Review of the Simon's Algorithm

1 記号

定義 1. $N = 2^n$ として

$$H_N = H_{N/2} \otimes H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \tag{1}$$

と定める. ここで, $H_1 = 1$ とする.

アダマール変換の一般系 H_N について次の補題が成立する.

補題 2. For row $r = (r_1, r_0) \in \{0,1\}^{N-1} \times \{0,1\}$ and column $c = (c_1, c_0) \in \{0,1\}^{N-1} \times \{0,1\}$,

$$H_N[r, c] = (-1)^{r \bullet c} \tag{2}$$

証明. 一般に $n \times n$ 行列 A に対して, (i, j) 成分は $A\mathbf{e}_j$ の第 i 成分として求まる. よって, (r, c) 成分を求めるには, $H_N \mathbf{e}_{c_1} \otimes \mathbf{e}_{c_0}$ の r 成分を求めると良い.

$$H_N \mathbf{e}_{c_1} \otimes \mathbf{e}_{c_0} \quad = \quad H_{N/2} \mathbf{e}_{c_1} \otimes H_2 \mathbf{e}_{c_0} \tag{3}$$

であるので, $r = (r_1, r_0) \in \{0,1\}^{N-1} \times \{0,1\}$ 成分は, 帰納法の仮定から, $(-1)^{r_1 \bullet c_1} \cdot (-1)^{r_0 \bullet c_0} = (-1)^{r \bullet c}$ とわかる. □

2 Simon Algorithm

Let $f : \{0,1\}^n \to \{0,1\}^n$. We assume two condition;
(1) there is a s (s.t) for $^\forall y, ^\forall z$, $f(y) = f(z) \Leftrightarrow y = z \oplus s$
(2) f is a one to one or two to one.
また, $x \in \{0,1\}^n$ に対して, $x^* : \{0,1\}^n \to \{0,1\}$ を $v \mapsto x \bullet v$ と定義する. また, 函数 $h : \{0,1\}^n \to \{0,1\}$ に対して, $V(h) := \{x \in \{0,1\}^n | h(x) = 0\}$ と定義をする.
【戦略】
1. $V(0)$
2-1. $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} \mathbf{e}_x \otimes \mathbf{e}_{f(x)}$
2-2. 第一レジスタに対して, Hadamard 変換をし, 測定をし, 第一レジスタ x_i とする.
2-3. $V(x_1^*, \cdots, x_i^*) = s$ となるまで 2-1, 2-2 を繰り返す.

3 解析

補題 3. Suppose f is periodic with nonzero s. Then the measured x's are random Boolean strings in $\{0,1\}^n$ such that $x \bullet s = 0$.

証明. Step 2-2 で, Hadamard 変換を施すと,

$$\frac{1}{N}\sum_{x\in\{0,1\}^n}\sum_{t\in\{0,1\}^n}(-1)^{x\bullet t}\mathbf{e}_t\otimes\mathbf{e}_{f(x)} \tag{4}$$

であり, f periodic と仮定しているので, $^{\exists}x_1, x_2 = x_1 \oplus s$ (s.t) $f(x_1) = f(x_2)$. このとき, $e_t \otimes e_{f(x_1)}$ の係数は,

$$\frac{1}{N}(-1)^{t\bullet x_1}(1+(-1)^{x\bullet s}). \tag{5}$$

なので, 第二レジスタが Range(f) の時のみ, 確率 $\frac{4}{N^2}$ で第一レジスタ t に対して, $t\bullet s = 0$ □

4 研究課題

最短でどのくらいか見積もってみる.