O-18

量子情報におけるノークローニング定理

The no-cloning theorem in quantum information theory

○ 関野　裕司[1]
Yuji Sekino[1]

Abstract: A statement, "we cannot make a machine which enables us to obtain copies of any states," known as the no-cloning theorem has a very big impact. Not only one intuitively expects its importance, but also very essential in quantum information. To show this in concrete manner, in this review, we first prove the no-cloning theorem and then discuss a few important examples including well-known "quantum telepotation" and "quantum cryptography" where the no-cloning theorem plays an essential role.

1. ノークローニング定理とその役割

量子情報において状態を複製 (:知られていない元の状態はそのままに，もうひとつそれとまったく同じ状態を作り出すこと) できないことは本質的である．このことはノークローニング定理 (1982 年に Wootters, Zurek[1] と Dieks[2]) として知られていて，証明は以下に示すように極めて単純である．

まずある状態 $|A\rangle$ 複製を作ることは式で

$$|A\rangle \longrightarrow |A\rangle|A\rangle \tag{1}$$

と表せる．また $|A\rangle$ ではない別の状態 $|B\rangle$ にも当然

$$|B\rangle \longrightarrow |B\rangle|B\rangle \tag{2}$$

が成り立たねばならない．ここから先は仮定の仕方によって 3 通りの証明法がある．

A．線形性を仮定する方法 1([1],[2])
複製に線形性を仮定すると，上の 2 つの式の左辺の線形結合の複製は右辺の線形結合にならねばならない．つまり

$$a|A\rangle + b|B\rangle \longrightarrow a|A\rangle|A\rangle + b|B\rangle|B\rangle \tag{3}$$

となる．一方で $a|A\rangle + b|B\rangle$ を一つの状態とみなして複製を適用したとすると，

$$|s\rangle \longrightarrow |s\rangle|s\rangle \tag{4}$$

となるはずである．ただし $|s\rangle = a|A\rangle + b|B\rangle$ と定義した．しかしながら $|e\rangle \neq |s\rangle|s\rangle$ であるから複製は可能でない．ここで $|e\rangle = a|A\rangle|A\rangle + b|B\rangle|B\rangle$ とした．

B．線形性を仮定する方法 2([4])
入力が $|s\rangle$ で出力が $|e\rangle$ であるとき，量子力学では確率を保存するので

$$\langle s|s\rangle = \langle e|e\rangle \tag{5}$$

でなくてはならない．左辺を具体的に書くと

$$\langle s|s\rangle = |a|^2 + |b|^2 + a^*b\langle A|B\rangle + ab^*\langle B|A\rangle \tag{6}$$

であり，右辺は

$$\langle e|e\rangle = |a|^2 + |b|^2 + a^*b\langle A|B\rangle\langle A|B\rangle + ab^*\langle B|A\rangle\langle B|A\rangle \tag{7}$$

であるから，任意の状態にたいして (5) が成立するためには

$$\langle A|B\rangle = \langle A|B\rangle\langle A|B\rangle \tag{8}$$

が必要かつ十分である．しかしこれは一般には成り立たない．

C．ユニタリー性を仮定する方法 ([4])
もし複製がユニタリーであったとすると

$$|A\rangle \xrightarrow{U} |A\rangle|A\rangle \tag{9}$$

$$|B\rangle \xrightarrow{U} |B\rangle|B\rangle \tag{10}$$

であるから，

$$\langle A|U^\dagger U|B\rangle = \langle A|\langle A|B\rangle|B\rangle \tag{11}$$

より

$$\langle A|B\rangle = \langle A|B\rangle\langle A|B\rangle \tag{12}$$

を得る．しかしこれも一般には成り立たない．

このようにこのノークローニング定理では，互いに直交しない状態を見ることが本質的である．

以下ではこのノークローニング定理が量子情報のいくつかの事柄に対していかに有効に働いているかを具体的にみていく．

2. 量子暗号

量子暗号にはいくつかのプロトコルがあるが，ここでは Bennett と Brassard によるもの (BB84 [3]) を考える．これは光子の偏光状態を利用して秘密鍵を共有しようというもので手順は以下のとおりである．

(1) 送信者 Alice と受信者 Bob は双方とも縦横偏光フィルター，斜め偏光フィルター両方を用意する．
(2)Alice は光子をランダムに選んだ偏光フィルターを通して送信する．このときフィルターの種類と偏光の向きを記録

[1]日大理工・院・量子

しておく．Bob はこの光子をランダムに選んだフィルターを通して受信する．このとき Bob もまたフィルターの種類と偏光の向きを記録しておく．
(3)Alice と Bob はどちらの偏光フィルターを選んだか公にする．ただし偏光の向きは言わない．
(4) 同じフィルターを選んだときの偏光の向きの結果が秘密鍵になる．

ただしこの秘密鍵の中からランダムにいくつかは公開して，確かに途中に盗聴者 Eve がいなかったかを確かめる必要がある．こうすることで Eve が途中で光子を奪い別の光子に入れ替えたとしても (盗聴)，それに気づくことができるからである．

さてここで重要なのは，Eveが代わりに入れる光子は，奪った光子とは偏光状態が異なることを暗黙のうちに仮定していることである．もし Eve が，奪った光子とまったく同じ状態の光子を作ることができるのならば，暗号の安全性は保障されない．しかしながら前述したように，そのようなことはノークローニング定理によって否定されているわけである．

3. 超光速通信の不可能性

Alice が Bob に 1bit の情報を送ることを考える．まずエンタングルした状態

$$|\psi\rangle = (|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)/\sqrt{2} \tag{13}$$

を用意する．ただし $|0\rangle$, $|1\rangle$ は σ_z の固有状態であり，添え字 A は Alice, B は Bob を表している．この状態は σ_x の固有状態 $|0'\rangle$, $|1'\rangle$ を使って

$$|\psi\rangle = (|0'\rangle_A|1'\rangle_B - |1'\rangle_A|0'\rangle_B)/\sqrt{2} \tag{14}$$

と書き換えることができることに注意する．Alice は 2 つの異なる基底 $\{|0\rangle, |1\rangle\}$, $\{|0'\rangle, |1'\rangle\}$ のどちらかで測定することによって，1bit の情報をエンコードできる．このとき Bob がどのような測り方をしても情報をデコードできない．なぜなら測定して得た結果が, かき乱されたものか否かの区別ができないからである．ここでもし Bob に複製をすることのできる機械が与えられていたとすると，大量の複製を作り，そしてそれを測定することによって正しくデコードできるだろう．したがって Alice と Bob がある程度の距離離れていれば，光速以上の速度で通信できたことになる．しかしノークローニング定理がこれを禁止している．

4. 量子テレポーテーション

テレポーテーションを行うにはエンタングルさせた 1 つの qbit

$$|\Psi_{AB}\rangle = (|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle)/\sqrt{2} \tag{15}$$

を用意する．　A 側の状態は，送りたい情報を持っている人 (Alice) に，B 側の状態はその情報を再現する人 (Bob) へそれぞれ送ることにする．Alice が送りたい qbit の情報は, 係数 a, b をうまく選ぶことで必ず $|\Phi\rangle = a|0\rangle + b|1\rangle$ と書けるはずであるから，全系の状態 $|\Phi_{AB}\rangle$ は

$$|\Phi_{AB}\rangle = |\Phi\rangle|\Psi_{AB}\rangle = (a|0\rangle + b|1\rangle)(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle)/\sqrt{2} \tag{16}$$

と書ける. しかしながらこの状態は異なる基底を使って

$$\begin{aligned}|\Phi_{AB}\rangle = \frac{1}{2}[&|\Phi^+\rangle(a|0\rangle + b|1\rangle)\\ &+|\Phi^-\rangle(a|0\rangle - b|1\rangle)\\ &+|\Psi^+\rangle(a|1\rangle + b|0\rangle)\\ &+|\Psi^-\rangle(a|1\rangle - b|0\rangle)]\end{aligned} \tag{17}$$

と書くこともできる．ただし

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \tag{18}$$

$$|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2} \tag{19}$$

$$|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2} \tag{20}$$

$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \tag{21}$$

である．ここで重要なのはベクトル $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ は Alice 側の 2 つの qbit 分の正規直交基底になっていることである．このことは, 射影演算子が $|\Phi^+\rangle\langle\Phi^+|$, $|\Phi^-\rangle\langle\Phi^-|$, $|\Psi^+\rangle\langle\Psi^+|$, $|\Psi^-\rangle\langle\Psi^-|$ であたえられる von Neumann 測定が可能であることを示している．Alice がこの測定を行った後, ４つのありうる結果のうちどれが出たかを Bob に (古典的な方法で) 伝える．Bob はその結果に応じて適当なユニタリー変換を自分の側に飛んできた qbit に施せば，Alice が送りたかった状態 $|\Phi\rangle = a|0\rangle + b|1\rangle$ が Bob の側で再現できたことになる．ここで Alice の側に，もはや $|\Phi\rangle$ の情報がないことは自明だろう．この事実はノークローニング定理と矛盾していないことを示している．

5. むすび

量子情報においては目的はどうであれ，ある情報をどのように伝えるかということを議論することがしばしばあるが，前述したものはその代表例である．これらの例を通してノークローニング定理がいかに重要な位置にあるかを見てきた．

今後は，ノークローニング定理が量子情報のほかの部分でどのような役割を果たしているか理解し，さらに広範な量子論全般においてどのような位置づけになるか探りたい．

参考文献

[1] W. K. Wootters and W. H. Zurek, ”A single quantum cannot be cloned”, Nature, Vol.299, No5886, pp802-803 (1982).

[2] D. Dieks, ”COMMUNICATION BY EPR DEVICES”, Phys. Lett., Vol.92A, no6, pp271-272 (1982).

[3] C. H. Bennett and G. Brassard,“ Quantum Cryptography: Public key distribution and coin tossing ”, Proc. IEEE Int. , p. 175 (1984)

[4] W. K. Wootters, W. H. Zurek, ”The no-cloning theorem”, Phys. Today, pp76-77, February (2009).