Compatible programs

Two programs P and Q are said to be compatible when their initial valuations and their arity maps coincide on the intersection of their domains of definition. In that case we define the parallel composition $P|Q$.

By extension we define the parallel composition of $P_1, \ldots, P_N$ when the programs are pairwise compatible.

Two programs are said to be syntactically independent when the set of resources they use are disjoint:

- they have no variables in common,
- they have no semaphores in common, and
- they have no barriers in common.

Syntactically independent programs are compatible.

Syntactical independence can be decided statically, it is compositional, but it is too restrictive.

Model Independence

Suppose the programs $P_1, \ldots, P_N$ are conservative.

The programs $P_1, \ldots, P_N$ are said to be model independent when

$$[\![P_1 | \cdots | P_N]\!] = [\![P_1]\!] \times \cdots \times [\![P_N]\!]$$

Model independence can be decided statically.

Compatible permutations

Assume we have a partition

$$\{1,\ldots,n\} \quad = \quad S_1 \sqcup \cdots \sqcup S_N$$

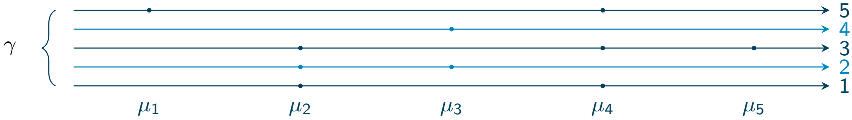
Two multi-instructions μ and μ' ($\mathrm{dom}(\mu), \mathrm{dom}(\mu') \subseteq \{1,\ldots,n\}$) can be swapped when

$$\{j \in \{1,\ldots,N\} \mid S_j \cap \mathrm{dom}(\mu) \neq \emptyset\} \cap \{j \in \{1,\ldots,N\} \mid S_j \cap \mathrm{dom}(\mu') \neq \emptyset\} = \emptyset$$

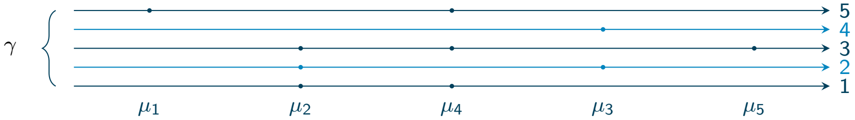
A permutation π of the set $\{0,\ldots,q-1\}$ is said to be compatible with the sequence of multi-instructions $\mu_0,\ldots,\mu_{q-1}$ when it is order preserving on all pairs $\{k,k'\}$ such that μ_k and $\mu_{k'}$ cannot be swapped.

The permutation π is said to be compatible with the directed path γ when it is compatible with its associated sequence of multi-instructions.

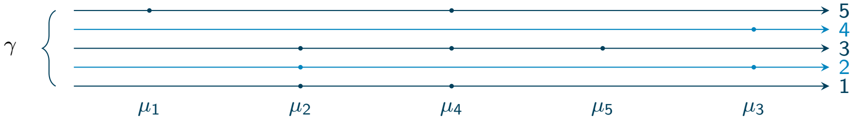
Assume that $S_1 = \{1, 3, 5\}$ and $S_2 = \{2, 4\}$.



Assume that $S_1 = \{1, 3, 5\}$ and $S_2 = \{2, 4\}$.



Assume that $S_1 = \{1, 3, 5\}$ and $S_2 = \{2, 4\}$.



Observational independence

related to partial order reduction (?)

Suppose that the programs $P_1, \ldots, P_N$ are compatible and that P_j has n_j running processes.

The identifiers of the running processes of $P_1|\cdots|P_N$ are the elements of $\{1, \ldots, n\}$ with

$$n \quad = \quad \sum_{j=1}^{N} n_j \;, \qquad \text{and for } j \in \{1, \ldots, N\} \qquad s_j \quad = \quad \sum_{k=1}^{j} n_k$$

$$S_j \quad = \quad \{\ i \in \{1, \ldots, n\} \ \mid \ s_{j-1} \ < \ i \ \leqslant \ s_j\ \}$$

The programs $P_1, \ldots, P_N$ are said to be observationally independent when:

- for all execution traces γ
- for all permutations π compatible with the sequence of multi-instructions $(\mu_0 \cdots \mu_{q-1})$ associated with γ,

there exists an execution trace γ' whose associated sequence of multi-instructions is $\pi \cdot (\mu_0 \cdots \mu_{q-1})$, which has the same action on the system state than γ, that is to say

$$\sigma \cdot (\mu_0 \cdots \mu_{q-1}) \quad = \quad \sigma \cdot (\mu_{\pi^{-1}(0)} \cdots \mu_{\pi^{-1}(q-1)}) \;.$$

Observational independence cannot be decided statically, moreover it is too loose.

Main theorem

syntactic independence

$\Downarrow$

model independence

$\Downarrow$

observational independence

One-dimensional regions

Let G be a finite graph, the collection $\mathcal{R}_1 G$ of all finite unions of connected subsets of $|G|$ forms a Boolean subalgebra of $\mathrm{Pow}(|G|)$.

Moreover

$$\mathcal{R}_1 G \quad \cong \quad \mathrm{Pow}(V) \times (\mathcal{R}_1]0,1[)^{\mathrm{card} A}$$

with A (resp. V) being the set of arrows (resp. vertices) of G, and $\mathcal{R}_1]0,1[$ being the Boolean algebra of finite unions of subintervals of $]0,1[$.

The elements of $\mathcal{R}_1 G$ are seen as one-dimensional blocks.

Proof: If X is a connected subset of $|G|$ then for all arrows $\alpha \in G$, $X \cap (\{\alpha\} \times]0,1[)$ has at most two connected components.

The finiteness condition is not necessary e.g.

$$\cdots \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdot \longrightarrow \cdots$$

Yet some infinite graphs may not enjoy the property e.g. when G is a graph with a single vertex and infinitely many arrows.

Higher dimensional blocks

- A block of dimension $n \in \mathbb{N}$, or n-block, is the product of n connected subsets of the metric graph $|G|$.
- A collection of blocks is called a block covering of $X \subseteq |G|^n$ when the union of its elements is X.
- The collection of n-dimensional block coverings is denoted by $\mathrm{Cov}_n G$, it is preordered by

$$C \preccurlyeq C' \quad \equiv \quad \forall b \in C \; \exists b' \in C', \; b \subseteq b'$$

Maximal blocks

- A block contained in X is said to be a block of X. Such a block is said to be maximal when no block of X strictly contains it.
- The maximal connected block covering of $X \subseteq |G|^n$ is the set of all its maximal connected blocks, it is denoted by $\alpha_n(X)$.
- $\alpha_n(X) = \{\emptyset\}$ if and only if $X = \emptyset$.

A Galois connection

We have a Galois connection (γ_n, α_n) between $\mathrm{Cov}_n G$ and $\mathrm{Pow}(|G|^n)$ with $\gamma_n(D) = \bigcup D$ for all $D \in \mathrm{Cov}_n G$.

$$\mathrm{Cov}_n G \underset{\alpha_n}{\overset{\gamma_n}{\rightleftarrows}} \mathrm{Pow}(|G|^n)$$

In particular $\gamma_n \circ \alpha_n = id$ and $id \preccurlyeq \alpha_n \circ \gamma_n$. That Galois connection induces an isomorphism of Boolean algebras between $\mathrm{Pow}(|G|^n)$ and the image of α_n i.e. the collection of maximal connected block coverings.

Proof: any *connected* block is contained in a maximal *connected* block (by the Hausdorff maximal principle).

$$\bigcup_i^{\uparrow} \left(B_1^{(i)} \times \cdots \times B_n^{(i)} \right) \quad = \quad \left(\bigcup_i^{\uparrow} B_1^{(i)} \right) \times \cdots \times \left(\bigcup_i^{\uparrow} B_n^{(i)} \right)$$

Isothetic regions

- An isothetic region of dimension n is a subset of $|G|^n$ that admits a finite block covering.
- The geometric model of a conservative program is an isothetic region.
- The collection of isothetic regions of dimension n is denoted by $\mathcal{R}_n G$.
- The collection of finite block covering of dimension n is denoted by $\mathrm{Cov}_{nf}\, G$.

The previous Galois connection

restricted to isothetic regions

Suppose that the graph G is finite. The collection of n-dimensional isothetic regions $\mathcal{R}_n G$ forms a Boolean subalgebra of $\mathrm{Pow}(|G|^n)$ and the previous Galois connection restricts to a Galois connection between $\mathrm{Cov}_{nf}\ G$ and $\mathcal{R}_n G$, which induces an isomorphism of Boolean algebras between $\mathcal{R}_n G$ and the image of α_n i.e. the collection of finite maximal block coverings.

$$\mathrm{Cov}_{nf}\ G \underset{\alpha_n}{\overset{\gamma_n}{\rightleftarrows}} \mathcal{R}_n G$$

A subset $X \subseteq |G|^n$ is an isothetic region iff the collection of maximal subblocks of X is finite and covers X.

The complement of a block is an isothetic region

If X is 1-dimensional then its maximal blocks are its connected components.
The complement of a block $B = B_1 \times \cdots \times B_n$ can be written as

$$B^c = \bigcup_{k=1}^{n} |G| \times \cdots \times B_k^c \times \cdots \times |G|$$

Its maximal blocks are found among that of B^c therefore they have the form

$$D_1 \times \cdots \times D_{k-1} \times C_k \times D_{k+1} \times \cdots \times D_n$$

with $k \in \{1, \ldots, n\}$, C_k ranging through the connected components of B_k^c and D_j, for $j \neq k$, ranging through the connected components of $|G|$.

Intersection of two isothetic regions

The intersection of the blocks B and B' is given by

$$B \cap B' = (B_1 \cap B_1') \times \cdots \times (B_n \cap B_n')$$

The maximal blocks of $B \cap B'$ are therefore of the form

$$C_1 \times \cdots \times C_n$$

with each C_k ranging trough the connected components of $(B_k \cap B_k')$.

It follows from De Morgan's laws that the intersection of two regions is still a region.

Moreover if $\mathcal{B}$ and $\mathcal{B}'$ are block coverings of X and X' containing all their maximal blocks, then the collection of maximal blocks of $B \cap B'$ for $B \in \mathcal{B}$ and $B' \in \mathcal{B}'$ is a block covering of $X \cap X'$ containing all its maximal blocks.

Concluding the proof

If $\mathcal{F}$ is any finite block covering of X, then

$$X^c = \bigcap_{B \in \mathcal{F}} B^c$$

- The collection of maximal blocks of B^c is finite and covers B^c.
- The maximal blocks of X^c are obtained as certain finite intersection of the form

$$\bigcap \{M_B \mid B \in \mathcal{F}\}$$

where M_B is a maximal block of B^c.
- The maximal blocks of X^c thus form a finite block covering of X^c.

A result from directed topology

For all directed paths γ on $\upharpoonleft G \downharpoonright^n$ and all $X \in \mathcal{R}_n G$, the inverse image of X by γ has finitely many connected components.

Closure, interior, and boundary of an isothetic region

The closure operator preserves finite products, therefore it preserves blocks.

The closure operator preserves finite unions hence it preserves isothetic regions.

The boundary of a set is the intersection of its closure and the closure of its complement, hence it also preserves isothetic regions.

The interior of a set is the difference between its closure and its boundary. It follows that the interior operator also preserves isothetic regions.

The forward and the backward operators

Let A, B be subsets of a local pospace X.

- The forward and the backward operators are defined as

$$\mathrm{frw}(A,B) = \{\partial^{+}\delta \mid \delta \text{ directed path on } X;\ \partial^{-}\delta \in A;\ \mathrm{im}(\delta) \subseteq A \cup B\}$$

$$\mathrm{bck}(A,B) = \{\partial^{-}\delta \mid \delta \text{ directed path on } X;\ \partial^{+}\delta \in A;\ \mathrm{im}(\delta) \subseteq A \cup B\}$$

- The future cone of A in X is $\mathrm{cone}^{\mathrm{f}}A := \mathrm{frw}(A,X)$ and
  the past cone of A in X is $\mathrm{cone}^{\mathrm{p}}A := \mathrm{bck}(A,X)$.
- The future closure of A in X is $\overline{A}^{\mathrm{f}} := \mathrm{frw}(A,\overline{A})$ and
  the past closure of A in X is $\overline{A}^{\mathrm{p}} := \mathrm{bck}(A,\overline{A})$.
  The closure $\overline{A}$ being understood in X.

Theorem: if A, B, and X are isothetic regions, then so are $\mathrm{frw}(A,B)$, $\mathrm{cone}^{\mathrm{f}}A$, $\overline{A}^{\mathrm{f}}$, and their duals.

Future/past stable subsets of X

let A be a subset of a local pospace X.

- $\text{cone}^{\text{f}}\text{cone}^{\text{f}}A = \text{cone}^{\text{f}}A$ and $\text{cone}^{\text{p}}\text{cone}^{\text{p}}A = \text{cone}^{\text{p}}A$
- A is said to be future (resp. past) stable (in X) when $\text{cone}^{\text{f}}A = A$ (resp. $\text{cone}^{\text{p}}A = A$)
- A is future stable iff $X \setminus A$ is past stable
- The collection of future stable subsets of X is a complete lattice, the greatest lower (resp. least upper) bound of a family being given by its intersection (resp. union).
- The same holds for past stable subsets.

Past/future attractors

Let A be a subset of a local pospace X.

$$\mathrm{cone}^{\mathrm{p}} A \quad = \quad \{p \in X \text{ from which } A \text{ can be reached}\} \quad = \quad \mathrm{bck}(A, X) \quad = \quad \mathrm{cone}^{\mathrm{p}} A$$

$$\mathrm{escape}^{\mathrm{f}} A \quad = \quad \{p \in X \text{ from which } A \text{ is avoided}\} \quad = \quad \{p \in X \text{ from which } A \text{ cannot be reached}\}$$

$$\mathrm{escape}^{\mathrm{f}} A \quad = \quad (\mathrm{cone}^{\mathrm{p}} A)^c$$

$$\mathrm{att}^{\mathrm{p}} A \quad = \quad \{p \in X \text{ from which } A \text{ cannot be avoided}\}$$

$$\mathrm{att}^{\mathrm{p}} A \quad = \quad \mathrm{escape}^{\mathrm{f}}(\mathrm{escape}^{\mathrm{f}} A)$$

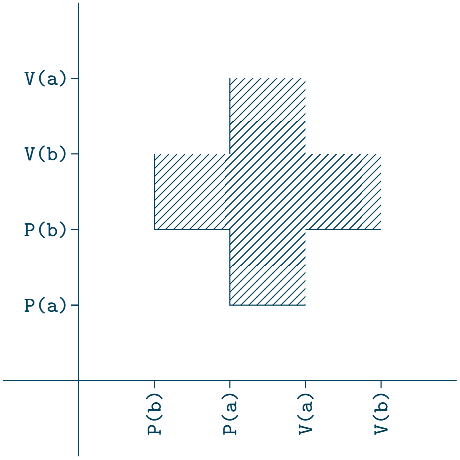
The deadlock attractor of a conservative program

Let $G_1, \ldots, G_n$ be the running processes of a conservative program P.
Let $[\![P]\!]$ be the geometric model of the program.

- The reachable space of $[\![P]\!]$ is the future cone of the initial point
- A point $p \in \upharpoonleft G_i \downharpoonright$ is said to be terminal when $[\![\gamma]\!]$ is empty for all directed paths on $\upharpoonleft G_i \downharpoonright$ starting at p.
- A point $p \in [\![P]\!]$ is said to be terminal when so are all its projections
- The terminal points form a future stable isothetic region of $[\![P]\!]$
- A point $p \in [\![P]\!]$ is said to be deadlock when its future cone neither contains directed loops (i.e. it is loop-free) nor terminal points.
- The deadlock points form a future stable isothetic region of $[\![P]\!]$
- The deadlock attractor of the program is the past attractor of its deadlock region.

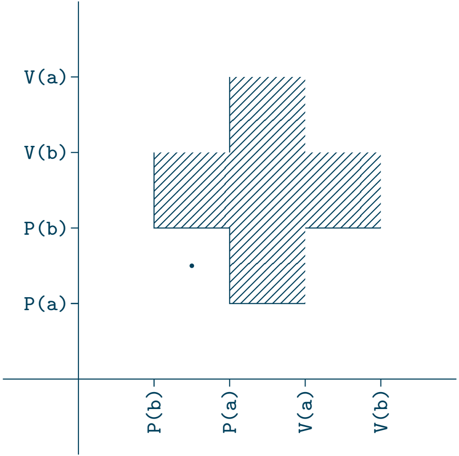
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



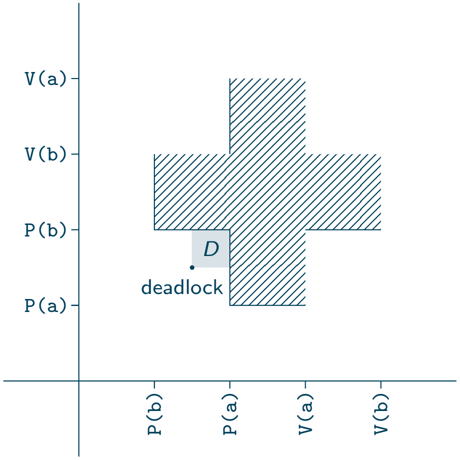
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



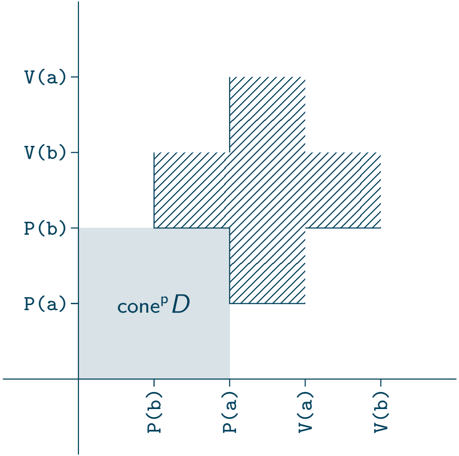
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



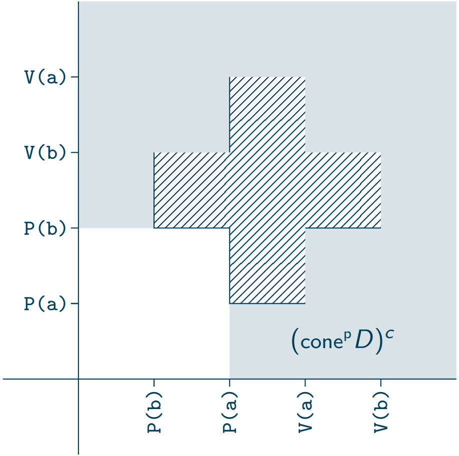
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



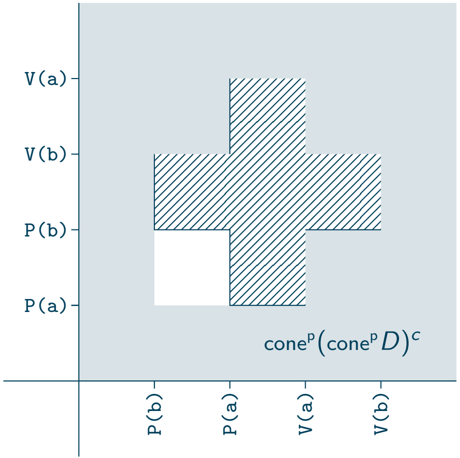
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



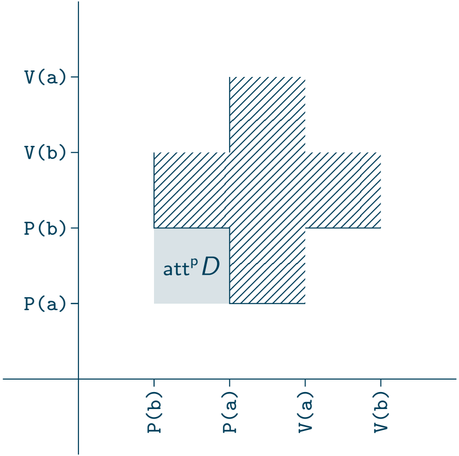
Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```

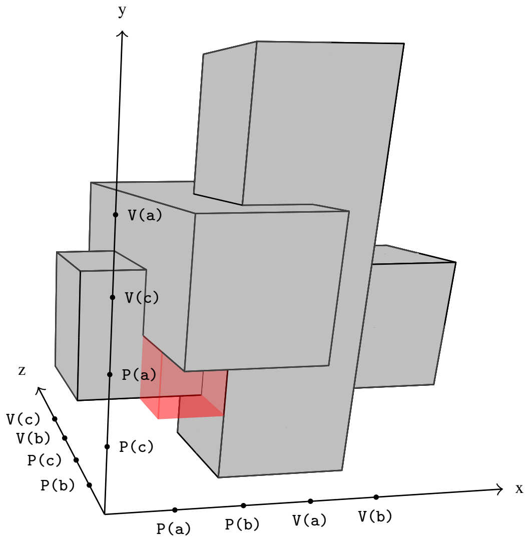


Deadlock attractor of the Swiss Cross

```
sem 1 a b
proc:
p = P(a).P(b).V(b).V(a)
q = P(b).P(a).V(a).V(b)
init:  p q
```



Three dining philosophers



Commutative monoids

- $(M, *, \varepsilon)$ such that for all $a, b, c \in M$,
  - $(ab)c = a(bc)$
  - $\varepsilon a = a = a\varepsilon$
  - $ab = ba$
- For all set X the collection MX of multisets over X
  i.e. maps $\phi : X \to \mathbb{N}$ s.t. $\{x \in X \mid \phi(x) \neq 0\}$ is finite
  forms a commutative monoid with pointwise addition
- A commutative monoid is said to be free when
  it is isomorphic with some MX
- Functor $M : \mathcal{Set} \to \mathcal{Cmon}$
  - A multiset ϕ can be written as

$$\sum_{x \in X} \phi(x)x$$

  - In particular, if $f : X \to Y$ is a set map, then

$$M(f)(\phi) = \sum_{x \in X} \phi(x)f(x)$$

Prime *vs* irreducible

- d divides x, denoted by $d|x$, when there exists x' such that $x = dx'$
- u unit: exists u' s.t. $uu' = \varepsilon$ then write $x \sim y$ when $y = ux$ for some unit u
- i irreducible: i nonunit and $x|i$ implies $x \sim i$ or x unit
- p prime: p nonunit and $p|ab$ implies $p|a$ or $p|b$
- If M contains nontrivial units, then one can consider the quotient monoid $M/\sim$ where $x \sim y$ stands for: there exists a unit u s.t. $y = ux$

Examples

monoid	irreducibles	primes	units
$\mathbb{N} \setminus \{0\}, \times, 1$	{prime numbers}		$\{1\}$
$\mathbb{N}, +, 0$	$\{1\}$		$\{0\}$
$\mathbb{R}_+, +, 0$	$\emptyset$		$\{0\}$
$\mathbb{R}_+, \vee, 0$	$\emptyset$	$\mathbb{R}_+ \setminus \{0\}$	$\{0\}$
$\mathbb{Z}_6, \times, 1$	$\emptyset$	$\{2, 3, 4\}$	$\{1, 5\}$

Graded commutative monoid

- $(M, *, \varepsilon)$ graded: there is a morphism $g : (M, *, \varepsilon) \to (\mathbb{N}, +, 0)$
  s.t. $g^{-1}(\{0\}) = \{\text{units of } M\}$
- If M is graded then
  - $\{\text{irreducibles of } M\}$ generates M
  - $\{\text{primes of } M\} \subseteq \{\text{irreducibles of } M\}$

Irreducible that are not prime

$M = (\{a + b\sqrt{10} \mid a, b \in \mathbb{Z}; a \neq 0 \text{ or } b \neq 0\}, \times, 1)$

- $N : M \to (\mathbb{Z} \setminus \{0\}, \times, 1)$; $N(a + b\sqrt{10}) = a^2 - 10b^2$
  $N(uv) = N(u)N(v)$
  u unit iff $N(u) \in \{\pm 1\}$ [hint: $u^{-1} = N(u)\bar{u}$ with $\bar{u} = a - b\sqrt{10}$ if $u = a + b\sqrt{10}$]
  $N(a + b\sqrt{10}) \bmod 10 \in \{0, 1, 4, 5, 6, 9\}$
  therefore $N(a + b\sqrt{10}) \notin \{\pm 2, \pm 3\}$

uv	N(uv)	N(u)
2	4	$\pm 1, \pm 2, \pm 4$
3	9	$\pm 1, \pm 3, \pm 9$
$4 \pm \sqrt{10}$	6	$\pm 1, \pm 2, \pm 3, \pm 6$

- 2, 3, and $4 \pm \sqrt{10}$ are irreducible but not prime
  since $2 \cdot 3 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10})$
- $\{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\} \setminus \{0\}$ is graded by the number of prime factors of $N(u)$

$\mathbb{N}[X]$ polynomials with coefficients in $\mathbb{N}$

On Direct Product Decomposition of Partially Ordered Sets. Junji Hashimoto
Annals of Mathematics **2**(54), pp 315-318 (1951)

$X^5 + X^4 + X^3 + X^2 + X + 1 =$

$$\begin{cases} (X+1)(X^4+X^2+1) = (X^3+1)(X^2+X+1) & \text{in } \mathbb{N}[X] \\ (X+1)(X^2+X+1)(X^2-X+1) & \text{in } \mathbb{Z}[X] \end{cases}$$

- therefore $X+1$, X^2+X+1, X^3+1, and X^4+X^2+1 are irreducible but not prime
- $\mathbb{N}[X] \setminus \{0\}$ is graded by the degree

Characterization of the free commutative monoids

Unique factorization

- The following are equivalent:
  - M is free commutative
  - any element of M can be written as a product
    of irreducibles in a unique way up to reordering
  - {primes of M} = {irreducibles of M} and generates M
  - M is graded and {irreducibles of M} $\subseteq$ {primes of M}
- Standard examples:
  - $(\mathbb{N} \setminus \{0\}, \times, 1)$
  - $(\mathbb{N}, +, 0)$ and its finite products in the category of commutative monoids.
    Indeed $(\mathbb{N}, +, 0)^n \cong M(\{1, \ldots, n\})$
  - $(\mathbb{Z}[X] \setminus \{0\}, \times, 1)$ (if F is a factorial ring, then so is $F[X]$) *Algebra*, Serge Lang. Springer (2002)
  - Note that two free commutative monoids are isomorphic in $\mathcal{Cmon}$ iff
    their set of prime elements have the same cardinality
    e.g. $(\mathbb{N} \setminus \{0\}, \times, 1) \cong (\mathbb{Z}[X] \setminus \{0\}, \times, 1)$ in $\mathcal{Cmon}$

Connected sum of manifolds

A less common example

In differential geometry, the compact, connected, oriented, smooth n-dimensional manifolds without boundary equipped with the connected sum $\#$ form a commutative monoid $\mathcal{M}_n$ whose neutral element is the n-sphere.

tom Dieck, T. Algebraic Topology. European Mathematical Society 2008. p.390

$\mathcal{M}_2$ is freely generated by the torus T^2.

Massey, W.S. A Basic Course in Algebraic Topology. Springer 1991. Chapter 1.

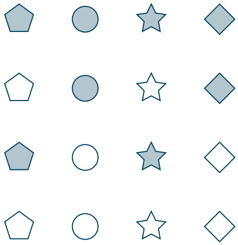
$\mathcal{M}_3$ is freely generated by countably many elements.

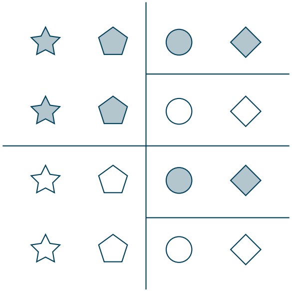
Hempel, J. 3-Manifolds. American Mathematical Society 1976. Chapter 3.

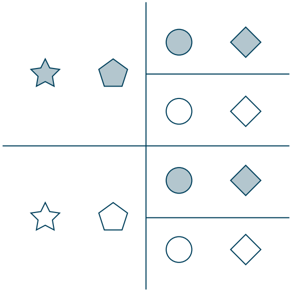
Jaco, W. Lectures on Three-Manifold Topology. American Mathematical Society 1980. Chapter 2.

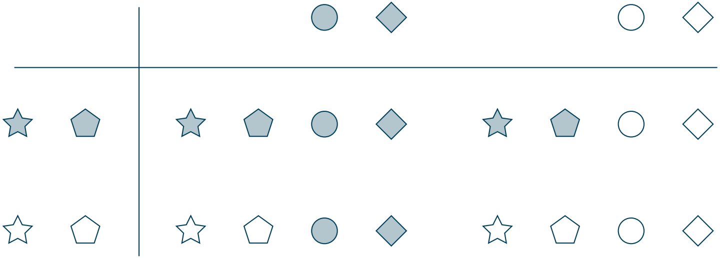
- existence of the decomposition is due to Hellmuth Kneser (1929)
  Kneser, H. Geschlossene Flächen in dreidimensionalen Mannigfaltigkeiten.
  Jahresbericht der Deutschen Mathematiker-Vereinigung 38:248–259 1929.
- uniqueness of the decomposition is due to John W. Milnor (1962)
  Milnor, J. A Unique Decomposition Theorem for 3-Manifolds.
  American Journal of Mathematics 84(1):1–7 1962.

In particular $\mathcal{M}_2 \cong (\mathbb{N}, +, 0)$ and $\mathcal{M}_3 \cong (\mathbb{N} \setminus \{0\}, \times, 1)$









The noncommutative monoid of languages

- $\mathbb{A}^*$ (non commutative) monoid of words on the alphabet $\mathbb{A}$.
  Let ε denotes the empty word
- A language is a set of words on $\mathbb{A}$. Let D and D' be languages
  - define $D \cdot D' := \{w \cdot w' \mid w \in D; w' \in D'\}$
  - one has $\emptyset \cdot D = D \cdot \emptyset = \emptyset$ and $\{\varepsilon\} \cdot D = D \cdot \{\varepsilon\} = D$
  - The monoid of nonempty languages is $\mathcal{D}(\mathbb{A})$
  - $\mathcal{D}(\mathbb{A})$ is commutative iff $\mathrm{Card}(\mathbb{A}) \leqslant 1$. Note that $\mathcal{D}(\emptyset) \cong \{\{\varepsilon\}\}$
  - however $\mathcal{D}(\{a\})$ is not freely commutative

The noncommutative monoid of homogeneous languages

- $H \in \mathcal{D}(\mathbb{A})$ is homogeneous when all the words in H have the same length
- Define $\dim(H)$ as the length common to all the words of H.
  It is well defined since H is nonempty.
- $H \cdot H' = \{w \cdot w' \mid w \in H \; ; \; w' \in H'\}$ is homogeneous iff so are H and H'
- $\mathcal{D}_h(\mathbb{A}) \subseteq \mathcal{D}(\mathbb{A})$ the pure submonoid of homogeneous languages.
- $H \in \mathcal{D}_h(\mathbb{A}) \mapsto \dim(H) \in (\mathbb{N}, +, 0)$ is a morphism of monoid
- $\dim(H) = 0$ iff $H = \{\varepsilon\}$
- $\mathcal{D}_h(\mathbb{A})$ is commutative iff $\mathrm{Card}(\mathbb{A}) \leqslant 1$
- $\mathcal{D}_h(\{a\}) \cong (\mathbb{N}, +, 0)$

Action of the symmetric groups

on the left of the homogeneous languages

- The n^{th} symmetric group $\mathfrak{S}_n$ acts on the left of the set of words of length n i.e. mappings from $\{1, \dots, n\}$ to $\mathbb{A}$, by $\sigma \cdot \omega := \omega \circ \sigma^{-1}$
- Then $\mathfrak{S}_n$ acts on the left of the homogeneous languages of dimension n
- Write $H \sim H'$ when $\dim(H) = \dim(H')$ and $H' = \sigma \cdot H$ for some $\sigma \in \mathfrak{S}_{\dim(H)}$
- If $\sigma \in \mathfrak{S}_n$ and $\sigma' \in \mathfrak{S}_{n'}$ then define $\sigma \otimes \sigma' \in \mathfrak{S}_{n+n'}$ as:

$$\sigma \otimes \sigma'(k) := \begin{cases} \sigma(k) & \text{if} \quad 1 \leqslant k \leqslant n \\ (\sigma'(k-n)) + n & \text{if} \quad n+1 \leqslant k \leqslant n+n' \end{cases}$$

- A Godement exchange law is satisfied, which ensures that $\sim$ is actually a congruence:

$$(\sigma \cdot H) \cdot (\sigma' \cdot H') = (\sigma \otimes \sigma') \cdot (H \cdot H')$$

i.e. $H \sim K$ and $H' \sim K'$ implies $HH' \sim KK'$

The commutative monoid of homogeneous languages

- The commutative monoid of homogeneous languages is $\mathcal{H}(\mathbb{A}) = (\mathcal{D}_h(\mathbb{A}), \cdot, \{\varepsilon\})/\sim$
- The monoid $\mathcal{H}(\mathbb{A})$ is graded by $H \in \mathcal{H}(\mathbb{A}) \mapsto \mathrm{dim}(H) \in (\mathbb{N}, +, 0)$

The commutative monoid $\mathcal{H}(\mathbb{A})$ is free

- For any homogeneous language H and $\sigma \in \mathfrak{S}_{\mathrm{dim}(H)}$, $\mathrm{card}(H) = \mathrm{card}(\sigma \cdot H)$ so we can define the cardinality of any element of $\mathcal{H}(\mathbb{A})$

The commutative monoid of finite homogeneous languages

- $M' \subseteq M$ is said to be pure when for all $x, y \in M$, $xy \in M'$ implies $x, y, \in M'$
- A pure submonoid of a free commutative monoid is free
- The submonoid $\mathcal{H}_f(\mathbb{A}) \subseteq \mathcal{H}(\mathbb{A})$ of finite languages is pure, therefore it is free
- $H \in \mathcal{H}_f(\mathbb{A}) \mapsto \mathrm{Card}(H) \in (\mathbb{N} \setminus \{0\}, \times, 1)$ is a morphism of monoid
- The primality of Card(H) does not imply that of H
  e.g. $H = \{ab, ac\} = \{a\} \cdot \{b, c\}$ though card(H) $= 2$
- The primality of H does not imply that of Card(H)
  e.g. $H = \{a, b, c, d\}$ is prime though card(H) $= 4$

The brute force algorithm for factoring in $\mathcal{H}_f(\mathbb{A})$

Theory

Given $w \in \mathbb{A}^n$ and $I \subseteq \{1, \ldots, n\}$, we write $w_{|_I}$ for the subword of w consisting of letters with indices in I.

Given a homogeneous language H of dimension n, we write

$$H_{|_I} \quad = \quad \{w_{|_I} \mid w \in H\}$$

Denoting I^c for $\{1, \ldots, n\} \setminus I$, we have

$$[H] \quad = \quad [H_{|_I}] \cdot [H_{|_{I^c}}]$$

in $\mathcal{H}_f(\mathbb{A})$ if and only if for all words $u, v \in H$ there exists a word $w \in H$ such that

$$w_{|_I} \quad = \quad u_{|_I} \qquad \text{and} \qquad w_{|_{I^c}} \quad = \quad v_{|_{I^c}}$$

The brute force algorithm for factoring in $\mathcal{H}_f(\mathbb{A})$

Practice

For $I \subseteq \{1, \ldots, n\}$ let $\pi_{|_I}$ be the "projection" that sends $w \in H$ to $w_{|_I} \in \mathbb{A}^{\mathsf{card(I)}}$.

1. choose $I \subseteq \{1, \ldots, n\}$ of cardinality $k \leqslant n/2$
2. if $\pi_{|_{I^c}}(\pi_{|_I}^{-1}(u))$ does not depend on $u \in H_{|_I}$, then we have the factorization

$$[H] \quad = \quad [H_{|_I}] \cdot [H_{|_{I^c}}]$$

   and we are done
3. otherwise check whether there are still subsets of $\{1, \ldots, n\}$ to check:
   1. yes: go to step 1
   2. no: $[H]$ is prime

Factoring a program

```
sem:  1 a b
sem:  2 c
```

```
proc:
  p = P(a);P(c);V(c);V(a)

  q = P(b);P(c);V(c);V(b)
```

```
init:  p q p q
```

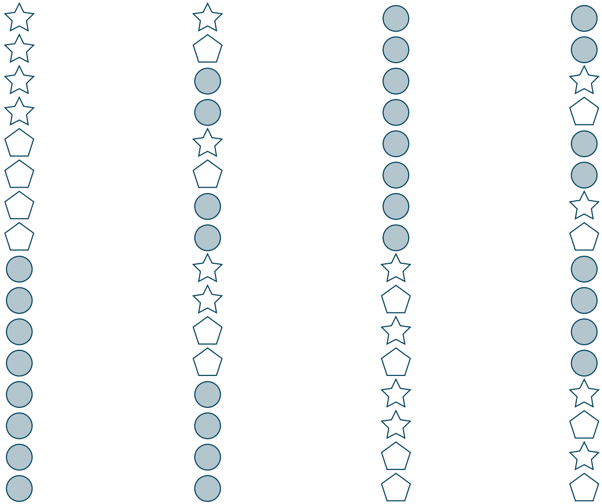
Factoring the space of states

brute force

[0,1[	[0,1[	[0,+∞[	[0,+∞[
[0,1[	[4,+∞[	[0,+∞[	[0,+∞[
[0,1[	[0,+∞[	[0,+∞[	[0,1[
[0,1[	[0,+∞[	[0,+∞[	[4,+∞[
[4,+∞[	[0,1[	[0,+∞[	[0,+∞[
[4,+∞[	[4,+∞[	[0,+∞[	[0,+∞[
[4,+∞[	[0,+∞[	[0,+∞[	[0,1[
[4,+∞[	[0,+∞[	[0,+∞[	[4,+∞[
[0,+∞[	[0,1[	[0,1[	[0,+∞[
[0,+∞[	[0,1[	[4,+∞[	[0,+∞[
[0,+∞[	[4,+∞[	[0,1[	[0,+∞[
[0,+∞[	[4,+∞[	[4,+∞[	[0,+∞[
[0,+∞[	[0,+∞[	[0,1[	[0,1[
[0,+∞[	[0,+∞[	[0,1[	[4,+∞[
[0,+∞[	[0,+∞[	[4,+∞[	[0,1[
[0,+∞[	[0,+∞[	[4,+∞[	[4,+∞[

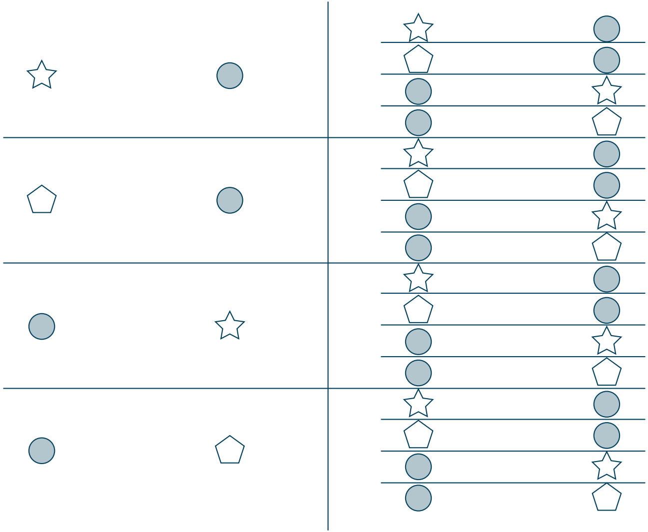
Factoring the space of states

brute force



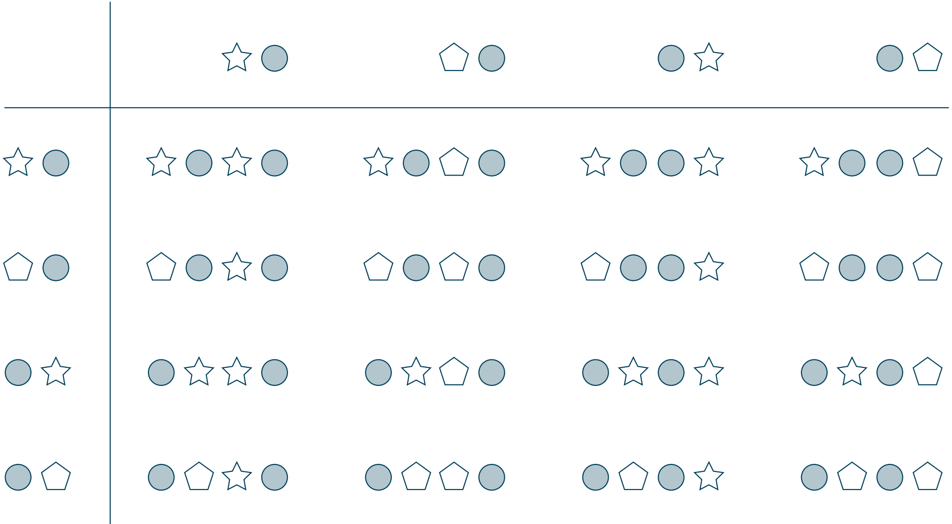
Factoring the space of states

brute force



Factoring the space of states

brute force



Factoring a program

```
sem:  1 a b
sem:  2 c
```

```
proc:
  p = P(a);P(c);V(c);V(a)

  q = P(b);P(c);V(c);V(b)
```

```
init:  p q p q
```

Factoring a program

`sem: 1 a`	`sem: 1 b`
`proc:` `p = P(a);V(a)`	`proc:` `q = P(b);V(b)`
`init: 2p`	`init: 2q`

The preorder $\preccurlyeq$ over $\mathcal{H}(\mathbb{A})$

inherited from a preorder $\preccurlyeq$ over $\mathbb{A}$

- Let $\preccurlyeq^n$ be the product preorder on the words of length n
- Given $H, H' \in \mathcal{D}_h(\mathbb{A})$ of the same dimension n, write $H \preccurlyeq H'$ when for all $\omega \in H$ there exists $\omega' \in H'$ such that $\omega \preccurlyeq^n \omega'$
- Given $X, Y \in \mathcal{H}(\mathbb{A})$ of the same dimension n write $X \preccurlyeq Y$ when there exist $H \in X$ and $K \in Y$ such that $H \preccurlyeq K$
- $X \preccurlyeq Y$ and $X' \preccurlyeq Y'$ implies $X \cdot X' \preccurlyeq Y \cdot Y'$
  i.e. $(\mathcal{H}(\mathbb{A}), \preccurlyeq)$ is a preordered commutative monoid
- If $\preccurlyeq$ is actually a partial order on $\mathbb{A}$, then so is $\preccurlyeq$ on $\mathcal{H}(\mathbb{A})$
- If $\preccurlyeq$ is the equality relation, then $X \preccurlyeq Y$ amounts to $H_X \subseteq H_Y$ for some representatives H_X and H_Y of X and Y.

Homogeneous languages

over the alphabets $\rceil G \lfloor$ and $\mathcal{R}_1 G \setminus \{\emptyset\}$ with G being a finite graph

- $\mathbb{A} = \rceil G \lfloor$ is the geometric realization of a finite graph:
  - a point of $\rceil G \lfloor^n$ can be seen as a word of length n on $\mathbb{A}$
  - a nonempty subset of $\rceil G \lfloor^n$ is thus a homogeneous language on $\mathbb{A}$
  - the product of the monoid $\mathcal{D}_h(\mathbb{A})$ corresponds to the cartesian product of isothetic regions
- $\mathbb{A} = \mathcal{R}_1 G \setminus \{\emptyset\}$ is the collection of nonempty finite unions of connected subsets of $\rceil G \lfloor$:
  - an n-block is an n-fold product of nonempty elements of $\mathcal{R}_1 G$
    i.e. a word of length n on $\mathbb{A}$
  - a nonempty family of n-blocks is thus an homogeneous language on $\mathbb{A}$ (of dimension n)
  - the concatenation of words on $\mathbb{A}$ corresponds to the cartesian product of blocks

The canonical morphism of monoids $\gamma : \mathcal{H}(\mathcal{R}_1 G \setminus \{\emptyset\}) \to \mathcal{H}(\upharpoonleft G \downharpoonleft)$

- Let γ be the map sending an homogeneous language on $\mathcal{R}_1 G \setminus \{\emptyset\}$ to the union of its elements
  - γ is a morphism of monoids from $\mathcal{D}_h(\mathcal{R}_1 G \setminus \{\emptyset\})$ to $\mathcal{D}_h(\upharpoonleft G \downharpoonleft)$
  - γ is compatible with the action of the symmetric groups in the sense that $H' = \sigma \cdot H \ \Rightarrow \ \bigcup H' = \sigma \cdot (\bigcup H)$
  - γ induces a morphism of monoids from $\mathcal{H}(\mathcal{R}_1 G \setminus \{\emptyset\})$ to $\mathcal{H}(\upharpoonleft G \downharpoonleft)$
- The induced morphism γ does not preserve the prime elements e.g. consider a covering of $[0,1]^2$ with 3 disctinct rectangles

The canonical morphism of monoids $\alpha : \mathcal{H}(\upharpoonleft G \downharpoonleft) \to \mathcal{H}(\mathcal{R}_1 G \setminus \{\emptyset\})$

- Define $\alpha(X)$ as the collection of maximal blocks of X:
  - given $X \subseteq \upharpoonleft G \downharpoonleft^n$ and $Y \subseteq \upharpoonleft G \downharpoonleft^m$, the collection of maximal blocks of $X \times Y$ is $\{C \times D \mid C \text{ and } D \text{ are maximal blocks of } X \text{ and } Y\}$
  - the unique maximal block of the unique nonempty subset of $\upharpoonleft G \downharpoonleft^0$ is ε
  - α is a morphism of monoids from $\mathcal{D}_h(\upharpoonleft G \downharpoonleft)$ to $\mathcal{D}_h(\mathcal{R}_1 G \setminus \{\emptyset\})$
  - if C is a maximal block of $X \subseteq \upharpoonleft G \downharpoonleft^n$ then $\sigma \cdot C$ is a maximal block of $\sigma \cdot X$.
  - α induces a morphism of monoids from $\mathcal{H}(\upharpoonleft G \downharpoonleft)$ to $\mathcal{H}(\mathcal{R}_1 G \setminus \{\emptyset\})$
  - $\mathrm{im}(\alpha)$ is a submonoid of $\mathcal{H}(\mathcal{R}_1 G \setminus \{\emptyset\})$
- the morphisms γ and α induce isomorphisms of ordered monoids between $\mathrm{im}(\alpha)$ and $\mathcal{H}(\upharpoonleft G \downharpoonleft)$, the order relation being inherited from inclusion over $\mathcal{R}_1 G \setminus \{\emptyset\}$ and equality over $\upharpoonleft G \downharpoonleft$.
- therefore $\mathrm{im}(\alpha)$ is commutative free

The free commutative monoids of isothetic regions

- By definition, an isothetic region is a finite union of blocks of $X \subseteq \upharpoonleft G \downharpoonleft^n$.
- We have seen that an isothetic region has finitely many maximal blocks .
- For $X, Y \in \mathcal{H}(\upharpoonleft G \downharpoonleft)$, $\alpha(X \cdot Y)$ is finite iff $\alpha(X)$ and $\alpha(Y)$ are so:
  - then $\{X \in \mathrm{im}(\alpha) \mid \mathrm{card}(X) \text{ is finite}\}$ is a pure submonoid of $\mathrm{im}(\alpha)$
  - this commutative monoid is thus free and isomorphic to the monoid of isothetic regions, the latter being defined as

$$\boxed{\gamma(\{X \in \mathrm{im}(\alpha) \mid \mathrm{card}(X) \text{ is finite}\})}$$

  - The monoid of isothetic regions is thus free commutative.

A better factoring algorithm

by Nicolas Ninin

Let $X \subseteq |G|^n$ be an isothetic region and $\mathcal{F}$ be a finite block covering of X^c

- For each block $(\omega_1, \ldots, \omega_n)$ that belongs to $\mathcal{F}$ define the subset

$$B_\omega \quad = \quad \{k \in \{1, \ldots, n\} \mid \omega_k \neq |G|\}$$

- The finest partition of $\{1, \ldots, n\}$ that is coarser than the collection

$$\{B_\omega \mid \omega \in \mathcal{F}\}$$

induces a factorization of X.

If $\mathcal{F} = \alpha(X^c)$ then we obtain the prime factorization of X

Factoring a program

```
sem:  1 a b
sem:  2 c
```

```
proc:
  p = P(a);P(c);V(c);V(a)

  q = P(b);P(c);V(c);V(b)
```

```
init:  p q p q
```

Factoring the space of states

subtle

[2,3[	[2,3[	[2,3[	[0,+∞[
[2,3[	[2,3[	[0,+∞[	[2,3[
[1,4[	[0,+∞[	[1,4[	[0,+∞[
[2,3[	[0,+∞[	[2,3[	[2,3[
[0,+∞[	[1,4[	[0,+∞[	[1,4[
[0,+∞[	[2,3[	[2,3[	[2,3[

Factoring the space of states

subtle

$[1,4[$	$[0,+\infty[$	$[1,4[$	$[0,+\infty[$
$[0,+\infty[$	$[1,4[$	$[0,+\infty[$	$[1,4[$