数理解析研究所講究録
第1976巻 2015年 45-51

非等式制約に対する実閉体上の限量記号消去

岩根秀直*
(株) 富士通研究所/国立情報学研究所
HIDENAO IWANE
NATIONAL INSTITUTE OF INFORMATICS/FUJITSU LABORATORIES LTD

1 はじめに

限量記号消去法（Quantifier Elimination: QE）[2, 10] は限量記号がついた一階述語論理式を入力として，それと等価で限量記号のない論理式を出力するアルゴリズムである．例えば，$\exists x(x^2+bx+c=0)$ に対して QE を適用すると，それと等価で限量記号がついた変数 x のない論理式 $b^2-4c\geq 0$ を得る．一階述語論理式は，限量記号である $\forall$（全称記号），$\exists$（存在記号），多項式の等式 $(f=0)$・不等式 $(f<0, f\leq 0)$・非等式 $(f\neq 0)$ からなる原子論理式，$\wedge$（かつ）・$\vee$（または）・$\neg$（否定）などの論理演算子から成る．

QE はさまざまな応用があり，アルゴリズムの効率化に関する多くの研究が行われている．しかし，任意の入力に適用可能な汎用 QE アルゴリズムは，現在知られている最も効率のいい手法である Cylindrical Algebraic Decomposition [3] でも，その最悪計算量の下限は変数の数に対して 2 重指数 [1] で，多くとも 5 変数程度までの問題しか解けない．そのため，入力を特別な場合に制限することで高速化を実現する専用 QE に関する研究がすすめられている: 例えば線形の場合など入力の次数を制限したもの (Virtual Substitution: VS) [8, 9], 2 次または線形の等式制約をもつ $(\exists x(ax^2+bx+c=0\wedge\psi))$ もの [6], $\forall x(f(x)>0)$ や $\forall x(x\geq 0\rightarrow f(x)>0)$ に対するもの [5, 7] がある．

本稿では，非等式を含む一階述語論理式に対する QE を対象とする．また，入力の一階述語論理式には否定演算子は含まないと仮定し，ある変数 x についてのみ，存在限量記号がついているとする．つまり，

$$\exists x(f(x)\neq 0\wedge\psi)$$

のような一階述語論理式を考える．例えば，

$$\exists x(a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0\neq 0)$$

が本稿で扱う対象である．この問題では，次数ごとに場合分けして考えれば容易に等価な論理式

$$a_5\neq 0\vee a_4\neq 0\vee a_3\neq 0\vee a_2\neq 0\vee a_1\neq 0\vee a_0\neq 0$$

を得られる．これは係数に対する非等式の論理和で，手計算でも求められるが，このような QE は Mathematica, Redlog などの QE ツールでは実装されておらず，汎用 QE 手法で解くしかないため計算は 1 時間かけても停止しなかった．

非等式制約は，非縮約条件などとして実問題でも現れる．他にも次数ごとに処理をする QE [6] や包括的グレブナー基底系を利用した QE [4] の出力として現れるので非等式をもつ一階述語論理式に対する効率的な QE の実現は重要である．

*iwane@jp.fujitsu.com

2 非等式のみをもつ一階述語論理式に対する QE

定義 1
一階述語論理式 φ が, 否定演算子 $\neg$ をひとつも含まないとき, φ を**正** *(positive)* であるという.

定義 2
一階述語論理式が, 限量記号を含まない場合, *quantifier-free formula (QFF)* という.

記法 1
正の *QFF* $\varphi(x)$ に含まれる原子論理式が, 変数 x を含む場合には常に非等式の場合, $\varphi_{\neq}(x)$ と書く.

記法 2
QFF ψ を満たす異なる実数 x がちょうど n 個存在するとき, $\exists^n x(\psi)$ と書き, ψ を満たす異なる実数が無限個存在するとき, $\exists^\infty x(\psi)$ と書く.

定理 3
QFF $\varphi_{\neq}(x)$ に対する操作 $'$ を以下のように定義する.

$$\varphi'_{\neq}(x) \equiv \begin{cases} \vee_{c\in \mathrm{coeff}_x(f)} c \neq 0 & \text{if } \varphi_{\neq}(x) \equiv f \neq 0 \\ \varphi'_1(x) \wedge \varphi'_2(x) & \text{if } \varphi_{\neq}(x) \equiv \varphi_1(x) \wedge \varphi_2(x) \\ \varphi'_1(x) \vee \varphi'_2(x) & \text{if } \varphi_{\neq}(x) \equiv \varphi_1(x) \vee \varphi_2(x) \\ \varphi_{\neq}(x) & \text{otherwise } (\varphi_{\neq}(x) \text{ は原子論理式で、} x \text{ を含まない}) \end{cases}$$

このとき, 以下が成立する.

$$\exists x(\varphi_{\neq}(x)) = \varphi'_{\neq}(x)$$

証明 最初に $\varphi_{\neq}(x)$ が原子論理式の場合を考える. $\varphi_{\neq} \equiv f\rho 0, \rho \in \{<, \leq, =, \neq\}$: f に x が含まれない場合は, 明らかである. x を含む場合は, f が恒等的に零になる場合には明らかに $\varphi_{\neq}$ は偽である. そうでない場合は, 多項式の次数を $m > 0$ とすると, 多項式は $m+1$ 点以上の点で零になることはできないので, 真である. したがって, $\exists x(f \neq 0) \equiv \vee_{c\in \mathrm{coeff}_x(f)} c \neq 0 \equiv \varphi'_{\neq}$ が成立する.

次に, 論理積のみが現れる場合を考える. $\varphi_{\neq} \equiv \wedge_i f_i \neq 0$: f_i が x を含まない場合には限量記号の外に出すことができるので, f_i の x に対する次数はすべて正であると仮定して良い. このとき, $\varphi_{\neq} \equiv (\prod_i f_i) \neq 0$ となるので, $\varphi_{\neq}$ が原子論理式の場合と同様に考えれば良い. f_i の一つが恒等的に零になる場合には明らかに $\varphi_{\neq}$ は偽である. そうでない場合を考える. m を $\prod_i f_i$ の x に対する次数, つまり, $m = \sum_i \deg_x(f)$ とする. 多項式の実根の個数は高々その次数までなので, 適当に $m+1$ 点を選択すると, その中の少なくとも一点ですべての f_i が零にならない. したがって, $\exists x(\wedge_i f_i \neq 0) \equiv \wedge_i \vee_{c\in \mathrm{coeff}_x(f_i)} c \neq 0 \equiv \varphi'_{\neq}$ が成立する.

最後に任意の $\varphi_{\neq}$ について考える: 任意の QFF は, 積和標準形 $\psi \equiv \vee_i \wedge_j f_{ij}\rho_{ij}0$ の形式に変換可能である. 変換後の式に対して,

$$\exists x(\vee \wedge f_{ij}\rho_{ij}0) \equiv \vee \exists x(\wedge f_{ij}\rho_{ij}0) \equiv \vee(\wedge f_{ij}\rho_{ij}0)' \equiv \vee \wedge (f_{ij}\rho_{ij}0)'$$

となる. これは単に ψ の各原子論理式に操作 $'$ を適用しただけなので, 積和標準形への変換の逆の変換によって, 元の論理式 $\varphi_{\neq}$ に操作 $'$ を適用した式が得られる. ∎

以下の系は, 上記の証明において, 十分な実根の数のみが必要なことから容易に得られる.

系 4
定理 *3* と同じ記号を用いて, 以下が成立する.

$$\exists^\infty x(\varphi_{\neq}(x)) \equiv \varphi'_{\neq}(x)$$

3 適用範囲の拡張

一般に, $\exists x(\psi_1 \wedge \psi_2)$ と $\exists x(\psi_1) \wedge \exists x(\psi_2)$ は等価にならないが，非等式に対する QE においては十分な数の x が存在しさえ良いことから以下の系が得られる.

系 5
定理 *3* と同じ記号を用いて, *QFF* ψ, $\varphi_{\neq}$ に対して以下が成立する.

$$\exists^{\infty} x(\psi \wedge \varphi_{\neq}) \equiv \exists^{\infty} x(\psi) \wedge \varphi'_{\neq}$$

実閉体上の QE を考える場合には，適当な自然数 m (例えば，原子論理式に現れる多項式の x に関する次数の和) に対して,

$$\begin{aligned}\exists x(\psi \wedge \varphi_{\neq}) \equiv & \exists^1 x(\psi \wedge \varphi_{\neq}) \vee \exists^2 x(\psi \wedge \varphi_{\neq}) \vee \cdots \vee \exists^m x(\psi \wedge \varphi_{\neq}) \vee \exists^{\infty} x(\psi \wedge \varphi_{\neq}) \\ & \exists^1 x(\psi \wedge \varphi_{\neq}) \vee \exists^2 x(\psi \wedge \varphi_{\neq}) \vee \cdots \vee \exists^m x(\psi \wedge \varphi_{\neq}) \vee \exists^{\infty} x(\psi) \wedge \varphi'_{\neq}\end{aligned}$$

が成立する．したがって，右辺が専用 QE を利用して効率的に解けるような ψ を設定できれば，操作 $'$ による QE の適用範囲が広がる.

3.1 狭義の不等式のみから構成される場合

QFF $\psi_<$ のすべての原子論理式が狭義の不等式のみから構成される場合,

$$\exists x(\psi_<) \equiv \exists^{\infty} x(\psi_<)$$

が成立する，したがって,

$$\exists x(\psi_< \wedge \varphi_{\neq}) \equiv \exists x(\psi_<) \wedge \varphi'_{\neq}$$

となる．左辺の QE をそのまま実行するよりも，右辺の QE のほうが明らかに容易になっている.

3.2 一つの原子論理式の場合

ψ が原子論理式の場合を考える．$f < 0$ の場合は，3.1 節で対応可能なこと，$f = 0$ の場合は恒等的に零になる場合以外は対応できないので，$\psi \equiv f \leq 0$ を考える．この場合，f の主係数が負または奇数次の場合は, $\exists x(\psi) = \exists^{\infty} x(\psi) = \top$ が成立する．2 次の場合には判別式を利用して問題を分割できる．また，一変数多項式であれば, 実根の分離を利用して判定できる場合がある.

Algorithm 1 にアルゴリズムを示す．ここで, $\mathsf{QE}_{\mathsf{lineq}}$ は線形の等式制約を含む場合に適用可能な専用 QE [6] を表し, $\deg_x(f)$, $\mathrm{LC}_x(f)$, $\mathrm{discrim}_x(f)$, $\mathrm{diff}_x(f)$ はそれぞれ f の x に関する次数，主係数，判別式，微分を表す．2 行目からのループで，次数ごとに処理を行なっている．4 行目の奇数次または主係数が負の場合には必ず条件を満たすものが無限個存在する．6 行目の定数の場合には，x を含まないので f が条件を満たせば良い．8 行目は 2 次の場合で,

$$\exists x(ax^2 + bx + c \leq 0) \equiv \exists^1 x(ax^2 + bx + c = 0) \vee \exists^{\infty} x(ax^2 + bx + c < 0)$$

を利用している．10 行目は一変数の場合を処理しており，それ以外の場合には FAIL を復帰する.

Algorithm 1 $\mathsf{QE}_{\neq,\mathsf{atom}}(f(x), \varphi_{\neq})$

Input: polynoamial f, quantifer-free formula $\varphi_{\neq}$

Output: an equivalent quantifier-free formula for $\exists x(f \leq 0 \wedge \varphi_{\neq})$

1: $r \leftarrow \bot$
2: **loop**
3: $d \leftarrow \deg_x(f)$, $c_d \leftarrow \mathrm{LC}_x(f)$
4: **if** (c_d is numeric **and** $c_d < 0$) **or** d is odd **then**
5: $r \leftarrow r \vee (c_d \neq 0 \wedge \varphi'_{\neq})$
6: **else if** $d = 0$ **then**
7: **return** $r \vee (f \leq 0 \wedge \varphi'_{\neq})$
8: **else if** $d = 2$ **then**
9: $r \leftarrow r \vee (c_2 < 0 \wedge \varphi'_{\neq}) \vee ((c_2 > 0 \wedge \mathrm{discrim}_x(f) > 0) \wedge \varphi'_{\neq})$
10: $r \leftarrow r \vee c_2 > 0 \wedge \mathrm{discrim}_x(f) = 0 \wedge \mathsf{QE}_{\mathsf{lineq}}(\exists x(\mathrm{diff}_x(f) = 0 \wedge \varphi_{\neq}))$
11: **else if** f is univariate **then**
12: $r \leftarrow r \vee \mathsf{QE}_{\neq,\mathsf{univ}}(f, \varphi_{\neq})$
13: **else**
14: **return** FAIL
15: **end if**
16: $\varphi_{\neq} \leftarrow \varphi_{\neq} \wedge (c_d = 0)$, $f \leftarrow f - c_d x^d$
17: **end loop**

Algorithm 2 は f が一変数の場合のアルゴリズムである．1 行目，3 行目，9 行目の QE は因数分解と実根の分離によって判定可能である．6 行目以降が実施されるのは，$f \leq 0 \equiv f = 0$ を満たす場合であるので，f の既約因子が零になる場合を条件として分解している．f_i の次数が 2 次以下であれば，等式制約を含む場合に適用可能な専用 QE [6] $\mathsf{QE}_{\mathsf{eq}}$ により効率的に解くことが可能である．

Algorithm 1 と Algorithm 2 では，3 次以上の場合には FAIL を復帰することがあるが，これは現在提案されている専用 QE のみを利用することを仮定しているためである．例えば，3 次の等式制約をもつ一階述語論理式に対する専用 QE を用意するなどして判定不能な場合を減らせることに注意されたい．

3.3 線形不等式の論理積の場合

$\psi \equiv \wedge_i f_i \rho_i 0$ ($\rho_i \in \{<, \leq\}$) の場合を考える．ψ を満たす x は区間または一点で現れることになるので，以下が成立する．

$$\begin{aligned}\exists x(\psi \wedge \varphi_{\neq}) \equiv & \exists^1 x(\psi \wedge \varphi_{\neq}) \vee \exists^{\infty} x(\psi \wedge \varphi_{\neq}) \\ \equiv & \exists^1 x(\psi \wedge \varphi_{\neq}) \vee \exists^{\infty} x(\psi) \wedge \varphi'_{\neq}\end{aligned}$$

$\exists^1 x(\psi \wedge \varphi_{\neq})$ は線形の等式制約を持つので，専用 QE [6] が適用可能で効率的に解くことができる．

$\exists^{\infty} x(\psi)$ は区間で現れる場合である．この場合には異なる 2 点で ψ を満たすことになるので，以下が成立する．

$$\exists^{\infty} x(\psi(x)) \equiv \exists x_1 \exists x_2(\psi(x_1) \wedge \psi(x_2) \wedge x_1 \neq x_2)$$

右辺は x_1,x_2 に関する総次数が 1 なので VS [8] で効率的に解くことができる．

Algorithm 2 $\mathsf{QE}_{\neq,\mathsf{univ}}(f(x), \varphi_{\neq})$

Input: univariate polynoamial f, quantifer-free formula $\varphi_{\neq}$

Output: an equivalent quantifier-free formula for $\exists x(f \leq 0 \wedge \varphi_{\neq})$

```
1: if ∃x(f < 0) then
2:     return φ'_≠
3: else if ∀x(f ≠ 0) then
4:     return ⊥
5: end if
6: factorization f = f_1^{m_1} ··· f_u^{m_u}
7: r ← ⊥
8: for i = 1 to u do
9:     if ∃x(f_i = 0) then
10:        if deg_x(f_i) > 2 then
11:            return FAIL
12:        else
13:            r ← r ∨ QE_eq(∃x(f_i = 0 ∧ φ_≠))
14:        end if
15:    end if
16: end for
17: return r
```

Algorithm 3 に線形不等式の論理式で構成される場合のアルゴリズムを示す．1 行目で，$\exists^{\infty}x(\psi) \wedge \varphi'_{\neq}$ を求め，それ以降で $\exists^{1}x(\psi \wedge \varphi_{\neq})$ を求めている．$\mathsf{QE}_{\mathsf{lineq}}$ は線形の等式制約を含む場合に適用可能な専用 QE [6] を表す．

$\varphi_{\neq}$ が x に関して線形となる原子論理式のみから構成される場合には，直接 VS を適用可能なので，その場合はどちらが計算効率がよいか考慮する必要がある．

4 まとめ

本稿では非等式制約に関する QE とその拡張について述べた．操作 $'$ による QE は係数のみで表されるので他の専用 QE に比べて冗長になりにくく，使い勝手の良い手法である．また，非等式制約は，入力で現れていなかったとしても，他の QE の実行結果として現れることがあり，適用の機会は少なくない．適用範囲の拡大により，以下のような他の手法では困難な計算を効率的に解くことが出来るようになった．

- 5 変数で 1 次の非等式を 2 つもつ: $\exists x(x^2 - 2xa_3 + a_4^2 - 2a_4a_2 + a_2^2 + a_3^2 < 0 \wedge x \neq 0 \wedge (a_4a_1 - a_4a_3 + a_1a_2 - a_2a_3)x + (a_4^2 - a_4^2a_2 - a_4a_1a_3 + a_4a_3^2) \neq 0)$
- 5 変数で 2 次の非等式を 1 つもつ: $\exists x(x < a_3 \wedge (1 - 2a_4a_2 - 2a_1a_3)x \geq (2a_4a_1a_2 - 2a_2^2a_3 - a_1) \wedge (8a_4 + 8a_1a_3 - 4)x^2 + (8a_2^2a_3 - 8a_4a_1a_2 - 8a_4a_2a_3 - 8a_1a_3^2 + 4a_1 + 4a_3)x + a_2 + 4a_4a_2 - 4a_2^2 - 1 \neq 0)$
- 4 変数で 1 次と 2 次の非等式をもつ: $\exists x(x < 0 \wedge (3 - a_3)x < 2 \wedge (a_3^2 - 8a_3 + 24)x \geq 20 - 4a_3 \wedge a_1x - a_2 \neq 0 \wedge (a_1^2 + a_1a_3 - 4a_1 - 2)x^2 + (2a_1 + 4a_2 - 2a_1a_2 - a_2a_3 + 1)x + (a_2 - 1)^2 \neq 0)$

今後の課題としては，より適用範囲を広げるために新しい ψ のクラスを構成することが考えられる．

Algorithm 3 $\mathsf{QE}_{\neq,\mathsf{lin}}(\psi \equiv \wedge_{i=1}^{n} f_i \rho_i 0, \varphi_{\neq})$

Input: linear polynoamial f_i , $\rho_i \in \{<, \leq\}$, quantifer-free formula $\varphi_{\neq}$

Output: an equivalent quantifier-free formula for $\exists x(\psi \wedge \varphi_{\neq})$

1: $r \leftarrow \exists x_1 \exists x_2(\psi(x_1) \wedge \psi(x_2) \wedge x_1 \neq x_2) \wedge \varphi'_{\neq}$
2: $S \leftarrow \emptyset$
3: **for** $i = 1$ **to** n **do**
4: **if** $\rho_i = \leq$ **then**
5: $S \leftarrow S \cup \{f_i\}$
6: **end if**
7: **end for**
8: **for all** $\ell, u \in S$ **do**
9: $r \leftarrow r \vee \mathsf{QE}_{\mathsf{lineq}}(\exists x(u = 0 \wedge \ell = 0 \wedge \mathrm{LC}_x(u) > 0 \wedge \mathrm{LC}_x(\ell) < 0 \wedge \psi \wedge \varphi_{\neq}))$
10: **end for**
11: **return** r

参 考 文 献

[1] Christopher W. Brown and James H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, ISSAC '07, pp. 54–60, New York, NY, USA, 2007. ACM.

[2] Bob F. Caviness and Jeremy R. Johnson, editors. *Quantifier Elimination and Cylindrical Algebraic Decomposition (Texts and Monographs in Symbolic Computation)*. Springer Vienna, softcover reprint of the original 1st ed. 1998 edition, April 1998.

[3] George E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20-23, 1975*, Vol. 33 of *Lecture Notes in Computer Science*, pp. 134–183. Springer-Verlag, 1975.

[4] Ryoya Fukasaku, Hidenao Iwane, and Yosuke Sato. Real quantifier elimination by computation of comprehensive Gröbner systems. In Kazuhiro Yokoyama, Steve Linton, and Daniel Robertz, editors, *Proceedings of the 40th international symposium on Symbolic and algebraic computation*, ISSAC '15, pp. 173–180. ACM, 2015.

[5] Laureano González-Vega, Tomas Recio, Henri Lombardi, and M.-F Roy. *Sturm-Habicht sequences determinants and real roots of univariate polynomials*, pp. 300–316. In Caviness, Bob F. and Johnson, Jeremy R. [2], softcover reprint of the original 1st ed. 1998 edition, April 1998.

[6] Hoon Hong. Quantifier elimination for formulas constrained by quadratic equations. In *Proceedings of the 1993 international symposium on Symbolic and algebraic computation*, ISSAC '93, pp. 264–274, New York, NY, USA, 1993. ACM.

[7] Hidenao Iwane, Hiroyuki Higuchi, and Hirokazu Anai. An effective implementation of a special quantifier elimination for a sign definite condition by logical formula simplification. In Vladimir P. Gerdt, Wolfram Koepf, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *CASC*, Vol. 8136 of *Lecture Notes in Computer Science*, pp. 194–208. Springer, 2013.

[8] Volker Weispfenning. The complexity of linear problems in fields. *Journal of Symbolic Computation*, Vol. 5, pp. 3–27, February 1988.

[9] Volker Weispfenning. Quantifier elimination for real algebra - the quadratic case and beyond. *Applicable Algebra in Engineering, Communication and Computing*, Vol. 8, pp. 85–101, 1993.

[10] 穴井宏和, 横山和弘. QE の計算アルゴリズムとその応用 – 数式処理による最適化. 東京大学出版会, August 2011.