有限オートマトンと Presburger 算術

y. (@waidotto)

数学的な主張を，記号を用いて表すことを考えてみましょう．ひとまず，

$$\wedge, \vee, \neg, \to, \forall, \exists, 0, 1, +, \times, =, < \tag{1}$$

などの論理記号・定数記号・関数記号・関係記号があれば，自然数 (ここでは非負整数のこと) に関する様々な主張を論理式で表すことができます．例えば，「p が素数である」という日本語で書かれた主張は

$$1 < p \wedge \forall u \forall v[u < p \wedge v < p \to u \times v \neq p] \tag{2}$$

のように論理式の形に書くことができます (ここで，$\forall$ や $\exists$ で指定されている変数は自然数の範囲を動くものとします)．この論理式 (2) を $\mathrm{Prime}(p)$ と略記することにすれば，素数が無限に存在するという主張

$$\forall n \exists p[n < p \wedge \mathrm{Prime}(p)] \tag{3}$$

なども書くことができます．この主張が正しいことは皆さん先刻ご承知のことでしょう．論理式 (3) を少し変形して

$$\forall n \exists p[n < p \wedge \mathrm{Prime}(p) \wedge \mathrm{Prime}(p+2)] \tag{4}$$

としてみるとどうでしょうか．この論理式 (4) は双子素数予想と呼ばれている主張で，その真偽は 2018 年現在未解決です．

このように，(1) のようなごくごく小さな語彙であっても真偽の判定が非常に難しい主張を書くことができます．してみると，(1) を用いて書ける主張の全体を考えたならば，その中には双子素数予想よりもはるかに難しい魑魅魍魎が跋扈しているに違いありません．これでは全ての主張の真偽を確かめることなど夢のまた夢です．しかしその一方で，人類はかの有名な Fermat の最終定理でさえも，360 年の格闘の末についには証明に成功しました．ですから，いつかは (1) を用いて書き表されるあらゆる主張の真偽が確かめられる日が来ると信じたくなります．

いったいどちらが正しいのでしょうか？ 実は，Gödel の第一不完全性定理によって，そのような日は永遠に来ないことがわかっています．つまり，(1) を用いて書ける全ての主張に，真または偽のラベルを正しく割り当てるような機械的手続き (プログラム) をあらかじめ用意しておくことはできないというのです．

どうしてこのようなことが起こってしまうのでしょうか？ その理由のひとつには，(1) の語彙の表現能力が (見た目に反して)「高すぎる」ことが挙げられます．実は，足し算 $+$ と掛け算 $\times$ があれば，あらゆる計算可能な関数を論理式で表現できることが知られています．そのため，(1) を用いて書かれた主張の真偽を判定することは「少なくとも」Turing 機械の停止問題を解く以上に難しいということになるのです．

以上までで，足し算 $+$ と掛け算 $\times$ を同時に使用することが悲劇の原因であることはわかりました．では，掛け算 $\times$ の記号の使用を禁止したらどうでしょうか．小学校で習うように，掛け算は足し算の繰り返しで定義できるので，(1) から掛け算 $\times$ の記号を取り除いても論理式の表現力は変わらないのではないかと思われるかもしれません．ところが，実際にはこの足し算のみの弱い算術の理論 (**Presburger 算術**) は決定可能になることが知られています．すなわち，掛け算 $\times$ が含まれないどんな主張についてもその真偽を正しく判定するような，ひとつのアルゴリズムを作ることができるのです．本講演ではこのことを証明します．

Presburger 算術の決定可能性の証明にはたいていは量化記号消去の技法が用いられますが，ここでは**有限オートマトン** (finite automaton) を使ったわかりやすい証明を紹介しようと思います．余力があれば周辺の話題についても触れたいと思います．

前提知識は特にありませんが，$\forall, \exists$ などの記号に拒否反応がなければ大丈夫です．(たとえば結城 [3] を読んでいれば十分です．)

参考文献

[1] M. Sipser (太田和夫・田中圭介 監訳, 阿部正幸・植田広樹・藤岡淳・渡辺治 訳), 計算理論の基礎 [原著第 2 版] 1. オートマトンと言語, 共立出版, 2008.

[2] M. Sipser (太田和夫・田中圭介 監訳, 阿部正幸・植田広樹・藤岡淳・渡辺治 訳), 計算理論の基礎 [原著第 2 版] 2. 計算可能性の理論, 共立出版, 2008.

[3] 結城浩. 数学ガール／ゲーデルの不完全性定理. ソフトバンククリエイティブ, 2009.