数理解析研究所講究録
第2050巻 2017年 162-167

限量子記号消去アルゴリズムとその計算の現状について

佐藤洋祐
YOSUKE SATO
東京理科大学理学部応用数学科
DEPARTMENT OF APPLIED MATHEMATICS, TOKYO UNIVERSITY OF SCIENCE *

1 はじめに

限量子記号消去 (Quantifier Elimination、以下では QE と略記する) とは代数的な一階述語論理式から限量子記号$\exists, \forall$を取り除き、それと等価な自由変数のみの代数的な式を求めることである。数式処理で最もよく扱われるのは実数領域と複素数領域における QE である。以下の例は、数式処理システム Mathematica の QE プログラム Reduce の実行例である。

```
In[1]:= Reduce[Exists[X, X^2 + A X + B == 0], {A,B},Reals]
                2
               A
Out[1]= B <= --
               4
In[2]:= Reduce[Exists[X, A X^2 + B X + C == 0], Complex]

Out[2]= (A == 0 && B != 0) || (C == 0 && B == 0 && A == 0) || A != 0
```

最初の例が実数領域における QE プログラム、後の例が複素数領域における QE プログラムの実行例である。本稿では、実数領域と複素数領域における QE アルゴリズムとその応用例について概説を与える。さらに、一般に利用できるプログラムの現状についても紹介する。

2 実数領域の QE

実数領域における最初の QE アルゴリズムは Tarski によって与えられた。(古い論文であるが、[7] に原論文がそのまま掲載されている。) 一変数実多項式の実根に関する情報を与える Sturm 列 (例えば [6] に詳しい解説が与えられている) を巧妙に利用したアルゴリズムであるが、計算量を考慮していないため実際にプログラムとして実装しても使い物にならない。その後 [3] によって部分終結式の計算による効率的な Sturm 列の計算を利用した CAD(Cylindrical Algebraic Decomposition) の計算に基づく QE アルゴリズムが提唱され、前章にあげた Mathematica のプログラムや、今日利用できる QE プログラムの多くがこの方法に基づいている。CAD に基づく QE の平易な日本語の解説本 [1] が出版されているので、詳しく知りたい読者はそちらを参照されたい。

*ysato@rs.kagu.tus.ac.jp

しかしながら、扱う一階述語論理式が多くの等式が含むような場合、CADによるQEは無駄な計算を多数おこなってしまうため効率が悪い。[5]では、多変数代数方程式の実根の個数に関するHermiteの理論を利用して、包括的グレブナー基底の計算に基づくQEアルゴリズムを導入している。このアルゴリズムは数式処理システムMaple用のパッケージとして実装され、等式を多く含む一階述語論理式にたいしては、他のプログラムより高性能であることが報告されている。例えば、初等幾何学の問題は実数領域のQEによってコンピューターによる自動解法が可能であるが、国際数学オリンピックで出題されるような複雑な幾何問題の解法や、[2]で報告されている大学入試問題の解法のためには、一般に多数の等式を含む一階述語論理式に対するQEが必要になる。この種の論理式にたいしては、[5]の方法が他の方法よりも圧倒的に有効であることが報告されている。

3 複素数領域のQE

複素数領域は代数的閉体なので、複素数領域のQEは実数領域のQEよりも遥かに容易である。例えば、$\exists X(X^2+AX+B=0)$ は複素数領域ではTrueであり $\exists X(X^2+AX+C=0\wedge X^2+BX+C=0)$ は X に関する2つの1変数多項式 X^2+AX+C と X^2+BX+C の最大公約元が定数でないことと同値であり、$(C=0\wedge A\neq B)\vee A=B$ と同値になる。一般に、複素数領域のQEアルゴリズムはパラメーター付きの1変数多項式の最大公約元の計算を繰り返すことで容易に構成できるが、パラメーター空間の分割が複雑になるため効率的ではない。実際、Mathematicaの複素数領域のQEアルゴリズムはこの方法に基づいて実装されているが、性能はよくない。これに対し、多変数多項式環におけるイデアルの包括的グレブナー基底系の計算を利用したHilbertの零点定理に基づく方法の方が一般には効率がよい。

包括的グレブナー基底系(Comprehensive Gröbner System、以下CGSと略記する)とはパラメーターを含む多項式が生成するイデアルのグレブナー基底のことである。

例1.
$\mathbb{Q}[X,Y]$ においてパラメーター A を持つイデアル $I=\langle AX+Y^2+1,Y^3+1\rangle$ の辞書式項順序 $X>Y$ に対するCGSは、$\{(\{A=0\},\{1\}),(\{A\neq 0\},\{AX+Y^2+1,Y^3+1)\}$ である。
つまり、I のグレブナー基底は $A=0$ のときは $\{1\}$、$A\neq 0$ のときは $\{AX+Y^2+1,Y^3+1)\}$ であることを意味している。これより、グレブナー基底の基本的性質とHilbertの零点定理より

$$\exists X,Y\in\mathbb{C}(AX+Y^2+1=0\wedge Y^3+1=0)\Leftrightarrow A\neq 0$$

が成り立つことがわかる。

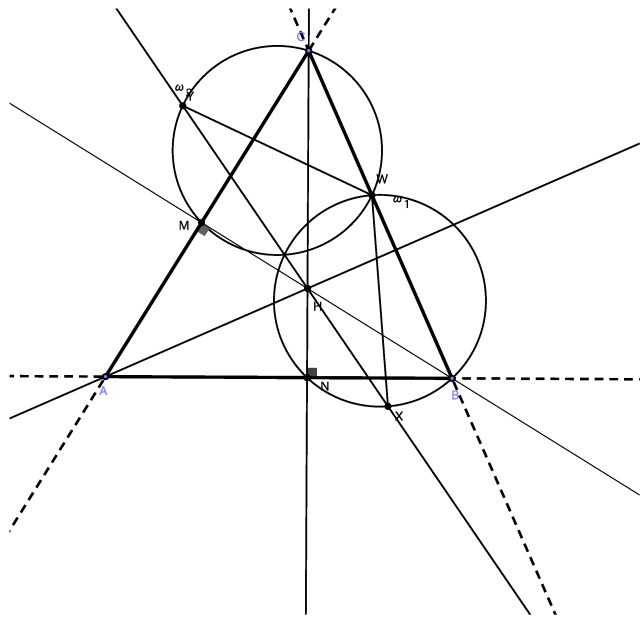
[8]で導入された包括的グレブナー基底系の高速アルゴリズムのおかげで、今日では一般的にこの方法が最も性能がよい実装を実現している。[4]では、包括的グレブナー基底系とパラメーター付きの1変数多項式の最大公約元の計算を組合わせることでさらに高速なQEアルゴリズムを実現している。

4 QEの応用例

実数領域におけるQEと複素数領域におけるQEが実際の問題にどのように適用されるのか、次の数学オリンピックに出題された問題を題材に概説を与える。

問題 (国際数学オリンピック 2013)

鋭角三角形 ABC にたいして、点 M, N をそれぞれ B, C から AC, AB へ下ろした垂線の足とし、H を垂心とする。線分 BC 上の B, C と異なる点 W にたいして、ω_1 を三角形 BWN の外心円、ω_2 を三角形 CWM の外心円とする。ω_1 上の点 X を WX が ω_1 の直径となるようにとり、ω_2 上の点 Y を WY が ω_2 の直径となるようにとる。このとき、三点 X, Y, H が一直線上にあることを証明せよ。



A, B, C, M, X, Y の座標を以下のように取る。$A(0,0)$, $B(1,0)$, $C(c_1,c_2)$, $M(m_1,m_2)$, $X(x_1,x_2)$, $Y(y_1,y_2)$。

このとき、以下の式が成り立つ。

1. 点 C は AB 上にはない $\Leftrightarrow c_2 \neq 0$。
2. 三角形 ABC は鋭角三角形である $\Leftrightarrow 0 < c_1 < 1 \wedge (c_1 - 1/2)^2 + c_2^2 > 1/4$。
3. CN $\perp$ AB $\Leftrightarrow$ 点 N の座標は $(c_1, 0)$。
4. 点 H は CN 上にある $\Leftrightarrow$ H の座標はある実数 h_2 にたいして (c_1, h_2) である。
5. 点 W は線分 BC 上の B,C と異なる点である
   $\Leftrightarrow$ W の座標は $0 < w < 1$ なる実数 w にたいして $(1 + w(c_1 - 1), wc_2)$ である。
6. 点 M は AC 上にある $\Leftrightarrow m_1c_2 - m_2c_1 = 0$。
7. BH $\perp$ AC $\Leftrightarrow (c_1 - 1)c_1 + h_2c_2 = 0$。
8. BM $\perp$ AC $\Leftrightarrow$ 点 H は BM 上にある $\Leftrightarrow (m_1 - 1)c_1 + m_2c_2 = 0$。
9. WX は ω_1 の直径 $\Leftrightarrow$

$$\begin{aligned}((1 + w(c_1 - 1)) - x_1)^2 + (wc_2 - x_2)^2 &= ((1 + w(c_1 - 1)) + x_1 - 2c_1)^2 + (wc_2 + x_2)^2 \\ &= ((1 + w(c_1 - 1)) + x_1 - 2)^2 + (wc_2 + x_2)^2。\end{aligned}$$

10. WY は ω_2 の直径 $\Leftrightarrow$

$$((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2=((1+w(c_1-1))+y_1-2mc_1)^2+(wc_2+y_2-2mc_2)^2$$
$$=((1+w(c_1-1))+y_1-2c_1)^2+(wc_2+y_2-2c_2)^2。$$

11. 三点 X,Y,H は一直線上にある $\Leftrightarrow (y_1-c_1)(y_2-x_2)-(y_2-h_2)(y_1-x_1)=0$。

$F_1,\ldots,F_7,P$ を以下のように取ると、

$F_1=m_1c_2-m_2c_1$, $F_2=(c_1-1)c_1+h_2c_2$, $F_3=(m_1-1)c_1+m_2c_2$,
$F_4=((1+w(c_1-1))-x_1)^2+(wc_2-x_2)^2-(((1+w(c_1-1))+x_1-2c_1)^2+(wc_2+x_2)^2)$,
$F_5=((1+w(c_1-1))-x_1)^2+(wc_2-x_2)^2-(((1+w(c_1-1))+x_1-2)^2+(wc_2+x_2)^2)$,
$F_6=((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2$
$\quad -(((1+w(c_1-1))+y_1-2mc_1)^2+(wc_2+y_2-2mc_2)^2)$,
$F_7=((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2$
$\quad -(((1+w(c_1-1))+y_1-2c_1)^2+(wc_2+y_2-2c_2)^2)$,
$P=(y_1-c_1)(y_2-x_2)-(y_2-h_2)(y_1-x_1)$,

この問題は以下の論理式が真になることを示すことに他ならない。

$$\begin{aligned}&\forall x_1,x_2,y_1,y_2,m_1,m_2,h_2,w,c_1,c_2\in\mathbb{R}\\&\quad c_2\neq 0\ \wedge\ 0<c_1<1\ \wedge\ (c_1-1/2)^2+c_2^2>1/4\ \wedge\ 0<w<1\ \wedge\\&\quad F_1=0\ \wedge\ F_2=0\ \wedge\ F_3=0\ \wedge\ F_4=0\ \wedge\ F_5=0\ \wedge\ F_6=0\ \wedge\ F_7=0\\&\Rightarrow\quad P=0\end{aligned}$$

残念ながら、現時点での Mathematica(version11.0.1) の QE プログラムではこの式を扱うことはできない。

実は、この問題は Metric 幾何とよばれる初等幾何学の問題になっている。Metric 幾何では不等式は扱わない。この問題は必要のない条件「 ABC は鋭角三角形」 を仮定している。実際に必要な仮定は ω_1 と ω_2 が定義されるための以下の条件のみである。

W $\neq$ B ($w\neq 0$), W $\neq$ C($w\neq 1$), $\angle$ABC $\neq \frac{\pi}{2}$ ($c_1\neq 1$), $\angle$ACB $\neq \frac{\pi}{2}$ ($(c_1-1/2)^2+c_2^2\neq 1/4$)。

つまり、以下の論理式が真になる。

$$\begin{aligned}&\forall x_1,x_2,y_1,y_2,m_1,m_2,h_2,w,c_1,c_2\in\mathbb{R}\\&\quad c_2\neq 0\ \wedge\ c_1\neq 1\ \wedge\ (c_1-1/2)^2+c_2^2\neq 1/4\ \wedge\ w\neq 0\ \wedge\ w\neq 1\ \wedge\\&\quad F_1=0\ \wedge\ F_2=0\ \wedge\ F_3=0\ \wedge\ F_4=0\ \wedge\ F_5=0\ \wedge\ F_6=0\ \wedge\ F_7=0\\&\Rightarrow\quad P=0\end{aligned}$$

Metric 幾何の定理は複素数領域でも成り立つので、実はこれより強い以下の論理式が真になる。

$$\begin{aligned}&\forall x_1,x_2,y_1,y_2,m_1,m_2,h_2,w,c_1,c_2\in\mathbb{C}\\&\quad c_2\neq 0\ \wedge\ c_1\neq 1\ \wedge\ (c_1-1/2)^2+c_2^2\neq 1/4\ \wedge\ w\neq 0\ \wedge\ w\neq 1\ \wedge\\&\quad F_1=0\ \wedge\ F_2=0\ \wedge\ F_3=0\ \wedge\ F_4=0\ \wedge\ F_5=0\ \wedge\ F_6=0\ \wedge\ F_7=0\\&\Rightarrow\quad P=0\end{aligned}$$

自由変数を 含まない論理式にたいする QE(すなわちそれが真か偽かを 判定すること) はグレブナー基底のみの計算で可能なので、この式にたいしては Mathematica の複素数領域の QE プログラムでも 瞬時に計算

を終了し trueを返す。

それでは、必要な条件、例えばCに関する条件 $c_2 \neq 0 \ \wedge \ c_1 \neq 1 \ \wedge \ (c_1 - 1/2)^2 + c_2^2 \neq 1/4$ を得るにはどうすればよいであろうか。理論的には以下の論理式にたいするQEによってこの条件が得られる。

$$\begin{array}{l} \forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w \in \mathbb{R} \\ \quad w \neq 0 \ \wedge \ w \neq 1 \ \wedge \\ \quad F_1 = 0 \ \wedge \ F_2 = 0 \ \wedge \ F_3 = 0 \ \wedge \ F_4 = 0 \ \wedge \ F_5 = 0 \ \wedge \ F_6 = 0 \ \wedge \ F_7 = 0 \\ \Rightarrow \quad P = 0 \end{array}$$

Mathematica(version11.01)の実数領域のQEプログラムはこの入力にたいして計算が終了しないが、[5]で公開されているプログラムは一般のノートPCで数秒で計算が終了し、同値な式

$$(c_1 = 0 \wedge c_2 = 0) \vee (c_1 - 1)((c_1 - 1/2)^2 + c_2^2 - 1/4) \neq 0$$

を出力する。

前に述べたように、複素数領域のQEは実数領域のQEよりも遥かに容易な計算である。[4]で公開されているプログラムは

$$\begin{array}{l} \forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w, c_1, c_2 \in \mathbb{C} \\ \quad w \neq 0 \ \wedge \ w \neq 1 \ \wedge \\ \quad F_1 = 0 \ \wedge \ F_2 = 0 \ \wedge \ F_3 = 0 \ \wedge \ F_4 = 0 \ \wedge \ F_5 = 0 \ \wedge \ F_6 = 0 \ \wedge \ F_7 = 0 \\ \Rightarrow \quad P = 0 \end{array}$$

の入力にたいして、瞬時に以下の同値な式を出力する。

$$(c_1 = 1 \wedge c_2^2 + 1 = 0) \vee (c_1 = 0 \wedge c_2 = 0) \vee (c_1 - 1)((c_1 - 1/2)^2 + c_2^2 - 1/4) \neq 0$$

Mathematica(version11.0.1)の複素数領域のQEプログラムはこの入力にたいしても計算が終了しない。

参 考 文 献

[1] 穴井、横山、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 2011.

[2] Arai, N. H., Matsuzaki, T., Iwane, H., Anai, H.: Mathematics by Machine, Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 1-8, ACM-Press, 2014.

[3] Collins, G, E. : Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), pp. 134-183. Lecture Notes in Comput. Sci., Vol. 33, Springer, Berlin, 1975.

[4] Fukasaku, R.,Inoue, S. and Sato, Y. On QE Algorithms over Algebraically Closed Field based on Comprehensive Gröbner Systems. Mathematics in Computer Science, Vol.9-3, pp267-288. 2014.

[5] Fukasaku, R., Iwane, H. and Sato, Y. Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173-180, ACM, 2015.

[6] 高木貞治 (著), 代数学講義, 共立出版.

[7] Tarski, A. A Decision Method for Elementary Algebra and Geometry. Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts & Monographs in Symbolic Computation, pp. 24-84, Springer, 1998.

[8] Suzuki, A., Sato, Y.: A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.326-331, ACM-Press, 2006