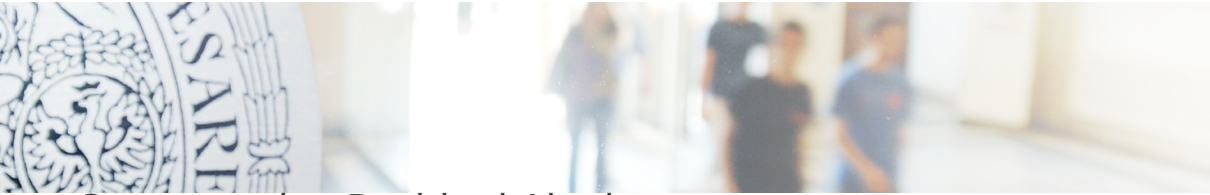
universität
innsbruck



Commutative Residual Algebras

Vincent van Oostrom

http://cl-informatik.uibk.ac.at

1. Commutative residual algebras
2. Derived properties and operations
3. Unique decomposition if well-founded
4. Inclusion/exclusion principle
5. EWD1313
6. cBCK algebras with relative cancellation
7. Residual systems

Commutative residual algebra (CRA)

Definition (CRA)

algebra $\langle A, 1, / \rangle$ with unit 1 ('one') and residual $/$ (pronounce a/b as 'a after b') for all $a, b, c \in A$:

$$a/1 = a \tag{1}$$
$$a/a = 1 \tag{2}$$
$$1/a = 1 \tag{3}$$
$$(a/b)/(c/b) = (a/c)/(b/c) \tag{4}$$
$$(a/b)/a = 1 \tag{5}$$
$$a/(a/b) = b/(b/a) \tag{6}$$

Commutative residual algebra (CRA)

Definition (CRA)

algebra $\langle A, 1, / \rangle$ with unit 1 and residual $/$
for all $a, b, c \in A$:

$$a/1 = a \tag{1}$$
$$(a/b)/(c/b) = (a/c)/(b/c) \tag{4}$$
$$(a/b)/a = 1 \tag{5}$$
$$a/(a/b) = b/(b/a) \tag{6}$$

Remark

(2) and (3) derivable by $a/a \overset{(1)}{=} (a/1)/a \overset{(5)}{=} 1$ *and* $1/a \overset{(1)}{=} (1/a)/1 \overset{(5)}{=} 1$
each among (1),(4),(5),(6) independent of others (easy models).

Examples of CRAs

Example

CRA $\langle \mathbb{N}, 0, \dot{-} \rangle$ of natural numbers $\mathbb{N}$ with zero 0 and monus $\dot{-}$ (cut-off minus)

Examples of CRAs

Example

CRA $\langle \mathbb{N}, 0, \dot{-} \rangle$ of natural numbers $\mathbb{N}$ with zero 0 and monus $\dot{-}$
for all $n, m, k \in \mathbb{N}$:

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

by cases on total $\leq$-order of n, m, k
for instance $3 \leq 5$, so $5 \dot{-} (5 \dot{-} 3) = 3 = 3 \dot{-} 0 = 3 \dot{-} (3 \dot{-} 5)$

Examples of CRAs

Example

CRA $\langle \mathbb{N}_{\leq N}, 0, \dot{-} \rangle$ of natural numbers $\leq N$ with zero 0 and monus $\dot{-}$
for all $n, m, k \in \mathbb{N}_{\leq N}$:

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

by cases on total $\leq$-order of n, m, k in $\mathbb{N}_{\leq N}$, as for $\mathbb{N}$
$\mathbb{N}_{\leq N}$ not closed under $+$ or $\cdot$, but closed under 0 and $\dot{-}$; initial segment of $\mathbb{N}$

Examples of CRAs

Example

CRA $\langle \mathbb{R}_{\geq 0}, 0, \dot{-} \rangle$ of non-negative real numbers $\mathbb{R}_{\geq 0}$ with zero 0 and monus $\dot{-}$ for all $x, y, z \in \mathbb{R}_{\geq 0}$:

$$
\begin{aligned}
x \dot{-} 0 &= x \\
(x \dot{-} y) \dot{-} (z \dot{-} y) &= (x \dot{-} z) \dot{-} (y \dot{-} z) \\
(x \dot{-} y) \dot{-} x &= 0 \\
x \dot{-} (x \dot{-} y) &= y \dot{-} (y \dot{-} x)
\end{aligned}
$$

by cases on total $\leq$-order of x, y, z in $\mathbb{R}_{\geq 0}$, as for $\mathbb{N}$ and $\mathbb{N}_{\leq N}$
same for initial segment $[0, R]$ of $\mathbb{R}_{\geq 0}$

Examples of CRAs

Example

CRA $\langle \mathsf{Mst}(A), \emptyset, - \rangle$ of multisets over A with empty multiset $\emptyset$ and difference $-$ for all $M, N, L \in \mathsf{Mst}(A)$:

$$
\begin{aligned}
M - \emptyset &= M \\
(M - N) - (L - N) &= (M - L) - (N - L) \\
(M - N) - M &= \emptyset \\
M - (M - N) &= N - (N - M)
\end{aligned}
$$

seen to hold by pointwise extending CRA on $\mathbb{N}$ (viewing $\mathsf{Mst}(A)$ as $A \to \mathbb{N}$)
multisets have finite multiplicities but may have infinite support

Examples of CRAs

Example

CRA $\langle \wp(A), \emptyset, - \rangle$ of subsets of A with empty set $\emptyset$ and difference $-$
for all $B, C, D \subseteq A$:

$$
\begin{aligned}
B - \emptyset &= B \\
(B - C) - (D - C) &= (B - D) - (C - D) \\
(B - C) - B &= \emptyset \\
B - (B - C) &= C - (C - B)
\end{aligned}
$$

seen to hold by pointwise extending CRA on $\mathbb{N}_{\leq 1}$ (viewing $\wp(A)$ as $A \to \{0, 1\}$)
CRA $\langle \{\bot, \top\}, \top, \leftarrow \rangle$ of booleans with top $\top$ and rev. implication $\leftarrow$ ($\{*\}$-subsets)

Examples of CRAs

Definition

algebra $\mathcal{A}$ is collection of subsets of ambient set A containing A and closed under union and complement with respect to A

formally, $\mathcal{A}$ sub-algebra of the Boolean algebra $\wp(A)$
simple case of algebra in measure theory where closed under countable union

Examples of CRAs

Definition

algebra $\mathcal{A}$ is collection of subsets of ambient set A containing A and closed under union and complement with respect to A

Definition

multiset M is $\mathcal{A}$-measurable if

- $M^i \in \mathcal{A}$ for each i, with $M^i := \{a \mid M(a) = i\}$ (set at height i of M)
- $M^{>i} = \emptyset$ for some i, with $M^{>i} := \bigcup_{j>i} M^j = \{a \mid M(a) > i\}$ (least i is height of M)

the M^i partition A; $M^{>0}$ is support of M; M empty iff height 0

Examples of CRAs

Example

CRA $\langle \mathsf{Mst}(\mathcal{A}), \emptyset, - \rangle$ of $\mathcal{A}$-measurable multisets, for all $M, N, L \in \mathsf{Mst}(\mathcal{A})$:

$$
\begin{aligned}
M - \emptyset &= M \\
(M - N) - (L - N) &= (M - L) - (N - L) \\
(M - N) - M &= \emptyset \\
M - (M - N) &= N - (N - M)
\end{aligned}
$$

because hold for multisets and $\mathcal{A}$-measurable multisets closed under $\emptyset$ and $-$:

- $\emptyset^0 = A \in \mathcal{A}$ and $\emptyset^{>0} = \emptyset = A - A \in \mathcal{A}$;
- if M, N $\mathcal{A}$-measurable $(M - N)^i = \bigcup_{j-k=i} M^j \cap N^k \in \mathcal{A}$ and height below M

Examples of CRAs

Example

CRA $\langle \mathsf{Pos}, 1, \cdot/ \rangle$ of positive natural numbers Pos with one 1 and division $\cdot/$

cut-off division $n \cdot/ m := \frac{n}{\gcd(n,m)}$; for instance $15 \cdot/ 6 := \frac{15}{\gcd(15,6)} = \frac{15}{3} = 5$.

Examples of CRAs

Example

CRA $\langle \text{Pos}, 1, \cdot\!/ \rangle$ of positive natural numbers Pos with one 1 and dovision $\cdot\!/$
for all $n, m, k \in \text{Pos}$:

$$
\begin{aligned}
n \cdot\!/\, 1 &= n \\
(n \cdot\!/\, m) \cdot\!/\, (k \cdot\!/\, m) &= (n \cdot\!/\, k) \cdot\!/\, (m \cdot\!/\, k) \\
(n \cdot\!/\, m) \cdot\!/\, n &= 1 \\
n \cdot\!/\, (n \cdot\!/\, m) &= m \cdot\!/\, (m \cdot\!/\, n)
\end{aligned}
$$

view positive natural number as multiset of prime factors
then 1 corresponds to $\emptyset$ and $\cdot\!/$ to $-$
same for initial segment of Pos

Natural order $\leqslant$

Definition (natural order)

$a \leqslant b := a/b = 1$

Natural order $\leqslant$

Definition (natural order)

$a \leqslant b := a/b = 1$

Lemma

natural order $\leqslant$ is a partial order

Proof.

(reflexivity) $a \leqslant a \iff a/a \overset{(2)}{=} 1$;

(transitivity) $a \leqslant b \leqslant c \iff a/b = 1$ and $b/c = 1 \implies$
$a/c \overset{(1),\text{ass}}{=} (a/c)/(b/c) \overset{(4)}{=} (a/b)/(c/b) \overset{\text{ass},(3)}{=} 1 \iff a \leqslant b$;

(anti-symmetry) $a \leqslant b \leqslant a \iff a/b = 1$ and $b/a = 1 \implies$
$a \overset{(1),\text{ass}}{=} a/(a/b) \overset{(6)}{=} b/(b/a) \overset{\text{ass},(1)}{=} b$ □

Natural order $\leqslant$

Definition (natural order)

$a \leqslant b := a/b = 1$

Lemma

natural order $\leqslant$ is a partial order

Example

CRA	$\mathbb{N}$	$\mathbb{R}_{\geq 0}$	Mst	Pos
natural order $\leqslant$	less–than–or–equal $\leq$	idem	sub-multiset $\subseteq$	divisibility $\mid$
total?	✓	✓		
well-founded?	✓		✓(on finite)	✓

Meet $\wedge$

Definition (meet)

$a \wedge b := a/(a/b)$

Meet $\wedge$

Definition (meet)

$a \wedge b := a/(a/b)$

Lemma

$\langle A, \wedge \rangle$ is a meet-semilattice, and $a \leqslant b \iff a = a \wedge b$

Proof (of first part).

(idempotent) $a \wedge a \overset{\text{def}}{=} a/(a/a) \overset{(2)}{=} a/1 \overset{(1)}{=} a$

(commutative) $a \wedge b \overset{\text{def}}{=} a/(a/b) \overset{(6)}{=} b/(b/a) \overset{\text{def}}{=} b \wedge a$ (reason for naming CRA)

(associative) $a \wedge (b \wedge c) \overset{\text{com},\text{def}}{=} (b \wedge c)/((b \wedge c)/a) \overset{\text{def},(*)}{=} (b/(b/c))/((b/a)/(b/c))$
$\overset{(4)}{=} (b/(b/a))/((b/c)/(b/a)) \overset{(*),\text{def}}{=} (b \wedge a)/((b \wedge a)/c) \overset{\text{def},\text{com}}{=} (a \wedge b) \wedge c$
using $(a/b)/c \overset{(*)}{=} (a/c)/b$ twice $\square$

Meet $\wedge$

Definition (meet)

$a \wedge b := a/(a/b)$

Example

CRA	$\mathbb{N}$	$\mathbb{R}_{\geq 0}$	Mst	Pos
meet $\wedge$	minimum min	idem	intersection $\cap$	greatest–common–divisor gcd

on $\{\bot, \top\}$ with $\top$ and $\leftarrow$, meet is inclusive–or ($\vee$)

Product $\cdot$

Definition (product)

$a \cdot b$ denotes c such that $a/c = 1$ and $c/a = b$

Product $\cdot$

Definition (product)

$a \cdot b$ denotes c such that $a/c = 1$ and $c/a = b$

Remark (product is partial function)

(partial) $3 \cdot 4$ *does not exist in initial segment* ≤ 5 *of* Pos*;*

(function) suppose $a/d = 1$ *and* $d/a = b$*. by (anti-)symmetry* $c \leqslant d$ *suffices. follows from* $c/d \overset{(1),ass}{=} (c/d)/(a/d) \overset{(4),ass}{=} (c/a)/b \overset{ass,(2)}{=} 1$

product typically partial on initial segments (e.g. pract/philosophical motivation)

Product $\cdot$

Definition (product)

$a \cdot b$ denotes c such that $a/c = 1$ and $c/a = b$

Lemma

$\langle A, 1, \cdot \rangle$ is a partial commutative monoid, and $a \leqslant b \iff b \simeq a \cdot (b/a)$

$\simeq$ is Kleene equality: if one side denotes, then other side too with same value
here denoting is strict: to denote includes all sub-expressions denoting

$b \simeq a \cdot (b/a)$ expresses that $a \cdot (b/a)$ exists/denotes since b does

compatible with $\leqslant$: if $c \leqslant a$ and $a \cdot b$ denotes then $c \cdot b$ too, namely $(a \cdot b)/(a/c)$

Product $\cdot$

Definition (product)

$a \cdot b$ denotes c such that $a/c = 1$ and $c/a = b$

Lemma

$\langle A, 1, \cdot \rangle$ is a partial commutative monoid, and $a \leqslant b \iff b \simeq a \cdot (b/a)$

Proof (of first part).

(commutative) to show $a \cdot b \simeq b \cdot a$, assume $c \simeq a \cdot b$, i.e. $a/c = 1$ and $c/a = b$.
then $b/c \overset{\text{ass},(5)}{=} 1$ and $c/b \overset{\text{ass},(6)}{=} a/(a/c) \overset{\text{ass},(1)}{=} a$, so also $c \simeq b \cdot a$;

(unit) $a/a \overset{(2)}{=} 1$, so $a \simeq a \cdot 1$ (left/right product with 1 always exists);

(transitive) if $d \simeq (a \cdot b) \cdot c$, then $d/a \simeq b \cdot c$ and $d \simeq a \cdot (b \cdot c)$ $\square$

Product $\cdot$

Definition (product)

$a \cdot b$ denotes c such that $a/c = 1$ and $c/a = b$

Lemma

$\langle A, 1, \cdot \rangle$ is a partial commutative monoid, and $a \leqslant b \iff b \simeq a \cdot (b/a)$

Example

CRA	$\mathbb{N}$	$\mathbb{R}_{\geq 0}$	Mst	Pos
product $\cdot$	sum $+$	idem	sum $\uplus$	product $\cdot$

on booleans $\{\bot, \top\}$ with $\top$ and $\leftarrow$, product is partial and (partial on $\bot, \bot$)

on sets $\wp(A)$ with $\emptyset$ and $-$, product is disjoint union (partial on non-disjoint sets)

Join $\vee$

Definition (join)

$a \vee b$ denotes $a \cdot (b / a)$

Join $\vee$

Definition (join)

$a \vee b$ denotes $a \cdot (b/a)$

Remark (join is partial function)

(partial) $\mathrm{lcm}(3,4)$ *does not exist in initial segment* ≤ 5 *of* Pos*; another example:* $\{a\} \cup \{b\}$ *does not exist in initial segment of* $\wp(\{a,b\})$ *with cardinality* ≤ 1

(function) because defined in terms of product $\cdot$*, which is a partial function*

join typically partial on initial segments

Join $\vee$

Definition (join)

$a \vee b$ denotes $a \cdot (b/a)$

Lemma

$\langle A, \vee \rangle$ is a partial join-semilattice with neutral 1*, and* $a \leqslant b \iff a \vee b \simeq b$

compatible with $\leqslant$: if $c \leqslant a$ and $a \vee b$ denotes then $c \vee b$ too (as holds for product)

Join $\vee$

Definition (join)

$a \vee b$ denotes $a \cdot (b/a)$

Lemma

$\langle A, \vee \rangle$ *is a partial join-semilattice with neutral* 1, *and* $a \leqslant b \iff a \vee b \simeq b$

Proof (of some parts).

(idempotent) a is the join of a with itself: $a/a \overset{(2)}{=} 1$ and $a/a \overset{\text{refl}}{=} a/a$;

(commutative) if $a \vee b := a \cdot (b/a)$ denotes, $b/(a \cdot (b/a)) \overset{(7),(2)}{=} 1$ and $(a \cdot (b/a))/b \overset{(8)}{=} (a/b) \cdot ((b/a)/(b/a)) \overset{(2),\text{unit}}{=} a/b$, so $b \vee a$ denotes, using

$$c/(a \cdot b) = (c/a)/b \tag{7}$$

$$(a \cdot b)/c = (a/c) \cdot (b/(c/a)) \tag{8}$$

Join $\vee$

Definition (join)

$a \vee b$ denotes $a \cdot (b/a)$

Lemma

$\langle A, \vee \rangle$ is a partial join-semilattice with neutral 1*, and* $a \leqslant b \iff a \vee b \simeq b$

Example

CRA	$\mathbb{N}$	$\mathbb{R}_{\geq 0}$	Mst	Pos
join $\vee$	maximum max	idem	union $\cup$	least–common–multiple lcm

on booleans $\{\bot, \top\}$ with $\top$ and $\leftarrow$, join is and

on sets $\wp(A)$ with $\emptyset$ and $-$, join is union

Unique decompositions

Definition

for $\langle A, 1, \cdot \rangle$ a partial commutative monoid

- a is indecomposable if $a \neq 1$ and $a = b \cdot c$ implies $b = 1$ or $c = 1$;
- multiset $[a_1, \ldots, a_n]$ decomposition of a if a_i indecomposable, $a \simeq a_1 \cdot \ldots \cdot a_n$.

definition of indecomposable coincides with that of irreducible for rings

Unique decompositions

Definition

for $\langle A, 1, \cdot \rangle$ a partial commutative monoid

- a is indecomposable if $a \neq 1$ and $a = b \cdot c$ implies $b = 1$ or $c = 1$;
- multiset $[a_1, \ldots, a_n]$ decomposition of a if a_i indecomposable, $a \simeq a_1 \cdot \ldots \cdot a_n$.

Question

do CRAs have unique decomposition?

Unique decompositions

Definition

for $\langle A, 1, \cdot \rangle$ a partial commutative monoid

- a is indecomposable if $a \neq 1$ and $a = b \cdot c$ implies $b = 1$ or $c = 1$;
- multiset $[a_1, \ldots, a_n]$ decomposition of a if a_i indecomposable, $a \simeq a_1 \cdot \ldots \cdot a_n$.

Question

do CRAs have unique decomposition?

no, CRA $\mathbb{R}_{\geq 0}$ does not have any indecomposables
note the natural order $\leqslant$ is not well-founded on $\mathbb{R}_{\geq 0}$

Unique decompositions

Definition

for $\langle A, 1, \cdot \rangle$ a partial commutative monoid

- a is indecomposable if $a \neq 1$ and $a = b \cdot c$ implies $b = 1$ or $c = 1$;
- multiset $[a_1, \ldots, a_n]$ decomposition of a if a_i indecomposable, $a \simeq a_1 \cdot \ldots \cdot a_n$.

Question

do well-founded CRAs have unique decomposition?

Unique decompositions

Definition

for $\langle A, 1, \cdot \rangle$ a partial commutative monoid

- a is indecomposable if $a \neq 1$ and $a = b \cdot c$ implies $b = 1$ or $c = 1$;
- multiset $[a_1, \ldots, a_n]$ decomposition of a if a_i indecomposable, $a \simeq a_1 \cdot \ldots \cdot a_n$.

Question

do well-founded CRAs have unique decomposition?

yes, but how to prove?
unique decomposition holds for unique factorisation domains but CRAs different structure (partial operations; no ring). instead will rely on $\leqslant$ being decomposition order on the partial commutative monoid $\langle A, 1, \cdot \rangle$

Unique decomposition by decomposition order

Definition (for partial order $\preccurlyeq$ on partial commutative monoid $\langle A, 1, \cdot \rangle$)

(well-founded) no infinite descending $\prec$-chains;

(least) $1 \preccurlyeq a$ for all a;

(strictly compatible) if $a \prec b$ and $b \cdot c$ defined, then $a \cdot c$ defined and $a \cdot c \prec b \cdot c$;

(Riesz decomposition) if $a \preccurlyeq b \cdot c$, then $a = b' \cdot c'$ for some $b' \preccurlyeq b$ and $c' \preccurlyeq c$;

(Archimedean) if a^n defined and $a^n \prec b$ for all n, then $a = 1$.

Unique decomposition by decomposition order

Definition (for partial order $\preccurlyeq$ on partial commutative monoid $\langle A, 1, \cdot \rangle$)

(well-founded) no infinite descending $\prec$-chains;

(least) $1 \preccurlyeq a$ for all a;

(strictly compatible) if $a \prec b$ and $b \cdot c$ defined, then $a \cdot c$ defined and $a \cdot c \prec b \cdot c$;

(Riesz decomposition) if $a \preccurlyeq b \cdot c$, then $a = b' \cdot c'$ for some $b' \preccurlyeq b$ and $c' \preccurlyeq c$;

(Archimedean) if a^n defined and $a^n \prec b$ for all n, then $a = 1$.

Theorem (Luttik & vO 05)

$\langle A, 1, \cdot \rangle$ has unique decomposition iff it has a decomposition order

Proof.

Milner's technique; does not rely on cancellation (if $a \cdot c = b \cdot c$, then $a = b$). □

Unique decomposition by decomposition order

Theorem (Luttik & vO 05)

$\langle A, 1, \cdot \rangle$ *has unique decomposition iff it has a decomposition order*

Example

- divisibility on $\langle \mathrm{Pos}, 1, \cdot \rangle$ is a decomposition order
  unique decomposition into prime factors (FTA, Euclid c. 300 BC)
- unique decomposition as parallel composition of sequential processes
  CCS (Milner & Moller 93), BPP (Christensen 93), ACP^{ϵ} (L & vO 05)
- substate on separation algebras in (Calcagno, O'Hearn & Yang 07)
  partial functions with finite domains; indecomposables singleton domains
- . . .

Well-founded CRAs have unique decomposition

Corollary (L & vO 05)

unique decomposition iff divisibility wf, strictly compatible, Riesz decomposition

divisibility $\leqslant$ in $\langle A, 1, \cdot \rangle$: $a \leqslant b$ if $a \cdot c = b$ for some c

Well-founded CRAs have unique decomposition

Corollary (L & vO 05)

unique decomposition iff divisibility wf, strictly compatible, Riesz decomposition

Theorem

well-founded CRA $\langle A, 1, / \rangle$ has unique decomposition

Proof (using corollary).

- wf: natural CRA order $\leqslant$ is divisibility of partial commutative monoid $\langle A, 1, \cdot \rangle$;
- strictly compatible: if $b \cdot c$ defined and $a < b$, then $a \cdot c \leqslant b \cdot c$ by compatibility (before), so $a \cdot c < b \cdot c$ as $(b \cdot c)/(a \cdot c) \overset{\text{com},(7),(8),(2),(1)}{=} b/a \neq 1$;
- Riesz decomposition: if $a \preccurlyeq b \cdot c$ setting $b' := b/d \leqslant b$ and $c' := c/(d/a) \leqslant c$ for $d := (b \cdot c)/a$ works as $a \overset{\text{ass}}{=} a/(a/(b \cdot c)) \overset{(6)}{=} (b \cdot c)/d \overset{(8)}{=} b' \cdot c'$ $\square$

Well-founded CRAs have unique decomposition

Corollary (L & vO 05)

unique decomposition iff divisibility wf, strictly compatible, Riesz decomposition

Theorem

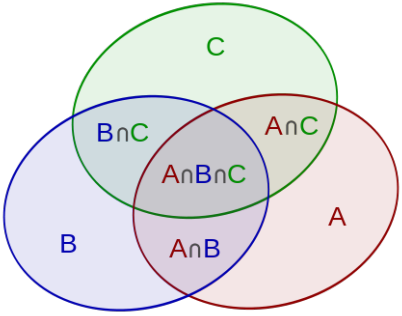
well-founded CRA $\langle A, 1, / \rangle$ has unique decomposition

Theorem (representation)

well-founded CRA $\langle A, 1, / \rangle$ isomorphic to multiset CRA $\langle A', \emptyset, - \rangle$
A' initial segment wrt sub-multiset $\subseteq$ of finite multisets of indecomposables of A

$a_1 \cdot \ldots \cdot a_n \mapsto [a_1, \ldots, a_n]$ with a_i indecomposable, $\leqslant \mapsto \subseteq$, $1 \mapsto \emptyset$, $/ \mapsto -$, $\cdot \mapsto \uplus$
up-shot: elements of such CRAs are finite multisets and vice versa

Inclusion/exclusion principle (IE) for 3 sets



$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

(picture/historical info from Wikipedia)

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion (de Moivre, da Silva, Sylvester (17/18th))

for non-empty finite family $a_I := (a_i)_{i \in I}$ *of finite sets*

$$\left|\bigcup a_I\right| = \sum_{\emptyset \subset J \subseteq I} (-1)^{|J|-1} \cdot \left(\left|\bigcap a_J\right|\right)$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion (de Moivre, da Silva, Sylvester (17/18th))

for non-empty finite family $a_I := (a_i)_{i \in I}$ *of finite sets*

$$\left|\bigcup a_I\right| = \sum_{\emptyset \subset J \subseteq I} (-1)^{|J|-1} \cdot \left(\left|\bigcap a_J\right|\right)$$

Example

for $I := \{1,2,3\}$, $a_1 := \{x,y\}$, $a_2 := \{y,z\}$, and $a_3 := \{z,x\}$

$$|\{x,y,z\}| = 3 = |\{x,y\}| + |\{y,z\}| + |\{z,x\}| - |\{y\}| - |\{z\}| - |\{x\}| + |\emptyset|$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion (de Moivre, da Silva, Sylvester (17/18th))

for non-empty finite family $a_I := (a_i)_{i \in I}$ of finite sets

$$\left|\bigcup a_I\right| = \sum_{\emptyset \subset J \subseteq I} (-1)^{|J| \dot{-} 1} \cdot \left(\left|\bigcap a_J\right|\right)$$

Example

for $I := \{1, 2, 3\}$, $a_1 := \{x, y\}$, $a_2 := \{y, z\}$, and $a_3 := \{z, x\}$

$$|\{x, y, z\}| = 3 = |\{x, y\}| + |\{y, z\}| + |\{z, x\}| + |\emptyset| \dot{-} |\{y\}| \dot{-} |\{z\}| \dot{-} |\{x\}|$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion)

for non-empty finite family $a_I := (a_i)_{i \in I}$ of finite sets

$$\left|\bigcup A_I\right| = \left(\sum_{J_o \subseteq I} \left|\bigcap A_J\right|\right) \dot{-} \left(\sum_{\emptyset \subset J_e \subseteq I} \left|\bigcap A_J\right|\right)$$

subsets of odd and even cardinality

Example

for $I := \{1,2,3\}$, $a_1 := \{x,y\}$, $a_2 := \{y,z\}$, and $a_3 := \{z,x\}$

$$|\{x,y,z\}| = 3 = |\{x,y\}| + |\{y,z\}| + |\{z,x\}| + |\emptyset| \dot{-} |\{y\}| \dot{-} |\{z\}| \dot{-} |\{x\}|$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

for non-empty finite family $a_I := (a_i)_{i \in I}$ *of objects of CRA*
if $\prod_{J_o \subseteq I} \bigwedge a_J$, *and* $\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J$ *denote*

$$\bigvee a_I \simeq \left(\prod_{J_o \subseteq I} \bigwedge a_J \right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J \right)$$

Example

for $I := \{1, 2, 3\}$, $\quad a_1 := 6$, $a_2 := 15$, and $a_3 := 10$ in $\langle \mathbb{N}, 1, \cdot \rangle$

$$\max(6, 15, 10) = \min(6, 15, 10) + 6 + 15 + 10 \dot{-} \min(6, 15) \dot{-} \min(15, 10) \dot{-} \min(10, 6)$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

for non-empty finite family $a_I := (a_i)_{i \in I}$ *of objects of CRA*
if $\prod_{J_o \subseteq I} \bigwedge a_J$, *and* $\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J$ *denote*

$$\bigvee a_I \simeq \left(\prod_{J_o \subseteq I} \bigwedge a_J \right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J \right)$$

Example

for $I := \{1, 2, 3\}$, $\quad a_1 := 6$, $a_2 := 15$, and $a_3 := 10$ in $\langle \mathrm{Pos}, 1, \cdot \rangle$

$$\mathrm{lcm}\,(6, 15, 10) = \gcd(6, 15, 10) \cdot 6 \cdot 15 \cdot 10 \cdot / \gcd(6, 15) \cdot / \gcd(15, 10) \cdot / \gcd(10, 6)$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

for non-empty finite family $a_I := (a_i)_{i \in I}$ *of objects of CRA*
if $\prod_{J_o \subseteq I} \bigwedge a_J$, *and* $\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J$ *denote*

$$\bigvee a_I \simeq \left(\prod_{J_o \subseteq I} \bigwedge a_J \right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J \right)$$

Example

for $I := \{1, 2, 3\}$, $a_1 := [2, 3]$, $a_2 := [3, 5]$, and $a_3 := [5, 2]$ in $\langle \mathsf{Mst}, \emptyset, - \rangle$

$$[2, 3] \cup [3, 5] \cup [5, 2] = [2, 3, 5] = \emptyset \uplus [2, 3] \uplus [3, 5] \uplus [5, 2] - [3] - [5] - [2]$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq \left(\prod_{J_o \subseteq I} \bigwedge a_J\right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J\right)$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq O/E = [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Proof (outline).

by induction on cardinality of index set I simultaneously showing $E \leqslant O$ □

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Proof (outline).

$$[a_j]_{J_o \subseteq I \cup \{k\}} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I \cup \{k\}}$$

in step case □

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Proof (outline).

$$([a_j]_{J_o \subseteq I} \cdot [a_j \wedge a_k]_{\emptyset \subset J_e \subseteq I} \cdot a_k)/([a_j]_{\emptyset \subset J_e \subseteq I} \cdot [a_j \wedge a_k]_{J_o \subseteq I})$$

singling out a_k using $\cdot$ a partial monoid and $\wedge$ a meet-semilattice $\square$

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Proof (outline).

$$([a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}) / ([a_j \wedge a_k]_{J_o \subseteq I} \,/\, [a_j \wedge a_k]_{\emptyset \subset J_e \subseteq I}) \quad \cdot$$

$$a_k / (([a_j \wedge a_k]_{J_o \subseteq I} \,/\, [a_j \wedge a_k]_{\emptyset \subset J_e \subseteq I}) / ([a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}))$$

by $(a \cdot b \cdot a_k)/(c \cdot d) = ((a/c)/(d/b)) \cdot (a_k/((d/b)/(a/c)))$ □

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq [a_j]_{J_o \subseteq I} \,/\, [a_j]_{\emptyset \subset J_e \subseteq I}$$

Proof (outline).

$$((\bigvee a_I)/(\bigvee (a_i \wedge a_k)_{i \in I})) \cdot (a_k/((\bigvee (a_i \wedge a_k)_{i \in I})/(\bigvee a_I)))$$

by IH for a_I, $(a_i \wedge a_k)_{i \in I}$ □

Inclusion/exclusion principle (IE)

Theorem (Inclusion/exclusion for CRAs)

$$\bigvee a_I \simeq \left(\prod_{J_o \subseteq I} \bigwedge a_J\right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J\right)$$

Proof (outline).

$$((\bigvee a_I)/(a_k \wedge \bigvee a_I)) \cdot a_k = ((\bigvee a_I)/a_k) \cdot a_k = a_k \vee \bigvee a_I = \bigvee a_{I \cup \{k\}}$$

using $\vee$ a join-semilattice and distributivity of $\wedge$ over $\vee$ $\square$

Inclusion/exclusion principle for cardinalities

Theorem (Inclusion/exclusion for cardinalities)

for non-empty finite family $a_I := (a_i)_{i \in I}$ of finite sets

$$\left|\bigcup A_I\right| = \left(\sum_{J_o \subseteq I} \left|\bigcap A_J\right|\right) \dot{-} \left(\sum_{\emptyset \subset J_e \subseteq I} \left|\bigcap A_J\right|\right)$$

Proof.

$$\left|\bigcup A_I\right| = \left|\left(\biguplus_{J_o \subseteq I} \bigcap A_J\right) - \left(\biguplus_{\emptyset \subset J_e \subseteq I} \bigcap A_J\right)\right| = \left(\sum_{J_o \subseteq I} \left|\bigcap A_J\right|\right) \dot{-} \left(\sum_{\emptyset \subset J_e \subseteq I} \left|\bigcap A_J\right|\right)$$

using $|M \uplus N| = |M| + |N|$ so $|M - N| = |M| \dot{-} |N|$ if $N \subseteq M$ □

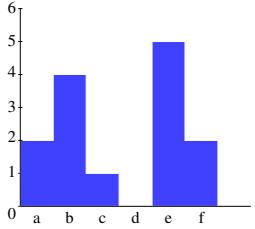
Inclusion/exclusion principle for measures

Definition

function μ from algebra $\mathcal{A}$ to non-negative reals is measure if

- $\mu(\emptyset) = 0$
- $\mu(A \cup B) = \mu(A) + \mu(B)$ for $A, B \in \mathcal{A}$ and disjoint

extended to measurable multisets by $\mu(M) := \sum_i \mu(M^{>i})$



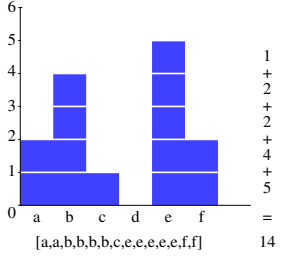
Inclusion/exclusion principle for measures

Definition

function μ from algebra $\mathcal{A}$ to non-negative reals is measure if

- $\mu(\emptyset) = 0$
- $\mu(A \cup B) = \mu(A) + \mu(B)$ for $A, B \in \mathcal{A}$ and disjoint

extended to measurable multisets by $\mu(M) := \sum_i \mu(M^{>i}) = \sum_j j \cdot \mu(L^j)$



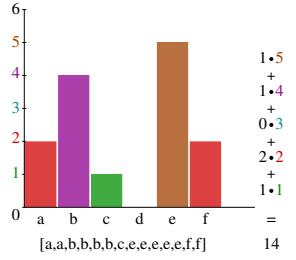
Inclusion/exclusion principle for measures

Definition

function μ from algebra $\mathcal{A}$ to non-negative reals is measure if

- $\mu(\emptyset) = 0$
- $\mu(A \cup B) = \mu(A) + \mu(B)$ for $A, B \in \mathcal{A}$ and disjoint

extended to measurable multisets by $\mu(M) := \sum_i \mu(M^{>i}) = \sum_j j \cdot \mu(L^j)$



Inclusion/exclusion principle for measures

Definition

function μ from algebra $\mathcal{A}$ to non-negative reals is measure if

- $\mu(\emptyset) = 0$
- $\mu(A \cup B) = \mu(A) + \mu(B)$ for $A, B \in \mathcal{A}$ and disjoint

extended to measurable multisets by $\mu(M) := \sum_i \mu(M^{>i}) = \sum_j j \cdot \mu(L^j)$

Lemma

$\mu(M \uplus N) = \mu(M) + \mu(M)$

Proof.

$\mu(M \uplus N) = \sum_{j,k}(j+k) \cdot \mu(M^j \cap N^k) = \mu(M) + \mu(N)$ using Lebesgue = Riemann $\square$

Inclusion/exclusion principle for measures

Theorem (Inclusion/exclusion for measures)

for non-empty finite family $a_I := (a_i)_{i\in I}$ of measurable sets

$$\mu(\bigcup A_I) = \left(\sum_{J_o\subseteq I} \mu(\bigcap A_J)\right) \dot{-} \left(\sum_{\emptyset\subset J_e\subseteq I} \mu(\bigcap A_J)\right)$$

Proof.

$$\mu(\bigcup A_I) = \mu(\left(\biguplus_{J_o\subseteq I} \bigcap A_J\right) - \left(\biguplus_{\emptyset\subset J_e\subseteq I} \bigcap A_J\right)) = \left(\sum_{J_o\subseteq I} \mu(\bigcap A_J)\right) \dot{-} \left(\sum_{\emptyset\subset J_e\subseteq I} \mu(\bigcap A_J)\right)$$

using $\mu(M \uplus N) = \mu(M) + \mu(N)$ so $\mu(M - N) = \mu(M) \dot{-} \mu(N)$ if $N \subseteq M$ □

Standard formulation of inclusion/exclusion principle?

Theorem

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|} \dot{-} 1} \quad ?$$

cannot express -1 in language; only non-negative/fractional resources in CRAs

Standard formulation of inclusion/exclusion principle?

Theorem

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|} \dot{-} 1} \quad ?$$

Idea

- integer -2 as pair of natural numbers $(0, 2)$, or $(5, 7)$, or ...

Standard formulation of inclusion/exclusion principle?

Theorem

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|} \dot{-} 1} \quad ?$$

Idea

- integer -2 as pair of natural numbers $(0, 2)$, or $(5, 7)$, or ...
- positive rational $\frac{1}{2}$ as pair of positive numbers $(1, 2)$, or $(5, 10)$, or ...

Standard formulation of inclusion/exclusion principle?

Theorem

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|} \dot{-} 1} \quad ?$$

Idea

- integer -2 as pair of natural numbers $(0, 2)$, or $(5, 7)$, or ...
- positive rational $\frac{1}{2}$ as pair of positive numbers $(1, 2)$, or $(5, 10)$, or ...
- fraction $\frac{a}{b}$ as pair (a, b) of CRA elements; a numerator, b denominator

Standard formulation of inclusion/exclusion principle?

Theorem

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|} \dot{-} 1} \quad ?$$

Idea

- integer -2 as pair of natural numbers $(0, 2)$, or $(5, 7)$, or ...
- positive rational $\frac{1}{2}$ as pair of positive numbers $(1, 2)$, or $(5, 10)$, or ...
- fraction $\frac{a}{b}$ as pair (a, b) of CRA elements; a numerator, b denominator

will assume CRA $\langle A, 1, \cdot \rangle$ having all products, i.e. $\cdot$-closed

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid, embedding monoid* $\langle A, 1, \cdot \rangle$*, for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid, embedding monoid* $\langle A, 1, \cdot \rangle$*, for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Proof (reciprocal cases).

$((\frac{a}{b})^{-1})^{-1} = (\frac{b}{a})^{-1} = \frac{a}{b}$ *involutive*

□

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Proof (reciprocal cases).

$((\frac{a}{b})^{-1})^{-1} = (\frac{b}{a})^{-1} = \frac{a}{b}$ *involutive*

$(\frac{a}{b} \cdot \frac{a'}{b'})^{-1} = \left(\frac{a \cdot (a'/b)}{b' \cdot (b/a')}\right)^{-1} = \frac{b' \cdot (b/a')}{a \cdot (a'/b)} = \frac{b'}{a'} \cdot \frac{b}{a} = (\frac{a'}{b'})^{-1} \cdot (\frac{a}{b})^{-1}$ *anti−automorphic* □

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Proof (reciprocal cases).

$((\frac{a}{b})^{-1})^{-1} = (\frac{b}{a})^{-1} = \frac{a}{b}$ *involutive*

$(\frac{a}{b} \cdot \frac{a'}{b'})^{-1} = \left(\frac{a \cdot (a'/b)}{b' \cdot (b/a')}\right)^{-1} = \frac{b' \cdot (b/a')}{a \cdot (a'/b)} = \frac{b'}{a'} \cdot \frac{b}{a} = (\frac{a'}{b'})^{-1} \cdot (\frac{a}{b})^{-1}$ *anti − automorphic* □

product neither commutative nor (fully) normalised; (5),(6) not used in proof

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Example

- for natural numbers yields stack numbers, e.g. $(0,0) \neq (1,1)$ and $(1,0) + (1,1) = (2,1) \neq (1,0) = (1,1) + (1,0)$

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Example

- for natural numbers yields stack numbers, e.g. $(0,0) \neq (1,1)$ and $(1,0) + (1,1) = (2,1) \neq (1,0) = (1,1) + (1,0)$
- for positive numbers yields partially normalised fractions, e.g. $\frac{2}{4} \cdot \frac{6}{3} = \frac{6}{6}$

Embedding CRAs in involutive monoids

Lemma

$\langle A \times A, 1, \cdot, (\ )^{-1} \rangle$ *is involutive monoid for*

- *one* 1 *is* $\frac{1}{1}$*, via embedding of* A *into* $A \times A$ *mapping* $a \mapsto \frac{a}{1}$
- *product* $\frac{a}{b} \cdot \frac{a'}{b'}$ *is* $\frac{a \cdot (a'/b)}{b' \cdot (b/a')}$
- *reciprocal* $(\frac{a}{b})^{-1}$ *is* $\frac{b}{a}$

Example

- for natural numbers yields stack numbers, e.g. $(0,0) \neq (1,1)$ and $(1,0) + (1,1) = (2,1) \neq (1,0) = (1,1) + (1,0)$
- for positive numbers yields partially normalised fractions, e.g. $\frac{2}{4} \cdot \frac{6}{3} = \frac{6}{6}$

may extend stack numbers with 3rd component to test if stack high enough

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is commutative group , embedding monoid* $\langle A, 1, \cdot \rangle$*, where* $\equiv$ *relates fractions having same normalisation:*

- *normalisation of* $\frac{a}{b}$ *is* $\frac{a/b}{b/a}$

being normalised of $\frac{a}{b}$ may be alternatively defined by $a \wedge b = 1$

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is commutative group ,* *embedding* *monoid* $\langle A, 1, \cdot \rangle$*, where* $\equiv$ *relates fractions having same normalisation:*

- *normalisation of* $\frac{a}{b}$ *is* $\frac{a/b}{b/a}$

Proof.

- $\equiv$ congruence for all 3 operations $\implies$ involutive monoid by previous lemma
- $f^{-1} \cdot f \equiv 1$ for all fractions f
- $\cdot$ is commutative

half of these trivial, others proven using Prover9 (take up to a few minutes) □

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is commutative group where* $\equiv$ *relates fractions having same normalisation:*

- *normalisation of* $\frac{a}{b}$ *is* $\frac{a/b}{b/a}$

Proof.

- $\equiv$ congruence for all 3 operations $\implies$ involutive monoid by previous lemma
- $f^{-1} \cdot f \equiv 1$ for all fractions f
- $\cdot$ is commutative

half of these trivial, others proven using Prover9 (take up to a few minutes) □

$\equiv$ may be alternatively defined by $\frac{a}{b} \equiv \frac{a'}{b'}$ if $a/a' = b/b'$ and $a'/a = b'/b$

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is commutative group where* $\equiv$ *relates fractions having same normalisation:*

- *normalisation of* $\frac{a}{b}$ *is* $\frac{a/b}{b/a}$

Example

- for natural numbers yields integers, pairs (n, m) where n or m is 0

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is commutative group where* $\equiv$ *relates fractions having same normalisation:*

- *normalisation of* $\frac{a}{b}$ *is* $\frac{a/b}{b/a}$

Example

- for natural numbers yields integers, pairs (n, m) where n or m is 0
- for positive numbers yields normalised fractions $\frac{n}{m}$, where $\gcd(n, m) = 1$

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ is commutative group where $\equiv$ relates fractions having same normalisation:

- *normalisation of $\frac{a}{b}$ is $\frac{a/b}{b/a}$*

Example

- for natural numbers yields integers, pairs (n, m) where n or m is 0
- for positive numbers yields normalised fractions $\frac{n}{m}$, where $\gcd(n, m) = 1$
- for multisets yields signed multisets having integer multiplicities

Embedding CRAs in groups

Lemma

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ is commutative group where $\equiv$ relates fractions having same normalisation:

- *normalisation of $\frac{a}{b}$ is $\frac{a/b}{b/a}$*

Example

- for natural numbers yields integers, pairs (n, m) where n or m is 0
- for positive numbers yields normalised fractions $\frac{n}{m}$, where $\gcd(n, m) = 1$
- for multisets yields signed multisets having integer multiplicities
- ...

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group, embedding monoid* $\langle A, 1, \cdot \rangle$*, for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$ *(if* $f \vee g = g$*)*

$\{f \mid 1 \leqslant f\}$ embeds carrier; division $f \,/\, g$ defined by $g^{-1} \cdot f$; embeds a/b if $b \leqslant a$

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group, embedding monoid* $\langle A, 1, \cdot \rangle$*, for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$

Proof.

- being normalised preserved by both meet $\wedge$ and join $\vee$
- commutativity, associativity, idempotence, absorption by same for CRA $\wedge, \vee$
- orderedness $\frac{a}{b} \cdot \frac{e}{f} \leqslant \frac{c}{d} \cdot \frac{e}{f}$ if $\frac{a}{b} \leqslant \frac{c}{d}$ verified by Prover9: if $a \leqslant c$, $d \leqslant b$ then
  $(f \cdot (b/e))/(a \cdot (e/b)) = ((f \cdot (b/e))/(a \cdot (e/b))) \wedge ((f \cdot (d/e))/(c \cdot (e/d)))$ denominator
  $(a \cdot (e/b))/(f \cdot (b/e)) = ((a \cdot (e/b))/(f \cdot (b/e))) \wedge ((c \cdot (e/d))/(f \cdot (d/e)))$ numerator $\square$

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$

Example

- on integers, minimum and maximum ordered by less–than–or–equal

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$

Example

- on integers, minimum and maximum ordered by less–than–or–equal
- on normalised fractions, $\frac{a}{b} \leqslant \frac{a'}{b'}$ iff $a \mid a'$ and $b' \mid b$ so $\frac{1}{4} \leqslant \frac{1}{2}$ but not $\frac{1}{3} \leqslant \frac{1}{2}$

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$

Example

- on integers, minimum and maximum ordered by less–than–or–equal
- on normalised fractions, $\frac{a}{b} \leqslant \frac{a'}{b'}$ iff $a \mid a'$ and $b' \mid b$ so $\frac{1}{4} \leqslant \frac{1}{2}$ but not $\frac{1}{3} \leqslant \frac{1}{2}$
- on multisets, elementwise minimum, maximum, and (all) comparison

Embedding CRAs in lattice ordered groups

Theorem (Dvurečenskij & Graziano)

$\langle (A \times A)/\equiv, 1, \cdot, (\ )^{-1} \rangle$ *is lattice ordered group for*

- *meet* $\frac{a}{b} \wedge \frac{c}{d}$ *is* $\frac{a \wedge c}{b \vee d}$
- *join* $\frac{a}{b} \vee \frac{c}{d}$ *is* $\frac{a \vee c}{b \wedge d}$
- *natural order* $f \leqslant g$ *if* $f = f \wedge g$

Example

- on integers, minimum and maximum ordered by less–than–or–equal
- on normalised fractions, $\frac{a}{b} \leqslant \frac{a'}{b'}$ iff $a \mid a'$ and $b' \mid b$ so $\frac{1}{4} \leqslant \frac{1}{2}$ but not $\frac{1}{3} \leqslant \frac{1}{2}$
- on multisets, elementwise minimum, maximum, and (all) comparison
- ...

Inclusion/exclusion for lattice ordered groups

Corollary

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A embedded as fractions

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|-1}}$$

Inclusion/exclusion for lattice ordered groups

Corollary

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of elements of A embedded as fractions

$$\bigvee a_I = \prod_{\emptyset \subset J \subseteq I} \left(\bigwedge a_J\right)^{(-1)^{|J|-1}}$$

Proof.

have group ($\cdot$ associ/commutative, -1 anti-automorphic) so may rearrange rhs as:

$$\left(\prod_{J_o \subseteq I} \bigwedge a_J\right) / \left(\prod_{\emptyset \subset J_e \subseteq I} \bigwedge a_J\right)$$

conclude by assumption and embedding, from inclusion/exclusion for CRAs □

Standard formulation of I/E for cardinalities of sets

Corollary

For a non-empty finite family $a_I := (a_i)_{i \in I}$ *of sets,*

$$\left|\bigcup a_I\right| = \sum_{\emptyset \subset J \subseteq I} (-1)^{|J|-1} \cdot \left(\left|\bigcap a_J\right|\right)$$

Standard formulation of I/E for cardinalities of sets

Corollary

For a non-empty finite family $a_I := (a_i)_{i\in I}$ of sets,

$$\left|\bigcup a_I\right| = \sum_{\emptyset\subset J\subseteq I} (-1)^{|J|-1} \cdot \left(\left|\bigcap a_J\right|\right)$$

Proof.

as on previous slide but relying on integers being a group to rearrange summands and on CRA version of inclusion/exclusion for cardinalities of sets □

Standard formulation of I/E for cardinalities of sets

Corollary

For a non-empty finite family $a_I := (a_i)_{i \in I}$ of sets,

$$\left|\bigcup a_I\right| = \sum_{\emptyset \subset J \subseteq I} (-1)^{|J|-1} \cdot \left(\left|\bigcap a_J\right|\right)$$

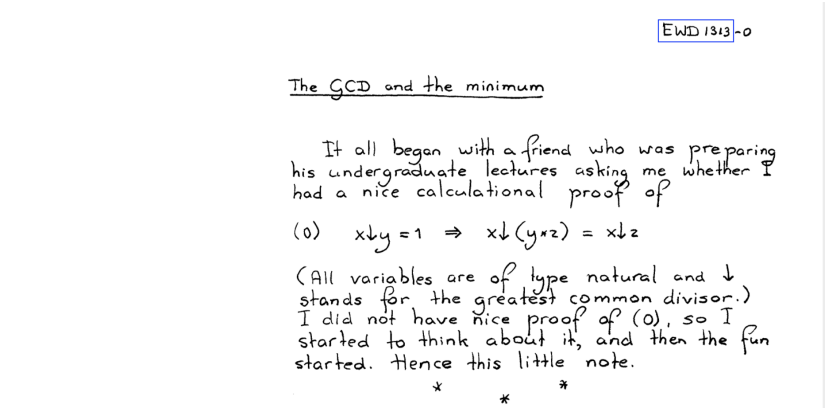
Proof.

as on previous slide but relying on integers being a group to rearrange summands and on CRA version of inclusion/exclusion for cardinalities of sets □

Remark

similarly for measures (instead of cardinalities) of sets

The GCD and the minimum



EWD 1313-0

The GCD and the minimum

It all began with a friend who was preparing his undergraduate lectures asking me whether I had a nice calculational proof of

(0) $x \downarrow y = 1 \Rightarrow x \downarrow (y \times z) = x \downarrow z$

(All variables are of type natural and $\downarrow$ stands for the greatest common divisor.) I did not have nice proof of (0), so I started to think about it, and then the fun started. Hence this little note.

* * *

Edsger W. Dijkstra Archive, EWD 1313, Austin, 27 November 2001

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ if $d := b \cdot c$ is defined, i.e. $d/b = c$ and $b/d = 1$

Proof.

$$
\begin{aligned}
a \wedge d &\overset{\text{meet}}{=} a/(a/d) \\
&\overset{(1)}{=} a/((a/d)/1) \\
&\overset{\text{ass}}{=} a/((a/d)/(b/d)) \\
&\overset{(4)}{=} a/((a/b)/(d/b)) \\
&\overset{\text{ass}}{=} a/(a/(d/b)) \\
&\overset{\text{ass,meet}}{=} a \wedge c \quad \square
\end{aligned}
$$

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Corollary

- *for positive numbers,* $\gcd(n, m) = 1 \implies \gcd(n, m \cdot k) = \gcd(n, k)$

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Corollary

- *for positive numbers,* $\gcd(n, m) = 1 \implies \gcd(n, m \cdot k) = \gcd(n, k)$
- *for natural numbers,* $\min(n, m) = 0 \implies \min(n, m + k) = \min(n, k)$

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Corollary

- *for positive numbers,* $\gcd(n, m) = 1 \implies \gcd(n, m \cdot k) = \gcd(n, k)$
- *for natural numbers,* $\min(n, m) = 0 \implies \min(n, m + k) = \min(n, k)$
- *for multisets,* $M \cap N = \emptyset \implies M \cap (N \uplus L) = M \cap L$

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Corollary

- *for positive numbers,* $\gcd(n, m) = 1 \implies \gcd(n, m \cdot k) = \gcd(n, k)$
- *for natural numbers,* $\min(n, m) = 0 \implies \min(n, m + k) = \min(n, k)$
- *for multisets,* $M \cap N = \emptyset \implies M \cap (N \uplus L) = M \cap L$
- ...

Calculational proof of EWD1313 in CRAs

Lemma

$a \wedge b = 1 \implies a \wedge d = a \wedge c$ *if* $d := b \cdot c$ *is defined, i.e.* $d/b = c$ *and* $b/d = 1$

Corollary

- *for positive numbers,* $\gcd(n, m) = 1 \implies \gcd(n, m \cdot k) = \gcd(n, k)$
- *for natural numbers,* $\min(n, m) = 0 \implies \min(n, m + k) = \min(n, k)$
- *for multisets,* $M \cap N = \emptyset \implies M \cap (N \uplus L) = M \cap L$
- ...

all the same in CRAs; need not have unique decomposition
CRAs capture lattice theory with bottom (top optional)

Commutative BCK algebras with relative cancellation

Definition (BCI algebra (Imai & Iséki & Tanaka 66–))

$\langle A, 1, / \rangle$ with for all $a, b, c \in A$:

$$(a/b)/(a/c) \leqslant c/b \tag{9}$$
$$a/(a/b) \leqslant b \tag{10}$$
$$a \leqslant a \tag{11}$$
$$a = b \quad \text{if } a \leqslant b \text{ and } b \leqslant a \tag{12}$$
$$a = 1 \quad \text{if } a \leqslant 1 \tag{13}$$

where $a \leqslant b$ if $a/b = 1$

unify set difference and (reverse) implication in propositional logic

Commutative BCK algebras with relative cancellation

Definition (BCK algebra (Imai & Iséki & Tanaka 66–))

$\langle A, 1, / \rangle$ with for all $a, b, c \in A$:

$$(a/b)/(a/c) \leqslant c/b \tag{9}$$
$$a/(a/b) \leqslant b \tag{10}$$
$$a \leqslant a \tag{11}$$
$$a = b \quad \text{if } a \leqslant b \text{ and } b \leqslant a \tag{12}$$
$$1 \leqslant a \tag{13}$$

where $a \leqslant b$ if $a/b = 1$

unify set difference and (reverse) implication in propositional logic

Commutative BCK algebras with relative cancellation

Definition (cBCK algebra (Dvurečenskij & Graziano 98–))

$\langle A, 1, / \rangle$ with for all $a, b, c \in A$:

$$(a/b)/(a/c) \leqslant c/b \tag{9}$$
$$a/(a/b) \leqslant b \tag{10}$$
$$a \leqslant a \tag{11}$$
$$a = b \quad \text{if } a \leqslant b \text{ and } b \leqslant a \tag{12}$$
$$1 \leqslant a \tag{13}$$
$$a \wedge b = b \wedge a \tag{14}$$

where $a \leqslant b$ if $a/b = 1$ and $a \wedge b$ is $a/(a/b)$

Commutative BCK algebras with relative cancellation

Definition (cBCK w/ rel. cancellation (Dvurečenskij & Graziano 98–))

$\langle A, 1, / \rangle$ with for all $a, b, c \in A$:

$$(a/b)/(a/c) \leqslant c/b \tag{9}$$
$$a/(a/b) \leqslant b \tag{10}$$
$$a \leqslant a \tag{11}$$
$$a = b \quad \text{if } a \leqslant b \text{ and } b \leqslant a \tag{12}$$
$$1 \leqslant a \tag{13}$$
$$a \wedge b = b \wedge a \tag{14}$$
$$b = c \quad \text{if } a \leqslant b, c \text{ and } b/a = c/a \tag{15}$$

where $a \leqslant b$ if $a/b = 1$ and $a \wedge b$ is $a/(a/b)$

Equational characterisation of cBCK w/ rel. cancellation

Theorem (D & G)

$\langle A, 1, / \rangle$ is cBCK algebra with relative cancellation iff for all $a, b, c \in A$

$$a/a = 1 \tag{15}$$
$$a/1 = a \tag{16}$$
$$(a/b)/c = (a/c)/b \tag{17}$$
$$a/(a/b) = b/(b/a) \tag{18}$$
$$(a/b)/(b/a) = a/b \tag{19}$$

automatically verified by Prover9; most difficult (19) took 30 minutes

Equational characterisation of cBCK w/ rel. cancellation

Theorem (D & G)

$\langle A, 1, / \rangle$ is cBCK algebra with relative cancellation iff for all $a, b, c \in A$

$$a/a = 1 \tag{15}$$
$$a/1 = a \tag{16}$$
$$(a/b)/c = (a/c)/b \tag{17}$$
$$a/(a/b) = b/(b/a) \tag{18}$$
$$(a/b)/(b/a) = a/b \tag{19}$$

Theorem

$\langle A, 1, / \rangle$ is cBCK algebra with relative cancellation iff is CRA

Example proof in equivalence theorem by Prover9

Prover9 proof that (4) holds from (15)–(19).

```
============================== PROOF =================================

% Proof 1 at 9.37 (+ 0.08) seconds.
% Length of proof is 54.
% Level of proof is 13.
% Maximum clause weight is 23.000.
% Given clauses 182.

1 (x / y) / (z / y) = (x / z) / (y / z) # label(non_clause) # label(goal).  [goal].
2 x / x = 1.  [assumption].
3 x ^ y = x / (x / y).  [assumption].
4 x ^ y = y ^ x.  [assumption].
5 x / (x / y) = y / (y / x).  [copy(4),rewrite([3(1),3(3)])].
6 (x / y) / z = (x / z) / y.  [assumption].
7 x / 1 = x.  [assumption].
8 (x / y) / (y / x) = x / y.  [assumption].
9 (c1 / c3) / (c2 / c3) != (c1 / c2) / (c3 / c2).  [deny(1)].
10 x / (y / (y / x)) = x / (x / (x / y)).  [para(5(a,1),3(a,2,2)),rewrite([3(2)]),flip(a)].
11 (x / y) / x = 1 / y.  [para(2(a,1),6(a,1,1)),flip(a)].
13 (x / y) / ((x / z) / y) = z / (z / (x / y)).  [para(6(a,1),5(a,1,2))].
14 (x / (x / y)) / z = (y / z) / (y / x).  [para(5(a,1),6(a,1,1))].
15 ((x / y) / z) / u = ((x / u) / y) / z.  [para(6(a,1),6(a,1,1)),flip(a)].
20 ((x / y) / z) / (y / x) = (x / y) / z.  [para(8(a,1),6(a,1,1)),flip(a)].
28 (x / y) / (1 / y) = x / (y / (y / x)).  [para(10(a,2),5(a,1)),rewrite([11(6)]),flip(a)].
31 (x / (y / (y / x))) / z = (x / z) / (x / (x / y)).  [para(10(a,2),6(a,1,1))].
39 1 / (x / y) = 1.  [para(5(a,1),11(a,1,1)),rewrite([6(3),2(3)]),flip(a)].
40 ((x / y) / z) / x = (1 / y) / z.  [para(11(a,1),6(a,1,1)),flip(a)].
46 1 / x = 1.  [para(7(a,1),39(a,1,2))].
48 ((x / y) / z) / x = 1.  [back_rewrite(40),rewrite([46(5),46(5)])].
49 x / (y / (y / x)) = x / y.  [back_rewrite(28),rewrite([46(3),7(3)]),flip(a)].
50 (x / y) / x = 1.  [back_rewrite(11),rewrite([46(4)])].
52 (x / y) / (x / (x / z)) = (x / z) / y.  [back_rewrite(31),rewrite([49(3)]),flip(a)].
55 x / (x / (x / y)) = x / y.  [back_rewrite(10),rewrite([49(3)]),flip(a)].
58 (x / (x / y)) / ((y / z) / (y / x)) = z / (z / (y / (y / x))).  [para(5(a,1),13(a,1,1))].
59 (x / y) / ((z / (z / x)) / y) = (x / z) / ((x / z) / (x / y)).  [para(5(a,1),13(a,1,2,1))].
71 x / (x / ((x / y) / z)) = (x / y) / z.  [para(50(a,1),13(a,1,2,1)),rewrite([46(4),7(4)]),flip(a)].
73 (x / y) / (x / (y / z)) = 1.  [para(5(a,1),48(a,1,1)),rewrite([6(4)])].
92 (x / y) / (x / z) = (z / y) / (z / x).  [para(14(a,1),6(a,1))].
94 (x / (x / y)) / z = (y / (y / x)) / z.  [para(14(a,2),6(a,1))].
115 (x / y) / (x / ((y / z) / u)) = 1.  [para(48(a,1),14(a,2,1)),rewrite([6(5),46(10)])].
182 ((x / y) / z) / u = ((x / u) / z) / y.  [para(15(a,2),6(a,1))].
187 ((x / y) / z) / (z / x) = (x / z) / y.  [para(8(a,1),15(a,1,1)),flip(a)].
347 (x / y) / ((y / x) / z) = x / y.  [para(20(a,1),49(a,1,2,2)),rewrite([2(6),7(3)]),flip(a)].
747 (x / y) / (x / (x / z)) = (x / y) / z.  [para(52(a,2),6(a,1))].
838 (x / y) / ((y / z) / x) = x / y.  [para(6(a,1),347(a,1,2))].
926 (x / (y / (y / (z / (z / x))))) / ((z / y) / (z / x)) = x / z.  [para(58(a,1),13(a,1,2)),rewrite([6(9),115(16),7(12)])].
945 (x / (x / y)) / ((x / (x / y)) / z) = y / (y / (x / (x / z))).  [para(55(a,1),58(a,1,2,1)),rewrite([58(6),747(11)]),flip(a)].
1254 (x / (y / z)) / ((z / (z / y)) / (y / x)) = x / y.  [para(14(a,2),59(a,1,2)),rewrite([73(12),7(10)])].
1262 (x / (y / (y / z))) / ((y / (y / x)) / z) = x / y.  [para(55(a,1),59(a,1,2)),rewrite([945(6),55(5),945(15),55(14),73(13),7(10)])].
1267 x / (y / ((y / x) / z)) = x / y.  [para(73(a,1),59(a,1,2)),rewrite([7(6),73(11),7(7)])].
1484 x / (y / ((z / x) / (z / y))) = x / y.  [para(92(a,1),1267(a,1,2,2))].
1548 (x / (x / y)) / ((y / (y / x)) / z) = y / (y / (x / (x / z))).  [para(94(a,1),3(a,2,2)),rewrite([3(3),945(6)]),flip(a)].
1559 x / (y / (y / (z / (z / x)))) = x / (y / (y / z)).  [para(94(a,1),49(a,1,2)),rewrite([1548(6)])].
1630 (x / (y / (y / z))) / ((z / y) / (z / x)) = x / z.  [back_rewrite(926),rewrite([1559(5)])].
2872 (((x / y) / z) / u) / (u / x) = (x / u) / (x / ((x / y) / z)).  [para(71(a,1),187(a,1,1,1))].
2897 ((x / y) / z) / u = (x / y) / (x / ((x / z) / u)).  [para(187(a,1),182(a,1,1)),rewrite([6(8),2872(8)])].
5634 (x / y) / (z / (y / x)) = (x / y) / z.  [para(8(a,1),1484(a,1,2,2,1)),rewrite([49(6)])].
5839 (x / y) / (z / ((y / u) / x)) = (x / y) / z.  [para(838(a,1),5634(a,1,1)),rewrite([2897(5),8(5),747(5),838(9)])].
17428 (x / y) / (z / (y / (y / x))) = (x / y) / (z / y).  [para(1262(a,1),5839(a,1,2)),flip(a)].
19369 (x / (y / (y / z))) / (z / y) = x / z.  [para(1630(a,1),1254(a,1,1)),rewrite([17428(11),2897(10),347(13)]),flip(a)].
19647 (x / y) / (z / y) = (x / z) / (y / z).  [para(19369(a,1),19369(a,1,1)),rewrite([50(6),7(6),6(6)])].
19648 $F.  [resolve(19647,a,9,a)].

============================== end of proof ==========================
```

Gradification: algebra to system

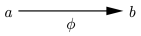
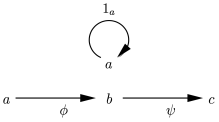
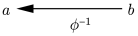
Idea

turn object into step (Latin *gradus* = *step*; cf. Pous typed algebras)

Gradification: algebra to system

Idea

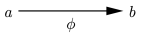
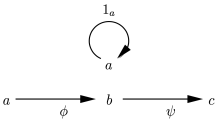
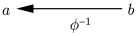
turn object (also called letter) into step ; well-known construction hierarchy :

letter a	string abc	French string $\acute{a}\grave{b}\acute{c}$	normalized . . .
alphabet $\rightsquigarrow$ graph	monoid $\rightsquigarrow$ category	involutive . . .	group $\rightsquigarrow$ groupoid
step ϕ	reduction $\phi\psi\chi$	conversion $\acute{\phi}\grave{\psi}\acute{\chi}$	normalised . . .
			
	$1 \cdot x \to x$ $x \cdot 1 \to x$ $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$	$1^{-1} \to 1$ $(x \cdot y)^{-1} \to y^{-1} \cdot x^{-1}$ $(x^{-1})^{-1} \to x$	$x \cdot x^{-1} \to 1$ $x^{-1} \cdot x \to 1$

Gradification: algebra to system

Idea

turn object (also called letter) into step ; well-known construction hierarchy :

letter a	string abc	French string $\acute{a}\grave{b}\acute{c}$	normalized . . .
alphabet $\rightsquigarrow$ graph	monoid $\rightsquigarrow$ category	involutive . . .	group $\rightsquigarrow$ groupoid
step ϕ	reduction $\phi\psi\chi$	conversion $\acute{\phi}\grave{\psi}\acute{\chi}$	normalised . . .
			
	$1 \cdot x \to x$ $x \cdot 1 \to x$ $(x \cdot y) \cdot z \to x \cdot (y \cdot z)$	$1^{-1} \to 1$ $(x \cdot y)^{-1} \to y^{-1} \cdot x^{-1}$ $(x^{-1})^{-1} \to x$	$x \cdot x^{-1} \to 1$ $x^{-1} \cdot x \to 1$ $x \cdot (x^{-1} \cdot y) \to y$ $x^{-1} \cdot (x \cdot y) \to y$

Gradification: CRA to commutative residual system?

CRA hierarchy; recall from before (I/E)

additively: $\mathbb{B} \hookrightarrow \mathbb{N} \hookrightarrow \mathbb{Z}$

- CRA $\mathbb{B}$ of bits $\{0, 1\}$ (no composition, no inverse) $\hookrightarrow$
- CRA $\mathbb{N}$ of (unary) natural numbers $\{0, 1, 11, 111, \ldots\}$ monoid (formal sum as composition, no inverse) $\hookrightarrow$
- group $\mathbb{Z}$ of integers $\{\ldots, (0, 11), (0, 1), (0, 0), (1, 0), (11, 0), \ldots\}$ (juxtaposition and normalisation as composition, swapping as inverse)

Gradification: CRA to commutative residual system?

CRA hierarchy

CRA $\hookrightarrow$ CRA and monoid of formal products $\hookrightarrow$ group of normalised fractions

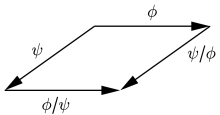
Gradification: CRA to commutative residual system?

CRA hierarchy

CRA $\hookrightarrow$ CRA and monoid of formal products $\hookrightarrow$ group of normalised fractions

Idea

residual ϕ/ψ of step ϕ after co-initial step ψ



skolemisation of diamond property

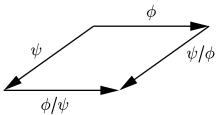
Gradification: CRA to commutative residual system?

CRA hierarchy

CRA $\hookrightarrow$ CRA and monoid of formal products $\hookrightarrow$ group of normalised fractions

Idea

residual ϕ/ψ of step ϕ after co-initial step ψ



skolemisation of diamond property

Problem for gradification of CRAs

commutativity forces source = target of ψ for $(\phi/\psi)/\phi$ (5) and $\phi/(\phi/\psi)$ (6)

CRA obtained by making composition commutative

Definition

residual algebra RA $\langle A, 1, / \rangle$ with for all $a, b, c \in A$:

$$a/1 = a \tag{1}$$
$$a/a = 1 \tag{2}$$
$$1/a = 1 \tag{3}$$
$$(a/b)/(c/b) = (a/c)/(b/c) \tag{4}$$

CRA obtained by making composition commutative

Definition

residual algebra RAC $\langle A, 1, /, \cdot \rangle$ with composition and for all $a, b, c \in A$:

$$a/1 = a \tag{1}$$
$$a/a = 1 \tag{2}$$
$$1/a = 1 \tag{3}$$
$$(a/b)/(c/b) = (a/c)/(b/c) \tag{4}$$
$$c/(a \cdot b) = (c/a)/b \tag{7}$$
$$(a \cdot b)/c = (a/c) \cdot (b/(c/a)) \tag{8}$$

CRA obtained by making composition commutative

Definition

residual algebra RAC $\langle A, 1, /, \cdot \rangle$ with composition and for all $a, b, c \in A$:

$$a/1 = a \tag{1}$$
$$a/a = 1 \tag{2}$$
$$1/a = 1 \tag{3}$$
$$(a/b)/(c/b) = (a/c)/(b/c) \tag{4}$$
$$c/(a \cdot b) = (c/a)/b \tag{7}$$
$$(a \cdot b)/c = (a/c) \cdot (b/(c/a)) \tag{8}$$

composition commutative:

$$(a \cdot b)/(b \cdot a) \overset{(7,8)}{=} (\overbrace{(a/b)/a}^{(5)}) \cdot (\overbrace{(b/(b/a))/(a/(a/b))}^{(6)}) \overset{(5,6)}{=} 1 \cdot 1 = 1$$

Gradification: RA to residual system

Definition (Residual system, Ch. 8 of Term Rewriting Systems 2003)

residual system $\langle \to, 1, / \rangle$ with for coinitial ϕ, ψ, χ in abstract rewrite system $\to$:

$$\phi/1 = \phi \tag{1}$$
$$\phi/\phi = 1 \tag{2}$$
$$1/\phi = 1 \tag{3}$$
$$(\phi/\psi)/(\chi/\psi) = (\phi/\chi)/(\psi/\chi) \tag{4}$$

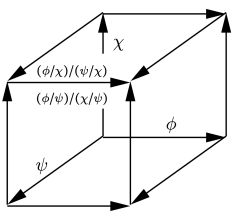
Gradification: RA to residual system

Definition (Residual system, Ch. 8 of Term Rewriting Systems 2003)

residual system $\langle \to, 1, / \rangle$ with for coinitial ϕ, ψ, χ in ARS $\to$:

$$\phi/1 = \phi \tag{1}$$
$$\phi/\phi = 1 \tag{2}$$
$$1/\phi = 1 \tag{3}$$
$$(\phi/\psi)/(\chi/\psi) = (\phi/\chi)/(\psi/\chi) \tag{4}$$

(4) is Lévy's cube:



Residual systems

Example

- single β-steps in linear $\lambda\beta$-calculus (do not have joins)
  proofterms as steps; terms over signature and rules (single rule)

Residual systems

Example

- parallel steps $\rightarrow\!\!\!\!\!\!+\!\!\!\!\!\!\rightarrow$ in orthogonal TRSs (do not have joins)
  proofterms as steps; terms over signature and rules (non-nested)

Residual systems

Example

- multi-steps $\multimap\!\!\!\!\circ\!\!\!\!\rightarrow$ in orthogonal HRSs (have joins), e.g. $\lambda\beta$
  proofterms as steps; terms over signature and rules (no restriction)

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- sets of non-overlapping patterns for associativity

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- parallel crossings of strands for positive braids

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- sets of closed parallel distributions for self-distributivity

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- multi-redexes or multi-treks in axiomatic residual theory (Melliès, RTA 2002)

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- multi-redexes or multi-treks in axiomatic residual theory (Melliès, RTA 2002)

Remark

do not rely on a notion of development (Church–Rosser 1936):

- *cube fails for developments in λ-calculus, term rewriting, braids, . . .*
- *proofterms also work for orthogonal (non-collapsing) infinitary rewriting*

Residual systems

Example

- multi-steps in orthogonal structure rewrite systems (joins), e.g. term, graph proofterms as steps; structures over signature and rules
- multi-redexes or multi-treks in axiomatic residual theory (Melliès, RTA 2002)

Lemma

- *projection order* $\phi \leqslant \psi := \phi/\psi = 1$ *is quasi-order; need not be partial order*
- *projection equivalence* $\leqslant \cap \geqslant$ *is congruence; quotient RA is RA*

Gradification: RA to residual system, with composition

Definition (Residual system with composition, Ch. 8 of Terese 2003)

residual system $\langle \to, 1, /, \cdot \rangle$ with composition $\cdot$ and for coinitial ϕ, ψ, χ in ARS $\to$:

$$\phi/1 = \phi \tag{1}$$
$$\phi/\phi = 1 \tag{2}$$
$$1/\phi = 1 \tag{3}$$
$$(\phi/\psi)/(\chi/\psi) = (\phi/\chi)/(\psi/\chi) \tag{4}$$
$$\chi/(\phi \cdot \psi) = (\chi/\phi)/\psi \tag{7}$$
$$(\phi \cdot \psi)/\chi = (\phi/\chi) \cdot (\psi/(\chi/\phi)) \tag{8}$$

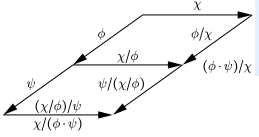
Gradification: RA to residual system, with composition

Definition (Residual system with composition, Ch. 8 of Terese 2003)

residual system $\langle \to, 1, /, \cdot \rangle$ with composition $\cdot$ and for coinitial ϕ, ψ, χ in ARS $\to$:

$$\phi/1 = \phi \tag{1}$$
$$\phi/\phi = 1 \tag{2}$$
$$1/\phi = 1 \tag{3}$$
$$(\phi/\psi)/(\chi/\psi) = (\phi/\chi)/(\psi/\chi) \tag{4}$$
$$\chi/(\phi \cdot \psi) = (\chi/\phi)/\psi \tag{7}$$
$$(\phi \cdot \psi)/\chi = (\phi/\chi) \cdot (\psi/(\chi/\phi)) \tag{8}$$

composite identities (7) and (8):



Residual systems with composition

Example

- reductions of CRA steps
  reductions as normal forms of orienting monoid identities, (7),(8) left to right

Residual systems with composition

Example

- reductions of CRA steps
  reductions as normal forms of orienting monoid identities, (7),(8) left to right
- any countable confluent ARS admits residual system with composition
  by choosing first common reduct along trunk of tree obtained by cofinality

Residual systems with composition

Example

- reductions of CRA steps
  reductions as normal forms of orienting monoid identities, (7),(8) left to right
- any countable confluent ARS admits residual system with composition
  by choosing first common reduct along trunk of tree obtained by cofinality

Lemma

projection equivalence $\leqslant \cap \geqslant$ *is congruence; quotient RA w/ composition is such*

Residual systems with composition

Example

- reductions of CRA steps
  reductions as normal forms of orienting monoid identities, (7),(8) left to right
- any countable confluent ARS admits residual system with composition
  by choosing first common reduct along trunk of tree obtained by cofinality

Lemma

projection equivalence $\leqslant \cap \geqslant$ is congruence; quotient RA w/ composition is such

Remark

projection equivalent $\Leftrightarrow$ homotopic in axiomatic residual theory (Melliès)

Residual systems with composition

Example

- reductions of CRA steps
  reductions as normal forms of orienting monoid identities, (7),(8) left to right
- any countable confluent ARS admits residual system with composition
  by choosing first common reduct along trunk of tree obtained by cofinality

Lemma

projection equivalence $\leqslant \cap \geqslant$ is congruence; quotient RA w/ composition is such

Remark

projection $\Leftrightarrow$ permutation, labelling, standardisation, extraction, causal?
Lévy ((weak) $\lambda\beta$, Stark (processes), Terese (TRSs), Wolfram (causal invariance)

Gradification: Involutive monoid to fractions

Definition

fraction (valley) $\frac{\phi}{\psi}$ for ϕ, ψ cofinal in RS with composition. for $f := \frac{\phi}{\psi}$, $g := \frac{\phi'}{\psi'}$:

reciprocal f^{-1} of f is $\frac{\psi}{\phi}$, product $f \cdot g$ of f and g is $\frac{\phi \cdot (\phi'/\psi)}{\psi' \cdot (\psi/\phi')}$, division $f \,/\, g$ is $g^{-1} \cdot f$

Gradification: Involutive monoid to fractions

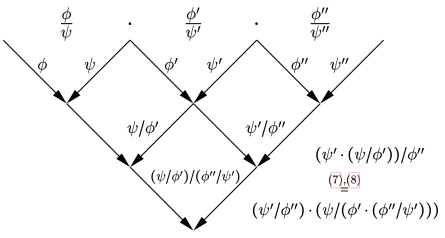
Definition

fraction (valley) $\frac{\phi}{\psi}$ for ϕ, ψ cofinal in RS with composition. for $f := \frac{\phi}{\psi}$, $g := \frac{\phi'}{\psi'}$:

reciprocal f^{-1} of f is $\frac{\psi}{\phi}$, product $f \cdot g$ of f and g is $\frac{\phi \cdot (\phi'/\psi)}{\psi' \cdot (\psi/\phi')}$, division $f \,/\, g$ is $g^{-1} \cdot f$

Lemma

fractions constitute a typed involutive monoid



associativity by orthogonality:

Timeline

(1990–1995) equational reasoning for extensions of multisets (in 1994 PhD thesis; after review of decreasing diagrams by Jean–Pierre Jouannaud)

(1995–2000) residual systems as abstract notion of orthogonality in rewriting. (Jan Willem Klop: braids are confluent; Paul–André Melliès: braids are orthogonal; Chapter 8 in 2003 book Term Rewriting Systems)

(2000–2005) commutative residual algebras for equational reasoning on multisets (sorting formalisation in Coq for teaching Type Theory). representation theorem for finite CRAs (with Albert Visser). embeddings $\mathbb{B} \hookrightarrow \mathbb{N} \hookrightarrow \mathbb{Z}$ for residual algebra.

(2005–2010) CRA $\Leftrightarrow$ cBCK algebra with relative cancellation (using William McCune's Prover9/Mace; finding Dvurečenskij & Graziano). self-distributivity as RS (question EB?; reviewing Patrick Dehornoy for Pierre–Louis Curien). representation theorem well-founded CRAs (with Bas Luttik using decomposition orders in 2005 paper)

(2018–) inclusion/exclusion for CRAs (teaching Discrete Mathematics); EWD 1313 using CRAs (talking with Fabian Mitterwallner on creating exercises by using IMOs, EWDs)

Questions

Equational theory of CRAs

- equational theory decidable?

Questions

Equational theory of CRAs

- equational theory decidable if $\leqslant$ well-founded?

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment?

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?
  hope some people can answer/have answered?

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?
  guess: yes (Presburger?); no (Squier?)

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?
  guess: yes (Presburger?); no (Squier?)
- CRA-based equational reasoning about multisets in proof assistants?

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?
  guess: yes (Presburger?); no (Squier?)
- CRA-based equational reasoning about multisets in proof assistants?
  (Burak Ekici?; Isabelle finite multisets (no measures); Coq several; ad hoc)

Questions

Equational theory of CRAs

- equational theory decidable for interesting fragment; by complete TRS?
  guess: yes (Presburger?); no (Squier?)
- CRA-based equational reasoning about multisets in proof assistants?
  (Burak Ekici?; Isabelle finite multisets (no measures); Coq several; ad hoc)

Extensions

- reasoning for multiset-extension $M <_{ext} N$ if $(M/N) \leq \vee(N/M)$, $N \neq 1$?
- meet for residual systems (no commutativity/(5),(6); cf. join via residual)?

function mapping co-final steps to meeting step: