秘密分散法における量子超越性の符号理論にもとづく探求

発表者の趣味の研究です

Ryutaroh Matsumoto

Nagoya University, Japan
Send your comments to ryutaroh.matsumoto@nagoya-u.jp

September 2018
@ 符号理論のワークショップ

量子超越性ってなに？

Quantum supremacy or quantum advantage is the potential ability of quantum computing devices to solve problems that classical computers practically cannot. (Wikipedia)

本講演では

- 古典物理学的な情報処理では出来ないことが量子的には出来る
- 古典物理学的な情報処理よりも量子的に速く出来る

という意味で量子超越性を使う。量子情報処理と古典情報処理の違いをより明確化するために量子超越性の研究は大事でしょう

どのような量子超越性を紹介するのか？

秘密分散法で、古典情報処理を用いると実現出来ないアクセス構造を、
量子情報処理を用いると実現出来ることを紹介する

秘密分散法の例 (Shamir-Blakley)

$\mathbf{F}_q \ni s$: 秘密
n: 秘密分散への参加者の数
$\mathbf{F}_q \ni \alpha_1, \ldots, \alpha_n$: 非ゼロ定数

1. $f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$ をランダムに選ぶ
2. $f(\alpha_i)$ を第 i 参加者に配る

- $k-1$ 人以下の参加者の情報からは s がわからない
- k 人以上の参加者は s を再構成できる

シェア: 参加者に配るデータ（この場合 $f(\alpha_i)$）

秘密分散法のアクセス構造とは何ぞや？

禁止集合: 秘密に関してなんの情報も持たない参加者の集合 (先程の例だと $k-1$ 人以下の参加者の集合はすべて禁止集合)
有資格集合: 秘密を再構成できる参加者の集合 (先程の例だと k 人以上の参加者の集合はすべて有資格集合)

アクセス構造: 参加者の集合のうちどれが有資格または禁止集合になるのかという構造

古典情報処理で実現出来ないアクセス構造

目標: 1 ビットの秘密を 5 人に配布し、 3 人集まると再構成出来るが 2 人しか集まらないと何もわからないようにしたい。
解法：Shamir-Blakley の方法で有限体 q の大きさを 7 以上にすれば実現出来る。しかし 1 ビットの秘密を $\log_2 7$ ビットのシェアに格納していて効率が悪い

各シェアを 1 量子ビットにすると、上記目標を達成し、1 ビットの秘密を最大 1 ビットしか格納出来ない 1 量子ビットのシェアに格納しているから効率がよい

本講演では、各シェアを 1 ビットにすると実現出来ないが、各シェアを 1 量子ビットにすると実現出来るアクセス構造について議論する。

量子ビットとは何ぞや？（わからなくても後に差し支えない）

量子状態は（長さ 1 の）複素縦ベクトルで表される。縦ベクトルを $|0\rangle$ などと書く（ここで 0 はベクトルの添字でありゼロベクトルではない）
1 量子ビット: 2 次元複素線形空間で表される量子状態で、その正規直交基底を通常 $\{|0\rangle, |1\rangle\}$ で表す
n 量子ビット: 1 量子ビットを n 個並べたもので、2^n 次元複素線形空間で表され、その正規直交基底を通常 $\{|v\rangle \mid v \in \{0,1\}^n\}$ で表す

量子超越性を示す秘密分散法

秘密がビット 0 であるときは

$$
\begin{aligned}
&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\
&+ |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\
&- |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\
&- |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle,
\end{aligned}
$$

を 5 つのシェア (5 量子ビット) とし、秘密がビット 1 であるときは

$$
\begin{aligned}
&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\
&+ |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\
&- |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\
&- |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle.
\end{aligned}
$$

を 5 つのシェア (5 量子ビット) とし、各量子ビットを各参加者に配る

松本, IEICE Trans. Fundamentals, vol.E100-A, no.12, pp. 2738–2739, Dec. 2017

他に量子超越性を示す秘密分散法はあるのか？

先程の具体例を一般論のなかに位置づけ、量子超越性を示す他の例を探した。

二元量子誤り訂正符号と秘密分散法

k 量子ビットを n 量子ビットに符号化し、$d-1$ 個以下の量子消失誤り（誤り位置がわかっている量子誤り）を訂正できる量子誤り訂正符号を $[[n,k,d]]$ 量子符号と呼ぶ。
k ビットの秘密 $v \in \{0,1\}^k$ を量子情報 $|v\rangle$ に対応させてから $[[n,k,d]]$ 量子符号で符号化し、量子符号語の各量子ビットを各参加者に配ると古典情報を分散する量子秘密分散法になる（前述の例は $[[5,1,3]]$ 量子符号）

$n-d+1$ 人以上の参加者は必ず有資格集合になる。

小川らによる量子アクセス構造の性質

$\{1, \ldots, n\} \supset S$ が有資格集合である
$\Leftrightarrow \{1, \ldots, n\} \setminus S$ が禁止集合である (小川ら, PRA2005)

k ビットの秘密 $v \in \{0,1\}^k$ を量子情報 $|v\rangle$ に対応させてから $[[n,k,d]]$ 量子符号で符号化し、量子符号語の各量子ビットを各参加者に配ると古典情報を分散する量子秘密分散法になる (再掲)
$n-d+1$ 人以上の参加者は必ず有資格集合になる。(再掲、式◆とする)

$d-1$ 人以下の参加者は必ず禁止集合になる。(式◆◆)

古典情報処理により実現できるアクセス構造の限界

r 人以上の参加者は必ず有資格集合になる
t 人以下の参加者は必ず禁止集合になる
各シェアのサイズは $\log_2 q$ ビット、である場合必ず

$$r - t \geq \frac{r+1}{q} \tag{1}$$

が成立してしまう (Bogdanov, Guo and Komargodski, Theory of Cryptography 2016)。前ページの式（◆）、（◆◆）と式 (1) を組み合わせると

$$n + 2 - 2d < \frac{n+2-d}{2} \tag{2}$$

である $[[n, k, d]]$ 量子符号はアクセス構造に関する量子超越性を示す。

式の形から、n に対してなるべく d がの割合が大きくなる量子符号を用いると量子超越性を示す可能性が高いことがわかる

n に対して k と d がなるべく大きい量子符号の表を用いて量子超越性を探した

http://www.codetables.de/ に n に対して k と d をどこまで大きく出来るかをまとめた表がある。それを用いて式 (2) を満たす量子符号パラメータを探したところ

n	k	d
6	1	3
11	1	5
12	1	5
17	1	7
18	1	7
29	1	11
30	1	11

という量子符号がアクセス構造に関する量子超越性を示すことがわかった (松本, ISITA2018)

線形秘密分散法に対する量子超越性

秘密秘密法も線形性を持たないと符号化の計算量が膨大になるため、実用上は線形秘密分散法が主に使われる。有資格集合のシェアから秘密への写像が線形であるときに秘密秘密法が線形であると言う。線形秘密分散法は線形符号の対と一対一に対応する (Martinez-Penas 2016)。

r 人以上の参加者は必ず有資格集合になる
t 人以下の参加者は必ず禁止集合になる
各シェアのサイズは $\log_2 q$ ビット
秘密のサイズは $k \log_2 q$ ビット、である線形秘密分散法の場合必ず

$$r - t \geq \frac{q^m - 1}{q^{m+1} - 1}(n+2) + \frac{q^{m+1} - q^m}{q^{m+1} - 1}(k - 2m) \quad (\text{for all } 0 \leq m \leq k-1). \tag{3}$$

が成り立つ (Cascudo, Skovsted Gundersen and Ruano, 2018)。

線形秘密分散法に対して超越性を示す量子符号

このことから

$$n+2-d < \frac{q^m-1}{q^{m+1}-1}(n+2) + \frac{q^{m+1}-q^m}{q^{m+1}-1}(k-2m)$$
$$(\text{for some } 0 \le m \le k-1), \tag{4}$$

を満たす $[[n,k,d]]$ 量子符号はアクセス構造に関する量子超越性を示す。
式 (4) を満たす量子符号のパラメータは

n	k	d	m
27	3	9	$m=2$
28	3	9	$m=2$

まとめ

- 秘密分散法アクセス構造に関する量子超越性を紹介した
- 量子誤り訂正符号を用いて、古典情報である秘密を量子情報であるシェアに分散する秘密分散法を紹介した
- 量子符号パラメータ $[[n, k, d]]$ とアクセス構造の関係を紹介した
- 古典情報処理で実現できるアクセス構造の限界式を紹介した
- これらを用いてアクセス構造に関する量子超越性を示す量子符号を紹介した