QE の応用例

Eureka GAP

July 1, 2017

Theorem

T を理論とする．次は T が QE を許すことと同値：任意の T のモデル $\mathcal{M}_1, \mathcal{M}_2$ と，それらの共通部分構造 $\mathcal{A} \subseteq \mathcal{M}_1, \mathcal{M}_2$ をとる．任意の qunatifier-free な論理式 $\phi(x, v_1, \ldots, v_n)$ と $a_1, \ldots, a_n \in A$ に対して，

$$\mathcal{M}_1 \models \exists x \phi(x, a_1, \ldots, a_n) \Longrightarrow \mathcal{M}_2 \models \exists x \phi(x, a_1, \ldots, a_n)$$

が成り立つ．

この判定法によって代数閉体，実閉体といった理論が QE を許すことを示し，その簡単な応用を紹介するのが，この発表の目的である．

Theorem

(Tarski) 代数閉体の理論 ACF は QE を許す.

Proof.

1. K_1, K_2 を代数閉体とし，R をそれらに共通の部分環とする．また，$\phi(x, \bar{v})$ を QF 論理式とし，$\bar{a}$ を R の元の列とする．
   $K_1 \models \exists x\, \phi(x, \bar{a})$ と仮定し，$K_2 \models \exists x\, \phi(x, \bar{a})$ を示す.
2. F_1, F_2 をそれぞれ K_1, K_2 における R の商体の代数閉包とする．R 上の恒等写像を拡大して，同型射 $f : F_1 \to F_2$ を得る．K_1 において，$\phi(b, \bar{a})$ となるような $b \in K_1$ をとる.
3. $b \in F_1$ ならば，$f(b) \in K_2$ をとれば，$K_2 \models \phi(f(b), \bar{a})$ となる.
4. $b \notin F_1$ ならば，b は F_1 上超越的で $F_1(b) \models \phi(b, \bar{a})$．$K_2$ を含むような初等拡大 K_3 をとる．すると $c \in K_3 \setminus K_2$ が存在して，c は F_2 上超越的．$F_1(b) \simeq F_2(c)$ より $F_2(c) \models \phi(c, \bar{a})$ で，$K_3 \models \exists x\, \phi(x, \bar{a})$.
   よって，$K_2 \models \exists x\, \phi(x, \bar{a})$.

□

QE によって代数閉体における定義可能集合がどのようなものかが分かる.

Definition

K を代数閉体とする．$X \subseteq K^n$ が構成可能集合であるとは，それが Zariski 閉集合の補集合，有限和，有限共通部分から作ることのできる集合であること.

RCF は QE を許すので，構成可能であることと定義可能であることは同値である．特に 1 次元の場合は次が成り立っている.

Theorem

K を代数閉体とする．K の定義可能部分集合は有限個の点もしくはその補集合である.

この事実は ACF の強極小性とよばれる.

Chevalley による次の定理もいまやほとんど自明である.

Theorem (Chevalley)

構成可能集合 $X \subseteq K^m$ の多項式写像 $f\colon K^m \to K^n$ による像 $f(X) \subseteq K^n$ もまた構成可能である.

Proof.

X が定義可能であることから,

$$f(X) = \{y \in K^n \mid \exists x\, (x \in X \wedge y = f(x))\}$$

もまた定義可能なので, 構成可能である. □

QE からは他のモデル理論的性質を示すことが可能である．例えば，前回 Hilbert の零点定理の証明で用いたのは，QE から導かれる次の性質であった：

Definition

理論 T がモデル完全であるとは，T の任意のモデル $\mathcal{M}, \mathcal{N}$ に対して，

$$\mathcal{M} \text{ は } \mathcal{N} \text{ の部分構造} \iff \mathcal{M} \text{ は } \mathcal{N} \text{ は初等部分構造}$$

が成り立つことである．

Definition

理論 T が完全であるとは，任意の閉論理式 ϕ と任意の T のモデル $\mathcal{M}, \mathcal{N}$ に対して，

$$\mathcal{M} \models \phi \iff \mathcal{N} \models \phi$$

となることである．

T が完全であるとき，ある T のモデルで閉論理式 ϕ が真ならば，任意の T のモデルで ϕ が真になる（これを $T \models \phi$ と書く）ことが同値になるのがポイントである．さらに，T が完全ならば，$T \not\models \phi$ と $T \models \neg\phi$ が同値になることにも注意．

ACF は完全ではない．なぜなら，代数閉体には標数の違いがあるからである．そこで，ACF_p（$p = 0$ または素数）という理論を，ACF に「標数が p」という意味の論理式を加えたものとする．

Theorem

ACF_p は完全である．

Proof.

ACF_p のモデルは，$p = 0$ なら $\mathbb{Q}$，$p > 0$ なら $\mathbb{F}_p$ の代数閉包を部分構造として含んでいる．モデル完全性より，ACF_p の任意のモデル $\mathcal{M}, \mathcal{N}$ に対して，

$$\mathcal{M} \models \phi \iff \overline{\mathbb{Q}} \models \phi \ (\text{or } \overline{\mathbb{F}_p} \models \phi) \iff \mathcal{N} \models \phi$$

□

この事実は代数幾何において Lefschez 原理とよばれていたものである．

ACF_p の完全性を用いると，次のような補題を得る．

Lemma

ϕ を閉論理式とすると，次は同値である：

1. $\mathrm{ACF}_0 \models \phi$.
2. $\mathrm{ACF}_p \models \phi$ を満たす任意に大きな p が存在する．

Proof.

1. 完全性定理より，$T \models \phi$ であることと，ϕ が T の論理的帰結であることが同値になることに注意しよう．$\mathrm{ACF}_0 \models \phi$ とすると，有限部分集合 $\Delta \subseteq \mathrm{ACF}_0$ が存在して，$\Delta \models \phi$．十分大きな全ての p に対して，$\Delta \subseteq \mathrm{ACF}_p$ となり，$\mathrm{ACF}_p \models \phi$.
2. 逆を示すため，$\mathrm{ACF}_0 \not\models \phi$ とする．ACF_p の完全性より，$\mathrm{ACF}_0 \models \neg\phi$ となるから，上と同様の議論により，十分大きなすべての p に対して，$\mathrm{ACF}_p \models \neg\phi$．再び完全性より $\mathrm{ACF}_p \not\models \phi$.

□

Theorem (Ax-Grothendieck)

多項式写像 $f\colon \mathbb{C}^n \to \mathbb{C}^n$ は単射ならば全単射である．

Proof.

1. k を有限体とする．k^n 上の多項式写像は単射ならば全単射．
2. 多項式写像 $f\colon \overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ は単射ならば全単射．そうでないとして，反例となる f をとり，出てくる多項式の係数たちを $\bar{a}$ とし，f の値域に入らない元を $\bar{b}$ とする．$\overline{\mathbb{F}_p} = \bigcup_m \mathbb{F}_{p^m}$ より，$\bar{a}, \bar{b}$ を含むような $k = \mathbb{F}_{p^m}$ が存在する．しかし，f を k^n に制限した写像は単射だが全単射となっておらず，一番目の結果と矛盾する．
3. 任意の自然数 d に対して，「高々次数 d の多項式写像は単射ならば全単射である」という文章は閉論理式でかけていて，すべての $\overline{\mathbb{F}_p}$ で成り立つ．先の補題を使えば，$\mathbb{C}$ でもこれが成り立つ．

□

代数閉体，代数幾何の文脈から離れて，実閉体，実代数幾何の話題へ移る．実閉体を定義するため，まず次の定義をする．

Definition

体 K が形式的実体であるとは，-1 が K の元の二乗和で表せないことである．

順序付け可能な体は形式的に実であることは容易に分かる．

Theorem

形式的実体は順序づけ可能である．特に，$-a$ が二乗和で表せない元の場合，$a > 0$ となるように順序を入れることができる．

Definition

形式的実体 K が，真の代数拡大で形式的に実なものをもたないとき，K は実閉体であるという．

Theorem

形式的実体 K に対して次は同値である：

1. K は実閉体
2. 任意の $a \in K$ に対して a または $-a$ は平方数であり，かつ任意の奇数次多項式は根を持つ．

以上の準備のもとで，実閉体の理論（RCF）を定義することができる．

Definition

$\mathcal{L}_{\mathrm{oring}} = \{0, 1; +, \times, -; <\}$ を順序環の言語とする．実閉体の理論（RCF）は以下の $\mathcal{L}_{\mathrm{oring}}$-閉論理式からなる．

- 体の公理.
- 各 $n \geq 1$ に対して，$\forall x_1, \ldots, x_n \, (x_1^2 + \cdots + x_n^2 + 1 = 0)$.
- $\forall x \exists y \, (x > 0 \to x = y^2)$.
- 各 n に対して，$\forall a_0, \ldots, a_{2n} \exists x \, (x^{2n+1} + a_{2n} x^{2n} + \cdots + a_1 x + a_0 = 0)$.

Theorem (Tarski-Seidenberg)

RCF は QE を許す.

Proof.

1. K_1, K_2 を実閉体とし，R をそれらに共通の部分環とする．また，$\phi(x, \bar{v})$ を QF 論理式とし，$\bar{a}$ を R の元の列とする．
   $K_1 \models \exists x\, \phi(x, \bar{a})$ と仮定し，$K_2 \models \exists x\, \phi(x, \bar{a})$ を示す.
2. F_1, F_2 をそれぞれ K_1, K_2 における R の商体の実閉包とする．R 上の恒等写像を拡大して，同型射 $f : F_1 \to F_2$ を得る．K_1 において，$\phi(b, \bar{a})$ となるような $b \in K_1$ をとる.
3. $b \in F_1$ ならば，$f(b) \in K_2$ をとれば，$K_2 \models \phi(f(b), \bar{a})$ となる.
4. $b \notin F_1$ ならば，b は F_1 上超越的．$F_1^l = \{x \in F_1 \mid x < b\}$, $F_1^r = \{x \in F_1 \mid b < x\}$ とおく．さらに，$F_2^l = f(F_2^l)$，$F_2^r = f(F_2^r)$ とすれば，F_2^l の任意の元は F_r^2 の任意の元よりも小さい.

Proof.

5. K_2 の初等拡大 K_3 をとる．順序体における順序は稠密なので，K_3 には F_2^l と F_2^r の間の元 c が存在し，これは F_2 上超越的である．すると，f を拡大するような $g\colon F_1(b) \to F_2(c)$ が存在する．これは実際，順序も保存している．
6. それを示すには，h が $F_1[b]$ 上で順序を保存することをみれば十分である．$p(b) \in F_1[b]$ とおく．実閉体上のモニック既約多項式は $X - a$ または $(X-b)^2 + c$（$c > 0$）という形しかないことを使うと，

$$p(X) = \epsilon \prod (X - a_i) \prod \left((X - b_j)^2 + c_j\right)$$

という形に書ける．よって，$p(b)$ の符号は $\epsilon, b - a_i$ にしかよらないが，c の定め方から，$b - a_i$ の符号と $c - f(a_i)$ の符号は変わらない．ゆえに，$p(b)$ と $g(p(b))$ の符号は一致する．
7. ゆえに，$F_1(b) \models \phi(b, \bar{a}) \iff F_2(c) \models \phi(c, \bar{a})$ で，$K_3 \models \phi(c, \bar{a})$. $K_3 \models \exists x\, \phi(x, \bar{a})$ より $K_2 \models \exists x\, \phi(x, \bar{a})$.

□

Corollary

RCF はモデル完全であり，かつ完全である．

Proof.

まず，モデル完全性は QE から直接導かれる．さらに，完全であることは，すべての実閉体は標数が 0 なので $\mathbb{Q}$ の実閉包 A を含むことから示される．実際，任意の閉論理式 ϕ と，任意の RCF のモデル $\mathcal{M}, \mathcal{N}$ に対して，

$$\mathcal{M} \models \phi \iff A \models \phi \iff \mathcal{N} \models \phi$$

となる． □

モデル完全性の応用例として，Hilbert の第 17 問題がある．

Theorem

R を実閉体とし，$f(\bar{X}) \in R[\bar{X}]$ とする．このとき，すべての $\bar{a} \in R^n$ に対して $f(\bar{a}) \geq 0$ ならば，f は有理関数の二乗和で書くことができる．

Proof.

$f(\bar{X}) \in R[\bar{X}]$ は有理関数の二乗和で書くことができないとする．$R(\bar{X})$ は形式的実なので，$f(\bar{X})$ を負にするような順序を入れることができる．このように順序を入れた $R(\bar{X})$ の実閉包を K とすると，

$$K \models \exists \bar{v}\ f(\bar{v}) < 0.$$

モデル完全性より，

$$R \models \exists \bar{v}\ f(\bar{v}) < 0.$$

□

実代数幾何の文脈では次のような集合が興味の対象である．

Definition

R を実閉体とする．$X \subseteq R^n$ が半代数集合であるとは，多項式の連立不等式の解空間となっていることである．

RCF は QE を許すので，半代数的であることと定義可能であることは同値である．特に 1 次元の場合は次が成り立っている．

Theorem

R を実閉体とする．R の定義可能集合は有限個の点と有限個の区間の和である．

この事実は RCF の o-minimality とよばれる．では，2 次元以上の定義可能集合はどのようなものだろうか？

帰納的に n-cell という定義可能集合のクラスを定義する．

- $X \subseteq F^n$ が 0-cell であるとは，X が一点集合であること．
- $X \subseteq F$ が 1-cell であるとは，X が開区間 (a, b) であること．[1]
- $Y \subseteq F^{m+1}$ が n-cell であるとは，ある n-cell $X \subseteq F^m$ と定義可能な連続関数 $f : X \to F$ が存在して，

$$Y = \{(x, f(x)) \mid x \in X\}$$

となること．

- $X \subseteq F^{n+1}$ が $(n+1)$-cell であるとは，ある n-cell $X \subseteq F^n$ と，ある定義可能関数 $f, g : X \to F$ が存在して，$f(x) < g(x)$ がすべての $x \in X$ に対して成りたち，

$$Y = \{(x, y) \mid x \in X \wedge f(x) < y < g(x)\}$$

となることである．[2]

[1] ただし，$a = -\infty, b = \infty$ の場合も含める．
[2] ただし，f や g として，$f : X \to \{-\infty\}, g : X \to \{\infty\}$ の場合も許すことにする．

時間の都合上，単なる結果の紹介にとどめるが，証明は今まで話した知識だけで理解することができる．

Theorem (Cell Decomposition)

$X \subseteq F^n$ を半代数的集合とすると，互いに交わらない有限個の cell たち $C_1, \ldots, C_k$ が存在して，

$$X = C_1 \cup C_2 \cup \cdots \cup C_k$$

となる．

面白いことに cell decomposition を先に証明することで，QE の構成的証明を得ることもできる．さらに，その証明は QE をするための効率の良いアルゴリズムを与える．$\mathbb{R}$ 上の QF 論理式の真偽判定は，連立不等式の問題に過ぎないので，(順序体としての）$\mathbb{R}$ についての命題の真偽はすべてコンピュータで判定できる．