ネットワーク基礎論 2
2011 年度 量子情報理論

小川朋宏

電気通信大学 大学院情報システム学研究科

2011 年 4 月 8 日

自己紹介

- **小川朋宏 (おがわともひろ)**
- **情報システム学研究科 ネットワーク基礎学講座**
- **専門分野：情報理論，量子情報理論，情報理論的暗号**
- **研究室：**IS **棟** 8F 821
- **連絡先：**ogawa **あっと** is.uec.ac.jp (**内線：**5625)
- **ホームページ：** http://www.quest.is.uec.ac.jp/ogawa/

講義の進め方

- **内容：量子情報理論**
- **予備知識：線形代数，確率論の初歩**
- **次回から講義は黒板で行います．資料を後日 WEB に掲載します．**
- **質問はいつでもどうぞ**

評価の方法

- **レポート：3 回程度**
- **出席状況**

量子情報理論とは

Shannon の情報理論（1948 年〜）

- 「情報」を抽象的な記号の流れとして体系化
- 確率論に基づく
- データ圧縮，通信，暗号に関する数学的理論・法則

量子情報理論（1960 年代〜）

- 1960 年：レーザーの発明
- 「情報」には物理的な媒体が関与するはず！
  $\Rightarrow$ 量子状態を媒体とする通信の議論に端を発する
- 量子力学的確率論に基づく（＝非可換確率論）
- 古典系にない問題がある（難しいけど面白い）
  - 測定の最適化：
    量子状態は測定により変化 $\Rightarrow$ 一度の測定で出来るだけ最適化
  - エンタングルメント：量子力学的相関

量子情報理論の歴史

- **量子状態の統計的推定，検定（1960 年代後半〜70 年代）**
  - Helstrom (**教科書** 1976), Holevo (**教科書** 1982 **など**), Yuen (D **論** 1970)
- **量子通信理論（1970 年代）**
  - **ソ連の数学者達，**Holevo (1973, 1979)
- **数学的理論** (1950 **年代〜**1980 **年代**)
  - **量子通信路（完全正写像）**
  - **量子相対エントロピー**
  - **作用素単調関数，作用素凸関数，作用素平均**

- **新しい流れ（1980 年代〜，米国）**
  - Bennett-Brassard (1984)：**量子暗号** (BB84 **プロトコル**)
  - Shor (1994)：**量子コンピュータによる素因数分解アルゴリズム**
- **量子通信路符号化定理の完成**
  - 1996 **年に** Holevo **と** Schmacher-Westmoreland **が独立に証明**
  - Holevo **の定式化から** 20 **年かかった（難しかった）**
- 2000 **年〜**
  量子暗号の安全性証明，量子状態伝送容量など，さらに発展

講義内容

□ 目標：古典-量子通信路符号化定理 (アドバンストです)

- イントロダクション＋量子情報理論の簡単な紹介 (4/8)
- 線形代数の復習：1 回〜2 回
- 量子力学系の状態と測定
- 合成系とテンソル積，エンタングルメント
- 量子テレポーテーション，量子高密度符号化 (dense coding)
  ——————————————— ここまでは，あまり難しくないと思います
- 量子力学系における情報量とその性質
  von Neumann エントロピー，量子相対エントロピー，
  Fiedelity，トレース距離，Holevo 相互情報量
- 量子通信路 (完全正写像) と情報量の単調性
- 量子仮説検定と量子相対エントロピー
- 量子通信路 (完全正写像)，量子通信路符号化

(進み具合によっては，変更するかも知れません)

参考文献の紹介

- **量子情報理論の教科書**
  - M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge, 2000.
  - **林正人**, **量子情報理論入門**, **サイエンス社**, 2004.
  - M. Hayashi, Quantum Information: An Introduction, Springer, 2006. (**上記の英訳＋内容大幅増**)
- **線形代数**
  - **川久保勝夫**, **線形代数学**, **日本評論社**, 1999. (**初心者向け**)
  - **竹内外史**, **線形代数と量子力学**, **裳華房**, 1981. (**復刊版が出ている**)
  - **日合文雄**, **柳研二郎**, **ヒルベルト空間と線型作用素**, **牧野書店**, 1995.
  - **その他多数**
- **情報理論**
  - T. M. Cover, J. A. Thomas, Elements of Information Theory, Wiley, 1991 (2nd ed. 2006).
- **量子力学**
  - **清水明**, **新版**: **量子論の基礎**, **サイエンス社**, 2003.
  - J. J. Sakurai, Modern Quantum Mechanics, Addison Wesley, 1985. (J. J. **サクライ**, **現代の量子力学**, **吉岡書店**, 1989.)
  - **その他多数．有限次元の系では，量子力学の難しい内容は必要ない．**

量子情報理論の簡単な紹介

以下のテーマについて，ガイダンス的説明をします．

- 量子力学系の状態と測定
- 量子暗号 (量子鍵配送，BB84 プロトコル)
- 合成系とテンソル積
- エンタングルメント
- 量子テレポーテーション
- 量子高密度符号化

量子力学系の公理について

量子力学系の特徴

- **確率法則**
  測定結果は**系の状態**と**測定**に依存して確率的にのみ定まる
- **系の状態変化**
  測定結果に依存して状態が変化 → 測定順序によって結果が異なる

⇓ スカラーでは記述しきれない

Hilbert 空間上の作用素（行列）により記述される

- Hilbert 空間：内積を持つ（複素）ベクトル空間
- 有限次元の場合：$\mathcal{H} \simeq \mathbb{C}^d$
- 内積 $\langle \varphi \,|\, \psi \rangle \quad (\varphi, \psi \in \mathcal{H})$ を持つ

Dirac のブラケット記法　（$\mathcal{H} = \mathbb{C}^d$ 数ベクトル空間，標準内積）

- **角括弧 $\langle \quad \rangle$ は英語で** bracket**．慣れると便利な記法．**
- **ケット（縦ベクトル） → ブラ（共役転置：横ベクトル）**

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} \quad \rightarrow \quad \langle\psi| = \begin{pmatrix} \psi_1^* & \cdots & \psi_d^* \end{pmatrix}$$

- **内積：**

$$\langle\varphi\,|\,\psi\rangle = \begin{pmatrix} \varphi_1^* & \cdots & \varphi_d^* \end{pmatrix} \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} = \sum_{i=1}^{d} \varphi_i^* \psi_i$$

- **ケットブラは行列：**

$$|\psi\rangle\langle\varphi| = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} \begin{pmatrix} \varphi_1^* & \cdots & \varphi_d^* \end{pmatrix} = \begin{pmatrix} \psi_1\varphi_1^* & \cdots & \psi_1\varphi_d^* \\ \vdots & & \vdots \\ \psi_d\varphi_1^* & \cdots & \psi_d\varphi_d^* \end{pmatrix}$$

量子状態と測定

- **量子状態＝長さ (ノルム) が 1 のベクトルで表現**

  量子状態：$|\psi\rangle \in \mathcal{H}$　(**規格化条件：**$\|\psi\| = \sqrt{\langle\psi \,|\, \psi\rangle} = 1$)

- m **個の測定結果を持つ測定** (m-valued measurement)

  測定：$E = \{E_1, \ldots, E_m\}$

  $E_i\,(i = 1, \ldots, m)$ **は** $\mathcal{H}$ **上の正方行列で以下を満たすもの**

$$E_i E_j = \delta_{i,j} E_i, \quad \sum_{i=1}^{m} E_i = I$$

  互いに直交する部分空間への射影子の集合，単位の分解

測定と状態の重ね合わせ

- **測定 $\Rightarrow$ 直交する単位ベクトルによる線形和 (重ね合わせ) を指定**

$$|\psi\rangle = \sum_{i=1}^{m} E_i |\psi\rangle = \sum_{i=1}^{m} \alpha_i |e_i\rangle$$

ただし

- $$|e_i\rangle := \frac{E_i |\psi\rangle}{\| E_i |\psi\rangle \|} = \frac{E_i |\psi\rangle}{\sqrt{\langle\psi| E_i |\psi\rangle}}$$ **(互いに直交，ノルム 1)**

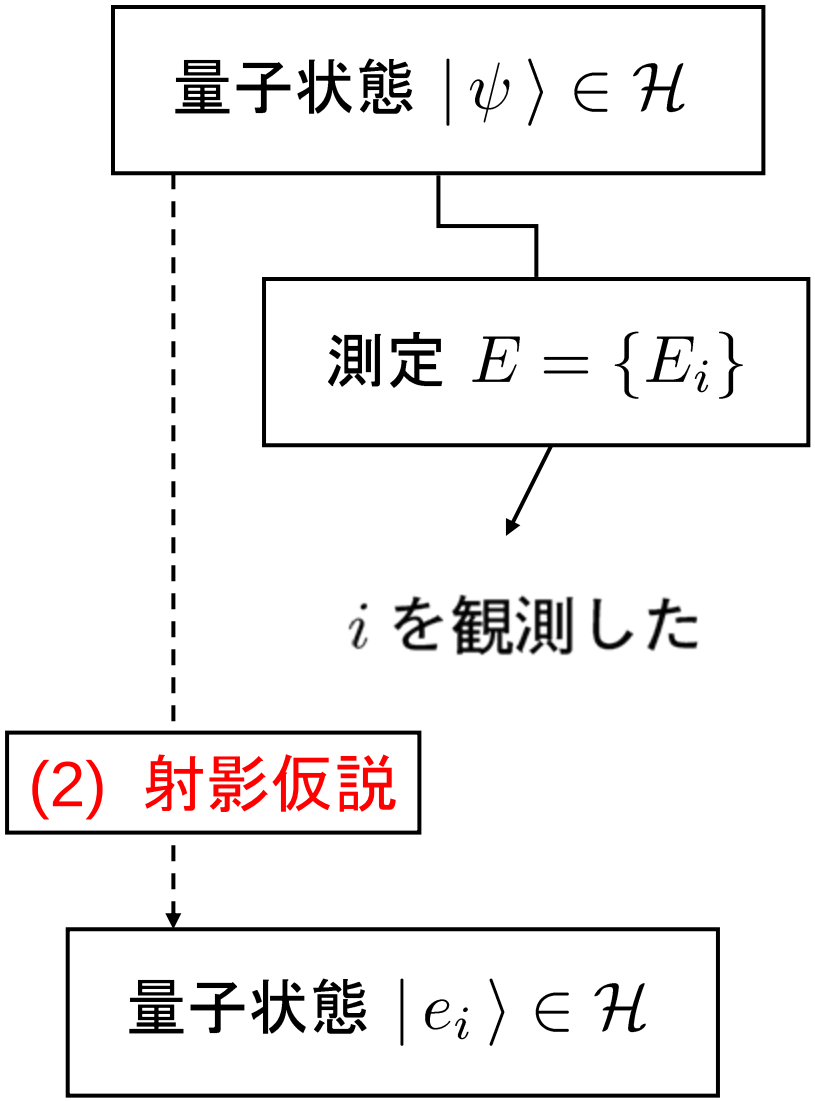
$$\because \quad \| E_i |\psi\rangle \|^2 = \langle\psi| E_i^* E_i |\psi\rangle = \langle\psi| E_i |\psi\rangle$$

- $$\alpha_i := \langle e_i | \psi\rangle = \frac{\langle\psi| E_i |\psi\rangle}{\sqrt{\langle\psi| E_i |\psi\rangle}} = \sqrt{\langle\psi| E_i |\psi\rangle}$$ **(振幅)**

- **振幅の二乗 $|\alpha_i|^2$ は確率分布**

$$|\alpha_i|^2 = \langle\psi| E_i |\psi\rangle, \quad \sum_{i=1}^{m} |\alpha_i|^2 = \langle\psi| \sum_{i=1}^{m} E_i |\psi\rangle = 1$$

量子力学の公理



$$|\psi\rangle = \sum_{i=1}^{m} E_i|\psi\rangle = \sum_{i=1}^{m} \alpha_i|e_i\rangle$$

(1) 確率法則

測定値 i を観測する確率

$$|\alpha_i|^2 = \langle\psi|E_i|\psi\rangle$$

量子暗号の背景:ワンタイムパッド

送信メッセージ
11001･･･

受信メッセージ
11001･･･

共有鍵
01101･･･

乱数を事前に共有

共有鍵
01101･･･

暗号化（XOR）

復号（XOR）

暗号文
10100･･･

10100･･･

暗号文
10100･･･

盗聴者
暗号文は鍵を知らないとランダムなビット列

背景：なぜ量子暗号？

○ ワンタイムパッド暗号 (Shannon, 1948)

メッセージ：010010		復号メッセージ：010010
暗号鍵(共有乱数)：101011		鍵(共有乱数)：101011
送信系列(XOR)：111001	⟶	受信系列：111001

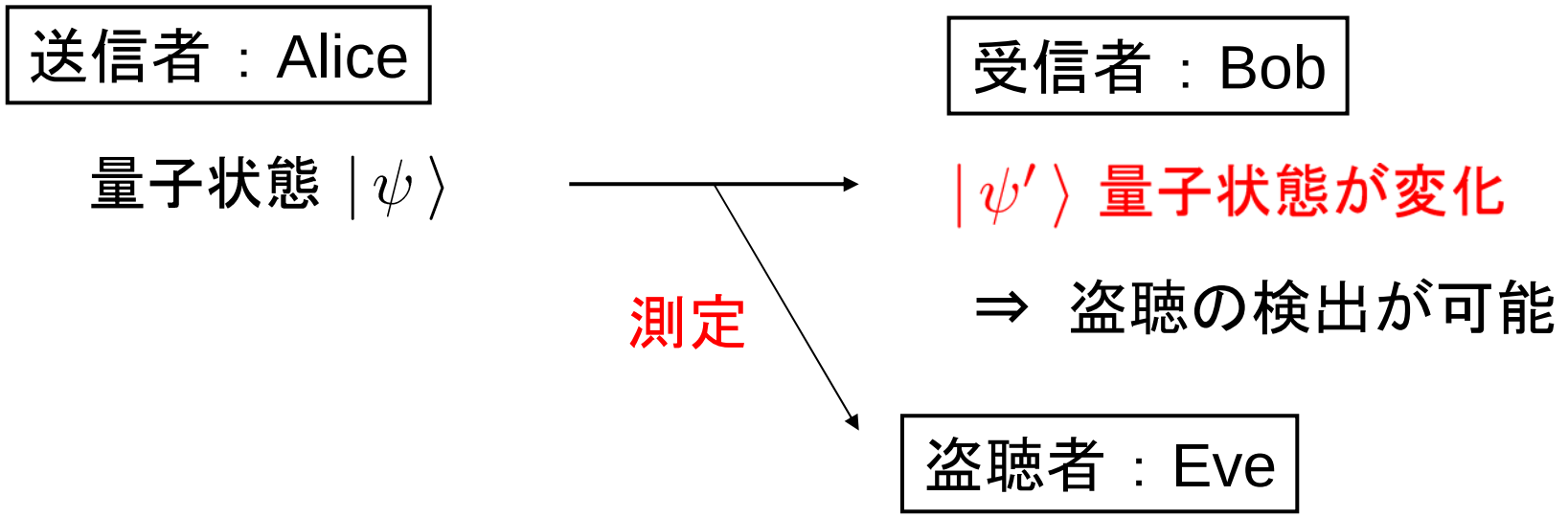
- 情報理論的に安全なことが証明されている
- メッセージと同じ長さの鍵が必要，1回の使用で捨てる
- 鍵の共有方法が問題

○ 公開鍵暗号 (Rivest-Shamir-Adleman, 1978)

- 秘密鍵と公開鍵を分けることで，鍵の共有問題を回避
- 素因数分解の難しさ(一方向性)に依存
- 安全性が理論的に証明されていない
- 量子計算機による素因数分解アルゴリズム (Shor, 1994)
  ⇒ 暗号解読の危険性

量子暗号とは

- 量子状態送受信による乱数(鍵)の共有方法
- 量子力学 (射影仮説) が安全性を理論的に保証



- Bennett-Brassard (1984), BB84プロトコル

プラス基底とクロス基底

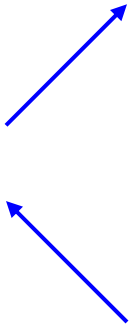
0,1のbit列 ⇒ 2種類の送信，受信方法

○ 送信

プラス基底 (＋)	クロス基底 (×)

$$|e_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|e_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

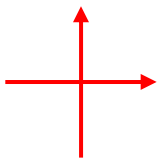


$$|f_0\rangle = \frac{|e_0\rangle + |e_1\rangle}{\sqrt{2}}$$

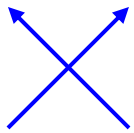
$$|f_1\rangle = \frac{|e_0\rangle - |e_1\rangle}{\sqrt{2}}$$

○ 受信 (測定)

$$|\psi\rangle = \alpha_0|e_0\rangle + \alpha_1|e_1\rangle$$



$$|\psi\rangle = \beta_0|f_0\rangle + \beta_1|f_1\rangle$$

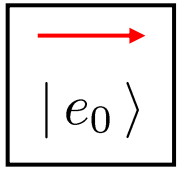


受信方向と測定結果

測定
プラス基底

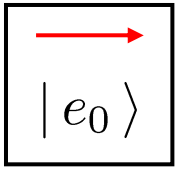
確率1

測定結果
0



$$|\,e_0\,\rangle = 1|\,e_0\,\rangle + 0|\,e_1\,\rangle$$

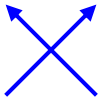
送信
プラス基底



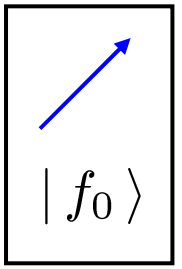
射影仮説

確率1/2

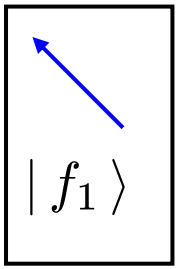
測定
クロス基底



測定結果
0



測定結果
1



確率1/2

$$|\,e_0\,\rangle = \frac{1}{\sqrt{2}}|\,f_0\,\rangle + \frac{1}{\sqrt{2}}|\,f_1\,\rangle$$

量子暗号鍵配布プロトコル (BB84)

送信者：Alice

1. ランダムなbit列を用意する
2. ランダムな送信方向を用いてbit列を送信

受信者：Bob

3. ランダムな受信方向を用いて量子状態を測定

双方：公開通信路

4. 送信方向と受信方向を伝え，両者が一致していたものを残す
5. 残ったbit列からランダムにテストbitを取り一致を確認

量子暗号鍵配布プロトコル (BB84)：例

送信者 Alice

送信 bit 列	1	0	1	1	0	0	1	1	0	0	1	1	1	0
送信方向	＋	×	＋	＋	×	×	＋	＋	×	＋	×	×	＋	＋
送信偏光	↑	↗	↑	↑	↗	↗	↑	↑	↗	→	↖	↖	↑	→

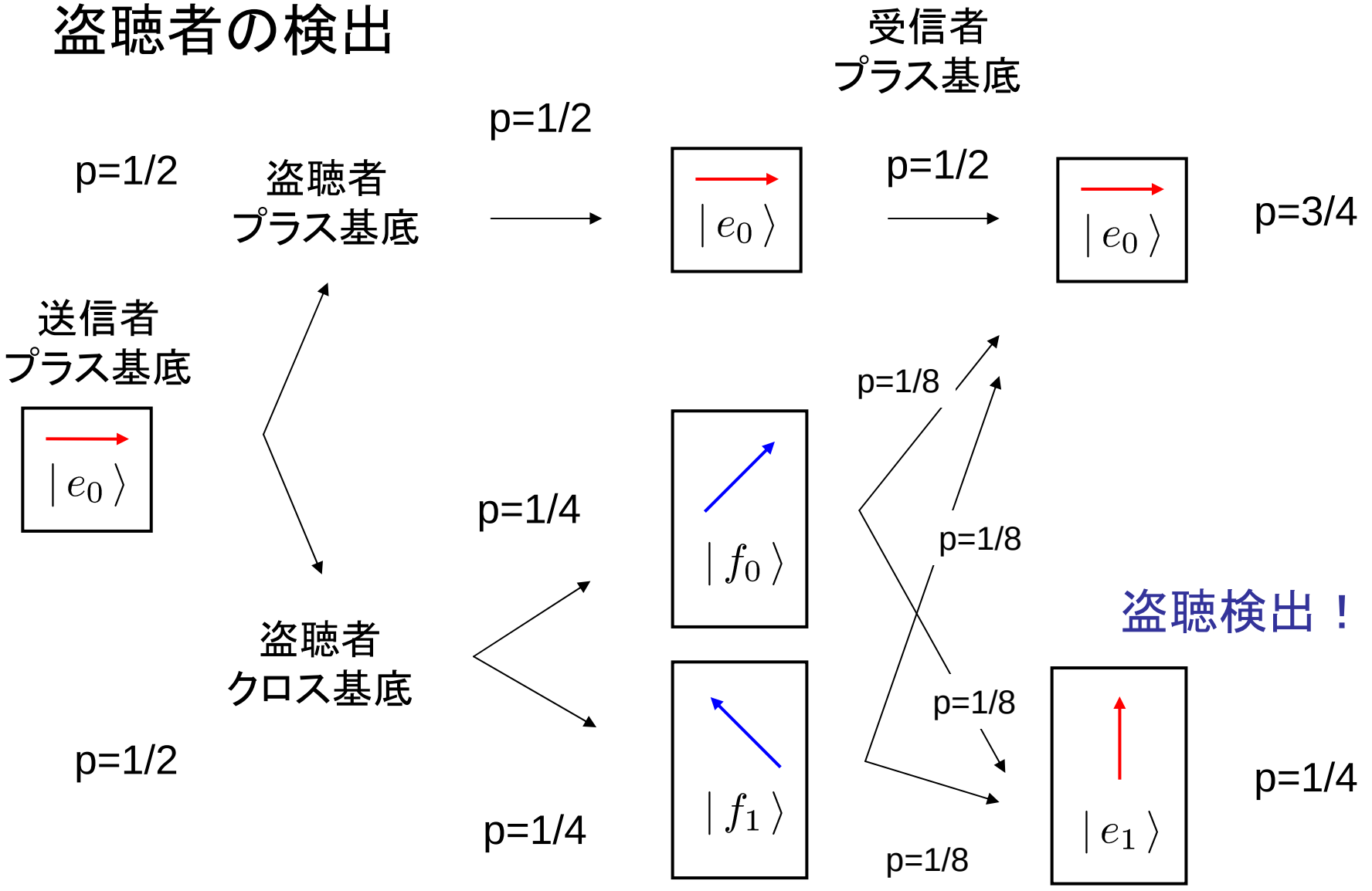
受信者 Bob

測定方向	＋	＋	×	＋	×	×	×	＋	×	＋	＋	×	×	＋
受信偏光	↑			↑	↗	↗		↑	↗	→		↖		→
受信 bit 列	1			1	0	0		1	0	0		1		0

盗聴者チェック

テスト bit	○				○					○				
完成 bit 列				1		0		1	0			1		0

盗聴者の検出



盗聴を見逃す確率：$(3/4)^n \to 0$ (n テスト bit 数 $\to \infty$)

合成系

○ 物理系 $\mathcal{H}_A$ と $\mathcal{H}_B$ の合成系 $\Longrightarrow$ テンソル積空間 $\mathcal{H}_A \otimes \mathcal{H}_B$

○ テンソル積演算（ベクトル）

$$|\,\psi_A\,\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}$$

$$|\,\psi_B\,\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$|\,\psi_A\,\rangle \otimes |\,\psi_B\,\rangle = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ \vdots \\ a_m \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{pmatrix}$$

クロネッカー積

テンソル積空間

○ テンソル積演算の性質

$$(\alpha|\,\psi_A\,\rangle + \beta|\,\varphi_A\,\rangle) \otimes |\,\psi_B\,\rangle = \alpha|\,\psi_A\,\rangle \otimes |\,\psi_B\,\rangle + \beta|\,\varphi_A\,\rangle \otimes |\,\psi_B\,\rangle$$

$$|\,\psi_A\,\rangle \otimes (\alpha|\,\psi_B\,\rangle + \beta|\,\varphi_B\,\rangle) = \alpha|\,\psi_A\,\rangle \otimes |\,\psi_B\,\rangle + \beta|\,\psi_A\,\rangle \otimes |\,\varphi_B\,\rangle$$

○ 内積 ：$\langle\,\psi_A \otimes \psi_B\,|\,\varphi_A \otimes \varphi_B\,\rangle = \langle\,\psi_A\,|\,\varphi_A\,\rangle\langle\,\psi_B\,|\,\varphi_B\,\rangle$

○ テンソル積空間

$$\mathcal{H}_A \otimes \mathcal{H}_B = \left\{ \sum_{ij} c_{ij}|\,e_i\,\rangle \otimes |\,f_j\,\rangle \;\middle|\; c_{ij} \in \mathbb{C},\ |\,e_i\,\rangle : \mathcal{H}_A\text{の基底},\ |\,f_j\,\rangle : \mathcal{H}_B\text{の基底} \right\}$$

行列のテンソル積

○ X : $\mathcal{H}_A$ 上の行列，Y : $\mathcal{H}_B$ 上の行列

$$(X \otimes Y)(|\,\psi_A\,\rangle \otimes |\,\psi_B\,\rangle) = (X|\,\psi_A\,\rangle) \otimes (Y|\,\psi_B\,\rangle)$$

を線形に拡大して $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の行列 $X \otimes Y$ を定義

○ テンソル積 = クロネッカー積

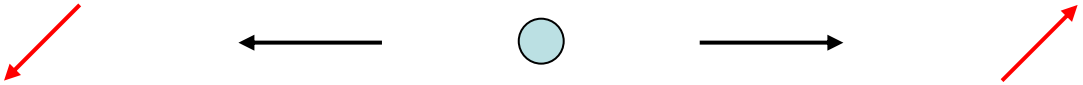
$$X = \begin{pmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mm} \end{pmatrix} \qquad Y = \begin{pmatrix} y_{11} & \cdots & y_{1n} \\ \vdots & & \vdots \\ y_{n1} & \cdots & y_{nn} \end{pmatrix}$$

$$\Longrightarrow \quad X \otimes Y = \begin{pmatrix} x_{11}Y & \cdots & x_{1m}Y \\ \vdots & & \vdots \\ x_{m1}Y & \cdots & x_{mm}Y \end{pmatrix}$$

エンタングルメント (量子もつれ)

Einstein-Podolsky-Rosen (EPR) の思考実験 (1935)

$\mathcal{H}_A = \mathbb{C}^2$ $\mathcal{H}_B = \mathbb{C}^2$



原子：一対の光子生成，角運動量保存

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \in \mathcal{H}_A \otimes \mathcal{H}_B$$

射影仮説

A：プラス(＋)基底で測定

p=1/2 測定結果 0：$|\Psi^+\rangle \longrightarrow |01\rangle$

p=1/2 測定結果 1：$|\Psi^+\rangle \longrightarrow |10\rangle$

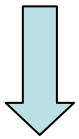
○ Aの測定結果にしたがって，Bの状態が瞬時に変化

歴史：Bell の不等式とエンタングルメント

○ EPR :「実在の局所性」⇒ 量子力学は不完全？

○ Bell の不等式 (1964)
- 「実在の局所性」から導かれる実験的に検証可能な不等式

○ Aspect et al. による実験 (1982)
- 「実在の局所性」ではなく，量子力学を支持



パラダイムシフト

エンタングルメントを積極的に利用

Bell 基底

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad |10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$$

$\longleftrightarrow$

ユニタリ変換

$\mathbb{C}^2 \otimes \mathbb{C}^2$ **上の正規直交基底**

量子テレポーテーション (Bennett et. al, 1993)

$\mathcal{H} = \mathbb{C}^2$

Alice : $\mathcal{H}_A = \mathbb{C}^2$

Bob : $\mathcal{H}_B = \mathbb{C}^2$

未知の量子状態

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$(|\alpha|^2 + |\beta|^2 = 1)$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

エンタングルメント共有

$$|\psi\rangle \otimes |\Phi^+\rangle = \frac{1}{2}\Big\{|\Phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle)$$
$$+ |\Psi^+\rangle \otimes (\beta|0\rangle + \alpha|1\rangle) + |\Psi^-\rangle \otimes (-\beta|0\rangle + \alpha|1\rangle)\Big\}$$

Alice : $\mathcal{H} \otimes \mathcal{H}_A$ をベル基底で測定

$\Longrightarrow$

Bob : 測定結果に応じてユニタリ変換

測定結果を通信

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を復元

二準位系のユニタリ変換

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

bit flip $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ phase flip $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$X|0\rangle = |1\rangle \qquad Z|0\rangle = |0\rangle$$
$$X|1\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

$$|\psi\rangle \otimes |\Phi^+\rangle = \frac{1}{2}\Big\{|\Phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |\Psi^+\rangle \otimes (\beta|0\rangle + \alpha|1\rangle) + |\Psi^-\rangle \otimes (-\beta|0\rangle + \alpha|1\rangle)\Big\}$$

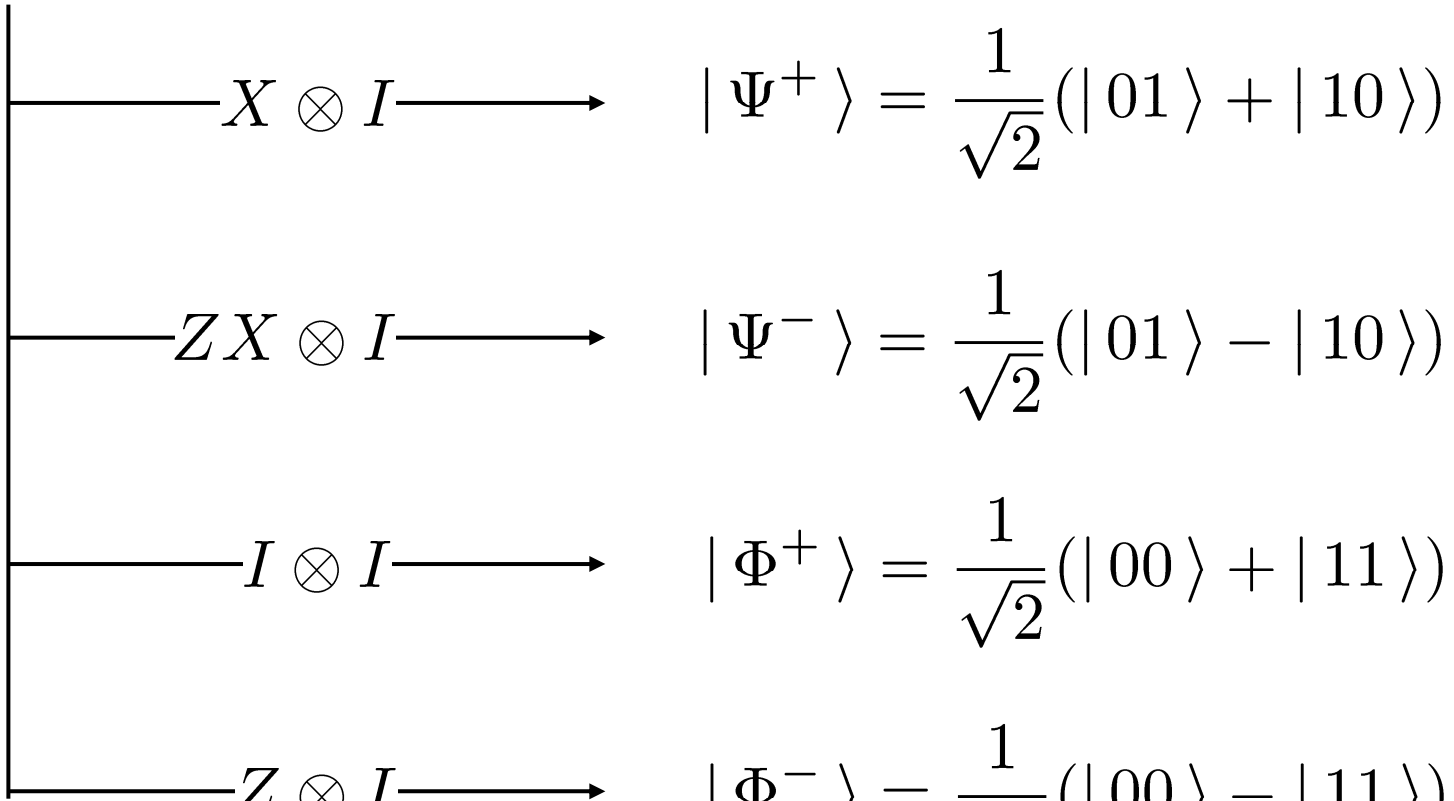
Alice 測定結果

$$\Phi^+ \Longrightarrow I \text{ (恒等変換)}$$
$$\Phi^- \Longrightarrow Z$$
$$\Psi^+ \Longrightarrow X$$
$$\Psi^- \Longrightarrow ZX$$

Bob : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を復元

Bell 基底とユニタリ変換

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



量子高密度符号化　dense coding (Bennett-Wiesner, 1992)

Alice : $\mathcal{H}_A = \mathbb{C}^2$

Bob : $\mathcal{H}_B = \mathbb{C}^2$

エンタングルメント共有　$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice : ユニタリ変換　⇒　粒子を送信

メーセージ				
1	$X \otimes I$	$\longrightarrow$	$\|\Psi^+\rangle$
2	$ZX \otimes I$	$\longrightarrow$	$\|\Psi^-\rangle$
3	$I \otimes I$	$\longrightarrow$	$\|\Phi^+\rangle$
4	$Z \otimes I$	$\longrightarrow$	$\|\Phi^-\rangle$

Bob : Bell基底で測定

○　一回の粒子の送信で 2 bit のメッセージ伝達