y[z]]} \arrow[d] \\
{[z][y[z]][x[y][z]]} \arrow[rr] & & {[z][y[z]][x[z][y[z]]]}
\end{tikzcd}$$

self-distributivity rule: $[y][z] \to [z][y[z]]$

- elements on spine juxtaposed
- rule to be applied modulo associativity
- the critical pair becomes:

$$\begin{tikzcd}
 & {[x][y][z]} \arrow[dl, "i"'] \arrow[dr, "i+1"] & \\
{[y][x[y]][z]} \arrow[d, "i+1"'] & & {[x][z][y[z]]} \arrow[d, "i"] \\
{[y][z][x[y][z]]} \arrow[d, "i"'] & & {[z][x[z]][y[z]]} \arrow[d, "i+1"] \\
{[z][y[z]][x[y][z]]} \arrow[rr] & & {[z][y[z]][x[z][y[z]]]}
\end{tikzcd}$$

- almost braiding, but one extra step . . .

braiding vs. self-distributivity

- $[y][z] \to [z][y[z]]$ swaps z and y, remembering y crossed z...

braiding vs. self-distributivity

- $[y][z] \to [z][y[z]]$ swaps z and y, remembering y crossed z...
- braids.

braiding vs. self-distributivity

- $[y][z] \to [z][y[z]]$ swaps z and y, remembering y crossed z...
- braids.
- self-distributivity braids inside memory...

braiding vs. self-distributivity

- $[y][z] \to [z][y[z]]$ swaps z and y, remembering y crossed z...
- braids.
- self-distributivity braids inside memory...
- extra step.

orthogonality of self-distributivity

Theorem

self-distributivity gives a residual system

Idea.

Multi-distribution defined similar to multi-conversions, but

- relates positions in the (rectified) term
- may relate only to right-wing uncles; $\widehat{(piq)(pj)}$ with $i < j$
- must be left-convex; $\widehat{(piq_1q_2)(pj)}$ implies $\widehat{(piq_1)(pj)}$

/ as before; constructed by using standard residual theory to relate positions before and after the (non-linear) term rewrite step $\square$

the substitution lemma of the λ-calculus

$$\begin{tikzcd}
& (\lambda y.(\lambda x.M)N)P \arrow[dl] \arrow[dr] & \\
(\lambda x.M[y{:=}P])N[y{:=}P] \arrow[dr, dashed] & & (\lambda y.M[x{:=}N])P \arrow[dl, dashed] \\
& M[y{:=}P][x{:=}N[y{:=}P]] \approx M[x{:=}N][y{:=}P] &
\end{tikzcd}$$

Substitution Lemma of the λ-calculus

the substitution lemma of the λ-calculus

$$\begin{tikzcd}
 & (\lambda y.(\lambda x.M)N)P \arrow[dl] \arrow[dr] & \\
(\lambda x.M[y{:=}P])N[y{:=}P] \arrow[dr, dashed] & & (\lambda y.M[x{:=}N])P \arrow[dl, dashed] \\
 & M[y{:=}P][x{:=}N[y{:=}P]] \leftarrow M[x{:=}N][y{:=}P] &
\end{tikzcd}$$

Critical pair for λ-calculus with explicit substitutions

the substitution lemma of the λ-calculus

$$
\begin{tikzcd}
& (\lambda y.(\lambda x.M)N)P \arrow[dl] \arrow[dr] & \\
(\lambda x.M[y{:=}P])N[y{:=}P] \arrow[dr, dashed] & & (\lambda y.M[x{:=}N])P \arrow[dl, dashed] \\
& M[y{:=}P][x{:=}N[y{:=}P]] \leftarrow M[x{:=}N][y{:=}P] &
\end{tikzcd}
$$

Critical pair for λ-calculus with explicit substitutions
Is this rule in itself confluent? (left-to-right no)

the substitution lemma of the λ-calculus

$$\begin{tikzcd}
 & (\lambda y.(\lambda x.M)N)P \arrow[dl] \arrow[dr] & \\
(\lambda x.M[y{:=}P])N[y{:=}P] \arrow[dr, dashed] & & (\lambda y.M[x{:=}N])P \arrow[dl, dashed] \\
 & M[y{:=}P][x{:=}N[y{:=}P]] & M[x{:=}N][y{:=}P] \arrow[l]
\end{tikzcd}$$

Critical pair for λ-calculus with explicit substitutions
This is self-distributivity, so even orthogonal!

residual systems (with composition)

Definition

- 1 the empty reduction
- / the residual map from pairs of reductions to reductions
- $\circ$ the composition map on composable reductions
- $$\begin{array}{rcl} \phi/\phi & \approx & 1 \\ \phi/1 & \approx & \phi \\ 1/\phi & \approx & 1 \\ (\phi/\psi)/(\chi/\psi) & \approx & (\phi/\chi)/(\psi/\chi) \\ 1 \circ 1 & \approx & 1 \\ \chi/(\phi \circ \psi) & \approx & (\chi/\phi)/\psi \\ (\phi \circ \psi)/\chi & \approx & (\phi/\chi) \circ (\psi/(\chi/\phi)) \end{array}$$

Union a defined operation: $\phi \cup \psi = \phi \circ (\psi/\phi)$ (pushout)

residual systems (with composition)

Example

- multi-inversions in sorting

residual systems (with composition)

Example

- multi-inversions in sorting
- braids

residual systems (with composition)

Example

- multi-inversions in sorting
- braids
- self-distributivity

residual systems (with composition)

Example

- multi-inversions in sorting
- braids
- self-distributivity
- orthogonal term rewriting systems (β-reduction, CL)

residual systems (with composition)

Example

- multi-inversions in sorting
- braids
- self-distributivity
- orthogonal term rewriting systems (β-reduction, CL)
- associativity

residual systems (with composition)

Example

- multi-inversions in sorting
- braids
- self-distributivity
- orthogonal term rewriting systems (β-reduction, CL)
- associativity
- ...

residual systems (with composition)

Example

- multi-inversions in sorting
- braids
- self-distributivity
- orthogonal term rewriting systems (β-reduction, CL)
- associativity
- ...
- also many residual algebras (singleton carrier) ...

residual algebras (with composition)

- natural numbers (as steps from object to itself)
- $\dot{-}$ (cut-off subtraction), 0 (zero), $+$ (addition);

$$
\begin{aligned}
n \dot{-} n &\approx 0 \\
n \dot{-} 0 &\approx n \\
0 \dot{-} n &\approx 0 \\
(n \dot{-} m) \dot{-} (k \dot{-} m) &\approx (n \dot{-} k) \dot{-} (m \dot{-} k) \\
0 + 0 &\approx 0 \\
k \dot{-} (n + m) &\approx (k \dot{-} n) \dot{-} m \\
(n + m) \dot{-} k &\approx (n \dot{-} k) + (m \dot{-} (k \dot{-} n))
\end{aligned}
$$

Generated from its

residual algebras (with composition)

- natural numbers (as steps from object to itself)
- $\dot{-}$ (cut-off subtraction), 0 (zero), $+$ (addition);

$$
\begin{array}{rcl}
n \dot{-} n & \approx & 0 \\
n \dot{-} 0 & \approx & n \\
0 \dot{-} n & \approx & 0 \\
(n \dot{-} m) \dot{-} (k \dot{-} m) & \approx & (n \dot{-} k) \dot{-} (m \dot{-} k) \\
0 + 0 & \approx & 0 \\
k \dot{-} (n + m) & \approx & (k \dot{-} n) \dot{-} m \\
(n + m) \dot{-} k & \approx & (n \dot{-} k) + (m \dot{-} (k \dot{-} n))
\end{array}
$$

Truth-values with reverse implication, false (no composition)

Positive natural numbers with cut-off division, 1, multiplication

residual algebras (with composition)

- multisets over some set (as steps from object to itself)
- $-$ (multiset difference), $\emptyset$ (empty multiset), $\uplus$ (multiset sum);

$$
\begin{array}{rcl}
M - M & \approx & \emptyset \\
M - \emptyset & \approx & M \\
\emptyset - M & \approx & \emptyset \\
(M - N) - (K - N) & \approx & (M - K) - (N - K) \\
\emptyset \uplus \emptyset & \approx & \emptyset \\
K - (M \uplus N) & \approx & (K - M) - N \\
(M \uplus N) - K & \approx & (M - K) \uplus (N - (K - M))
\end{array}
$$

residual algebras (with composition)

- multisets over some set (as steps from object to itself)
- $-$ (multiset difference), $\emptyset$ (empty multiset), $\uplus$ (multiset sum);

$$
\begin{array}{rcl}
M - M & \approx & \emptyset \\
M - \emptyset & \approx & M \\
\emptyset - M & \approx & \emptyset \\
(M - N) - (K - N) & \approx & (M - K) - (N - K) \\
\emptyset \uplus \emptyset & \approx & \emptyset \\
K - (M \uplus N) & \approx & (K - M) - N \\
(M \uplus N) - K & \approx & (M - K) \uplus (N - (K - M))
\end{array}
$$

Sets with set-difference, $\emptyset$, disjoint union.

residual algebras (with composition)

- multisets over some set (as steps from object to itself)
- $-$ (multiset difference), $\emptyset$ (empty multiset), $\uplus$ (multiset sum);

$$
\begin{array}{rcl}
M - M & \approx & \emptyset \\
M - \emptyset & \approx & M \\
\emptyset - M & \approx & \emptyset \\
(M - N) - (K - N) & \approx & (M - K) - (N - K) \\
\emptyset \uplus \emptyset & \approx & \emptyset \\
K - (M \uplus N) & \approx & (K - M) - N \\
(M \uplus N) - K & \approx & (M - K) \uplus (N - (K - M))
\end{array}
$$

all compositions are commutative

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$\begin{array}{rcl}(\phi/\psi)/\phi & \approx & 1 \\ \phi/(\phi/\psi) & \approx & \psi/(\psi/\phi)\end{array}$$

(follows from computing $(\phi \circ \psi)/(\psi \circ \phi) \approx 1$!)

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$
\begin{aligned}
(\phi/\psi)/\phi &\approx 1 \\
\phi/(\phi/\psi) &\approx \psi/(\psi/\phi)
\end{aligned}
$$

- 2nd equation states commutativity of intersection $\phi/(\phi/\psi)$

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$\begin{aligned} (\phi/\psi)/\phi &\approx 1 \\ \phi/(\phi/\psi) &\approx \psi/(\psi/\phi) \end{aligned}$$

- 2nd equation states commutativity of intersection $\phi/(\phi/\psi)$
- Very useful for equational reasoning about multisets in Coq.

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$
\begin{aligned}
(\phi/\psi)/\phi &\approx 1 \\
\phi/(\phi/\psi) &\approx \psi/(\psi/\phi)
\end{aligned}
$$

- 2nd equation states commutativity of intersection $\phi/(\phi/\psi)$
- Very useful for equational reasoning about multisets in Coq.
- Iso to commutative BCK algebras with relative cancellation

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$\begin{array}{rcl} (\phi/\psi)/\phi & \approx & 1 \\ \phi/(\phi/\psi) & \approx & \psi/(\psi/\phi) \end{array}$$

- 2nd equation states commutativity of intersection $\phi/(\phi/\psi)$
- Very useful for equational reasoning about multisets in Coq.
- Iso to commutative BCK algebras with relative cancellation
- In above examples $\preceq$ well-founded; $a \preceq b$ if $a/b \approx 1$.

commutative residual algebras

Definition

commutative residual algebra with composition (CRAC) satisfies

$$\begin{array}{rcl} (\phi/\psi)/\phi & \approx & 1 \\ \phi/(\phi/\psi) & \approx & \psi/(\psi/\phi) \end{array}$$

- 2nd equation states commutativity of intersection $\phi/(\phi/\psi)$
- Very useful for equational reasoning about multisets in Coq.
- Iso to commutative BCK algebras with relative cancellation
- In above examples $\preceq$ well-founded; $a \preceq b$ if $a/b \approx 1$.
- Other interesting CRACs?

CRAs are multisets

Theorem

every well-founded CRAC iso to multiset CRAC

Proof.

The following axioms hold

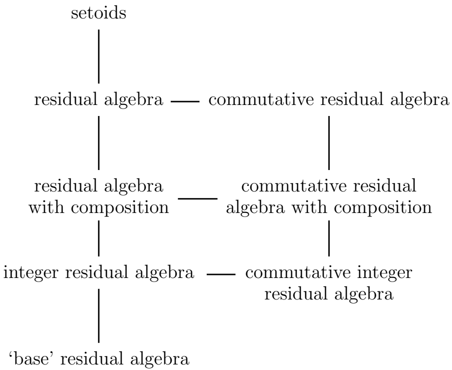
- $\preceq$ well-founded partial-order
- 1 least
- strictly compatible: $\phi \prec \psi \;\Rightarrow\; \phi \circ \chi \prec \psi \circ \chi$
- precompositional: $\phi \preceq \psi \circ \chi \;\Rightarrow\; \phi = \psi' \circ \chi',\, \psi' \preceq \psi,\, \chi' \preceq \chi$
- Archimedean: $\forall n\ \phi^n \preceq \psi \;\Rightarrow\; \phi = 1$.

so every element uniquely decomposes into atoms □

Unique decomposition result generalises FTA; also applies to process algebra

well-founded CRAs are multisets

Formalisation



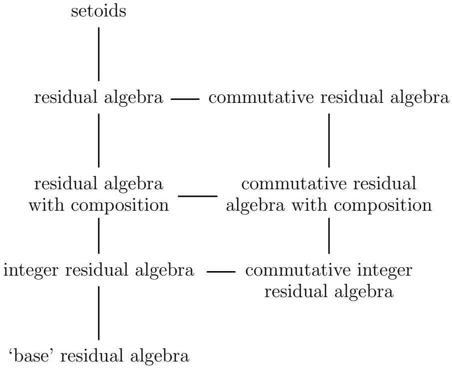

```
Eval compute in 17 ∧ 20.
Eval compute in 32 ∧ 18.
Eval compute in 5 ∧ 5.
```

Formalisation

$$
\begin{tikzcd}
\text{setoids} \arrow[d, dash] & \\
\text{residual algebra} \arrow[r, dash] \arrow[d, dash] & \text{commutative residual algebra} \arrow[d, dash] \\
\begin{array}{c}\text{residual algebra}\\ \text{with composition}\end{array} \arrow[r, dash] \arrow[d, dash] & \begin{array}{c}\text{commutative residual}\\ \text{algebra with composition}\end{array} \arrow[d, dash] \\
\text{integer residual algebra} \arrow[r, dash] \arrow[d, dash] & \begin{array}{c}\text{commutative integer}\\ \text{residual algebra}\end{array} \\
\text{`base' residual algebra} &
\end{tikzcd}
$$

Covers Visser's stack numbers

Formalisation

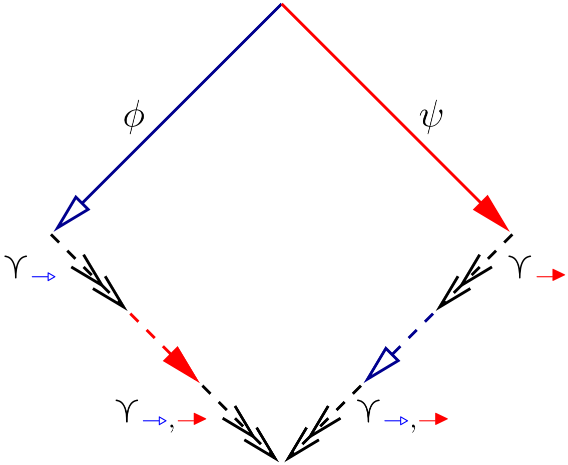


Multiple inheritance?

Conclusion

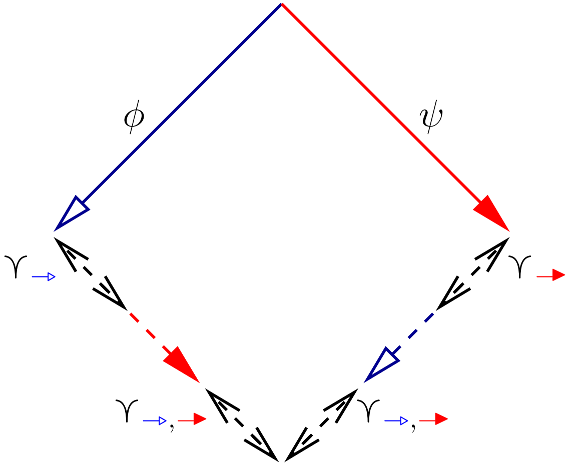
- connected and studied systems from diverse fields via residual systems
- 'more' examples of residual systems/algebras than expected
- algebras useful for equational reasoning with 'minus'
- do residuals come before or after composition?

decreasing diagrams theorem



$\prec$ well-founded order on labels in A $\Rightarrow$ $\bigcup A$ confluent

decreasing diagrams theorem



$\prec$ well-founded order on labels in $A \Rightarrow \bigcup A$ confluent
covers all 'local confluence $\Rightarrow$ confluence' results in Terese Ch1.