# ペトリネットによる量子アルゴリズムと量子暗号のモデル化と解析に関する研究

中西 潤一郎　　指導教員：辻 孝吉

## 1 はじめに

量子コンピュータの学問は量子力学や情報理論などの複数の分野から成り立っている．しかし，量子力学全般の知識がなくとも，量子状態の遷移や量子回路や量子ゲートを用いた計算手法をもとに量子コンピュータについて一から学び，理解することは可能である．一方で，数理モデルは通常，対象のシステムを簡略化したものである [1]．数理モデルの 1 つであるペトリネット [2] を用いて量子状態の離散的な変化を表現することによって量子計算を解析できる可能性がある．本研究で行うことは 2 つである．1 つ目はペトリネットを用いて量子アルゴリズムの 1 つである Grover のアルゴリズムのモデル化手法の提案を行う．2 つ目は共有鍵を作成する手順をペトリネットでモデル化することで量子暗号の 1 つである BB84 プロトコルのモデル化手法を提案し，そのモデルの動作結果からモデルの正当性を示す．

## 2 Grover のアルゴリズムのモデル化

Grover のアルゴリズムをカラーペトリネットでモデル化を行った．本章ではそのモデル化手法を示す．ペトリネットでは量子状態 $i$ を表すプレースを $P_{ij}$ とし，トランジションの発火を量子状態の遷移とする．Grover のアルゴリズムは唯一解なので，解である量子状態を表すプレースが 1 つと解でない量子状態を表すプレースが $N-1$ つに分けられる．そして $\frac{\text{解である量子状態を表すプレース内のトークン数}}{\text{解でない量子状態を表すプレース内のトークン数}} = \frac{\text{解である量子状態の重み係数}}{\text{解でない量子状態の重み係数}}$ が一致することでモデルの正当性を示す．また，$j$ はアルゴリズムの遷移状態を表し，プレース $P_{i0}$ からプレース $P_{i1}$ の遷移が位相反転，プレース $P_{i1}$ からプレース $P_{i2}$ の遷移が拡散変換を表す．そしてトークンは 1 と $-1$ を表す 2 通りの色をもつものとして定義する．以降，本論文では 1 を表すトークンの色を $A$ とし，$-1$ を表すトークンの色を $B$ とする．

また，プレース $Q_j(j=1,2,...,N)$ をモデルの制御プレース，そのプレースのトークンは 0,1,...,$2^{n-1}$ の $N$ 通りの色をもつものと定義する．

そして量子状態 $|i\rangle$ を表すプレースが遷移するときトランジション $T_{ij}$ が発火するものとする．

以下の表 1 にプレース，トークンの定義を示す．

表 1　時間付カラーペトリネットでの定義

| 要素 | 説明 |
|---|---|
| プレース $P_{ij}$ | 量子状態 $\|i\rangle$ を表す |
| プレース $Q_i(j=1,2,...,N)$ | $P_{ij}$ の制御プレース |
| プレース $P_{ij}$ 内のトークン | $A$,$B$ の 2 通り |
| プレース $Q_i$ 内のトークン | 1,...,$N$ の $N$ 通り |
| $A$,$B$ の値をとる変数 | $s$ |
| トークン色反転関数 | $v(A)=B$<br>$v(B)=A$ |
| トランジション $T_{ij}$ の発火 | プレース $P_{ij}$ の遷移 |

上記の定義をもとに一般の $N$ に対する Grover のアルゴリズムのペトリネットによるモデル化アルゴリズムを以下に示す．

**Grover のアルゴリズムのモデル化アルゴリズム**

(I) アダマール変換した量子状態 $|i\rangle$ を初期状態とし，プレース $P_{i0}$ で表す．これらのプレースには初期マーキングとしてトークン $A$ を 1 つ置く．

(II)　(I) で定義したプレースそれぞれに 2 つの出力トランジション $T_{i0}$,$T_i$ を接続する．これらのトランジションはどちらも同じ出力プレース $P_{i1}$ に出力する．どちらも入力プレースからのアーク重みは変数 $s$ であるが，出力プレースへのアーク重みは $(T_{i0},P_{i1})$ が $s$，$(T_i,P_{i1})$ が $v(s)$ である．後者のトランジションの発火によって位相反転を示す．また，トランジション $T_i$ の発火で制御プレース $Q_i$ にトークンを出力する．

(III)　拡散変換のモデル化を用いて拡散変換を行う．(II) の出力プレース $P_{i1}$ を量子状態 $|i\rangle$ における拡散変換適用前とし，トランジション $T_{i2}$ の発火によりプレース $P_{i2}$ にトークンを出力することで拡散変換を示す．拡散変換の結果を出力するトランジションを置く．ただし，アークの重みは以下の 2 通りである．

$$\begin{cases} 1(\text{入力プレース}:P_{i1},\text{出力プレース}:P_{i2}) \\ \frac{N-2}{2}(\text{入力プレース}:P_{i1},\text{出力プレース}:P_{i2}) \end{cases}$$

入力プレースからは 1 つの色つきトークンを入力し，入力プレースと同じ量子状態に対応する出力プレース $\frac{N-2}{2}$ 個の入力トークンと反対の色トークンを，それ以外の出力プレースには 1 個の同色のトークンを出力する．

(IV)　(I) における制御プレースを用いて (II) のモデルに遷移．

モデル化アルゴリズムを適用した $N=4$ におけるモデルを図 1 に示す．

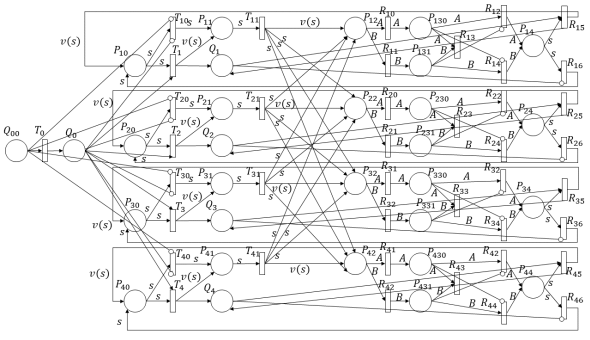

図 1　$N=4$ における Grover のアルゴリズムのモデル図

## 3 BB84 プロトコルのモデル

BB84 プロトコルは Benett と Brassard により 1984 年に提案されたプロトコルである．これは光子の偏光を利用して，送信者と受信者の間で共通の乱数である鍵を持つためのプロトコルである．暗号鍵を共有するために一往復程度の通信を行うのが

特徴である．送信者側と受信者側での作業がいくつかのステップに分かれており，本研究ではそれを基にモデル化を行った．モデルのアルゴリズムを以下に示す．

BB84 プロトコルのモデル化アルゴリズム

**送信者側**

(i) 送信者が作る適当な桁数の 2 つの 2 進数 $a$,$b$ において 0 を出力するプレースをそれぞれ $a_0$,$b_0$ とし，1 を出力するプレースをそれぞれ $a_1$,$b_1$ とし初期プレースとする．

(ii) プレース $a_0$ とプレース $b_0$ を入力プレースとし，出力プレース $|\psi_{00}\rangle$ に出力する．同様の操作を 3 組のプレース $a_0$,$b_1$, プレース $a_1$,$b_0$, プレース $a_1$,$b_1$ で行い，出力プレースをそれぞれ $|\psi_{01}\rangle$,$|\psi_{10}\rangle$,$|\psi_{11}\rangle$ とする．これでにおける量子状態 $|\psi_{a_ib_i}\rangle$ を作成のモデルを表す．

**受信者側**

(iii) 受信者が作る 2 進数 $b'$ において 0 を出力するプレースを $b_0^{'}$,1 を出力するプレースを $b_1^{'}$ とし，(ii) の出力プレースの中の 1 つとプレース $b_0^{'}$ を入力プレースとし，トランジションをアークで結ぶ．これを (ii) の出力プレース全てで行う．

(iv)　(iii) と同様のことを $b_1^{'}$ で行う．

**一致している桁の確認**

(v)　(iii),(iv) において $|\psi_{00}\rangle$ と $b_0^{'}$ を入力プレースとするトランジションはプレース $c_0$ にトークンを出力し，て $|\psi_{11}\rangle$ と $b_1^{'}$ を入力プレースとするトランジションはプレース $c_1$ にトークンを出力する．

モデルを図 2 に示す．

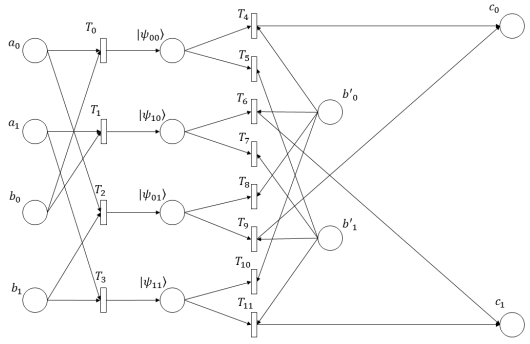


図 2　BB84 プロトコルのモデル図

## 4　Grover のアルゴリズムのモデルの動作結果

$N = 4$ における Grover のアルゴリズムの計算結果とモデルの動作結果を比較したものを表 2 に示す．モデルの解析手法として解となる量子状態の重み係数の比をアルゴリズムの計算結果とトークン数で比較を行う．表から解である重みと解でない重みの比率は解のプレースのトークン数とそうでないプレースのトークン数の比率と等しいことが分かる．実際，$k$ 回の繰り返しの後の各量子状態の振幅は，対応するプレースのトークン数に $\pm\frac{1}{\sqrt{N}}(\frac{2}{N})^k$ を乗じた値になる．

表 2　モデルの動作結果と計算結果の比較 ($N = 4$)

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 解を示す量子状態 | $\frac{1}{2}$ | 1 | $\frac{1}{2}$ | $-\frac{1}{2}$ |
| 解でない量子状態 | $\frac{1}{2}$ | 0 | $-\frac{1}{2}$ | $-\frac{1}{2}$ |
| 解を表すプレース内のトークン数 | $A$ が 1 個 | $A$ が 4 個 | $A$ が 4 個 | $B$ が 8 個 |
| 解でないプレース内のトークン数 | $A$ が 1 個 | 0 個 | $B$ が 4 個 | $B$ が 8 個 |

## 5　BB84 プロトコルのモデルの動作結果

$n = 5$ におけるモデルの動作結果を図 3 に示す．

表 3　モデルにより作成された暗号鍵 ($n = 5$)

| | モデルにより作成された暗号鍵 |
|---|---|
| 1 回目 | 000 |
| 2 回目 | 0101 |
| 3 回目 | 10 |
| 4 回目 | 1 |
| 5 回目 | 1100 |
| 6 回目 | 1010 |
| 7 回目 | 111 |
| 8 回目 | 00001 |
| 9 回目 | 0 |
| 10 回目 | 111 |

量子暗号のモデルで，送信者と受信者の共有する鍵を作成にあたり，捨てる桁があるので，共有したい鍵の長さのほぼ倍ぐらいの桁数の 2 進数と量子状態をやりとりする必要がある [3]．表は $n = 5$ における暗号鍵作成のモデルの検証結果である．

## 6　まとめ

本研究ではアダマール変換された量子状態を初期プレースとし，それに位相反転のモデル, 拡散変換のモデルを加えることで Grover のアルゴリズムのモデル化手法の提案し，モデルの正当性を示した．また，BB84 プロトコルにおける鍵を共有する手法を送信者の準備と受信者による測定の 2 つに分け，それらから得られた結果を組み合わせることで BB84 プロトコルのモデル化手法の提案を行った．これらのモデルは $N, n$ が大きくなるほどトークン数が増えて，解析するのが難しくなる．したがってトークン数を抑えたモデルに改良することが今後の課題である．

## 参考文献

[1] 山口真悟：数理的アプローチの未来への展望，電気電子情報通信学会誌，vol.100，No.6，479/483，2009.
[2] 村田忠夫：ペトリネットの解析と応用，近代科学社，1992.
[3] 西野友年：今度こそわかる量子コンピュータ，講談社，2015.