数理解析研究所講究録
第 1873 巻 2014 年 98-101

NP 完全問題の行列表現

富山化学工業株式会社　松木　伯元
Norichika Matsuki
Toyama Chemical Co., Ltd.

1．はじめに

$f(x_1,\ldots,x_n)\in Q[x_1,\ldots,x_n]$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもつか判定する問題を考えよう（本稿ではこの問題を 0-1SOL と省略して呼ぶことにする)。0-1SOL は代表的な NP 完全問題である 3-SAT[1]を特殊な場合として含む。なぜなら 3-SAT は

$$f(x_1,\ldots,x_n)=y_{11}y_{12}y_{13}+\cdots+y_{m1}y_{m2}y_{m3} \quad (y_{11},\ldots,y_{m1}\in\{x_1,1-x_1,\ldots,x_n,1-x_n\})$$

とおいた場合と同値だからである[2]。そのため計算複雑性が NP に属する問題はすべて 0-1SOL の形式で表されるが、残念ながら 0-1SOL を効率良く解くためのアルゴリズムは存在しないと強く予想されている（$P\neq NP$ 予想)。

本稿では、まず 0-1SOL を環論的に特徴づけ、表現論を通じて $f(x_1,\ldots,x_n)$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもつための必要十分条件が行列式で与えられることを示す。そして 0-1SOL を変数変換した問題である $f(x_1,\ldots,x_n)\in Q[x_1,\ldots,x_n]$が$\{-1,1\}\times\cdots\times\{-1,1\}$に零点をもつか判定する問題（これを$\pm$1SOL と呼ぶことにする）に対しても同様なことが成り立つことにふれる。

2．0-1SOL の代数的特徴

$I_n=(x_1(1-x_1),\ldots,x_n(1-x_n))\subset Q[x_1,\ldots,x_n]$をイデアルとする。このとき次が成り立つ（証明は[3]参照)。

補題 1 任意の $c_1,\ldots,c_n\in\{0,1\}$に対して $f(c_1,\ldots,c_n)=0$ であるためには、

$$f(x_1,\ldots,x_n)\equiv 0 \pmod{I_n}$$

が成り立つことが必要十分である。

これから次の補題が導かれる。

補題 2 $f(x_1,\ldots,x_n)\in Q[x_1,\ldots,x_n]$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもつためには、$f(x_1,\ldots,x_n)$が $Q[x_1,\ldots,x_n]/I_n$ の零元か零因子であることが必要十分である。

証明 十分性：$f(x_1,\ldots,x_n)\neq 0$ となる点$(c_1,\ldots,c_n)\in\{0,1\}\times\cdots\times\{0,1\}$に対して$\Pi((x_1-c_1)^2+\cdots+(x_n-c_n)^2)$をとれば

$$f(x_1,\ldots,x_n)\Pi((x_1-c_1)^2+\cdots+(x_n-c_n)^2)\equiv 0 \pmod{I_n}$$

必要性：$f(x_1,\ldots,x_n)$が $Q[x_1,\ldots,x_n]/I_n$ の零因子であれば、補題 1 から$\{0,1\}\times\cdots\times\{0,1\}$に零点をもたなければならいことが分かる。

補題 3 $f(x_1,\dots,x_n)\in Q[x_1,\dots,x_n]$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもたないためには、$f(x_1,\dots,x_n)$が$Q[x_1,\dots,x_n]/I_n$の可逆元であることが必要十分である。

証明 $f(x_1,\dots,x_n)$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもたないとき、

$$\Sigma(1-(x_1-c_1)^2)\cdots(1-(x_n-c_n)^2)/f(c_1,\dots,c_n)$$

（和はすべての$c_1,\dots,c_n\in\{0,1\}$にわたってとる）がその逆元である。逆は補題 2 から明らか。

補題 2,3 から $Q[x_1,\dots,x_n]/I_n$は零元、零因子、可逆元から構成されることが分かる。

3．0-1SOL の判定式

いま $f\equiv a_0+\Sigma a_ix_i+\Sigma a_{ij}x_ix_j+\cdots+a_{1\dots n}x_1\cdots x_n \pmod{I_n}$に対して、$Q[x_1,\dots,x_n]/I_n$から$2^n$次行列への写像$T(f)=(t_{ij})$を次のように定義する。

①$i\neq j$ならば $t_{ij}=0$

②$a_0,a_1,\dots,a_n,a_{12},a_{13},\dots,a_{n-1n},a_{123},\dots,a_{1\dots n}$を次数付辞書式順序に並べて i 番目が $a_{i(1)\cdots i(k)}$のとき $t_{ii}=a_0+a_{i(1)}+\cdots+a_{i(k)}+a_{i(1)i(2)}+\cdots+a_{i(k-1)i(k)}+\cdots+a_{i(1)\cdots i(k)}$

このとき次の性質が容易に導かれる。

補題 4 T は環準同型である。

そして補題 2,3,4 から直ちに次が従う。

定理 5 $f(x_1,\dots,x_n)\in Q[x_1,\dots,x_n]$が$\{0,1\}\times\cdots\times\{0,1\}$に零点をもつためには、$\det T(f)=0$であることが必要十分である。

しかしながら $\det T(f)=\Pi f(c_1,\dots,c_n)$（積はすべての$c_1,\dots,c_n\in\{0,1\}$にわたってとる）であるため、この判定式は有益ではない。

4．±1SOL の場合

±1SOL は 0-1SOL と異なった様相を呈する。まず $J_n=(x_1^2-1,\dots,x_n^2-1)\subset Q[x_1,\dots,x_n]$をイデアルとし、$\{j_1,\dots,j_q\},\{k_1,\dots,k_r\}$に対して演算△を次のように定義する。

①$\{j_1,\dots,j_q\}\triangle\{k_1,\dots,k_r\}=\{j_1,\dots,j_q\}\cup\{k_1,\dots,k_r\}-\{j_1,\dots,j_q\}\cap\{k_1,\dots,k_r\}$

②$\{j_1,\dots,j_q\}\triangle\{0\}=\{0\}\triangle\{j_1,\dots,j_q\}=\{j_1,\dots,j_q\}$

③$\{j_1,\dots,j_q\}\triangle\{j_1,\dots,j_q\}=\{0\}$、$\{0\}\triangle\{0\}=\{0\}$

さらに $f\equiv a_0+\Sigma a_ix_i+\Sigma a_{ij}x_ix_j+\cdots+a_{1\dots n}x_1\cdots x_n \pmod{J_n}$に対して、$Q[x_1,\dots,x_n]/J_n$から$2^n$次行列への写像$S(f)=(s_{ij})$を次のように定義する。

①$a_0,a_1,\dots,a_n,a_{12},a_{13},\dots,a_{n-1n},a_{123},\dots,a_{1\dots n}$を次数付辞書式順序に並べて i 番目が $a_{i(1)\cdots i(k)}$のとき $s_{1i}=a_{i(1)\cdots i(k)}$

②もし $s_{1j}=a_{j(1)\cdots j(q)}$、$s_{1k}=a_{k(1)\cdots k(r)}$ならば $s_{jk}=a_{\{j(1),\cdots,j(q)\}\triangle\{k(1),\cdots,k(q)\}}$（ただし右辺の添え字から記号{、}、,を除く）

このとき補題 1～4 と同様の性質と、それゆえ次が成り立つ[4]。

定理 6 $f(x_1,\ldots,x_n)\in Q[x_1,\ldots,x_n]$が$\{-1,1\}\times\cdots\times\{-1,1\}$に零点をもつためには、$\det S(f)=0$ であることが必要十分である。

5．例

(1) 5 変数 3-SAT を±1SOL 型の多項式に変換すると

$$f(x_1,\ldots,x_5)=y_{11}y_{12}y_{13}+\cdots+y_{m1}y_{m2}y_{m3}\equiv a_0+\Sigma a_ix_i+\Sigma a_{ij}x_ix_j+\cdots+\Sigma a_{ijk}x_ix_jx_k \pmod{J_n}$$

（$y_{11},\ldots,y_{m1}\in\{(1\pm x_1)/2,\ldots,(1\pm x_5)/2\}$）となるから、5 変数 3-SAT に対応する行列式 det S(f)は次の通りである。

$$\begin{vmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_{12} & a_{13} & a_{14} & a_{15} & a_{23} & a_{24} & a_{26} & a_{34} & a_{35} & a_{45} & a_{123} & a_{124} & a_{125} & a_{134} & a_{135} & a_{145} & a_{234} & a_{235} & a_{245} & a_{345} & 0 & 0 & 0 & 0 & 0 & 0 \\
a_1 & a_0 & a_{12} & a_{13} & a_{14} & a_{15} & a_2 & a_3 & a_4 & a_5 & a_{123} & a_{124} & a_{125} & a_{134} & a_{135} & a_{145} & a_{23} & a_{24} & a_{25} & a_{34} & a_{35} & a_{45} & 0 & 0 & 0 & 0 & a_{234} & a_{235} & a_{245} & a_{345} & 0 & 0 \\
a_2 & a_{12} & a_0 & a_{23} & a_{24} & a_{25} & a_1 & a_{123} & a_{124} & a_{125} & a_3 & a_4 & a_5 & a_{234} & a_{235} & a_{245} & a_{13} & a_{14} & a_{15} & 0 & 0 & 0 & a_{34} & a_{35} & a_{45} & 0 & a_{134} & a_{135} & a_{145} & 0 & a_{345} & 0 \\
a_3 & a_{13} & a_{23} & a_0 & a_{34} & a_{35} & a_{123} & a_1 & a_{134} & a_{135} & a_2 & a_{234} & a_{235} & a_4 & a_5 & a_{345} & a_{12} & 0 & 0 & a_{14} & a_{15} & 0 & a_{24} & a_{25} & 0 & a_{45} & a_{124} & a_{125} & 0 & a_{145} & a_{245} & 0 \\
a_4 & a_{14} & a_{24} & a_{34} & a_0 & a_{45} & a_{124} & a_{134} & a_1 & a_{145} & a_{234} & a_2 & a_{245} & a_3 & a_{345} & a_5 & 0 & a_{12} & 0 & a_{13} & 0 & a_{15} & a_{23} & 0 & a_{25} & a_{35} & a_{123} & 0 & a_{125} & a_{135} & a_{235} & 0 \\
a_5 & a_{15} & a_{25} & a_{35} & a_{45} & a_0 & a_{125} & a_{135} & a_{145} & a_1 & a_{235} & a_{245} & a_2 & a_{345} & a_3 & a_4 & 0 & 0 & a_{12} & 0 & a_{13} & a_{14} & 0 & a_{23} & a_{24} & a_{34} & 0 & a_{123} & a_{124} & a_{134} & a_{234} & 0 \\
a_{12} & a_2 & a_1 & a_{123} & a_{124} & a_{125} & a_0 & a_{23} & a_{24} & a_{25} & a_{13} & a_{14} & a_{15} & 0 & 0 & 0 & a_3 & a_4 & a_5 & a_{234} & a_{235} & a_{245} & a_{134} & a_{135} & a_{145} & 0 & a_{34} & a_{35} & a_{45} & 0 & 0 & a_{345} \\
a_{13} & a_3 & a_{123} & a_1 & a_{134} & a_{135} & a_{23} & a_0 & a_{34} & a_{35} & a_{12} & 0 & 0 & a_{14} & a_{15} & 0 & a_2 & a_{234} & a_{235} & a_4 & a_5 & a_{345} & a_{124} & a_{125} & 0 & a_{145} & a_{24} & a_{25} & 0 & a_{45} & 0 & a_{245} \\
a_{14} & a_4 & a_{124} & a_{134} & a_1 & a_{145} & a_{24} & a_{34} & a_0 & a_{45} & 0 & a_{12} & 0 & a_{13} & 0 & a_{15} & a_{234} & a_2 & a_{245} & a_3 & a_{345} & a_5 & a_{123} & 0 & a_{125} & a_{135} & a_{23} & 0 & a_{25} & a_{35} & 0 & a_{235} \\
a_{15} & a_5 & a_{125} & a_{135} & a_{145} & a_1 & a_{25} & a_{35} & a_{45} & a_0 & 0 & 0 & a_{12} & 0 & a_{13} & a_{14} & a_{235} & a_{245} & a_2 & a_{345} & a_3 & a_4 & 0 & a_{123} & a_{124} & a_{134} & 0 & a_{23} & a_{24} & a_{34} & 0 & a_{234} \\
a_{23} & a_{123} & a_3 & a_2 & a_{234} & a_{235} & a_{13} & a_{12} & 0 & 0 & a_0 & a_{34} & a_{35} & a_{24} & a_{25} & 0 & a_1 & a_{134} & a_{135} & a_{124} & a_{125} & 0 & a_4 & a_5 & a_{345} & a_{245} & a_{14} & a_{15} & 0 & 0 & a_{45} & a_{145} \\
a_{24} & a_{124} & a_4 & a_{234} & a_2 & a_{245} & a_{14} & 0 & a_{12} & 0 & a_{34} & a_0 & a_{45} & a_{24} & 0 & a_{25} & a_{134} & a_1 & a_{145} & a_{123} & 0 & a_{124} & a_3 & a_{345} & a_5 & a_{235} & a_{13} & 0 & a_{15} & 0 & a_{35} & a_{135} \\
a_{25} & a_{125} & a_5 & a_{235} & a_{245} & a_2 & a_{15} & 0 & 0 & a_{12} & a_{35} & a_{45} & a_0 & 0 & a_{23} & a_{24} & a_{135} & a_{145} & a_1 & 0 & a_{123} & a_{124} & a_{345} & a_3 & a_4 & a_{234} & 0 & a_{13} & a_{14} & 0 & a_{34} & a_{134} \\
a_{34} & a_{134} & a_{234} & a_4 & a_3 & a_{345} & 0 & a_{14} & a_{13} & 0 & a_{24} & a_{24} & 0 & a_0 & a_{45} & a_{34} & a_{124} & a_{123} & 0 & a_1 & a_{145} & a_{135} & a_2 & a_{245} & a_{235} & a_5 & a_{12} & 0 & 0 & a_{15} & a_{25} & a_{125} \\
a_{35} & a_{135} & a_{235} & a_5 & a_{345} & a_3 & 0 & a_{15} & 0 & a_{13} & a_{25} & 0 & a_{23} & a_{45} & a_0 & a_{34} & a_{125} & 0 & a_{123} & a_{145} & a_1 & a_{134} & a_{245} & a_2 & a_{234} & a_4 & 0 & a_{12} & 0 & a_{14} & a_{24} & a_{124} \\
a_{45} & a_{145} & a_{245} & a_{345} & a_5 & a_4 & 0 & 0 & a_{15} & a_{14} & 0 & a_{25} & a_{24} & a_{35} & a_{34} & a_0 & 0 & a_{125} & a_{124} & a_{135} & a_{134} & a_1 & a_{235} & a_{234} & a_2 & a_3 & 0 & 0 & a_{12} & a_{13} & a_{23} & a_{123} \\
a_{123} & a_{23} & a_{13} & a_{12} & 0 & 0 & a_3 & a_2 & a_{234} & a_{235} & a_1 & a_{134} & a_{135} & a_{124} & a_{125} & 0 & a_0 & a_{34} & a_{35} & a_{24} & a_{25} & 0 & a_{14} & a_{15} & 0 & 0 & a_4 & a_5 & a_{345} & a_{245} & a_{145} & a_{45} \\
a_{124} & a_{24} & a_{14} & 0 & a_{12} & 0 & a_4 & a_{234} & a_2 & a_{245} & a_{134} & a_1 & a_{145} & a_{123} & 0 & a_{125} & a_{34} & a_0 & a_{45} & a_{23} & 0 & a_{25} & a_{13} & 0 & a_{15} & 0 & a_3 & a_{345} & a_5 & a_{235} & a_{135} & a_{35} \\
a_{125} & a_{25} & a_{15} & 0 & 0 & a_{12} & a_5 & a_{235} & a_{245} & a_2 & a_{135} & a_{145} & a_1 & 0 & a_{123} & a_{124} & a_{35} & a_{45} & a_0 & 0 & a_{23} & a_{24} & 0 & a_{13} & a_{14} & 0 & a_{345} & a_3 & a_4 & a_{234} & a_{134} & a_{34} \\
a_{134} & a_{34} & 0 & a_{14} & a_{13} & 0 & a_{234} & a_4 & a_3 & a_{345} & a_{124} & a_{123} & 0 & a_1 & a_{145} & a_{135} & a_{24} & a_{23} & 0 & a_0 & a_{45} & a_{35} & a_{12} & 0 & 0 & a_{15} & a_2 & a_{245} & a_{235} & a_5 & a_{125} & a_{25} \\
a_{135} & a_{35} & 0 & a_{15} & 0 & a_{13} & a_{235} & a_5 & a_{345} & a_3 & a_{125} & 0 & a_{123} & a_{145} & a_1 & a_{134} & a_{25} & 0 & a_{23} & a_{45} & a_0 & a_{34} & 0 & a_{12} & 0 & a_{14} & a_{245} & a_2 & a_{234} & a_4 & a_{124} & a_{24} \\
a_{145} & a_{45} & 0 & 0 & a_{15} & a_{14} & a_{245} & a_{345} & a_5 & a_4 & 0 & a_{124} & a_{124} & a_{135} & a_{134} & a_1 & 0 & a_{25} & a_{24} & a_{35} & a_{34} & a_0 & 0 & 0 & a_{12} & a_{13} & a_{235} & a_{134} & a_2 & a_3 & a_{123} & a_{23} \\
a_{234} & 0 & a_{34} & a_{24} & a_{23} & 0 & a_{134} & a_{124} & a_{123} & 0 & a_4 & a_3 & a_{345} & a_2 & a_{245} & a_{235} & a_{14} & a_{13} & 0 & a_{12} & 0 & 0 & a_0 & a_{45} & a_{35} & a_{25} & a_1 & a_{145} & a_{135} & a_{125} & a_5 & a_{15} \\
a_{235} & 0 & a_{35} & a_{25} & 0 & a_{23} & a_{135} & a_{125} & 0 & a_{123} & a_5 & a_{345} & a_3 & a_{245} & a_2 & a_{234} & a_{15} & 0 & a_{13} & 0 & a_{12} & 0 & a_{45} & a_0 & a_{34} & a_{24} & a_{145} & a_1 & a_{134} & a_{124} & a_4 & a_{14} \\
a_{245} & 0 & a_{45} & 0 & a_{25} & a_{24} & a_{145} & 0 & a_{125} & a_{124} & a_{345} & a_5 & a_4 & a_{235} & a_{234} & a_2 & 0 & a_{15} & a_{14} & 0 & 0 & a_{12} & a_{35} & a_{34} & a_0 & a_{23} & a_{135} & a_{134} & a_1 & a_{123} & a_3 & a_{13} \\
a_{345} & 0 & 0 & a_{45} & a_{35} & a_{34} & 0 & a_{145} & a_{135} & a_{134} & a_{245} & a_{235} & a_{234} & a_5 & a_4 & a_3 & 0 & 0 & 0 & a_{15} & a_{14} & a_{13} & a_{25} & a_{24} & a_{23} & a_0 & a_{125} & a_{124} & a_{123} & a_1 & a_2 & a_{12} \\
0 & a_{234} & a_{134} & a_{124} & a_{123} & 0 & a_{34} & a_{24} & a_{23} & 0 & a_{14} & a_{13} & 0 & a_{12} & 0 & 0 & a_4 & a_3 & a_{345} & a_2 & a_{245} & a_{235} & a_1 & a_{145} & a_{135} & a_{125} & a_0 & a_{45} & a_{35} & a_{25} & a_{15} & a_5 \\
0 & a_{235} & a_{135} & a_{125} & 0 & a_{123} & a_{35} & a_{25} & 0 & a_{23} & a_{15} & 0 & a_{13} & 0 & a_{12} & 0 & a_5 & a_{345} & a_3 & a_{245} & a_2 & a_{134} & a_{145} & a_1 & a_{134} & a_{124} & a_{45} & a_0 & a_{34} & a_{24} & a_{14} & a_4 \\
0 & a_{245} & a_{145} & 0 & a_{125} & a_{124} & a_{45} & 0 & a_{25} & a_{24} & 0 & a_{15} & a_{14} & 0 & 0 & a_{12} & a_{345} & a_5 & a_4 & a_{235} & a_{234} & a_2 & a_{135} & a_{134} & a_1 & a_{123} & a_{35} & a_{34} & a_0 & a_{23} & a_{13} & a_3 \\
0 & a_{345} & 0 & a_{145} & a_{135} & a_{134} & 0 & a_{45} & a_{35} & a_{34} & 0 & 0 & 0 & a_{15} & a_{14} & a_{13} & a_{245} & a_{235} & a_{234} & a_5 & a_4 & a_3 & a_{125} & a_{124} & a_{123} & a_1 & a_{25} & a_{24} & a_{23} & a_0 & a_{12} & a_2 \\
0 & 0 & a_{345} & a_{245} & a_{235} & a_{234} & 0 & 0 & 0 & 0 & a_{45} & a_{35} & a_{34} & a_{25} & a_{24} & a_{23} & a_{145} & a_{135} & a_{134} & a_{125} & a_{124} & a_{123} & a_5 & a_4 & a_3 & a_2 & a_{15} & a_{14} & a_{13} & a_{12} & a_0 & a_1 \\
0 & 0 & 0 & 0 & 0 & 0 & a_{345} & a_{245} & a_{235} & a_{234} & a_{145} & a_{135} & a_{134} & a_{125} & a_{124} & a_{123} & a_{45} & a_{35} & a_{34} & a_{25} & a_{24} & a_{23} & a_{15} & a_{14} & a_{13} & a_{12} & a_5 & a_4 & a_3 & a_2 & a_1 & a_0
\end{vmatrix}$$

(2) ±1 から成る n 次正方行列 H で $H^tH=nE$（E は単位行列）を満たすものはアダマール行列と呼ばれている。組合せ論で有名な未解決問題であるアダマール予想は、すべての 4 の倍数 n に対してアダマール行列が存在するという予想である（例えば[5]参照）。ここでアダマール行列の存在は

$$h_n=\Sigma_{i<j}(x_{i1}x_{j1}+\cdots+x_{in}x_{jn})^2$$

が$\{-1,1\}\times\cdots\times\{-1,1\}$に零点をもつことと同値であるから、上記予想を証明するには、

すべての 4 の倍数 n に対して det $S(h_n)=0$ が成り立つことを示せばよい。しかし計算は容易ではない。

参考文献

[1] S. A. Cook, The complexity of theorem-procedures, in Proceedings of the 3rd ACM Symposium on Theory of Computing (1971) 151-158.

[2] N. Matsuki, An analytic criterion for CSAT, Inform. Process. Lett., 112 (2012) 164-165.

[3] N. Matsuki, A note on Diophantine equations over finite fields, Univers. J. Math. Math. Sci. 3 (2013) 105-108.

[4] N. Matsuki, The linear representations of decision problems, submitted for publication.

[5] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block design, in Contemporary Design Theory, A Collection of Surveys (J. H. Dinitz and D. R. Stinson, eds.), John Wiley & Sons, New York, 1992, 431-560.