量子情報科学入門（共立出版）訂正表

平成 27 年 1 月 8 日

- 76 ページ 6 行目〜17 行目
  正： 今，二つのサンプル $m_1 = k_1 N/s$ と $m_2 = k_2 N/s$ が得られたとしよう（ここで $k_1, k_2 \in \{0, ..., s-1\}$）．既知なのは m_1, m_2 および N であり，s と k_1, k_2 は未知である．もし k_1 が k_2 と互いに素であれば，m_1 と m_2 の最大公約数が N/s となるので，m_1, m_2 と N/s から Euclid の互除法を用いて s を求めることができる．

  k_1 が k_2 と互いに独立にならない確率は

$$\begin{aligned} &\Pr\{\cup_{p:\text{素数}}\, k_1 \text{ と } k_2 \text{ が } p \text{ の倍数 }\} \\ &\leq \sum_{p:\text{素数}} \Pr\{k_1 \text{ と } k_2 \text{ が } p \text{ の倍数 }\} \leq \sum_{p:\text{素数}} \frac{1}{p^2} < \sum_{n\geq 2} \frac{1}{n^2} < 0.65, \end{aligned}$$

  となる．ここで最後の不等式は $\sum_{n\in\mathbb{N}} n^{-2} = \pi^2/6$ から得られる．よって例えば $2n$ 個のサンプルから s は $1 - 0.65^n$ 以上の確率で得られる．