Solving constraints in ordinals

Frédéric Blanqui

Deduc⊢eam

Which kind of constraints?

$$\underbrace{(\forall \vec{\alpha}) a < b}_{\Pi_1^0 \text{ formula}} \quad | \quad \underbrace{\overbrace{(\forall \vec{\alpha})\,(\exists \vec{\beta})\,\bigwedge_{i=1}^{n} a_i \leq b_i}^{\Sigma_1^0 \text{ formula}}}_{\Pi_2^0 \text{ formula}}$$

where:

- $a = \alpha \mid a + 1 \mid \infty$ with $\infty + 1 \simeq \infty$
- variables in some initial segment of ordinals $[0, \infty]$

in addition, we need:

- if there is a solution, there is a smallest one
- the smallest solution is syntactically expressible

Outline

Termination of typed higher-order rewrite systems

given a set $\mathcal{R}$ of rewrite rules $\mathsf{f}\vec{l} \to r$,
does $\to_\beta \cup \to_{\mathcal{R}}$ terminates on well-typed terms?

in 1996, Hughes, Pareto & Sabry proposed to use typing
to reason on the size of terms:

- add a type L_a for lists of size $\leq a$
- this induces a subtyping relation $\mathsf{L}_a \leq \mathsf{L}_b$ if $a \leq b$
- typing rules become deduction rules on the size of terms:

$$\frac{t : \mathsf{L}_a \to \mathsf{L}_b \quad u : \mathsf{L}_a}{tu : \mathsf{L}_b}$$

Reducing termination to type-checking & decreasingness

$\to_\beta \cup \to_{\mathcal{R}}$ terminates if

for all $\mathsf{f} : (\forall\beta)\mathsf{L}_\beta \to T(\beta)$,

for all rules $\mathsf{f}(l) \to r \in \mathcal{R}$,

for all size variables $\vec{\alpha}$ and $\Gamma = x_1 : \mathsf{L}_{\alpha_1}, \ldots, x_k : \mathsf{L}_{\alpha_k}$,

for all sizes b such that $\Gamma \vdash l : L_b$,

1. $\Gamma \vdash r : T(b)$ [preservation of typing & size bound by rewriting]
2. for all calls $\mathsf{f}(m)$ in r with $\Gamma \vdash m : \mathsf{L}_c$, we have $c < b$

example: $\mathsf{f}(\underbrace{\mathsf{cons}\ x\ \underbrace{l}_{\text{of size } \alpha}}_{\text{of size } \alpha+1}) \to \mathsf{f}(\underbrace{\mathsf{map}\ \mathsf{g}\ l}_{\text{of size } \alpha})$

with $\mathsf{map} : (\forall\beta)(T \to T) \to \mathsf{L}_\beta \to \mathsf{L}_\beta$

How to check $t : T$ without subtyping?

in 1969, Hindley showed that $\{T \mid t : T\}$ has a smallest element wrt the instantiation quasi-ordering $T \sqsubseteq U$ if $(\exists\theta)T\theta = U$

$t : T$ decided by

1. inferring the smallest type of t, say T'
2. checking that $T' \sqsubseteq T$

how to compute the smallest type of a function call $\mathrm{f}(m)$?

1. infer the smallest type of f, say C
2. check that C is of the form $A \to B$
3. infer the smallest type of m, say A'
4. check that A and A' are unifiable: $(\exists\theta)A\theta = A'\theta$
5. return $B\theta$ where $\theta = \mathrm{mgu}\{A =^? A'\}$

How to check $t : T$ with~~out~~ subtyping?

replace $=$ by $\leq$: let $T \sqsubseteq U$ if ~~$(\exists\theta)\, T\theta = U$~~ $(\exists\theta)\, T\theta \leq U$

$t : T$ decided by

1. inferring the smallest type of t, say T'
2. and checking that $T' \sqsubseteq T$

how to infer the type of a function call f(m)?

1. infer the smallest type of f, say C
2. check that C is of the form $A \to B$
3. infer the smallest type of m, say A'
4. check that ~~$(\exists\theta)\, A\theta = A'\theta$~~ $(\exists\theta)\, A\theta \leq A'\theta$
5. return $B\theta$ where ~~$\theta = \mathrm{mgu}\{A =^? A'\}$~~ $\theta = \mathrm{mgs}\{A \leq^? A'\}$

Reducing subtyping constraints to size constraints

$$\frac{a \leq b}{\mathsf{L}_a \leq \mathsf{L}_b} \qquad \frac{T' \leq T \quad U \leq U'}{T \to U \leq T' \to U'}$$

- because of subtyping rules $T \leq U \Leftrightarrow \bigwedge_{i=1}^{n} a_i \leq b_i$
- because functions have types of the form $(\forall\beta)\mathsf{L}_\beta \to T(\beta)$
  type inference generates problems of the form $(\exists\vec{\beta}) \bigwedge_{i=1}^{n} a_i \leq b_i$
- hence, the termination criterion generates problems of the form $(\forall\vec{\alpha})(\exists\vec{\beta}) \bigwedge_{i=1}^{n} a_i \leq b_i$ or $(\forall\vec{\alpha})a < b$

Solving constraints of the form $(\forall\vec{\alpha})(\exists\vec{\beta})\bigwedge_{i=1}^{n} a_i \leq b_i$

$(\forall\vec{\alpha})(\exists\vec{\beta})P(\vec{\alpha},\vec{\beta}) \Leftrightarrow (\exists\vec{f})(\forall\vec{\alpha})P(\vec{\alpha},\overrightarrow{f(\vec{\alpha})})$ by the Axiom of Choice

1. replace $\vec{\alpha}$ by fresh constants $\vec{c}$
2. find terms $\vec{b}$ such that $P(\vec{c},\vec{b})$
   whatever the interpretations of $\vec{c}$ are

Outline

Successor algebra $\mathtt{A}^\infty$

$\mathtt{A}^\infty = \mathtt{A} \cup \{\infty\}$ where $\mathtt{A}$ is the first-order term algebra with:

- variables α, β, ...
- a unary symbol $\mathsf{s} : \mathtt{A} \to \mathtt{A}$ for successor
- an infinite set of constants c, d, ...

$\Rightarrow$ every term a is of one of the following forms:

a	∞	$\mathsf{s}^k\alpha$	$\mathsf{s}^k\mathsf{c}$
$\mathrm{base}(a)$	∞	α	c

Order on the successor algebra

$$[(\forall\vec{\alpha})a \leq b] \Leftrightarrow [a\kappa \leq^{\infty}_{\mathtt{A}} b\kappa]$$

where:

- $\kappa = \{\vec{\alpha} \mapsto \vec{c}\}$
- $t \leq^{\infty}_{\mathtt{A}} u \Leftrightarrow t \leq_{\mathtt{A}} u \vee u = \infty$
- $$\frac{}{t \leq_{\mathtt{A}} t} \qquad \frac{t <_{\mathtt{A}} u}{t \leq_{\mathtt{A}} u} \qquad \frac{}{t <_{\mathtt{A}} \mathtt{s}\, t} \qquad \frac{t <_{\mathtt{A}} u \quad u <_{\mathtt{A}} v}{t <_{\mathtt{A}} v}$$

so:

$$[(\forall\vec{\alpha})(\exists\vec{\beta}) \bigwedge_{i=1}^{n} a_i \leq b_i] \Leftrightarrow [(\exists\vec{\beta}) \bigwedge_{i=1}^{n} a_i\kappa \leq^{\infty}_{\mathtt{A}} b_i\kappa]$$

Graph representation of a problem $P = \{a_1 \leq^? b_1, \ldots\}$

$$\mathtt{s}^k g \leq^? \mathtt{s}^l h \in P \quad \Leftrightarrow \quad g \xrightarrow{k-l} h \in \mathrm{Graph}(P) \quad \Rightarrow \quad g \leq_P h$$

example:

$$\begin{array}{l} \mathtt{s}\alpha \leq_{\mathtt{A}}^{\infty ?} \beta \\ \beta \leq_{\mathtt{A}}^{\infty ?} \mathtt{s}^2\alpha \\ \infty \leq_{\mathtt{A}}^{\infty ?} \alpha \\ \beta \leq_{\mathtt{A}}^{\infty ?} \mathtt{s}\mathtt{c} \end{array} \qquad \infty \longrightarrow \alpha \underset{\xleftarrow{-2}}{\xrightarrow{1}} \beta \xrightarrow{-1} \mathtt{c}$$

Satisfiability when there is no constant c, d, ...

a problem with n variables is equivalent to $mx \oplus v \leq x$ with x in $(\overline{\mathbb{Z}}_{\max}^n, \oplus, \otimes)$ where $\overline{\mathbb{Z}}_{\max} = \mathbb{Z} \cup \{\pm\infty\}$, $\oplus = \max$ and $\otimes = +$

example: for $\{\mathsf{s}\alpha \leq^? \beta, \beta \leq^? \mathsf{s}^2\alpha, \infty \leq^? \alpha\}$,
take $x = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, $m = \begin{pmatrix}-\infty & -2\\ 1 & -\infty\end{pmatrix}$, $v = \begin{pmatrix}+\infty\\ -\infty\end{pmatrix}$

$$\begin{array}{rcl}\alpha+1 & \leq & \beta\\ \beta & \leq & \alpha+2\\ +\infty & \leq & \alpha\end{array} \rightsquigarrow \begin{array}{rcl}\beta-2 & \leq & \alpha\\ +\infty & \leq & \alpha\\ \alpha+1 & \leq & \beta\end{array} \rightsquigarrow \begin{array}{rcl}-2\otimes\beta\oplus+\infty & \leq & \alpha\\ 1\otimes\alpha & \leq & \beta\end{array}$$

$$\rightsquigarrow \begin{array}{rcl}-\infty\otimes\alpha\oplus\ -2\otimes\beta\oplus+\infty & \leq & \alpha\\ 1\otimes\alpha\oplus-\infty\otimes\beta\oplus-\infty & \leq & \beta\end{array}$$

Satisfiability when there is no constant c, d, ...

after [C79], [BCOQ92], [ABG14] (Hankbook of linear algebra):

theorem 1: $ax \oplus b \leq x$ has smallest solution $a^* b$ with $a^* = \bigoplus_{i=0}^{\infty} a^i$

(in $(\mathbb{R}, +, \times)$, $x = \frac{b}{1-a} = b \cdot \sum_{i=0}^{\infty} a^i$)

theorem 2: $a^* = \bigoplus_{i=0}^{n} a^i$ if there is no positive cycle

Dealing with constants

solutions of $\{\alpha \leq^? \mathtt{s}^l\mathtt{c}\}$? substitutions $\{(\alpha, \mathtt{s}^k\mathtt{c})\}$ with $0 \leq k \leq l$

step 1: extend $\mathtt{A}$ with

- a sort $\mathtt{N}$ for natural numbers with $\mathtt{0}_\mathtt{N} : \mathtt{N}$ and $\mathtt{s}_\mathtt{N} : \mathtt{N} \to \mathtt{N}$
- a function symbol $\mathtt{i} : \mathtt{N} \to \mathtt{A} \to \mathtt{A}$ for successor iteration with $\mathtt{i}x\alpha$ written $\mathtt{s}^x\alpha$

$$[\alpha \leq^? \mathtt{s}^l\mathtt{c}] \Leftrightarrow [\alpha =^? \mathtt{s}^{\mathrm{x}_\alpha}\mathtt{c} \wedge \mathrm{x}_\alpha \leq^? l]$$

modulo normalization rules (e.g. $\mathtt{i}(\mathtt{s}_\mathtt{N}x)\alpha = \mathtt{s}(\mathtt{i}x\alpha)$),
a term is either: ∞, $\mathtt{s}^k\alpha$ or $\mathtt{s}^e\mathtt{c}$ with $e \in \{k, k + \mathrm{x}_\alpha\}$

step 2: transform P into an equivalent problem on $\overline{\mathbb{Z}}_{\max}$

Transformation rules

simplification rules:

$$P \uplus \{\mathtt{s}\, a \leq^? \mathtt{s}\, b\} \rightarrow P \cup \{a \leq^? b\}$$
$$P \uplus \{\mathtt{s}^e \mathtt{c} \leq^? \mathtt{s}^f \mathtt{c}\} \rightarrow P \cup \{e \leq^? f\}$$
$$P \uplus \{\infty \leq^? \mathtt{s}^{\mathtt{s}e}\alpha\} \rightarrow P \cup \{\infty \leq^? \alpha\}$$

constraints always true:

$$P \uplus \{a \leq^? \infty\} \rightarrow P \cup \{\alpha \leq^? \infty \mid \alpha \in \mathrm{Var}(a) - \mathrm{Var}(P)\}$$
if $a \notin \mathtt{X} \vee a \in \mathrm{Var}(P)$
$$P \uplus \{a \leq^? \mathtt{s}^e a\} \rightarrow P \cup \{\alpha \leq^? \infty \mid \alpha \in \mathrm{Var}(a) - \mathrm{Var}(P)\}$$

constraints always false:

$$P \uplus \{\infty \leq^? \mathtt{s}^e \mathtt{c}\} \rightarrow \bot$$
$$P \uplus \{\mathtt{s}^{\mathtt{s}e}\alpha \leq^? \mathtt{c}\} \rightarrow \bot$$
$$P \uplus \{\mathtt{s}^e \mathtt{c} \leq^? \mathtt{s}^f \mathtt{d}\} \rightarrow \bot \text{ if } \mathtt{c} \neq \mathtt{d}$$
$$P \uplus Q \rightarrow \bot \text{ if } \mathrm{Var}_{\mathtt{A}}(Q) = \emptyset \text{ and } \mathrm{Sol}(Q) = \emptyset$$

Transformation rules

variables that must be set to ∞:

$$P \uplus \{\infty \leq^? \alpha\} \rightarrow P\{(\alpha, \infty)\} \cup \{\infty \leq^? \alpha\} \quad \text{if } \alpha \in \mathrm{Var}(P)$$

$$P \uplus \{\mathtt{s}^{\mathtt{se}}\alpha \leq^? \alpha\} \rightarrow P\{(\alpha, \infty)\} \cup \{\infty \leq^? \alpha\}$$

$$P \uplus Q \rightarrow P\{(\alpha, \infty) \mid \alpha \in \mathrm{Var}(Q)\} \cup \{\infty \leq^? \alpha \mid \alpha \in \mathrm{Var}(Q)\} \quad \text{if } \mathrm{Graph}(Q) \text{ is a positive cycle}$$

$$P \rightarrow P\{(\alpha, \infty)\} \cup \{\infty \leq^? \alpha\} \quad \text{if } \mathtt{c} \leq_P \alpha, \mathtt{d} \leq_P \alpha, \mathtt{c} \neq \mathtt{d}$$

variables that must be set to a constant:

$$P \uplus \{\mathtt{s}^k\alpha \leq^? \mathtt{s}^e\mathtt{c}\} \rightarrow P\{(\alpha, \mathtt{s}^{\mathrm{x}_\alpha}\mathtt{c})\} \cup \{\alpha =^? \mathtt{s}^{\mathrm{x}_\alpha}\mathtt{c}, k + \mathrm{x}_\alpha \leq^? e\} \quad \text{if } (k, e) \neq (0, \mathrm{x}_\alpha)$$

theorem: the rules terminate, are correct and complete

Problems in normal form

after normalization, we get $\bot$ or an affine problem:

- constraints are of the form $\mathtt{s}^k\alpha \leq^? \mathtt{s}^l\beta$ or $\mathtt{s}^e\mathtt{c} \leq^? \mathtt{s}^m\beta$
- there is no positive cycle
- there is no tuple $(\alpha, \mathtt{c}, \mathtt{d})$ such that $\mathtt{c} \leq_P \alpha$, $\mathtt{d} \leq_P \alpha$ and $\mathtt{c} \neq \mathtt{d}$
  $\Rightarrow$ an equivalence class modulo $\simeq_P$ contains at most 1 constant

theorem 1: an affine problem is always satisfiable (with $\varphi = \infty$)

Normalized problems

theorem 2: the finite solutions are isomorphic to the solutions of the integer problem obtained by replacing constants with 0

example: $P = \{\mathtt{s}^k\alpha \leq^? \mathtt{s}^l\beta, \mathtt{s}^e\mathtt{c} \leq^? \mathtt{s}^m\beta\}$ is mapped to
$Q = \{k + \alpha \leq^? l + \beta, e \leq^? m + \beta\}$
from $\psi \in \mathrm{Sol}(Q)$, we get $\widehat{\psi} \in \mathrm{Sol}(P)$ by taking $\alpha\widehat{\psi} = \mathtt{s}^{\alpha\psi}\chi([\alpha]_{\simeq_P})$
where $\chi : \mathcal{F}/\simeq_P \to \mathcal{F}$ is a choice function with $\chi(E) = \mathtt{c}$ if $\mathtt{c} \in E$

theorem 3: an integer problem with at most 2 variables per constraint and no positive cycle has a smallest solution

Satisfiability of a problem in the successor algebra

1. P is satisfiable iff any normal form of P is distinct from $\bot$
2. satisfiability is decidable in polynomial time
3. every satisfiable problem has a smallest solution
4. the smallest solution is computable in polynomial time

Next?

extend the algebra $\mathtt{A}$ with:

- a constant $0 : \mathtt{A}$ for zero (then $0 \leq c \ldots$)
- an operator $\mathtt{max} : \mathtt{A} \to \mathtt{A} \to \mathtt{A}$
- addition $\mathtt{add} : \mathtt{A} \to \mathtt{A} \to \mathtt{A}$