The VJGL Lemma*

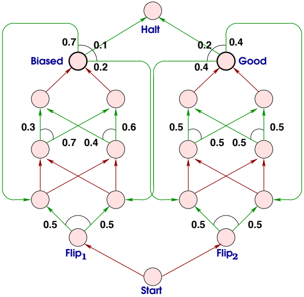
Jean Goubault-Larrecq

DMV/WQO – 25 sep. 2015

* Name found by Philippe Schnoebelen, 2009.

Our setting

- Verification of certain infinite state transition systems
- . . . that use wqos in an essential way.



- The VJGL Lemma of the title is an easy observation
- . . . and an excuse to introduce a larger field.

Outline

Well-structured transition systems

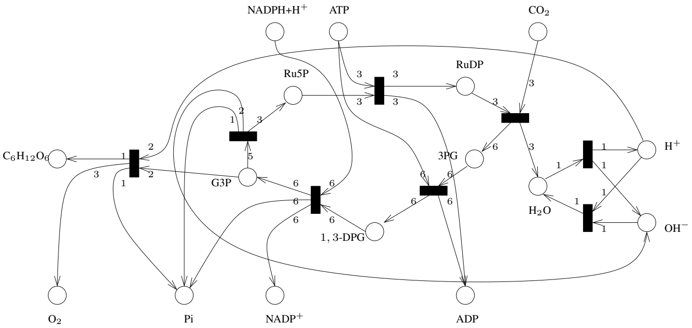
- WSTS: an extremely successful paradigm [F87,FS01,AJ93,ACJY96], including Petri nets, lossy channel systems, etc.
- Ingredients:
  - A transition relation $\delta \subseteq X \times X$;
  - A well quasi-ordering (wqo) $\leq$ on X;
  - $+$ monotonicity:

$$\begin{tikzcd} x \arrow[r, "\leq"] \arrow[d, "\delta"'] & x' \arrow[d, dotted, "\delta"] \\ y \arrow[r, dotted, "\leq"] & y' \end{tikzcd}$$

- $\leq$ is wqo iff (equivalently):
  - no infinite descending chain, and no infinite antichain;
  - every upward-closed subset U is of the form $\uparrow A$, A **finite**

... A is called a basis of U.

Example: Petri nets



- Set P of places ◯ + transitions shown as black rectangles
- $X = \mathbb{N}^P$, transitions given by vectors in $\mathbb{Z}^p$
- E.g., a state is $(n_{CO_2}, n_{RuDP}, n_{3PG}, n_{H_2O}, \cdots, n_{C_6H_{12}O_6}, n_{O_2})$
- Exercise: spot the transition $(-3, -3, +6, +3, 0, 0, \cdots)$.

Coverability is decidable

Let $Pre(U) = \{x \mid \exists y \in U \cdot x \xrightarrow{\delta} y\}$.
Say that a WSTS is effective iff:

- $\leq$ decidable
- one can compute a finite basis A of $Pre(\uparrow t)$ $\quad (Pre(\uparrow t) = \uparrow A)$

Coverability

Input: states s, t

Q: $\exists s'$, $s \xrightarrow{\delta}^{*} s' \geq t$?

Theorem

Coverability is decidable for every effective WSTS.

Proof. Equivalently, $s \in \bigcup_k Pre^k(U)$ where $U = \uparrow t$.
Stabilizes at some k by wqo; computable by effectiveness. □

Outline

Valk and Jantzen's effective basis theorem

How do we compute a basis? [for $X = \mathbb{N}^k$]

- By ad hoc algorithms, depending on δ
- Or by Valk-Jantzen's theorem:

Theorem (Valk-Jantzen, 1985)

Given $U \subseteq \mathbb{N}^k$ upward-closed, one can compute a finite basis for U if the following is decidable:

> **Input:** $\vec{m} \in \mathbb{N}^k_\omega$
> **Q:** *does U meet $\downarrow \vec{m} \cap \mathbb{N}^k$?*

Proof . . . I'll prove a more general theorem later. □

- $-$: not really a basis for implementation
- $+$: easy proofs that bases are computable

Example: affine counter systems

Finitely many transitions $\vec{x} \in \mathbb{N}^k \mapsto A_i\vec{x} + \vec{b}_i$,
with $A_i \in Mat_{\mathbb{N}}(k \times k)$, $\vec{b}_i \in \mathbb{Z}^k$ (Petri nets=special case A_i =id)
... enabled iff $A_i\vec{x} + \vec{b}_i \geq 0$.

- Compute $Pre(\uparrow t)$ directly: feasible, will require you to make several cases;
- By Valk-Jantzen: $U = Pre(\uparrow t)$. Check that:

  Input: $\vec{m} \in \mathbb{N}_\omega^k$
  Q: *is there an* i *such that* $A_i\vec{m} + \vec{b}_i \geq t$*?*

  is obviously decidable.

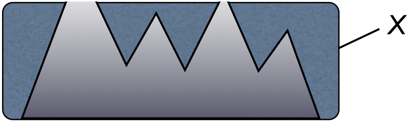
Outline

The VJGL lemma (1/4)

Fact (Finkel, JGL, STACS09; Pouzet and others earlier, I'm sure)

Every wqo $X, \leq$ embeds into a completion $\widehat{X}$ so that:

$$\textit{Downward closed subsets of } X \equiv {\downarrow} B \cap X,\ B \textit{ finite} \subseteq \widehat{X}.$$



Note: $\widehat{X}$=ideal completion of X

(=sobrification of X, in the more general case of Noetherian spaces).

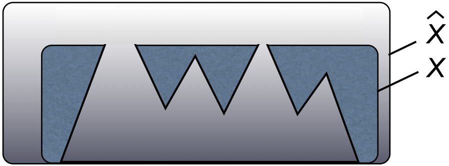
E.g., for $X = \mathbb{N}^k$, $\widehat{X} = \mathbb{N}^k_\omega$.

The VJGL lemma (1/4)

Fact (Finkel, JGL, STACS09; Pouzet and others earlier, I'm sure)

Every wqo $X, \leq$ embeds into a completion $\widehat{X}$ so that:

Downward closed subsets of $X \equiv \downarrow B \cap X$, B *finite* $\subseteq \widehat{X}$.



Note: $\widehat{X}$=ideal completion of X

(=sobrification of X, in the more general case of Noetherian spaces).

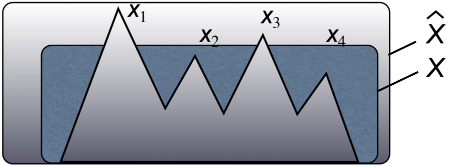
E.g., for $X = \mathbb{N}^k$, $\widehat{X} = \mathbb{N}_\omega^k$.

The VJGL lemma (1/4)

Fact (Finkel, JGL, STACS09; Pouzet and others earlier, I'm sure)

Every wqo $X, \leq$ embeds into a completion $\widehat{X}$ so that:

$$\textit{Downward closed subsets of } X \equiv \downarrow B \cap X,\ B \textit{ finite} \subseteq \widehat{X}.$$



[Here $B = \{x_1, \ldots, x_4\}$]

Note: $\widehat{X}$=ideal completion of X

(=sobrification of X, in the more general case of Noetherian spaces).

E.g., for $X = \mathbb{N}^k$, $\widehat{X} = \mathbb{N}_\omega^k$.

The VJGL lemma (2/4)

[I now assume effective representations for points in X, and X r.e.]

For $E \subseteq X$, complement of $\uparrow A$ is of the form

$$\downarrow\{\vec{m}_1, \cdots, \downarrow\vec{m}_n\} \cap X, \qquad \text{with } \vec{m}_i \in \widehat{X}.$$

Definition (Effective Complement)

Say X has effective complement iff

$\{\vec{m}_1, \cdots, \vec{m}_n\}$ is computable from A.

Example: $X = \mathbb{N}^k$, $\widehat{X} = \mathbb{N}^k_\omega$

E.g., let $A = \{1\ 3\ 2, 4\ 1\ 3\} \subseteq \mathbb{N}^3$

$$\begin{aligned} \complement{\uparrow} A &= \complement{\uparrow} 1\ 3\ 2 \cap \complement{\uparrow} 4\ 1\ 3 \\ &= \downarrow\{0\ \omega\ \omega, \omega\ 2\ \omega, \omega\ \omega\ 1\} \cap \downarrow\{3\ \omega\ \omega,\ \omega\ 0\ \omega,\ \omega\ \omega\ 2\} \\ &= \downarrow\{0\ \omega\ \omega,\ 3\ 2\ \omega,\ \omega\ 0\ \omega,\ \omega\ 2\ 2,\ \omega\ \omega\ 1\}. \end{aligned}$$

The VJGL lemma (3/4)

Theorem (JGL, RR 05/2009)

Let X have effective complement.
Given $U \subseteq X$ upward-closed, one can compute a finite basis A for U (i.e., $U = \uparrow A$) if the following is decidable:

> **Input:** $\vec{m} \in \widehat{X}$
> **Q:** *does U meet $\downarrow \vec{m} \cap X$?*

Proof. Note: we can test $\vec{a} \in U$ for $\vec{a} \in X$ (take $\vec{m} = \vec{a}$).

- Start with $A := \emptyset$.
- Enumerate $\vec{a} \in X$: for each, if $\vec{a} \in U$, add it to A.
- A will eventually contain all the finitely many minimal elements of U, so $U = \uparrow A$. We check this by ...

The VJGL lemma (4/4)

Theorem (JGL, RR 05/2009)

Let X have effective complement.
Given $U \subseteq X$ upward-closed, one can compute a finite basis A for U (i.e., $U = \uparrow A$) if the following is decidable:

Input: $\vec{m} \in \widehat{X}$
Q: *does U meet $\downarrow \vec{m} \cap X$?*

Proof. We check that $\uparrow A = U$ by:

- computing $\complement \uparrow A$ as $\downarrow\{\vec{m}_1, \cdots, \downarrow \vec{m}_n\} \cap X$ (eff. complement)
- and testing whether $\neg$ (U meets some $\downarrow \vec{m}_i \cap X$).

Indeed, $\uparrow A = U$ iff $U \subseteq \uparrow A$
iff $U \cap \complement \uparrow A = \emptyset$
iff $U \cap (\downarrow\{\vec{m}_1, \cdots, \downarrow \vec{m}_n\} \cap X) = \emptyset$
iff for every i, U meets $\downarrow \vec{m}_i \cap X$. $\square$

Outline

Ph. Schnoebelen's original motivation

[Schnoebelen, Chambart, DLT10] rely on it for $X = \Sigma^*$, not $\mathbb{N}^k$.

Corollary (JGL, RR 05/2009; Abdulla, Mayr, LICS'11)

Let Σ be a finite alphabet.
Given $U \subseteq \Sigma^*$ upward-closed w.r.t. subword, one can compute a finite basis A for U (i.e., $U = \uparrow A$) if the following is decidable:

> **Input:** *R regular expression over Σ*
> **Q:** *does U meet R?*

Proof. For $X = \Sigma^*$, with subword, $\hat{X} = \{\text{word-products } P\}$
[Jullien 69; Abdulla *et al.* 04; Finkel, JGL 09].

$$P ::= \epsilon \mid a^? P \mid A^* P \qquad (A \neq \emptyset, A \subseteq \Sigma) \qquad \square$$

Note: In fact only need word-products, not general regexps, for R.

Used in:

- **Computing blocker sets for the Regular Post Embedding Problem** [Schnoebelen, Chambart, DLT10]
  PEP: Given two semigroup morphisms $u, v \colon A^* \to B^*$, a regular language $R \subseteq A^*$, decide whether $u(x) \leq v(x)$ for some $x \in R$.
  Decidable [Schnoebelen, Chambart].
  A *coblocker* is a word w such that $u(x) \leq w.v(x)$ for some $x \in R$.
  Coblockers are upward-closed, hence computable by VJGL.
- **On Reachability for Unidirectional Channel Systems Extended with Regular Tests** [Jančar, Karandikar, Schnoebelen 2015]
  Verification of certain lossy channel systems with one lossy and one non-lossy channel.
  With emptiness test on second channel, decidable.
  VJGL allows us to show that decidability is preserved with emptiness tests on *both* channels, reducing to previous case.

More words

Easily generalizes to infinite alphabets Σ, wqo by $\leq$.

Corollary (JGL, RR 05/2009)

Let $\Sigma, \leq$ be wqo.
Given $U \subseteq \Sigma^*$ upward-closed w.r.t. embedding, one can compute a finite basis A for U (i.e., $U = \uparrow A$) if the following is decidable:

> **Input:** *R word-product over Σ*
> **Q:** *does U meet R?*

Proof. For $X = \Sigma^*$, $\hat{X} = \{\text{word-products } P\}$
[Kabil, Pouzet, 92; Finkel, JGL, STACS 09].

$$P ::= \epsilon \mid a^? P \mid A^* P$$

where $a^? = \{\epsilon, b \mid b \leq a\}$, $A^* = \{\text{words with letters} \in {\downarrow} A\}$
($a \in \widehat{\Sigma}$, A finite non-empty $\subseteq \widehat{\Sigma}$).

Outline

A catalogue of wqo datatypes

Here is an infinite list of spaces X where VJGL applies:

X	$::=$	A	(finite poset; e.g., states of automata)
	$\mid$	$\mathbb{N}$	(natural numbers)
	$\mid$	$X_1 \times X_2 \times \ldots \times X_n$	(product; e.g., $\mathbb{N}^k$)
	$\mid$	$X_1 + X_2 + \ldots + X_n$	(disjoint sum)
	$\mid$	X^*	(finite words/word embedding)
	$\mid$	$X^{\circledast}$	(finite multisets/multiset embedding)
	$\mid$	$\mathcal{T}(X)$	(finite trees/tree embedding)

Fact

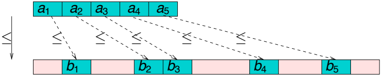
Each of these (wqo) spaces X has:

- an effectively representable completion $\widehat{X}$
- with decidable ordering
- and the effective complement property.

A catalogue of wqo datatypes: finite words (1/2)

Finite posets, $\mathbb{N}$, products, sums are easy.
We have already seen X^*... at least partly.
Let $Y = X^* = \{$finite sequences of elements of $X\}$.

- Order multisets Y by word embedding:



- $\widehat{Y}$: word-products $P ::= \epsilon \mid a^? P \mid A^* P$
- Ordering $\sqsubseteq$ decidable, using the following rules:

$$\frac{eP \sqsubseteq^{\mathrm{w}} P'}{eP \sqsubset^{\mathrm{w}} e'P'}\,(\mathrm{w1}) \qquad \frac{a \sqsubset a' \quad P \sqsubseteq^{\mathrm{w}} P'}{a^? P \sqsubset^{\mathrm{w}} a'^? P'}\,(\mathrm{w2}) \qquad \frac{P \sqsubset^{\mathrm{w}} P'}{a^? P \sqsubset^{\mathrm{w}} a^? P'}\,(\mathrm{w3})$$

$$\frac{\forall i \cdot e_i \sqsubset^{\mathrm{e}} A'^* \quad P \sqsubseteq^{\mathrm{w}} P'}{e_1 \dots e_k P \sqsubset^{\mathrm{w}} A'^* P'}\,(\mathrm{w4}) \qquad \frac{P \sqsubset^{\mathrm{w}} P'}{A^* P \sqsubset^{\mathrm{w}} A^* P'}\,(\mathrm{w5})$$

A catalogue of wqo datatypes: finite words (2/2)

Complements obtained by $\complement\!\uparrow A = \bigcap_{w \in A} \complement\!\uparrow w$, where:

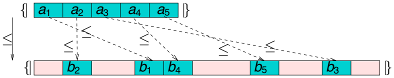
- $$\begin{aligned} \complement\!\uparrow_{X^*} a_0 a_1 \cdots a_n &= (\complement\!\uparrow_X a_0)^* X^? (\complement\!\uparrow_X a_1)^* X^? \cdots X^? (\complement\!\uparrow_X a_n)^* \\ &= \bigcup_{b_1, \cdots, b_{n-1}} A_0^* b_1^? A_1^* b_2^? \cdots b_{n-1}^? A_n^* \end{aligned}$$

  where A_i = max elements of $\complement\!\uparrow_X a_i$ in $\widehat{X}$
  and $b_1, \ldots, b_{n-1}$ range over max elements of $\widehat{X}$
- The outer intersection is computed by computing binary intersections $P \cap P'$, by induction on the sizes of P and P' (exercice).

A catalogue of wqo datatypes: multisets

Let $Y = X^{\circledast} = \{$finite multisets of elements of $X\}$.

- Order multisets Y by Parikh image of word embedding:



- $\widehat{Y}$: "linear logic contexts" $m ::= A^{\circledast}, a_1^?, \cdots, a_n^?$
  $m =$ set of multisets containing at most one element $\leq a_i$ for each i, plus as many in $\downarrow A$ as you wish
- Ordering on Y, intersection, complements: exercise.

A catalogue of wqo datatypes: finite trees

Let $Y = \{\text{finite trees with nodes labeled by elements of } X\}$.

- Order trees by tree embedding.
- $\widehat{Y}$: certain regular tree expressions called *tree-products* [Finkel, JGL, unpublished, 2012]

$$P ::= \epsilon \mid f^?(\vec{P}) \mid \mathcal{F}^*.\_\Box(P_1 \mid \cdots \mid P_n)$$

where $f \in \widehat{X}$,
$\vec{P}$ is word-product over $\widehat{Y}$,
$\mathcal{F}$ is a finite sum of depth-1 "contexts" with hole $\Box$,
and subject to certain normalization conditions.

- Ordering on Y, intersection, complements: as for words, only more complicated.

Outline

Conclusion

- VJGL is easy,
- has a growing base of applications (e.g., R. Bonnet's PhD thesis, where he uses it on $\mathbb{N}_\omega^k$)
- Giving effective representations of $\widehat{X}$ is an interesting, independent problem.
  - Already done for a rich class of wqos X
  - ... in fact for the larger class of Noetherian spaces (including new constructions: powerset, Hoare powerdomain, $\mathbb{Q}^k$ with Zariski topology, words with prefix topology)
  - Still a few other wqos not yet worked out: graphs/minor embedding, trees/nested word embedding (with appl. to bounded path graphs)