LICS 2012 DUBROVNIK

Tutorial

Term Rewriting & Lambda Calculus

Jan Willem Klop
Jörg Endrullis

VU UNIVERSITY Amsterdam

0. A few words on history

1. rewriting dictionary

2. two theorems in abstract rewriting

3. word rewriting: monoids and braids

TEA, COFFEE

4. term rewriting: divide et impera; termination by stars

5. Lambda calculus and combinatory logic

6. Infinitary rewriting

TEA, COFFEE

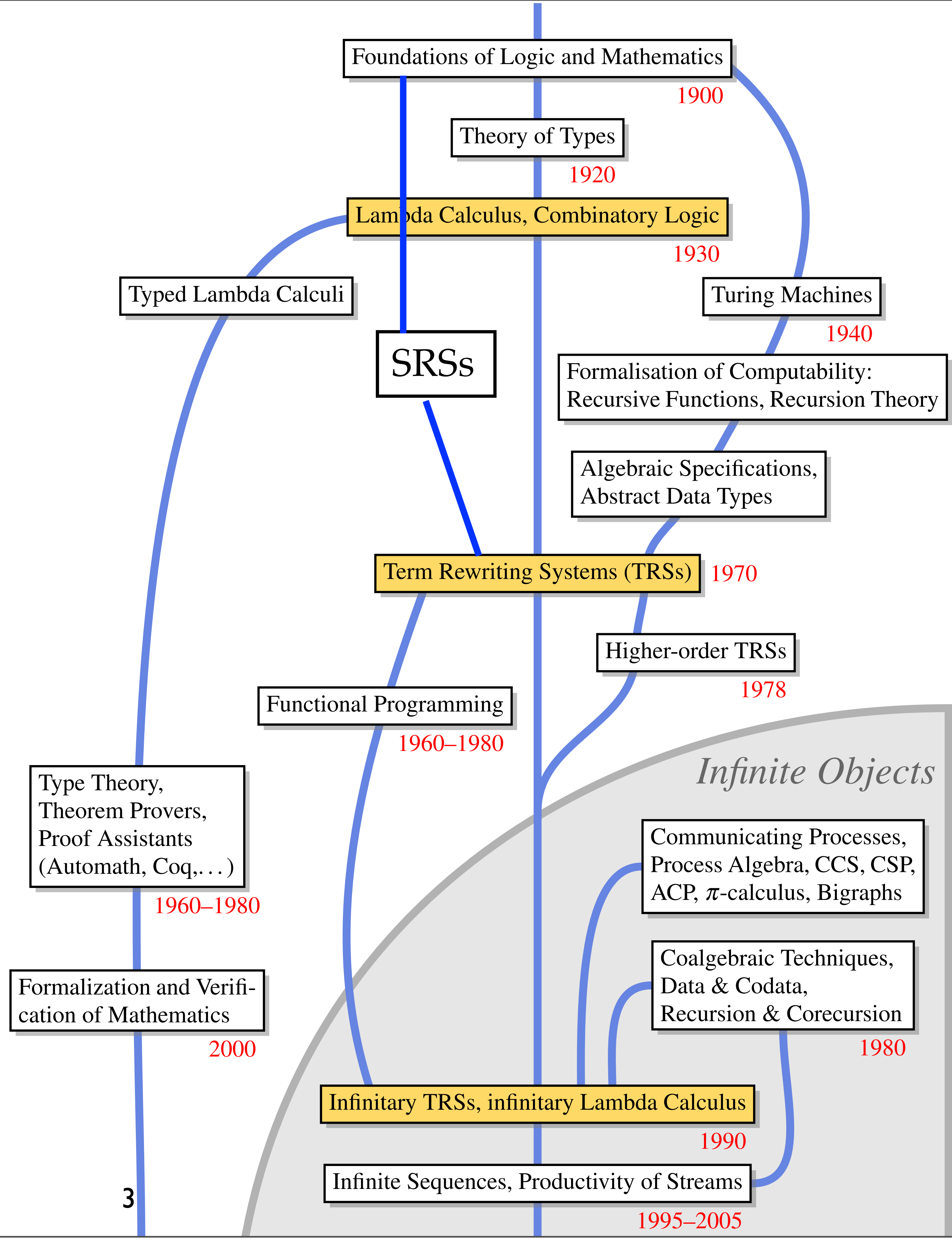
7. infinitary lambda calculus and the threefold path

8. clocked semantics of lambda calculus

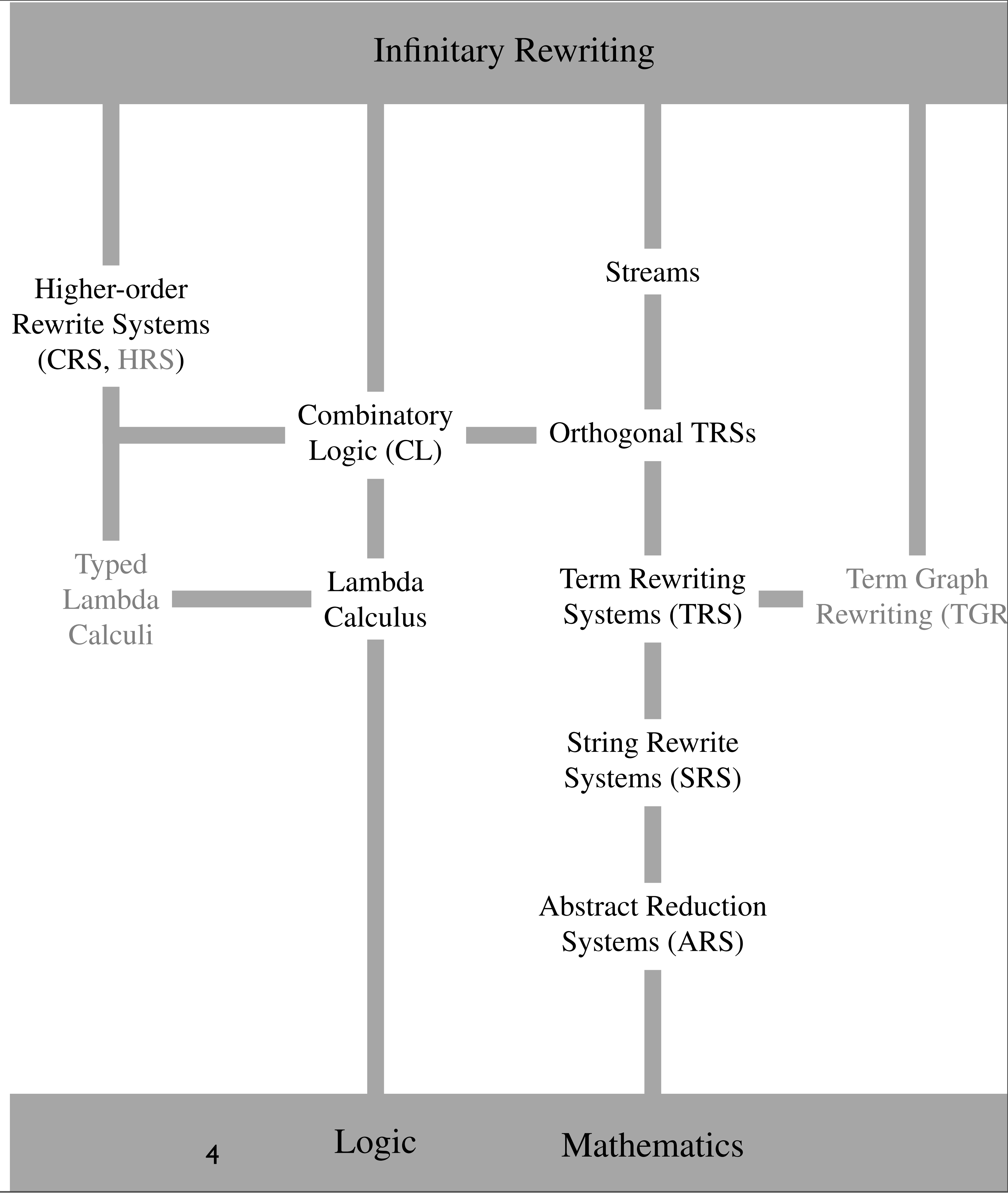
9. streams running forever

0. A few words on history

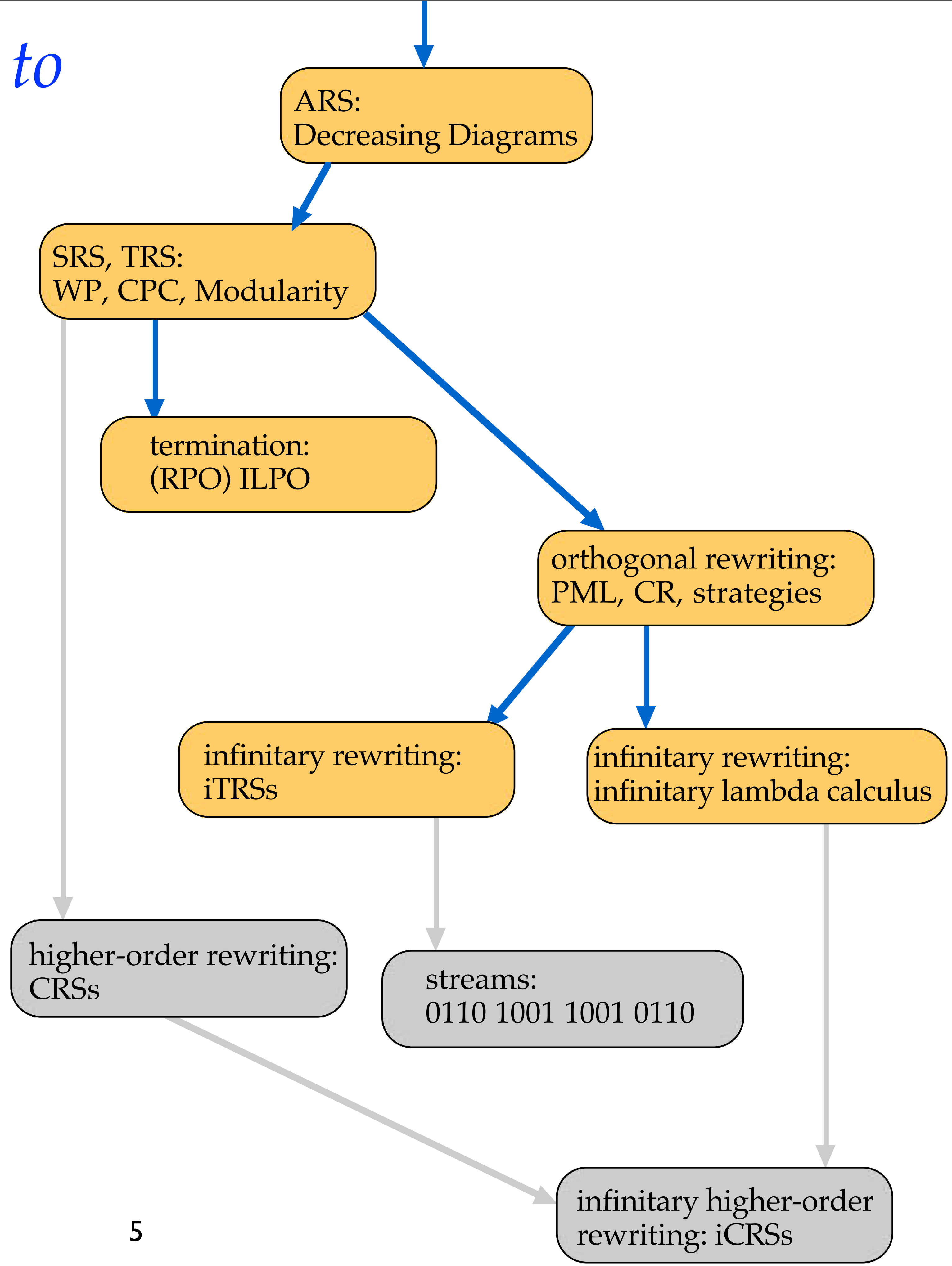
Some historical lines...



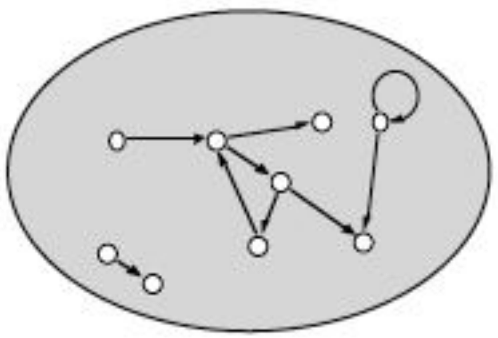
Some streets we want to walk



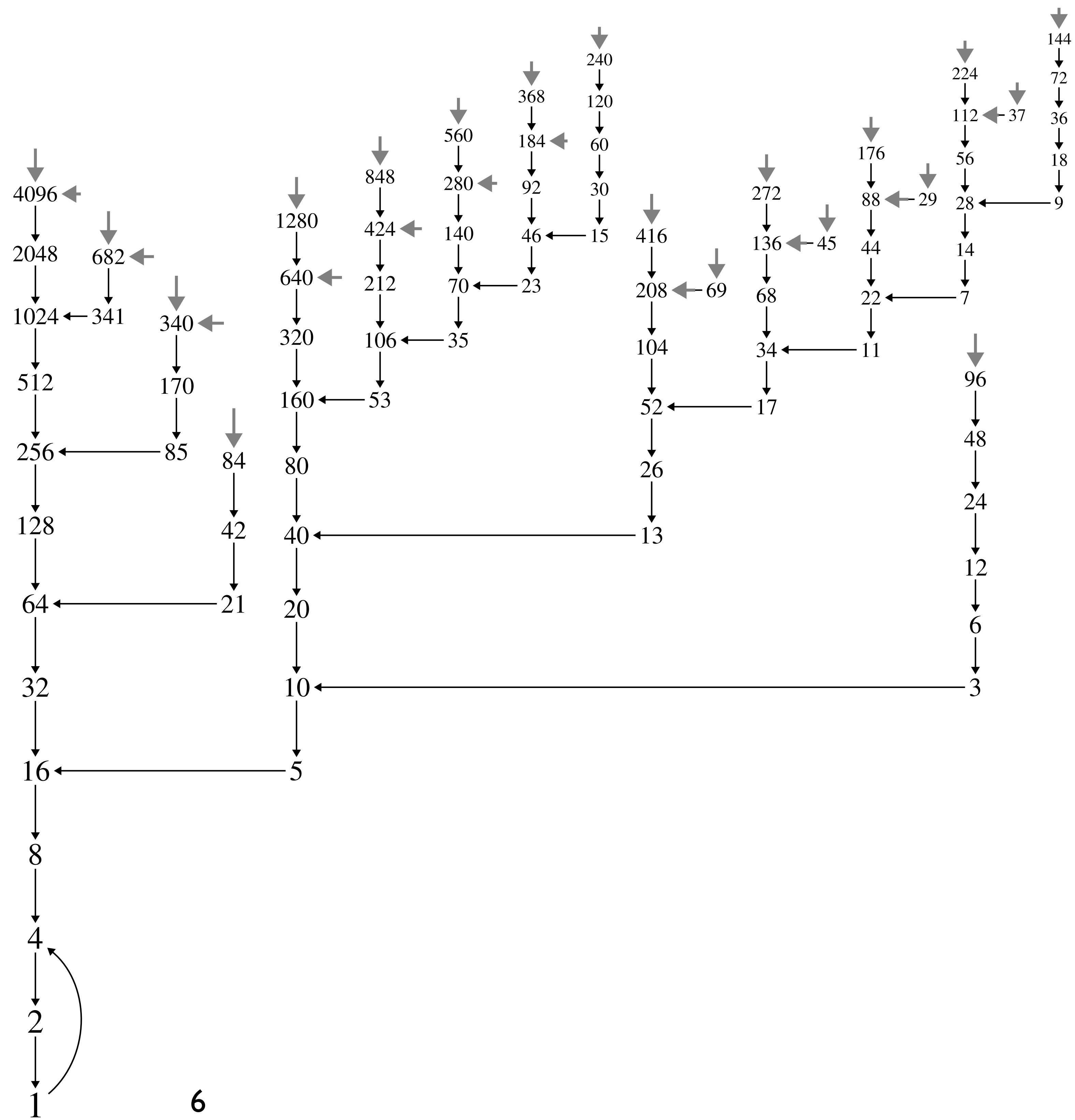
capita that we would like to discuss



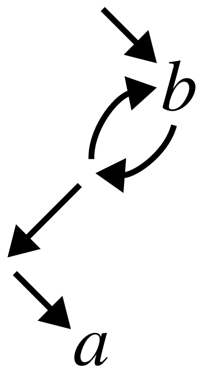
The famous Collatz ARS: 3n+1-problem



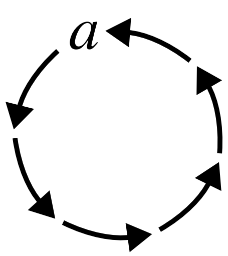
An ARS



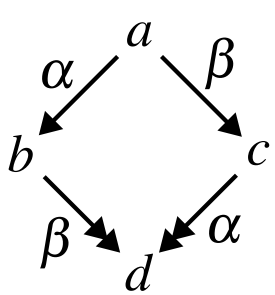
6



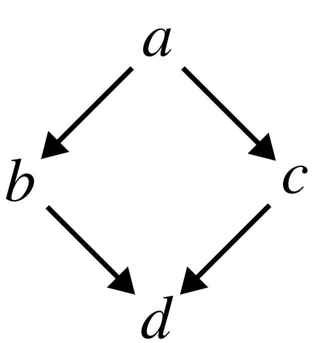
normal form



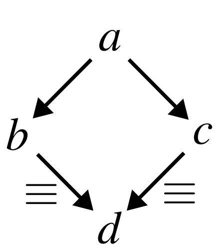
reduction cycle; loop if one step



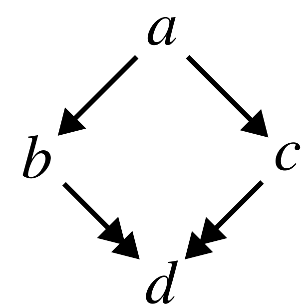
commuting



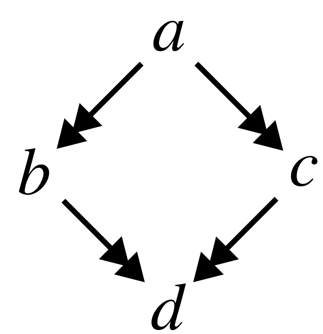
diamond property



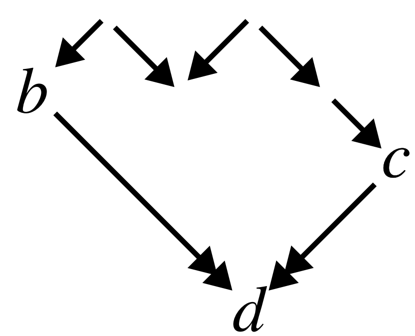
sub-commutative



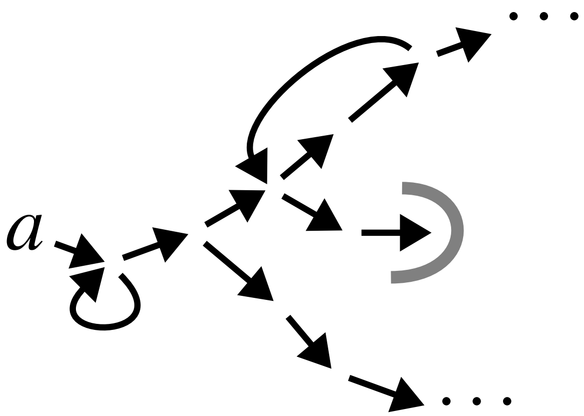
WCR, weakly Church-Rosser



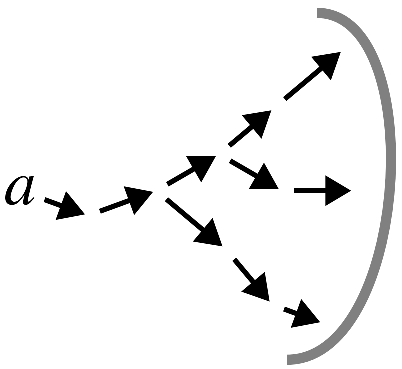
CR, Church-Rosser



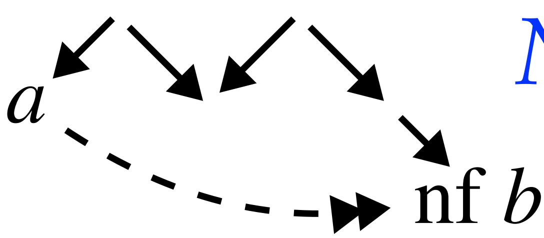
equivalent: CR, Church-Rosser



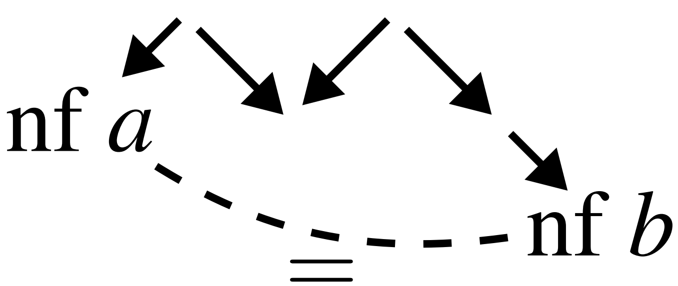
WN, weakly normalizing



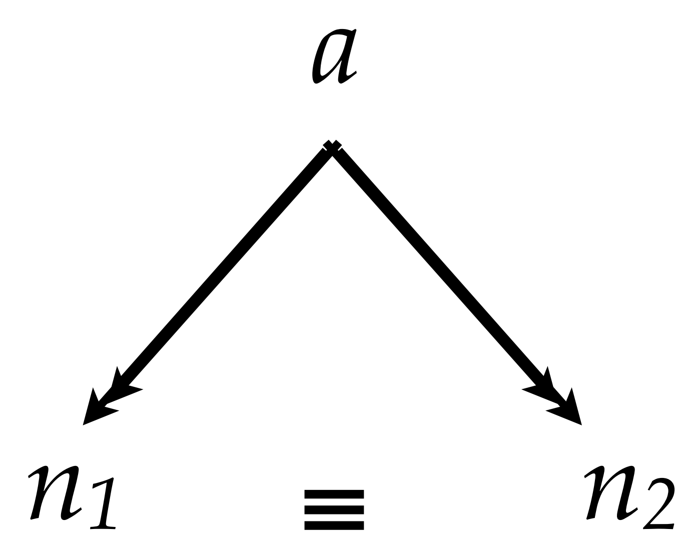
SN, strongly normalizing;terminating; noetherian



NF, normal form property

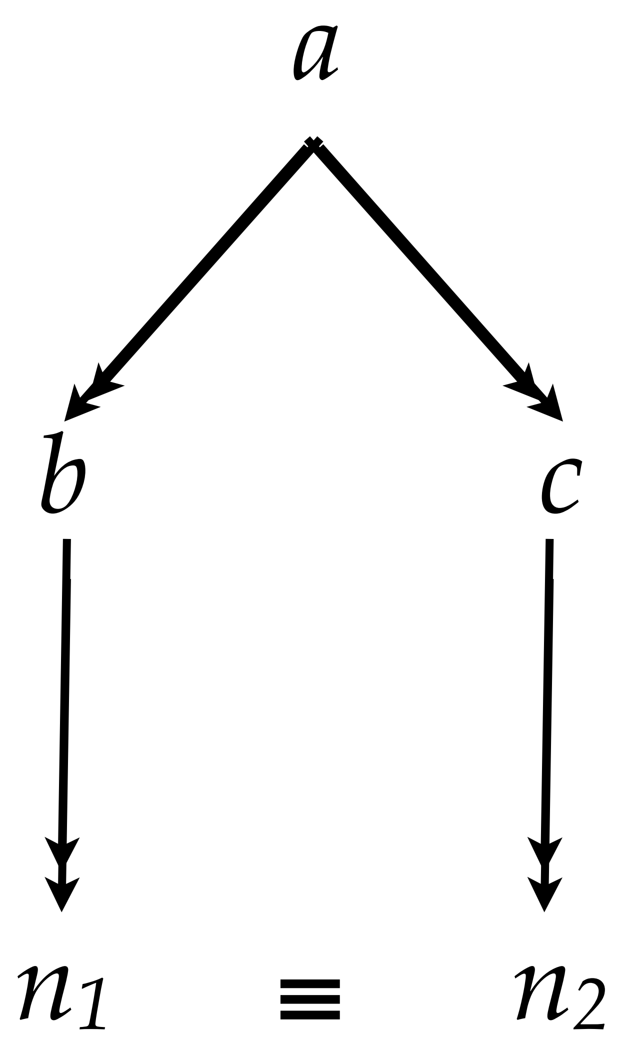


UN$^=$*, unique normal form property wrt* $=$

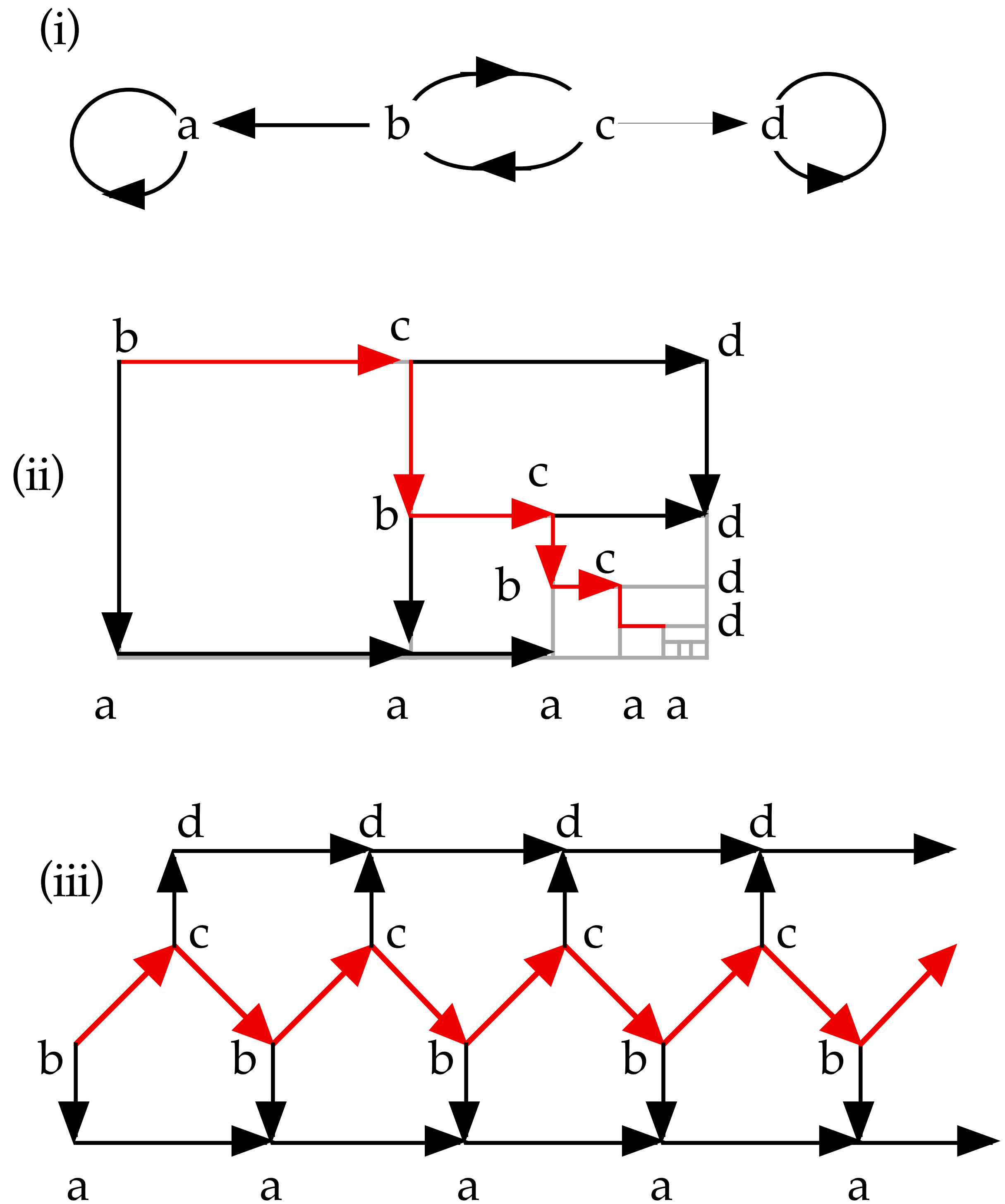


UN$^\rightarrow$*, unique normal form property wrt* $\rightarrow$

$UN^{\rightarrow} \,\&\, SN \Rightarrow CR$



CR ⇒ WCR, but not WCR ⇒ CR



shortest proof of Newman's Lemma:

$WCR\ \&\ SN \Rightarrow CR$

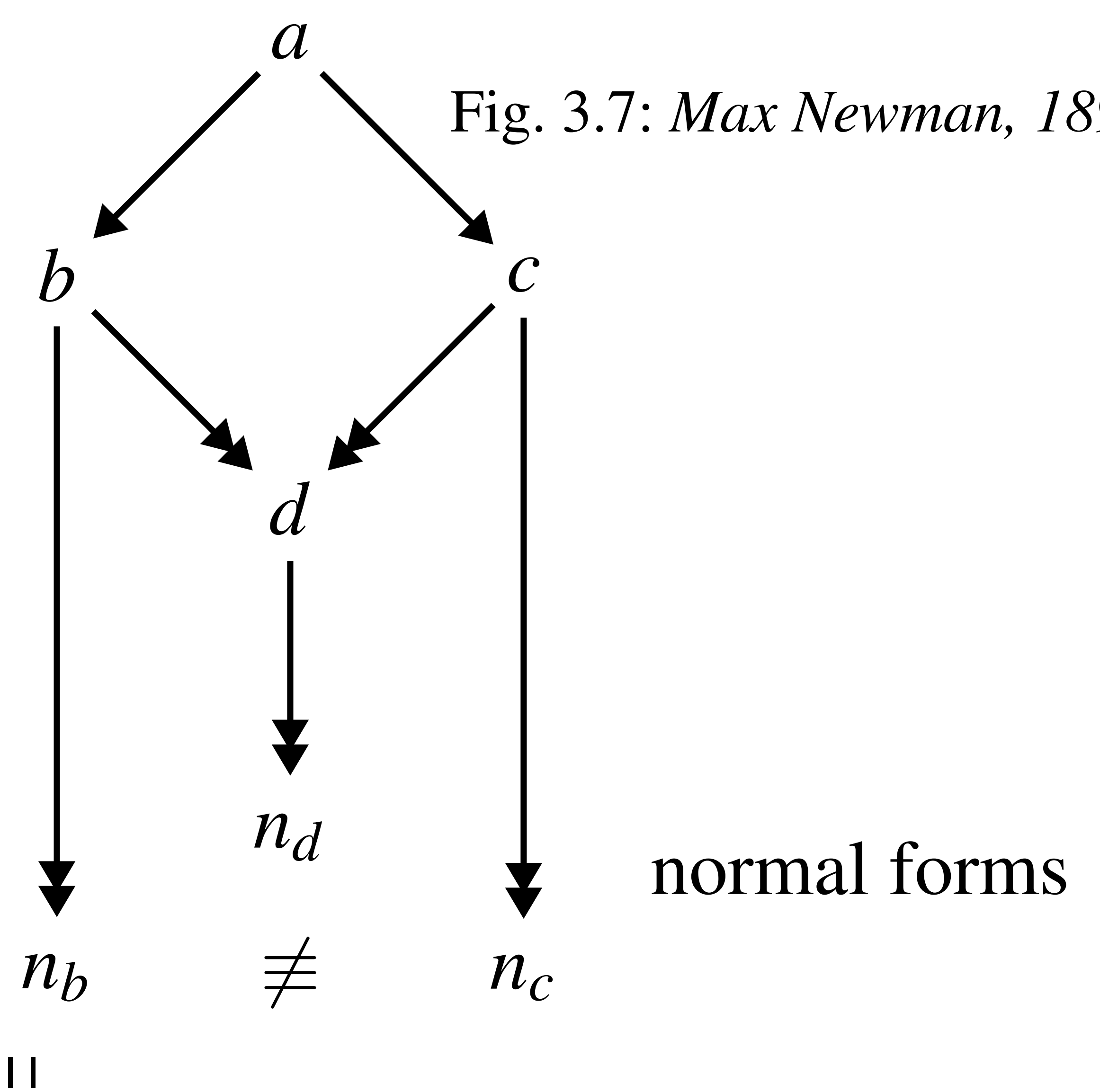
Fig. 3.7: *Max Newman, 1897-1984.*

$WCR\ \&\ SN \Rightarrow UN^{\rightarrow}\ \&\ SN \Rightarrow CR$

Call a point bad if it reduces to two different nf's.

A bad point a has a bad one step reduct, b or c.

Hence by SN there are no bad points, i.e. $UN^{\rightarrow}$ holds.



Church (1903-1995)
Studying mathematics at
Princeton 1922 or 1924

Supervisor	Oswald Veblen
Suggested topic	find an algorithm for the genus of a manifold $\{\vec{x}\in K^n \mid p(\vec{x}) = 0\}$ (e.g. $K = \mathbb{R}$, $n = 3$)

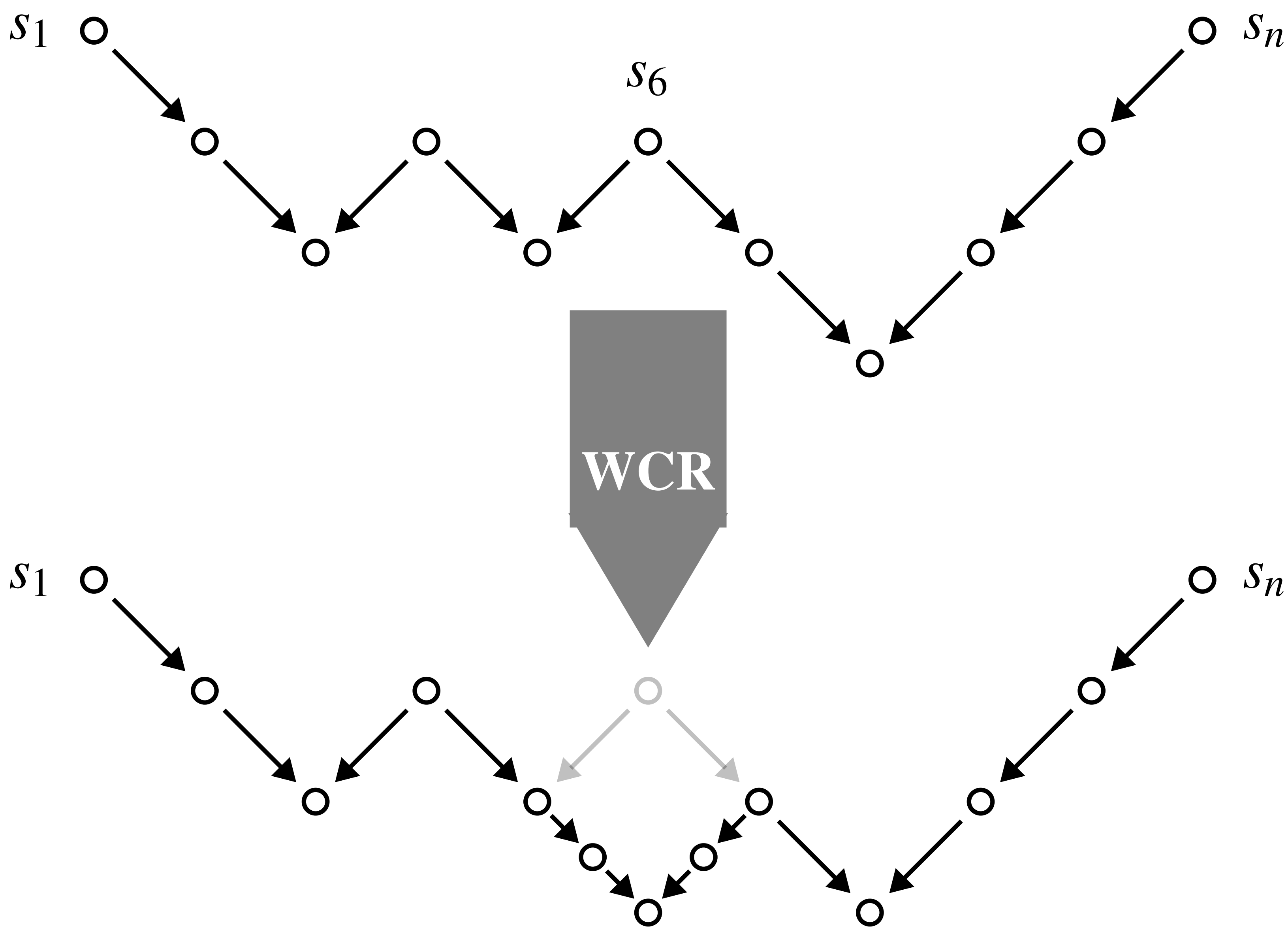
0 1 2 3 ?

Church could not do it
Started to wonder what computability is after all
Invented lambda calculus
Formulated Church's Thesis:

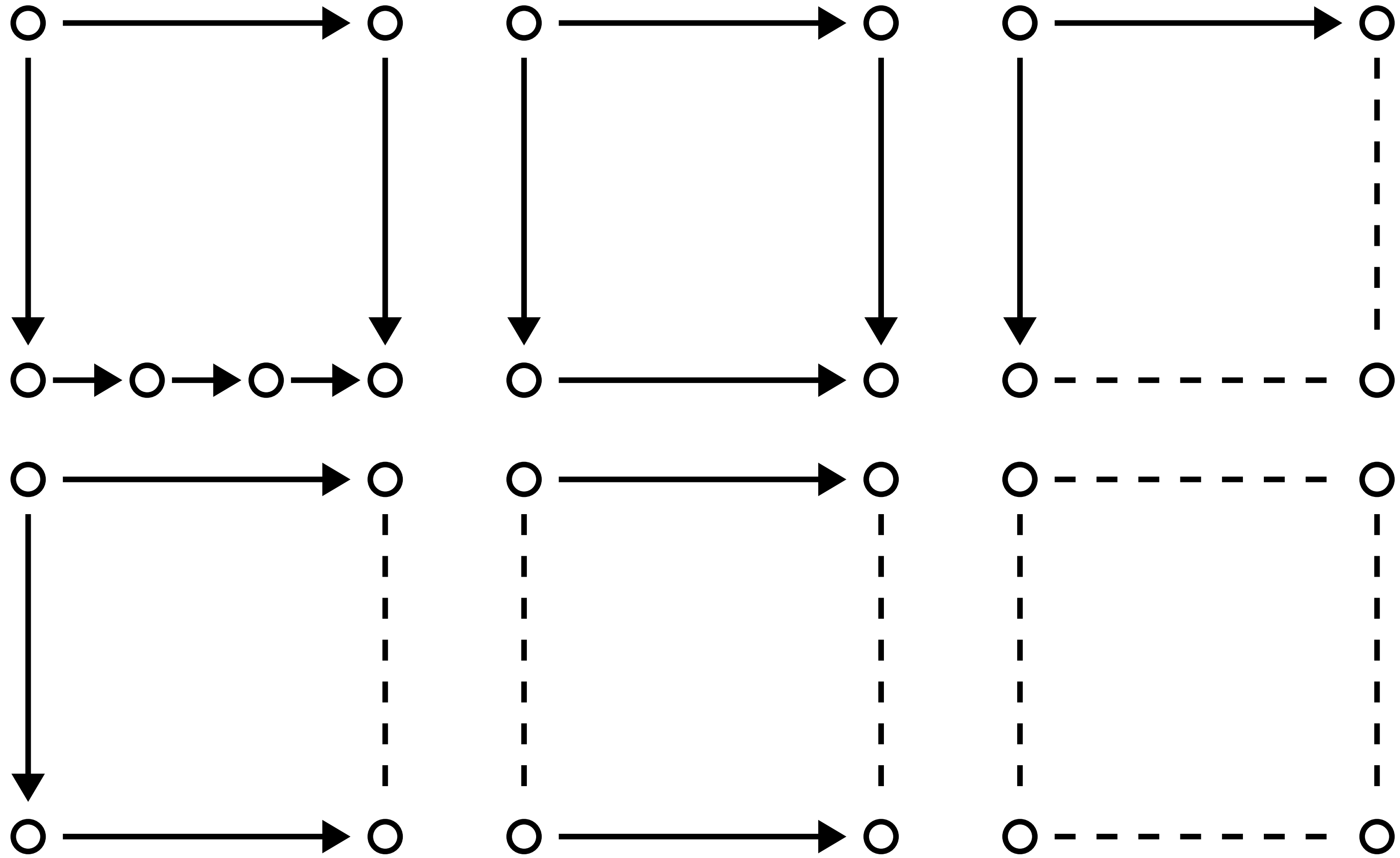
Given a function $f : \mathbb{N}^k \to \mathbb{N}$

Then f *is computable iff* f *is lambda definable*

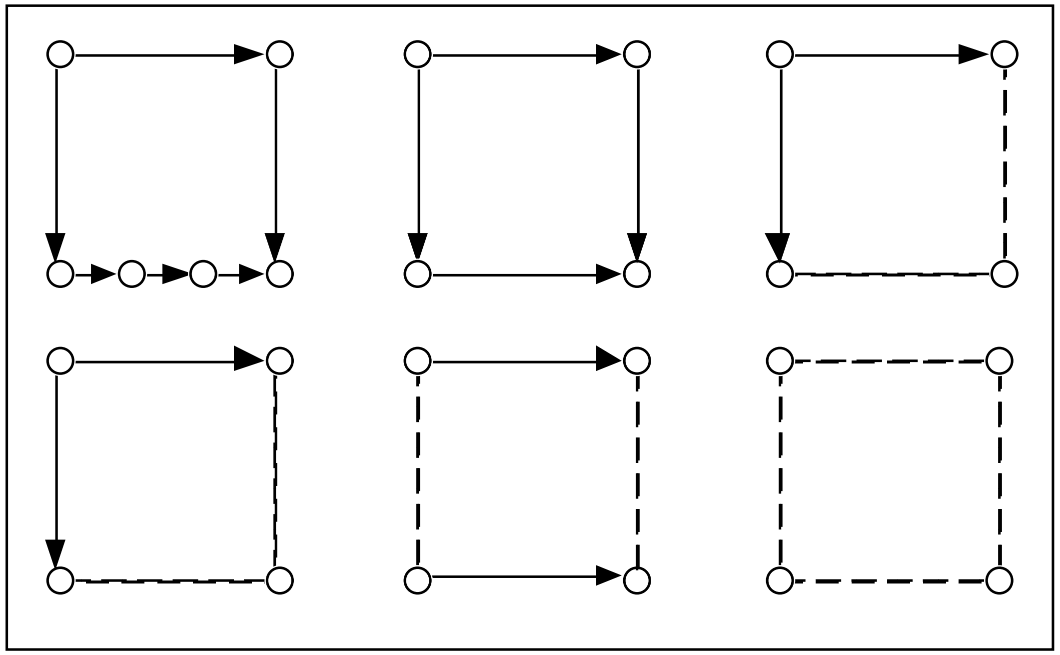
sophisticated multiset proof of Newman's Lemma:

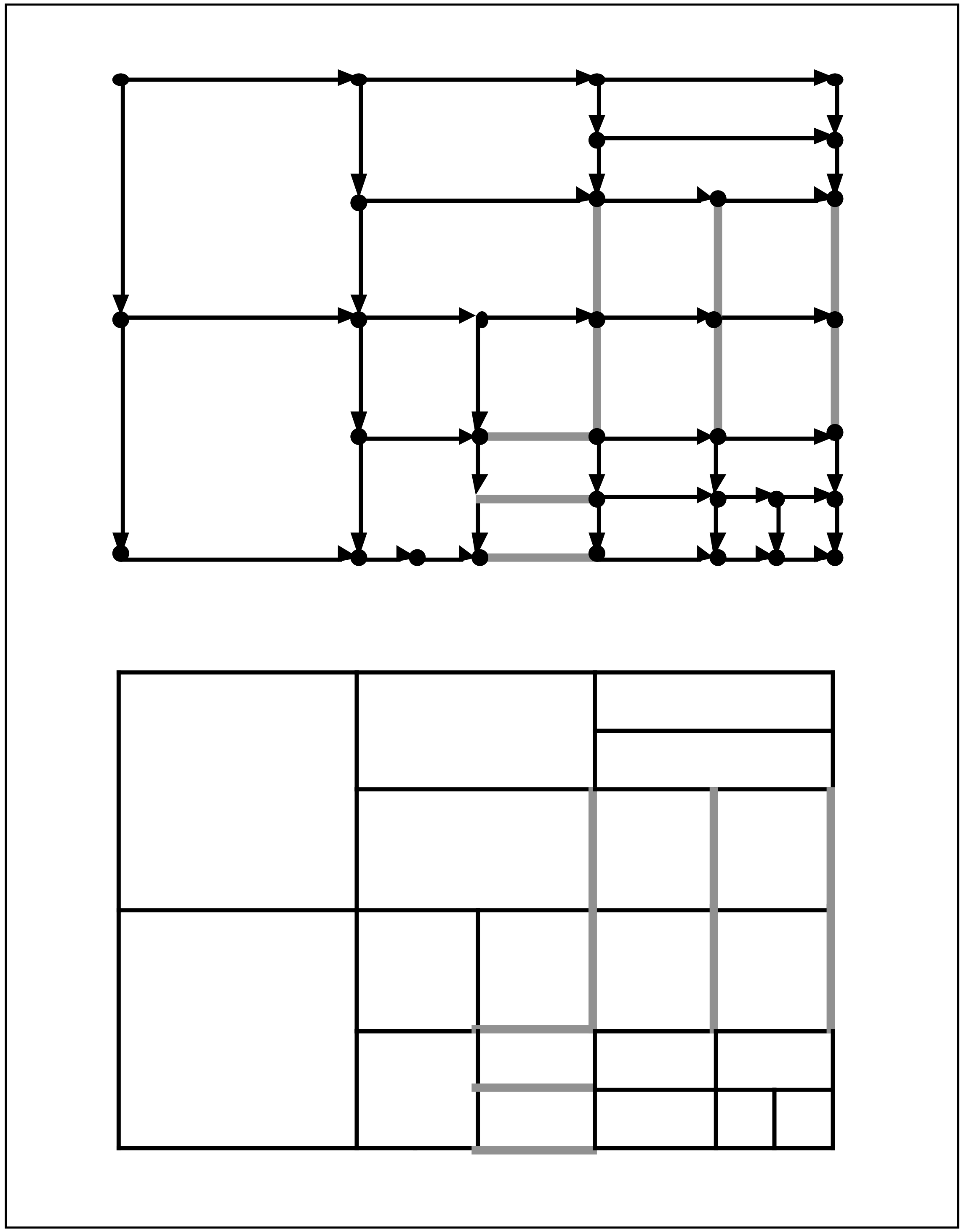


elementary diagrams to build reduction diagrams, given WCR

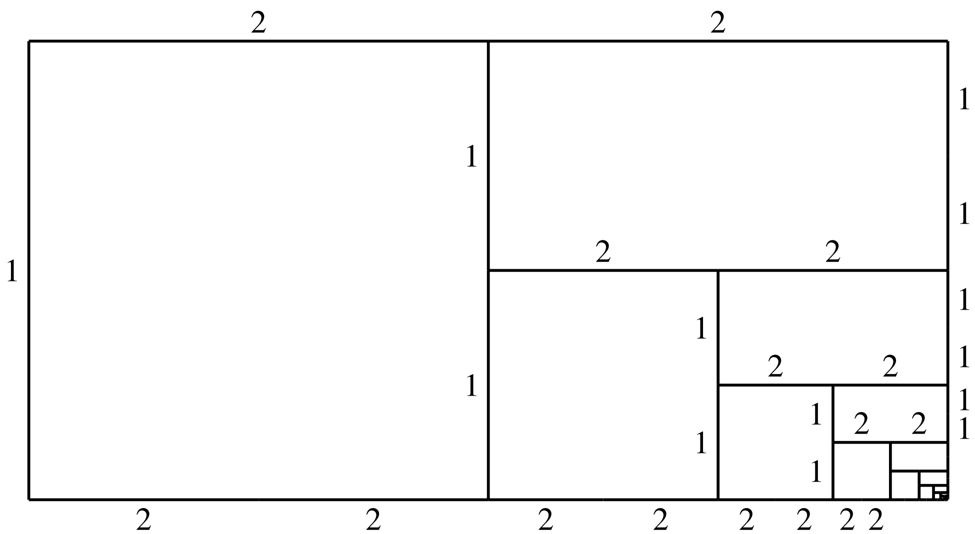


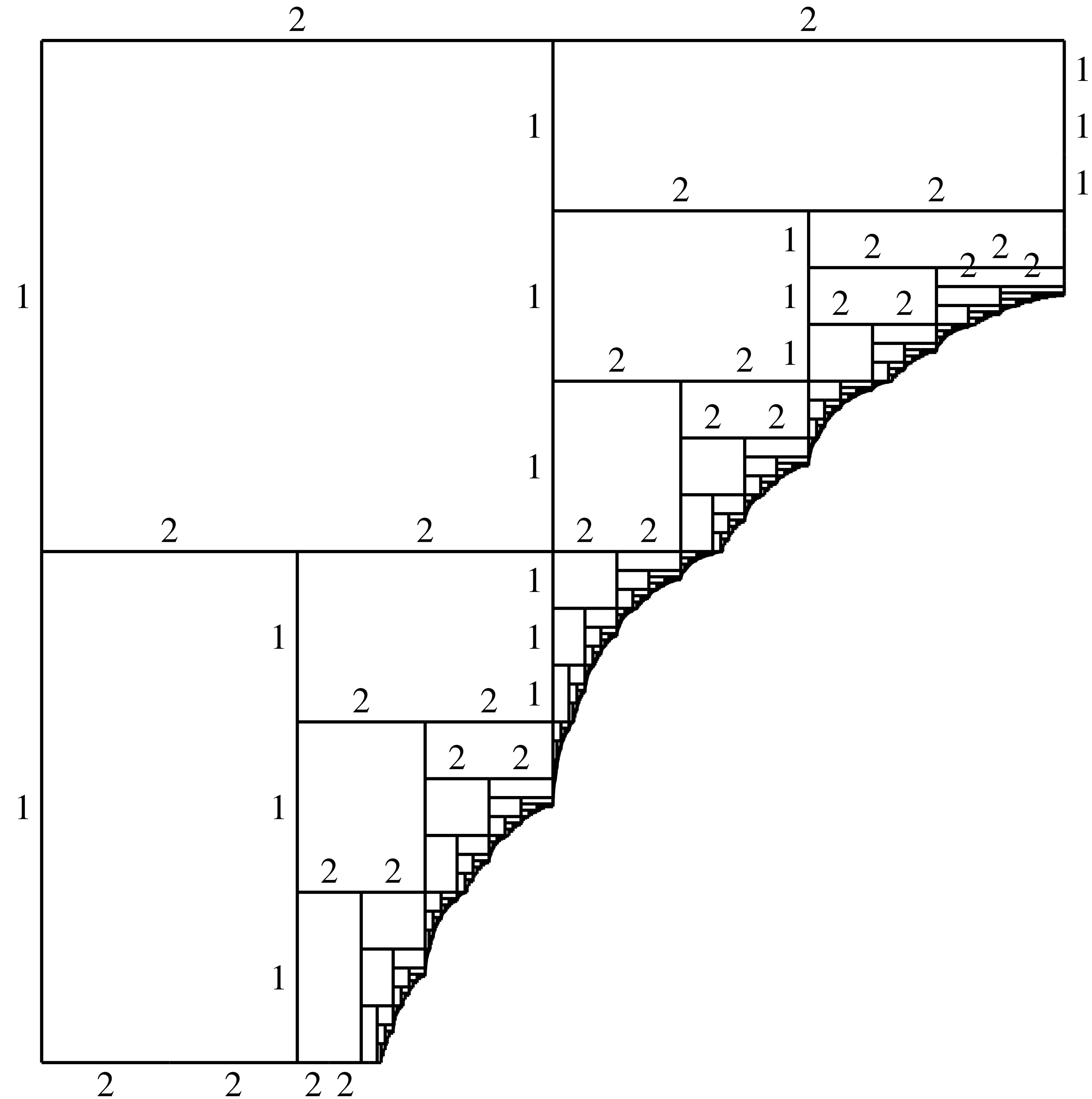
completed reduction diagrams



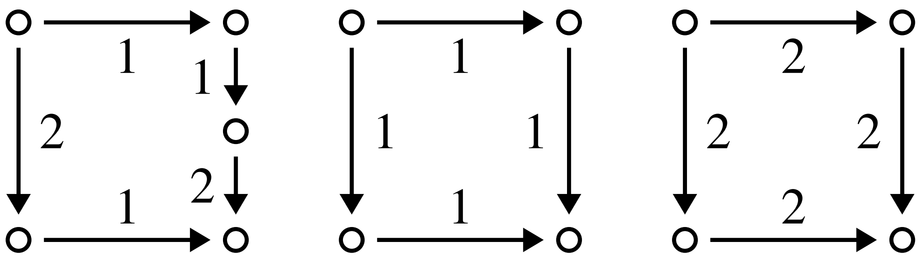


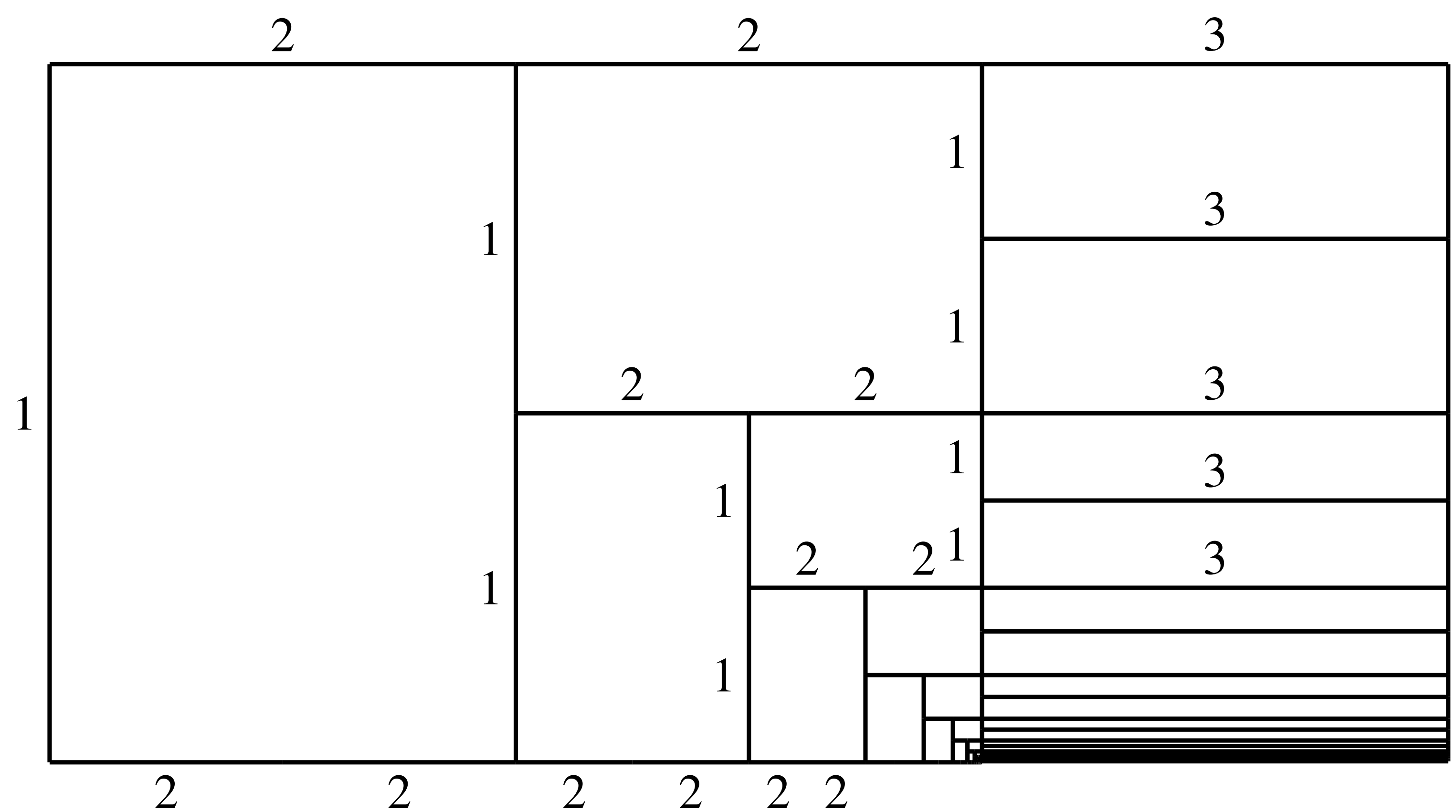
failed reduction diagrams



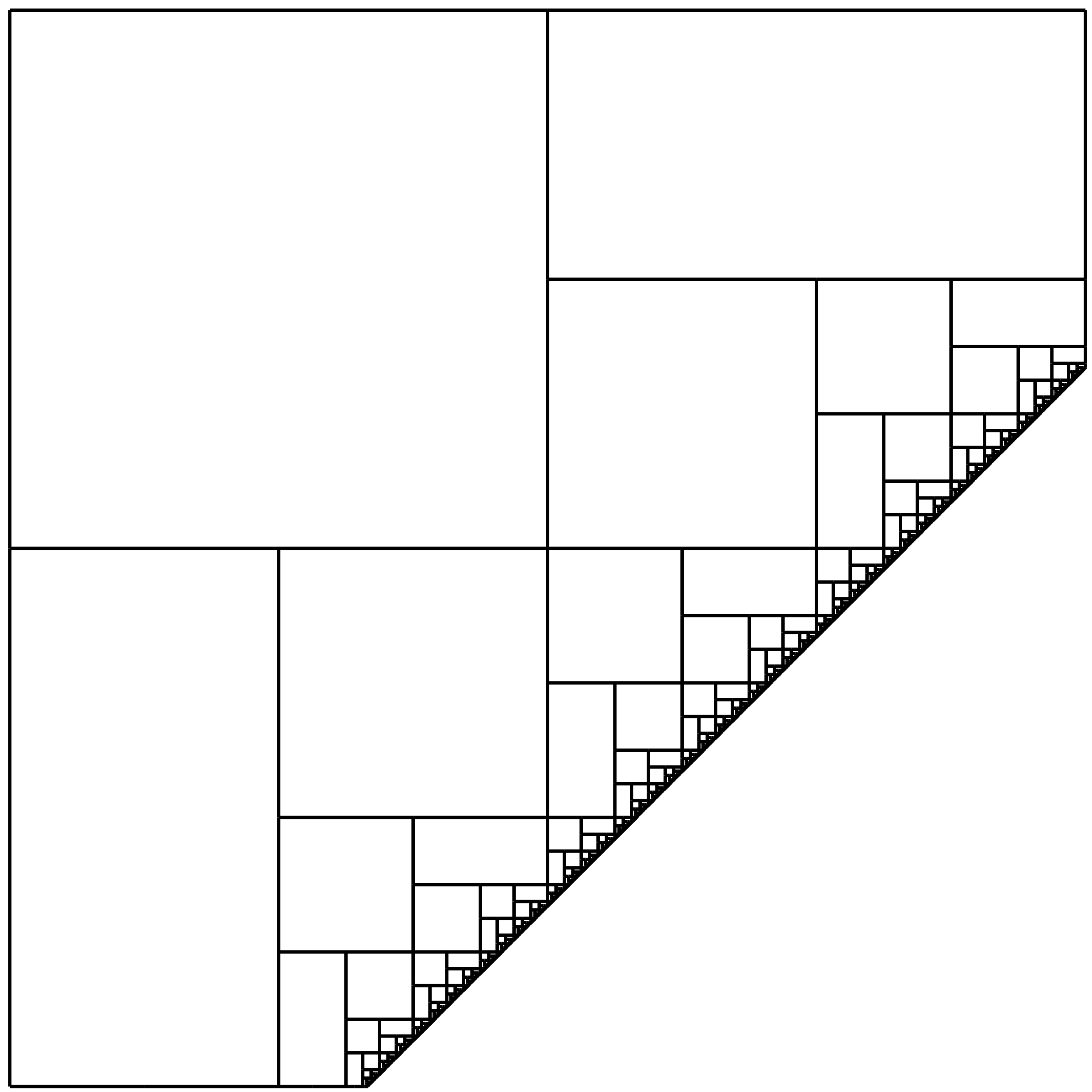


another failure



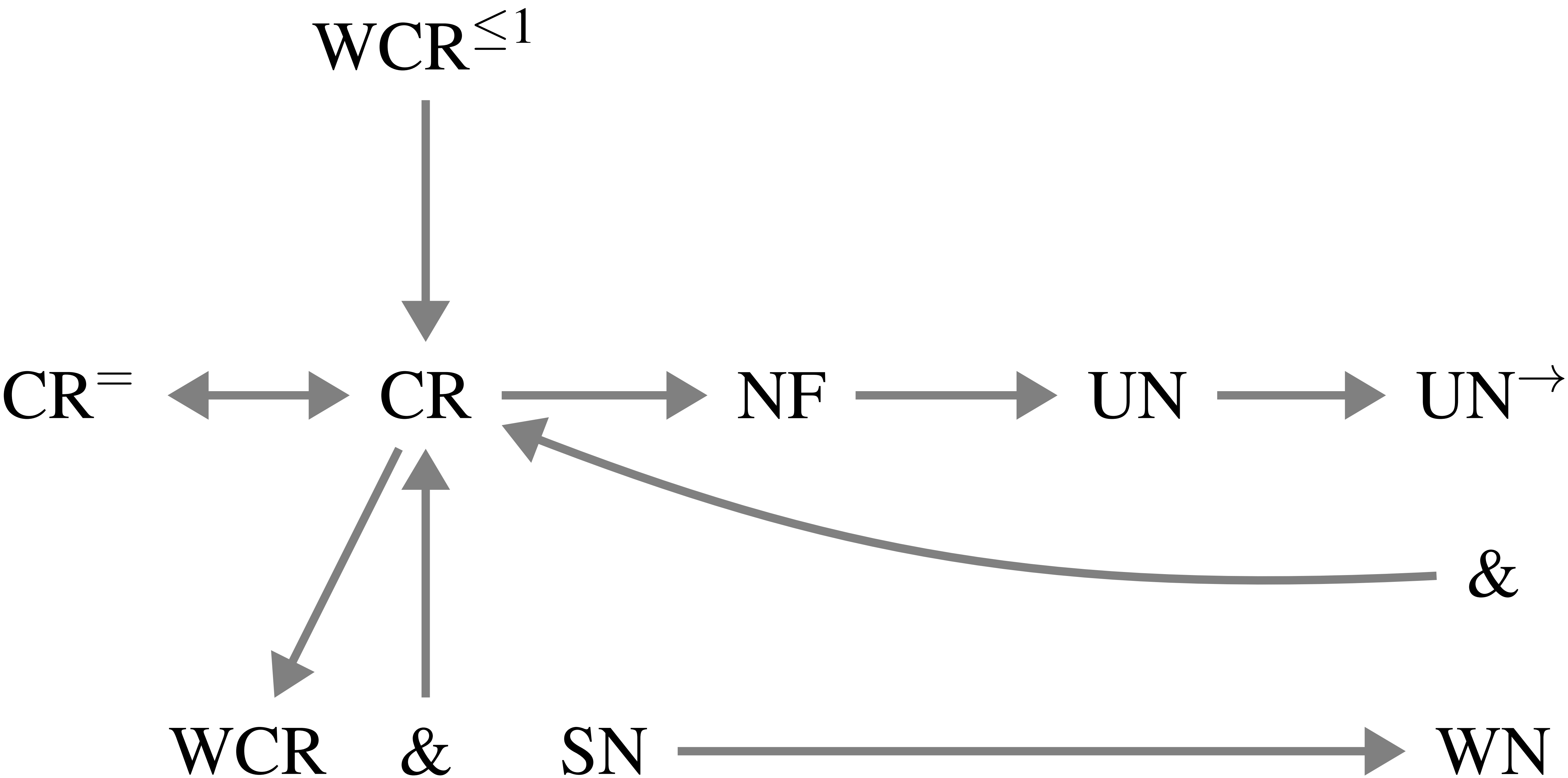


and one more

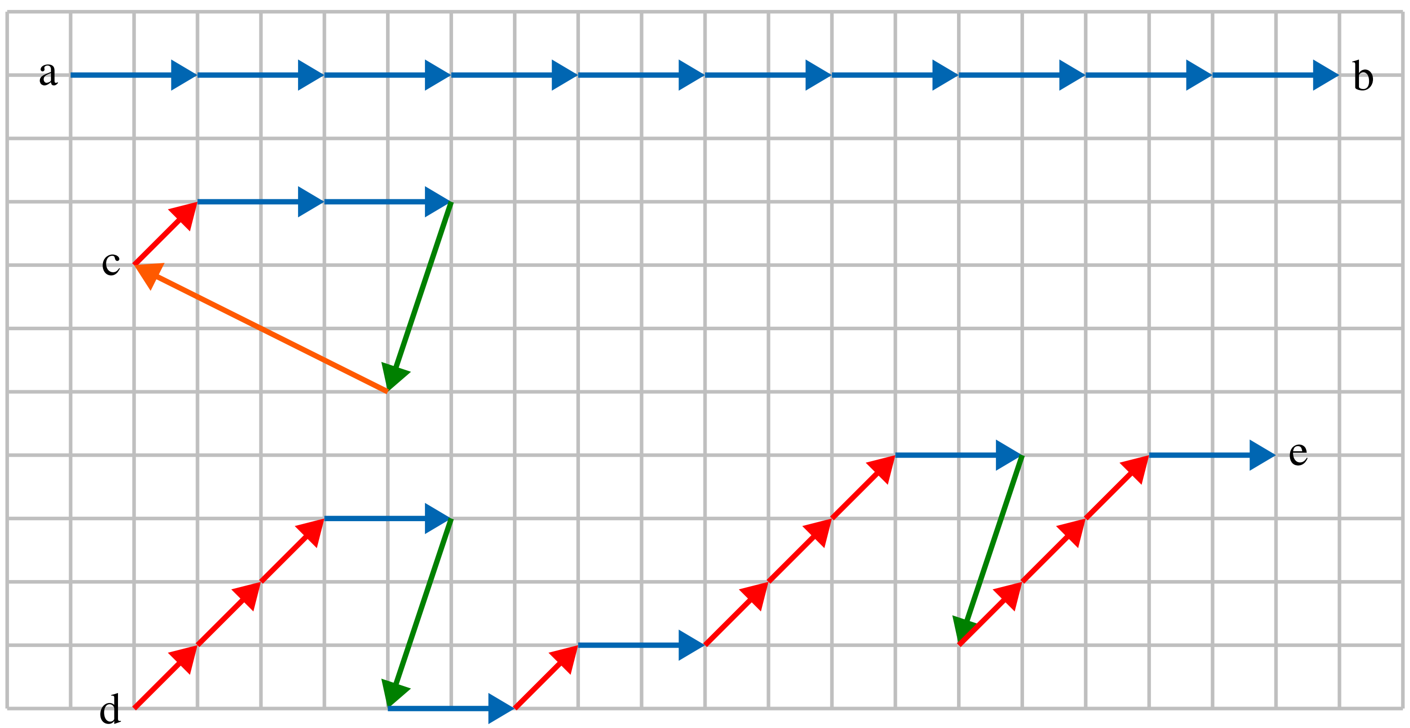


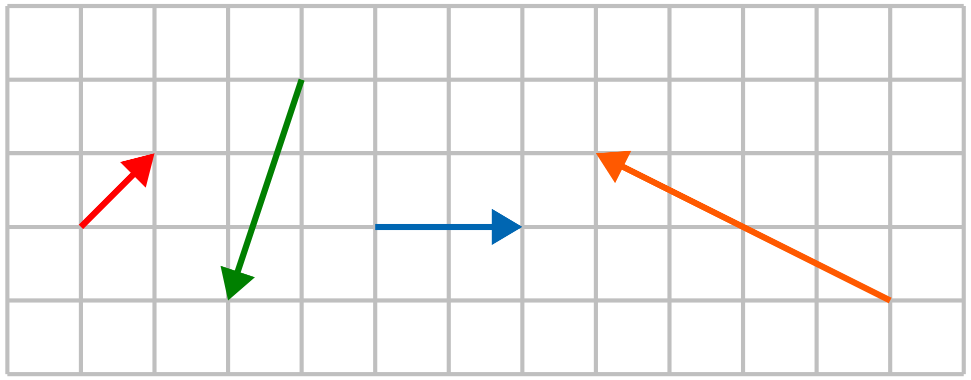
18

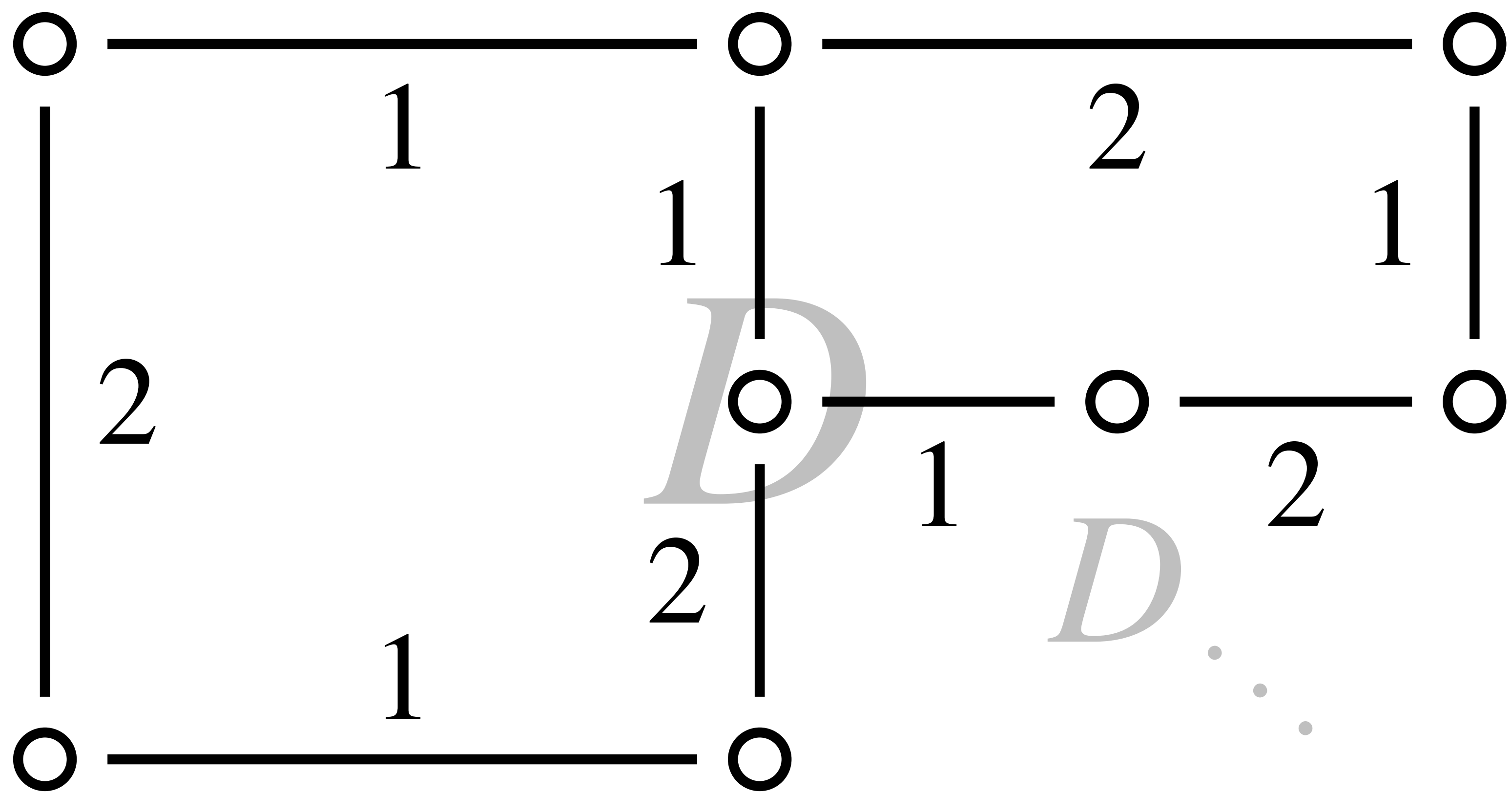
speaking for itself

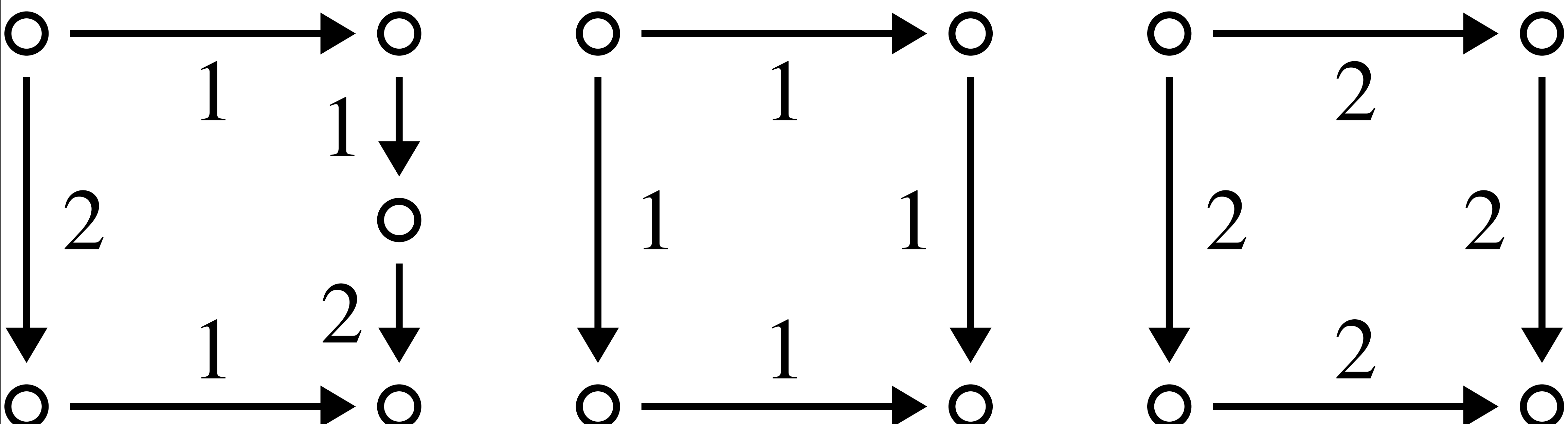


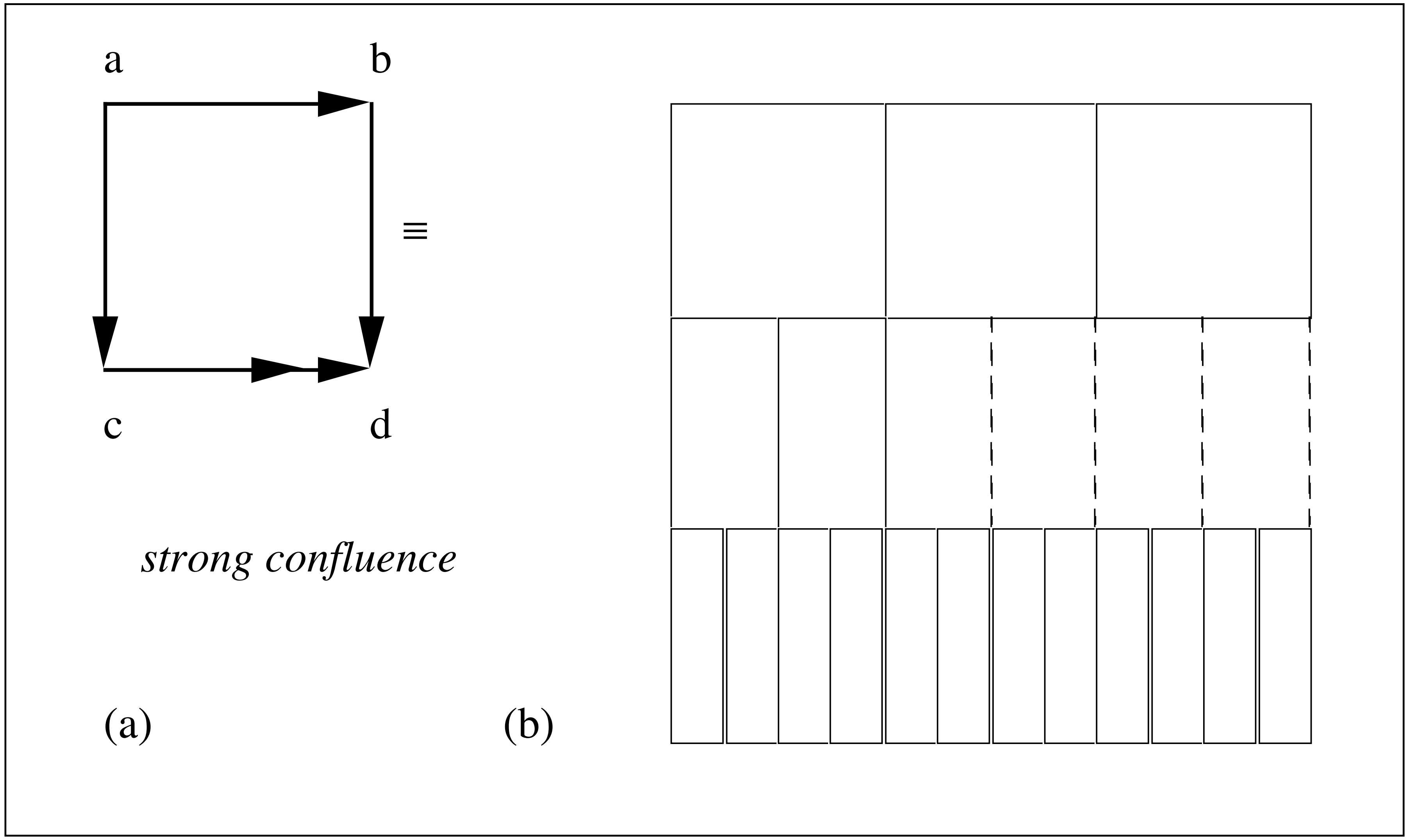
a vector addition system: indexed ARS






1
2
1
1
2
D
1
2
D
2
1


1
1
2
2
1
1
1
1
1
2
2
2
2

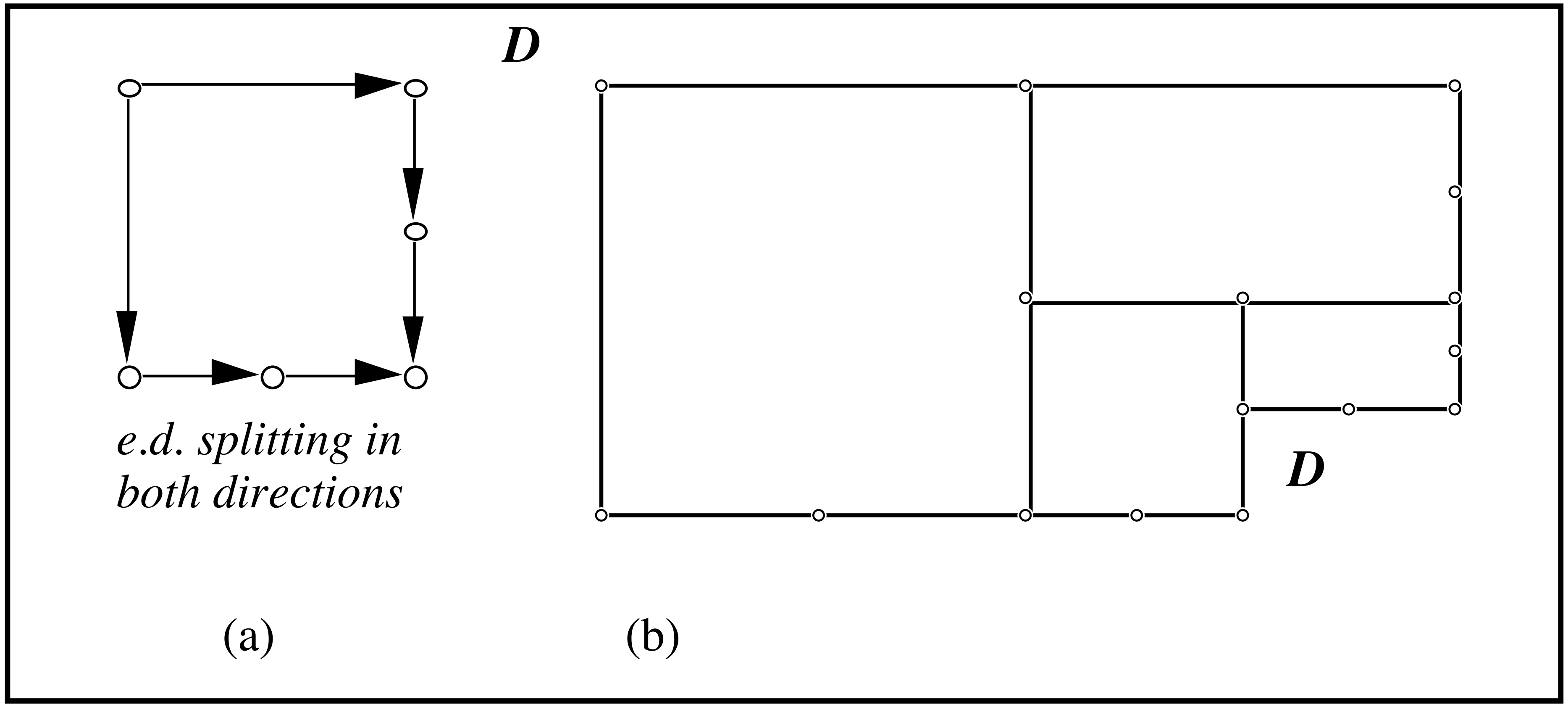


1.2.1. EXAMPLE. 1.2.2. DEFINITION. For an ARS $\mathcal{A} = \langle A, \to \rangle$ we define: $\to$ is *strongly confluent* if

$$\forall a, b, c \in A\, \exists d \in A (b \leftarrow a \to c \Rightarrow c \twoheadrightarrow d \twoheadleftarrow^{\equiv} b)$$

(See Figure 1.9(a)) (Here $\twoheadleftarrow^{\equiv}$ is the reflexive closure of $\twoheadleftarrow$, so $b \twoheadrightarrow^{\equiv} d$ is zero or one step.)

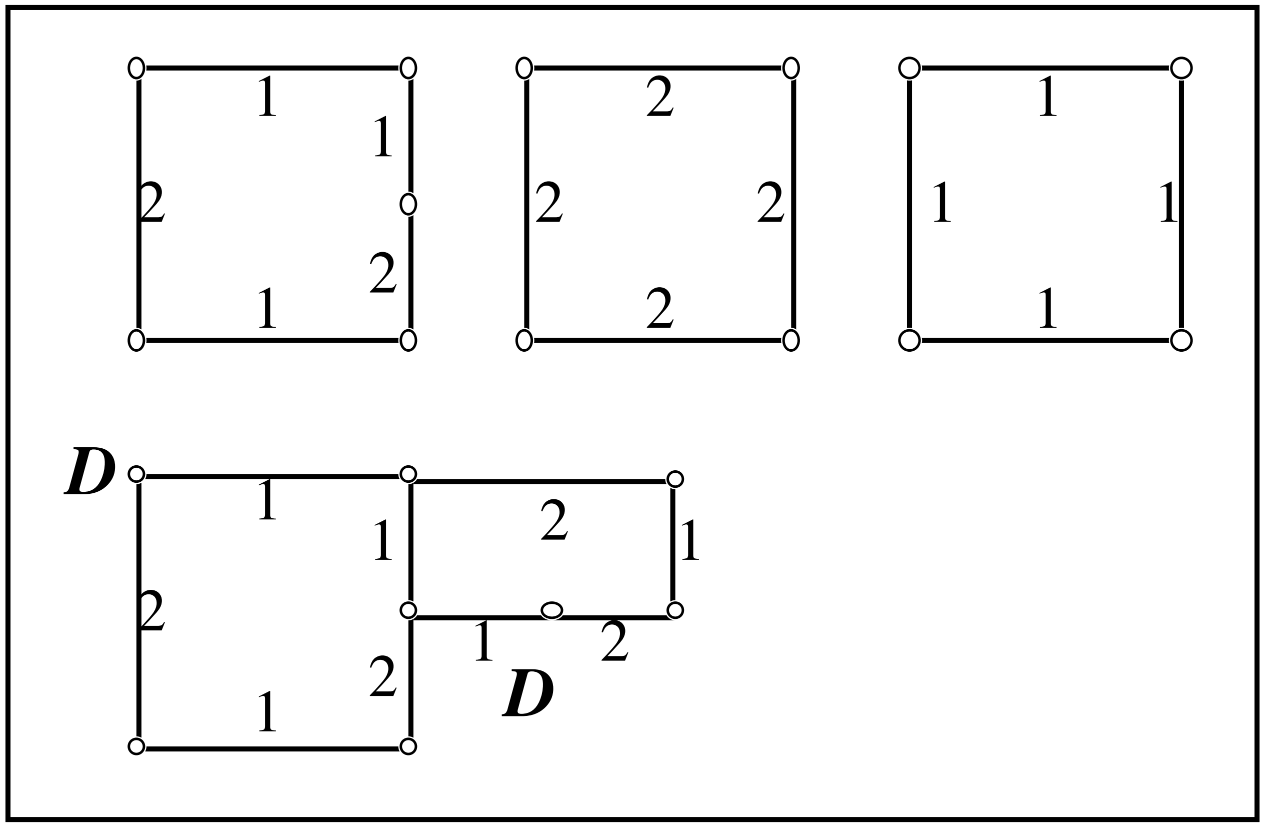
1.2.3. LEMMA. *(Huet [80]). Let A be strongly confluent. Then A is CR.*

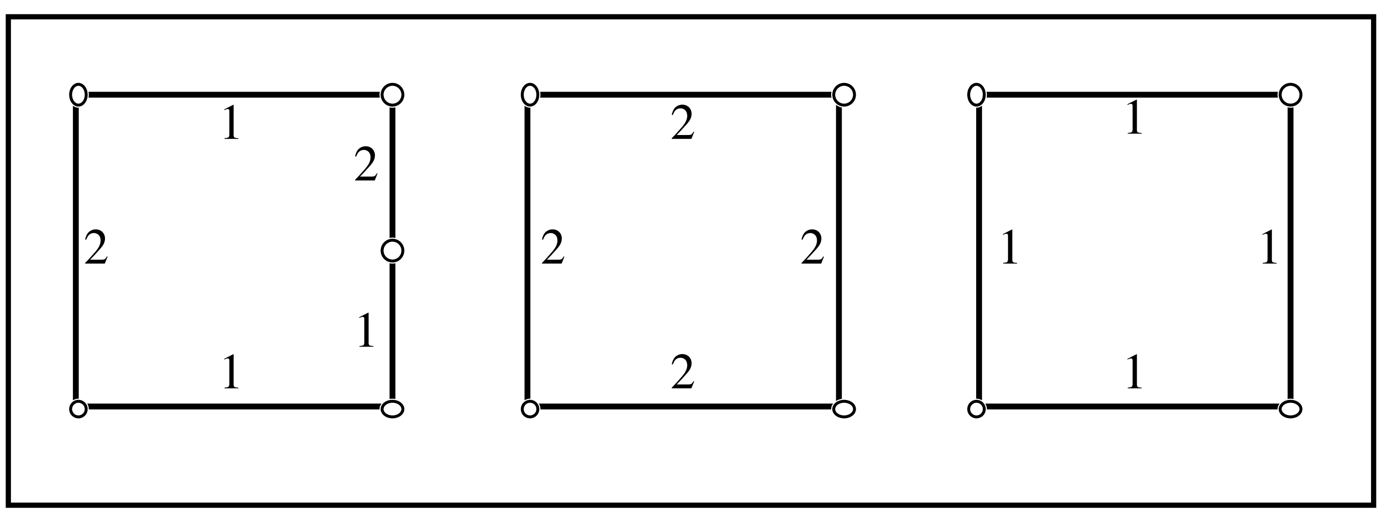


$$\forall a, b, c \in A \exists d, e, f \in A (c \leftarrow a \rightarrow b \Rightarrow c \rightarrow d \rightarrow e \leftarrow f \leftarrow b)$$

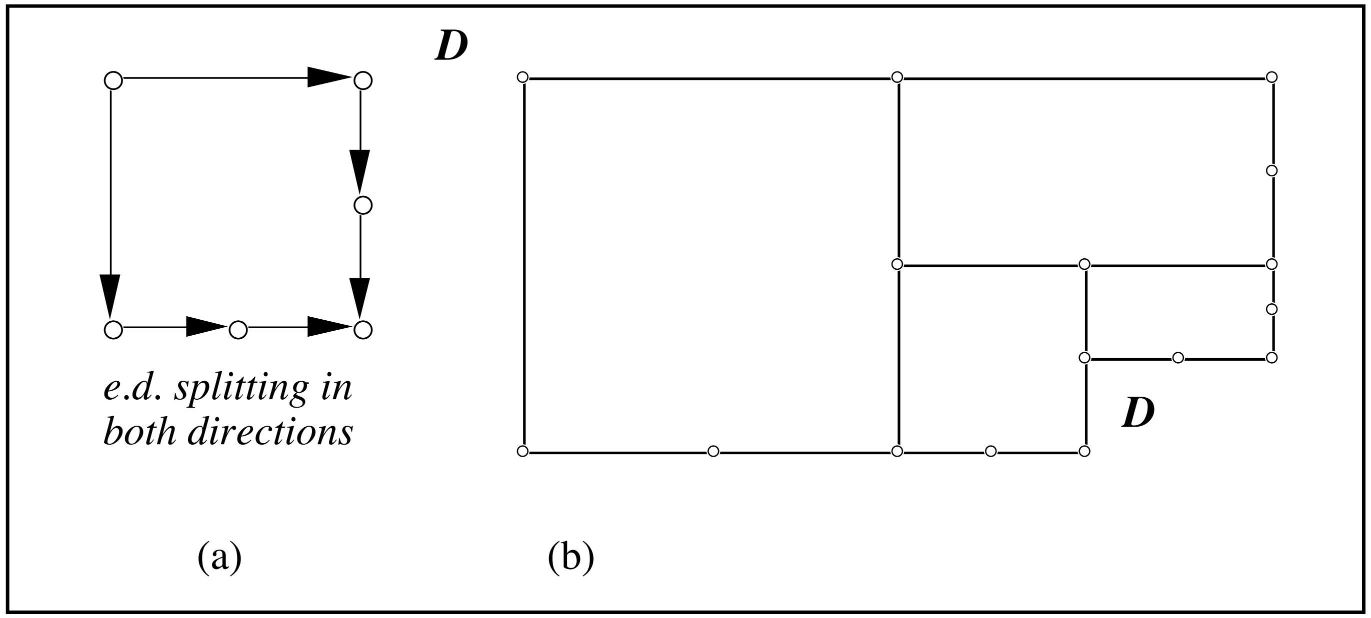
24

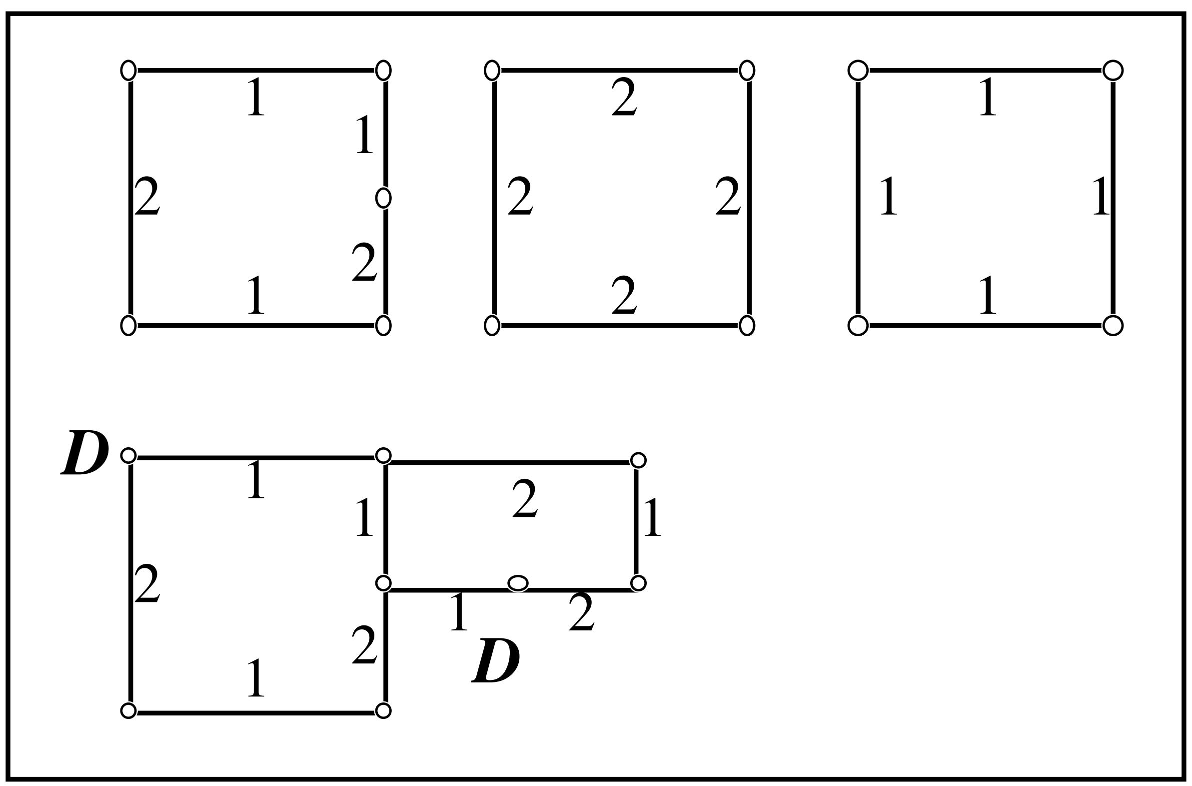
Question: does CR hold for $\to_{12}$?
Answer: No; for we may have a situation as in Figure 6.3.3, lower diagram.

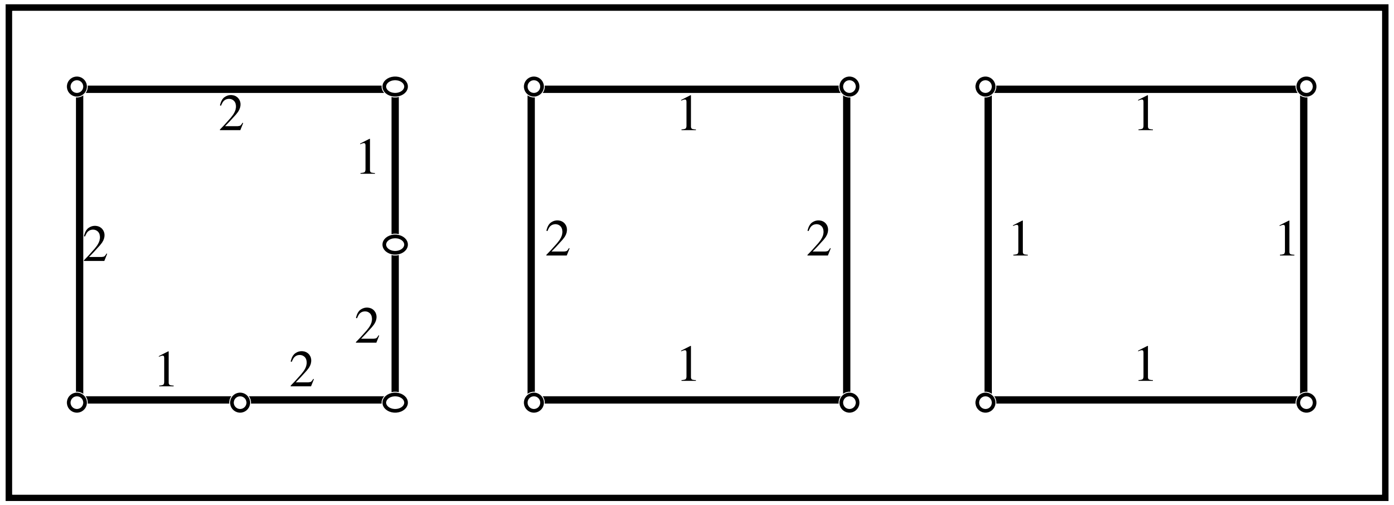




25


D
e.d. splitting in
both directions
D
(a)
(b)


1
1
2
2
1
2
2
2
2
1
1
1
1
D
1
1
2
2
1
1
2
1
2
D



Is tiling succesful?

Dick de Bruijn

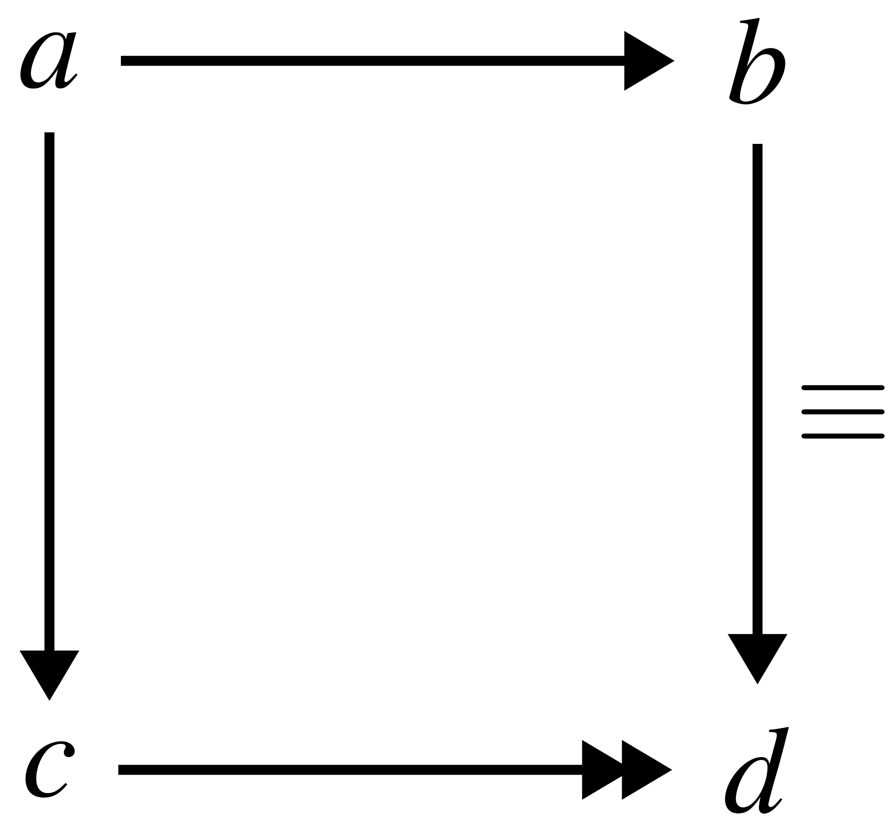
1918 - 2012

AUTOMATH ARCHIVE

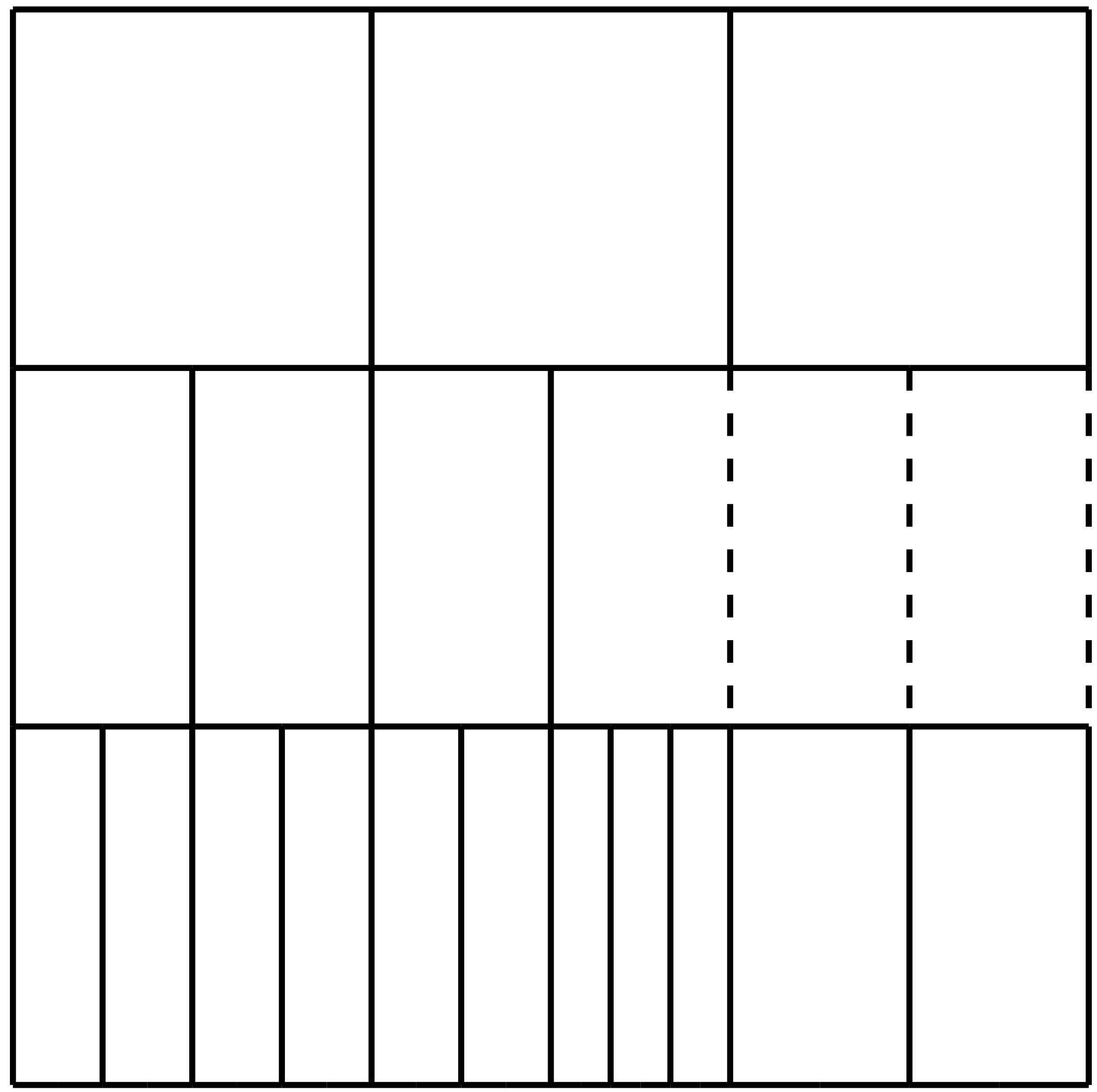
Institute in Nijmegen and the Formal Methods section of Eindhoven University of Technology. Started by prof. H. Barendregt, in cooperation with Rob Nederpelt, this archive project was launched to digitize valuable historical articles and other documentation concerning the Automath project.

Initiated by prof. N.G. de Bruijn, the project Automath (1967 until the early 80's) aimed at designing a language for expressing complete mathematical theories in such a way that a computer can verify the correctness. This project can be seen as the predecessor of type theoretical proof assistants such as the well known Nuprl and Coq.

28



29



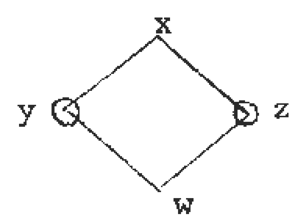
A note on weak diamond properties.

1. Introduction. Let S be a set with a binary relation >. We assume it to satisfy x > x for all $x \in S$. We are interested in establishing a property CR (named after its relevance for the Church-Rosser theorem of lambda calculus, cf. [1]). We say that $x \sim y$ if $x > y$ or $y > x$. We say that $x >^* y$ if there is a finite sequence $x_1, \ldots, x_n$ with $x = x_1 > x_2 > \ldots > x_n = y$, and also if x=y. We say that (S,>) satisfies CR if for any sequence $x_1, \ldots, x_n$ with

$$x_1 \sim x_2 \sim \ldots \sim x_n$$

there exist an element $x \in S$ with both $x_1 >^* z$ and $x_n >^* z$.

It is usual to say that (S,>) has the diamond property (DP) if for all x,y,z with $x > y$, $x > z$ there exists a w with $y > w$, $z > w$. This is depicted in the following diagram:



where $x > y$ is indicated by a line from x downwards to y, etc. The little circles around y and z illustrate the logical situation: the diagram $y \overset{x}{\wedge} z$ can be closed by $\underset{w}{y \vee z}$.

It is not hard to show that DP implies CR. A simple way to present a proof is by counting "inversions" in sequences like $x_1 > x_2 < x_3 < x_4 > x_5 < x_6 > x_7$: if $i < j$ and $x_i < x_{i+1}$, $x_j > x_{j+1}$, then we say that the pair (i,j) forms an inversion. Applications of DP, like replacing $x_3 < x_4 > x_5$ by $x_3 > x_4^* < x_5$, decrease the number of inversions. Once all inversions are gone, we have established CR.

The following property WDP_1 is weaker than DP. It says: "if $x > y$ and $x > z$ then w exists such that $y >^* w$ and $z >^* w$". It is very frustrating in attemps to prove the Church-Rosser theorem for various systems, that WDP_1 does not imply CR. A counterexample can be obtained by means of the following picture (cf. [2] p. 49):

31

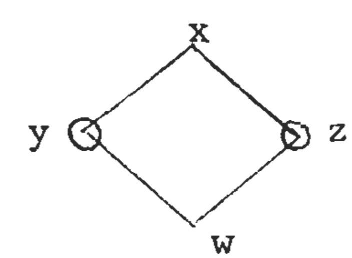
<u>A note on weak diamond properties.</u>

1. <u>Introduction</u>. Let S be a set with a binary relation $>$. We assume it to satisfy $x > x$ for all $x \in S$. We are interested in establishing a property CR (named after its relevance for the Church-Rosser theorem of lambda calculus, cf. [1]). We say that $x \sim y$ if $x > y$ or $y > x$. We say that $x >^* y$ if there is a finite sequence $x_1, \ldots, x_n$ with $x = x_1 > x_2 > \ldots > x_n = y$, and also if $x = y$. We say that $(S,>)$ satisfies CR if for any sequence $x_1, \ldots, x_n$ with

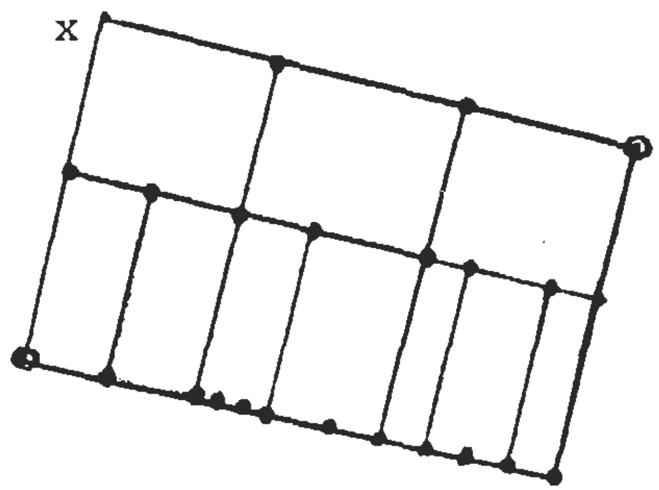
$$x_1 \sim x_2 \sim \ldots \sim x_n$$

there exist an element $x \in S$ with both $x_1 >^* z$ and $x_n >^* z$.

It is usual to say that $(S,>)$ has the <u>diamond</u> <u>property</u> (DP) if for all x,y,z with $x > y$, $x > z$ there exists a w with $y > w$, $z > w$. This is depicted in the following diagram:

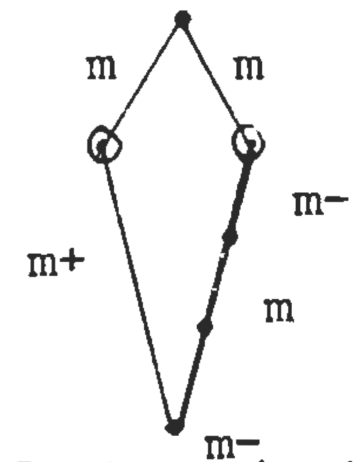


This example also shows that CR neither follows from WDP_2 where WDP_2 is slightly stronger than WDP_1 and says:"if $x > y$ and $x > z$ then w exists such that $y >^* w$ and $z >^* w$ and at least one of $y > w$ and $z > w$". Stronger again is WDP_3, expressing:"if $x > y$ and $x > z$ then w exists such that $y >^* w$ and $z > w$." This WDP_3 does imply CR. Actually WDP_3 implies WDP_4, which says: "if $x >^* y$ and $x >^* z$ then w exists such that both $y >^* w$ and $z >^* w$." This WDP_4 is the DP for $(S, >^*)$, and therefore implies CR for $(S, >^*)$, and that is the same thing as CR for $(S, >)$. The derivation of WDP_4 from WDP_3 is illustrated by the following picture (cf. [2] p. 59) which speaks for itself:



In this note we go considerably further. Instead of having just one relation $>$ we consider a set of relations $>_m$ where m is taken from an index set M. The idea behind this is that in the Church-Rosser theorem the relations represent lambda calculus reductions; there may be reductions of various types, and diamond properties may depend on these types. It is our purpose to establish weak diamond properties which guarantee CR (where CR has to be interpreted as in section 4.

5. <u>The basic diamond properties</u>. If $m \in M$, the diamond property $D_1(m)$ is defined by the following diagram.

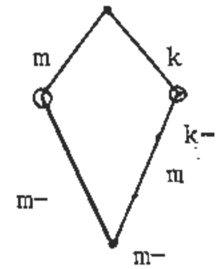
$D_1(m)$: 

This has to be read as follows (and further diagrams have to be interpreted analogously: If x,y,z are such that $x >_m y$, $x >_m z$, then u,v,w exist such that

$$y >_{m+} w, \quad z >_{m-} u >_m v >_{m-} w.$$

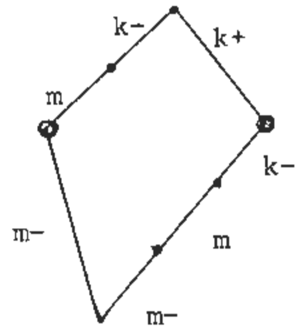
(so on the left we have a chain from y to w with all links $\leq m$; on the right we have a chain from z to w with all links $\leq m$ but with at most one $= m$).

$D_2(m,k)$:

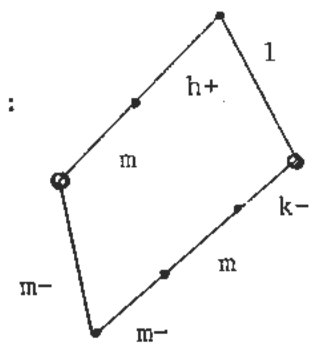


6. Some auxiliary diamond properties. We intend to show that $D_1(m)$ and $D_2(m,k)$ (for all m,k with $k < m$) lead to CR. In order to achieve this we formulate a number of diamond properties that will play a rôle in the proof.

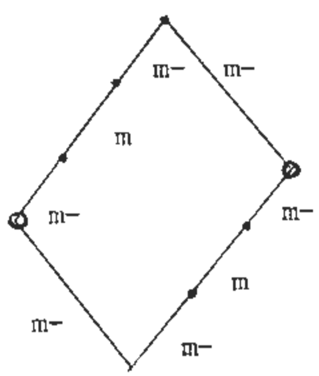
$D_3(m,k)$:



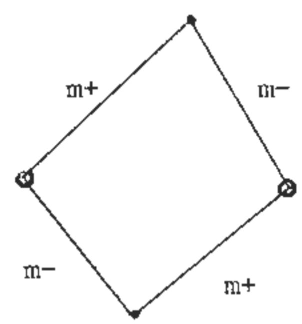
$D_4(m,k,l,h)$:



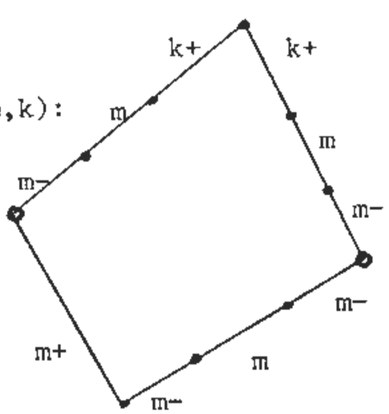
$D_5(m)$:



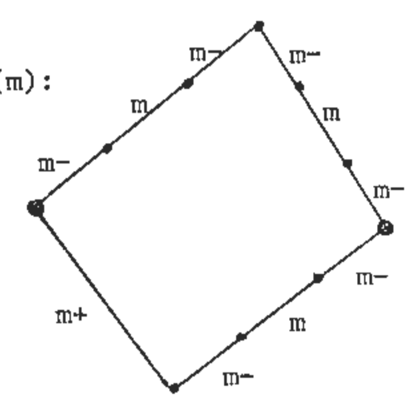
$D_6(m)$:



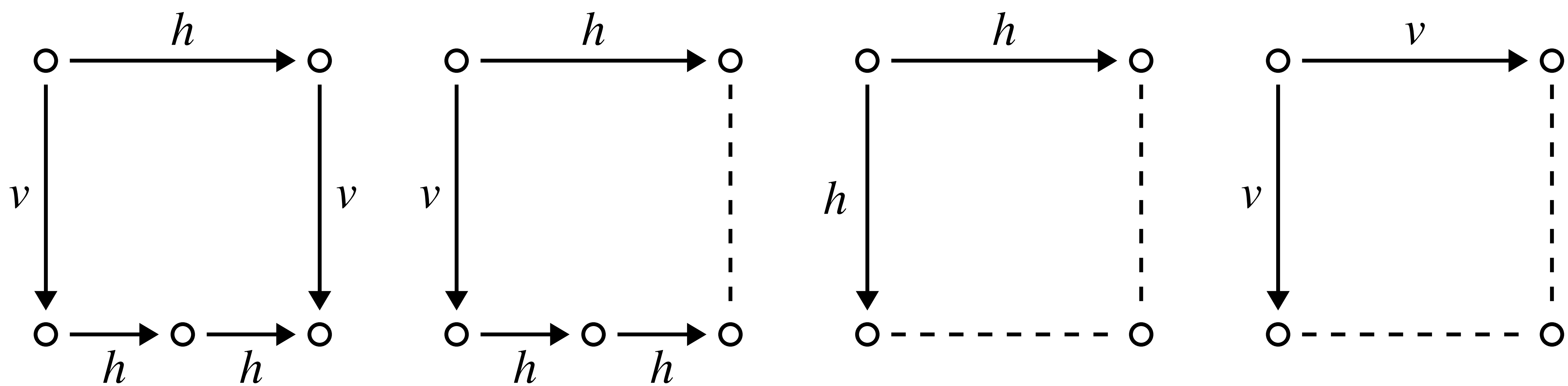
$D_7(m,k)$:



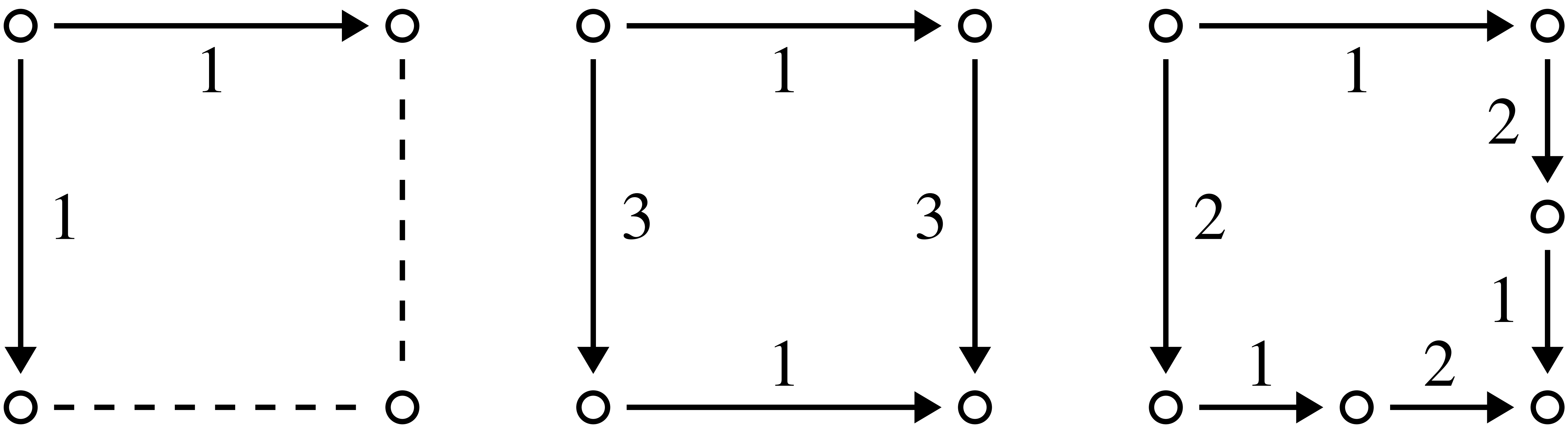
$D_8(m)$:



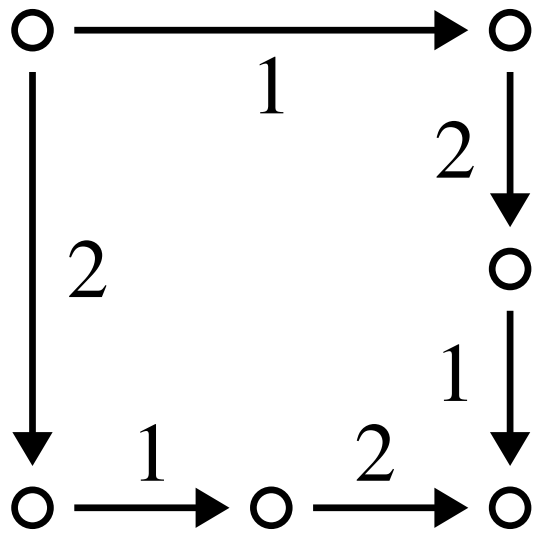
The diagrams D_3 and D_7 will play their rôle only if $k < m$, and D_4 only if $h < k < m$, $l \leq m$.

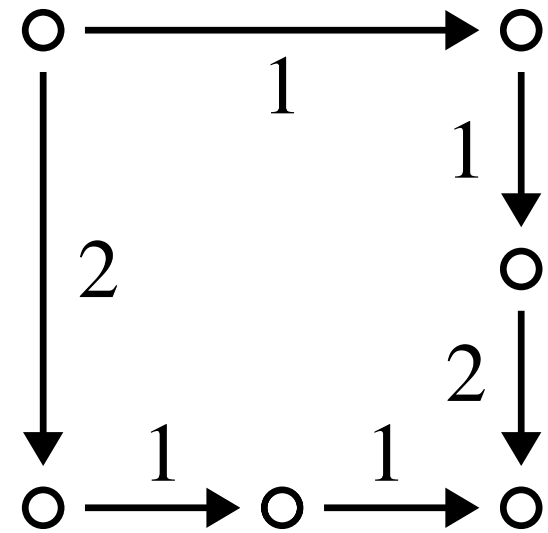


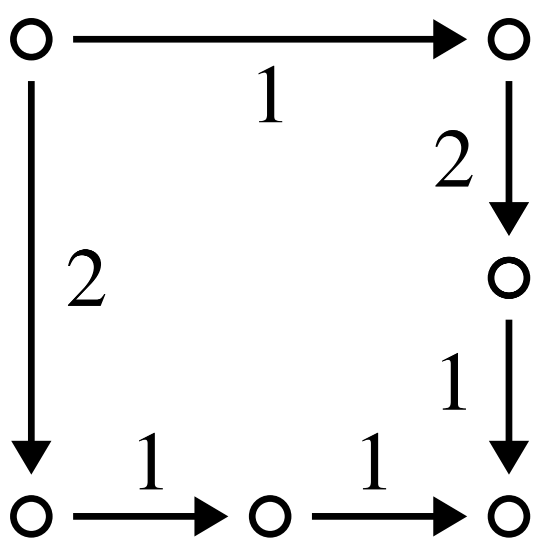
36

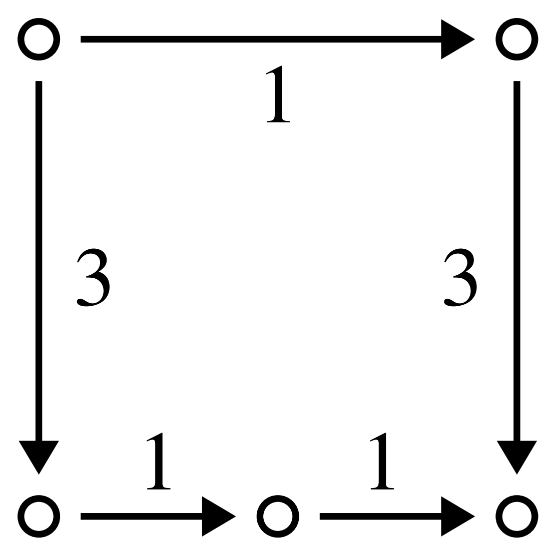


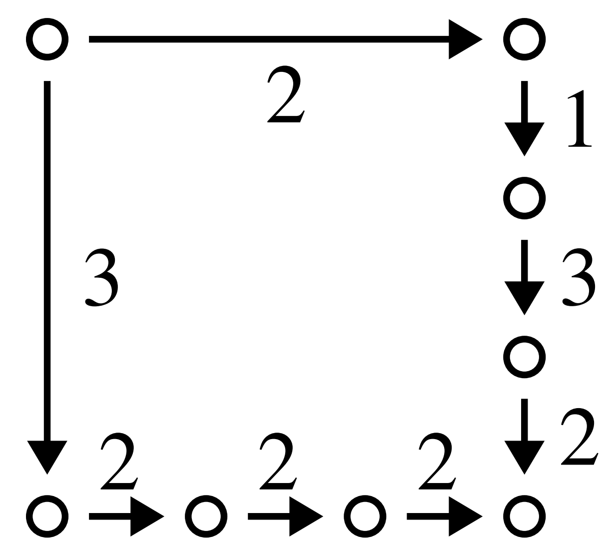
37



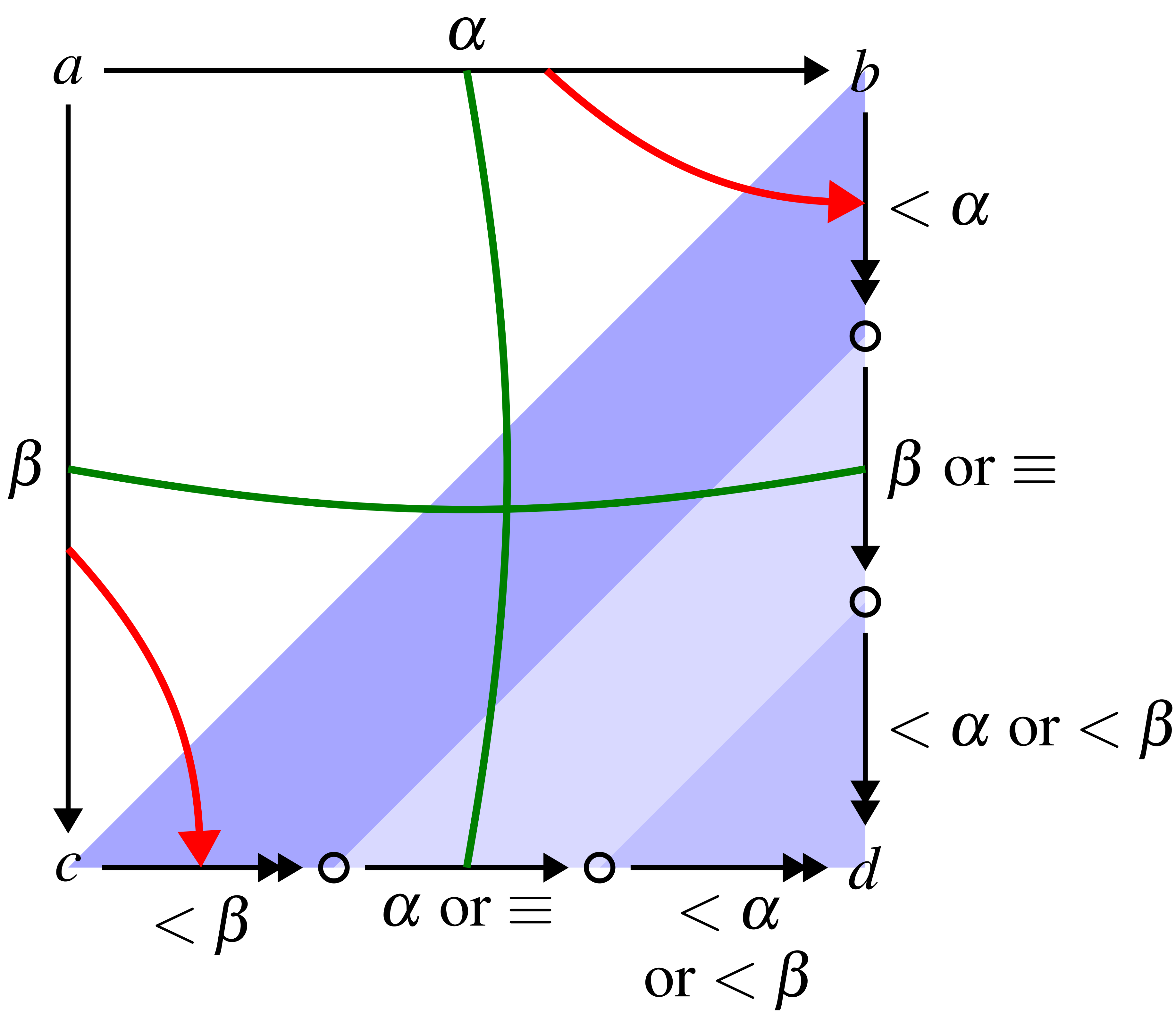


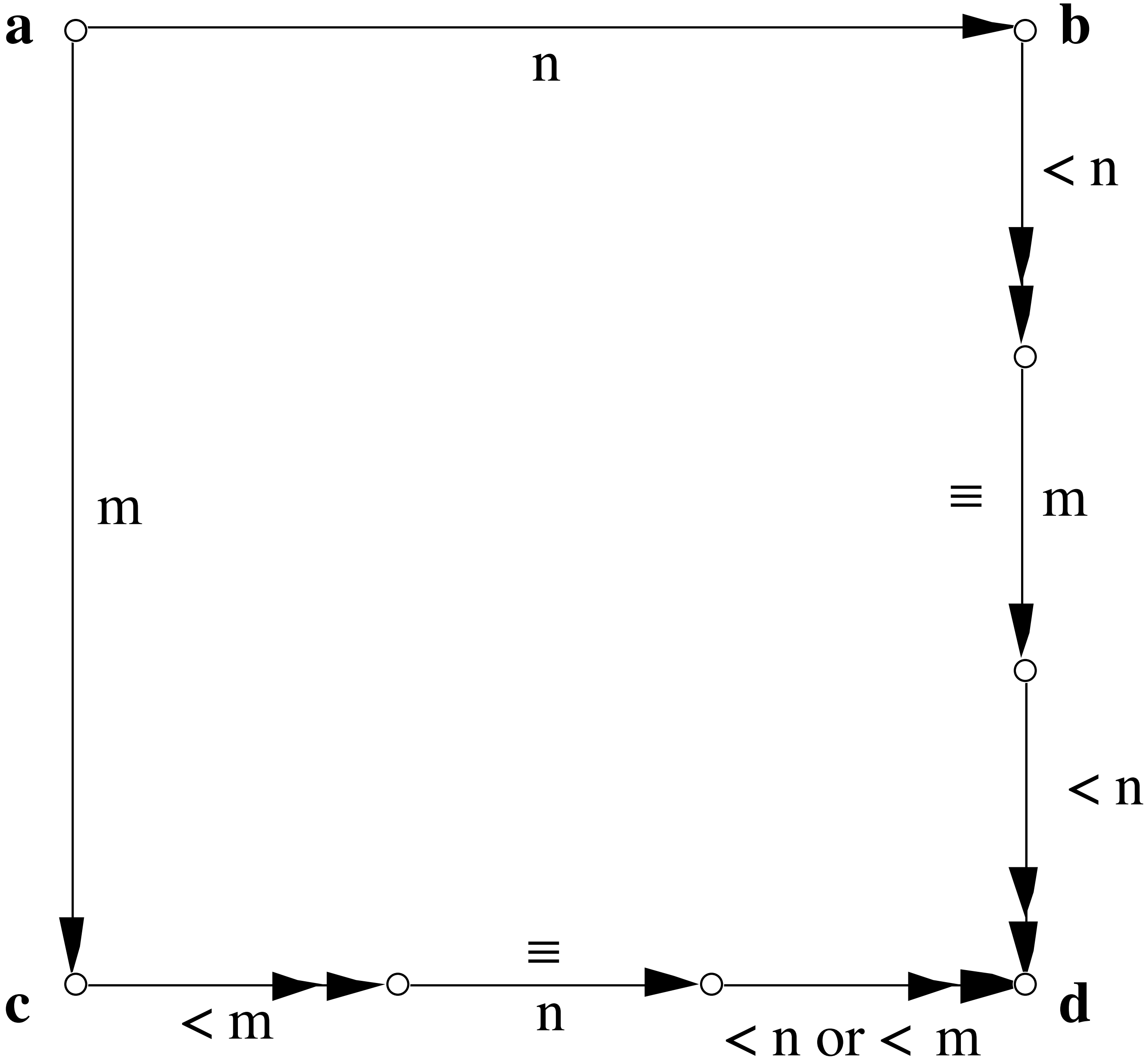


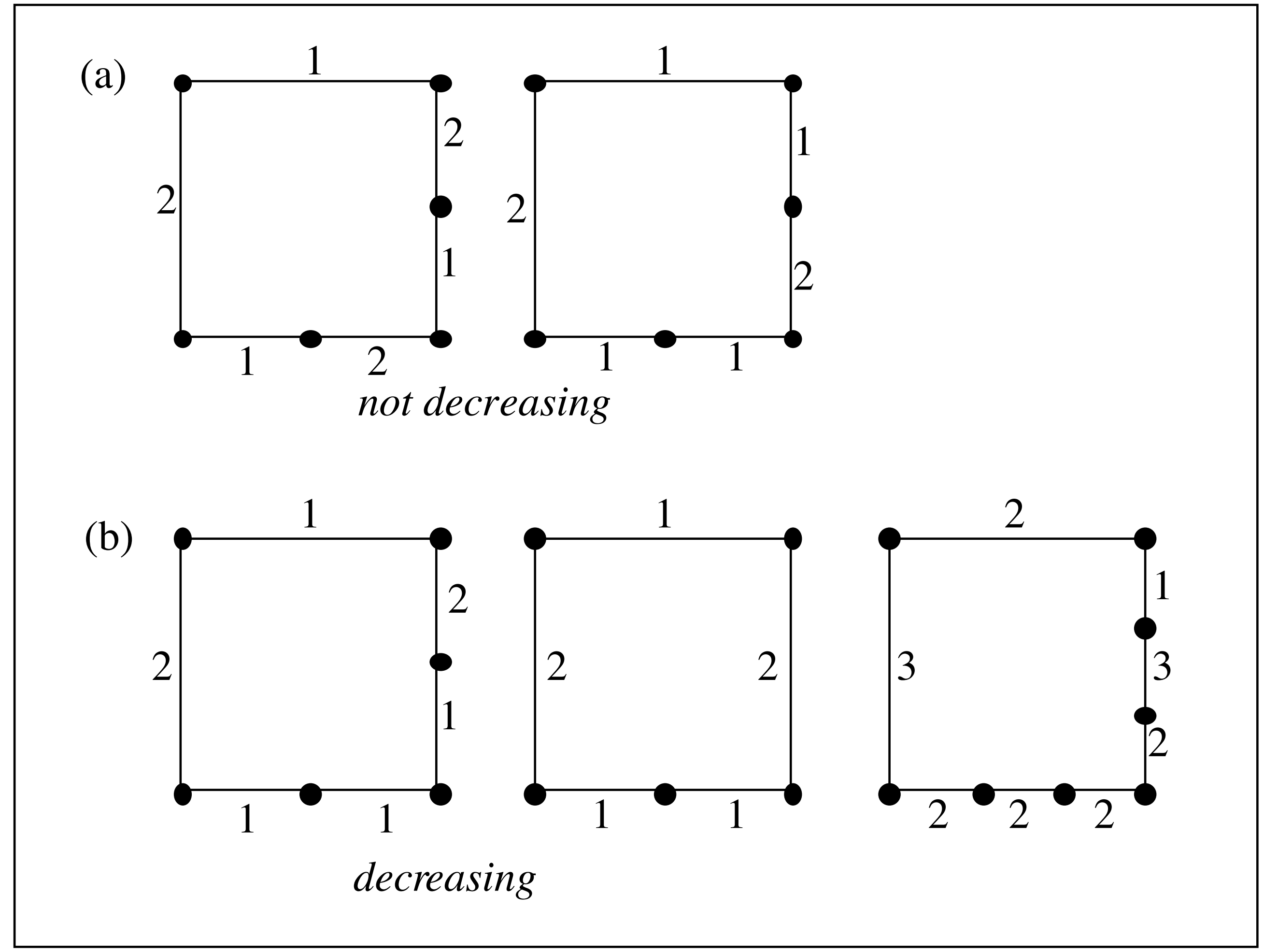




38


α
a
b
$< \alpha$
β
β or $\equiv$
$< \alpha$ or $< \beta$
c
d
$< \beta$
α or $\equiv$
$< \alpha$
or $< \beta$





Explanation: Given two diverging steps $a \to_n b$ and $a \to_m c$ with indices n, m there is a common reduct d such that

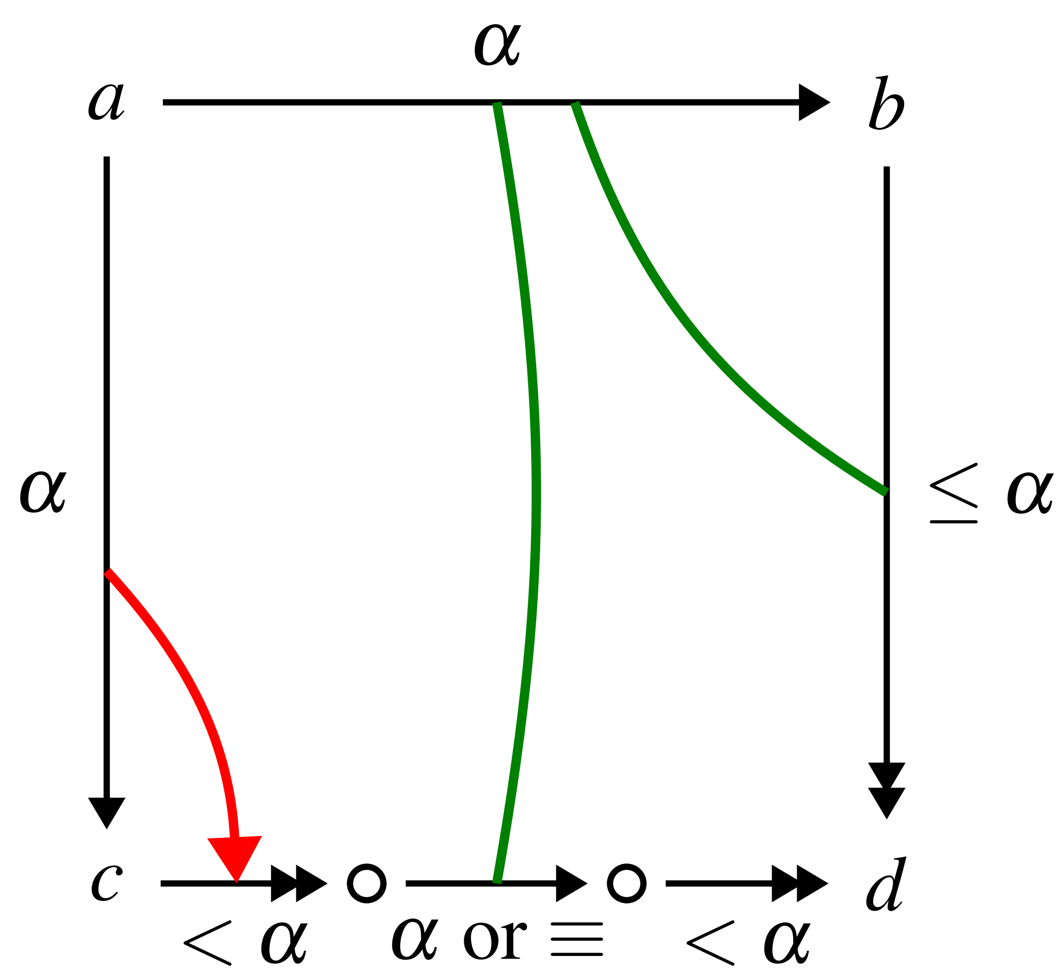
$$b \twoheadrightarrow_{<n} \cdot \to_m^{\equiv} \cdot \twoheadrightarrow_{<n \vee <m} d$$

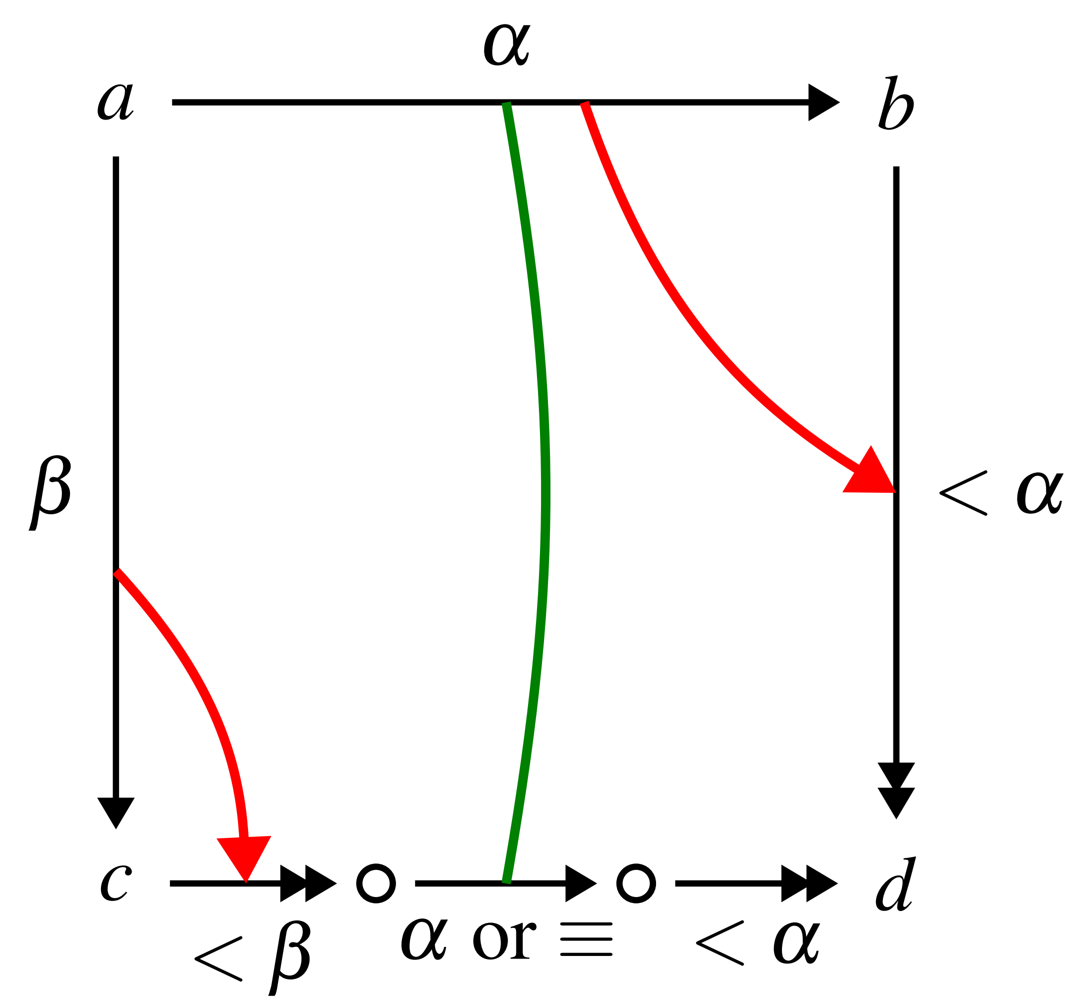
and dually

$$b \twoheadrightarrow_{<m} \cdot \to_n^{\equiv} \cdot \twoheadrightarrow_{<n \vee <m} d.$$

So from b we take some steps with indices $< n$, followed by 0 or 1 step with index m, followed by some steps with index $< n$ or $< m$, with result d. Dually, from c we have a reduction to d as indicated.

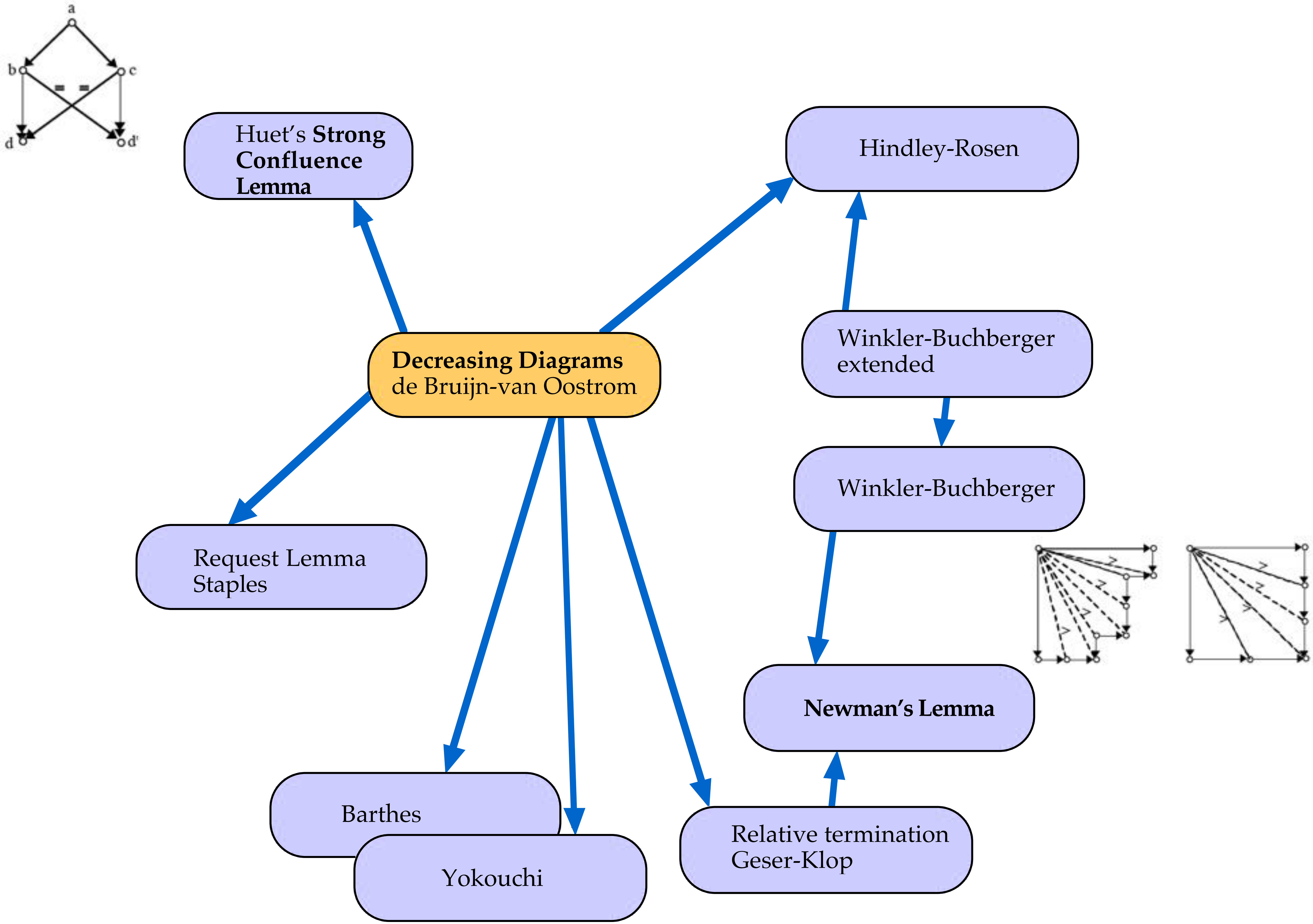
40



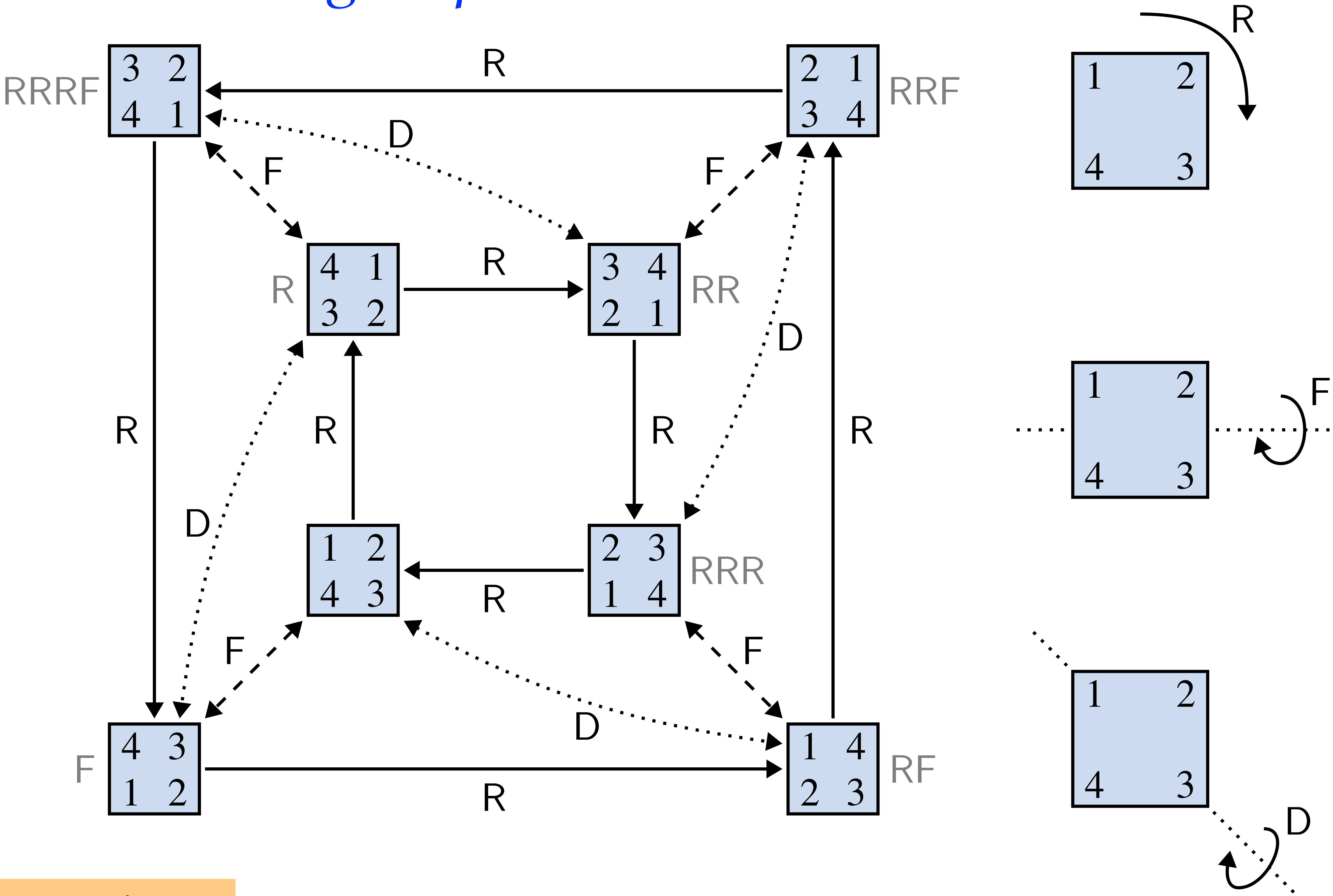


for $\beta < \alpha$

1.2.14. THEOREM. *(De Bruijn - Van Oostrom) Every ARS with reduction relations indexed by a well-founded partial order I, and satisfying the decreasing criterion for its e.d.'s, is confluent.*


a
b
c
d
d'
Huet's **Strong Confluence Lemma**
Hindley-Rosen
Decreasing Diagrams
de Bruijn-van Oostrom
Winkler-Buchberger extended
Winkler-Buchberger
Request Lemma
Staples
Newman's Lemma
Barthes
Yokouchi
Relative termination
Geser-Klop

dihedral group D_4



$$FF \to \lambda$$
$$RRRR \to \lambda$$
$$FR \to RRRF$$

is a complete TRS for this equality, thus solving its word problem

Other presentations of D_4

$$A \simeq B \;\Leftrightarrow\; A \Longleftrightarrow_{Tietze} B$$

Theorem 3.3 (Decreasing Diagrams – De Bruijn). *Let* $\mathscr{A} = (A, (\to_\alpha)_{\alpha \in I})$ *be an ARS with reduction relations indexed by a well-founded* total *order* $(I, >)$. *If for every peak* $c \leftarrow_\beta a \to_\alpha b$ *there exists an elementary diagram joining this peak of one of the forms in Figure 3.13, then* $\to$ *is confluent.*

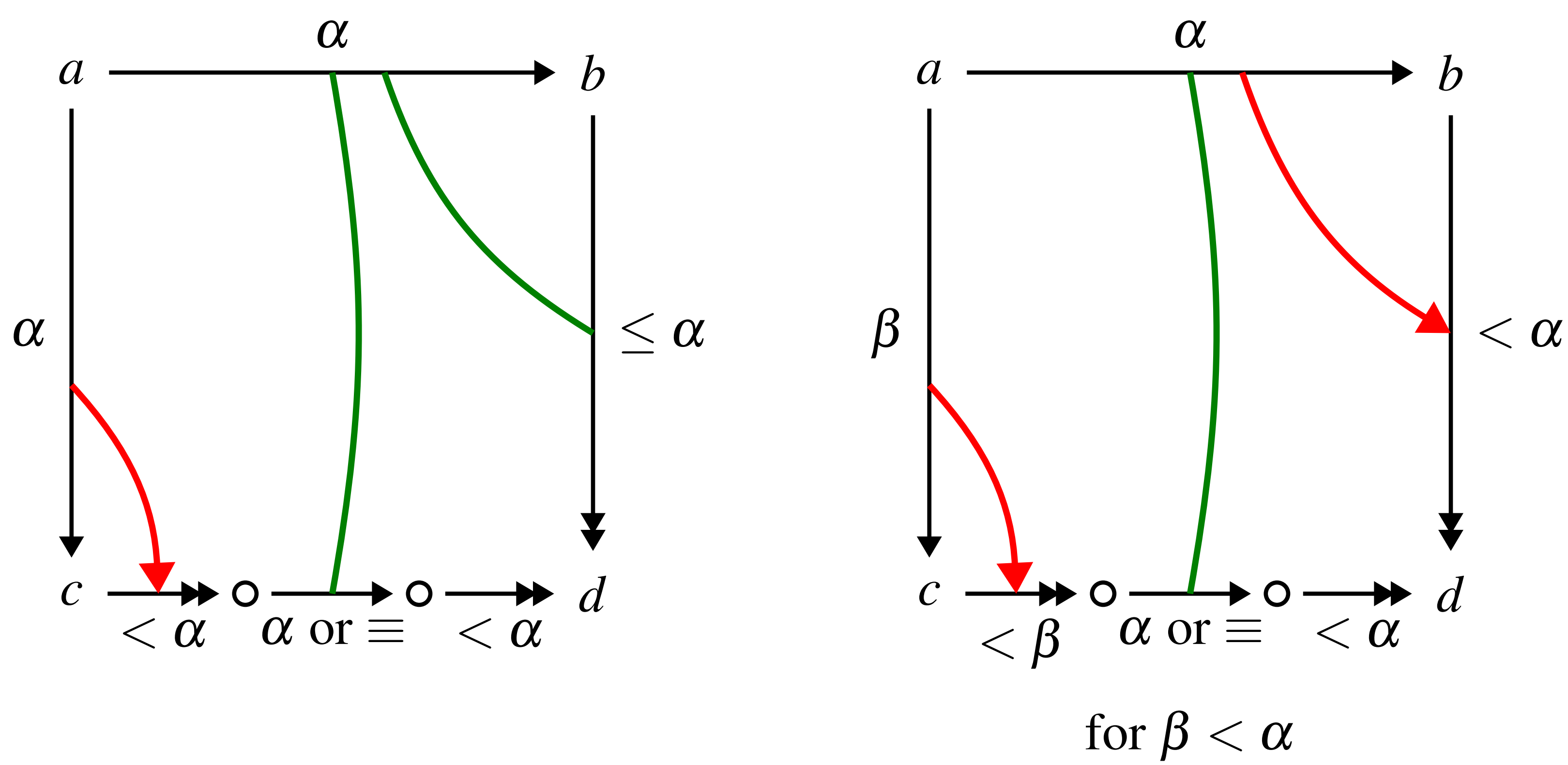


Fig. 3.13: *De Bruijn's asymmetrical decreasing elementary diagrams.*

Van Oostrom [vO94b, vO94a] presents a novel proof, and derives the following symmetrical version of decreasing elementary diagrams that allows for partial orders $>$, see Figure 3.14.

Theorem 3.4 (Decreasing Diagrams – Van Oostrom). *Let $\mathscr{A} = (A, (\rightarrow_\alpha)_{\alpha \in I})$ be an ARS with reduction relations indexed by a well-founded* partial *order $(I, >)$. An elementary diagram is called* decreasing *if it is of the form displayed in Figure 3.14. If for every peak $c \leftarrow_\beta a \rightarrow_\alpha b$ there exists a decreasing elementary diagram joining this peak, then $\rightarrow$ is confluent.*

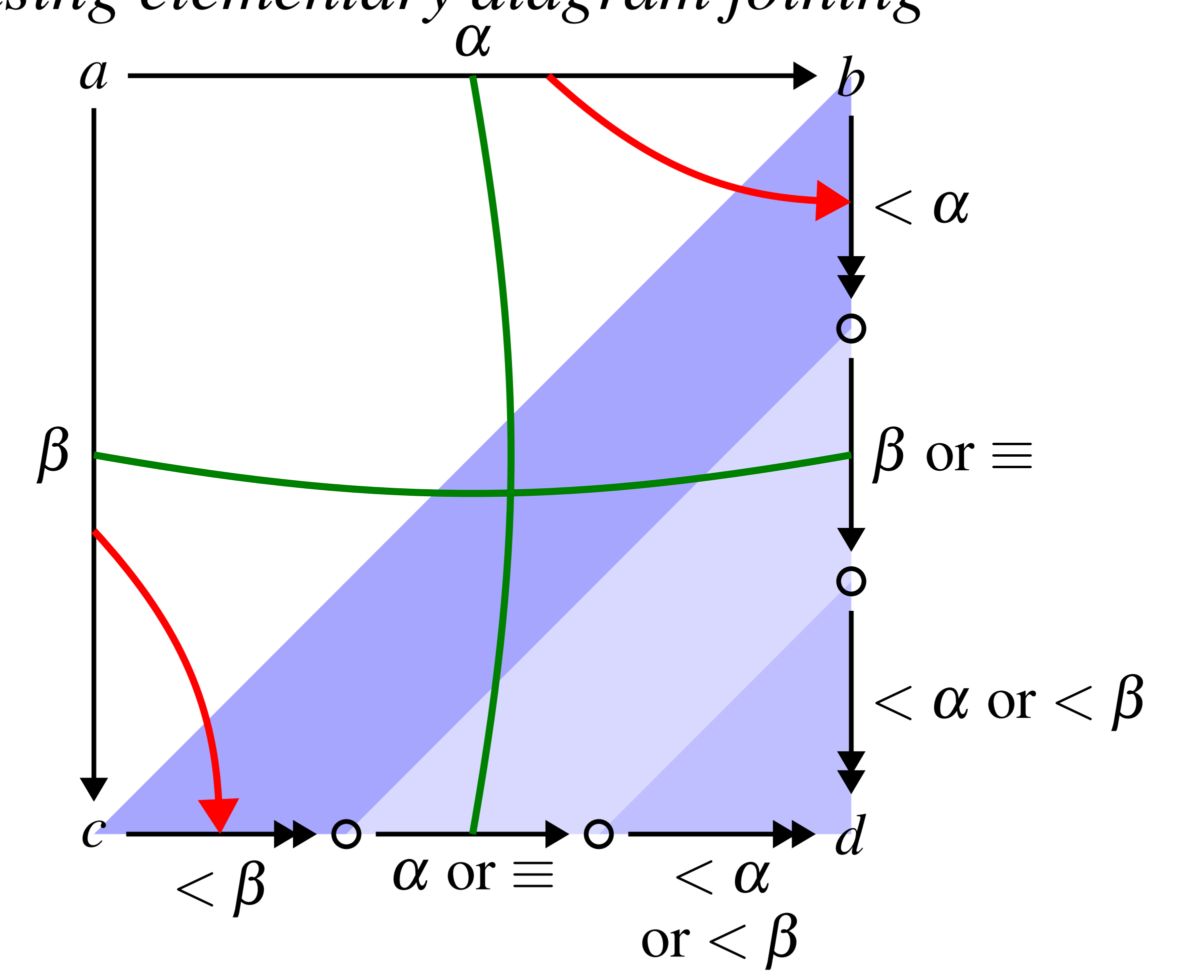


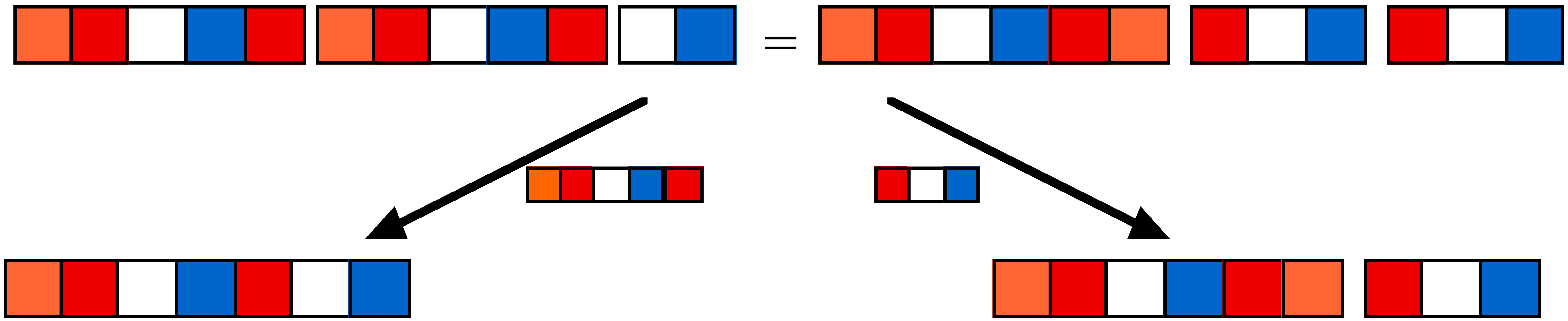
Fig. 3.14: *Decreasing elementary diagram.*

Definition 3.3. An ARS $\mathscr{A} = (A, \to)$ is said to be *decreasing Church-Rosser* (DCR), if there is an indexed ARS $\mathscr{B} = \langle A, (\to_\alpha)_{\alpha \in I} \rangle$ and a well-founded order $>$ on I such that $\mathscr{B}$ has decreasing elementary diagrams with respect to $>$, and $\to = \bigcup_{\alpha \in I} \to_\alpha$.

Theorem 3.5 (van Oostrom [vO94b]). *For countable ARSs: DCR $\Leftrightarrow$ CR.*

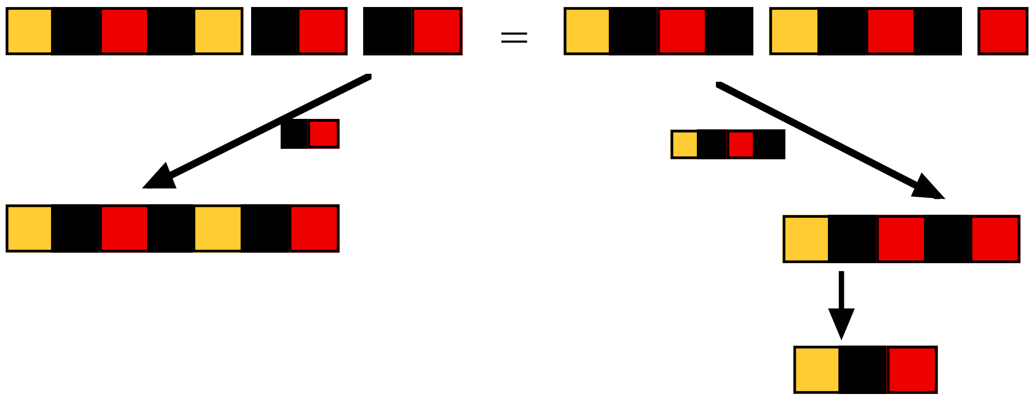
The proof, also present in Bezem, Klop & van Oostrom [BKvO98], employs the fact mentioned in chapter 1: CR $\Leftrightarrow$ CP for countable ARSs. It seems to be a difficult exercise to establish the (conjectured) result that the condition 'countable' is necessary.

free idempotent monoid: xx → x



$$dabcabc \leftarrow (dabca)(dabca)bc = dabcad(abc)(abc) \rightarrow dabcadabc$$

by Vincent van Oostrom



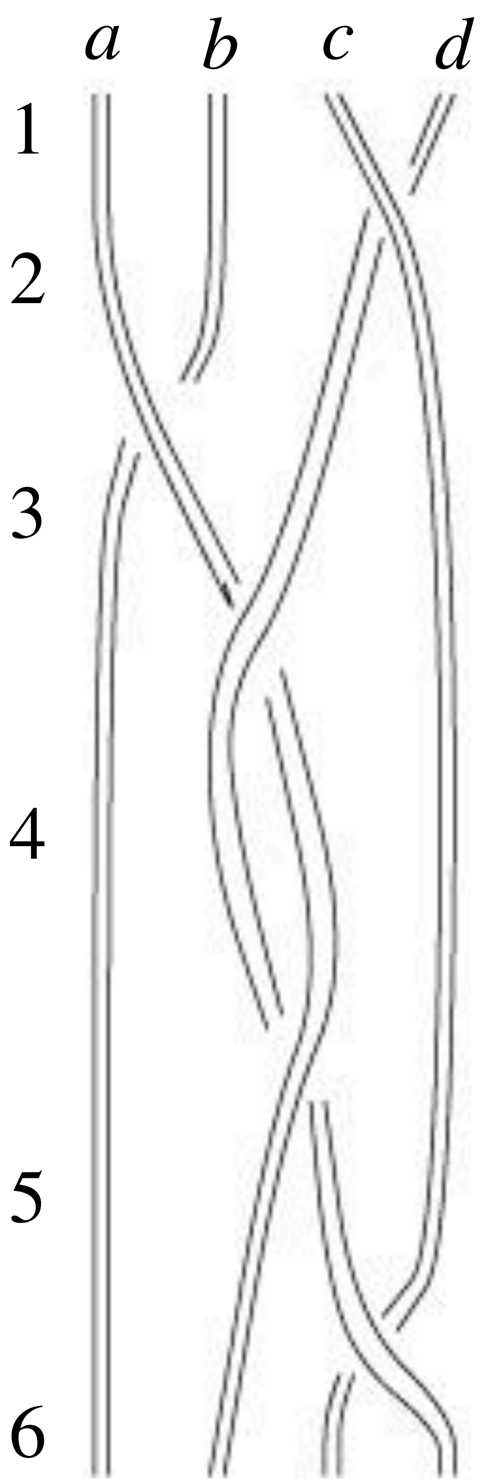
Zantema-Geser: does the rule 0011 → 111000 terminate?

the one-rule SRS $0^p 1^q \to 1^r 0^s$ terminates if and only if

(a) $p \geq s$ or $q \geq r$ or
(b) $p < s < 2p$ and $q < r$ and q is not a divisor of r or
$q < r < 2q$ and $p < s$ and p is not a divisor of s.

(so, does it terminate?)

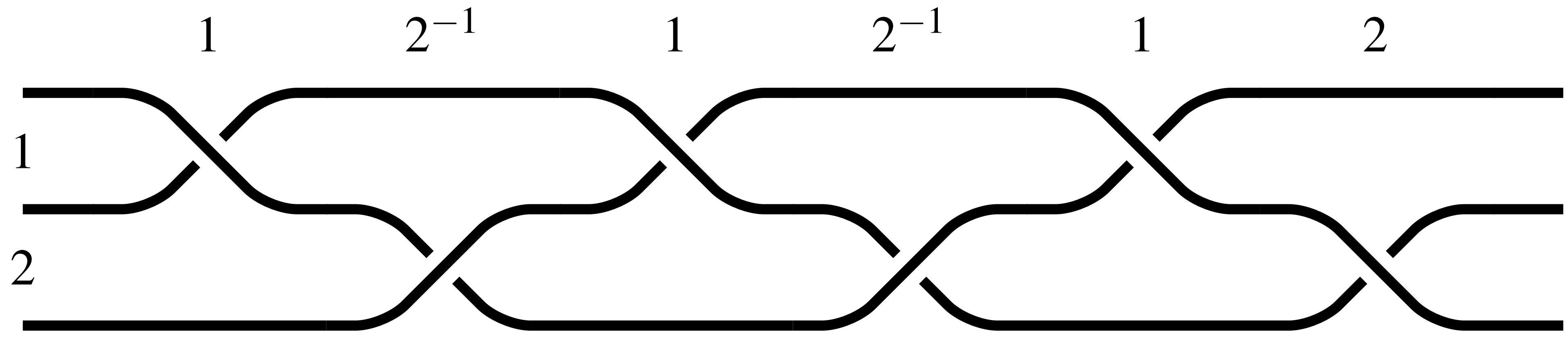
from the Notebook of Gauss

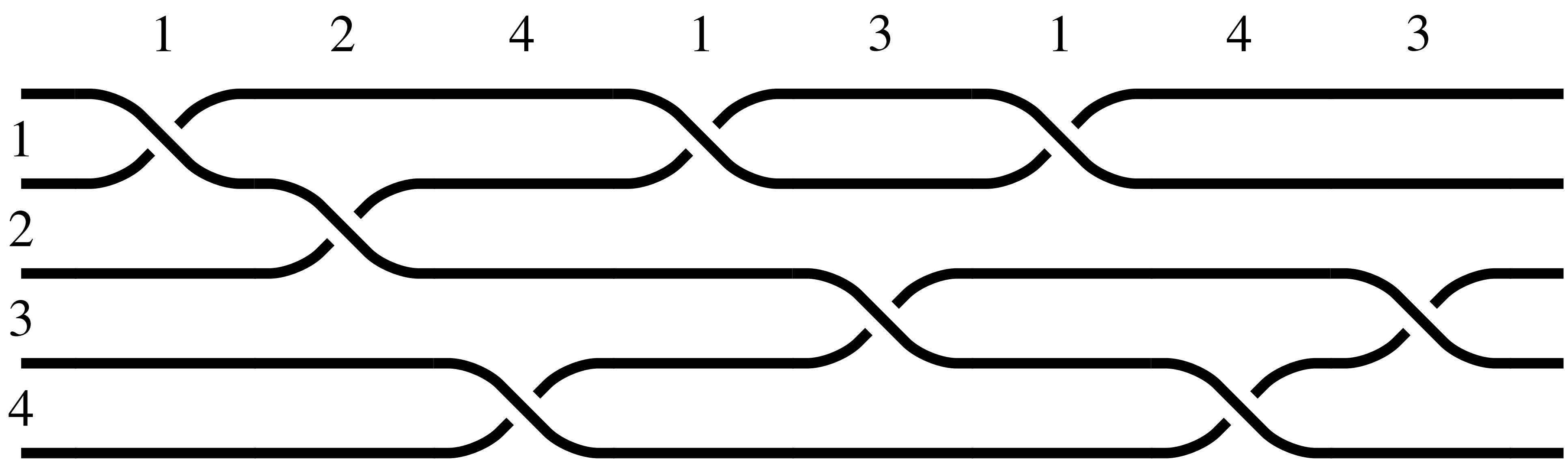


Veraindrung der Coordiniz

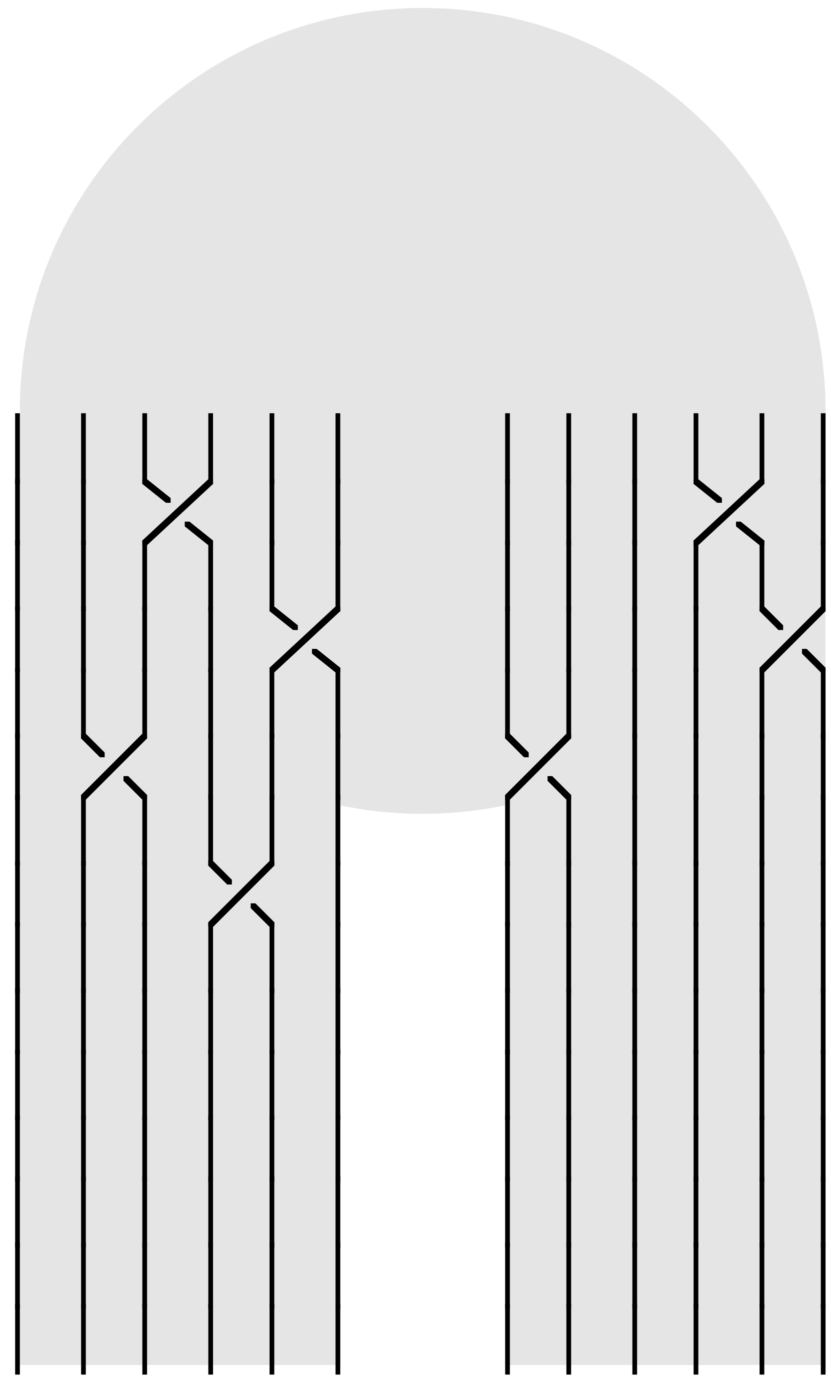
a	1	1	$2+i$	$3+i$	$2+2i$	$2+2i$
b	2	2	1	1	1	1
c	3	4	4	4	4	3
d	4	$3+i$	$3+i$	$2+2i$	$3+2i$	$4+3i$

notation of Braids





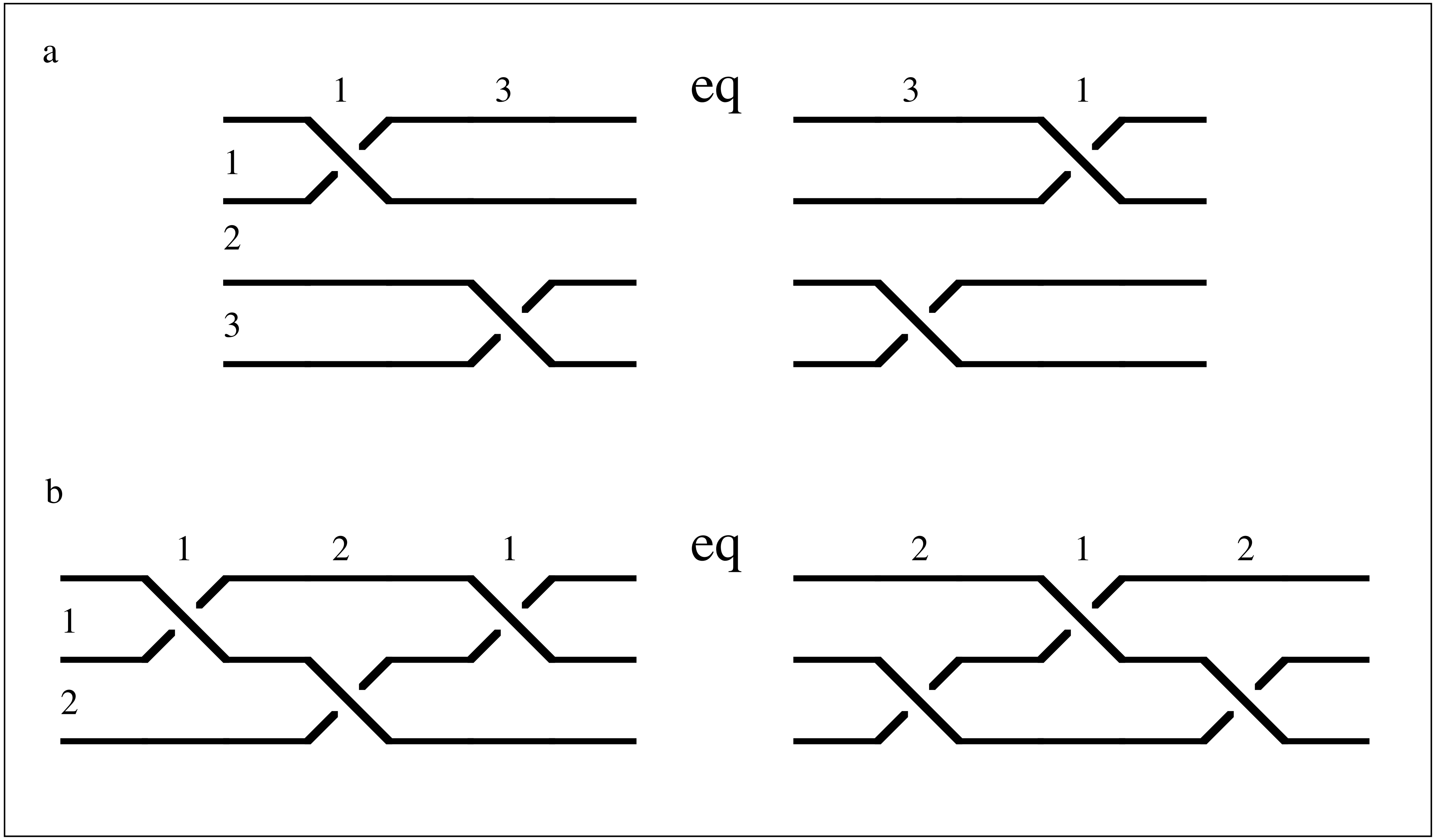
braiding problem



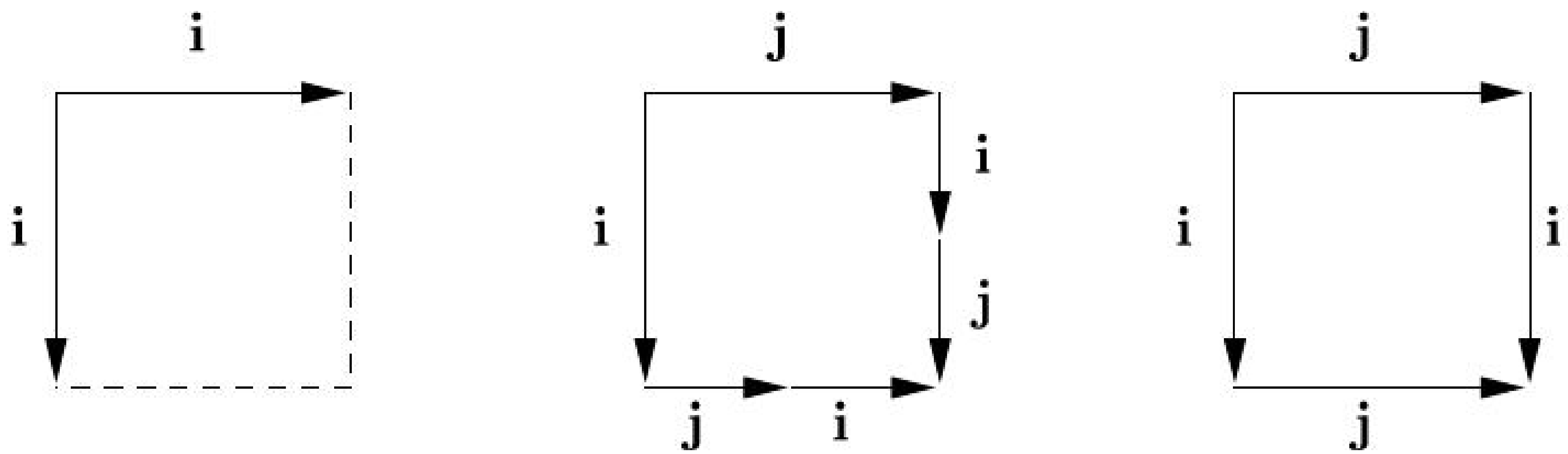
Girl with two braids

53

Artin's braid equations



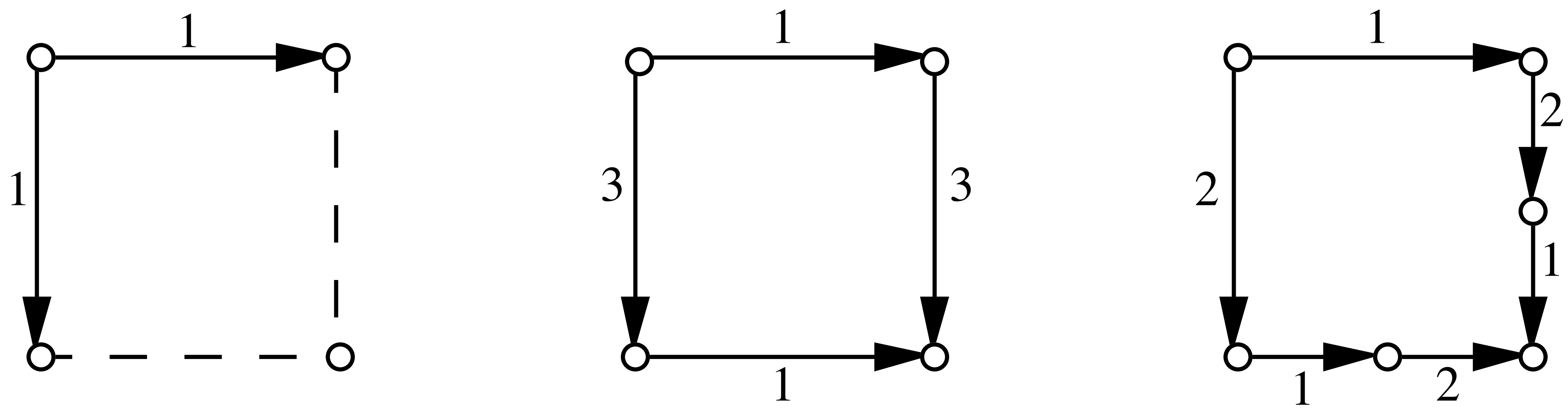
braid equations as e.d.'s



$|i - j| = 1$ $\quad$ $|i - j| \geq 2$

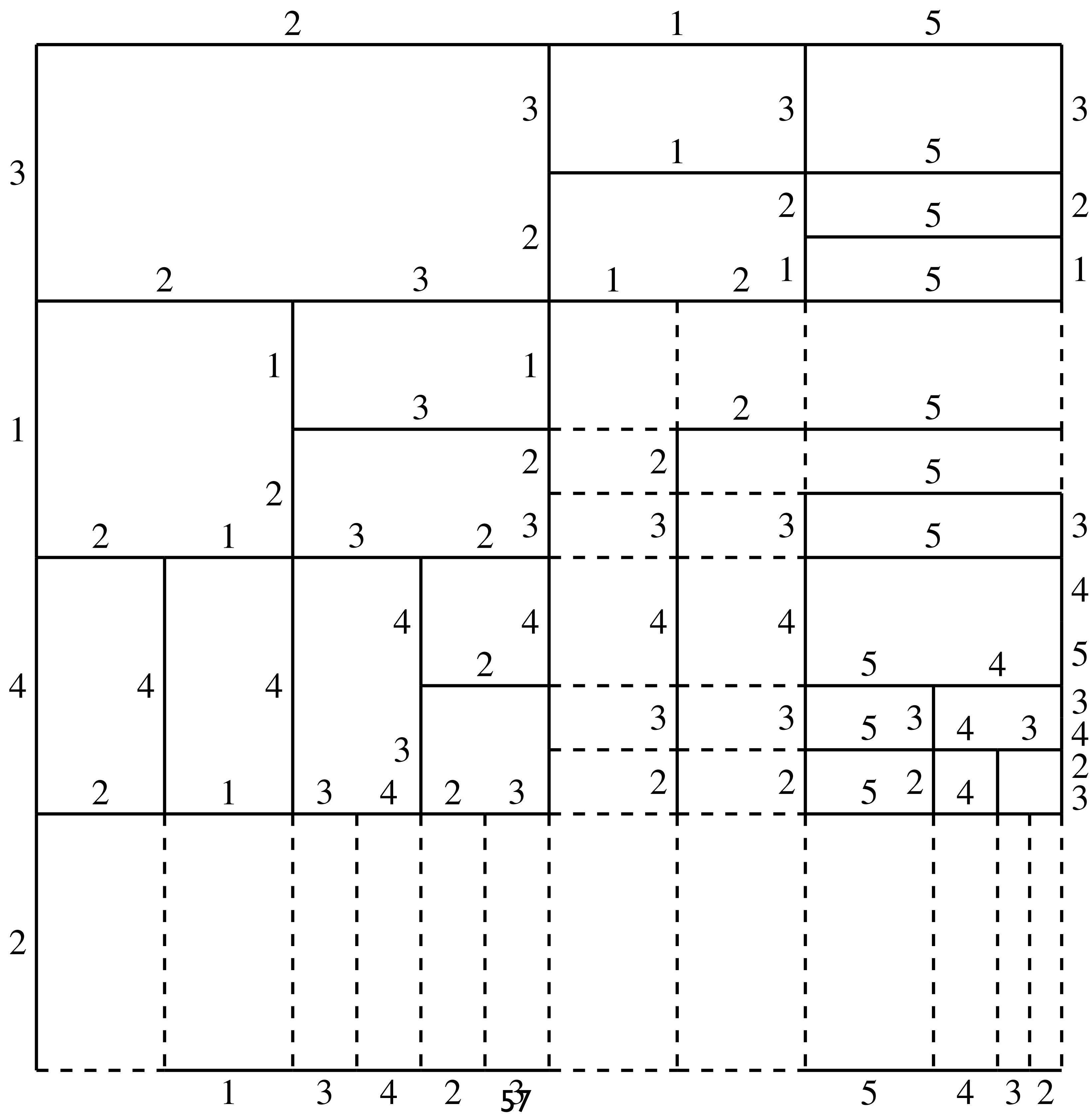
Figure 4: Elementary diagrams ($1 \leq i, j < n$)

55



elementary diagrams for confluence problem in braid semi-group

completed braid reduction diagram



57

$aba = bab$ and the need for signature extension

Kapur-Narendran 1985:
the monoid aba=bab has decidable equality (word problem), but there is no complete SRS generating this equality, like for D_4.

However, with extra symbols (signature extension) there is.
$ab = c$, $ca = bc$.
After completion:
$ab=c$, $ca=bc$, $bcb=cc$, $ccb=acc$.

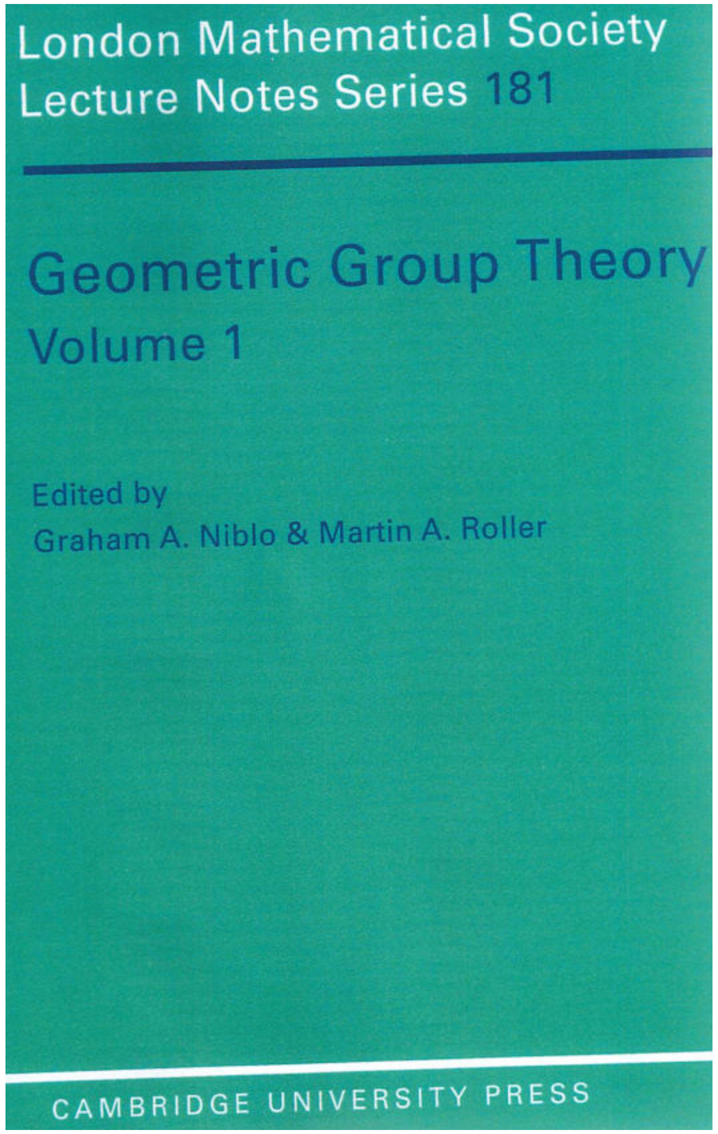
Another solution by Burckel-Riviere 2001:

1 → *1,*

212 → 12*1*

2122 → 1212

1211 → 2121



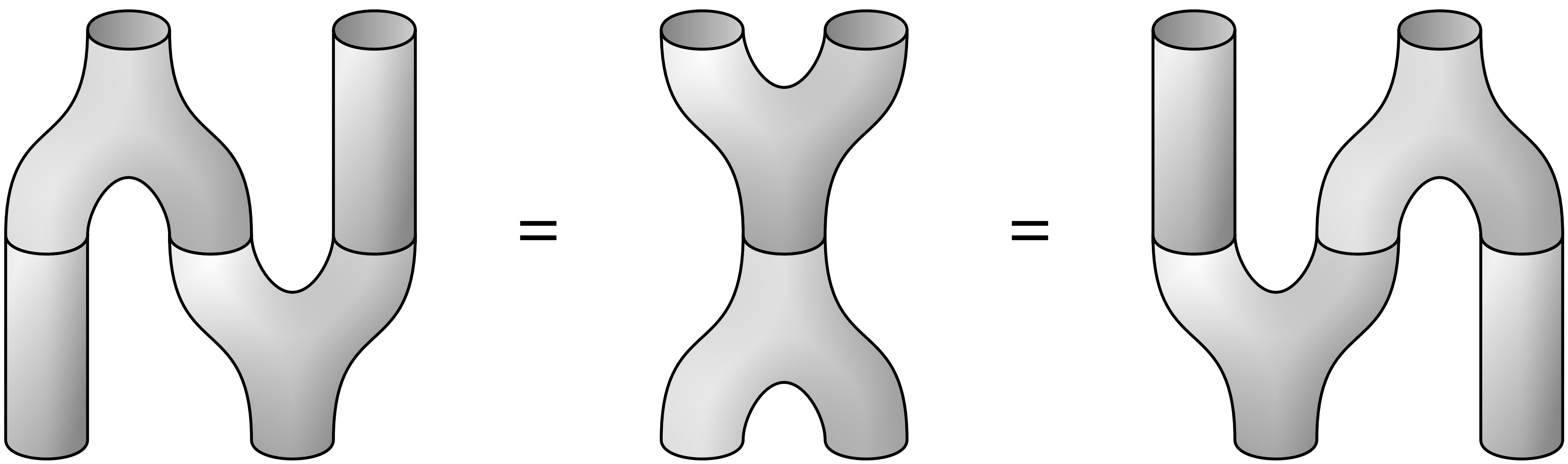
Remarkably, the word problem for monoids is not dependent on the actual presentation.

Shown by Tietze transformation rules.

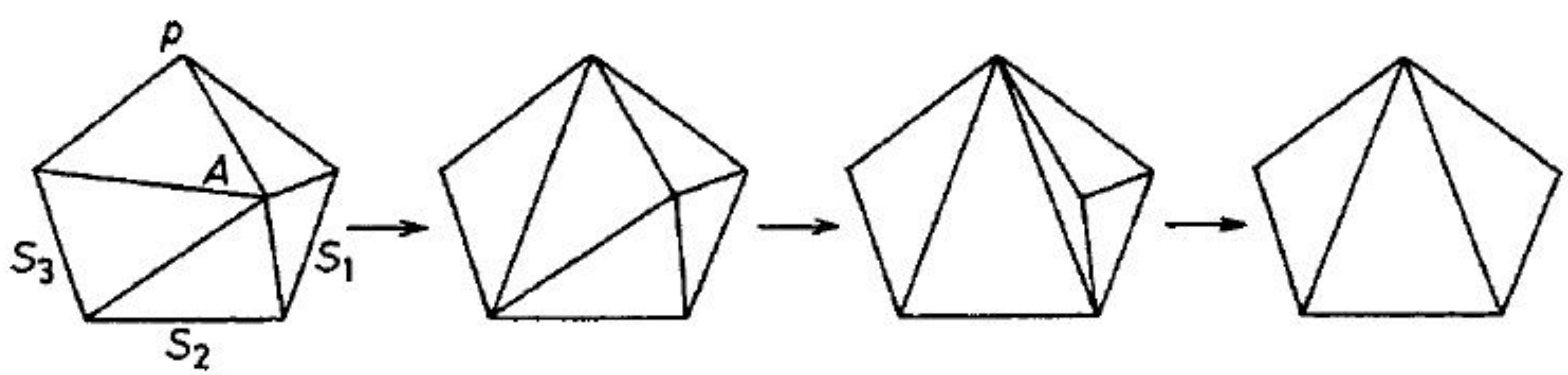
The same holds for a large class of Sigma-algebras.

(Pers. comm. by V. van Oostrom, June 2012.

axioms in Frobenius algebras



Pachner moves: for transforming different triangulations of topological surfaces into each other



Prijsvraag **Het Cola-gen**

Een team ... tische manipuleer-
ders ... riceren die
ge... n. Daartoe
moet... chte...
DN... van het melkgen:
TAGCTAGCTAGCT
ombouwen tot het cola-...
CTGACTGACT
Er zijn technieken ter beschikking om de volgende DNA-substituties – heen en weer – uit te voeren:

TCAT ↔ T
GAG ↔ AG
CTC ↔ TC
AGTA ↔ A
TAT ↔ CT

given DNA-string

transform it to

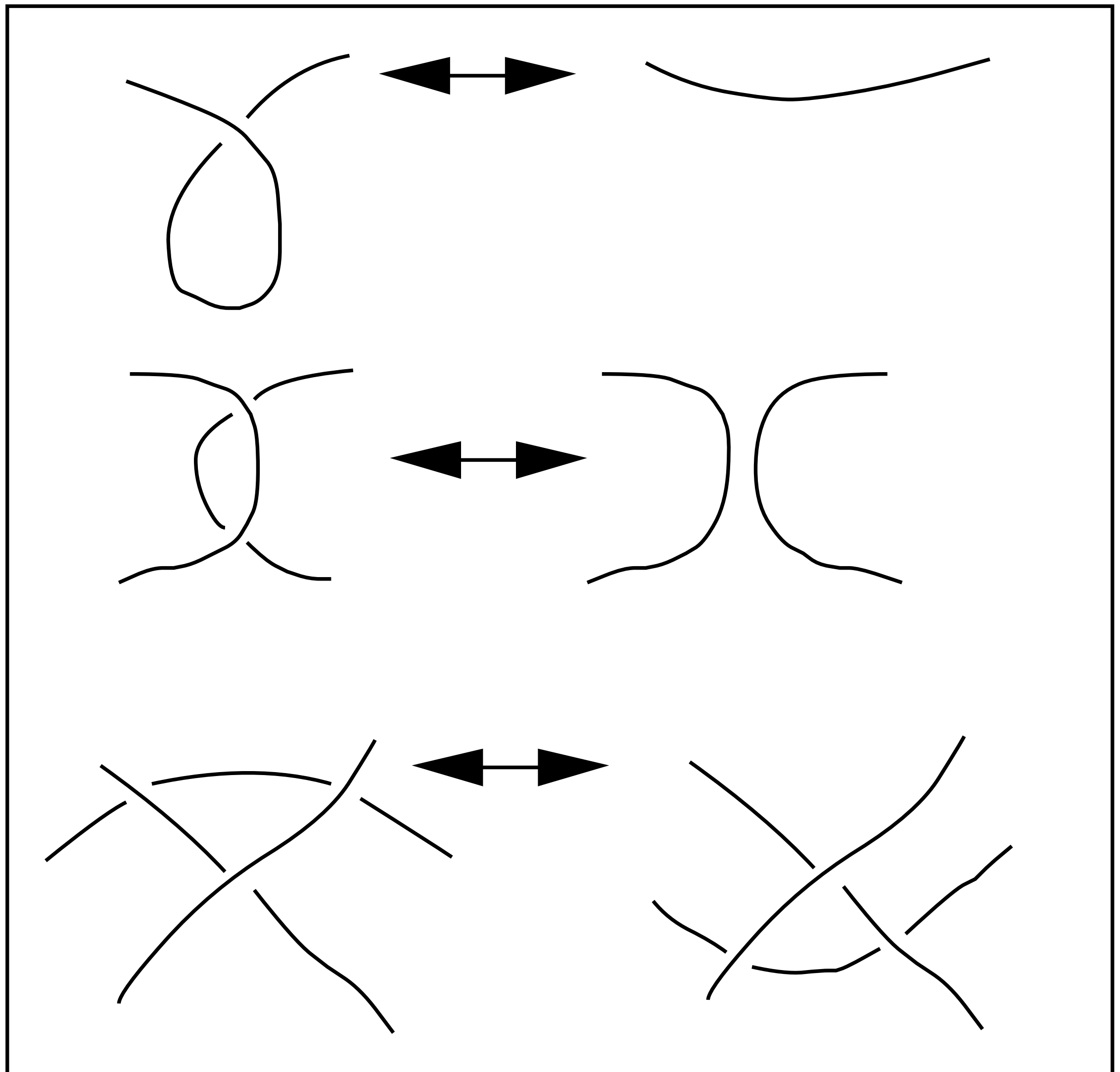
using

Kort daarvoor was echter o...
de gekke-koeienziekte wo...
zaakt door een retro-virus ...
DNA-volgorde:
CTGCTACTGACT
Wat nu, als onbedoeld koeien met dit virus ontstaan? Volgens de manipuleerders loopt dit zo'n vaart niet omdat het bij al hun experimenten nog nooit gebeurd is, maar diverse actiegroepen, zich beroepend op het voorzorgbeginsel, eisen keiharde garanties.
Hoe bewijs je dat dit virus nooit kan ontstaan? Het aantal mogelijke combinaties van substituties is vrijwel eindeloos, dus een slimme redenatie is hier nodig. Het maken van het cola-gen vergt wel behoorlijk wat gepuzzel.

but avoid BSE virus

Zorg dat de oplossing uiterlijk 7 januari 2005 bij de Prijsvraagredactie is, NW&T, postbus 256, 1110 AG Diemen, of *prijsvraag@natutech.nl* o.v.v. Prijsvraag januari.
De winnaar ontvangt een cadeaubon voor Natuurwetenschap&Techniek-producten van€ 35,-.
De prijsvraag voor februari staat vanaf maandag 17 januari al op *www.natutech.nl*.

Reidemeister moves to transform knots into each other



Reidemeister moves