PPL2005 Category 4 Talk
Well-Quasi-Ordering, Overview and its Applications

Mizuhito Ogawa (JAIST)

2005.3.9

Today's Menu

- Definition : What is WQO ?

- Theory
  - Kruskal-type theorems (on finite/infinite data structure)
  - WQO and regularity

- Applications
  - Simple termination
  - Deciding polynomial time complexity
  - Well structured transition system

WQO (Well-Quasi-Order)

Definition A QO (quasi ordering) $(A, \leq)$ is a reflexive transitive binary relation on A.

Definition For a QO $(A, \leq)$, a sequence $a_1, a_2, \cdots$ in A is *good* if there exist i, j s.t. $i < j$ and $a_i \leq a_j$, and *bad* otherwise.

Definition $(A, \leq)$ is a Well-Quasi-Order (WQO) if each infinite sequence in A is good.

Example A QO on a finite set, ordering on natural numbers, ...

Remark

- If $\leq$ is a WQO, $<$ $(= \ \leq \setminus \geq)$ is a WFO (but not vice versa).
- The minimal elements of a subset of A is finite.

Theory: Kruskal-type theorems on finite structures

Kruskal-type theorems at a glance

For pair (product) ··· (Dickson 28)

For finite structures ···

Finite words	(Higman 54)
Finite trees	(Kruskal 60)
··· simple proof (Ramsey Th. + MBS)	(Nash-Williams 63)
··· with gap-condition (finite labels)	(H.Friedman 85)
··· with gap-condition (ordinal labels)	(Igor Křîž 1989)
Finite graphs with bounded tree-width	(RS 89)
Fintie graphs	(RS 88)

For infinite structures ···

Infinite words	(Nash-Williams 65)
Infinite trees (ω-trees)	(Nash-Williams 65,Laver 78)
··· with gap-condition (finite labels)	(R.Thomas 89)
··· with gap-condition (ordinal labels)	(R.Thomas 95)
Infinite graphs with bounded tree-width	(R.Thomas 89)
Countable graphs ?	
Conter-example for uncountable graphs	(R.Thomas 89)

Higman's Lemma : embedding on finite words

Higman's lemma If $(A, \leq)$ is a WQO, $(A^*, \preceq)$ is a WQO where $\preceq$ is the embedding.

e.g., $$(2,3,1,4) \preceq (3,1,5,1,1,6)$$
$$(2,3,1,4) \not\preceq (1,5,2,2,2,6)$$

Proof = Ramsey's Th. + Minimal Bad Sequence (MBS)

Ramsey's theorem (infinite version) Paint each edge of a countable complete graph either *red* or *green*. Then, it contains a monochromatic countable complete subgraph.

Corollary An infinite sequence $a_1, a_2, a_3, \cdots$ in A contains either an infinite bad sequence or an infinite ascending chain.

Proof For each i, j with $i < j$, paint (a_i, a_j) *red* if $a_i \leq a_j$, and *green* if $a_i \not\leq a_j$. ∎

Proof = Ramsey's Th. + Minimal Bad Sequence (MBS)

Higman's lemma If $(A, \leq)$ is a WQO, $(A^*, \preceq)$ is a WQO.

Definition An infinite bad sequence that is minimal wrt the lexicographical order of the word length is *Minimal Bad Sequence* (MBS).

Remark If an infinite bad sequence exists, an MBS exists (by Zorn's Lemma).

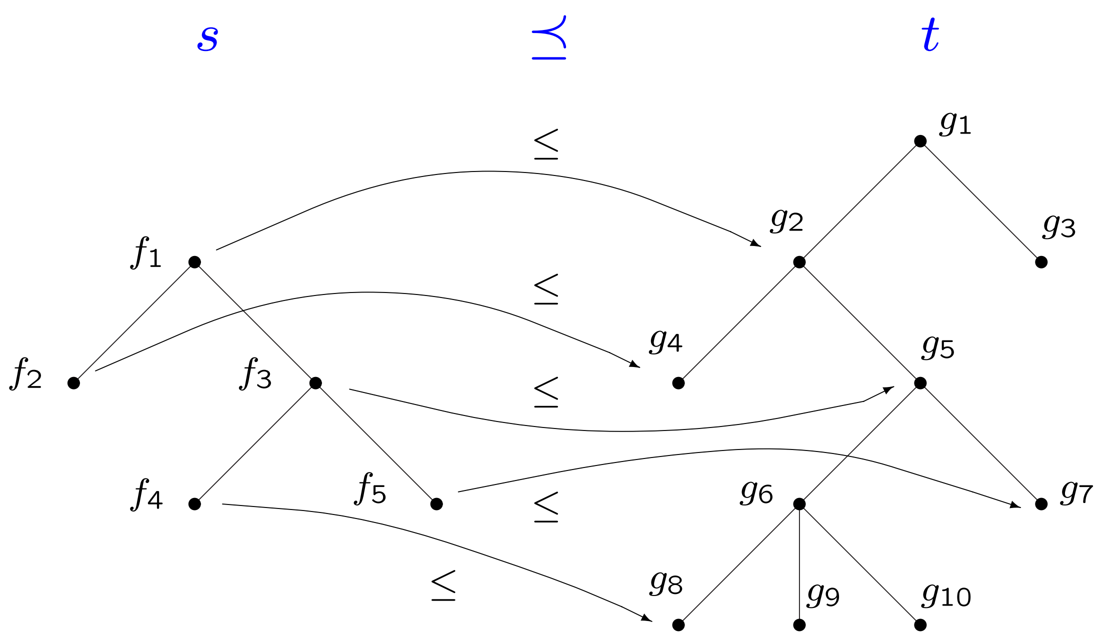
Proof For an MBS $t_1, t_2, t_3, \cdots$, let $t_i = a_i \cdot t'_i$.

If $t'_1, t'_2, t'_3, \cdots$ contains an infinite bad sequence $t'_{j_1}, t'_{j_2}, t'_{j_3}, \cdots$, $t_1, t_2, \cdots, t_{j_1 - 1}, t'_{j_1}, t'_{j_2}, t'_{j_3}, \cdots$ contradicts to the MBS. Thus, from Corollary, there is an infinite ascending chain $t'_{j_1}, t'_{j_2}, t'_{j_3}, \cdots$.

Since $a_{j_1}, a_{j_2}, a_{j_3} \cdots$ is good, thus there are k, k' with $k < k'$ and $a_{j_k} \leq a_{j_{k'}}$. Thus $t_{j_k} \preceq t_{j_{k'}}$ and a contradiction. ∎

Kruskal's Theorem : embedding on finite words

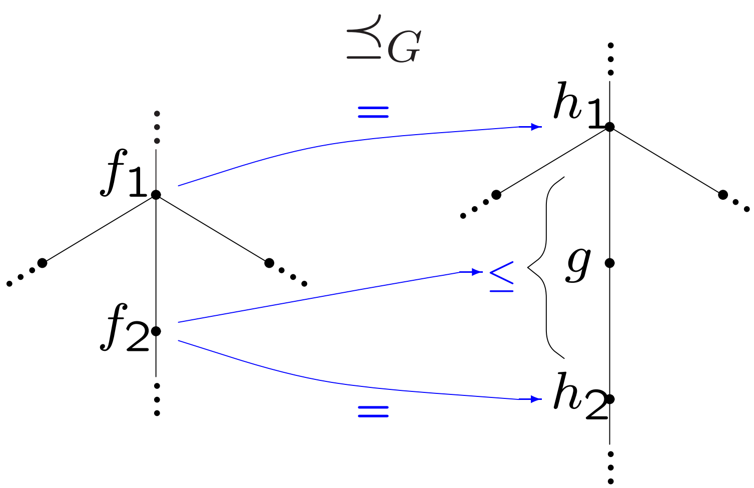
Kruskal's Theorem If $(A, \leq)$ is a WQO, $(T(A), \preceq)$ is a WQO.



embedding

Extension with Gap-condition : Finite labels

Let labels of nodes be in $\{1, 2, \cdots, n\}$. Define the embedding not only from correspondence between nodes, but also from *gap*.



$$f_1 = h_1$$
$$f_2 = h_2$$
$$+$$

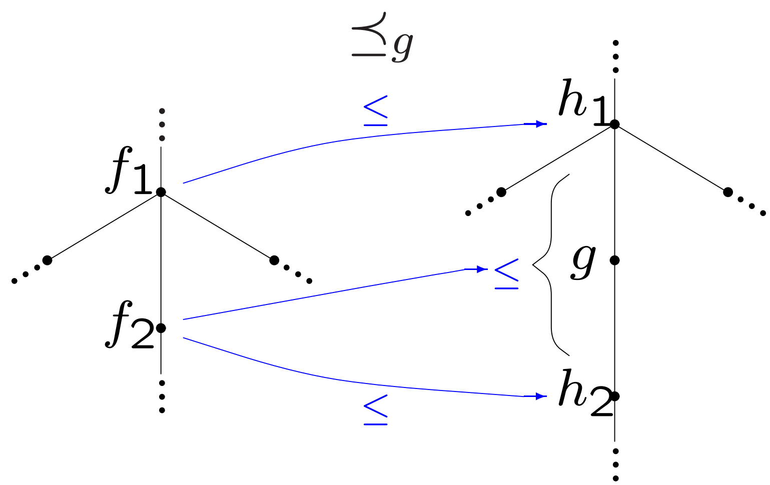
gap-condition

$$f_2 \leq g$$

Kruskal-Friedman's theorem $(T([1, n]), \preceq_G)$ is a WQO.

Extension with Gap-condition : Ordinal labels

Let labels of nodes be in *ordinals* $\{1, 2\cdots, \omega, \cdots, \Gamma_0\cdots\}$.



$$f_1 \leq h_1$$
$$f_2 \leq h_2$$
$$+$$
gap-condition
$$f_2 \leq g$$

Theorem (Igor Křı̌ž 1989) $(T(Ord), \leq_g)$ is a WQO.

Remark $\leq_G$ does not work.

e.g., $(\omega, \omega), (\omega, 0, \omega), (\omega, 0, 1, \omega), \cdots, (\omega, 0, 1, \cdots, n, \omega), \cdots$

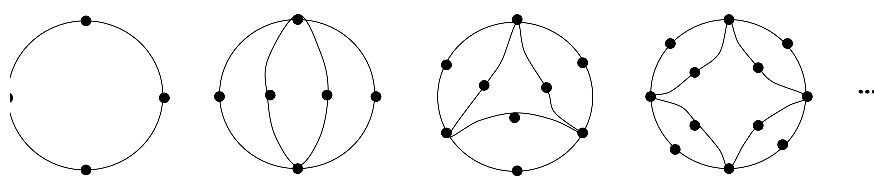
Immersion and Minor (for simple graphs)

Immersion (embedding) $G \preceq_I G' \;\Leftrightarrow\; G \to_I^* G'$ where $\to_I$ is an edge/node addition.

Minor $G \preceq_M G' \;\Leftrightarrow\; G \leftarrow_M^* G'$ where $\to_M$ is either an edge contraction or an edge/node removal.

Lemma For graphs with degree less-than-equal-to 3, $\preceq_I$ and $\preceq_M$ are equivalent.

Remark Imme



D_1 D_2 D_3 D_4

Graph Minor Theorem (Wagner's Conjecture)

Theorem (RS88) Minor relation $\preceq_M$ is a WQO on finite graphs.

(Very Rough) Proof Scenario Let $G_1, G_2, \cdots$.

(1a) If a finite graph G_i is planar, a finite graph G with $G_i \not\preceq_M G$ has an upperbound of its *tree width*.

(1b) The minor relation $\preceq_M$ on graphs with *bounded tree width* is a WQO (by Kruskal-Friedman Th. + Menger-like property).

(2a) If each finite graph G_i is non-planar, each finite graph $G_i (i > 0)$ with $G_1 \not\preceq_M G_i$ can be embedded on an algebraic surface.

(2b) An algebraic surface Σ is constructed as "1 *sphere* + a *handles* + b *cross-caps* − c *dishes*". Use induction on $C(\Sigma) = 4a+2b+c$.

Remark The proof is more than 100 pages, refering a few results in (more than 20) *Graph Minor* paper series. The main proof still remains as *preprint* from 1988 (*Need a simple proof!*).

Algebraic characterization of tree width (Arnborg, et.al 93)

Let B_k be a sort of k-terminal graphs with $k \geq 0$. Signatures are:

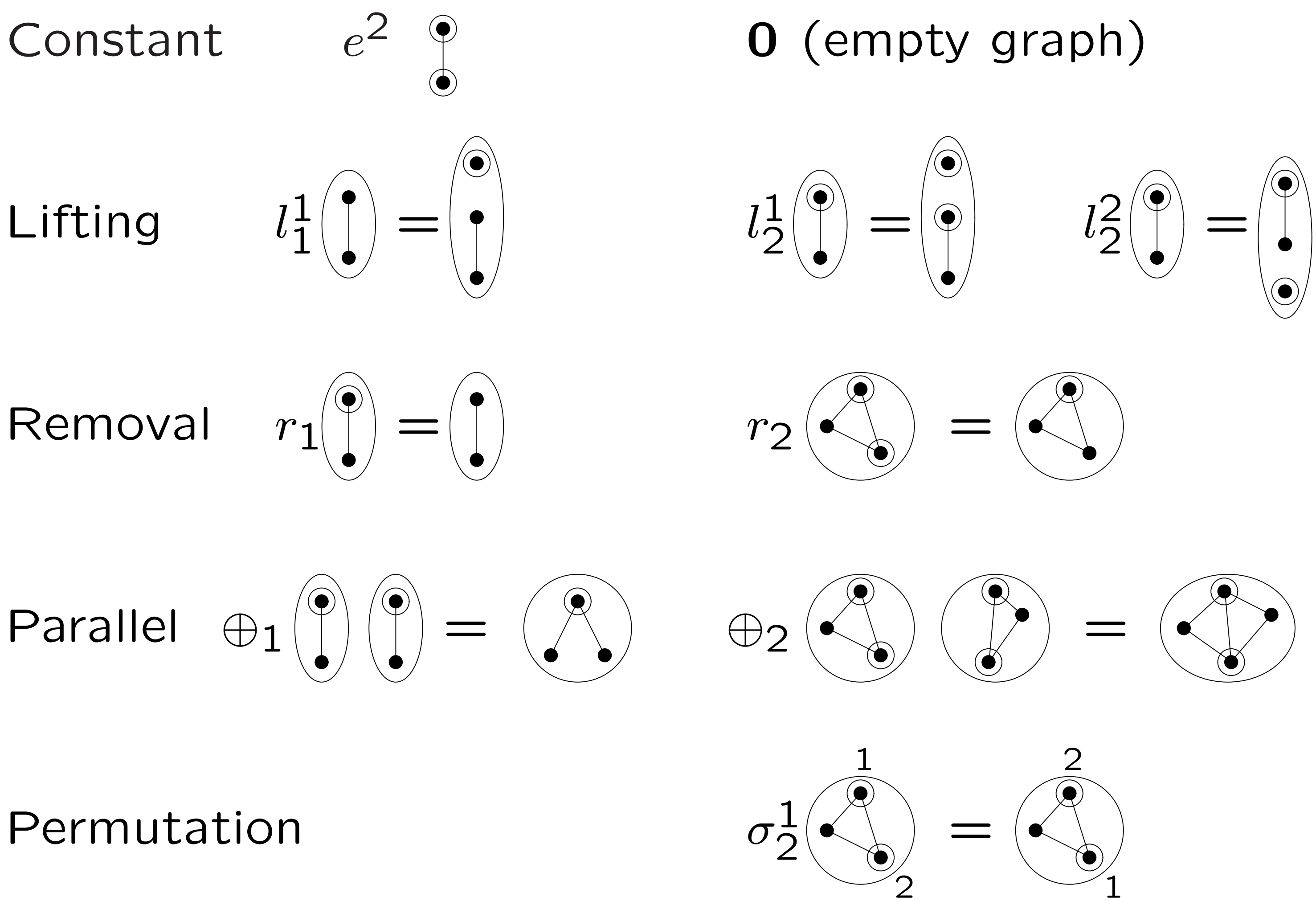
$$\begin{cases} l_k^i \; : \; B_{k-1} \to B_k, & \oplus_k \; : \; B_k \times B_k \to B_k, & e^2 \; : \; B_2, \\ r_k \; : \; B_k \to B_{k-1}, & \sigma_k^j \; : \; B_k \to B_k, & \mathbf{0} \; : \; B_0, \end{cases}$$

where

- $l_k^i(G)$ is *lifting*, i.e., insert a *fresh* terminal at the i-th position in $k-1$ terminals for $1 \leq i \leq k$.
- $r_k(G)$ is *removal*, i.e., remove the last terminal.
- $G \oplus_k G'$ is *parallel composition*, i.e., fuse each pair of the i-th terminals for $1 \leq i \leq k$.
- $\sigma_k^j(G)$ is *permutation*; permute the numbering of the j-th and $j+1$-th terminals for $1 \leq j < k$.

Lemma A graph G is constructed by l_j^i, r_j, p_j, e^2, and **0** with $i \leq j \leq k$, if, and only, if $twd(G) \leq k-1$.

Operations for graphs with tree width at most 2



Theory: Kruskal-type theorems on infinite structures

Rado's example : embedding on ω-words

Even if $(A, \leq)$ *is a WQO,* $(A^\omega, \preceq)$ *may not be a WQO!*

Example Let $A = \{(i,j) \mid 0 \leq i < j\}$ and
let $(i,j) \leq (k,l)$ iff either $i = k \wedge j \leq l$ or $j < k$.

$\alpha_1, \alpha_2, \cdots$ is a *bad sequence* where

$$
\begin{array}{rcc}
\alpha_1 & = & \langle (0,1),(1,2),(1,3),(1,4),\cdots \rangle \\
\alpha_2 & = & \langle (0,1),(1,2),(2,3),(2,4),\cdots \rangle \\
\cdots & = & \cdots \\
\alpha_i & = & \langle (0,1),\cdots,(i,i+1),(i,i+2),(i,i+3),\cdots \rangle
\end{array}
$$

$\Rightarrow$ Extension of WQO = *Better-Quasi-Order* (BQO).

Barrier

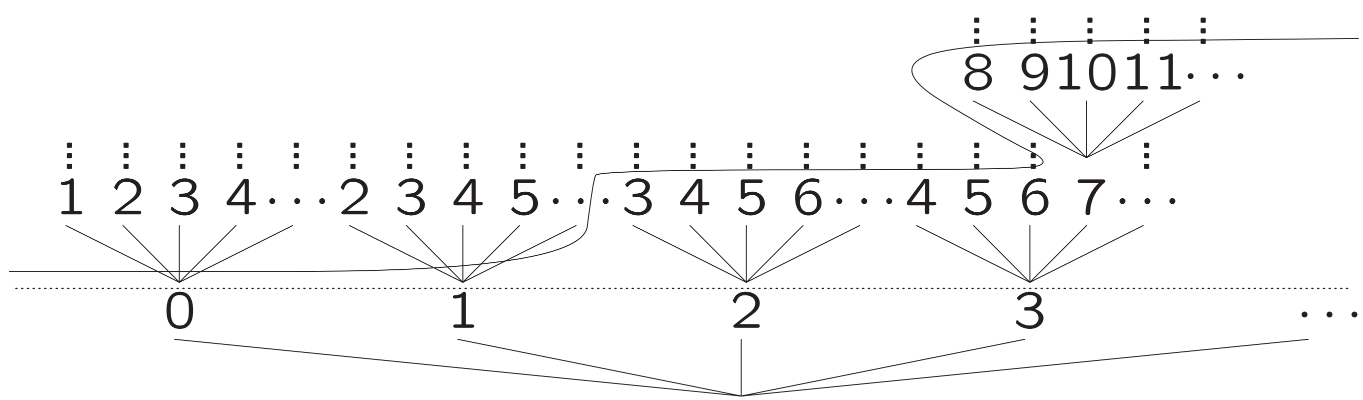
Definition For ascending chains s, t (of natural numbers), we define $pref(s,t)$ if s is an initial segment of t.

e.g., $pref((3,4,6),(3,4,6,7,9,\cdots))$, $pref((3),(3,4,6))$,

Definition B is a barrier (on an infinite set $X \subseteq \mathbf{N}$) if B is a set of finite ascending chains on X satisfying

- $\emptyset \notin B$.
- For any infinite ascending chain Y (in X), $\exists s \in B$ s.t. $pref(s,Y)$.
- $s,t \in B$ and $s \neq t$ imply $s \not\subset t$.

e.g.,



Tree of infinite ascending chains on Nat

Better-Quasi-Order (BQO)

Definition For finite ascending chains s, t, $s \triangleleft t$ if there exist $i_0 < i_1 < \cdots < i_n$ and $m(< n)$ s.t. $s = (i_0, i_1, \cdots, i_m)$, $t = (i_1, i_2, \cdots, i_n)$.

e.g., $(3) \triangleleft (5)$, $(3, 5, 6) \triangleleft (5, 6, 8, 9)$, $(3, 5, 6) \not\triangleleft (5, 6)$.

Definition $(A, \leq)$ is a Better-Quasi-Order (BQO) if for a barrier B and a function $g : B \to A$, there exist $s, t \in B$ such that $s \triangleleft t \wedge g(s) \leq g(t)$.

Remark The definition of WQO corresponds to a special barrier $B = \{(0), (1), (2), \cdots\}$, thus a WQO is a BQO.

Theorem (Nash Williams 65, Laver 78) If $(A, \leq)$ is BQO, $(A^\alpha, \preceq)$ is a BQO (where α is an ordinal).

Proof = Ramsey's Th. + Minimal Bad Sequence (MBS)

Definition For a barrier B, $f : B \to A$ is *perfect* (resp.*bad*) if $s \lhd t$ implies $f(s) \leq f(t)$ (resp. $f(s) \not\leq f(t)$) for $s, t \in B$.

Theorem (Galvin-Prikry 73) If $B = B_1 \cup B_2$ is a barrier, either B_1 or B_2 contains a barrier.

Corollary For a barrier B and $f : B \to A$, there exists a barrier $C \subseteq B$ such that $f|_C$ is either *perfect* or *bad*.

Lemma If B is a barrier, $B(2) = \{b_1 \cup b_2 \mid b_1 \lhd b_2\}$ is a barrier.

Proof of Corollary Let $D_1 = \{b_1 \cup b_2 \mid b_1, b_2 \in B,\ b_1 \lhd b_2,\ f(b_1) \leq f(b_2)\}$ and $D_2 = \{b_1 \cup b_2 \mid b_1, b_2 \in B,\ b_1 \lhd b_2,\ f(b_1) \not\leq f(b_2)\}$.
Since $B(2) = D_1 \cup D_2$, either D_1 or D_2 contains a barrier D. Let $C = \{b \in B \mid b \subseteq \cup_{d \in D}\ d\}$. $f|_C$ is *perfect* when $D \subseteq D_1$, and *bad* otherwise. ∎

Proof $=$ Ramsey's Th. $+$ Minimal Bad Sequence (MBS)

Definition $<'$ is a *partial ranking* of $(A, \leq)$ if $<'$ is a WFO and $<' \subseteq <$.

Definition For barriers B, C, $B \sqsubseteq C$ if $\cup C \subseteq \cup B$ and, for each $c \in C$, there exists $b \in B$ with $b = c$ or $pref(b, c)$. (e.g. $B \sqsubseteq B(2)$.)

Definition Let $f : B \to A$, $g : C \to A$ for barriers B, C. $f \sqsubseteq g$ if $B \sqsubseteq C$ and

- $g(a) = f(a)$ (if $a \in B \cap C$),
- $g(c) <' f(b)$ (if $b \in B$, $c \in C$, $pref(b, c)$).

Definition $f : B \to A$ is *minimal bad*, if f is maximum wrt $\sqsubseteq$.

Theorem (Laver 78) Let $<'$ be a partial ranking of $(A, \leq)$. If f is *bad*, there exists *minimal bad* g with $f \sqsubseteq g$.

Infinite Kruskal-type theorems

Fraïssé's Conjecture (Laver 71) For *countable* linearly ordered sets, $\preceq$ is a BQO.

Theorem (Laver 78) If $(A, \leq)$ is a BQO, $(T^\omega(A), \preceq)$ is a BQO.

Theorem (R.Thomas 89) $(T^\omega([1..n]), \preceq_G)$ is a BQO.

Theorem (R.Thomas 95) $(T^\omega(Ord), \preceq_g)$ is a BQO.

Open Problem Minor relation $\preceq_M$ is a WQO on countable graphs? (Probably, the length of each path in a graph must be at most ω.)

Theory: WQO and regularity

Myhill-Nerode's theorem

Let $\mathcal{A} = (A, Q, Q_f, s_0, \Delta)$ be an automaton and let $L(\mathcal{A})$ be a set of (finite) words accepted by $\mathcal{A}$.

Definition An equivalence relation $\sim$ over A^* is a *congruence* $u \sim v$ implies $w_1 u w_2 \sim w_1 v w_2$ for each $u, v, w_1, w_2 \in A^*$. If congruence classes are finite, $\sim$ is a *finite congruence*.

Myhill-Nerode's theorem The followings are equivalent.

- L $(\subseteq A^*)$ is regular.
- There is a finite congruence $\sim$ over A^* such that $u \in L$ and $u \sim v$ imply $v \in L$.

Proof

($\Rightarrow$) Define $u \sim_{\mathcal{A}} v$ by $q \xrightarrow[u]{} q' \Leftrightarrow q \xrightarrow[v]{} q'$ for $\forall q, q' \in Q$.

($\Leftarrow$) Define an automata by $Q = \{\text{equivalent class of } \sim\}$, $Q_f = \{[u] \mid u \in L\}$, $s_0 = [\epsilon]$, $\Delta = \{[u] \xrightarrow[v]{} [uv]\}$. ∎

Ehrenfeuchet's theorem

Definition L ($\subseteq A^*$) is *closed* wrt $\leq$ iff $x \in L \wedge x \leq y$ implies $y \in L$.

Theorem (Ehrenfeuchet 83) The followings are equivalent.

- L ($\subseteq A^*$) is regular.
- L is closed wrt a monotonic WQO $\leq$.

Proof

($\Rightarrow$) Define $\leq$ by $\sim_{\mathcal{A}}$.

($\Leftarrow$) Define $u \sim_L v$ by $w_1uw_2 \in L \Leftrightarrow w_1vw_2 \in L$ for $\forall w_1, w_2 \in A^*$. If congruence classes of $\sim_L$ are infinitely many, since $\leq$ is a WQO there is an infinite ascending chain $u_1 \leq u_2 \leq \cdots$ of representatives. Since $F(u) = \{(v,w) \mid vuw \in L\}$ is closed wrt $\leq \times \leq$, $F(u_1) \subseteq F(u_2) \subseteq \cdots$ from $u_1 \leq u_2 \leq \cdots$.
On the other hand, since $u_i \not\sim_L u_j$, $F(u_1) \subset F(u_2) \subset \cdots$. This contradicts to that $\leq \times \leq$ is a WQO. ∎

Ehrenfeuchet's theorem on ω-language

Definition A QO $(A^\omega, \preceq)$ is a periodic extension of $(A^*, \leq)$ if

- $u_i \leq v_i$ for each $u_i, v_i \in A^*$ implies $u_1 u_2 u_3 \cdots \preceq v_1 v_2 v_3 \cdots$.
- For each $\alpha \in A^\omega$, there exist $u, v \in A^*$ such that $\alpha \preceq u.v^\omega$ and $\alpha \succeq u.v^\omega$.

Theorem (Ogawa 04) $L(\subseteq A^\omega)$ is regular if, and only if, L is $\preceq$-closed wrt a periodic extension $(A^\omega, \preceq)$ of a monotone WQO $(A^*, \leq)$.

Application: Simple termination

Simple termination of TRSs

A TRS $R = \{l \to r\}$ terminates if there exists a WFO $>$ such that $s \to_R t$ implies $s > t$.

Theorem (Dershwitz 82) A TRS R terminates if there exists an order $>$ such that, for each ground term s, t, $>$ satisfies

- $s \geq t \;\Rightarrow\; C[s] \geq C[t]$ (monotonicity)
- $C[s] \geq s$ (subterm property)
- $s \to_R t \;\Rightarrow\; s > t$

Proof From the monotonicity and the subterm property, $\geq \supseteq \succeq_T$ on finite terms. From Kruskal's theorem $\preceq_T$ is a WQO, and $\leq$ is also a WQO. Thus $>$ is a WFO. ∎

Lexicographic Path Ordering (LPO)

Definition Let a precedence be an order on a finite set of function symbols. If ground terms $s = f(s_1, \cdots, s_m)$ and $t = g(t_1, \cdots, t_n)$ satisfy either (1),(2), or (3), then $s <_{LPO} t$.

(1) There exists i such that $s \leq t_i$.
(2) If $f = g$, there exists i such that $s_j = t_j$ for each j with $j < i$, $s_i < t_i$, and $s_k < t$ for each k with $i < k$.
(3) If $f < g$, $s_i < t$ for each i.

Theorem $<_{LPO}$ is a WFO on ground terms.

Remark There are many variants of path orederings, e.g., *Recursive Path Ordering* (RPO), *Path of Subterms Ordering* (PSO), *Recursive Decomposition Ordering* (PDO), $\cdots$.

Automated Termination Detection : Ackerman function

Definition (of Ackerman function)

$$\left\{ \begin{array}{lcl} ack(0,j) & = & s(j) \\ ack(s(i),0) & = & ack(i,s(0)) \\ ack(s(i),s(j)) & = & ack(i,ack(s(i),j)) \end{array} \right\}$$

Algorithm

(1) The naive way is to regard variables as fresh constants.
(2) Search a suitable precedence among the (finite) set of function symbols such that a TRS becomes terminating.

e.g., $0 < i, j < s < ack$ for Ackerman function.

Remark Some applications in partial evaluation, program transformation.

Application: Deciding Polynomial Time Complexity

Deciding a polynomial upper bound of graph algorithms

Recall that if $(A, \leq)$ is a WQO, minimal elements of a subset of A is finite. Further, minor relation $\preceq_M$ is a WQO on finite graphs.

Definition L is *closed* if $x \in L \wedge x \leq y$ implies $y \in L$.

Remark Assume L is closed. $t \in L$ if, and only if, $s \preceq_M t$ for a minimal element s in L. For example, a graph G is *not planar* if, and only if, $K_5 \preceq_m G$ or $K_{3,3} \preceq_m G$ (Kuratowski's Th.).

Theorem (RS 1995) The s-minor containment $s \preceq_M t$ is solved in $O(n^3)$ for a fixed s. (improved $O(n^2)$, Reed 1997)

Theorem (RS 1995) Given a graph s and a planar graph u, if $u \not\preceq_M t$, $s \preceq_M t$ is solved in $O(n^2)$. (improved $O(n)$, Reed 1997)

Remark For an arbitrary s, the s-minor containment is NP-complete (Hamilton cycle problem when $s = C_{|V(t)|}$).

Examples of polynomial upper bounds

Problem	known algorithm	upper bound
embedding to surface	$O(n)^{\dagger 1}$	$O(n^2)$
linkless spatial embedding	$O(n^2)^{\dagger 2}$	$O(n^2)$
knotless spatial embedding	?	$O(n^2)$
k-disjoint path‡	$O(n^2)$	$O(n^2)$
k-vertex separation‡	$O(n^{k^2+2k+4})$	$O(n)$
k-leaf max spanning tree‡	$O(n^{2k+1})$	$O(n)$
k-searcher‡	$O(n^{2k^2+4k+8})$	$O(n)$
$\vdots$	$\vdots$	$\vdots$

Note that

†1 The algorithm also detects obstructions (Mohar 1996).

†2 Obstructions are decided (RST 1993).

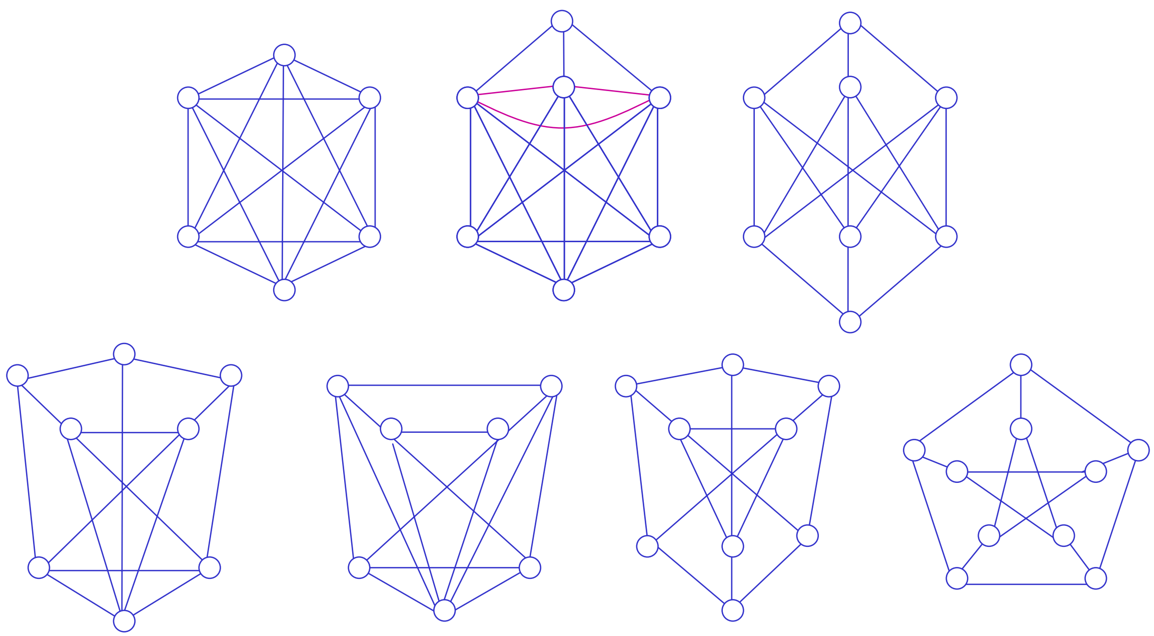
‡ Problems are for fixed k. For an arbitrary k is NP-complete.

Linkless spatial embedding

Theorem (RST93) G has a linkless spatial embedding if, and only if, G does not contain a graph in Petersen family.

The Petersen family

(graphs arising from K_6 by ¢-Y and Y-¢)



k-disjoint path, k-vertex separation

k-disjoint path problem

Instance: A graph G, and pairs of vertices $(s_1, t_1), \cdots, (s_k, t_k)$.

Question: Do there exist mutually vertex-disjoint paths P_i's in G s.t. P_i joins s_i and t_i ?

k-vertex separation problem

A linear layout of a graph G of $|V(G)| = n$ is a bijection $l : V(G) \to \{1, 2, \cdots, n\}$. Let $s_l(G) = max\{s_l(G, i)\}$ where

$$s_l(G, i) = |\{u \in V(G) \mid l(u) \leq i \text{ and } \exists (u, v) \in E(G). l(v) > i\}|$$

Instance: A graph G.

Question: Does there exist a linear layout l s.t. $s_l(G) \leq k$?
(Note that $s_l(S) > k$ for a $2k+1$-ary star S, which is planar.)

Constructive Proof of Higman's Lemma

Although we can decide polynomial complexity, hard to construct an algorithm of that complexity!

Reason

- We can detect obstructions, but we cannot decide whether we found all obstructions.
- The proof of Kruskal-type theorems does not give a sight - MBS is highly nonconstructive (Zorn's Lemma).

Fortunately, we have constructive proofs for Higman's Lemma.

- Higman's original proof is quite constructive (though lengthy).
- First constructive proof (Murthy-Russel 90).
- Several constructive proofs are known, even as a Coq proof!

The idea of contructive proof by Murthy-Russell

Show that a bad sequence is finite.

Idea For each prefix of a bad sequence, write down the possible choice of the next element by (*sequential*) regular expressions.

Example Let $\Sigma = \{a, b\}$. For a bad sequence $ab, bbaa, ba, bb, a, b$,

$$
\begin{array}{lcl}
\Theta_0 & = & (\Sigma - \epsilon)^* \\
\Theta_1 & = & (\Sigma - a)^*(b + \epsilon)(\Sigma - b)^* \cup (\Sigma - a)^*(a + \epsilon)(\Sigma - b)^* \ = \ \{b^*a^*\} \\
\Theta_2 & = & (b + \epsilon)(\Sigma - b)^* \cup (\Sigma - a)^*(a + \epsilon) \ = \ \{ba^*, b^*a\} \\
\Theta_3 & = & (\Sigma - b)^* \cup (b + \epsilon) \cup (a) \cup (\Sigma - a)^* \ = \ \{a^*, b^*\} \\
\Theta_4 & = & (\Sigma - b)^* \cup (b + \epsilon) \ = \ \{a^*, b\} \\
\Theta_5 & = & \{\epsilon, b\} \\
\Theta_6 & = & \{\epsilon\}
\end{array}
$$

Define WFO such that the sequential regular expressions for the longer prefix is smaller.

Query processing of indefinite database
(Van der Meyden, ACM PODS 1992)

Indefinite database = incomplete information of events on time

- (n-ary) Query processing with inquality $\cdots$ Π_2^p-complete (solves open problems)
- Monadic query processing with inquality $\cdots$ co-NP
- Fixed (n-ary) query processing with inquality $\cdots$ co-NP
- Fixed monadic query processing with inquality $\cdots$ $O(n)$

Remark Only existence of an $O(n)$ time algorithm is proved by Higman's lemma. The construction had been open.

Remark Generate a $O(n)$ time algorithm (= finding obstructions) based on Murthy-Russel's constructive proof of Higman's Lemma (Ogawa 03).

Example of a disjunctive monadic query

Fix a query $\varphi = \psi_1 \vee \psi_2 \vee \psi_3$ where

$$\begin{cases} \psi_1 &= \exists xyz[P(x) \wedge Q(y) \wedge R(z) \wedge \ x < y < z], \\ \psi_2 &= \exists xyz[Q(x) \wedge R(y) \wedge P(z) \wedge \ x < y < z], \text{ and} \\ \psi_3 &= \exists xyz[R(x) \wedge P(y) \wedge Q(z) \wedge \ x < y < z]. \end{cases}$$

Input $D = \{P(a), Q(b), a < b, Q(c), R(d), c < d, R(e), P(f), e < f\}$

Output *yes* (i.e., $D \models \varphi$)

Note that neither $D \models \psi_1$, $D \models \psi_2$, nor $D \models \psi_3$.

Obstructions are :

$$\left\{ \begin{array}{l} \{[P,Q,R]\}, \{[Q,R,P]\}, \{[R,P,Q]\}, \{[P,Q],[Q,R],[R,P]\}, \\ \{[P,Q,P],[Q,R]\}, \{[Q,R,Q],[R,P]\}, \{[R,P,R],[P,Q]\}, \\ \{[P,R,P],[Q,R]\}, \{[Q,P,Q],[R,P]\}, \{[R,Q,R],[P,Q]\}, \\ \{[P,Q,P,Q],[R]\}, \{[Q,R,Q,R],[P]\}, \{[R,P,R,P],[Q]\}, \\ \{[Q,P,Q,P],[R]\}, \{[R,Q,R,Q],[P]\}, \{[P,R,P,R],[Q]\} \end{array} \right\}$$

Application: Well structured transition system

Model Checking on infinite state transition systems

Model checking are mostly on *finite state* transition systems ($\approx$ *automata*).

Few decidable results on *infinite* *state* transition systems

- Pushdown transition system (Esparza, et.al. 03, Nitta, Seki 03)
- Timed CTL on dense time (??? 93)
- Well structured transition system (Finkel, Schnoebelen, 00)

Well structured transitions system (WSTS)

Definition A *WSTS* $M = (S, D, s_0, \Delta)$ consists of

- a finite set S of control states,
- a WQO $(D, \leq)$ on a possible infinite set of data,
- an initial state $(s_0, d_0) \in S \times D$,
- transition relation $\Delta \subseteq (S \times D) \times (S \times D)$.

A WQO $(D, \leq)$ is extended to a WQO $(S \times D, = \times \leq)$.

Definition A WSTS $M = (S, D, s_0, \Delta)$ is *monotonic* if $u_1 \to v_1$ and $u_1 \leq u_2$ for $u_1, u_2, v_1 \in S \times D$, there exists $v_2 \in S \times D$ such that $u_2 \to^* v_2$ and $v_1 \leq v_2$.

$$\begin{tikzcd} & s_1 \arrow[d] & \leq & t_1 \arrow[d, "*"'] & \\ \forall & s_2 & \leq & t_2 & \exists \end{tikzcd}$$

Example of a WSTS : Communicating Finite State Machines (CFSM)

Lossy channel is an unreliable communication system among *finite* objects (i.e., message may be correctly sent, or may be lost).

- Control states: the set S of configurations of a FSM.
- Data : the set $(\underbrace{A^* \times \cdots \times A^*}_{n}, \underbrace{\preceq \times \cdots \times \preceq}_{n})$ of products of messages at each channel, where A is finite alphbet.
- Initial state : $(\underbrace{s_0 \times \cdots \times s_0}_{n}, \underbrace{\epsilon \times \cdots \times \epsilon}_{n})$, where s_0 is the initial configuration.
- Transition : $c_i!a$, $c_i?a$, where c_i is the i-th channel and $a \in A$.

Example A CFSM is a monotonic WSTS.

Decidable properties for monotonic WSTSs

Notation $pre(I) = \{v \mid v \to u \in I\}$ for $I \subseteq S \times D$.

Assumption For a WSTS $M = (S, D, s_0, \Delta)$, the set of minimal elements in $pre(I)$ is effectively computed for each closed set I.

Theorem (Reachability) For a closed set $I (\subseteq S \times D)$, whether (an element of) I is reachable from the initial state (s_0, d_0) is decidable.

Proof Decide whether $(s_0, d_0) \in pre^*(I) = \cup_i \ pre^i(I)$, and $pre^*(I)$ finitely converges. ∎

Theorem (Eventuallity) If transitions at each state are finite, $EG\ I$ is decidable for a closed set $I (\subseteq S \times D)$.