$\mathbb{F}_2$ 線形演算と算術和が絡む連立方程式が解を持つか判定する問題は NP 完全

でぃぐ (@fujidig)

2019 年 12 月 14 日

定義. 式を次のように再帰的に定義する.

1. 変数記号は式.
2. s, t が式ならば $s \operatorname{xor} t$ も式.
3. t が式で $c \in \mathbb{N}$ ならば $t \,\&\, c$ も式.
4. t が式で $n \in \mathbb{N}$ ならば $t \gg n$ も式.
5. t が式で $n \in \mathbb{N}$ ならば $t \ll n$ も式.
6. t が式で $c \in \mathbb{N}$ ならば $t + c$ も式.

定義. 変数記号から自然数への対応を**割り当て**という. 式とそこに現れる変数をすべて割り当てる割り当てがあったときその自然数値を取る**解釈**が自然に定まる. ただし, $\operatorname{xor}, \&, \gg, \ll, +$ はそれぞれ排他的論理和, 論理積, 右ビットシフト, 左ビットシフト, 算術和で解釈する. 式 t に対して変数に変数名の若い方から順に $a_1, a_2, \dots$ を割り当てる割り当てでの解釈を $t(a_1, a_2, \dots)$ と書く.

問題 ($\mathbb{F}_2$ 線形演算と算術和の方程式の解の存在性)**.** 表れる変数が x のみの式 $t_1, \dots, t_n$ と自然数 m と自然数 $a_1, \dots, a_n$ が与えられる. ある $x < 2^m$ が存在して方程式

$$t_1(x) = a_1, \dots, t_n(x) = a_n$$

を満たすかという問題を「$\mathbb{F}_2$ **線形演算演算と算術和の方程式の解の存在性問題**」と呼ぶことにする.

定理 1. $\mathbb{F}_2$ 線形演算と算術和の方程式の解の存在性問題は NP 完全である.

算術和が式に含まれていなければすべて $\mathbb{F}_2$ 線形演算なので線形代数で片付く問題なことに注意しよう.

定理の証明. 解の候補が与えられたとき, それが解になるかどうかは多項式時間でできるので NP 問題なことはよい. NP 完全性は CNF-SAT を帰着させる.

節 φ が

$$\varphi \equiv X_{i_1} \vee \cdots \vee X_{i_r} \vee \overline{X_{i_{r+1}}} \vee \cdots \vee \overline{X_s}$$

のとき式 t_φ を次で定義する:

$$\begin{aligned} t_\varphi =& ((x \gg i_1) \,\&\, 1) \operatorname{xor} (((x \gg i_2) \,\&\, 1) \ll 1) \operatorname{xor} \cdots \operatorname{xor} (((x \gg i_r) \,\&\, 1) \ll (r-1)) \operatorname{xor} \\ & ((((x \gg i_{r+1}) \operatorname{xor} 1) \,\&\, 1) \ll r) \operatorname{xor} ((((x \gg i_{r+2}) \operatorname{xor} 1) \,\&\, 1) \ll (r+1)) \operatorname{xor} \\ & \cdots \operatorname{xor} ((((x \gg i_r) \operatorname{xor} 1) \,\&\, 1) \ll (s-1)). \end{aligned}$$

直観的にはこれはすべての変数の真偽値割り当てのビット列 x から φ に現れる変数の真偽値割り当てだけを集めてできるビット列を表している．そして式 y_φ を次で定義する:

$$s_\varphi = (((t_\varphi + (2^{s+1} - 1)) \gg s) \operatorname{xor} 1) \,\&\, 1.$$

ここで算術和を使って論理和を翻訳していることがポイントである．このとき

$$\begin{aligned} &\text{変数の数 } m \text{ の CNF 論理式 } \varphi_1 \wedge \cdots \wedge \varphi_n \text{ を真にする真偽割り当てが存在} \\ \iff\ &\text{方程式 } s_{\varphi_1}(x) = 0, \ldots, s_{\varphi_n}(x) = 0 \text{ の解 } x < 2^m \text{ が存在} \end{aligned}$$

となる．さらにこの CNF の入力から「$\mathbb{F}_2$ 線形演算と算術和の方程式の解の存在性問題」の入力を作る作業は多項式時間で行える．よって，CNF を「$\mathbb{F}_2$ 線形演算と算術和の方程式の解の存在性問題」に多項式時間還元できた．CNF は NP 完全だったので「$\mathbb{F}_2$ 線形演算と算術和の方程式の解の存在性問題」も NP 完全である． □

参考文献

[1] Aviezri S Fraenkel and Yaacov Yesha. “Complexity of problems in games, graphs and algebraic equations”. In: *Discrete Applied Mathematics* 1.1-2 (1979), pp. 15–30.