A Constructive Proof of Higman's Lemma

Thomas Powell

Queen Mary, University of London

CL&C'12

University of Warwick, 8 July 2012

Overview of paper

'Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma.'

Overview of paper

'Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma.'

1. Use the Dialectica interpretation to obtain a constructive version of the classical 'minimal bad sequence' proof of Higman's lemma.

Overview of paper

'Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma.'

1. Use the Dialectica interpretation to obtain a constructive version of the classical 'minimal bad sequence' proof of Higman's lemma.
2. Extract a program for finding emdedded pairs in sequences of words, and attempt to understand how it works.

Overview of paper

'Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma.'

1. Use the Dialectica interpretation to obtain a constructive version of the classical 'minimal bad sequence' proof of Higman's lemma.
2. Extract a program for finding emdedded pairs in sequences of words, and attempt to understand how it works.
3. Present a case study in which formal program extraction is carried out intuitively - output presented as a mathematical proof.

Overview of paper

'Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma.'

1. Use the Dialectica interpretation to obtain a constructive version of the classical 'minimal bad sequence' proof of Higman's lemma.
2. Extract a program for finding emdedded pairs in sequences of words, and attempt to understand how it works.
3. Present a case study in which formal program extraction is carried out intuitively - output presented as a mathematical proof.
4. Provide some insight into constructive aspects of WQO theory.

Overview of talk

Overview of talk

1. State Higman's lemma and present its classical proof.

Overview of talk

1. State Higman's lemma and present its classical proof.
2. Give a very informal account of how we can extract constructive content from this proof using the Dialectica interpretation.

Overview of talk

1. State Higman's lemma and present its classical proof.
2. Give a very informal account of how we can extract constructive content from this proof using the Dialectica interpretation.

Important things not in talk!

- Details of the Dialectica interpretation.

Overview of talk

1. State Higman's lemma and present its classical proof.
2. Give a very informal account of how we can extract constructive content from this proof using the Dialectica interpretation.

Important things not in talk!

- Details of the Dialectica interpretation.
- Statement of the extracted program.

Overview of talk

1. State Higman's lemma and present its classical proof.
2. Give a very informal account of how we can extract constructive content from this proof using the Dialectica interpretation.

Important things not in talk!

- Details of the Dialectica interpretation.
- Statement of the extracted program.
- A comparison with programs extracted using other methods.

Contents

Well-Quasi-Orders

A preorder $\leq_X$ on X is a reflexive, transitive binary relation. Define a sequence $(x_i)_{i\in\mathbb{N}}$ in X to be bad if we have $x_i \not\leq_X x_j$ for all $i < j$. It is good otherwise.

Well-Quasi-Orders

A preorder $\leq_X$ on X is a reflexive, transitive binary relation. Define a sequence $(x_i)_{i \in \mathbb{N}}$ in X to be bad if we have $x_i \not\leq_X x_j$ for all $i < j$. It is good otherwise.

WQO (Definition 1). A preorder $(X, \leq_X)$ is a well-quasi-order (WQO) if all sequences in X are good i.e. for all sequences $(x_i)_{i \in \mathbb{N}}$ we have $x_i \leq_X x_j$ for some $i < j$.

Well-Quasi-Orders

A preorder $\leq_X$ on X is a reflexive, transitive binary relation. Define a sequence $(x_i)_{i\in\mathbb{N}}$ in X to be bad if we have $x_i \not\leq_X x_j$ for all $i < j$. It is good otherwise.

WQO (Definition 1). A preorder $(X, \leq_X)$ is a well-quasi-order (WQO) if all sequences in X are good i.e. for all sequences $(x_i)_{i\in\mathbb{N}}$ we have $x_i \leq_X x_j$ for some $i < j$.

- A is a WQO whenever A is finite: in any infinite sequence at least one element of A appears twice.

Well-Quasi-Orders

A preorder $\leq_X$ on X is a reflexive, transitive binary relation. Define a sequence $(x_i)_{i\in\mathbb{N}}$ in X to be bad if we have $x_i \not\leq_X x_j$ for all $i < j$. It is good otherwise.

WQO (Definition 1). A preorder $(X, \leq_X)$ is a well-quasi-order (WQO) if all sequences in X are good i.e. for all sequences $(x_i)_{i\in\mathbb{N}}$ we have $x_i \leq_X x_j$ for some $i < j$.

- A is a WQO whenever A is finite: in any infinite sequence at least one element of A appears twice.
- $(\mathbb{N}, \leq)$ is a WQO: by well foundedness of $\mathbb{N}$ there can be no infinite decreasing chains $x_0 > x_1 > \ldots$.

Well-Quasi-Orders

A preorder $\leq_X$ on X is a reflexive, transitive binary relation. Define a sequence $(x_i)_{i \in \mathbb{N}}$ in X to be bad if we have $x_i \not\leq_X x_j$ for all $i < j$. It is good otherwise.

WQO (Definition 1). A preorder $(X, \leq_X)$ is a well-quasi-order (WQO) if all sequences in X are good i.e. for all sequences $(x_i)_{i \in \mathbb{N}}$ we have $x_i \leq_X x_j$ for some $i < j$.

- A is a WQO whenever A is finite: in any infinite sequence at least one element of A appears twice.
- $(\mathbb{N}, \leq)$ is a WQO: by well foundedness of $\mathbb{N}$ there can be no infinite decreasing chains $x_0 > x_1 > \ldots$.
- $(\mathbb{N}, |)$ is *not* a WQO: The prime numbers $2, 3, 5, \ldots$ form an infinite bad sequence.

There are many alternative ways to characterise WQOs:

WQO (Definition 2). $(X, \leq_X)$ is a WQO iff all sequences $(x_i)_{i \in \mathbb{N}}$ in X have an infinite increasing subsequence $x_{g0} \leq x_{g1} \leq x_{g2} \leq \ldots$.

There are many alternative ways to characterise WQOs:

WQO (Definition 2). $(X, \leq_X)$ is a WQO iff all sequences $(x_i)_{i \in \mathbb{N}}$ in X have an infinite increasing subsequence $x_{g0} \leq x_{g1} \leq x_{g2} \leq \ldots$.

- For A finite, by the infinite pigeonhole principle for any infinite sequence in A at least one element appears infinitely often.

There are many alternative ways to characterise WQOs:

WQO (Definition 2). $(X, \leq_X)$ is a WQO iff all sequences $(x_i)_{i\in\mathbb{N}}$ in X have an infinite increasing subsequence $x_{g0} \leq x_{g1} \leq x_{g2} \leq \ldots$.

- For A finite, by the infinite pigeonhole principle for any infinite sequence in A at least one element appears infinitely often.
- Given $(x_i)_{i\in\mathbb{N}}$ in $\mathbb{N}$, define $g0$ such that $x_{g0} := \min\{x_k \colon k \in \mathbb{N}\}$

  Define $g(i+1) > gi$ such that $x_{g(i+1)} := \min\{x_k \colon k > gi\}$.

  Then we must have $x_{g0} \leq x_{g1} \leq \ldots$.

Building new WQOs

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Building new WQOs

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

Building new WQOs

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

X a WQO $\Rightarrow$ $(x_i)_{i \in \mathbb{N}}$ has an infinite increasing subsequence $x_{g0} \leq_X x_{g1} \leq_X x_{g2} \leq \ldots$.

Building new WQOs

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

X a WQO $\Rightarrow$ $(x_i)_{i \in \mathbb{N}}$ has an infinite increasing subsequence $x_{g0} \leq_X x_{g1} \leq_X x_{g2} \leq \ldots$.

Y a WQO $\Rightarrow$ the sequence $(y_{gi})_{i \in \mathbb{N}}$ has $y_{gi} \leq_Y y_{gj}$ for some $i < j$.

Building new WQOs

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

X a WQO $\Rightarrow (x_i)_{i \in \mathbb{N}}$ has an infinite increasing subsequence $x_{g0} \leq_X x_{g1} \leq_X x_{g2} \leq \ldots$.

Y a WQO $\Rightarrow$ the sequence $(y_{gi})_{i \in \mathbb{N}}$ has $y_{gi} \leq_Y y_{gj}$ for some $i < j$.

Therefore $(x_{gi}, y_{gi}) \leq_{X \times Y} (x_{gj}, y_{gj})$. $\square$

Higman's lemma

Given a preorder $(X, \leq_X)$ we can define a preorder $(X^*, \leq_{X^*})$ on *words* over X via the embeddability relation:

$$\langle x_0, \ldots, x_{m-1} \rangle \leq_{X^*} \langle x'_0, \ldots, x'_{n-1} \rangle$$

if there is a strictly increasing map $f \colon [m] \to [n]$ with $x_i \leq_X x'_{fi}$ for all $i < m$.

Higman's lemma

Given a preorder $(X, \leq_X)$ we can define a preorder $(X^*, \leq_{X^*})$ on *words* over X via the embeddability relation:

$$\langle x_0, \ldots, x_{m-1} \rangle \leq_{X^*} \langle x'_0, \ldots, x'_{n-1} \rangle$$

if there is a strictly increasing map $f \colon [m] \to [n]$ with $x_i \leq_X x'_{fi}$ for all $i < m$.

Higman's Lemma (Higman, 1952). If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Classical proof of Higman's lemma

Proof (Nash-Williams, 1963). Suppose that $(u_i)_{i \in \mathbb{N}}$ is a bad sequence in X^*. Using dependent choice, construct a minimal bad sequence $(v_i)_{i \in \mathbb{N}}$ as follows:

Classical proof of Higman's lemma

Proof (Nash-Williams, 1963). Suppose that $(u_i)_{i\in\mathbb{N}}$ is a bad sequence in X^*. Using dependent choice, construct a minimal bad sequence $(v_i)_{i\in\mathbb{N}}$ as follows:

1. v_0 extends to a bad sequence, but no prefix $y \lhd v_0$ extends to a bad sequence;

Classical proof of Higman's lemma

Proof (Nash-Williams, 1963). Suppose that $(u_i)_{i\in\mathbb{N}}$ is a bad sequence in X^*. Using dependent choice, construct a minimal bad sequence $(v_i)_{i\in\mathbb{N}}$ as follows:

1. v_0 extends to a bad sequence, but no prefix $y \lhd v_0$ extends to a bad sequence;
2. given $v_0, \ldots, v_{n-1}$, choose v_n such that $v_0, \ldots, v_{n-1}, v_n$ extends to a bad sequence, but $v_0, \ldots, v_{n-1}, y$ does not for any prefix $y \lhd v_n$.

Classical proof of Higman's lemma

Proof (Nash-Williams, 1963). Suppose that $(u_i)_{i\in\mathbb{N}}$ is a bad sequence in X^*. Using dependent choice, construct a minimal bad sequence $(v_i)_{i\in\mathbb{N}}$ as follows:

1. v_0 extends to a bad sequence, but no prefix $y \lhd v_0$ extends to a bad sequence;
2. given $v_0, \ldots, v_{n-1}$, choose v_n such that $v_0, \ldots, v_{n-1}, v_n$ extends to a bad sequence, but $v_0, \ldots, v_{n-1}, y$ does not for any prefix $y \lhd v_n$.

$(v_i)_{i\in\mathbb{N}}$ bad sequence, minimal under the lexicographic ordering on $(X^*)^\omega$.

Classical proof of Higman's lemma

Each v_i must be non-empty, so we can write $v_i = \tilde{v}_i * x_i$.

Classical proof of Higman's lemma

Each v_i must be non-empty, so we can write $v_i = \tilde{v}_i * x_i$.

X a WQO $\Rightarrow (x_i)_{i \in \mathbb{N}}$ has an infinite increasing subsequence $x_{g0} \leq_X x_{g1} \leq_X x_{g2} \leq \ldots$.

Classical proof of Higman's lemma

Each v_i must be non-empty, so we can write $v_i = \tilde{v}_i * x_i$.

X a WQO $\Rightarrow (x_i)_{i\in\mathbb{N}}$ has an infinite increasing subsequence $x_{g0} \leq_X x_{g1} \leq_X x_{g2} \leq \ldots$.

But then the sequence

$$v_0, \ldots, v_{g0-1}, \tilde{v}_{g0}, \tilde{v}_{g1}, \tilde{v}_{g2}, \ldots$$

is bad, contradicting minimality of $(v_i)_{i\in\mathbb{N}}$. $\square$

Bounds for the length bad sequences

Given a WQO $(X, \leq_X)$ can we produce an explicit functional Γ satisfying

$$\forall x \in X^\omega \exists i < j \leq \Gamma(x)(x_i \leq_X x_j)?$$

Bounds for the length bad sequences

Given a WQO $(X, \leq_X)$ can we produce an explicit functional Γ satisfying

$$\forall x \in X^\omega \exists i < j \leq \Gamma(x)(x_i \leq_X x_j)?$$

- For any $(x_i)_{i \in \mathbb{N}}$ in A we have $x_i = x_j$ for some $i < j \leq |A| + 1$.

Bounds for the length bad sequences

Given a WQO $(X, \leq_X)$ can we produce an explicit functional Γ satisfying

$$\forall x \in X^\omega \exists i < j \leq \Gamma(x)(x_i \leq_X x_j)?$$

- For any $(x_i)_{i\in\mathbb{N}}$ in A we have $x_i = x_j$ for some $i < j \leq |A| + 1$.
- For any $(x_i)_{i\in\mathbb{N}}$ in $\mathbb{N}$ we have $x_i \leq x_j$ for some $i < j \leq x_0 + 2$ (the maximum length of a bad sequence $x_0 > x_1 > \ldots$ is $x_0 + 1$).

Bounds for the length bad sequences

Given a WQO $(X, \leq_X)$ can we produce an explicit functional Γ satisfying

$$\forall x \in X^\omega \exists i < j \leq \Gamma(x)(x_i \leq_X x_j)?$$

- For any $(x_i)_{i \in \mathbb{N}}$ in A we have $x_i = x_j$ for some $i < j \leq |A| + 1$.
- For any $(x_i)_{i \in \mathbb{N}}$ in $\mathbb{N}$ we have $x_i \leq x_j$ for some $i < j \leq x_0 + 2$ (the maximum length of a bad sequence $x_0 > x_1 > \ldots$ is $x_0 + 1$).

Challenge: Analyse the classical proof of Higman's lemma to extract a program Γ_{X^*} bounding bad sequences in $(X^*, \leq_*)$, for arbitrary WQOs $(X, \leq_X)$?

Why Higman's Lemma?

Why Higman's Lemma?

- It has a short, elegant classical proof based on a non-trivial combinatorial idea.

Why Higman's Lemma?

- It has a short, elegant classical proof based on a non-trivial combinatorial idea.
- Minimal bad sequence argument important building block in theory of WQOs, lies behind Kruskal's theorem.

Why Higman's Lemma?

- It has a short, elegant classical proof based on a non-trivial combinatorial idea.
- Minimal bad sequence argument important building block in theory of WQOs, lies behind Kruskal's theorem.
- Higman's lemma has practical implications - termination proofs in rewriting systems.

Why Higman's Lemma?

- It has a short, elegant classical proof based on a non-trivial combinatorial idea.
- Minimal bad sequence argument important building block in theory of WQOs, lies behind Kruskal's theorem.
- Higman's lemma has practical implications - termination proofs in rewriting systems.
- Extensively studied in logic and proof theory.

Contents

Methods of program extraction

Methods of program extraction

Inductive definitions *Reformulation of Nash-Williams' proof using inductive definition of WQO by Coquand and Fridlender (1993), extended to Kruskal's theorem by Seisenberger (2001).*

Methods of program extraction

Inductive definitions *Reformulation of Nash-Williams' proof using inductive definition of WQO by Coquand and Fridlender (1993), extended to Kruskal's theorem by Seisenberger (2001).*

A-**translation and realizability** *Formal program extraction carried out by Murthy (1990), improved and implemented in* MINLOG *by Seisenberger (2003).*

Methods of program extraction

Inductive definitions *Reformulation of Nash-Williams' proof using inductive definition of WQO by Coquand and Fridlender (1993), extended to Kruskal's theorem by Seisenberger (2001).*

A**-translation and realizability** *Formal program extraction carried out by Murthy (1990), improved and implemented in* MINLOG *by Seisenberger (2003).*

Negative translation and Dialectica interpretation

- Maps formulas A to (classically equivalent) formulas $\exists x \forall y A_D(x, y)$.
- If $\mathrm{PA}^\omega \vdash A$ then there exists closed term $t \in \mathrm{T}$ s.t. $\mathrm{T} \vdash A_D(t, y)$.

Dialectica interpretation

Dialectica interpretation

Π_2-formulas

$$\forall x^X \exists y^Y \, A(x,y) \overset{ND}{\mapsto} f^{X \to Y} \, . \, \forall x \, A(x, fx).$$

Can directly extract programs from classical proofs of Π_2 theorems.
How do we interpret ineffective lemmas used in the proof?

Dialectica interpretation

Π_2-formulas

$$\forall x^X \exists y^Y \; A(x, y) \overset{ND}{\mapsto} f^{X \to Y} \, . \, \forall x \; A(x, fx).$$

Can directly extract programs from classical proofs of Π_2 theorems. How do we interpret ineffective lemmas used in the proof?

Σ_2-formulas

$$\begin{aligned} \exists x^X \forall y^Y \; B(x, y) &\overset{N}{\mapsto} \neg\neg \exists x \forall y \; B(x, y) \\ &\leftrightarrow \forall \varphi^{X \to Y} \exists x \; B(x, \varphi x) \\ &\overset{D}{\mapsto} F^{(X \to Y) \to X} \, . \, \forall \varphi A(F\varphi, \varphi(F\varphi)). \end{aligned}$$

φ specifies how x is going to be used in a computation and F constructs an 'approximation' to x based on φ.

In the proof of Higman's lemma, the assumption X is a WQO is used in the sense of Definition 2 i.e. the following ineffective form:

$$\mathrm{MS}[X] \;:\; \forall x^{X^\omega} \exists g^{\mathbb{N}\to\mathbb{N}} \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$$

In the proof of Higman's lemma, the assumption X is a WQO is used in the sense of Definition 2 i.e. the following ineffective form:

$$\mathrm{MS}[X] \,:\, \forall x^{X^\omega} \exists g^{\mathbb{N}\to\mathbb{N}} \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$$
$$\downarrow$$
$$\forall x, \varphi^{\mathbb{N}^\mathbb{N}\to\mathbb{N}} \exists g \forall i < j \leq \varphi g (gi < gj \wedge x_{gi} \leq_X x_{gj})$$

In the proof of Higman's lemma, the assumption X is a WQO is used in the sense of Definition 2 i.e. the following ineffective form:

$$\mathrm{MS}[X] \ : \ \forall x^{X^{\omega}} \exists g^{\mathbb{N}\to\mathbb{N}} \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$$

$$\downarrow$$

$$\forall x, \varphi^{\mathbb{N}^{\mathbb{N}}\to\mathbb{N}} \exists g \forall i < j \leq \varphi g (gi < gj \wedge x_{gi} \leq_X x_{gj})$$

$$\downarrow$$

$$\mathrm{MS}[X]' \ : \ \exists G \forall x, \varphi \forall i < j \leq \varphi(G^x_\varphi)(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$$

In the proof of Higman's lemma, the assumption X is a WQO is used in the sense of Definition 2 i.e. the following ineffective form:

$$\mathrm{MS}[X]\ :\ \forall x^{X^\omega}\exists g^{\mathbb{N}\to\mathbb{N}}\forall k\forall i<j\leq k(gi<gj\wedge x_{gi}\leq_X x_{gj})$$

$$\downarrow$$

$$\forall x,\varphi^{\mathbb{N}^\mathbb{N}\to\mathbb{N}}\exists g\forall i<j\leq\varphi g(gi<gj\wedge x_{gi}\leq_X x_{gj})$$

$$\downarrow$$

$$\mathrm{MS}[X]'\ :\ \exists G\forall x,\varphi\forall i<j\leq\varphi(G^x_\varphi)(Gi<Gj\wedge x_{Gi}\leq_X x_{Gj})$$

WQO (definition 3). $(X,\leq_X)$ is a WQO iff there exists G realizing $\mathrm{MS}[X]'$ i.e. for all sequences $(x_i)_{i\in\mathbb{N}}$ in X have arbitrary high quality approximations to infinite increasing sequences.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

1. X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

1. X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$.
2. Y a WQO $\Rightarrow \exists i < j \leq \Gamma_Y(y_g)(y_{gi} \leq_Y y_{gj})$.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

1. X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$.

2. Y a WQO $\Rightarrow \exists i < j \leq \Gamma_Y(y_g)(y_{gi} \leq_Y y_{gj})$.

Therefore $\exists i < j \leq \Gamma_Y(y_g)(\langle x_{gi}, y_{gi} \rangle \leq_{X \times Y} \langle x_{gj}, y_{gj} \rangle)$.

Theorem. If $(X, \leq_X)$, $(Y, \leq_Y)$ are WQOs, then so is $(X \times Y, \leq_{X \times Y})$.

Proof. Take $(x_i, y_i)_{i \in \mathbb{N}}$ in $X \times Y$.

1. X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge x_{gi} \leq_X x_{gj})$.
2. Y a WQO $\Rightarrow \exists i < j \leq \Gamma_Y(y_g)(y_{gi} \leq_Y y_{gj})$.

Therefore $\exists i < j \leq \Gamma_Y(y_g)(\langle x_{gi}, y_{gi} \rangle \leq_{X \times Y} \langle x_{gj}, y_{gj} \rangle)$.

g ineffectively constructed, but only really need an approximation of g up to $\Gamma_Y(y_g)$.

Constructive version. Given G satisfying $\mathrm{MS}[X]'$ and Γ_Y realizing well-quasi-orderedness of Y we have

$$\exists i < j \leq G^x_\varphi(\Gamma_Y(y_{G^x_\varphi}))(\langle x_i, y_j\rangle \leq_{X\times Y} \langle x_j, y_j\rangle)$$

where $\varphi := \lambda g\ .\ \Gamma_Y(y_g)$.

Constructive version. Given G satisfying MS$[X]'$ and Γ_Y realizing well-quasi-orderedness of Y we have

$$\exists i < j \leq G^x_\varphi(\Gamma_Y(y_{G^x_\varphi}))(\langle x_i, y_j\rangle \leq_{X\times Y} \langle x_j, y_j\rangle)$$

where $\varphi := \lambda g\ .\ \Gamma_Y(y_g)$.

Proof. We have

1. $\forall i < j \leq \varphi G^x_\varphi(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$ i.e. $\forall i < j \leq \Gamma_Y(y_{G^x_\varphi})(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$.

Constructive version. Given G satisfying $\mathrm{MS}[X]'$ and Γ_Y realizing well-quasi-orderedness of Y we have

$$\exists i < j \leq G^x_\varphi(\Gamma_Y(y_{G^x_\varphi}))(\langle x_i, y_j\rangle \leq_{X\times Y} \langle x_j, y_j\rangle)$$

where $\varphi := \lambda g \,.\, \Gamma_Y(y_g)$.

Proof. We have

1. $\forall i < j \leq \varphi G^x_\varphi(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$ i.e.
   $\forall i < j \leq \Gamma_Y(y_{G^x_\varphi})(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$.
2. $\exists i < j \leq \Gamma_Y(y_{G^x_\varphi})(y_{Gi} \leq y_{Gj})$.

Constructive version. Given G satisfying $\mathrm{MS}[X]'$ and Γ_Y realizing well-quasi-orderedness of Y we have

$$\exists i < j \leq G^x_\varphi(\Gamma_Y(y_{G^x_\varphi}))(\langle x_i, y_j\rangle \leq_{X\times Y} \langle x_j, y_j\rangle)$$

where $\varphi := \lambda g\ .\ \Gamma_Y(y_g)$.

Proof. We have

1. $\forall i < j \leq \varphi G^x_\varphi(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$ i.e.
   $\forall i < j \leq \Gamma_Y(y_{G^x_\varphi})(Gi < Gj \wedge x_{Gi} \leq_X x_{Gj})$.

2. $\exists i < j \leq \Gamma_Y(y_{G^x_\varphi})(y_{Gi} \leq y_{Gj})$.

Therefore $\langle x_{Gi}, y_{Gi}\rangle \leq_{X\times Y} \langle x_{Gj}, y_{Gj}\rangle$ for $Gi < Gj \leq G(\Gamma_Y(y_{G^x_\varphi}))$.

Higman's Lemma. If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Higman's Lemma. If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Proof. Suppose that u is a bad sequence in X^*. Using dependent choice, construct $v^i \colon (X^*)^\omega$ and $f^i \colon (X^*)^\omega \to \mathbb{N}$ as follows:

Higman's Lemma. If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Proof. Suppose that u is a bad sequence in X^*. Using dependent choice, construct $v^i : (X^*)^\omega$ and $f^i : (X^*)^\omega \to \mathbb{N}$ as follows:

1. v^0 is bad but for any $y \lhd_0 v^0$ we have $\exists i < j \leq f^0(y)(y_i \leq_{X^*} y_j)$

Higman's Lemma. If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Proof. Suppose that u is a bad sequence in X^*. Using dependent choice, construct $v^i \colon (X^*)^\omega$ and $f^i \colon (X^*)^\omega \to \mathbb{N}$ as follows:

1. v^0 is bad but for any $y \lhd_0 v^0$ we have $\exists i < j \leq f^0(y)(y_i \leq_{X^*} y_j)$
2. $[v^{n-1}](n) = [v^n](n)$ and v^n is bad, but for any $y \lhd_n v^n$ we have $\exists i < j \leq f^n(y)(y_i \leq_{X^*} y_j)$.

Higman's Lemma. If $(X, \leq_X)$ is a WQO then so is $(X^*, \leq_{X^*})$.

Proof. Suppose that u is a bad sequence in X^*. Using dependent choice, construct $v^i\colon (X^*)^\omega$ and $f^i\colon (X^*)^\omega \to \mathbb{N}$ as follows:

1. v^0 is bad but for any $y \lhd_0 v^0$ we have $\exists i < j \leq f^0(y)(y_i \leq_{X^*} y_j)$
2. $[v^{n-1}](n) = [v^n](n)$ and v^n is bad, but for any $y \lhd_n v^n$ we have $\exists i < j \leq f^n(y)(y_i \leq_{X^*} y_j)$.

(v^i_i) is a bad sequence, minimal under the lexicographic ordering on $(X^*)^\omega$.

Each v_j^i must be non-empty, so we can write $v_j^i = \tilde{v}_j^i * \bar{v}_j^i$.

Each v_j^i must be non-empty, so we can write $v_j^i = \tilde{v}_j^i * \bar{v}_j^i$.

X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge \bar{v}_{gi}^{gi} \leq_X \bar{v}_{gj}^{gj})$.

Each v^i_j must be non-empty, so we can write $v^i_j = \tilde{v}^i_j * \bar{v}^i_j$.

X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge \bar{v}^{gi}_{gi} \leq_X \bar{v}^{gj}_{gj})$.

Therefore the sequence $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}^{gi}_{gi})$ must be bad.

Each v^i_j must be non-empty, so we can write $v^i_j = \tilde{v}^i_j * \bar{v}^i_j$.

X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge \bar{v}^{gi}_{gi} \leq_X \bar{v}^{gj}_{gj})$.

Therefore the sequence $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}^{gi}_{gi})$ must be bad.

But by minimality at $g0$, ψ must have one element contained in a later one before $f^{g0}(\psi)$.

Each v_j^i must be non-empty, so we can write $v_j^i = \tilde{v}_j^i * \bar{v}_j^i$.

X a WQO $\Rightarrow \exists g \forall k \forall i < j \leq k (gi < gj \wedge \bar{v}_{gi}^{gi} \leq_X \bar{v}_{gj}^{gj})$.

Therefore the sequence $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}_{gi}^{gi})$ must be bad.

But by minimality at $g0$, ψ must have one element contained in a later one before $f^{g0}(\psi)$.

This implies that $v^{g(f^{g0}(\psi))}$ must have one element contained in a later one before $g(f^{g0}(\psi)) \rightarrow$ **contradiction**.

Monotone sequence g and minimal bad sequence v, f ineffectively constructed, but to obtain contradiction only need

Monotone sequence g and minimal bad sequence v, f ineffectively constructed, but to obtain contradiction only need

- g up to $f^{g0}(\psi)$,

where $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}_{gi}^{gi})$.

Monotone sequence g and minimal bad sequence v, f ineffectively constructed, but to obtain contradiction only need

- g up to $f^{g0}(\psi)$,
- v up to $g(f^{g0}(\psi))$ and of length $g(f^{g0}(\psi))$,

where $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}^{gi}_{gi})$.

Monotone sequence g and minimal bad sequence v, f ineffectively constructed, but to obtain contradiction only need

- g up to $f^{g0}(\psi)$,
- v up to $g(f^{g0}(\psi))$ and of length $g(f^{g0}(\psi))$,
- f^{g0} applied to ψ.

where $\psi_{g,v} := [v^{g0-1}](g0) * (\tilde{v}^{gi}_{gi})$.

Higman's lemma (constructive version): Given any G satisfying $\mathrm{MS}[X]'$ there exists $\Gamma_{X^*} : (X^*)^\omega \to \mathbb{N}$ satisfying

$$\forall u^{(X^*)^\omega} \exists i < j \leq \Gamma_{X^*}(u)(u_i \leq_{X^*} u_j).$$

Proof.

Higman's lemma (constructive version): Given any G satisfying $\mathrm{MS}[X]'$ there exists $\Gamma_{X^*} : (X^*)^\omega \to \mathbb{N}$ satisfying

$$\forall u^{(X^*)^\omega} \exists i < j \leq \Gamma_{X^*}(u)(u_i \leq_{X^*} u_j).$$

Proof.

1. Interpret minimal bad sequence argument: find procedure for producing 'approximations' to minimal bad sequences.

Higman's lemma (constructive version): Given any G satisfying $\mathrm{MS}[X]'$ there exists $\Gamma_{X^*} : (X^*)^\omega \to \mathbb{N}$ satisfying

$$\forall u^{(X^*)^\omega} \exists i < j \leq \Gamma_{X^*}(u)(u_i \leq_{X^*} u_j).$$

Proof.

1. Interpret minimal bad sequence argument: find procedure for producing 'approximations' to minimal bad sequences.

2. Calibrate approximations of g and minimal bad sequence required to obtain contradiction.

Higman's lemma (constructive version): Given any G satisfying $\mathrm{MS}[X]'$ there exists $\Gamma_{X^*} : (X^*)^\omega \to \mathbb{N}$ satisfying

$$\forall u^{(X^*)^\omega} \exists i < j \leq \Gamma_{X^*}(u)(u_i \leq_{X^*} u_j).$$

Proof.

1. Interpret minimal bad sequence argument: find procedure for producing 'approximations' to minimal bad sequences.
2. Calibrate approximations of g and minimal bad sequence required to obtain contradiction.
3. Work backwards from contradiction to obtain bound for u.

Interpreting minimal bad sequence construction

Central part of program extraction! Details in paper...

System T no longer sufficient to interpret dependent choice...

dependent choice $\mapsto$ bar recursion

Interpreting minimal bad sequence construction

Central part of program extraction! Details in paper...

System T no longer sufficient to interpret dependent choice...

dependent choice $\mapsto$ bar recursion (product of selection functions)

Novelty: Use recently discovered *product of selection functions*, form of bar recursion with natural game theoretic semantics.

Interpreting minimal bad sequence construction

Central part of program extraction! Details in paper...

System T no longer sufficient to interpret dependent choice...

dependent choice $\mapsto$ bar recursion (product of selection functions)

Novelty: Use recently discovered *product of selection functions*, form of bar recursion with natural game theoretic semantics.

Question. Can we construct direct realizer for minimal bad sequence argument, and does it lead to a more intuitive/efficient program?

Further comments

Further comments

- Can we understand algorithm in qualitative terms - unwrap the syntax and appreciate its operational behaviour?

Further comments

- Can we understand algorithm in qualitative terms - unwrap the syntax and appreciate its operational behaviour?
- How does it compare, both qualitatively and in terms of efficiency to programs extracted using other methods?

Further comments

- Can we understand algorithm in qualitative terms - unwrap the syntax and appreciate its operational behaviour?
- How does it compare, both qualitatively and in terms of efficiency to programs extracted using other methods?
- It would be intructive to formalise this work in a theorem prover, and test the extracted program on some explicit examples.

Further comments

- Can we understand algorithm in qualitative terms - unwrap the syntax and appreciate its operational behaviour?
- How does it compare, both qualitatively and in terms of efficiency to programs extracted using other methods?
- It would be intructive to formalise this work in a theorem prover, and test the extracted program on some explicit examples.
- Does our program yield any new quantitative information i.e. new bounds for length of bad sequences?

Further comments

- Can we understand algorithm in qualitative terms - unwrap the syntax and appreciate its operational behaviour?
- How does it compare, both qualitatively and in terms of efficiency to programs extracted using other methods?
- It would be intructive to formalise this work in a theorem prover, and test the extracted program on some explicit examples.
- Does our program yield any new quantitative information i.e. new bounds for length of bad sequences?
- Can we interpret general minimal bad sequence argument and extract programs from more complex proofs like Kruskal's theorem?

References

Higman's lemma

G. Higman. Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. 2:326-336.* 1952

C. St. J. A. Nash-Williams. On well-quasi-ordering finite trees. *Proc. Cambridge Phil. Soc. 59:833-835.* 1963

Constructive proofs of Higman's lemma

U. Berger and M. Seisenberger. Applications of inductive definitions and choice principles to program synthesis. *From Sets and Types to Topology and Analysis, Oxford Logic Guides 48:137-148.* 2005.

T. Coquand and D. Fridlender. A proof of Higman's lemma by structural induction. *Unpublished manuscript, available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.47.486.* 1993.

C. Murthy. Extracting constructive content from classical proofs. *Ph.D. thesis , Cornell University.* 1990.

M. Seisenberger. On the constructive content of proofs. *Ph. D. thesis, Ludwigs-Maximilians-Universität München.* 2003.

Dialectica interpretation and product of selection functions

K. Gödel. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. *Dialectica. 12:280287.* 1958.

P. Oliva and T. Powell A game-theoretic computational interpretation of proofs in classical analysis. *Preprint, available at http://arxiv.org/abs/1204.5244.* 2012.