Noetherian Spaces

Jean Goubault-Larrecq
LSV, ENS Cachan

CCC’14, September 18, 2014

9 Stably compact spaces and compact pospaces 397
  9.1 Stably locally compact spaces, stably compact spaces 397
  9.2 Coproducts and retracts of stably compact spaces 411
  9.3 Products and subspaces of stably compact spaces 413
  9.4 Patch-continuous, perfect maps 419
  9.5 Spectral spaces 423
  9.6 Bifinite domains 440
  9.7 Noetherian spaces 453
Noetherian Spaces

Outline

1 Introduction
2 Algebraic Geometry 101
3 Verification of Infinite-State Systems
   ▪ Wqos
   ▪ WSTS
4 Noetherian Spaces as Generalized Wqos
   ▪ From Wqos to Noetherian Spaces
   ▪ Case Study: LCPPs
5 The Mathematics of Noetherian Spaces
6 Computing with Noetherian Spaces
   ▪ Computable Bases
   ▪ S-representations
7 Conclusion
Objective of This Talk

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

Definition

A topological space $X$ is **Noetherian** iff every open subset is compact.

- Arises naturally in algebraic geometry (mathematics)
- Also in verification (computer science)
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
An algebraic variety in $\mathbb{C}^n$ is the set of common zeroes of a family $F$ of polynomials in $\mathbb{C}[X_1, \cdots, X_n]$.

Example:

$$F = \{X_1^2 + X_1 X_2 + X_2^2 - 4, X_1^3 + 2X_1^2 - X_1 X_2^2 - 1, X_1^2 X_2^2 - 4X_1 X_2^2 + 3X_1 X_2 + 5\}$$

Note: the ideal $\langle F \rangle$ generated by $F$ has exactly the same common zeroes.
An **algebraic variety** in $\mathbb{C}^n$ is the set $\mathbb{Z}(I)$ of common zeroes of a polynomial ideal $I$ in $\mathbb{C}[X_1, \cdots, X_n]$.

**Special case:** every point $(a_1, \cdots, a_n)$ defines an algebraic variety:

$$\{(a_1, \cdots, a_n)\} = \mathbb{Z}\langle X_1 - a_1, \cdots, X_n - a_n \rangle$$
Prime Ideals

An **algebraic variety** in $\mathbb{C}^n$ is the set $\mathbb{Z}(I)$ of common zeroes of a polynomial ideal $I$ in $\mathbb{C}[X_1, \cdots, X_n]$.

**Special case:** every point $(a_1, \cdots, a_n)$ defines an algebraic variety:

$$\{(a_1, \cdots, a_n)\} = \mathbb{Z}(X_1 - a_1, \cdots, X_n - a_n)$$

**Note:** $I = \langle X_1 - a_1, \cdots, X_n - a_n \rangle$ is a prime ideal, meaning that $1 \notin I$ and $PQ \in I \Rightarrow P \in I \lor Q \in I$. 
Radical Ideals

An algebraic variety in $\mathbb{C}^n$ is the set $\mathbb{Z}(I)$ of common zeroes of a polynomial ideal $I$ in $\mathbb{C}[X_1, \cdots, X_n]$.

Conversely, the ideal $\mathcal{I}(E)$ of all polynomials $P$ that vanish at every point of $E$ is radical: if $P^n \in \mathcal{I}(E)$ then $P \in \mathcal{I}(E)$.

**Note:** The radical $\sqrt{I}$ of an ideal $I$ is $\{P \mid \exists n \geq 1, P^n \in I\}$. $\sqrt{I}$ is a radical ideal.

$I$ is radical iff $I = \sqrt{I}$. 
Replace the study of algebraic varieties \( \mathcal{Z}(I) = \{ \vec{a} \in \mathbb{C}^n \mid \forall P \in I, P(\vec{a}) = 0 \} \)

by the study of (radical) ideals \( I \) in the polynomial ring \( \mathbb{C}[X_1, \cdots, X_n] \).

**Theorem (Hilbert’s Nullstellensatz)**

*For every radical ideal \( I \), the set of polynomials \( P \) that vanish at every element of \( \mathcal{Z}(I) \) is exactly \( I \).*

(More generally, \( \mathfrak{J}(\mathcal{Z}(I)) = \sqrt{I} \).)
Replace the study of algebraic varieties $\mathcal{Z}(I) = \{ \vec{a} \in \mathbb{C}^n \mid \forall P \in I, P(\vec{a}) = 0 \}$ by the study of (radical) ideals $I$ in the polynomial ring $\mathbb{C}[X_1, \cdots, X_n]$.

**Definition**

The **spectrum** of a ring $R$ is its set of prime ideals.

$\Rightarrow$ recovers the points of $\mathbb{C}^n$ (and some more; here $(X_2^2 - X_1^3 - X_1^2)$).
The Zariski Topology

Let $R$ be a commutative ring. For every (radical) ideal $I$, let

$$F_I = \{ p \text{ prime ideal} \mid I \subseteq p \}$$

- $\bigcap_{j \in J} F_{I_j} = F_{\sum_{j \in J} I_j}$ where $\sum_{j \in J} I_j = \langle \bigcup_{j \in J} I_j \rangle$
- $\bigcup_{j=1}^n F_{I_j} = F_{\bigcap_{j=1}^n I_j}$

**Definition**

The sets $F_I$ form the closed sets for a topology on $\text{Spec}(R)$ called the **Zariski topology**.

**Note:** Since $\mathbb{C}^n$ embeds into $\text{Spec}(\mathbb{C}[X_1, \cdots, X_n])$, induces a topology (again called Zariski) with closed sets $F_I = \mathcal{Z}(I)$. 
The Zariski Topology

Let $R$ be a commutative ring. For every (radical) ideal $I$, let

$$F_I = \{ p \text{ prime ideal} \mid I \subseteq p \}$$

**Theorem**

*If $R$ is a Noetherian ring (monotone chains $I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots$ stabilize), then $\text{Spec}(R)$ is Noetherian.*

**Proof.** $F_I \subseteq F_J$ iff $\sqrt{J} \subseteq \sqrt{I}$.

- Any antitone chain of closed sets $F_{I_1} \supseteq \cdots \supseteq F_{I_k} \supseteq \cdots$ induces a monotone chain $\sqrt{I_1} \subseteq \cdots \subseteq \sqrt{I_k} \subseteq \cdots$, hence must stabilize.
- Equivalently, any monotone chain of opens $U_1 \subseteq \cdots \subseteq U_k \subseteq \cdots$ stabilizes.
- If there were a non-compact open $U$, 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. Impossible. So $\text{Spec}(R)$ Noetherian.
The Zariski Topology

Let $R$ be a commutative ring.
For every (radical) ideal $I$, let

$$F_I = \{ p \text{ prime ideal} \mid I \subseteq p \}$$

$\mathbb{C}[X_1, \cdots, X_n]$ is a Noetherian ring, hence:

**Corollary**

$\text{Spec}(\mathbb{C}[X_1, \cdots, X_n])$ is Noetherian.
$\mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$ are Noetherian in their Zariski topology.
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Dickson’s Lemma

Lemma (Dickson 1913)

Every infinite sequence $\vec{x}_0, \vec{x}_1, \cdots, \vec{x}_n, \cdots$ in $\mathbb{N}^k$ ($k$ fixed) has an infinite **monotonic** subsequence $\vec{x}_{i_0} \leq \vec{x}_{i_1} \leq \cdots \leq \vec{x}_{i_m} \leq \cdots$ ($i_0 < i_1 < \cdots < i_m < \cdots$)

Proof. Induction on $k$. Write $\vec{x}_n$ as

\[
\begin{bmatrix}
  x_{n0} \\
  x_{n1} \\
  \vdots \\
  x_{nk}
\end{bmatrix}.
\]

- By i.h., can assume

\[
\begin{bmatrix}
  x_{00} \\
  x_{01} \\
  \vdots \\
  x_{0k}
\end{bmatrix}, \begin{bmatrix}
  x_{10} \\
  x_{11} \\
  \vdots \\
  x_{1k}
\end{bmatrix}, \cdots, \begin{bmatrix}
  x_{m0} \\
  x_{m1} \\
  \vdots \\
  x_{mk}
\end{bmatrix}, \cdots \text{ monotonic}
\]

- Find $i_0$ with $x_{0i_0}$ minimal
- Find $i_1$ with $x_{0i_1}$ minimal among elements to the right of $x_{0i_0}$
- Etc.
Lemma (Dickson 1913)

For every $k$, $(\mathbb{N}^k, \leq)$ is a wqo.

Definition (Wqo)

A wqo (well-quasi-order) is a quasi-order $(X, \leq)$ in which every infinite sequence has an infinite monotonic subsequence.

Equivalently:
- every sequence $(x_n)_{n \in \mathbb{N}}$ is good: $x_i \leq x_j$ for some $i < j$
- $\leq$ is well-founded and has no infinite antichain
The Rich Theory of Wqos

- Many other examples:
  - word embedding [Higman52]
  - tree embedding [Kruskal60]
  - graph minor [RobertsonSeymour04]
  etc.

- **Theorem:** Every ideal in $\mathbb{K}[X_1, \ldots, X_n]$ is **finitely generated** (follows from Dickson)

- **Theorem:** Coverability in Petri nets is **decidable**
  (in general, in any effective WSTS)

- An ever growing number of applications.
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
A widely used formalism for specifying concurrent systems:

- **State space** $\mathbb{N}^k$  
  
- **Transitions**: $\vec{x} \rightarrow \vec{x} + \vec{\delta}$ provided $\vec{x} + \vec{\delta} \geq 0$

(e.g., $b : \vec{x} \rightarrow \vec{x} + (1, -1, 0, 0, -1, 1, 0, 0, -1, 1, 0, 0)$)
Well-Structured Transition Systems

By Dickson, one sees that Petri nets are WSTS [F87,FS01,AJ93,ACJY96]:

**Definition (WSTS)**

A WSTS on a set of states $X$ is given by:

- A transition relation $\delta \subseteq X \times X$;
- A wqo $\leq$ on $X$;
- + (strong) monotonicity:

```
\begin{align*}
  \delta & \downarrow \\
  x \xrightarrow{\leq} x' \\
  \delta & \downarrow \\
  y \xrightarrow{\leq} y'
\end{align*}
```

Many other examples: affine programs [FMcKP04], lossy channel systems [ACJY96], data nets [LNORW07], (quotients of) timed Petri nets [ACBJ04], various process algebras [BA09,WZH10], etc.
The Theory of WSTS

Problem (Coverability)

Given \( s, t \in X \), is there a path \( s \xrightarrow{\delta} \xrightarrow{\delta} \cdots \xrightarrow{\delta} t \)?

For \( U \subseteq X \), let

\[
\text{Pre}(U) = \{ x \in X \mid \exists y \in U, x \xrightarrow{\delta} y \}
\]

\[
\text{Pre}^*(U) = \{ x \in X \mid \exists y \in U, x \xrightarrow{\delta} \xrightarrow{\delta} \cdots \xrightarrow{\delta} y \}
\]
The Theory of WSTS

Problem (Coverability)

Given \( s, t \in X \), is there a path \( s \xrightarrow{\delta} \cdots \xrightarrow{\delta} \geq t \)?

For \( U \subseteq X \), let

\[
Pre(U) = \{ x \in X \mid \exists y \in U, x \xrightarrow{\delta} y \}
\]

\[
Pre^*(U) = \{ x \in X \mid \exists y \in U, x \xrightarrow{\delta} \cdots \xrightarrow{\delta} y \}
\]

Note: Under monotonicity, if \( U \) is upward closed,
then \( Pre(U), Pre^*(U) \) are upward closed.
The Theory of WSTS

Problem (Coverability)

Given $s, t \in X$, is there a path $s \xrightarrow{\delta} \cdots \xrightarrow{\delta} \geq t$?

For $U \subseteq X$, let

$$Pre(U) = \{x \in X \mid \exists y \in U, x \xrightarrow{\delta} y\}$$

$$Pre^*(U) = \{x \in X \mid \exists y \in U, x \xrightarrow{\delta} \cdots \xrightarrow{\delta} y\}$$

**Note:** Under monotonicity, if $U$ is upward closed, then $Pre(U)$, $Pre^*(U)$ are upward closed.

Theorem (Finkel-Schnoebelen, Abdulla 1990s)

*Coverability is decidable in effective WSTS.*

**Proof.** Let $U = \uparrow t$. Compute $Pre^*(U) = \bigcup_{n \in \mathbb{N}} Pre^{\leq n}(U)$.

Must stabilize (why?).

Then test $s \in Pre^*(U)$. 


Lemma

In a wqo, every upward-closed $U$ is of the form $\uparrow E$, $E$ finite.

Proof. Let $E = \{\text{minimal elements of } U\}$. Every $x \in U$ is above some element in $E$, since $\leq$ well-founded.

$E$ is an antichain, hence must be finite.

Lemma

In a wqo, every chain $U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n \subseteq \cdots$ of upward-closed subsets stabilizes.

Proof. $U = \bigcup_n U_n$ is upward-closed, hence of the form $\uparrow E$, $E$ finite.

For each $x \in E$, find $n_x$ s.t. $x \in U_{n_x}$.

Let $n = \max_{x \in E} n_x$. $U = \uparrow E \subseteq U_n$, hence $U_n = U_{n+1} = \cdots = U$.

Apply this to $U_n = Pre^{\leq n}(U)$ to finish proof of decidability.
Hence coverability is decidable in Petri nets (already mentioned), but also:

**Theorem (Abdulla-Jonsson93)**

Reachability is decidable in lossy channel systems.

(Undec. if non-lossy.)

**Proof.**

- State space $Q_1 \times Q_2 \times \Sigma^* \times \Sigma^*$
- $\Sigma^*$ with word embedding is wqo [Higman52]
- Transitions $!a$ (send $a$), $?a$ (receive $a$) + “spontaneously lose letters” are monotonic
- So coverability is decidable
- But coverability=reachability since lossy.
1 Introduction
2 Algebraic Geometry 101
3 Verification of Infinite-State Systems
   - Wqos
   - WSTS
4 Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5 The Mathematics of Noetherian Spaces
6 Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7 Conclusion
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Alexandroff Topologies

The upward closed subsets are the opens of a topology, called the **Alexandroff topology**.
A Noetherian space is one where opens are compact.

**Lemma**

\((X, \leq)\) is wqo iff its Alexandroff topology is Noetherian.

**Proof.**

(\(\Rightarrow\)) If \(U\) were open, non-compact
hence has an infinite open cover \((V_n)_n\) with no finite subcover.
\(V_0 \subset (V_0 \cup V_1) \subset (V_0 \cup V_1 \cup V_2) \subset \cdots\) would contradict previous lemma.

(\(\Leftarrow\)) Consider \(x_0, x_1, \ldots, x_n \ldots\).
The sequence \(U_n = \uparrow\{x_0, x_1, \ldots, x_n\}\) stabilizes, say at \(j\):
\(x_j \in U_{j-1}\), so \(x_i \leq x_j\) for some \(i < j\). \(\square\)
Topological WSTS

**Definition**

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

Generalizes WSTS=special case where \(X\) is Alexandroff.

**Theorem**

*On effective topological WSTS, reachability of open subsets is decidable.*

**Proof.** \(s \overset{\delta}{\rightarrow} \overset{\delta}{\rightarrow} \cdots \overset{\delta}{\rightarrow} U\) iff \(s \in Pre^*(U)\).

Compute \(Pre^*(U) = \bigcup_n Pre^{\leq n}(U)\).

Stabilizes because \(Pre^*(U)\) open hence compact, and \((Pre^{\leq n}(U))_n\) open cover.  \(\square\)
Topological WSTS

Definition

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

Generalizes WSTS=special case where \(X\) is Alexandroff.

Theorem

On effective topological WSTS, reachability of open subsets is decidable.

- What is an effective topological WSTS? one where \(\cup, \subseteq\) are computable
- Are there uses of this generalization?
Noetherian Spaces

Noetherian Spaces as Generalized Wqos

Case Study: LCPPs

Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Lossy Concurrent Polynomial Programs

Definition (Lossy Concurrent Polynomial Programs)

Are networks of:

- **polynomial programs** [MOS02] that compute over finitely many variables in \( \mathbb{Q} \) through polynomial operations
- with lossy communication channels [ACJY96] transmitting control signals.
Deciding LCPPs

These are topological WSTS:

- **States:** Current line for program $A$, in $Q_A$ and same for $B$
  - Current values of numerical vars of $A$, in $Q^m$
- **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 + $ drop signals spontaneously.

All are lower semicontinuous.
Deciding LCPPs

while (*) {
    recv (SIG_CALC) \Rightarrow if (*) { x = 2; y = 3; }
    else { x = 3; y = 2; }
    x = x \cdot y - 6; y = 0;
    if (x^2 - 3 \cdot x \cdot y == 0)
        while (*) { x = x + 1; y = y - 1; }
    else send (SIG_FUZZ);
    x = x^2 + x \cdot y;
    | recv (SIG_QUIT) \Rightarrow return;
}

| channel c1
| \rightarrow a \ b \ d \ a \ c
| channel c2
| \rightarrow b \ c

Theorem (JGL10)

Reachability of open sets of states is decidable for LCPPs.
In particular, control-state reachability, and the eventual presence of a signal on a channel, are decidable.

Proof. Recall that reachability of open subsets is decidable in effective topological WSTS. Topology needed to link algebra (polynomial ideals) with order (words).
That result was essentially for free (and improves on several preexisting works), except for:

- **Mathematical** questions:
  - Are products of Noetherian spaces Noetherian? (yes)
    Needed since state space = finite space $\times \Sigma^* \times \text{Zariski}$.
  - What kind of operations preserve being Noetherian?

- **Computer science** questions:
  - How do you represent the opens? (two answers)
  - How do you compute $\cup$, $\subseteq$?
  - How do you compute $\text{Pre}(U)$?
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Equivalent Definitions of Noetherianness

#0 Every open is compact
#1 Every chain of opens stabilizes
#2 $\subset$ is well-founded on closed sets (used earlier)
Equivalent Definitions of Noetherianness

#0 Every open is compact
#1 Every chain of opens stabilizes
#2 $\subset$ is well-founded on closed sets (used earlier)
#3 Every subspace is compact
Equivalent Definitions of Noetherianness

#0 Every open is compact
#1 Every chain of opens stabilizes
#2 $\subseteq$ is well-founded on closed sets (used earlier)
#3 Every subspace is compact
#4 Every net has a self-convergent subnet
Equivalent Definitions of Noetherianness

#0 Every open is compact
#1 Every chain of opens stabilizes
#2 $\subset$ is well-founded on closed sets (used earlier)
#3 Every subspace is compact
#4 Every net has a self-convergent subnet
#5 Every ultrafilter is compact ($\lim \mathcal{U} \in \mathcal{U}$)
Equivalent Definitions of Noetherianness

#0 Every open is compact
#1 Every chain of opens stabilizes
#2 $\subset$ is well-founded on closed sets (used earlier)
#3 Every subspace is compact
#4 Every net has a self-convergent subnet
#5 Every ultrafilter is compact (Lim $\mathcal{U} \in \mathcal{U}$)
#6 Given any basis $\mathcal{B}$ of the topology, every sequence $(U_n)_{n \in \mathbb{N}}$ in $\mathcal{B}$ is good, i.e., $U_n \subseteq \bigcup_{i<n} U_i$. 
Equivalent Definitions of Noetherianness

#0  Every open is compact
#1  Every chain of opens stabilizes
#2  $\subseteq$ is well-founded on closed sets (used earlier)
#3  Every subspace is compact
#4  Every net has a self-convergent subnet
#5  Every ultrafilter is compact ($\text{Lim } \mathcal{U} \in \mathcal{U}$)
#6  Given any basis $\mathcal{B}$ of the topology, every sequence $(U_n)_{n \in \mathbb{N}}$ in $\mathcal{B}$ is good, i.e., $U_n \subseteq \bigcup_{i<n} U_i$.
#7  Its sobrification has the upper topology of a well-founded ordering such that every finite intersection $\bigcap_{i=1}^{n} \downarrow x_i$ can be written as a finite union $\bigcup_{j=1}^{m} \downarrow y_j$. 
A net \((x_n)_n\) is **self-convergent** iff converges to every \(x_n\).

Looks weird, but e.g., every monotonic sequence is self-convergent in an Alexandroff space.
Self-Convergent Nets

**Definition**

A net \((x_n)_n\) is **self-convergent** iff converges to every \(x_n\).

Looks weird, but e.g., every monotonic sequence is self-convergent in an Alexandroff space.

**Theorem (#4)**

*A space \(X\) is Noetherian iff every net has a self-convergent subnet*

Reminder: \(\leq\) wqo iff every sequence has a monotonic subsequence.
Back to Dickson: Finite Products of Noetherian Spaces

$\mathbb{N}^k$ is wqo, hence Noetherian.
Proof really shows that $\mathbb{N}$ is wqo + finite products of wqos are wqo.

Theorem

Finite products of Noetherian spaces are Noetherian.

Show that every net $\vec{x}_0, \vec{x}_1, \cdots, \vec{x}_n, \cdots$ in product space has self-convergent subnet.

Write $\vec{x}_n$ as

$$
\begin{bmatrix}
  x_{n0} \\
  x_{n1} \\
  \vdots \\
  x_{nk}
\end{bmatrix}
$$

- By i.h., can assume
  $$
  \begin{bmatrix}
    x_{00} \\
    x_{01} \\
    \vdots \\
    x_{0k}
  \end{bmatrix},
  \begin{bmatrix}
    x_{10} \\
    x_{11} \\
    \vdots \\
    x_{1k}
  \end{bmatrix},
  \cdots,
  \begin{bmatrix}
    x_{n0} \\
    x_{n1} \\
    \vdots \\
    x_{nk}
  \end{bmatrix},
  \cdots \text{ self-convergent}
  $$

- Extract self-convergent subsequence from first row $x_{00}, x_{10}, \cdots, x_{n0}, \cdots$ and reindex.
Constructions of Noetherian spaces

Until now, we know the following are Noetherian:

- $\text{Spec}(R)$ for Noetherian rings $R$  
  e.g. $\mathbb{R}^n \subseteq \text{Spec}(\mathbb{R}[X_1, \cdots, X_n])$
- Every wqo, Alexandroff topology
- Finite products of Noetherian spaces
Constructions of Noetherian spaces

Until now, we know the following are Noetherian:

- $\text{Spec}(R)$ for Noetherian rings $R$ e.g. $\mathbb{R}^n \subseteq \text{Spec}(\mathbb{R}[X_1, \ldots , X_n])$
- Every wqo, Alexandroff topology
- Finite products of Noetherian spaces

Easy to see that these are, too:

- Subspaces of Noetherian spaces
- Spaces with topology coarser than a Noetherian one
- Finite coproducts of Noetherian spaces
- Continuous images of Noetherian spaces e.g. topol. quotients
Constructions of Noetherian spaces

Until now, we know the following are Noetherian:

- $\text{Spec}(R)$ for Noetherian rings $R$  
  e.g. $\mathbb{R}^n \subseteq \text{Spec}(\mathbb{R}[X_1, \ldots, X_n])$
- Every wqo, Alexandroff topology
- Finite products of Noetherian spaces

Easy to see that these are, too:

- Subspaces of Noetherian spaces
- Spaces with topology coarser than a Noetherian one
- Finite coproducts of Noetherian spaces
- Continuous images of Noetherian spaces  
  e.g. topol. quotients

Harder:

- Powersets of Noetherian sp. (Hoare powerspaces)  
  [JGL07]
- Spaces of words over Noetherian alphabet ($\sim$Higman)  
  [JGL13]
- Spaces of terms over Noetherian signature ($\sim$Kruskal)  
  [JGL13]
## An Algebra of Noetherian datatypes

\[
D ::= A \quad \text{(finite qo)} \\
| N \quad \text{(<)} \\
| N \quad \text{(cofinite topology)} \ast \\
| \mathbb{Q}^k, \mathbb{R}^k, \mathbb{C}^k \quad \text{(Zariski topology)} \ast \\
| \text{Spec}(R) \quad \text{($R$ Noetherian ring)} \ast \\
| D_1 \times D_2 \times \ldots \times D_n \quad \text{(product)} \\
| D_1 + D_2 + \ldots + D_n \quad \text{(disjoint union)} \\
| D^* \quad \text{(words, Higman)} \\
| D^\circ \quad \text{(multisets)} \\
| \mathcal{T}(D) \quad \text{(trees, Kruskal)} \\
| D^*, \text{pref} \quad \text{(words, prefix topology)} \ast \\
| \mathcal{H}(D) \quad \text{(Hoare hyperspace)} \ast \\
| \mathcal{P}(D) \quad \text{(powerset)} \ast \\
| \mathcal{S}(D) \quad \text{(sobrification)} \ast \\
\]

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

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Computable Bases

Definition

A **computable basis** on a Noetherian space $X$ is:

- An r.e. set of codes for opens in $X$
- Computable functions implementing $\cup$, $\subseteq$.

(A localic thing, really; yet, we get points as $\cap$-irreducible opens.)

Theorem (JGL10, submitted)

**Every space in our algebra of Noetherian datatypes has a computable basis.**

(Well, keep $\mathbb{Q}^k$ but omit $\mathbb{R}^k$, $\mathbb{C}^k$ and, say, insist that $R = \mathbb{Q}[X_1, \ldots, X_n]$ in $\text{Spec}(R)$.)
I will only illustrate in the case of the LCPP state space.

(q_A, X_1, \ldots, X_m, q_B, Y_1, \ldots, Y_n, w)

- Current line for program A, in Q_A
- Current values of numerical vars of A, in Q^m
- Same for B
- Contents of comm. channel, in \Sigma^*

- A computable basis for Spec(Q[X_1, \ldots, X_n]) (real values)
- A computable basis for \Sigma^* (channels)
- A computable basis for Q_A, Q_B (finite sets)
- A computable basis for finite products
The case of \( \mathbb{Q}[X_1, \ldots, X_n] \)

Represent a polynomial ideal \( I \) as a finite set \( B \) of polynomials. Can see any polynomial as a rewrite rule:

\[
X_1^3 + 2X_1^2 - X_1X_2^2 - 1 \quad \quad \quad X_1^3 \rightarrow -2X_1^2 + X_1X_2^2 + 1
\]

Rewrite rules induce critical pairs (S-polynomials):

\[
P = X_1^3 + 2X_1^2 - X_1X_2^2 - 1 \\
Q = X_1^2X_2^2 - 4X_1X_2^2 + 3X_1X_2 + 5
\]

\[
\begin{align*}
S\text{-poly}(P, Q) & = \text{left} - \text{right} = -X_2^2P + X_1Q \\
& = -6X_1^2X_2^2 + 3X_1^2X_2 + X_1X_2^4 - 5X_1 + X_2^2
\end{align*}
\]

\[
\rightarrow 3X_1^2X_2 + X_1X_2^4 + 24X_1X_2^2 - 18X_1X_2 + X_2^2 - 5X_1 - 30
\]

(Normal form)
Buchberger’s Algorithm

Note

The following preserve $\langle B \rangle$:
- Interreducing: reducing $P \in B$ by $Q \in B$ ($Q \neq P$)
- Adding (normal forms of) S-polynomials of elements of $B$
- Removing 0

Theorem (Buchberger’s Algorithm, Gröbner Basis)

• The three operations above always terminate
• . . . yielding a set $B \downarrow$, called a Gröbner basis of $\langle B \rangle$.
• $B \downarrow$ is canonical: $\langle B \rangle = \langle B' \rangle$ iff $B \downarrow = B' \downarrow$.

Proof. Termination: by Dickson’s Lemma.
A Computable Basis for $\text{Spec}(\mathbb{Q}[X_1, \cdots, X_n])$

Represent open sets $O_I = \bigcap F_I = \{p \text{ prime ideal} \mid I \not\subset p\}$ by a Gröbner basis $B$ of $I$ ($B = B \downarrow$, $\langle B \rangle = I$).

- **Union:** $F_I \cap F_I' = F_{\langle I \cup I' \rangle}$, whence
  
  Given $B, B'$, return $(B \cup B') \downarrow$
A Computable Basis for $\text{Spec}(\mathbb{Q}[X_1, \cdots, X_n])$

Represent open sets $O_I = \bigcap F_I = \{p \text{ prime ideal } | \ I \not\subseteq p\}$ by a Gröbner basis $B$ of $I$ ($B = B \downarrow, \langle B \rangle = I$).

- **Union:** $F_I \cap F_{I'} = F_{\langle I \cup I' \rangle}$, whence
  
  Given $B, B'$, return $(B \cup B') \downarrow$

- **Inclusion:** $F_I \subseteq F_{I'}$ iff $\sqrt{I'} \subseteq \sqrt{I}$. Can be tested using Rabinowitch’s Trick:
  
  Given $B, B'$, $F_{\langle B \rangle} \subseteq F_{\langle B' \rangle}$ iff
  
  for every $P \in B'$, $(B \cup \{1 - YP\}) \downarrow$ contains a non-zero constant.
As in every wqo, opens = upward-closed subsets = $\uparrow E$ for finite $E$.

Represent opens by finite sets $E$ (of words, here).

- **Union:** Given $E$, $E'$, return $E \cup E'$
- **Inclusion:** $\uparrow E \subseteq \uparrow E'$ iff every word in $E$ contains an embedded word from $E'$
A Computable Basis for $X \times Y$

Will allow us to find computable basis for:

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

- Current line for program $A$, in $Q_A$
- Same for $B$
- Contents of comm. channel, in $\Sigma^*$
- Current values of numerical vars of $A$, in $\mathbb{Q}_A^m$

Fact

Given Noetherian $X$, $Y$, every open of $X \times Y$ is a finite union of open rectangles $U \times V$.

Hence computable basis given by finite sets of pairs $(U, V)$.
(Continued.)
A Computable Basis for $X \times Y$

Computable basis given by finite sets of pairs $(U, V)$.

- **Union**: given finite sets of pairs $E, E'$, return $E \cup E'$
- **Inclusion**: (needlessly?) complex.

\[
\bigcup_{i=1}^{m} U_i \times V_i \subseteq \bigcup_{j=1}^{n} U'_j \times V'_j
\]

iff
\[
\bigcup_{i=1}^{m} U_i \times V_i \cap \bigcap_{j=1}^{n} (\bigcup_{j} U'_j \times V'_j) = \emptyset
\]

iff
\[
\cdots
\]

iff $\forall i = 1 \cdots m, \forall J \subseteq \{1, \cdots, n\}, \ U_i \subseteq \bigcup_{j \in J} U'_j$ or $V_i \subseteq \bigcup_{j \notin J} V'_j$

(Exponential number of operations.)
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
**Irreducible Closed Subsets**

A closed subset $F$ is **irreducible** iff non-empty and $F \subseteq F_1 \cup F_2 \Rightarrow F \subseteq F_1$ or $F \subseteq F_2$.

These form the points in the **sobrification** $\mathcal{S}(X)$ of $X$.

**Theorem**

In a Noetherian space, every closed subset $F$ is a **finite** union of irreducible closed subsets.

I.e., $F$ contains of points below finitely many points in $\mathcal{S}(X)$:
Definition (JGL10, submitted)

An **S-representation** on a Noetherian space $X$ is:

- An r.e. set of codes for *irreducible closed subsets* of $X$ (a.k.a., elements of $S(X)$)
- A finite set $\top = \{C_1, \cdots, C_n\}$ representing the whole space: $C_1 \cup \cdots \cup C_n = X$
- A computable function $\land$ implementing intersection: $C \land C' = \{C_1, \cdots, C_n\}$ iff $C \cap C' = C_1 \cup \cdots \cup C_n$
- A decidable implementation $\sqsubseteq$ of $\subseteq$ on codes.
Any closed set $F$ can be represented by a finite set of codes
\{ $C_1, \cdots, C_n$ \} (namely, $F = C_1 \cup \cdots \cup C_n$).
Taking complements yields representations for opens.

- **Union:** compute intersection of corresponding closed set:

  Given \{ $C_1, \cdots, C_m$ \} and \{ $C'_1, \cdots, C'_n$ \}, return $\bigcup_{i,j} C_i \cap C'_j$

  Indeed  $(\bigcup_{i=1}^m C_i) \cap (\bigcup_{j=1}^n C'_j) = \bigcup_{i,j} (C_i \cap C'_j)$. 
Any closed set $F$ can be represented by a finite set of codes $\{C_1, \cdots, C_n\}$ (namely, $F = C_1 \cup \cdots \cup C_n$).
Taking complements yields representations for opens.

- **Union**: compute intersection of corresponding closed set:
  
  Given $\{C_1, \cdots, C_m\}$ and $\{C'_1, \cdots, C'_n\}$, return $\bigcup_{i,j} C_i \land C'_j$

  Indeed $(\bigcup_{i=1}^m C_i) \cap (\bigcup_{j=1}^n C'_j) = \bigcup_{i,j} (C_i \cap C'_j)$.

- **Inclusion**: Given $\{C_1, \cdots, C_m\}$ and $\{C'_1, \cdots, C'_n\}$,
  
  decide whether $\forall i, \exists j, C_i \subseteq C'_j$.

  Indeed:
  
  $\bigcup_{i=1}^m C_i \subseteq \bigcup_{j=1}^n C'_j$ \iff $\forall i, C_i \subseteq \bigcup_{j=1}^n C'_j$

  \iff $\forall i, \exists j, C_i \subseteq C'_j$ by irreducibility.

**Note**: only need polynomially many subcalls.
An S-representation for $X \times Y$

This is easy!

**Fact**

\[ S(X \times Y) \cong S(X) \times S(Y) \]  
In particular, the irreducible closed subsets of $X \times Y$ are the rectangles $C \times C'$, $C \in S(X)$, $C' \in S(Y)$.

Hence codes in $X \times Y$ are pairs of codes $(C, C')$.

- **Top:** $T_{X \times Y} = T_X \times T_Y$
- **Meet:**  
  \[ (C_1, C'_1) \land (C_2, C'_2) = \{ (C, C') \mid C \in C_1 \land C_2, C' \in C'_1 \land C'_2 \} \]
- **Order:** $(C_1, C'_1) \preceq (C_2, C'_2)$ iff $C_1 \preceq C_2$ and $C'_1 \preceq C'_2$
An $S$-representation for $\Sigma^*$

These are specific, and nice, regular expressions:

**Theorem (JGL+Finkel09)**

The irreducible closed subsets of $\Sigma^*$ are exactly the word products of [ACJY96]:

$$P ::= \epsilon$$

$$\mid C?P \quad (C \in S(\Sigma))$$

$$\mid F^*P \quad (F \text{ closed, represented as } \{C_1, \cdots , C_n\})$$

- **Top:** $\top_{\Sigma^*} = \top_{\Sigma}^*$

- **Meet:** easy recursive, poly-time procedure (exercise)

- **Order:** again recursive poly-time [ACJY96, JGL+Finkel09]

E.g., $C?P \triangleleft_{\Sigma^*} C'?P'$ iff $C \triangleleft_{\Sigma} C'$ and $P \triangleleft_{\Sigma^*} P'$, or $C \triangleleft_{\Sigma} C'$ and $C?P \triangleleft_{\Sigma^*} P'$
An S-representation for $\text{Spec}(\mathbb{Q}[X_1, \ldots, X_n])$

Damn, this one is complicated. . .

A primary ideal $I$ is one where $PQ \in I \Rightarrow P \in I$ or $\exists k, Q^k \in I$.
Since radicals of primary ideals are prime, and $F_I$ for $I$ prime is irreducible, primary ideals represent irreducible closed subsets.

Theorem (Lasker-Noether)

Every ideal $I$ in a Noetherian ring is the intersection of finitely many primary ideals $p_1, \ldots, p_n$.

In particular $F_I = F_{p_1} \cup \cdots \cup F_{p_n}$.

Moreover, one can compute Gröbner bases for $p_1, \ldots, p_n$ from a Gröbner basis for $I$ [Sturmfels 2002].
An $S$-representation for $\mathbb{Q}[X_1, \cdots, X_n]$

Take primary ideals as codes for irreducible closed subsets of $\text{Spec}(\mathbb{Q}[X_1, \cdots, X_n])$.

- **Top:** $\top = \{\langle 1 \rangle\}$
- **Meet:** Given Gröbner bases $B, B'$ for two primary ideals:
  - Compute a Gröbner basis for $\langle B \rangle \cap \langle B' \rangle$, e.g.
    $\exists Y, (YB \cup (1 - Y)B') \downarrow$
  - Apply Sturmfels’ algorithm to the latter.
- **Order:** by Rabinowitch’s Trick, $B \subseteq B'$ iff for every $P \in B$, $(B' \cup \{1 -YP\}) \downarrow$ contains a non-zero constant.
Outline

1. Introduction
2. Algebraic Geometry 101
3. Verification of Infinite-State Systems
   - Wqos
   - WSTS
4. Noetherian Spaces as Generalized Wqos
   - From Wqos to Noetherian Spaces
   - Case Study: LCPPs
5. The Mathematics of Noetherian Spaces
6. Computing with Noetherian Spaces
   - Computable Bases
   - S-representations
7. Conclusion
Conclusion

- **Noetherian** spaces: a natural topological extension of wqos
- The standard backward algorithm for WSTS still terminates
- A **rich** collection of Noetherian datatypes
- **Two** competing, complementary representations of opens (computable bases, S-representations).

Not said here:
- Forward procedures [FinkelJGL09]
- Stone duals of Noetherian spaces
- The VJGL lemma [JGL09, unpublished]
- Kruskal’s Theorem, constructive proofs [JGL13]

Open questions:
- Extending Robertson-Seymour (undirected graphs)
- Reverse mathematics (see [Marcone14])
- Better representations, complexity-wise?