Weak Quantifier Elimination for the Integers

Beyond the Linear Case

NOCAS 2007-2008, Passau, Germany

Aless Lasaruk

Joint work with Thomas Sturm

FORWISS, Universität Passau

3 December 2007

Quantifier Elimination (QE) by Virtual Substitution

Input

First-order formula φ

Output

Quantifier-free formula φ' such that

$$\varphi \longleftrightarrow \varphi'$$

Restriction: It is sufficient to consider $\exists x \psi$ for quantifier-free ψ:

- Compute prenex normal form: $Q_1 x_1 \dots Q_n x_n \psi$, ψ quantifier-free
- Eliminate from the inside to the outside
- $\forall x \psi \longleftrightarrow \neg \exists x \neg \psi$

Virtual Substitution Approach

Compute an **elimination set** $E = \{(\gamma_i, t_i) \mid i \in \{1, \dots, n\}\}$ such that

$$\exists x \psi \longleftrightarrow \bigvee_{(\gamma, t) \in E} (\gamma \wedge \psi[t /\!\!/ x]).$$

Elimination set entries (**Test points**): **Guards** γ_i, **pseudo-terms** t_i

For $\mathbb{R}$ and $\mathbb{Z}$ elements of elimination sets are constructed essentially from interval boundaries.

Recall Real QE by Virtual Substitution

$$\exists x \psi \longleftrightarrow \bigvee_{(\gamma, t) \in E} (\gamma \wedge \psi[t /\!/ x])$$

Example

- Consider $\mathbb{R}$, arithmetic, ordering:

$$\varphi \equiv \exists x(3x - b = 0).$$

- One possible QE result using $E = \{(\mathrm{true}, b/3)\}$:

$$\varphi \longleftrightarrow \bigvee_{t \in \{(\mathrm{true}, b/3)\}} (3x - b = 0)[t /\!/ x] \longleftrightarrow 0 = 0 \longleftrightarrow \mathrm{true}$$

- **Virtual substitution:**

$$(ax = b)\left[\frac{b'}{a'} /\!/ x\right] := (ab' = a'b), \quad (ax \leq b)\left[\frac{b'}{a'} /\!/ x\right] := (aa'b' \leq a'^2 b)$$

- For linear formulas one can always find elimination sets [Weispfenning 1988].
- This can be extended to higher degrees to some extent [Weispfenning 1997].

The Same Problem Over the Integers

Example

- Consider $\mathbb{Z}$, arithmetic, ordering, **congruences**:

$$\varphi \equiv \exists x(3x - b = 0).$$

- One possible QE result [Weispfenning 1990]:

$$\varphi \quad \longleftrightarrow \quad \bigvee_{k=-3}^{3} \left(b + k \equiv_3 0 \wedge (3x - b = 0) \left[\frac{b+k}{3} /\!\!/ x \right] \right)$$

$$\longleftrightarrow \quad \bigvee_{k=-3}^{3} (b + k \equiv_3 0 \wedge k = 0) \longleftrightarrow b \equiv_3 0$$

- Virtual substitution for congruences: $(ax \equiv_m b)\left[\frac{b'}{a'} /\!\!/ x\right] := (ab' \equiv_{ma'} a'b)$
- Systematic use of formal $\bigvee$-notation decreases complexity by one exponential step [Weispfenning 1990].
- QE can be interpreted within the virtual substitution framework: $E = \left\{\, (b + k \equiv_3 0, (b+k)/3) \;\middle|\; |k| \leq 3 \,\right\}$ [L. 2005, L./Sturm 2007].

Presburger Arithmetic

- $3x$ is possibly short for $x + x + x$.
- Presburger Arithmetic is the **additive** theory of $\mathbb{Z}$ with ordering and congruences.
- Our example $\exists x(3x - b = 0)$ is a Presburger formula.

Mojzesz Presburger

Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt

Dissertation, Warsaw 1929

Possible extensions:

- Multiplicative parameters: $\exists x \exists y(a^2 x + b^2 y \geq c)$
- Higher degrees: $\exists x \exists y(x^2 + y^2 < a)$

Introducing Parameters Into Presburger Arithmetic

- Again $\mathbb{Z}$, arithmetic, ordering, congruences
- Now make essential use of multiplication:

$$\varphi \equiv \exists x(a \cdot x - b = 0).$$

- Copy the elimination approach from before:

$$\begin{aligned}\varphi \quad &\longleftrightarrow \quad b = 0 \vee \bigvee_{k=-|a|}^{|a|} \left(a \neq 0 \wedge b + k \equiv_a 0 \wedge (ax - b = 0) \left[\frac{b+k}{a} /\!/ x \right] \right) \\ &\longleftrightarrow \quad b = 0 \vee \bigvee_{k=-|a|}^{|a|} (a \neq 0 \wedge b + k \equiv_a 0 \wedge k = 0) \longleftrightarrow b \equiv_a 0.\end{aligned}$$

Problem

$$\bigvee_{k=-|a|}^{|a|} \left(a \neq 0 \wedge b + k \equiv_a 0 \wedge (ax - b = 0) \left[\frac{b+k}{a} /\!/ x \right] \right)$$

is not a first-order formula.

Bounded Quantifiers and Weak QE

Formally extend logic by new quantifiers with the following semantics:

$$\bigsqcup_{k\colon\beta}\varphi \quad \text{iff} \quad \exists k(\beta \wedge \varphi), \qquad \bigsqcap_{k\colon\beta}\varphi \quad \text{iff} \quad \forall k(\beta \longrightarrow \varphi).$$

We say **bounded quantifier** if the **range** β is finite for all choices of parameters.

This solves our previous problem

$$\bigsqcup_{k\colon |k|\leq|a|}\left(a \neq 0 \wedge b+k \equiv_3 0 \wedge (ax-y=0)\left[\frac{b+k}{3} /\!\!/ x\right]\right)$$ is OK in extended logic.

- **Expansion:** If β contains only k, then $\bigsqcup_{k\colon\beta}\varphi \longleftrightarrow \bigvee_{i\in\{z\in\mathbb{Z}\mid\beta(z)\}} \varphi[i/k]$.

Weak quantifier elimination: Results may contain bounded quantifiers.

Major Result (L. 2005, L./Sturm, AAECC 2007)

Linear formulas (with arbitrary polynomial coefficients) admit weak QE.

Weak Quantifier Elimination in Detail

- **Reminder:** We restrict to input formulas of the form $\exists x \psi$

Regular QE by Virtual Sibstitution	Weak Quantifier Elimination
ψ quantifier-free	$\psi = \underset{k_1:\beta_1}{Q_1} \dots \underset{k_n:\beta_n}{Q_n} \omega$, ω quantifier-free.
Elimination set	Parametric elimination set
$E = \{(\gamma_i, t_i) \mid i \in I\}$	$E = \{(\gamma_i, t_i, B_i) \mid 1 \leq i \in I\}$, $B_i = (\,(k_{ij}, \beta_{ij}) \mid 1 \leq j \leq m_i)$
$\exists x \psi \longleftrightarrow \bigvee_{(\gamma,t)\in E} (\gamma \wedge \psi[t /\!/ x])$	$\exists x \psi \longleftrightarrow \bigvee_{(\gamma_i,t_i,B_i)\in E} \bigsqcup_{k_{i1}:\beta_{i1}} \dots \bigsqcup_{k_{im_i}:\beta_{im_i}} (\gamma_i \wedge \psi[t_i /\!/ x])$

Expansion and Projection

- Consider a parametric elimination set E for elimination of $\exists x$ from $\exists x \psi$, the bound parameters $a = (a_1, \dots, a_k)$ of ψ, and the integers $z = (z_1, \dots, z_k)$

$$\begin{aligned}\Pi(E, z, a) \quad = \quad & \{\, (\gamma'[y_1/k_1, \dots, y_m/k_m],\ t'[y_1/k_1, \dots, y_m/k_m]) \mid \\ & (\gamma, t, B) \in E, B = ((k_j, \beta_j) \mid 1 \leq j \leq m), \\ & y_1 \in S^{k_1}_{\beta'_1},\ \dots,\ y_m \in S^{k_m}_{\beta'_m[y_1/k_1, \dots, y_{m-1}/k_{m-1}]} \,\}.\end{aligned}$$

  The set $\Pi(E, z, a)$ is called the **projection** of E wrt. a and z

- Consider $\exists x \psi$, bound parameters a and integers z as above, all the other parameters $a' = (a_{k+1}, \dots, a_l)$, and the integers $z' = (z_{k+1}, \dots, z_l)$

$\exists x \psi \longrightarrow E \xrightarrow{\text{Weak QE}} \varphi'$

$E \downarrow$ Projection; $\varphi' \downarrow$ Substitution $\varphi'[z/a]$, Expansion

$\Pi(E, z, a) \xrightarrow[\text{for } (\exists x \psi)[z/a]]{\text{Regular QE}} \varphi''$

$\Pi(E, z, a) \downarrow$ Substitution; $\varphi'' \downarrow$ Substitution

$\Pi(E, z, a)[z'/a'] \xrightarrow[\text{for } (\exists x \psi)[z/a,\, z'/a']]{\text{Regular QE}} \varphi''[z'/a'] \xrightarrow{\text{Simplification}}$ Truth value

Towards Higher Degrees

- Is our extension of logic suitable even for nonlinear formulas?
- Yes, for certain ones!

Example

Weakly eliminate $\exists x$ from $\varphi \equiv \exists x(ax - y < 0 \wedge ax^2 + x + a > 0)$.

Our result:

$$\bigsqcup_{k\colon |k| \leq |a|} \left(a > 0 \wedge y + k \equiv_a 0 \wedge k < 0 \wedge |ay + ak| > |a|^3 + 2a^2\right) \vee$$

$$\bigsqcup_{k\colon |k| \leq |a|+2} \left(ak - y < 0 \wedge ak^2 + k + a > 0\right).$$

- For $a = 10$ this can be turned into a regular first-order formula:

$$\bigvee_{k=-10}^{10} (y+k \equiv_{10} 0 \wedge k < 0 \wedge |y+k| > 120) \vee \bigvee_{k=-12}^{12} (10k-y < 0 \wedge 10k^2+k+10 > 0).$$

Which Formulas Can We Handle So Far?

The set of **univariately nonlinear formulas** is defined by 3 properties:

1. No quantified variables within moduli of (in)congruences
2. (In)congruences are linear in the quantified variables.
3. Equations and inequalities are either linear in the quantified variables or superlinear univariate in one of the quantified variables.

Examples

- Linear w.r.t. x and y: $ax - y < 0, \quad ax - y \equiv_m 0$
- Linear: $\forall a \forall b(a < b \longrightarrow \exists z(a < z \wedge z < b))$
- Superlinear univariate w.r.t. x and y: $ax^2 + x + a > 0.$
- Univariately nonlinear: $\forall y \exists x(ax - y < 0 \wedge ax^2 + x + a > 0)$
- **Not** univariately nonlinear w.r.t. x and y: $x^2 + xy + y^2 > 0, \quad x^2 + y^2 + a > 0$
- **Not** univariately nonlinear: $\exists x \exists y \exists z(x^5 + y^5 = z^5)$

- Linear formulas are special cases of univariately nonlinear formulas.

Basic Technical Ideas

- Known test points for the linear case [L./Sturm, AAECC 2007]
- Introduce bounded quantifiers ranging within **Cauchy bounds** for superlinear univariate atomic formulas.
- Substitution of fractions into nonlinear formulas requires generalized concept of **constrained** virtual substitution.
- Elements of parametric elimination sets contain in addition the substitution procedure:

$$E = \{ (\gamma_i, t_i, \sigma_i, B_i) \mid 1 \leq i \leq n \}, \text{ where } B_i = ((k_{ij}, \beta_{ij}) \mid 1 \leq j \leq m_i).$$

- Elimination scheme:

$$\exists x \psi \longleftrightarrow \bigvee_{(\gamma_i, t_i, \sigma_i, B_i) \in E} \bigsqcup_{k_{i1}\,:\,\beta_{i1}} \dots \bigsqcup_{k_{im_i}\,:\,\beta_{im_i}} (\gamma_i \wedge \sigma_i(\psi, t_i, x))$$

Example

Regular part

Consider $\exists x \psi$ with $\psi = ax - y < 0 \wedge ax^2 + x + a > 0$

Elimination set:

$$E = \Big\{ \big(a \neq 0 \wedge y + k \equiv_a 0,\ \tfrac{y+k}{a},\ [\cdot /\!\!/ \cdot],\ ((k, |k| \leq |a|))\big), \\ \big(\mathrm{true},\ k,\ [\cdot / \cdot],\ ((k, |k| \leq |a| + 2))\big) \Big\}$$

Consider the first entry of E:

- The pseudo-term $\frac{y+k}{a}$ describes a finite set of points around the solution of $ax - y = 0$ using the range $|k| \leq |a|$.
- The guard $a \neq 0 \wedge y + k \equiv_a 0$ ensures that $\frac{y+k}{a}$ evaluates to an integer.
- $[\cdot /\!\!/ \cdot]$ is our constrained virtual substitution.
- Corresponding disjunct in the output:

$$\bigsqcup_{k:\ |k| \leq |a|} \left(a > 0 \wedge y + k \equiv_a 0 \wedge k < 0 \wedge |ay + ak| > |a|^3 + 2a^2\right) \vee \ldots$$

Example of Constrained Virtual Substitution

Problem: How should we define $(ax^2 + x + a > 0)\left[\frac{y+k}{a} /\!/ x\right]$?

- Naive formal substitution yields $a(y+k)^2 + a(y+k) + a^3 > 0$. This is neither linear nor superlinear univariate wrt. y and k.
- We define our (constrained virtual) substitution as follows:

$$(ax^2 + x + a > 0)\left[\frac{y+k}{a} /\!/ x\right] := a > 0 \wedge |ay + ak| > |a|^3 + 2a^2.$$

- Division of $|ay + ak| > |a|^3 + 2a^2$ by a^2 yields $|\frac{y+k}{a}| > |a| + 2$
- $|a| + 2$ is a Cauchy bound plus 1 of $ax^2 + x + a$.
- **Intuitive idea:** State that the test term $\frac{y+k}{a}$ lies **outside** the Cauchy-bounds of $ax^2 + x + a$ and additionally satisfies $ax^2 + x + a > 0$.
- **Warning:** For the possible case that $\frac{y+k}{a}$ lies in fact **within** the Cauchy bounds but still satisfies $ax^2 + x + a > 0$ there is something left to do.

Example

Univariately nonlinear part

Consider once more $\exists x \psi$ with $\psi = ax - y < 0 \wedge ax^2 + x + a > 0$

$$E = \Big\{ \big(a \neq 0 \wedge y + k \equiv_a 0,\ \tfrac{y+k}{a},\ [\cdot /\!\!/ \cdot],\ ((k, |k| \leq |a|))\big), \\ \big(\mathrm{true},\ k,\ [\cdot/\cdot],\ ((k, |k| \leq |a| + 2))\big) \Big\}.$$

Consider the second entry of E:

- k is a test term, which equals the corresponding bound variable.
- $|k| \leq |a| + 2$ is the range of a bounded quantifier that substituting k within its scope exactly covers every single point within the Cauchy bounds of $ax^2 + x + a$.
- The substitution $[\cdot/\cdot]$ is the regular substitution of terms for variables.
- Corresponding disjunct in the output

$$\cdots \vee \bigsqcup_{k:\,|k| \leq |a|+2} \big(ak - y < 0 \wedge ak^2 + k + a > 0\big)$$

Towards Higher Degrees

Example

Input: Eliminate $\exists x$ from

$$\varphi = \exists x(ax - y < 0 \wedge ax^2 + x + a > 0)$$

Elimination set:

$$E = \Big\{\big(a \neq 0 \wedge y + k \equiv_a 0,\ \tfrac{y+k}{a},\ [\cdot/\!\!/\cdot],\ ((k, |k| \leq |a|))\big),\\ \big(\text{true},\ k,\ [\cdot/\cdot],\ ((k, |k| \leq |a| + 2))\big)\Big\}$$

Output: φ is equivalent to

$$\bigsqcup_{k\colon |k| \leq |a|} \big(a > 0 \wedge y + k \equiv_a 0 \wedge k < 0 \wedge |ay + ak| > |a|^3 + 2a^2\big) \vee \\ \bigsqcup_{k\colon |k| \leq |a|+2} \big(ak - y < 0 \wedge ak^2 + k + a > 0\big).$$

Recent Major Result

Theorem (L./Sturm CASC 2007)

The ordered ring of the integers with congruences admits weak quantifier elimination for univariately nonlinear formulas.

- We can positively decide in advance, whether or not all quantifiers can be eliminated by our method.

Fact

Let L be a language, and let A be an L-Structure.

If A admits QE and variable-free atomic formulas are decidable in A, then $A|_{L'}$ is decidable for all $L' \subseteq L$.

- The argument remains correct even for weak QE!

Corollary (Decidability of Sentences)

In the ordered ring of the integers with congruences univariately nonlinear sentences are decidable.

Computation Examples

Our work discussed here is implemented and publicly available in REDLOG.

Where?

www.redlog.eu

Application domains include the following:

- Nonlinear discrete optimization problems
- **Integer linear optimization with superlinear univariate constraints**
- **Software security**
- Automatic loop parallelization
- Scheduling problems

Hardware Specs

All our computations discussed in the following have been performed on a 1.66 GHz Intel Core 2 Duo processor T5500 using only one core and 128 MB RAM.

Optimization

Parametric linear optimization problem with univariately nonlinear constraints:

Minimize a cost function $\gamma_1 x_1 + \cdots + \gamma_n x_n$ subject to

$$A\mathbf{x} \geq \mathbf{b}, \quad p_1 \ \varrho_1 \ 0, \quad \dots, \quad p_r \ \varrho_r \ 0.$$

- $A = (\alpha_{ij})$ is an $m \times n$-matrix, and $\mathbf{b} = (\beta_1, \dots, \beta_m)$ is an m-vector.
- All these coefficients α_{ij}, β_i, and γ_j are possibly parametric.
- The $p_1, \dots, p_r$ are parametric univariate polynomials.
- Each corresponding ϱ_s is one of $=$, $\neq$, $\leq$, $>$, $\geq$, or $<$.

Formulation within our framework

Let z be a new variable.

$$\exists x_1 \dots \exists x_n \Big(\sum_{j=1}^{n} \gamma_j x_j \leq z \wedge \bigwedge_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} x_j \geq \beta_i \wedge \bigwedge_{s=1}^{r} p_s \ \varrho_s \ 0 \Big)$$

Optimization Example

Minimize $x + y$ subject to the following constraints:

$$x \geq 0, \quad y \geq 0, \quad 2x - y \geq 5, \quad \text{and} \quad x^2 - a > 0.$$

Formulation as a quantifier elimination problem:

$$\exists x \exists y \big(x + y \leq z \wedge x \geq 0 \wedge y \geq 0 \wedge 2x - y \geq 5 \wedge x^2 - a > 0 \big).$$

Results obtained with REDLOG:

- Weak QE yields 137 atomic formulas in 70 ms.
- Setting $a = 10$ and automatically simplifying yields $z > 3$ in 14 s, i.e., the minimum for $x + y$ is 4.
- Setting $a = 10$ **before** the elimination, directly yields $z > 3$ in only 7 s.

Software Security - Data and Control Flow

Example code

```
if (a < b) then
   // BEGIN SECURE CODE
   if (a+b mod 2 = 0) then
      n := (a+b)/2
   else
      n := (a+b+1)/2
   fi
   A[n*n] := get_sensitive_data(x)
   send_sensitive_data(trusted_receiver,A[n*n])
   // END SECURE CODE
fi
y := A[abs(b-a)]
```

- Are there choices for `a` and `b` such that `y` is assigned the value of `A[n*n]`?
- That would be a security risk.

Our solution with REDLOG

First-order formulation of both code and question

$$\exists n\big((a < b \wedge a + b \equiv_2 0 \wedge 2n = a + b \wedge ((a < b \wedge b - a = n^2) \vee (a \geq b \wedge a - b = n^2))) \vee (a < b \wedge a + b \not\equiv_2 0 \wedge 2n = a + b + 1 \wedge ((a < b \wedge b - a = n^2) \vee (a \geq b \wedge a - b = n^2)))\big).$$

- This is univariately nonlinear.

Applying weak QE with REDLOG

Weakly quantifier-free description in less than 10 ms:

$$\bigsqcup_{k:\,|k|\leq(a-b)^2+2} (a - b < 0 \wedge a - b + k^2 = 0 \wedge a + b \not\equiv_2 0 \wedge a + b - 2k + 1 = 0) \vee$$

$$\bigsqcup_{k:\,|k|\leq(a-b)^2+2} (a - b < 0 \wedge a - b + k^2 = 0 \wedge a + b \equiv_2 0 \wedge a + b - 2k = 0).$$

Outlook and Future Research

- The concept of weak quantifier elimination does not depend on the domain integers but is generally applicable.
- **Work in progress:** Small extensions (nonlinear congruences, decompositions, quantified variables in non-linear leading coefficients)
- **Work in progress:** Probabilistic quantifier elimination
- **Work in progress:** Mixed real-integer quantifier elimination combining our methods with real quantifier elimination
- **Next step:** Switch to more suitable languages for the bound descriptions (e.g. include absolute values)
- **Future vision:** Axiomatic approach for the characterization of formula sets, which admit weak quantifier elimination
- **Interesting question:** How far the concept of weak quantifier elimination can be extended to treat non-linear formulas?

$$\forall x \exists y (x^2 + y^2 = a^2) \longleftrightarrow \forall x \bigsqcup_{k:\, |k| \leq |a^2 - x^2|} (x^2 + k^2 = a^2) \longleftrightarrow ?$$

Conclusions

- Weak quantifier elimination procedure for the univariately nonlinear formulas
- Price to pay: bounded quantifiers
- Expansion into regular first-order formulas for fixed choices of parameters
- Decision procedure even for the regular first-order framework
- Efficient publicly available implementation within REDLOG
- REDLOG is part of the computer algebra system REDUCE
- Various application examples have demonstrated the applicability
- Extensive promising further research

The Elimination Theorem

Lemma [L./Sturm, AAECC 2007]

Consider a linear formula $\exists x \varphi$ with parameters $a_1, \dots, a_r$, with

- φ is weakly quantifier-free, positive, and in prenex normal form

$$\varphi = \underset{k_1:\beta_1}{Q_1} \dots \underset{k_n:\beta_n}{Q_n} \psi.$$

- The set of all atomic formulas of ψ that contain x: $\{ n_i x \varrho_i s_i + r_i \mid i \in I_1 \dot{\cup} I_2 \}$

Define:

- Let $k, k_1^*, \dots, k_n^*$ denote new variables.
- $\beta_1^* = \beta_1[k_1^*/k_1, \dots, k_n^*/k_n], \quad \dots, \quad \beta_n^* = \beta_n[k_1^*/k_1, \dots, k_n^*/k_n]$.
- $m = \mathrm{lcm}\{ m_i^2 + 1 \mid i \in I_2 \}$. For $i \in I_1 \cup I_2$

$$s_i^* = s_i[k_1^*/k_1, \dots, k_n^*/k_n] \quad \text{and} \quad \delta_i = -|n_i|m \leq k - s_i^* \leq |n_i|m.$$

Then $E = \{ (\gamma_i, t_i, B_i) \mid i \in I_1 \cup I_2 \} \cup \{(\mathrm{true}, 0, \varnothing)\}$, where

$$\gamma_i = (n_i \neq 0 \wedge r_i + k \equiv_{n_i} 0), \quad t_i = \frac{r_i + k}{n_i}, \quad B_i = ((k_1^*, \beta_1^*), \dots, (k_n^*, \beta_n^*), (k, \delta_i)),$$

is a parametric elimination set for $\exists x \varphi$.

The Elimination Theorem

Lemma [L./Sturm, AAECC 2007]

Consider a linear formula $\exists x \varphi$ with parameters $a_1, \dots, a_r$, with

- φ is weakly quantifier-free, positive, and in prenex normal form

$$\varphi = \underset{k_1 : \beta_1}{Q_1} \dots \underset{k_n : \beta_n}{Q_n} \psi.$$

- The set of all atomic formulas of ψ that contain x: $\{ n_i x \varrho_i s_i + r_i \mid i \in I_1 \dot{\cup} I_2 \}$

Define:

- Let k, $k_1^*, \dots, k_n^*$ denote new variables.
- $\beta_1^* = \beta_1[k_1^*/k_1, \dots, k_n^*/k_n], \quad \dots, \quad \beta_n^* = \beta_n[k_1^*/k_1, \dots, k_n^*/k_n]$.
- $m = \mathrm{lcm}\{ m_i^2 + 1 \mid i \in I_2 \}$. For $i \in I_1 \cup I_2$

$$s_i^* = s_i[k_1^*/k_1, \dots, k_n^*/k_n] \quad \text{and} \quad \delta_i = -|n_i|m \le k - s_i^* \le |n_i|m.$$

Then $E = \{ (\gamma_i, t_i, B_i) \mid i \in I_1 \cup I_2 \} \cup \{(\mathrm{true}, 0, \varnothing)\}$, where

$$\gamma_i = (n_i \neq 0 \land r_i + k \equiv_{n_i} 0), \quad t_i = \frac{r_i + k}{n_i}, \quad B_i = ((k_1^*, \beta_1^*), \dots, (k_n^*, \beta_n^*), (k, \delta_i)),$$

is a parametric elimination set for $\exists x \varphi$.