Reducing the Complexity of Quantified Formulas via Variable Elimination

Aboubakr Achraf El Ghazi, Mattias Ulbrich, Mana Taghdiri, Mihai Herda

Karlsruhe Institute of Technology, Germany

SMT 2013
Helsinki, July 9

Motivation

Modelling with Quantifiers

Quantifier blasting vs. Quantifier engine

Reduced/Minimal Quantifier blasting vs. Heuristic instantiation

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} fGT(f,1) \supseteq \{c_1, c_4\}, \\ fGT(p,1) \supseteq \emptyset, \\ vGT(x) = fGT(f,1), \\ vGT(y) = fGT(f,1), vGT(y) = fGT(p,1) \end{array}\right\} \text{Instantiation sets}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} fGT(f,1) \supseteq \{c_1, c_4\}, \\ fGT(p,1) \supseteq \emptyset, \\ vGT(x) = fGT(f,1), \\ vGT(y) = fGT(f,1), vGT(y) = fGT(p,1) \end{array}\right\} \text{Instantiation sets}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} fGT(f,1) \supseteq \{c_1, c_4\}, \\ fGT(p,1) \supseteq \emptyset, \\ vGT(x) = fGT(f,1), \\ vGT(y) = fGT(f,1), vGT(y) = fGT(p,1) \end{array}\right\} \text{Instantiation sets}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} fGT(f,1) \supseteq \{c_1, c_4\}, \\ fGT(p,1) \supseteq \emptyset, \\ vGT(x) = fGT(f,1), \\ vGT(y) = fGT(f,1), vGT(y) = fGT(p,1) \end{array}\right\} \text{Instantiation sets}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} fGT(f,1) \supseteq \{c_1, c_4\}, \\ fGT(p,1) \supseteq \emptyset, \\ vGT(x) = fGT(f,1), \\ vGT(y) = fGT(f,1), vGT(y) = fGT(p,1) \\ \Rightarrow \\ vGT(x) = \{c_1, c_4\}, \\ vGT(y) = \{c_1, c_4\} \cup \emptyset \end{array}\right\} \text{Instantiation sets}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} vGT(x) = \{c_1, c_4\}, \\ vGT(y) = \{c_1, c_4\} \cup \emptyset \end{array}\right\} \text{Instantiation sets}$$

$$\left.\begin{array}{l} c_1 \neq c_2 \\ f(c_1) = f(c_1) \\ f(c_4) = f(c_1) \\ \neg p(c_1, c_3) \vee f(c_1) = c_2 \\ \neg p(c_4, c_3) \vee f(c_4) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A^{inst}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg p(y, c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} c_1 \neq c_2 \\ f(c_1) = f(c_1) \\ f(c_4) = f(c_1) \\ \neg p(c_1, c_3) \vee f(c_1) = c_2 \\ \neg p(c_4, c_3) \vee f(c_4) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A^{inst}$$

$$M(c_1) = 1, M(c_2) = 2, M(c_3) = 3, M(c_4) = 4$$

$$M(f)(v) = \begin{cases} 1 & \textit{if } v = 1 \\ 1 & \textit{if } v = 4 \\ 2 & \textit{else} \end{cases}$$

$$M^{\pi}(c_1) = 1, M^{\pi}(c_2) = 2, M^{\pi}(c_3) = 3, M^{\pi}(c_4) = 4$$

$$M^{\pi}(f)(v) = \begin{cases} M(f)(v) & \textit{if } v \in \{1, 4\} \\ M(f)(M(c_1)) & \textit{else} \end{cases}$$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg(y \leq c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} c_1 \neq c_2 \\ f(c_1) = f(c_1) \\ f(c_4) = f(c_1) \\ \neg(c_1 \leq c_3) \vee f(c_1) = c_2 \\ \neg(c_4 \leq c_3) \vee f(c_4) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A^{inst}$$

- What if f or p are interpreted?
- Assume that p is "$\leq$",
  - A becomes unsat, but A^{inst} stays sat
  - To detect unsat an additional gt, such that $\neg(gt \leq c_3)$, is needed
  - Exp. $vGT(y) = \{c_1, c_4, c_3 - 1\}$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg(y \leq c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} c_1 \neq c_2 \\ f(c_1) = f(c_1) \\ f(c_4) = f(c_1) \\ \neg(c_1 \leq c_3) \vee f(c_1) = c_2 \\ \neg(c_4 \leq c_3) \vee f(c_4) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A^{inst}$$

$$f(c_1) = f(c_4) \wedge f(c_4) = c_1 \wedge c_1 \neq c_2 \Rightarrow f(c_1) \neq c_2$$
$$f(c_1) = f(c_3 - 1) \wedge f(c_3 - 1) = c_2 \Rightarrow f(c_1) = c_2$$

- What if f or p are interpreted?
- Assume that p is "$\leq$",
  - A becomes unsat, but A^{inst} stays sat
  - To detect unsat an additional gt, such that $\neg(gt \leq c_3)$, is needed
  - Exp. $vGT(y) = \{c_1, c_4, c_3 - 1\}$

Example

$$\left.\begin{array}{l} c_1 \neq c_2 \\ \forall x \mid f(x) = f(c_1) \\ \forall y \mid \neg(y \leq c_3) \vee f(y) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A$$

$$\left.\begin{array}{l} c_1 \neq c_2 \\ f(c_1) = f(c_1) \\ f(c_4) = f(c_1) \\ \neg(c_1 \leq c_3) \vee f(c_1) = c_2 \\ \neg(c_4 \leq c_3) \vee f(c_4) = c_2 \\ f(c_4) = c_1 \end{array}\right\} A^{inst}$$

$$M'(c_1) = 1, M'(c_2) = 2, M'(c_3) = 0, M'(c_4) = 4, M'(f) \equiv 1$$

- What if f or p are interpreted?
- Assume that p is "$\leq$",
  - A becomes unsat, but A^{inst} stays sat
  - To detect unsat an additional gt, such that $\neg(gt \leq c_3)$, is needed
  - Exp. $vGT(y) = \{c_1, c_4, c_3 - 1\}$

Sufficient Ground Term Sets

Definition

Given a variable x in an SMT formula A (in CNF), a set of ground terms $S \subseteq \mathcal{H}(A)$[1] is *sufficient* for x w.r.t a theory $\mathcal{T}$ if A and $A[S/x]$ are equisatisfiable modulo $\mathcal{T}$.

- $\mathcal{H}(A)$ is always a sufficient set of ground terms (Gödel-Herbrand-Skolem)
- $\mathcal{H}(A)$ is usually infinite
- When can we find a finite sufficient ground term set for x?
- How can we calculate it?

[1] $\mathcal{H}(A)$ means the Herbrand universe of A

System of Set Constraints

Given a formula A we construct a system of set constraints $\mathcal{S}_\mathcal{A}$

- over ground term set variables $vGT(x)$, for each variable x in A,
- and $fGT(f, i)$, for each function f and argument position i
- The solution of $\mathcal{S}_\mathcal{A}$ is an assignment
  - of ground term sets $vGT(x)_{\mathcal{S}_A}$ to each set variable $vGT(x)$,
  - such that all constraints in $\mathcal{S}_\mathcal{A}$ hold

Rules for $\mathcal{S}_{\mathcal{A}}$

$$\mathsf{R}_0: \frac{x \dot{\in} C}{vGT(x) \neq \emptyset} \qquad \mathsf{R}_1: \frac{f(\cdots, \overbrace{x}^{\text{i-th}}, \cdots) \dot{\in} C}{vGT(x) = fGT(f, i)} \qquad \mathsf{R}_2: \frac{f(\cdots, \overbrace{gt}^{\text{i-th}}, \cdots) \dot{\in} C}{gt \in fGT(f, i)}$$

$$\mathsf{R}_3: \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \dot{\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f, i)}$$

$$\mathsf{R}_4: \frac{op(\cdots, x, \cdots) \in C,\ op \notin \{=, <, \leq, >, \geq\}}{vGT(x) = \infty} \qquad \mathsf{R}_5: \frac{op(x, y) \in C,\ op \in \{=, <, \leq, >, \geq\}}{vGT(x) = \infty \quad vGT(y) = \infty}$$

$$\mathsf{R}_6: \frac{(x \leq gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathsf{R}_7: \frac{(x \geq gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathsf{R}_8: \frac{\neg op(x, gt) \in C, where\ op \in \{\leq, \geq\}}{gt \in vGT(x)}$$

$$\mathsf{R}_9: \frac{\neg(x < gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathsf{R}_{10}: \frac{\neg(x > gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathsf{R}_{11}: \frac{op(x, gt) \in C, where\ op \in \{<, >\}}{gt \in vGT(x)}$$

$$\mathsf{R}_{12}: \frac{\neg(x = gt) \in C}{gt \in vGT(x)} \qquad \mathsf{R}_{13}: \frac{(x = gt) \in C, x \in \mathbb{Z}}{\{gt - 1, gt + 1\} \subseteq vGT(x)} \qquad \mathsf{R}_{14}: \frac{(x = gt) \in C, x \notin \mathbb{Z}}{vGT(x) = \infty}$$

Rules for $\mathcal{S}_{\mathcal{A}}$

$$\mathrm{R}_0: \frac{x \dot{\in} C}{vGT(x) \neq \emptyset} \qquad \mathrm{R}_1: \frac{f(\cdots, \overbrace{x}^{\text{i-th}}, \cdots) \dot{\in} C}{vGT(x) = fGT(f,i)} \qquad \mathrm{R}_2: \frac{f(\cdots, \overbrace{gt}^{\text{i-th}}, \cdots) \dot{\in} C}{gt \in fGT(f,i)}$$

$$\mathrm{R}_3: \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \dot{\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f,i)}$$

$$\mathrm{R}_4: \frac{op(\cdots, x, \cdots) \in C,\ op \notin \{=, <, \leq, >, \geq\}}{vGT(x) = \infty} \qquad \mathrm{R}_5: \frac{op(x,y) \in C,\ op \in \{=, <, \leq, >, \geq\}}{vGT(x) = \infty \quad vGT(y) = \infty}$$

$$\mathrm{R}_6: \frac{(x \leq gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_7: \frac{(x \geq gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_8: \frac{\neg op(x, gt) \in C, where\ op \in \{\leq, \geq\}}{gt \in vGT(x)}$$

$$\mathrm{R}_9: \frac{\neg(x < gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_{10}: \frac{\neg(x > gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_{11}: \frac{op(x, gt) \in C, where\ op \in \{<, >\}}{gt \in vGT(x)}$$

$$\mathrm{R}_{12}: \frac{\neg(x = gt) \in C}{gt \in vGT(x)} \qquad \mathrm{R}_{13}: \frac{(x = gt) \in C, x \in \mathbb{Z}}{\{gt - 1, gt + 1\} \subseteq vGT(x)} \qquad \mathrm{R}_{14}: \frac{(x = gt) \in C, x \notin \mathbb{Z}}{vGT(x) = \infty}$$

Rules for $\mathcal{S}_A$

$$\mathrm{R}_0: \frac{x \dot{\in} C}{vGT(x) \neq \emptyset} \qquad \mathrm{R}_1: \frac{f(\cdots, \overbrace{x}^{\text{i-th}}, \cdots) \dot{\in} C}{vGT(x) = fGT(f,i)} \qquad \mathrm{R}_2: \frac{f(\cdots, \overbrace{gt}^{\text{i-th}}, \cdots) \dot{\in} C}{gt \in fGT(f,i)}$$

$$\mathrm{R}_3: \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \dot{\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f,i)}$$

$$\mathrm{R}_4: \frac{op(\cdots, x, \cdots) \in C,\ op \notin \{=, <, \leq, >, \geq\}}{vGT(x) = \infty} \qquad \mathrm{R}_5: \frac{op(x,y) \in C,\ op \in \{=, <, \leq, >, \geq\}}{vGT(x) = \infty \quad vGT(y) = \infty}$$

$$\mathrm{R}_6: \frac{(x \leq gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_7: \frac{(x \geq gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_8: \frac{\neg op(x, gt) \in C, where\ op \in \{\leq, \geq\}}{gt \in vGT(x)}$$

$$\mathrm{R}_9: \frac{\neg(x < gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_{10}: \frac{\neg(x > gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_{11}: \frac{op(x, gt) \in C, where\ op \in \{<, >\}}{gt \in vGT(x)}$$

$$\mathrm{R}_{12}: \frac{\neg(x = gt) \in C}{gt \in vGT(x)} \qquad \mathrm{R}_{13}: \frac{(x = gt) \in C, x \in \mathbb{Z}}{\{gt - 1, gt + 1\} \subseteq vGT(x)} \qquad \mathrm{R}_{14}: \frac{(x = gt) \in C, x \notin \mathbb{Z}}{vGT(x) = \infty}$$

Rules for $\mathcal{S}_{\mathcal{A}}$

$$\mathrm{R}_0: \frac{x \dot{\in} C}{vGT(x) \neq \emptyset} \qquad \mathrm{R}_1: \frac{f(\cdots, \overbrace{x}^{\text{i-th}}, \cdots) \dot{\in} C}{vGT(x) = fGT(f,i)} \qquad \mathrm{R}_2: \frac{f(\cdots, \overbrace{gt}^{\text{i-th}}, \cdots) \dot{\in} C}{gt \in fGT(f,i)}$$

$$\mathrm{R}_3: \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \dot{\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f,i)}$$

$$\mathrm{R}_4: \frac{op(\cdots, x, \cdots) \in C,\ op \notin \{=, <, \leq, >, \geq\}}{vGT(x) = \infty} \qquad \mathrm{R}_5: \frac{op(x,y) \in C,\ op \in \{=, <, \leq, >, \geq\}}{vGT(x) = \infty \quad vGT(y) = \infty}$$

$$\mathrm{R}_6: \frac{(x \leq gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_7: \frac{(x \geq gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_8: \frac{\neg op(x, gt) \in C, where\ op \in \{\leq, \geq\}}{gt \in vGT(x)}$$

$$\mathrm{R}_9: \frac{\neg(x < gt) \in C}{gt - 1 \in vGT(x)} \qquad \mathrm{R}_{10}: \frac{\neg(x > gt) \in C}{gt + 1 \in vGT(x)} \qquad \mathrm{R}_{11}: \frac{op(x, gt) \in C, where\ op \in \{<, >\}}{gt \in vGT(x)}$$

$$\mathrm{R}_{12}: \frac{\neg(x = gt) \in C}{gt \in vGT(x)} \qquad \mathrm{R}_{13}: \frac{(x = gt) \in C, x \in \mathbb{Z}}{\{gt - 1, gt + 1\} \subseteq vGT(x)} \qquad \mathrm{R}_{14}: \frac{(x = gt) \in C, x \notin \mathbb{Z}}{vGT(x) = \infty}$$

Calculation of the $vGT(x)_{\mathcal{S}_A}$

$$R_4: \frac{op(\cdots, x, \cdots) \in C,\ op \notin \{=, <, \leq, >, \geq\}}{vGT(x) = \infty} \qquad R_5: \frac{op(x, y) \in C,\ op \in \{=, <, \leq, >, \geq\}}{vGT(x) = \infty \quad vGT(y) = \infty}$$

$$R_{14}: \frac{(x = gt) \in C, x \notin \mathbb{Z}}{vGT(x) = \infty}$$

Two objectives:

- Detection of infinite $vGT(x)_{\mathcal{S}_A}$ sets
  - Direct – *by* $R_{4,5,14}$

Calculation of the $vGT(x)_{\mathcal{S}_A}$

$$\mathsf{R}_1\colon \frac{f(\cdots, \overbrace{x}^{\text{i-th}}, \cdots) \mathrel{\dot\in} C}{vGT(x) = fGT(f,i)} \qquad \mathsf{R}_3\colon \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \mathrel{\dot\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f,i)}$$

Two objectives:

- Detection of infinite $vGT(x)_{\mathcal{S}_A}$ sets
  - Direct – *by* $R_{4,5,14}$
  - Propagation – *by* $R_{1,3}$

$$\begin{array}{ccc} t[vGT(x)/x] & \subseteq & fGT(f,i) \\ \rotatebox{90}{$=_{\mathcal{S}_A}$} & & \rotatebox{90}{$=_{\mathcal{S}_A}$} \\ fGT(g,j) & \supseteq & s[vGT(y)/y] \end{array}$$

Calculation of the $vGT(x)_{\mathcal{S}_A}$

$$\mathsf{R}_2\text{:}\frac{f(\cdots,\overbrace{gt}^{\text{i-th}},\cdots)\,\dot{\in}\,C}{gt \in fGT(f,i)} \qquad \mathsf{R}_6\text{:}\frac{(x \leq gt) \in C}{gt+1 \in vGT(x)} \qquad \cdots \qquad \mathsf{R}_{13}\text{:}\frac{(x = gt) \in C, x \in \mathbb{Z}}{\{gt-1, gt+1\} \subseteq vGT(x)}$$

Two objectives:

- Detection of infinite $vGT(x)_{\mathcal{S}_A}$ sets
  - Direct – *by* $R_{4,5,14}$
  - Propagation – *by* $R_{1,3}$
- Calculation/Construction of the $vGT(x)_{\mathcal{S}_A}$ sets:
  - Basic ground terms – *by* $R_{2,6\text{-}13}$

Calculation of the $vGT(x)_{\mathcal{S}_A}$

$$\mathrm{R}_3: \frac{f(\cdots, \overbrace{t[x_{1:n}]}^{\text{i-th}}, \cdots) \dot{\in} C}{t[vGT(x_1)/x_1, \cdots, vGT(x_n)/x_n] \subseteq fGT(f, i)}$$

Two objectives:

- Detection of infinite $vGT(x)_{\mathcal{S}_A}$ sets
  - Direct – *by* $R_{4,5,14}$
  - Propagation – *by* $R_{1,3}$
- Calculation/Construction of the $vGT(x)_{\mathcal{S}_A}$ sets:
  - Basic ground terms – *by* $R_{2,6\text{-}13}$
  - Complex ground terms – *by* R_3

Eliminable Variables

Theorem (Main Theorem)

Let x be a variable in A with $vGT(x)_{\mathcal{S}_A} \neq \infty$, then A and $A[vGT(x)_{\mathcal{S}_A}/x]$ are equisatisfiable.

- "$\Rightarrow$": easy
- "$\Leftarrow$": If $A[vGT(x)_{\mathcal{S}_A}/x]$ is satisfiable with a model $\mathcal{M}$, then we construct a modified model $\mathcal{M}^{\pi_x}$ (next slides) and show that $\mathcal{M}^{\pi_x}$ satisfies A.

Construction of $\mathcal{M}^{\pi_x}$

Given a model $\mathcal{M}$ for the formula $A[vGT(x)_{\mathcal{S}_A}/x]$, we construct a modified model $\mathcal{M}^{\pi_x}$ as follows:

- $|M^{\pi_x}| := |M|$
- For any constant $c \in Con$, $M^{\pi_x}(c) := M(c)$
- For any interpreted operator op, $M^{\pi_x}(op) := M(op)$
- For any uninterpreted function f, $M^{\pi_x}(f)(v_{1:n}) := M(f)(\pi_x(f,1)(v_1), \cdots, \pi_x(f,n)(v_n))$, where

$$\pi_x(f,i)(v) = \begin{cases} v & \text{if } fGT(f,i)_{\mathcal{S}_A} \dot{\notin} vGT(x)_{\mathcal{S}_A} \\ v & \text{else if } v \in M(fGT(f,i)_{\mathcal{S}_A}) \\ v' \in M(fGT(f,i)_{\mathcal{S}_A}) & \text{else if } v \notin \mathbb{Z} \\ v' \in M(fGT(f,i)_{\mathcal{S}_A}), s.t.\ |v - v'| \text{ is minimal} & \text{otherwise} \end{cases}$$

Optimization: *Selected Variable Elimination*

Let $\forall x \mid (\psi(x) \vee \forall y, z \mid \varphi(x, y, z))$ be a formula A,
$vGT(z)_{\mathcal{S}_A} = \{a_1, \ldots, a_n\}$,
$vGT(y)_{\mathcal{S}_A} = \{b_1, \ldots, b_m\}$ and
$vGT(x)_{\mathcal{S}_A} = \infty$. Then eliminating z and y results in A^{inst}:

$$\forall x \mid (\psi(x) \vee (\bigwedge_{1 \leq i \leq m} \bigwedge_{1 \leq j \leq n} \varphi(x, b_i, a_j)))$$

- A^{ints} is still quantified and thus considered by the quantifier engine
- The *occurrence increase* of x in A^{inst} is $n * m$
- Further instantiation of x becomes very costly

Optimization: *Selected Variable Elimination*

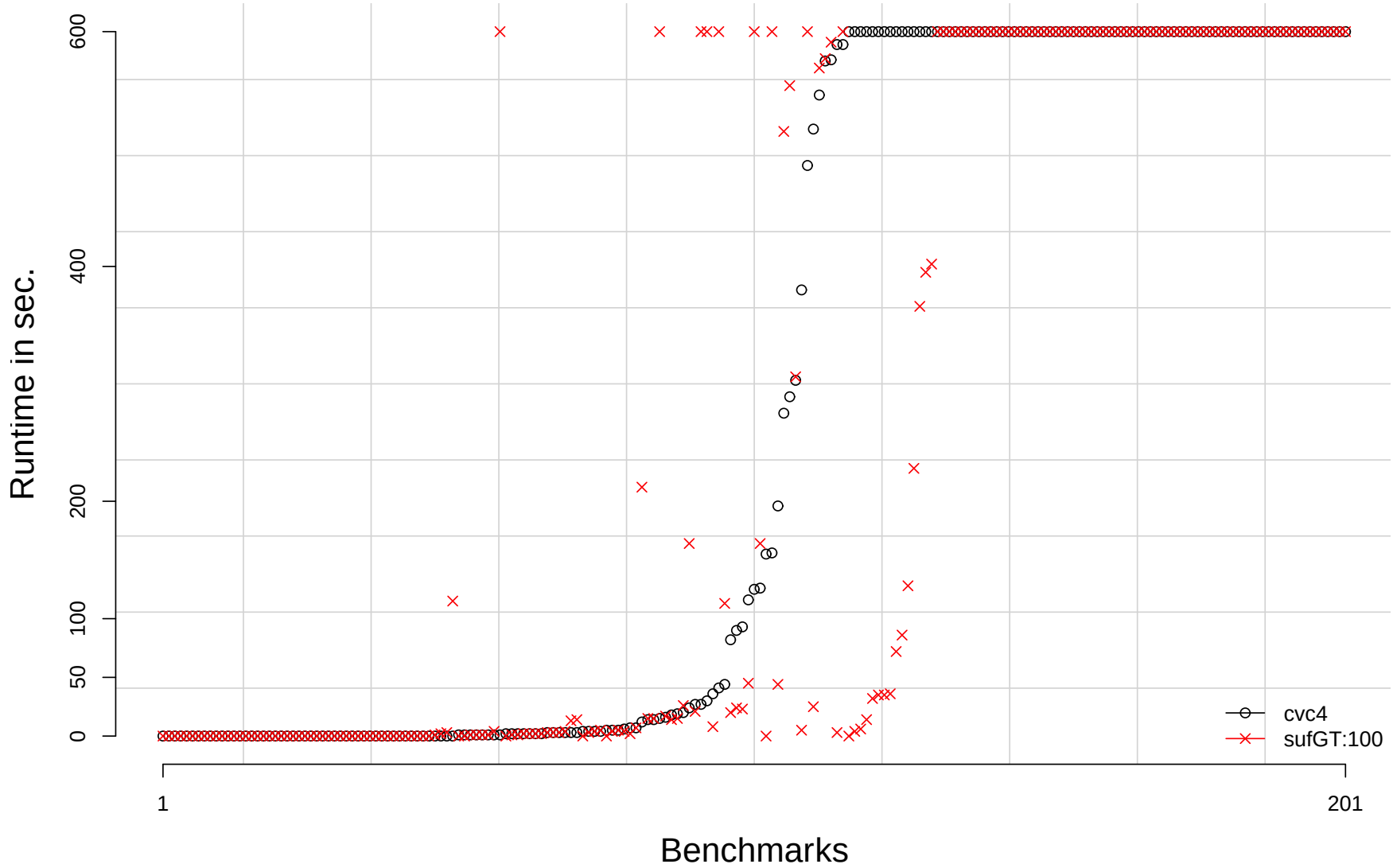
Definition

Let A be a formula and $S = \{x_1, \ldots, x_n\} \subseteq \{x \text{ in } A \mid vGT(x)_{S_A} \neq \infty\}$ a set of eliminable variables. The occurrence increase of quantified variables caused by eliminating all x_i in S is defined as:

$$C(S) := \max_{y \in A}\left(\frac{|occurr(y, A[vGT(x_1)/x_1, \ldots, vGT(x_n)/x_n])|}{|occurr(y, A)|}\right)$$

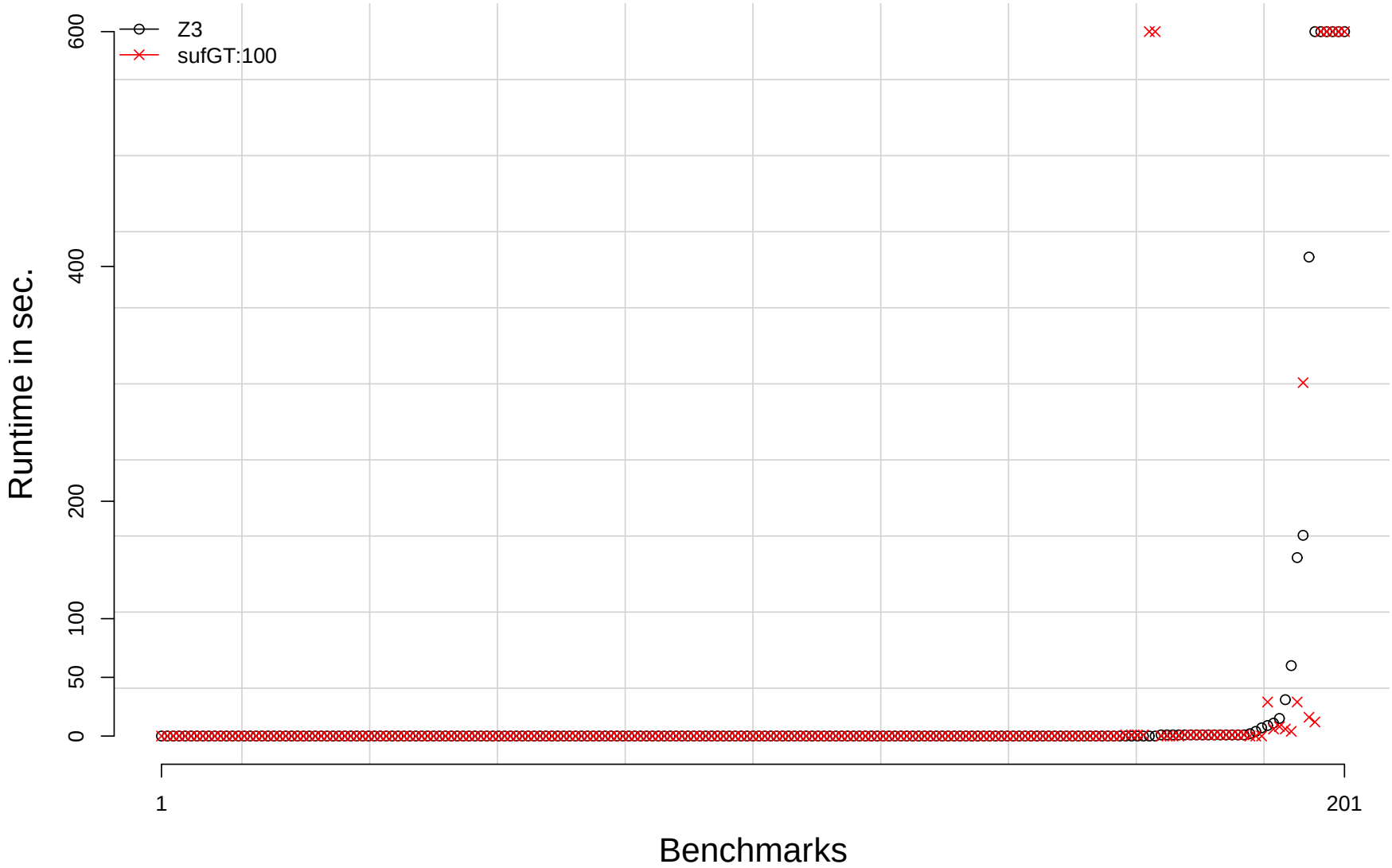
- $C(S)$ is our elimination cost function for the variables in S
- Given C_{max}, we search for the maximal S such that $C(S) < C_{max}$

Evaluation: *CVC4 vs. CVC4+sufGT*$_{C_{max}=100}$



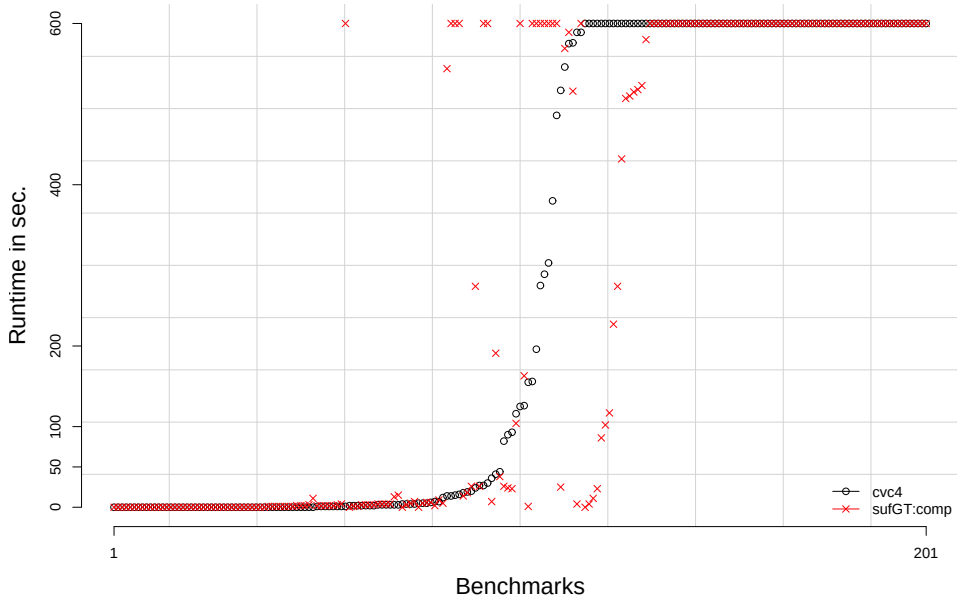
time-impr	avg-speedup	time-out-impr
39/32	57x/0.48x	15/9

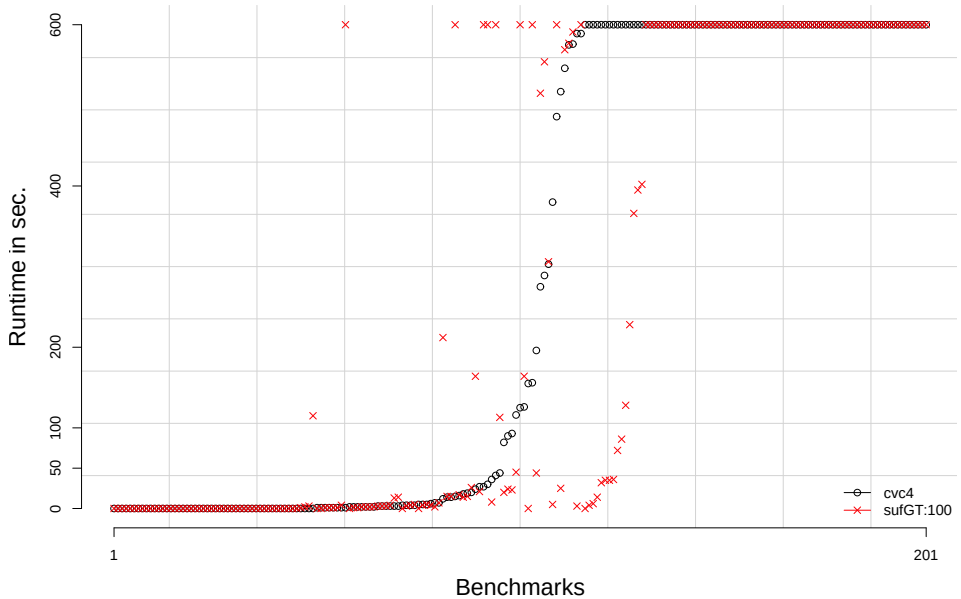
Evaluation: *Z3 vs. Z3+sufGT*$_{C_{max}=100}$



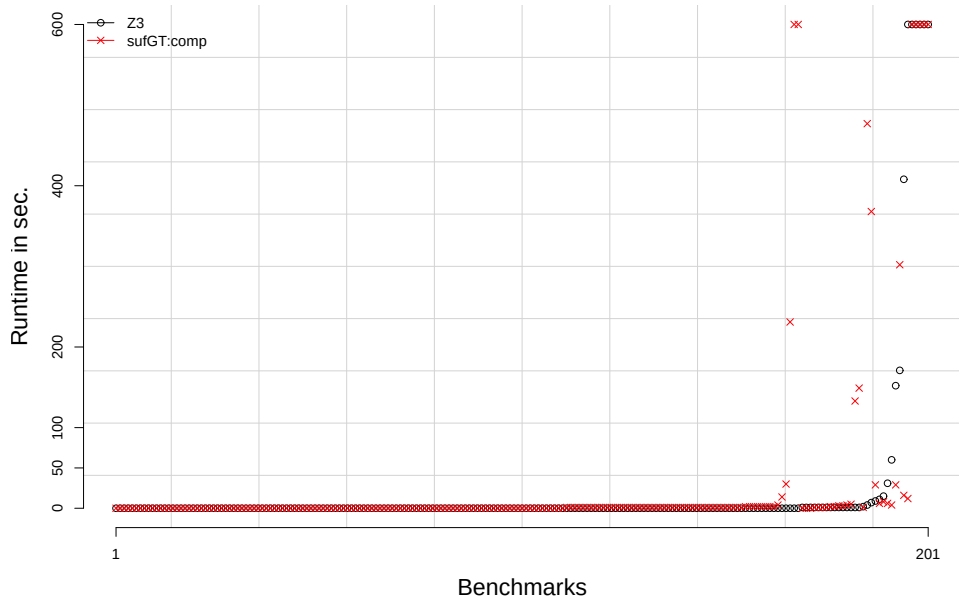
time-impr	avg-speedup	time-out-impr
14/8	9.4x/0.35x	1/2

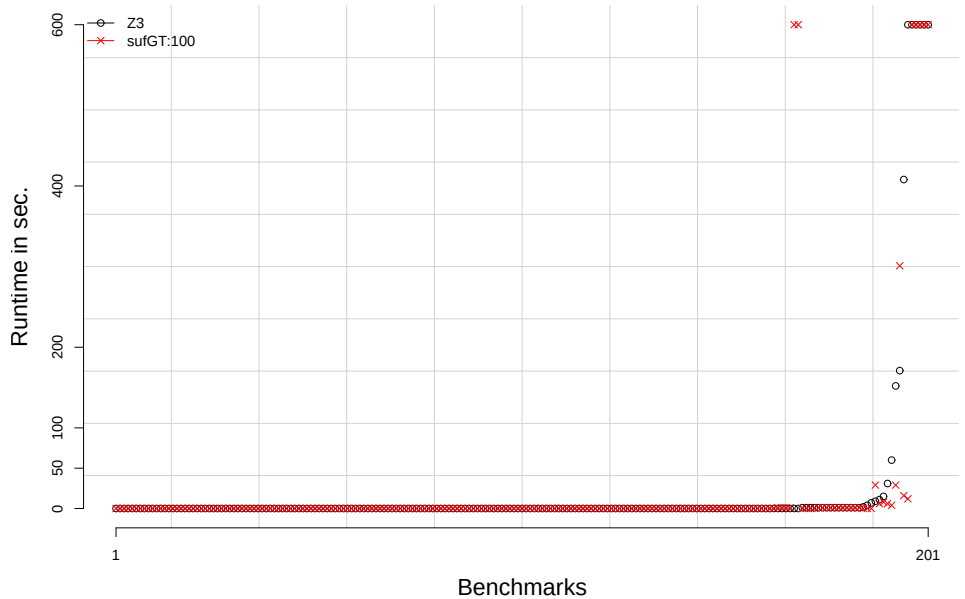
Evaluation: CVC4 – $sufGT_{C_{max}=\infty}$ *vs.* $sufGT_{C_{max}=100}$





Evaluation: Z3 – $sufGT_{C_{max}=\infty}$ *vs.* $sufGT_{C_{max}=100}$





Related work

- *Array Property* Fragment

  [Aaron R. Bradley, Zohar Manna, Henny B. Sipma]

  - Supports a combination of theories, *PA* for index terms, and *EUF* for array terms
  - Based on instantiation over ground terms
  - The results are restricted to the Array Property fragment ($\approx$ subsumed by ours)
  - No partial elimination

- *Model Based Quantifier Instantiation* (MBQI)

  [Yeting Ge, Leonardo de Moura]

  - Uses a similar system of set constraints Δ_F for the ground term sets ($\approx$ subsumes ours)
  - No upfront calculation of Δ_F
  - In theory, a fair enumeration of the (least) solution of Δ_F is proposed
  - Uses a (finite) model checker to explore the space of models incrementally

Conclusion

- A general simplification for quantified SMT formulas
  - Detection/Computation of (finite) sufficient ground term sets
  - Variable centric
  - Proved sound
  - Minimality of the constructed sets stays an open question
- Optimization is essential for practical application
  - Used the increase of variable occurrences as elimination cost
  - Use/Evaluation of other cost functions is possible

Conclusion

- The Experiment results show:
  - Some SMT benchmarks contain many eliminable variables w.r.t. our technique
  - The complete variable instantiation may slow down the solvers
  - Instantiation plus prioritization shows improvement of time and score.
- Calculation of minimal bounds – *future work*
- Extension of arbitrary SMTs with quantifier support – *future work*

Backup Slides

Evaluation: $sufGT_{C_{max}=\infty}$ *vs.* $sufGT_{C_{max}=100}$

Using CVC4

	$C_{max} = \infty$	$C_{max} = 100$
time-imp	37/55	39/32
avg-speedup	49x/0.45x	57x/0.48x
time-out-imp	16/15	15/9

Using Z3

	$C_{max} = \infty$	$C_{max} = 100$
time-imp	11/70	14/8
avg-speedup	10x/0.38x	9.4x/0.35x
time-out-imp	1/2	1/2