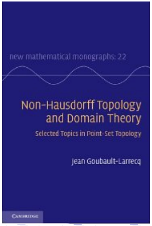
On Noetherian spaces and verification

Jean Goubault-Larrecq

LSV, ENS Cachan, INRIA

Top&Inf, March 22, 2013



Outline

Objective of This Talk

- Develop theory of Noetherian spaces
- Understand motivating applications from computer science.

Outline

How I came to (re)invent Noetherian spaces

In 2005, Alain Finkel asked me:

- The intuitive completion of $\mathbb{N}^k$ is $\mathbb{N}^k_\omega$;
  … used in Karp-Miller procedure for Petri nets (1969).
- For other well-structured transition systems, what should be the completion of their state space X?
- Is there anything in topology that would define the right notion of completion?

My answer:

How I came to (re)invent Noetherian spaces

In 2005, Alain Finkel asked me:

- The intuitive completion of $\mathbb{N}^k$ is $\mathbb{N}_\omega^k$;
  ... used in Karp-Miller procedure for Petri nets (1969).
- For other well-structured transition systems, what should be the completion of their state space X?
- Is there anything in topology that would define the right notion of completion?

My answer:
No way.
(I was wrong.)

How I came to (re)invent Noetherian spaces (2006)

Consider the logic $\mathcal{L}$:

$$F ::= \bot \mid \top \mid A \mid F \wedge F \mid F \vee F \mid \Diamond F \mid \mu A \cdot F(A)$$

interpreted over a transition system $(X, \longrightarrow)$:

$$\begin{aligned} x \models \Diamond F & \Leftrightarrow \exists x' \cdot x \longrightarrow x' \wedge x' \models F, \\ x \models \mu A \cdot F(A) & \Leftrightarrow \exists n \in \mathbb{N} \cdot x \models F^n(\bot). \end{aligned}$$

E.g., reachability ($\exists x' \cdot x \longrightarrow^* x' \wedge x' \models G$?): $\mu A \cdot G \vee \Diamond A$.

One can model-check F against $(X, \longrightarrow)$ by...

How I came to (re)invent Noetherian spaces (2006)

... by computing $[\![F]\!]$, the set of states x such that $x \models F$:

$$\begin{array}{rcl} [\![\Diamond F]\!] & = & Pre([\![F]\!]) \\ [\![\mu A \cdot F(A)]\!] & = & \bigcup^{\uparrow}_{n \in \mathbb{N}} [\![F]\!]^n (\emptyset). \end{array}$$

where $Pre(U) = \{x \mid \exists x' \in U \cdot x \longrightarrow x'\}$.

How I came to (re)invent Noetherian spaces (2006)

... by computing $[\![F]\!]$, the set of states x such that $x \models F$:

$$\begin{array}{rcl} [\![\Diamond F]\!] & = & Pre([\![F]\!]) \\ [\![\mu A \cdot F(A)]\!] & = & \bigcup^{\uparrow}_{n \in \mathbb{N}} [\![F]\!]^{n}(\emptyset). \end{array}$$

For effectivity, topologize X, then:

Lemma

If $\longrightarrow$ is lower semi-continuous and r.e., then:

- $[\![F]\!]$ *is open;*
- $[\![F]\!]$ *is r.e..*

(Many things hidden under the rug here. Effective codes for opens, notably.)

How I came to (re)invent Noetherian spaces (2006)

What about decidability?

- Reachability is undecidable in general
- Main culprit: the infinite union $\bigcup^{\uparrow}_{n \in \mathbb{N}} [\![F]\!]^n(\emptyset)$
- Let's make a bold move!

How I came to (re)invent Noetherian spaces (2006)

Definition (#0)

A topological space X is Noetherian iff every open is compact.

Compact = every open cover has a finite subcover (no separation here!)

How I came to (re)invent Noetherian spaces (2006)

Definition (#0)

A topological space X is Noetherian iff every open is compact.

Compact = every open cover has a finite subcover (no separation here!)

Lemma (#1)

X Noetherian $\Leftrightarrow$ ascending seqs $(U_n)_{n \in \mathbb{N}}$ of opens stabilize.

Proof.

($\Rightarrow$) $U = \bigcup^{\uparrow}_{n \in \mathbb{N}} U_n$ is compact; finite subcover contains maximal U_n, which equals U.

($\Leftarrow$) Let U non-compact open: let $(U_i)_{i \in I}$ open cover of U with no finite subcover; U_1 does not cover U: find U_2 such that $U_1 \cup U_2$ strictly larger; still does not cover, and so on. $\square$

Deciding reachability, and more

Theorem

Let $(X, \longrightarrow)$ be a transition system. Assume:

- *X is Noetherian*
- *Every open U has a code*
- *$\cup, \cap$ are computable, $\subseteq$ is decidable on opens*
- *Pre is computable on opens*

Then $[\![F]\!]$ is computable.

Proof. Previous algorithm terminates. □

In particular, if $x \in U$ is decidable, then $x \models F$ is decidable.

Examples?

- Any finite transition system

Examples?

- Any finite transition system
- Petri nets, $X = \mathbb{N}^k$ (space of markings on k places), with Alexandroff topology of $\leq$ (open$\stackrel{\text{def}}{=}$upward closed)

Proposition

Coverability (i.e., $\exists x' \geq t \cdot x \longrightarrow^* x'$?) is decidable on Petri nets.

Proof. Test $x \models \mu A \cdot G \vee \Diamond A$ with $[\![G]\!] = \uparrow t$, i.e., compute $Pre^*(\uparrow t) = \bigcup^{\uparrow}_{n \in \mathbb{N}} Pre^{\leq n}(\uparrow t)$ ("Std. backward algorithm.") □

Examples?

- Any finite transition system
- Petri nets, $X = \mathbb{N}^k$
- Lossy Channel Systems, $X = Q \times (\Sigma^*)^k$ (k queues), with Alexandroff topology of $= \times (\leq_{\text{emb}})^k$

Proposition

Coverability (i.e., $\exists x' \geq t \cdot x \longrightarrow^* x'$?) is decidable on LCS.

Proof. Test $x \models \mu A \cdot G \vee \Diamond A$ with $[\![G]\!] = \uparrow t$, i.e., compute $Pre^*(\uparrow t) = \bigcup^{\uparrow}_{n \in \mathbb{N}} Pre^{\leq n}(\uparrow t)$ ("Std. backward algorithm.") $\square$.

Examples?

- Any finite transition system
- Petri nets, $X = \mathbb{N}^k$
- Lossy Channel Systems, $X = Q \times (\Sigma^*)^k$
- In fact, every Well-Structured Transition System: X with Alexandroff topology of $\leq$ wqo, $\longrightarrow$ monotonic.

Proposition

Coverability (i.e., $\exists x' \geq t \cdot x \longrightarrow^* x'$?) is decidable on WSTS.

Proof. Test $x \models \mu A \cdot G \vee \Diamond A$ with $[\![G]\!] = \uparrow t$, i.e., compute $Pre^*(\uparrow t) = \bigcup^{\uparrow}_{n \in \mathbb{N}} Pre^{\leq n}(\uparrow t)$ ("Std. backward algorithm.") $\square$.

Wqos

WSTS are based on wqos $\leq$. Equivalently, $\leq$ is wqo on X (equivalently):

- every sequence $(x_n)_{n\in\mathbb{N}}$ is good: $x_i \leq x_j$ for some $i < j$
- every sequence $(x_n)_{n\in\mathbb{N}}$ is perfect:
  has non-decreasing subsequence $x_{i_1} \leq x_{i_2} \leq \ldots \leq x_{i_k} \leq \ldots$
- $\leq$ is well-founded and has no infinite antichain
- every upward closed subset is of the form $\uparrow E$, E finite.

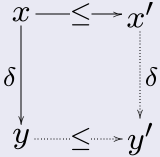
A rich supply of wqos:

- $=$ on finite sets
- $\leq$ on $\mathbb{N}^k$ (Dickson 1913)
- $\leq_{\text{emb}}$ on Σ^* (Higman 1952)
- embedding on finite trees (Kruskal 1960)
- etc.

The theory of WSTS

Definition

A WSTS is $(X, \leq, \longrightarrow)$
with $\leq$ wqo,
and $\longrightarrow$ monotonic.



Theorem (Finkel-Schnoebelen, Abdulla 1990s)

Coverability ($\exists x' \geq t \cdot x \longrightarrow^* x'$?) is decidable in eff. WSTS.

Proof. For U upw. closed, $Pre(U)$ upw. closed by monotonicity.
Compute $U = \bigcup_{n \in \mathbb{N}} Pre^{\leq n}(\uparrow t)$.
Must stabilize (why?).
Then test $x \in U$. □

Wqos and Noetherianness

Lemma

The Alexandroff topology of a wqo is Noetherian.

(Remember: here open $\stackrel{\text{def}}{=}$ upward closed.)

Proof. Let $U = \bigcup^{\uparrow}_{n \in \mathbb{N}} U_n$. By wqo, $U = \uparrow E$ for E finite.
Each $x \in E$ is in some U_n. Take the largest such n: $U = U_n$. □

Wqos and Noetherianness

Lemma

The Alexandroff topology of a wqo is Noetherian.

(Remember: here open $\stackrel{\text{def}}{=}$ upward closed.)

Proof. Let $U = \bigcup^{\uparrow}_{n \in \mathbb{N}} U_n$. By wqo, $U = \uparrow E$ for E finite.
Each $x \in E$ is in some U_n. Take the largest such n: $U = U_n$. $\square$

Proposition

$\leq$ wqo $\Leftrightarrow$ its Alexandroff topology is Noetherian.

Proof. Given $(x_n)_{n \in \mathbb{N}}$, the sequence $(\uparrow\{x_0, x_1, \ldots, x_j\})_{j \in \mathbb{N}}$ stabilizes, say at j:
$x_j \in \uparrow\{x_0, x_1, \ldots, x_{j-1}\}$, hence $x_i \leq x_j$ for some $i < j$. $\square$

Outline

Towards an algebra of Noetherian datatypes

- A rich supply of wqos; Noetherian spaces strictly richer?
- Reproving important wqo-related theorems in Noetherian spaces?
- New theorems with no equivalent in wqo theory?

Towards an algebra of Noetherian datatypes

- A rich supply of wqos; Noetherian spaces strictly richer?
  Yes. The spectrum of a Noetherian ring is Noetherian.
  E.g., $\mathrm{Spec}(\mathbb{C}[X_1, \ldots, X_n])$, or the induced topology on $\mathbb{C}^n$.
  Important in algebraic geometry.
  Certainly does not arise from a wqo.

  Useful in computer science?
- Reproving important wqo-related theorems in Noetherian spaces?
- New theorems with no equivalent in wqo theory?

Towards an algebra of Noetherian datatypes

- A rich supply of wqos; Noetherian spaces strictly richer?
- Reproving important wqo-related theorems in Noetherian spaces?

  Our plan: reproving suitable forms of Dickson, Higman, Kruskal.
- New theorems with no equivalent in wqo theory?

Towards an algebra of Noetherian datatypes

- A rich supply of wqos; Noetherian spaces strictly richer?
- Reproving important wqo-related theorems in Noetherian spaces?
- New theorems with no equivalent in wqo theory?

  Yes. My lips are sealed (for now).

Outline

A stab at Dickson

$\mathbb{N}^k$ is wqo, hence Noetherian.
Can be proved directly, or by showing that $\mathbb{N}$ is wqo, then showing that finite products of wqos are wqo.

Question

Are finite products of Noetherian spaces Noetherian?

Yes. But we need additional tools…

Convergence, self-convergence

- A net $(x_n)_n$ converges to x iff every open neighborhood of x contains x_n for every n large enough
- Limits are unique in Hausdorff spaces. . . but Noetherian spaces will rarely be Hausdorff

Definition

$(x_n)_n$ is self-convergent iff it converges to every x_n.

E.g.:

- in a wqo, the self-convergent sequences are those that are eventually monotonic (exercise!)
- (for experts) every irreducible closed set F defines a canonical self-convergent net $(x)_{x \in F, \leq}$

Three new characterizations

Theorem

The following are equivalent:

- #0 *X is Noetherian*
- #2 *Every subspace of X is compact*
- #3 *Every net $(x_n)_n$ contains a cluster point x_n*

  I.e., every open neighborhood of x_n contains inf many x_m.
- #4 *Every net $(x_n)_n$ has a self-convergent subnet*

Proof. See next slides.

Proof

#0 X is Noetherian
implies
#2 Every subspace A of X is compact

Well-known.
Take open cover $(U_i)_{i \in I}$ of A (inside A).
$U_i = V_i \cap A$ for V_i open in X.
$V = \bigcup_{i \in I} V_i$ open hence compact, so V has finite subcover V_i, $i \in J$.
Note that $A = \bigcup_{i \in J} U_i$. □

Proof

#2 Every subspace A of X is compact
implies

#3 Every net $(x_n)_n$ contains a cluster point x_n

I.e., every open neighborhood of x_n contains inf many x_m.

Let A be set of all x_ns. In a compact space, every net has a cluster point. □

Proof

#3 Every net $(x_n)_n$ contains a cluster point x_n
implies

#4 Every net $(x_n)_n$ has a self-convergent subnet

Let $I = \{n \mid x_n$ cluster point of $(x_n)_n\}$. $(x_n)_{n \in I}$ is a subnet:

- non-empty by #3,
- cofinal: for every m, $(x_n)_{n \text{ after } m}$ has a cluster point by #3,
- directed: for $i, j \in I$, $(x_n)_{n \text{ after } i,j}$ has a cluster point by #3.

By Kelley's Theorem, $(x_n)_{n \in I}$ has a subnet $(x_{\alpha(j)})_j$ that is an ultranet.
For every j, $x_{\alpha(j)}$ is a cluster point of $(x_{\alpha(j)})_j$ (cofinality), hence a limit (ultraness). □

Proof

#4 Every net $(x_n)_n$ has a self-convergent subnet
implies
#0 X is Noetherian

#4 trivially implies #3: every net contains a cluster point. And #1⇔#0. Let us prove ¬#1⇒ ¬#3.
Assume ¬#1: there is an ascending sequence $(U_n)_{n\in\mathbb{N}}$ of opens that does not stabilize.
In particular, pick $x_n \in U_n$, $x_n \notin U_{n-1}$.
x_n is no cluster point, since U_n only contains finitely many x_ms (those with $m \leq n$). □

Back to products

Theorem

Every finite product of Noetherian spaces is Noetherian.

Proof. Assume X, Y Noetherian. Use #4.
Given net $(x_n, y_n)_n$ in $X \times Y$, extract

- self-convergent sequence $(x_{\alpha(j)})_j$ from $(x_n)_n$,
- then self-convergent sequence $(y_{\alpha(\beta(k))})_k$ from $(y_{\alpha(j)})_j$.

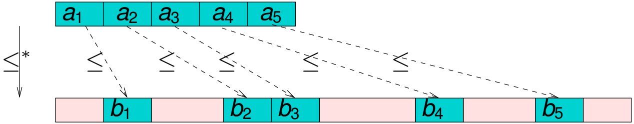
Now $(x_{\alpha(\beta(k))}, y_{\alpha(\beta(k))})_k$ is self-convergent. □

A stab at Higman

Standard form:

Theorem (Higman's Lemma — Application: LCS)

Given a wqo $\leq$ on Σ, the subword quasi-ordering $\leq^*$ on Σ^* is wqo.



A stab at Higman

Theorem (Topological Higman Lemma)

If X is Noetherian, then X^* is Noetherian.

- Requires *subword topology* on X^*, generated by $[U_1 U_2 \ldots U_m] \stackrel{\text{def}}{=} \{\text{words with a subword in } \prod_i U_i\}$
- Specialization quasi-ordering is $\leq^*$
- If X Alexandroff, then X^* Alexandroff, so Higman follows.

To show this, we require yet another characterization of Noetherian spaces… inspired from wqo theory.

The bad sequence lemma

Lemma (Bad sequence)

Let $\mathcal{B}$ be a subbase of the topology of Y. If Y is not Noetherian, then there are $U_n \in \mathcal{B}$ ($n \in \mathbb{N}$) such that $U_n \not\subseteq \bigcup_{m<n} U_m$. Call $(U_n)_{n\in\mathbb{N}}$ a bad sequence.

Note: trivial if $\mathcal{B} = \{\text{all opens}\}$. Analogous to Alexander's subbase lemma.

Proof. Take non-compact open U, $(U_i)_{i\in I}$ open cover of U with no finite subcover. Can take $U_i \in \mathcal{B}$ by Alexander.

Pick U_{i_1}, does not cover U: so some point in U is outside U_{i_1}, hence in some U_{i_2}; some point in U is outside $U_{i_1} \cup U_{i_2}$, hence in some U_{i_3}; and so on. □

The minimal bad sequence lemma

Imitating Nash-Williams (1963):

Lemma (Minimal bad sequence)

Let $\mathcal{B}$ be a base of the topology of Y, with a well-founded quasi-ordering $\sqsubseteq$. If Y is not Noetherian, then it has a minimal bad sequence $(U_n)_{n \in \mathbb{N}}$:

- *(bad)* $U_n \not\subseteq \bigcup_{m<n} U_m$
- *(minimal) every sequence* $(V_n)_{n \in \mathbb{N}}$ *such that* $V_0 = U_0$, $V_1 = U_1, \ldots, V_{n-1} = U_{n-1}$, $V_n \sqsubset U_n$ *for some n is good.*

Proof. Exercise. □

In X^*, define $[U_1 \ldots U_m] \sqsubseteq [U'_1 \ldots U'_{m'}]$ iff $U_1 \ldots U_m$ is subword of $U'_1 \ldots U'_{m'}$.

The zoom-in lemma

Lemma (Zoom-in)

Let X be Noetherian, $a_n \in U_n$, U_n open ($n \in \mathbb{N}$).
There is a subsequence $(a_{n_k})_{k \in \mathbb{N}}$ such that $a_{n_k} \in \bigcap_{j \leq k} U_{n_j}$.

Proof. By #3, pick a cluster point a_{n_0} of $(a_n)_{n \in \mathbb{N}}$. Infinitely many a_ns are in U_{n_0}: extract a subsequence starting with a_{n_0} contained in U_{n_0}. Repeat with the rest of the subsequence, obtaining a_{n_1}, etc. □

The topological Higman lemma

Theorem (Topological Higman Lemma)

If X is Noetherian, then X^* is Noetherian.

Proof. If X^* not Noetherian, let $\mathfrak{U}_n = [U_{n_1} \ldots U_{nm_n}]$ be minimal bad sequence.
Let $w_n \in \mathfrak{U}_n \smallsetminus \bigcup_{m<n} \mathfrak{U}_m$ (badness).
Write w_n as $w'_n a_n w''_n$ with $a_n \in U_{n1}$, $w''_n \in [U_{n2} \ldots U_{nm_n}]$. (Why is w_n non-empty?)
By zoom-in, extract subsequence $(a_{n_k})_{k\in\mathbb{N}}$ with $a_{n_k} \in \bigcap_{j\leq k} U_{n_j1}$. The sequence

$$\mathfrak{U}_0 \mathfrak{U}_1 \ldots \mathfrak{U}_{n_0-1} [U_{n_02} \ldots U_{n_0 m_{n_0}}] \ldots [U_{n_k2} \ldots U_{n_k m_{n_k}}] \ldots$$

is smaller than $(\mathfrak{U}_n)_{n\in\mathbb{N}}$ hence good (minimality).
So $[U_{n_k2} \ldots U_{n_k m_{n_k}}] \subseteq \bigcup_{m=0}^{n_0-1} \mathfrak{U}_m \cup \bigcup_{j<k} [U_{n_j2} \ldots U_{n_j m_{n_j}}]$ for some k.
Since w''_{n_k} is in $[U_{n_k2} \ldots U_{n_k m_{n_k}}]$,

- either $w''_{n_k} \in \mathfrak{U}_m$ for some $m < n_0$: impossible since $w_{n_k} = w'_{n_k} a_{n_k} w''_{n_k}$ would also be in $\mathfrak{U}_m$
- or $w''_{n_k} \in [U_{n_j2} \ldots U_{n_j m_{n_j}}]$ for some $j < k$, whence $w_{n_k} \in [U_{n_j1} U_{n_j2} \ldots U_{n_j m_{n_j}}] = \mathfrak{U}_{n_j}$, impossible as well. □

The topological Kruskal theorem

Theorem

If X is Noetherian, then so is $\mathcal{T}(X)$.

- $\mathcal{T}(X) =$ finite trees with nodes labeled by elements of X=terms over signature X
- under the tree topology, defined in the same style as the subword topology
- proof omitted!

  (Uses a very funny auxiliary topology built from differences of opens arising from some minimal bad sequence. See my book, Theorem 9.7.46)
- usual Kruskal tree theorem a special case.

Outline

Beyond wqos

Examples of Noetherian spaces that are not wqo:

- $\mathbb{C}^k$ with Zariski topology, spectra of polynomial rings, of Noetherian rings (already mentioned)
- Words under the prefix topology

  (prefix ordering not a wqo)
- $\mathbb{P}(X)$ under the lower Vietoris topology:
  - subbasic opens $\Diamond U = \{A \in \mathbb{P}(X) \mid A \cap U \neq \emptyset\}$
  - correspond quasi-ordering would be $A \leq^\flat B$ iff every $a \in A$ is below some $b \in B$...
  - not a wqo by Rado's counterexample.

The powerset

Theorem

For X Noetherian, $\mathbb{P}(X)$ is Noetherian.

Proof. If $\mathbb{P}(X)$ not Noetherian, bad sequence lemma gives opens U_n with $\Diamond U_n \not\subseteq \bigcup_{m<n} \Diamond U_m$.
Check that $\Diamond$ commutes with unions (recall $A \in \Diamond U$ iff A meets U), so $\Diamond U_n \not\subseteq \Diamond \bigcup_{m<n} U_m$.
Check that $\Diamond$ is monotonic, so $U_n \not\subseteq \bigcup_{m<n} U_m$: $(U_n)_{n\in\mathbb{N}}$ is bad, contradicting X Noetherian. □

Note to domain theorists: $\mathbb{P}(X)$ and Hoare powerdomain $\mathcal{H}(X)$ have same lattice of opens, so $\mathcal{H}(X)$ Noetherian as well.

An algebra of Noetherian datatypes

$$
\begin{array}{rclll}
D & ::= & A & \text{(finite qo)} & \\
 & | & \mathbb{N} & & \\
 & | & \mathbb{C}^k & \text{(Zariski topology)} & * \\
 & | & \mathrm{Spec}(R) & (R \text{ Noetherian ring}) & * \\
 & | & D_1 \times D_2 \times \ldots \times D_n & \text{(product)} & \\
 & | & D_1 + D_2 + \ldots + D_n & \text{(disjoint union)} & \\
 & | & D^* & \text{(words, Higman)} & \\
 & | & D^{\circledast} & \text{(multisets)} & \\
 & | & \mathcal{T}(D) & \text{(trees, Kruskal)} & \\
 & | & D^{*,\mathrm{pref}} & \text{(words, prefix topology)} & * \\
 & | & \mathcal{H}(D) & \text{(Hoare hyperspace)} & * \\
 & | & \mathbb{P}(D) & \text{(powerset)} & * \\
 & | & \mathcal{S}(D) & \text{(sobrification)} & *
\end{array}
$$

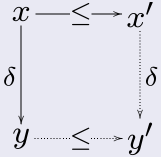
($*$: operator preserves Noetherianness, not wqo-ness.)

Outline

Reminder

Definition

A WSTS is $(X, \leq, \longrightarrow)$
with $\leq$ wqo,
and $\longrightarrow$ monotonic.



Theorem (Finkel-Schnoebelen, Abdulla 1990s)

Coverability ($\exists x' \geq t \cdot x \longrightarrow^* x'$?) is decidable in eff. WSTS.

In fact, logic $\mathcal{L}$ as a whole is decidable.

Topological WSTS

Definition

A topological WSTS is $(X, \longrightarrow)$ with X Noetherian, and $\longrightarrow$ lower semi-continuous (i.e., *Pre* maps opens to opens).

Generalizes WSTS=special case where X is Alexandroff.

Theorem

Let $(X, \longrightarrow)$ be an effective topological WSTS.

- *$[\![F]\!]$ is computable.*
- *Reachability of open subsets is decidable.*

Proof. Already said in a different form. Just compute:

$$\begin{array}{rcl} [\![\Diamond F]\!] & = & Pre([\![F]\!]) \\ [\![\mu A \cdot F(A)]\!] & = & \bigcup^{\uparrow}_{n\in\mathbb{N}} [\![F]\!]^n(\emptyset). \end{array} \quad \square$$

An intriguing application

- Can analyze even programs looking a lot less like WSTS, e.g., polynomial programs [MOS'02]:

```
if (*) { x = 2; y = 3; }
    else { x = 3; y = 2; }
x = x * y − 6; y = 0;
while (*) { x = x + 1; y = y − 1; };
x = x^2 + x * y;
return;
```

Deal with algebra (ideals I) through Zariski topology (opens O_I).

- Algorithmic tools: represent ideals by Gröbner bases.

$$X^3 - 3XY^2 \qquad XY^2Z + 4X^3 + 27$$
$$YZ^2 + 8YZ + 5X - 1 \qquad Z^4 - 81$$

An intriguing application

- Can analyze even programs looking a lot less like WSTS, e.g., polynomial programs [MOS'02]:

```
if (*) { x = 2; y = 3; }
    else { x = 3; y = 2; }
x = x * y − 6; y = 0;
while (*) { x = x + 1; y = y − 1; };
x = x^2 + x * y;
return;
```

Deal with algebra (ideals I) through Zariski topology (opens O_I).

- Algorithmic tools: represent ideals by Gröbner bases.

$$X^3 - 3XY^2 \qquad XY^2Z + 4X^3 + 27$$
$$YZ^2 + 8YZ + 5X - 1 \qquad Z^4 - 81$$

- Combine algebra with wqo theory: the case of lossy concurrent polynomial programs.

Lossy Concurrent Polynomial Programs

Aim: analyze networks of polynomial programs, with lossy communication channels transmitting control signals.

- States: $(q_A, X_1, \ldots, X_m, q_B, Y_1, \ldots, Y_n, w)$
  - q_A: Current line for program A, in Q_A
  - $X_1, \ldots, X_m$: Current values of numerical vars of A, in $\mathbb{C}^m$
  - $q_B, Y_1, \ldots, Y_n$: Same for B
  - w: Contents of comm. channel, in Σ^*
- Transitions:
  - $x := P(x_1, \ldots, x_m)$ (P polynomial), $x :=?$;
  - guards `if` $P(x_1, \ldots, x_m) \neq 0$ `then` $\ldots$;
  - $!a$, $?a$.

Lossy Concurrent Polynomial Programs

$$(q_A, \underbrace{X_1, \ldots, X_m}, q_B, \underbrace{Y_1, \ldots, Y_n}, w)$$

- q_A: Current line for program A, in Q_A
- $X_1, \ldots, X_m$: Current values of numerical vars of A, in $\mathbb{C}^m$
- $q_B, Y_1, \ldots, Y_n$: Same for B
- w: Contents of comm. channel, in Σ^*

Theorem (Decidability)

Given initial state s and set U described as forbidden patterns, it is decidable whether one can reach U from s.

Note: one needs Gröbner bases for the polynomial part
+ subsets $\uparrow E$ for the channel (wqo) part.

Topology allows us to blend the two seamlessly.

Key insight: the product of $Q_A \times \mathbb{C}^m$, $Q_B \times \mathbb{C}^n$ (Noetherian with Zariski) and Σ^* (Noetherian since wqo) is Noetherian. □

Outline

Forward procedures

- Until now, we stressed backward algorithms.
  - Always terminates.
  - Decides coverability
    (reachability for lossy/oblivious systems).

Forward procedures

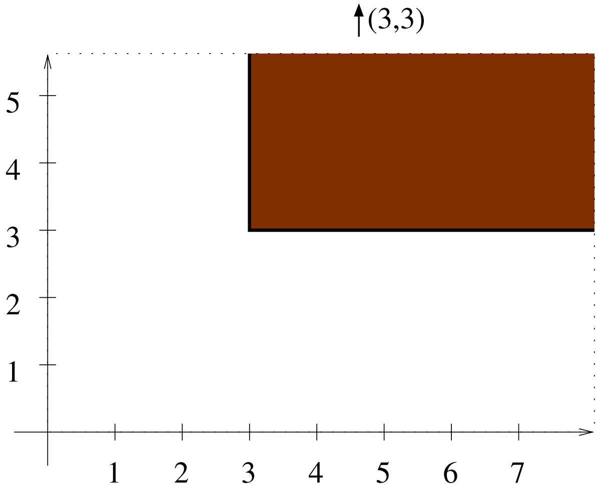
- Until now, we stressed backward algorithms.

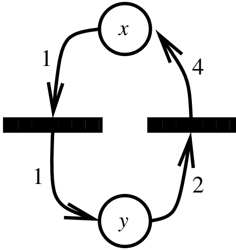
  - Always terminates.
  - Decides coverability
    (reachability for lossy/oblivious systems).

- Design forward procedures for general (topo.) WSTS?

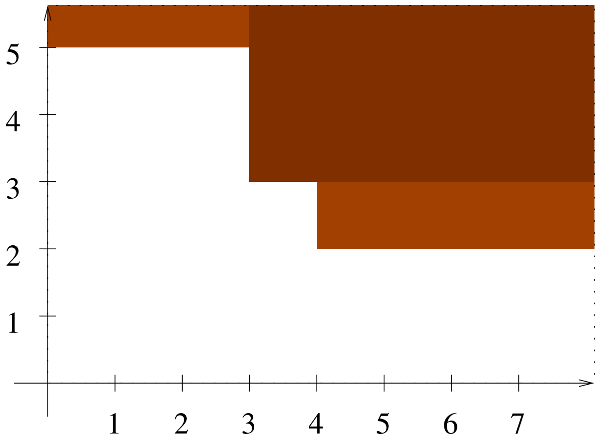
A la Karp-Miller [KM69] . . . which works only for (plain) Petri nets.

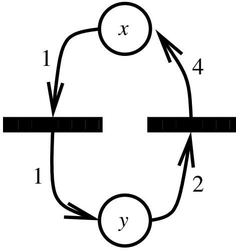
Instead of:



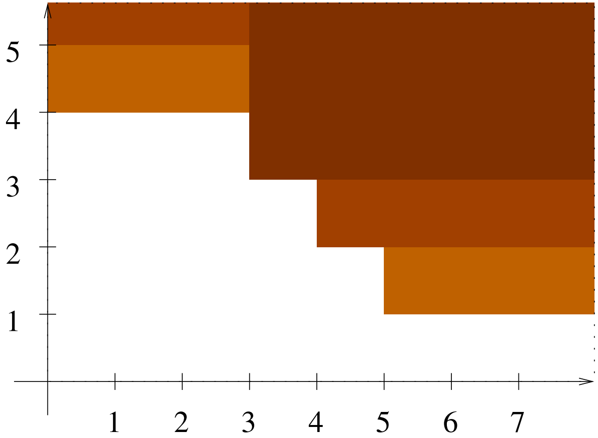


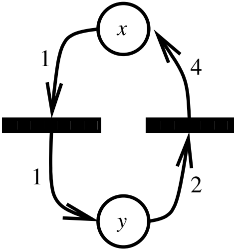
Instead of:



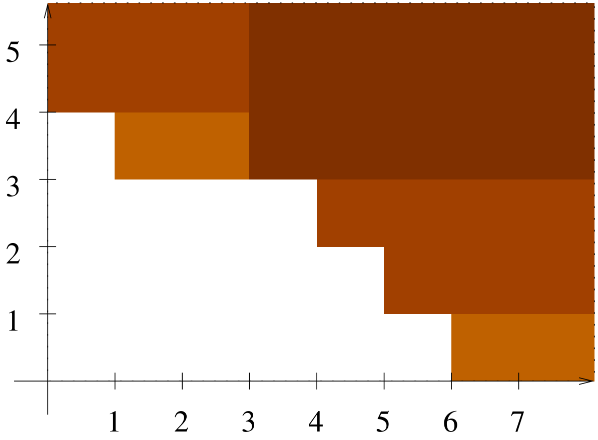


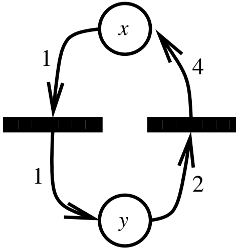
Instead of:



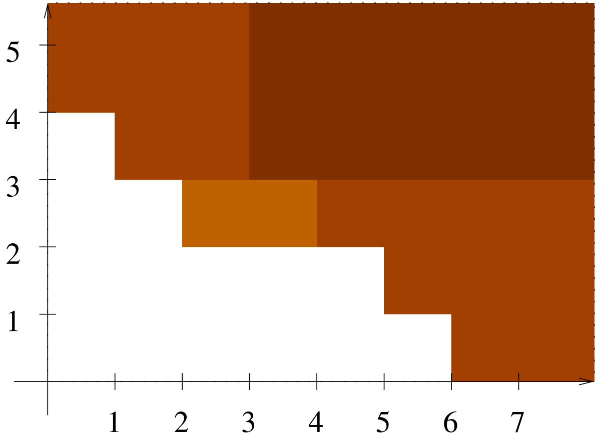


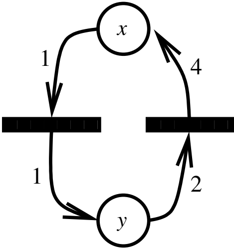
Instead of:



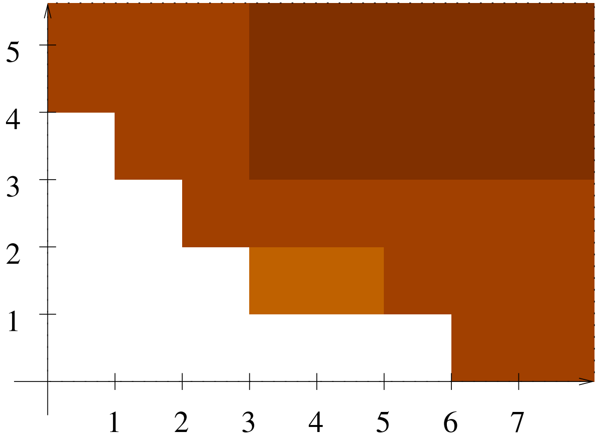


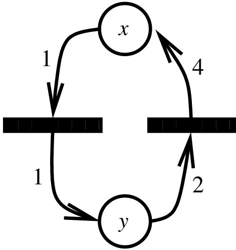
Instead of:



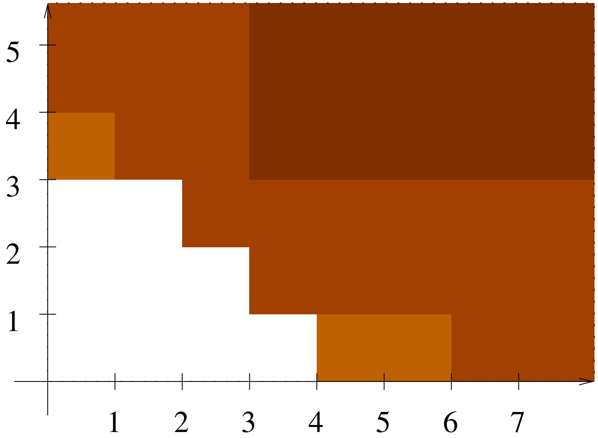


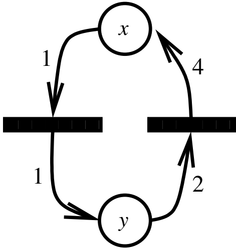
Instead of:



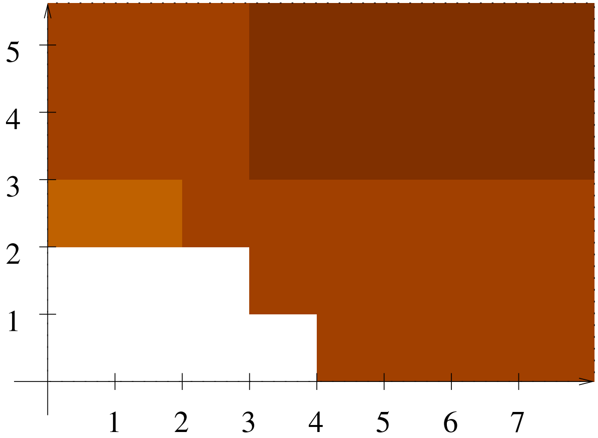


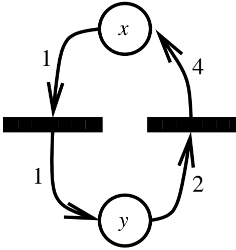
Instead of:



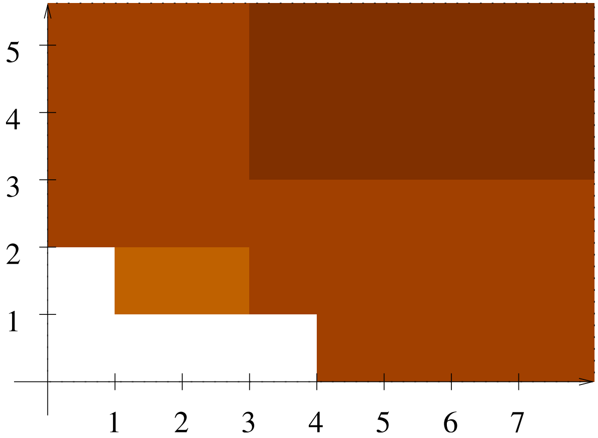


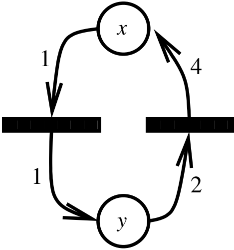
Instead of:



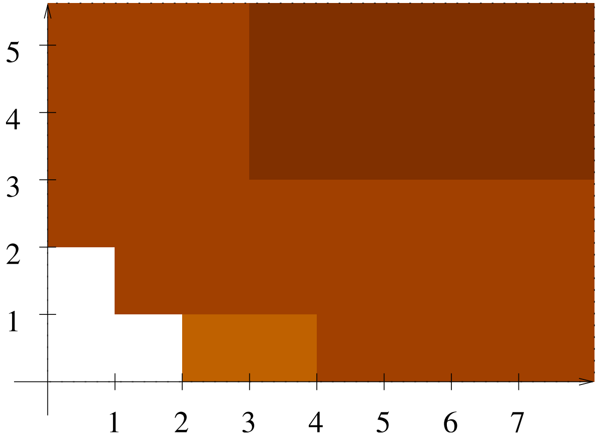


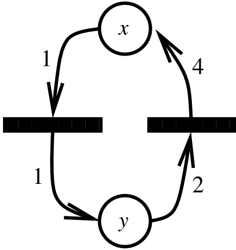
Instead of:



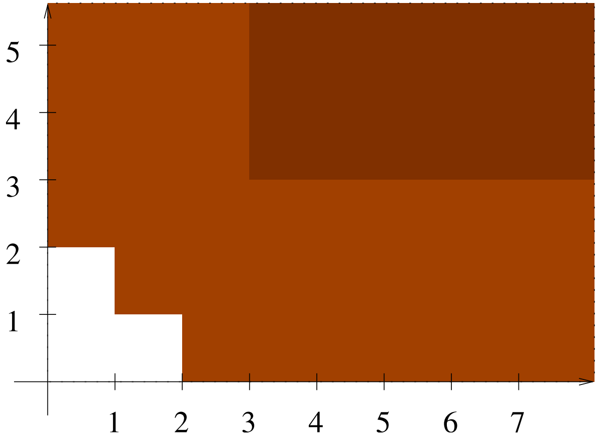


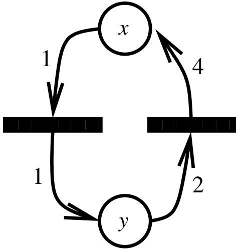
Instead of:



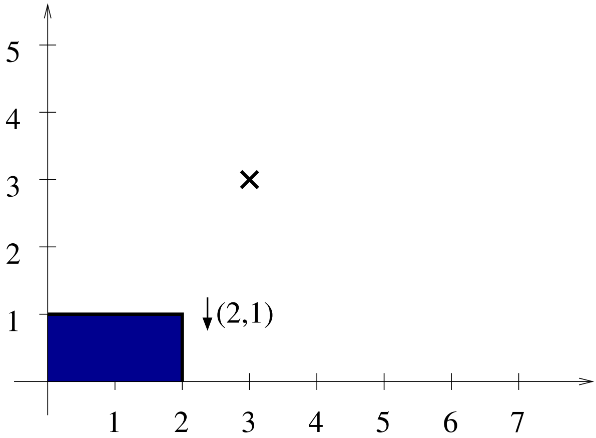


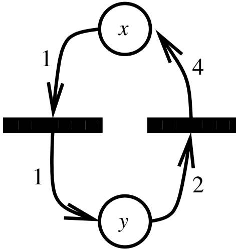
Instead of:



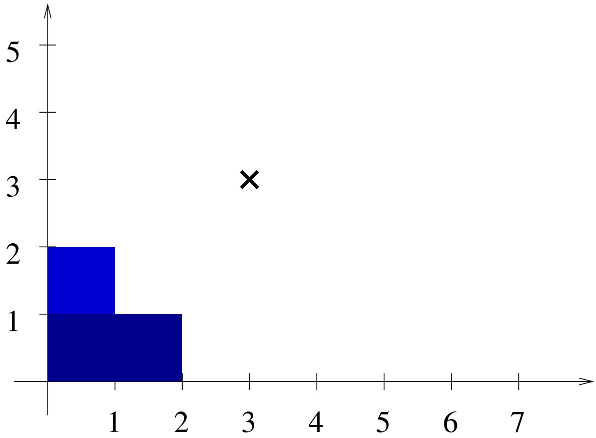


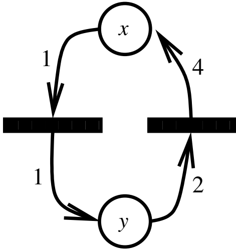
A naive forward algorithm



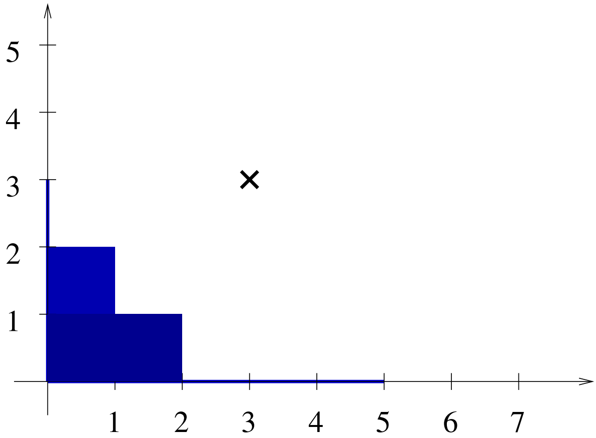


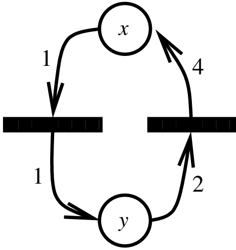
A naive forward algorithm



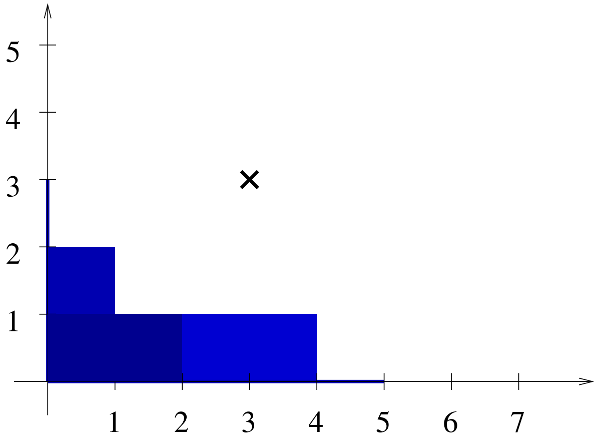


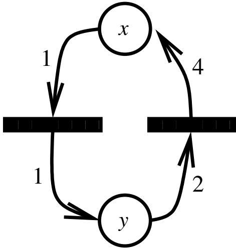
A naive forward algorithm



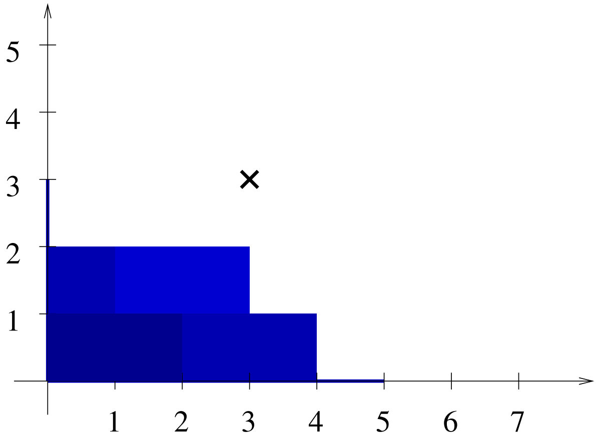


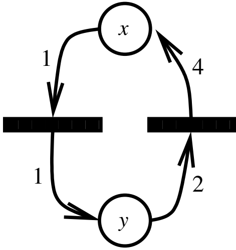
A naive forward algorithm



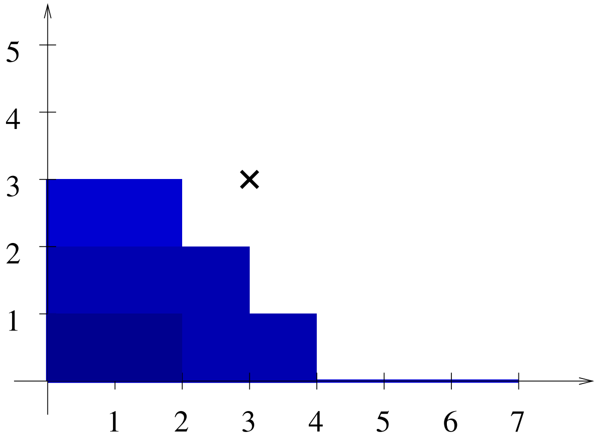


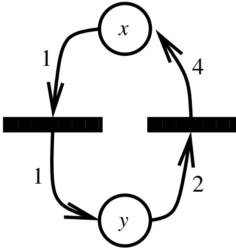
A naive forward algorithm



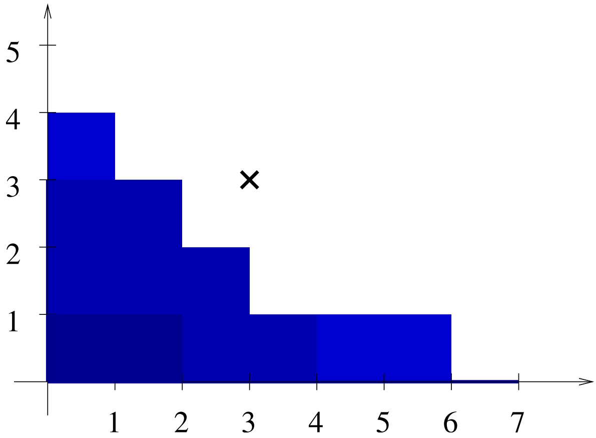


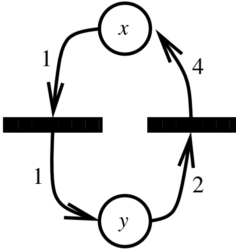
A naive forward algorithm



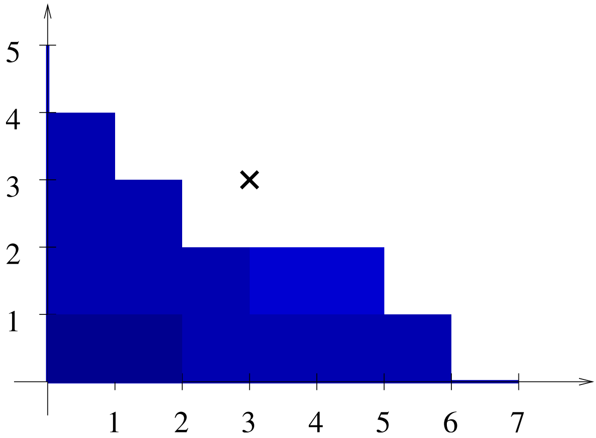


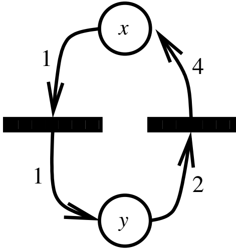
A naive forward algorithm



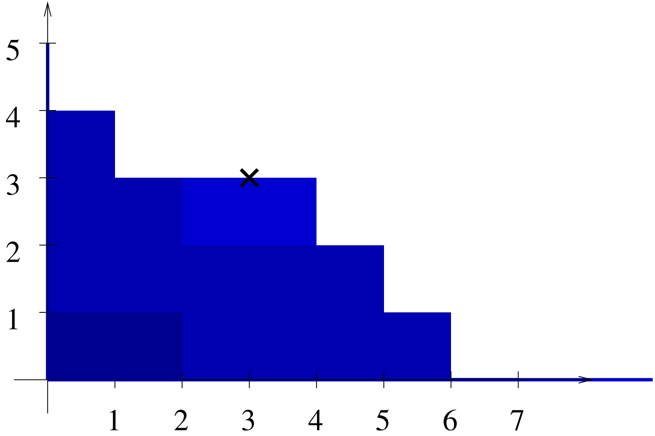


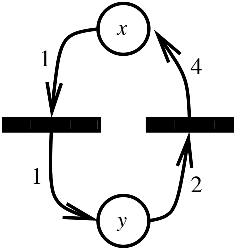
A naive forward algorithm



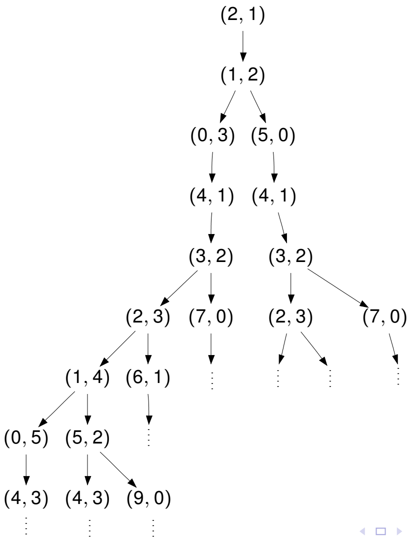


A naive forward algorithm

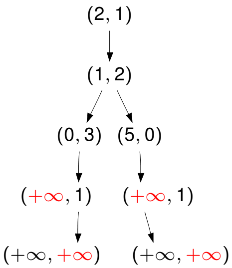




. . . This may fail to terminate



The Karp-Miller construction



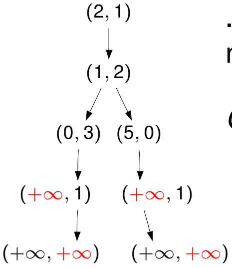
- $(0,3) \rightarrow (4,1) \geq$ ancestor $(2,1) \rightsquigarrow$ accelerate to $(+\infty, 2)$.
- Always terminates (only on [plain] Petri nets).
- Can be used for much more than coverability: boundedness, *U*-boundedness, liveness, etc.

The cover

Definition (Cover)

Let $Post^*(E)$ = set of reachable states from states in E.
The cover of E is $Cover(E) = \downarrow Post^*(E)$.

Note: s covers t iff $s \in Pre^*(\uparrow t)$ iff $t \in Cover\{s\}$.
Note: Karp-Miller computes the cover (exactly):



... as the downward-closure of the finite set of nodes of the tree:

$$Cover\{(2,1)\} = \downarrow\{(2,1),(1,2),(0,3),(5,0),(+\infty,1),(+\infty,1),(+\infty,+\infty),(+\infty,+\infty)\} \cap \mathbb{N}^2$$

Forward procedures

- Until now, we stressed backward algorithms.
  - Always terminates.
  - Decides coverability (reachability for lossy/oblivious systems).

- Design forward procedures for general (topo.) WSTS?
  - A la Karp-Miller [KM69].
  - Would decide boundedness, liveness, etc.
  - Cannot terminate on reset Petri nets [FMcKP04], on LCS [CFPI96] —boundedness undecidable there.

Outline

Adding infinities

We first need to extend state space X (e.g., $\mathbb{N}^k$) to a completion $\widehat{X}$ (e.g., $\mathbb{N}_\omega^k$).

Remember?

In 2005, Alain Finkel asked me:

- The intuitive completion of $\mathbb{N}^k$ is $\mathbb{N}_\omega^k$;
  ... used in Karp-Miller procedure for Petri nets (1969).
- For other well-structured transition systems, what should be the completion of their state space X?
- Is there anything in topology that would define the right notion of completion?

My answer:
No way.

I was wrong: $\widehat{X}$ is the sobrification of X.

Sober spaces

- closed F is *irreducible* iff: $F \subseteq \bigcup_{i=1}^{n} F_i \Rightarrow \exists i \cdot F \subseteq F_i$
- E.g., $\downarrow x$ is irreducible.

Definition

X is sober iff T_0 and the only irreducible closed subsets are $\downarrow x$, $x \in X$.

If F irreducible closed, $F = \downarrow x$ means that $x = \max F$.
E.g., in $\mathbb{N}$, $F = \mathbb{N}$ is missing a largest element.

Sobrification

Idea: add all missing elements... but keep the opens intact.

Definition

The sobrification $\mathcal{S}(X)$ is the space of all irreducible closed subsets of X, with the lower Vietoris topology ($\Diamond U = \{F \mid F \text{ meets } U\}$).

- embed X into $\mathcal{S}(X)$ by $x \mapsto \downarrow x$
- every continuous map $f \colon X \to Y$ (Y sober) has unique continuous extension to $\mathcal{S}(X)$.

The Alexandroff case

In the Alexandroff case (where wqo $\Leftrightarrow$ Noetherian):

Theorem

For any poset X, $\mathcal{S}(X) =$ ideal completion of X.

Closed subsets

Define $x \leq y$ iff $x \in cl(y)$. So $cl(x) = \downarrow x$.

Proposition

The closed subsets F of a sober Noetherian space are the subsets of the form $\downarrow E$, E finite.

Proof. Call F *good* if of the form $\downarrow E$, E finite, *bad* otherwise.

- Assume F bad.
- By #2 and taking complements, can take F *minimal* bad.
- If $F \subseteq \bigcup_{i=1}^{n} F_i$, but $F \subseteq F_i$ for no i, $F \cap F_i$ is good (minimality), so $F \cap F_i = \downarrow E_i$, so $F = \downarrow \bigcup_i E_i$ is good: contradiction.
- So F is irreducible. Sobriety implies $F = \downarrow x$, contradicting badness. □

Sobrification preserves Noetherianness

Theorem

X is Noetherian $\Leftrightarrow \mathcal{S}(X)$ is Noetherian.

Proof. Isomorphic lattices of opens. Characterization #2 shows that Noetherianness only depends on lattice of opens. □

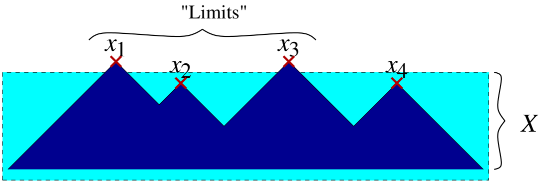
The fundamental theorem

Define completion of X as $\widehat{X} = \mathcal{S}(X)$.

Theorem

If X is Noetherian, every closed subset F of X is finitely representable as $\downarrow E \cap X$ for some finite $E \subseteq \widehat{X}$.

Proof. $F = cl(F) \cap X$, and $cl(F) = \downarrow E$. □



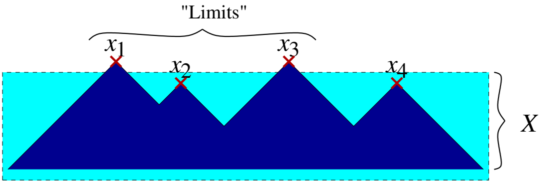
The fundamental theorem

Define completion of X as $\widehat{X} = \mathcal{S}(X)$.

Theorem

If X is wqo, every downward closed subset F of X is finitely representable as $\downarrow E \cap X$ for some finite $E \subseteq \widehat{X}$.

Proof. $F = cl(F) \cap X$, and $cl(F) = \downarrow E$. □



Outline

Computable completions

That every (downward-)closed can be finitely represented is:

- **necessary** to be able to compute on such sets;
  ...(Karp-Miller computes downward-closure of set of reachable states.)
- but not enough: we now show that $\widehat{X}$ is **computable**.

Theorem

For all the Noetherian datatypes given earlier, the quasi-ordering $\widehat{\leq}$ on $\widehat{X}$ is decidable. $\cup$, $\cap$, ascending unions are computable.

Completions: 1. $D = \mathbb{N}^k$

$\widehat{D}$ is the expected thing (remember Petri nets):

- Add a new limit element $+\infty$:

$$\widehat{\mathbb{N}^k} = (\mathbb{N} \cup \{+\infty\})^k$$

- Elements of $\widehat{\mathbb{N}^k}$, example: $(2, +\infty, 3, +\infty)$, represents $\mathbb{N}^k \cap \downarrow(2, +\infty, 3, +\infty) = \{(m, n, p, q) \mid m \leq 2 \wedge p \leq 3\}$.
- Applies to the more general class of k-counter systems.

Completions: 2. $D = D_1^*$

- $D = \{$words over a possibly infinite alphabet $D_1\}$.
- $\widehat{D}$ is a domain of regular expressions called word products:

$$P ::= \epsilon \quad | \quad d^? P \quad | \quad (d_1 \mid \ldots \mid d_n)^* P$$

where:

- $\downarrow_D d^? =$ words with at most one letter $\leq d \in \widehat{D}_1$;
- $\downarrow_D (d_1 \mid \ldots \mid d_n)^* =$ words whose letters are in $\downarrow_{D_1} d_1 \cup \ldots \cup \downarrow_{D_1} d_n$.

Completions: 2. $D = D_1^*$ (cont'd)

Deciding $\widehat{\leq}$ on $D = D_1^*$

$\widehat{\leq}$ on $\widehat{D}$ is P-time computable (with oracle $\widehat{\leq}_1$ on $\widehat{D}_1$). On atoms:

$$
\begin{array}{rll}
d^? \,\widehat{\leq}\, d'^? & \text{iff} & d \,\widehat{\leq}_1\, d' \\
d^? \,\widehat{\leq}\, (d_1 \mid \ldots \mid d_n)^* & \text{iff} & d \,\widehat{\leq}_1\, d_j \text{ for some } j \\
(d_1 \mid \ldots \mid d_m)^* \,\widehat{\not\leq}\, d^? & & \\
(d_1 \mid \ldots \mid d_m)^? \,\widehat{\leq}\, (d'_1 \mid \ldots \mid d'_n)^* & \text{iff} & \forall i \cdot \exists j \cdot d_i \,\widehat{\leq}_1\, d'_j
\end{array}
$$

On products, $AP \,\widehat{\leq}\, A'P'$ iff:

- $A \,\widehat{\not\leq}\, A'$ and $AP \,\widehat{\leq}\, P'$,
- or $A = d^?$, $A' = d'^?$, $d \,\widehat{\leq}_1\, d'$ and $P \,\widehat{\leq}\, P'$,
- or A' is starred, $A \,\widehat{\leq}\, A'$ and $P \,\widehat{\leq}\, A'P'$.

Completions: 2. $D = D_1^*$ (end)

Generalizes:

- the simple regular expressions [ABJ98], which were defined on a finite alphabet: $D = A^*$.
- the word language generators [ADMN04], i.e., simple regular expressions over an alphabet of multiset language generators $D = (A^{\circledast})^*$.

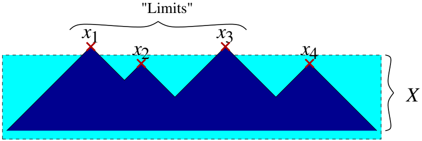
Completions: 5. $D = \mathbb{P}(D_1)$

(*: *outside theory of wqos.*)

- $\widehat{D}$ is the Hoare powerdomain $\mathcal{H}(D_1)$.
- By the Fundamental Theorem, elements of $\widehat{D}$ are:

$$P ::= \downarrow\{P_1, \ldots, P_n\} \qquad \text{(finite)}$$

where $P_1, \ldots, P_n \in \widehat{D}_1$.



Completions: 6. $D = \mathbb{C}^k$ (Zariski Topology)

(*: *outside theory of wqos.*)

- $\widehat{D} = \mathrm{Spec}(\mathbb{Q}[X_1, \ldots, X_k])$ (spectrum).
- Elements described by Gröbner bases.

$$X_1^3 - 3X_1X_2^2 \qquad X_1X_2^2X_3 + 4X^3 + 27$$
$$X_2X_3^2 + 8X_2X_3 + 5X_1 - 1 \qquad X_3^4 - 81$$

Outline

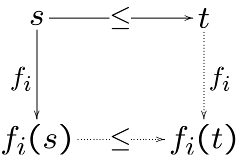
Functional WSTS

A (functional, strongly monotonic here) WSTS is $(X, (f_i)_{i=1}^n)$ where:

- X is wqo.
- $f_i : X \to X$, $1 \le i \le n$, are partial monotonic functions called the transitions.

Partial monotonicity means:

- $\mathrm{dom}\, f_i$ is upward-closed;
- if $s \in \mathrm{dom}\, f_i$ and $s \le t$ then $f_i(s) \le f_i(t)$.



Functional WSTS

A (functional, strongly monotonic here) WSTS is $(X, (f_i)_{i=1}^n)$ where:

- X is Noetherian.
- $f_i : X \to X$, $1 \leq i \leq n$, are partial continuous functions called the transitions.

Partial continuity means:

- $\mathrm{dom}\, f_i$ is open;
- $\forall U$ open, $f_i^{-1}(U)$ open.

Completions of Functional WSTS

X can be completed to $\widehat{X}$. There is also a canonical way to extend partial continuous maps to $\widehat{X}$:

Definition ($\mathcal{S}f$)

For every partial continuous $f : X \to X$, let $\mathcal{S}f : \widehat{X} \to \widehat{X}$ be defined by:

- $\mathrm{dom}\, \mathcal{S}f = \{C \in \widehat{S} \mid C \cap \mathrm{dom}\, f \neq \emptyset\}$;
- $\mathcal{S}f(C) = cl(f\langle C \rangle)$.

Completions of Functional WSTS (cont'd)

X embeds into $\widehat{X}$ through $\eta : s \mapsto \downarrow s$.

Lemma

For every partial continuous $f : X \to X$, $\mathcal{S}f$ is partial continuous, and extends f:

$$\begin{array}{ccc} X & \xrightarrow{\ \eta\ } & \widehat{X} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \mathcal{S}f} \\ X & \xrightarrow{\ \eta\ } & \widehat{X} \end{array}$$

$\mathcal{S}f$ is in fact the *only* continuous extension of f to $\widehat{X}$:
$\mathcal{S}f(\sup_i^{\uparrow} s_i) = \sup_i^{\uparrow} f(s_i)$.

Completions of functional WSTS (cont'd)

A canonical way to complete a whole WSTS:

Definition (Completion of a Topological WSTS)

For every functional topological WSTS $\mathfrak{X} = (X, (f_i)_{i=1}^n)$, the *completion* $\widehat{\mathfrak{X}}$ is $(\widehat{X}, (\mathcal{S} f_i)_{i=1}^n)$.

However, $\widehat{\mathfrak{X}}$ may fail to be a WSTS, even when $\mathfrak{X}$ is
…because $\widehat{\leq}$ may fail to be wqo.
… Repair by requiring X ω^2-wqo [FGL, ICALP'09],

Completions of functional WSTS (cont'd)

A canonical way to complete a whole WSTS:

Definition (Completion of a Topological WSTS)

For every functional topological WSTS $\mathfrak{X} = (X, (f_i)_{i=1}^n)$, the *completion* $\widehat{\mathfrak{X}}$ is $(\widehat{X}, (\mathcal{S} f_i)_{i=1}^n)$.

However, $\widehat{\mathfrak{X}}$ may fail to be a WSTS, even when $\mathfrak{X}$ is
…because $\widehat{\leq}$ may fail to be wqo.
… Repair by requiring X ω^2-wqo [FGL, ICALP'09], or don't repair:

Proposition

If $\mathfrak{X}$ is a topological WSTS, then so is $\widehat{\mathfrak{X}}$.

Proof. Because $\widehat{X} = \mathcal{S}(X)$ Noetherian iff X Noetherian. □

Outline

A simple, conceptual Karp-Miller procedure

- An analogue of Karp-Miller, computing $\mathit{Cover}(s) = \downarrow \mathit{Post}^*\{s\}$.
- We must first define lub-accelerations.

Definition (Lub-acceleration f^∞)

Let X be a dcpo, $f : X \to X$ partial continuous.

- $\mathrm{dom}\, f^\infty = \mathrm{dom}\, f$;
- $f^\infty(x) = \begin{cases} \sup_{n\in\mathbb{N}} f^n(x) & \text{if } x < f(x) \\ f(x) & \text{else} \end{cases}$

I.e., accelerate only if $x < f(x)$.

A simple, conceptual Karp-Miller procedure

- An analogue of Karp-Miller, computing $Cover(s) =$ ~~$\downarrow Post^*\{s\}$~~ $cl(Post^*\{s\})$.
  ... so that the concept generalizes to all topological WSTS (no other modification.)
- We must first define lub-accelerations.

Definition (Lub-acceleration f^∞)

Let X be a dcpo, $f : X \to X$ partial continuous.

- $\mathrm{dom}\, f^\infty = \mathrm{dom}\, f$;
- $f^\infty(x) = \begin{cases} \sup_{n\in\mathbb{N}} f^n(x) & \text{if } x < f(x) \\ f(x) & \text{else} \end{cases}$

I.e., accelerate only if $x < f(x)$.

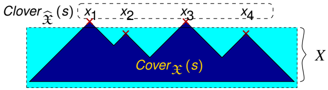
A Simple, Conceptual Karp-Miller Procedure (cont'd)

Let $\mathfrak{X} = (X, G = (g_i)_{i=1}^n)$ be an effective (top.) WSTS.

Procedure Clover$_{\widehat{\mathfrak{X}}}(s_0)$:
1. $A \leftarrow \{s_0\}$; `(* A finite subset of completion *)`
2. **while** $Post_{\mathfrak{S}}(A) \not\sqsubseteq A$ **do**
   (a) Choose fairly $(g, a) \in \mathcal{S}G^* \times A$ such that $a \in \mathrm{dom}\, g$;
   (b) $A \leftarrow A \cup \{g^\infty(a)\}$;
3. **return** $\mathrm{Max}\, A$;

Theorem (Clover)

If **Clover**$_{\widehat{\mathfrak{X}}}(s_0)$ *terminates, then it computes the* clover *Clover*$_{\widehat{\mathfrak{X}}}(s_0) = \{$*max elements of Cover*$_{\mathfrak{X}}(s_0)\}$.



Outline

Conclusion

- Noetherian spaces: a natural topological extension of wqos
- The standard™ backward algorithm still terminates
- A rich collection of Noetherian datatypes
- The right intuitions for forward procedures [FGL, ICALP'09]—and clovers, a finite representation of (downward-)closures of reachable states [FGL, STACS'09]
- Other things: Noetherian spaces are spectral, exact characterization of sober Noetherian spaces, Stone duals, the VJGL lemma, . . .
- Open: extending Robertson-Seymour XX? analogues of bqos?

Additional Notes

Not presented live.

- On a remark by Max Dickmann, asked after the talk.
- On another remark made to me after the talk.
- On a question by Paul-André Melliès, asked after the talk.
- On a question by Mai Gehrke, asked after the talk.
- What sober Noetherian spaces really are (not part of the talk.)

Max Dickmann’s remark

Max Dickmann made the observation that a lot of properties I presented of Noetherian spaces are well-known (e.g., characterizations #0 through #4, from what I understood; the *fundamental theorem* as well).
This should also appear in a forthcoming book of his on spectral spaces.

Another remark

I have said that proving that the product of two Noetherian spaces was Noetherian is tricky.
A participant told me that there was a more elementary proof than the one I presented, see `http://matheuscmss.wordpress.com/2012/03/01/spcs-8/`, Proposition 4.

Paul-André Melliès' question

Paul-André Melliès observed that the proof of the topological Higman lemma is incredibly close to the classical proof of Higman's Lemma.
He asked whether that could be generalized to some form of topological Ramsey theory.
I don't know the answer to this question (yet).

Mai Gehrke's question

I said that there were Noetherian spaces that did not arise from wqos, where I meant that the underlying quasi-ordering was no wqo.

Mai Gehrke asked whether this was still true, even by wildly changing the underlying space of points, but keeping the same opens (up to iso).

The answer is no, as found by Yann Péquignot: take $\mathbb{N}$ with the cofinite topology. This is Noetherian, and its sobrification is itself plus a fresh top element. Any wqo with the same opens would embed in the latter, but could only include only finitely many points from $\mathbb{N}$ (an infinite antichain); so would only have finitely many opens.

Sober Noetherian spaces

Lemma

Every sober Noetherian space X is spectral.

I.e.,

- sober (by assumption)
- compact-opens form a base (of course)
- compact-opens closed under intersection (obvious)
- compact (X is open)

Can now import theory of spectral spaces (Hochster, 1969). E.g., dual X^{d} (X with basis of complements of compact-opens of X) is spectral, and $X^{\mathrm{dd}} = X$.

Sober Noetherian spaces

Theorem

The sober Noetherian spaces are the posets $(X, \leq)$ *with:*

- $\leq$ *well-founded*
- *(T)* $X = \downarrow E$ *for some finite set* E
- *(W)* $\downarrow x \cap \downarrow y = \downarrow E_{xy}$ *for some finite set* E_{xy}

with the upper topology ($\downarrow x$ *subbasis of closed sets).*

Proof. ($\Rightarrow$) Take $\leq$ specialization ordering. Well-founded since $(x_n)_{n \in \mathbb{N}}$ descending $\Rightarrow$ $(\complement \downarrow x_n)_{n \in \mathbb{N}}$ ascending seq. of opens (#2).
X^{d} has (open) basis consisting of all closed subsets of X.
The unions of closed subsets are the down closed subsets: if A down-closed, then $A = \bigcup_{x \in A} \downarrow x$.
So topology of X^{d} is Alexandroff top. of $\geq$.
The sat. compacts of X^{d} are of the form $\uparrow_{\geq} E = \downarrow E$, E finite $\Rightarrow$ (T), (W).
By duality, the closed subsets of X^{d} are the sat. compacts of X^{d}, i.e., finite unions of $\downarrow x$ $\Rightarrow$ topology of X is upper.

Sober Noetherian spaces

Theorem

The sober Noetherian spaces are the posets $(X, \leq)$ *with:*

- $\leq$ *well-founded*
- *(T)* $X = \downarrow E$ *for some finite set* E
- *(W)* $\downarrow x \cap \downarrow y = \downarrow E_{xy}$ *for some finite set* E_{xy}

with the upper topology ($\downarrow x$ *subbasis of closed sets).*

Proof. ($\Leftarrow$) First show that any sequence $\downarrow E_0 \supseteq \downarrow E_1 \supseteq \ldots \supseteq \downarrow E_n \supseteq \ldots$ stabilizes (E_n finite).
So upper topology is Noetherian, by #2.

And closed subsets must be $\downarrow E$, E finite. Sobriety follows.