数理情報学モデル論概論２

Deutsch-Jozsa の量子アルゴリズム

問題 DJ

入力： 関数 $f : \{0,1\}^n \to \{0,1\}$．ただし，$f$ はオラクル（ブラックボックス）として与えられる．

制約： f は

(a) constant，すなわちすべての $x \in \{0,1\}^n$ について $f(x)$ は等しい

(b) balance, すなわち 2^{n-1} 個の $x \in \{0,1\}^n$ について $f(x) = 1$ で残りは $f(x) = 0$.

出力： f が (a) なら YES，(b) なら NO.

定理 (Deutsch-Jozsa 1992). DJ は古典アルゴリズムで誤りなく解くためには最悪で $2^{n-1}+1$ 回の f への質問を要するが，量子アルゴリズムでは 2 回の質問で誤りなく解ける．

Deutsch-Jozsa の量子アルゴリズム

1. $n+1$ 個の量子ビットを状態 $|0^n\rangle_A|0\rangle_B$ に準備する．
2. レジスタ A の各量子ビットに H を施す．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|0\rangle_B$$

になる．

3. A に格納された x をオラクルに質問してその答えを B に書き込む．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|f(x)\rangle_B$$

になる．

4. B に量子ゲート Z を施す．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A|f(x)\rangle_B$$

になる．

5. 再び A に格納された x をオラクルに質問してその答えを B に書き込む．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A|0\rangle_B$$

になる．

6. レジスタ A の各量子ビットに H を施したのち，測定する．
7. 測定値が 0^n なら YES，そうでなければ NO と判定する．

量子指紋

通信計算問題 EQ

設定：A は入力 $x \in \{0,1\}^n$，B は入力 $y \in \{0,1\}^n$ を持つ．R は入力を持たない．A および B は R にメッセージを送ることができる．

目的：A,B はなるべく短いメッセージで R に $x = y$ か否かを判定させたい．

定理　EQ の通信計算量について以下のギャップが得られる．

(i) 古典のメッセージでは EQ を誤り確率 1/3 で解くには $\Omega(n)$ の長さを必要とする．

(ii) 量子のメッセージでは EQ を誤り確率 1/3 で解くには $O(\log n)$ の長さでよい．

量子指紋プロトコル

$\mathbb{F}$ をサイズ $100n$ の有限体とする．n ビット列 $x = x_1 \cdots x_n$ に対して多項式 $p_x(z)$ を $p_x(z) = \sum_i x_i z^{i-1}$ とする．

1. A は量子状態

$$|\phi_x\rangle = \sum_{z \in \mathbb{F}} |z\rangle |p_x(z)\rangle,$$

B は量子状態 $|\phi_y\rangle = \sum_{z \in \mathbb{F}} |z\rangle |p_y(z)\rangle$ を R に送る．

2. R は $|\phi_x\rangle = |\phi_y\rangle$ か否かを以下の SWAP テストと呼ばれる方法でチェックする．

[SWAP TEST]

S1. 余分に $|0\rangle$ を用意して，状態 $|0\rangle_R |\phi_x\rangle_S |\phi_y\rangle_T$ を準備する．

S2. レジスタ R に H を施す．

S3. R の値が 1 なら S と T を交換する．すると状態は

$$\frac{1}{\sqrt{2}}(|0\rangle_R |\phi_x\rangle_S |\phi_y\rangle_T + |1\rangle_R |\phi_y\rangle_S |\phi_x\rangle_T)$$

になる．

S4. R に H を施す．すると状態は

$$\frac{1}{2}|0\rangle(|\phi_x\rangle|\phi_y\rangle + |\phi_y\rangle|\phi_x\rangle) + \frac{1}{2}|1\rangle(|\phi_x\rangle|\phi_y\rangle - |\phi_y\rangle|\phi_x\rangle)$$

になる．

S5. R を測定して 0 なら YES，1 なら NO を出力．

参考文献

H. Buhrman, R. Cleve, J. Watrous, R. de Wolf. Quantum fingerprinting. *Physical Review Letters* **87** 167902 (2001).