#P-complete problems and linear representations

Norichika Matsuki
Toyama Chemical Co., Ltd.

1 Introduction

Let \( I_n = (x_1^2 - 1, \ldots, x_n^2 - 1) \) be an ideal of \( \mathbb{Q}[x_1, \ldots, x_n] \) and let \( R_n = \mathbb{Q}[x_1, \ldots, x_n]/I_n \).

For \( f \in \mathbb{Q}[x_1, \ldots, x_n] \), we define \( \overline{f} \) as the right-hand side of the congruence

\[
\overline{f} \equiv \sum_{S \subseteq \{1, \ldots, n\}} a_S x^S \pmod{I_n},
\]

where \( x^S \) is a multilinear monomial that has factor \( x_i \) if and only if \( i \in S \). Denote by \( S_i \) the \( i \)-th set of the lexicographically ordered sets

\[
\emptyset < \{n\} < \{n-1\} < \{n-1, n\} < \{n-2\} < \cdots < \{1\} < \cdots < \{1, \ldots, n\}.
\]

We define \( T(\overline{f}) = (T(\overline{f})_{ij}) \) to be the matrix whose \((i, j)\) entry is \( a_{S_i \triangle S_j} \), where \( S_i \triangle S_j \) is the symmetric difference of \( S_i \) and \( S_j \). Then the following properties hold [4, 5]:

1. \( f \) has a zero point in \((-1, 1)^n\) if and only if \( f \) is either a zero element or a zero divisor of \( R_n \).
2. \( f \) has no zero point in \((-1, 1)^n\) if and only if \( f \) is a unit of \( R_n \).
3. \( T \) is an injective ring homomorphism from \( R_n \) to \( M(2^n, \mathbb{Q}) \).
4. \( f \) has a zero point in \((-1, 1)^n\) if and only if \( \det T(\overline{f}) = 0 \).

In this article, we describe the problem of counting the number of zero points in \((-1, 1)^n\) of \( f \). This is \#P-complete [9], so that it relates to many counting problems in discrete mathematics.

2 Number of zero points and rank of a matrix

Denote by \( v^t \) the transpose of a vector \( v \) and by \( v_i \) the column vector

\[
(1, c_{1n}, c_{n-1}, c_{n-1}c_{n}, c_{n-2}, \ldots, c_{i1}, \ldots, c_{i1} \cdots c_{in})^t,
\]

where \( c_{ij} = (-1)^{(i-1)/2^{j-1}} \) for \( 1 \leq i \leq 2^n \) and \( 1 \leq j \leq n \), namely,

\[
(c_{1j}, c_{2j}, \ldots, c_{2^n j}) = \left(\underbrace{1, \ldots, 1}_{2^{j-1}}, \underbrace{-1, \ldots, -1}_{2^{j-1}}\right).
\]

\((v_1, \ldots, v_{2^n})\) is an Hadamard matrix and \((v_1, \ldots, v_{2^n})\) are eigenvectors of \( T(\overline{f}) \). Hence we have the following theorem [6].
Theorem 1 Let $n(f)$ be the number of zero points in $\{-1, 1\}^n$ of $f \in \mathbb{Q}[x_1, \ldots, x_n]$. Then $n(f) = 2^n - \text{rank } T(\overline{f})$.

Next we consider a polynomial $f = a_0x^{p-2} + a_1x^{p-3} + \cdots + a_{p-2}$ over $\mathbb{F}_p$. We write

$$D = \begin{pmatrix}
a_0 & a_1 & \cdots & a_{p-2} \\
a_1 & a_2 & \cdots & a_0 \\
\cdots & \cdots & \cdots & \cdots \\
a_{p-2} & a_0 & \cdots & a_{p-3}
\end{pmatrix}.$$  

Kronecker proved that the number of roots distinct from one another and from zero of $f \equiv 0 \pmod{p}$ is $p - 1 - \text{rank } D$ (see [3]). Here $D$ can be interpreted as a linear representation of $\mathbb{F}_p[x]/(x^{p-1} - 1)$ in the same way as $T$.

3 Application

We apply Theorem 1 to the n-queens problem (see [1] for details).

Let $Q(n)$ be the number of ways to place $n$ nonattacking queens on an $n \times n$ board and let

$$f_i = \sum_{j=1}^{n} \left( \frac{x_{ij} + 1}{2} \right)^2 - 1, \quad g_i = \sum_{j=1}^{n} \left( \frac{x_{ji} + 1}{2} \right)^2 - 1,$$

$$h_k = \left( \sum_{i+j=k} \left( \frac{x_{ij} + 1}{2} \right)^2 \right) \left( \sum_{i+j=k} \left( \frac{x_{ij} + 1}{2} \right)^2 - 1 \right),$$

$$l_k = \left( \sum_{i-j=k} \left( \frac{x_{ij} + 1}{2} \right)^2 \right) \left( \sum_{i-j=k} \left( \frac{x_{ij} + 1}{2} \right)^2 - 1 \right).$$

Since there are $n$ nonattacking queens if and only if

$$q_n = \sum_{i=1}^{n} (f_i^2 + g_i^2) + \sum_{k=2}^{2n} h_k^2 + \sum_{k=-n+1}^{n-1} l_k^2$$

has a zero points in $\{-1, 1\}^n$, we have $Q(n) = 2^{n^2} - \text{rank } T(\overline{q_n})$.

4 System of polynomial equations

For the common solutions of a system of polynomial equations, we can not yet find the above relation with linear representation. Instead, we give an analogue of Smale's discussion [8]. The problem deciding whether a system of polynomial equations

$$\begin{align*}
s_1 &= a_{10} + \sum_{i=1}^{3} a_{1i}x_{1i} + \sum_{i<j} a_{1ij}x_{1i}x_{1j} + a_{1123}x_{11}x_{12}x_{13} = 0 \\
\vdots \\
s_m &= a_{m0} + \sum_{i=1}^{3} a_{mi}x_{mi} + \sum_{i<j} a_{mij}x_{mi}x_{mj} + a_{m123}x_{m1}x_{m2}x_{m3} = 0
\end{align*}$$

(1)
$(s_1, \ldots, s_m \in \mathbb{F}_2[x_1, \ldots, x_n])$ has a common solution in $\mathbb{F}_2^n$ is equivalent to 3-SAT [2]. From the following theorem [7], we see that (1) has no common solution in $\mathbb{F}_2^n$ if and only if there are $t_1, \ldots, t_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ such that

$$s_1 t_1 + \cdots + s_m t_m \equiv 1 \pmod{(x_1^2 - x_1, \ldots, x_n^2 - x_n)},$$

where $(x_1^2 - x_1, \ldots, x_n^2 - x_n)$ is an ideal of $\mathbb{F}_2[x_1, \ldots, x_n]$.

**Theorem 2** Let $(x_1^p - x_1, \ldots, x_n^p - x_n)$ is an ideal of $\mathbb{F}_p[x_1, \ldots, x_n]$. Then $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ has a zero point in $\mathbb{F}_p^n$ if and only if

$$f^{p-1} \not\equiv 1 \pmod{(x_1^p - x_1, \ldots, x_n^p - x_n)}.$$

Hence this problem is reduced to the system of linear equations whose unknowns are the coefficients of $t_1, \ldots, t_m$ and the computational complexity depends on $\max\{\deg t_1, \ldots, \deg t_m\}$.

**References**


