

2014 年電子情報通信学会ソサイエティ大会  
IT 研企画セッション

# 有限長解析

—情報理論から暗号, 通信, 量子への展開—

オーガナイザ: 林正人

2014.9.25

このファイルは、本企画セッションでの  
以下の4件の講演スライドをまとめたものです。

- 情報源圧縮, 乱数生成における有限長理論  
林正人(名大)
- 通信路符号化における有限長理論  
八木秀樹(電通大)
- 符号長無限大の極限 $N \rightarrow \infty$ より少し手前に広がる風景  
—低密度パリティ検査符号とポーラ符号の漸近解析—  
田中利幸(京大)
- 量子暗号における有限長解析  
鶴丸豊広(三菱電機)

# 概要

本企画セッションは、情報理論固有のテーマのみならず、隣接分野への展開を視野に入れたプログラムで開催された。

最初に、本セッションの提案者である林が、有限長理論の流れについて述べた後に、情報源圧縮、乱数生成における有限長理論について講演を行った。ここでは、独立同一分布のみならず、Markov情報源への拡張、量子系への拡張にも簡単に触れた。次に、八木が有限長理論の中で最もホットな話題である通信路符号化について有限長の視点から講演を行った。

休憩を挟んで、田中が通信への応用を視野に入れ、近年注目を浴びているPolar符号とLDPC符号についての有限長の成果について講演した。最後に、鶴丸が重要な応用の1つとして注目を浴びている量子暗号に関して有限長理論の視点から講演した。

# 秘密一様乱数生成, 情報源圧縮 における有限長理論

林正人

名古屋大学大学院 多元数理科学研究科

Centre for Quantum Technologies, National University of Singapore



# NAGOYA UNIVERSITY



共同研究者 渡辺峻 徳島大学大学院 ソシオテクノサイエンス研究部

# 2次漸近論のきっかけ

2003年の情報理論研究会(淡路島)の2つの講演

4. 情報スペクトル: あれこれ

○韓 太舜(電通大)

5. 量子情報理論における仮説検定の役割

○林 正人(科学技術振興機構)

韓先生の講演では, 正規化Divergenceを基準に取った場合での情報源符号化伝承定理が証明された. しかし, 2次漸近論を考慮すると, 変動距離を基準に取った場合には成り立たないことが確認できることに気がつき, 以下の論文を執筆するきっかけとなった.

**M. Hayashi**, Second-order asymptotics fixed-length source coding and intrinsic randomness," *IEEE Transactions on Information Theory*, Vol, 54, No. 10, 4619-4637 (2008).

一方, 後者の林の発表は, 韓・長岡の研究を引き継ぎ仮説検定をベースに情報理論の体系化を与えることが可能であることを指摘した講演であり, 現在のPolyanskiyらのアプローチのきっかけとなった⇒(八木).

## 従来の情報理論 (Shannon理論)

- $n \rightarrow$  無限大の漸近極限を主に扱っていた.
- 操作的な量をエントロピーのような分かりやすい量で表すことに成功した.
- しかも最適化までも厳密に扱うことができた
- しかし, 現実の問題では,  $n$ は有限である.
- そのため使えない机上の空論と考えられてきた.
- 実用には別途, 符号理論を考える必要があった.
- 昔の情報理論の教科書には, 前半にシャノン理論が書かれており, 途中から突然, 符号理論の話が始まっているものがあった.

# 通信理論・暗号理論・ 情報理論内部からの影響

- 通信において、実現可能な符号の性能が向上したため、有限サイズでの最適性能が知りたくなった(田中).
- 暗号理論では、そもそも独立同一性を仮定しない  
→min entropy→min entropy の近似が必要.
- min-entropyの近似と情報理論のスペクトル法はほとんど同じ.
- スペクトルを使えば、中心極限定理+ $\alpha$ で2次の漸近論が出る.
- 2次の漸近論を使えば、有限長の誤り確率の近似値が出る.

## 量子暗号からの影響

- 量子暗号では、有限サイズでの安全性を保証しないといけない。
- 量子暗号でのセキュリティの評価は、相補的な基底で、秘匿性増強に用いた符号と双対な符号で仮想的に通信し、最尤復号を用いて復号した場合の復号誤り確率で評価できる(鶴丸)。
- 実際に復号するわけでないので復号コストを考えなくても良い。
- 最尤復号を仮定してもよいので、意外と評価は簡単。



# 有限長理論の発展

- 実はこれらの有限長の評価は、かなり、Shannon 理論に近いタイプの評価で可能
- Shannon理論は、机上の空論から実用に結びついた理論に脱皮しようとしている。
- 有限長評価はかなり体系的に展開可能なので、Markov 過程にも容易拡張できる。  
(Markov過程の情報幾何)
- 量子情報処理全般への展開は、非可換性のため、困難であるが盛んに研究されている。

# 有限長性能評価式の要件

- 評価式が計算可能
  - 計算量が $O(1)$ ,  $O(n)$ ,  $O(n \log n)$ , もしくは、既存の計算パッケージを使って計算できる. (**one-shot=有限長ではない!**)
- 評価式が $n \rightarrow$ 無限大の極限で最適
  - 2次漸近最適性  $\varepsilon = \text{const}$
  - Moderate deviation 型の最適性  $\varepsilon = e^{-cn^t}$
  - Large deviation 型の最適性  $\varepsilon = e^{-cn}$
- どのクラスの操作に関する評価式か？
  - 実現コストを無視した最も広いクラス
  - 実現コストが一定の範囲に収まるクラス

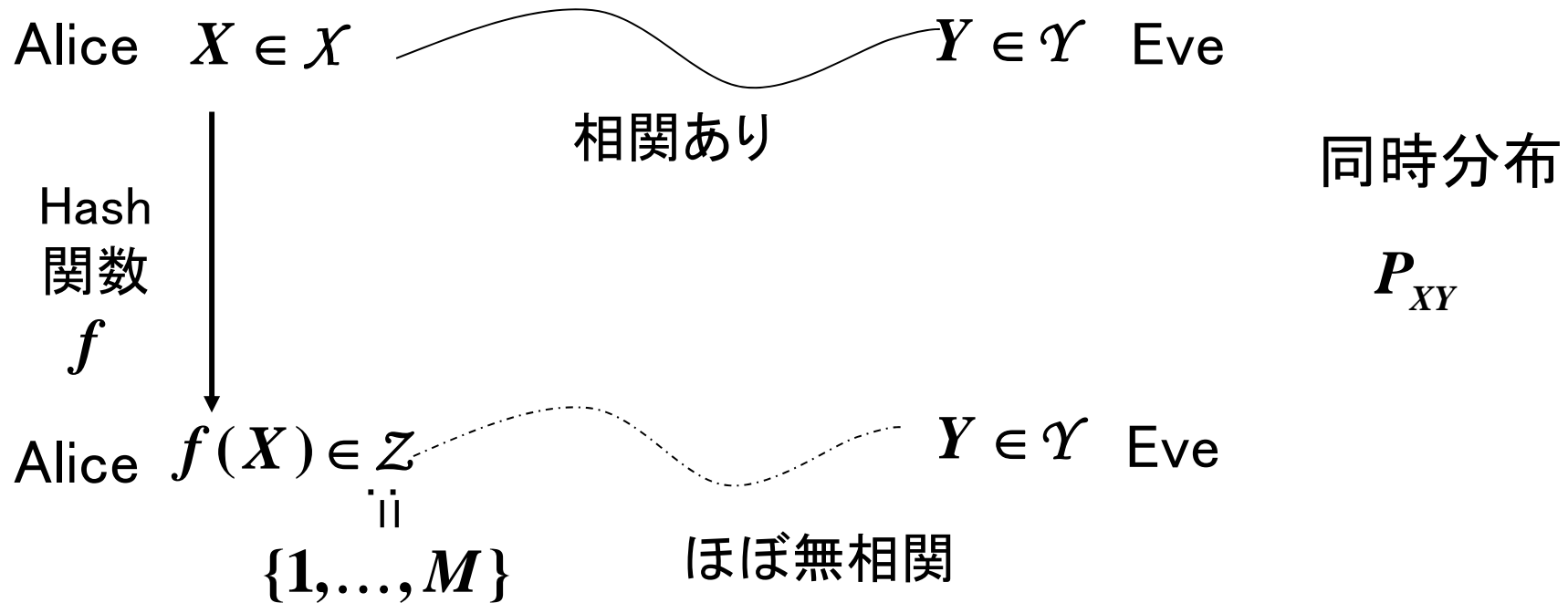
# 講演内容

- 秘密一様乱数生成での有限長理論
- 情報源圧縮での有限長理論
- 加法的通信路符号化での有限長理論
- 一般の通信路符号化での有限長理論(八木)

# 秘密一様乱数生成

- 暗号理論, 量子暗号, 情報理論それぞれからのアプローチの交差点
- 復号のことを気にしなくてもいいので, 実用性を考慮してもかなり精緻な議論が可能
- 誤り確率を評価するわけでないので, 従来の情報理論と異なった手法が必要.
- 情報源符号化の議論を組み合わせることで, 情報源符号化伝承の検証も可能

# セキュリティ基準



$P_{XY}$  : 同時分布

Universally composable criterion

$$\|P_{XY} - P_{U,X} \times P_Y\|_1 \quad P_{U,X} : \mathcal{X} \text{ 上の一様分布}$$

# 定式化

$$\Delta_n(f, P) := \frac{1}{2} \left\| P_{f(X^n)Y^n} - P_{U, \mathbf{F}_2^L} \times P_{Y^n} \right\|_1, \quad P_{f(X^n)Y^n} = P_{XY}^n$$

$$\Delta_n(F, P) := \frac{1}{2} E_F \left\| P_{F(X^n)Y^n} - P_{U, \mathbf{F}_2^L} \times P_{Y^n} \right\|_1 \quad f : \mathcal{X}^n \rightarrow \mathbf{F}_2^L$$

$F$  : ハッシュ関数のアンサンブル(ensemble)

以下の2つの量について注目:

$$L_{n, \max}(\varepsilon, P) := \max_f \left\{ L \mid \Delta_n(f, P) \leq \varepsilon, f : \mathcal{X}^n \rightarrow \mathbf{F}_2^L \right\}$$

$$L_{n, e, \max}(\varepsilon, P) := \max_F \left\{ L \mid \Delta_n(F, P) \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^L \right\}$$

$$L_{n, U, \max}(\varepsilon, P) := \max_{F \in U_2} \left\{ L \mid \Delta_n(F, P) \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^L \right\}$$

$$L_{n, U, \min}(\varepsilon, P) := \min_{F \in U_2} \left\{ L \mid \Delta_n(F, P) \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^L \right\}$$

$U_2$ : ユニバーサル2ハッシュ関数(以下を満たすもの)の集合

$$\Pr \{ F(x_1) = F(x_2) \} \leq \frac{1}{2^L} \quad \forall x_1 \neq \forall x_2 \in \mathcal{X}^n$$

$$L_{n, U, \min}(\varepsilon, P) \leq L_{n, U, \max}(\varepsilon, P) \leq L_{n, e, \max}(\varepsilon, P) = L_{n, \max}(\varepsilon, P)$$

# 例: Toeplitz 行列

$$\begin{aligned} A_Z &: m \times n \text{ 行列} \\ A_Z &: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \end{aligned}$$

$$Z = (a_1, \dots, a_{n-1}) \in \mathbb{F}_2^{n-1}$$

$$A_Z := \begin{pmatrix} a_m & a_{m+1} & \cdots & a_{n-2} & a_{n-1} & 1 & & & \\ a_{m-1} & a_m & \cdots & a_{n-3} & a_{n-2} & 1 & & 0 & \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \ddots & & \\ a_2 & a_3 & \cdots & a_{n-m} & a_{n-m+1} & 0 & & 1 & \\ a_1 & a_2 & \cdots & a_{n-m-1} & a_{n-m} & & & & 1 \end{pmatrix}$$

$\{A_Z\}$  はユニバーサル2条件を満たす

このハッシュ関数を構成するための計算量は小さい。  
ただし, random seeds  $Z$  は一様分布に従う。

# 様々な上下限

$L_{n,U,\min}(\varepsilon, P) \leq L_{n,\max}(\varepsilon, P)$  について共通の上下限が以下のように取れる.

$\bar{L}_{n,s}(\varepsilon, P), \underline{L}_{n,s}(\varepsilon, P)$ : 情報スペクトル形の上下限

$\bar{L}_{n,m}(\varepsilon, P), \underline{L}_{n,m}(\varepsilon, P)$ : Smooth min entropy による上下限

実は,  $\bar{L}_{n,s}(\varepsilon, P), \underline{L}_{n,s}(\varepsilon, P)$  は  $\bar{L}_{n,m}(\varepsilon, P), \underline{L}_{n,m}(\varepsilon, P)$  と同じ値になる.

$\bar{L}_{n,r}(\varepsilon, P), \underline{L}_{n,e}(\varepsilon, P)$ : 条件付Renyi entropyによる  $L_{n,U,\min}(\varepsilon, P)$  の上下限

## 計算量

$\bar{L}_{n,s}(\varepsilon, P), \underline{L}_{n,s}(\varepsilon, P)$ : 対応する確率分布の裾確率から計算できる.

$\bar{L}_{n,r}(\varepsilon, P), \underline{L}_{n,e}(\varepsilon, P)$ :  $n$ に依存しない.  $O(1)$ .



# スペクトル型上下限の具体形

$$\underline{L}_{n,s}(\varepsilon, P)$$

$$:= \sup \left\{ L \left| \inf_{\gamma \geq 0} P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) < \gamma \right\} + 2^{\frac{L-\gamma}{2}-1} \leq \varepsilon \right. \right\}$$

$$\bar{L}_{n,s}(\varepsilon, P)$$

$$:= \inf \left\{ L \left| \sup_{\gamma \geq 0} P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) < \gamma \right\} - 2^{\gamma-L} \geq \varepsilon \right. \right\}$$

# 独立同一分布の場合

大数の法則により以下の確率収束が成り立つ

$$\frac{-1}{n} \log P_{XY}^n(x | y) = \frac{-1}{n} \sum_{i=1}^n \log P_{X|Y}(x_i | y_i)$$

$$\rightarrow H_P(X | Y) := - \sum_{x,y} P_{XY}(x, y) \log P_{X|Y}(x | y)$$

$$x = (x_1, \dots, x_n), y = (y_1, \dots, y_n),$$

すなわち,

$$\frac{1}{n} \underline{L}_{n,s}(\varepsilon, P), \frac{1}{n} \bar{L}_{n,s}(\varepsilon, P) \rightarrow H_P(X | Y)$$

$$0 < \forall \varepsilon < 1$$

# 復習：大数の法則と中心極限定理

$X_1, \dots, X_n$  :  $X$  と同一な分布に独立に従う確率変数

## 大数の法則

$$\Pr\{|X^n - E(X)| > \varepsilon\} \rightarrow 0$$

$$X^n := \frac{X_1 + \dots + X_n}{n}$$

大数の法則から、有限の  $n$  について

$\Pr\{|X^n - E(X)| > \varepsilon\}$  の近似値を与えることは不可能.

# 復習：大数の法則と中心極限定理

$X_1, \dots, X_n$  :  $X$  と同一な分布に独立に従う確率変数  
中心極限定理

$$\Pr\left\{\left|\frac{\sqrt{n}(X^n - E(X))}{\sqrt{V(X)}}\right| > \varepsilon\right\} \rightarrow \Phi(\varepsilon) - \Phi(-\varepsilon)$$

$$X^n = (X_1, \dots, X_n) \quad \Phi(a) := \int_{-\infty}^a \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$$

中心極限定理から、有限の  $n$  について  
 $\Pr\{|X^n - E(X)| > \varepsilon\}$  の近似値を与えること  
とは可能.

# 中心極限定理を適用する

$$\bar{L}_{n,s}(\boldsymbol{\varepsilon}, P) = \underline{L}_{n,s}(\boldsymbol{\varepsilon}, P) + o(\sqrt{n})$$

$$= nH_P(X|Y) - \sqrt{nV_P(X|Y)}\Phi^{-1}(\boldsymbol{\varepsilon}) + o(\sqrt{n})$$

$$V_P(X|Y) := \sum_{x,y} P_{XY}(x,y) \left( H_P(X|Y) + \log P_{X|Y}(x|y) \right)^2$$

# 漸近最適性I

$\bar{L}_{n,s}(\varepsilon, P), \underline{L}_{n,s}(\varepsilon, P)$ : 2次漸近最適性を満たす.

$$\begin{aligned}\bar{L}_{n,s}(\varepsilon, P) &= \underline{L}_{n,s}(\varepsilon, P) + o(\sqrt{n}) \\ &= nH_P(X|Y) - \sqrt{nV_P(X|Y)}\Phi^{-1}(\varepsilon) + o(\sqrt{n})\end{aligned}$$

$\bar{L}_{n,s}(\varepsilon, P), \underline{L}_{n,s}(\varepsilon, P)$ : Moderate deviationについて漸近最適

$$\begin{aligned}\bar{L}_{n,s}(e^{-n^{1-2t}r}, P) &= \underline{L}_{n,s}(e^{-n^{1-2t}r}, P) + o(n^{1-t}) \\ &= nH_P(X|Y) - \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2\end{aligned}$$

$$H_P(X|Y) := -\sum_{x,y} P_{XY}(x,y) \log P_{X|Y}(x|y)$$

$$V_P(X|Y) := \sum_{x,y} P_{XY}(x,y) \left( H_P(X|Y) + \log P_{X|Y}(x|y) \right)^2$$

# 漸近最適性II

$\bar{L}_{n,r}(\varepsilon, P), \underline{L}_{n,r}(\varepsilon, P)$ : Moderate deviationについて漸近最適

$$\bar{L}_{n,r}(e^{-n^{1-2t}r}, P) = \underline{L}_{n,r}(e^{-n^{1-2t}r}, P) + o(n^{1-t})$$

$$= nH_P(X|Y) - \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2$$

$\bar{L}_{n,r}(\varepsilon, P), \underline{L}_{n,r}(\varepsilon, P)$ : Large deviationについて漸近最適

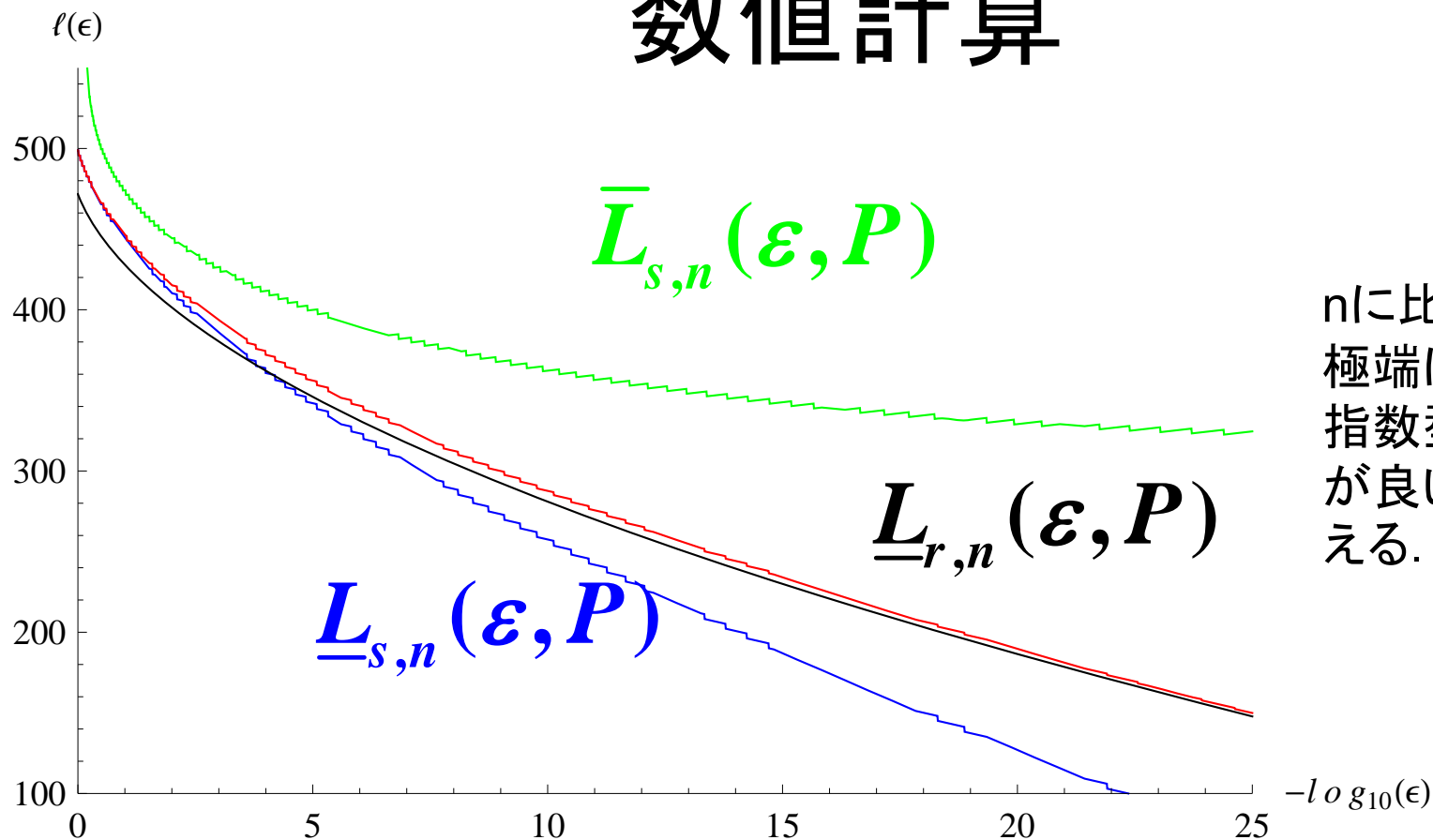
$$\bar{L}_{n,r}(e^{-nr}, P) = \underline{L}_{n,r}(e^{-nr}, P) + o(n) = n \sup_{0 < s < 1} H_{1+s|P}^\uparrow(X|Y) - \frac{(1+s)r}{s}$$

ただし,  $r$ は臨界指数以下.

$$\begin{aligned} H_{1+s|P}^\uparrow(X|Y) &:= -\frac{1+s}{s} \log \sum_y \left[ \sum_x P_{XY}(x, y)^{1+s} \right]^{\frac{1}{1+s}} \\ &= \max_{Q_Y} -\frac{1}{s} \log \sum_{x,y} P_{XY}(x, y)^{1+s} Q_Y(y)^{-s} \end{aligned}$$

$$H_{1+s|P}^\downarrow(X|Y) := -\frac{1}{s} \log \sum_{x,y} P_{XY}(x, y)^{1+s} P_Y(y)^{-s}$$

# 数値計算



nに比べて、 $\epsilon$ が  
極端に小さいと、  
指数型評価の方が  
良い評価を与える。

$$P_{XY}(x, y) = \begin{cases} q/2 & \text{if } x \neq y \\ (1-q)/2 & \text{if } x = y \end{cases}$$

$$\mathcal{X} = \mathcal{Y} = \{0, 1\}$$

n = 1000, 反転確率 q=0.11 での比較.  
赤はハイブリッド型



# Random seeds が一様分布に従わない場合

- Random seeds が一様乱数生成に従わない場合, ユニバーサル2にならない.
- しかし, Random seeds が一様乱数生成になるランダムなハッシュ関数は, そのRandom seeds が一様分布に従わない場合でも, そのmin entropy が十分一様分布の場合に近ければ, 評価は少し補正するだけで十分.

# わかったこと

- 一様乱数生成の場合, Toeplitz行列などでほぼ最適な性能が実現でできるため, ここで得られた評価は真に実用的な意味を持つ.
- $\varepsilon$ が $n$ の大きさに比して小さいときは, 指数型の評価の方が優れている.
- したがって, どのタイプの評価が優れているかについては, ケースバイケースとしか言いようがない.

# 関連課題

- 誤り訂正と漏洩情報が存在する設定での有限長理論は、今後の課題.
- 同様の設定で、得られた秘密乱数を認証やメッセージ認証に使うことができる.
- 認証やメッセージ認証では、証明者と認証者の持つ乱数の間に誤りがある場合は、誤り訂正を加えないといけない.
- 上述の設定での認証やメッセージ認証は最適性まで考慮すると、未解決であり今後の解析が必要である.

# 固定長情報源圧縮での有限長理論

- 仮説検定に帰着できるので、極めて簡単.
- 加法的通信路の符号化に直結するので意外と重要.
- 一様乱数生成の議論を組み合わせることで、情報源符号化伝承の検証も可能

# 定式化



符号化:  $f : \mathcal{X}^n \rightarrow \mathbf{F}_2^S$       復号化:  $g : \mathbf{F}_2^S \times \mathcal{Y}^n \rightarrow \mathcal{X}^n$        $\phi := (f, g)$

$$\mathbf{P}_{n,e}[\phi, P] := P_{XY}^n \{X \neq g(f(X), Y)\}$$

$$S_{n,\min}(\varepsilon, P) := \min_{\phi=(f,g)} \left\{ S \mid \mathbf{P}_{n,e}[\phi, P] \leq \varepsilon, f : \mathcal{X}^n \rightarrow \mathbf{F}_2^S \right\}$$

$$S_{n,e,\min}(\varepsilon, P) := \min_{\Phi=(F,G)} \left\{ S \mid \mathbf{P}_{n,e}[\Phi, P] \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^S \right\}$$

$$S_{n,U,\min}(\varepsilon, P) := \min_{\Phi=(F,G), F \in \mathcal{U}_2} \left\{ S \mid \mathbf{P}_{n,e}[\Phi, P] \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^S \right\}$$

$$S_{n,U,\max}(\varepsilon, P) := \max_{\Phi=(F,G), F \in \mathcal{U}_2} \left\{ S \mid \mathbf{P}_{n,e}[\Phi, P] \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbf{F}_2^S \right\}$$

$$S_{n,e,\min}(\varepsilon, P) \leq S_{n,\min}(\varepsilon, P) \leq S_{n,U,\min}(\varepsilon, P) \leq S_{n,U,\max}(\varepsilon, P)$$

# 様々な上下限

$S_{n,e,\min}(\varepsilon, P) \leq S_{n,U,\max}(\varepsilon, P)$  について共通の上下限が  
以下のように取れる.

$\bar{S}_{n,s}(\varepsilon, P), \underline{S}_{n,s}(\varepsilon, P)$ : 情報スペクトル形の上下限

$\bar{S}_{n,m}(\varepsilon, P), \underline{S}_{n,m}(\varepsilon, P)$ : Smooth min entropy による上下限

実は,  $\bar{S}_{n,s}(\varepsilon, P), \underline{S}_{n,s}(\varepsilon, P)$  は  $\bar{S}_{n,m}(\varepsilon, P), \underline{S}_{n,m}(\varepsilon, P)$  と同じ値になる.

$\bar{S}_{n,r}(\varepsilon, P), \underline{S}_{n,e}(\varepsilon, P)$ : 条件付Renyi entropyによる上下限

## 計算量

$\bar{S}_{n,s}(\varepsilon, P), \underline{S}_{n,s}(\varepsilon, P)$ : 対応する確率分布の裾確率から計算できる.

$\bar{S}_{n,r}(\varepsilon, P), \underline{S}_{n,e}(\varepsilon, P)$ :  $n$ に依存しない.  $O(1)$ .

# スペクトル型上下限の具体形

$$\bar{S}_{n,s}(\varepsilon, P) := \inf \left\{ S \mid P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) > S \right\} \leq \varepsilon \right\}$$

$$\underline{S}_{n,s}(\varepsilon, P)$$

$$:= \inf \left\{ S \mid \sup_{\gamma \geq 0} P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) > \gamma \right\} - 2^{S-\gamma} \geq \varepsilon \right\}$$

# 漸近最適性I

$\bar{S}_{n,s}(\varepsilon, P), \underline{S}_{n,s}(\varepsilon, P)$ : 2次漸近最適性を満たす.

$$\begin{aligned}\underline{S}_{n,s}(\varepsilon, P) &= \bar{S}_{n,s}(\varepsilon, P) + o(\sqrt{n}) \\ &= nH_P(X|Y) + \sqrt{nV_P(X|Y)}\Phi^{-1}(\varepsilon) + o(\sqrt{n})\end{aligned}$$

$\bar{S}_{n,s}(\varepsilon, P), \underline{S}_{n,s}(\varepsilon, P)$ : Moderate deviationについて漸近最適

$$\begin{aligned}\bar{S}_{n,s}(e^{-n^{1-2t}}, P) &= \underline{S}_{n,s}(e^{-n^{1-2t}}, P) + o(n^{1-t}) \\ &= nH_P(X|Y) + \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2\end{aligned}$$

$$H_P(X|Y) := -\sum_{x,y} P_{XY}(x,y) \log P_{X|Y}(x|y)$$

$$V_P(X|Y) := \sum_{x,y} P_{XY}(x,y) \left( H_P(X|Y) + \log P_{X|Y}(x|y) \right)^2$$



# 漸近最適性II

$\bar{S}_{n,r}(\varepsilon, P), \underline{S}_{n,r}(\varepsilon, P)$ : Moderate deviation(について漸近最適

$$\begin{aligned} \bar{S}_{n,r}(e^{-n^{1-2t}r}, P) &= \underline{S}_{n,r}(e^{-n^{1-2t}r}, P) + o(n^{1-t}) \\ &= nH_P(X|Y) + \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2 \end{aligned}$$

$\bar{S}_{n,r}(\varepsilon, P), \underline{S}_{n,r}(\varepsilon, P)$ : Large deviation(について漸近最適

$$\bar{S}_{n,r}(e^{-nr}, P) = \underline{S}_{n,r}(e^{-nr}, P) + o(n) = n \inf_{-\frac{1}{2} \leq s \leq 0} H_{1+s|P}^\uparrow(X|Y) - \frac{(1+s)r}{s}$$

ただし,  $r$ は臨界指数以下.

$$\begin{aligned} H_{1+s|P}^\uparrow(X|Y) &:= -\frac{1+s}{s} \log \sum_y \left[ \sum_x P_{XY}(x, y)^{1+s} \right]^{\frac{1}{1+s}} \\ &= \max_{Q_Y} -\frac{1}{s} \log \sum_{x,y} P_{XY}(x, y)^{1+s} Q_Y(y)^{-s} \\ H_{1+s|P}^\downarrow(X|Y) &:= -\frac{1}{s} \log \sum_{x,y} P_{XY}(x, y)^{1+s} P_Y(y)^{-s} \end{aligned}$$

# 情報源符号化伝承

- 情報源符号化伝承:「情報源圧縮と一様乱数生成の漸近レートがともにShannonエントロピーであるので, 限界まで圧縮して得られた乱数列は一様乱数に近づく。」と考えられていた.
- 韓は一様乱数の基準を正規化相対エントロピーとしたときに, 情報源符号化伝承を証明した.
- 正規化相対エントロピーは弱セキュリティに対応するので弱い.
- 2次漸近論より以下が導け, 成り立たない.

$$\lim_{n \rightarrow \infty} \mathbf{P}_{n,e} [(f_n, g_n), P] + \Delta_n [f_n, P] \geq 1$$

- 同じことはエンタングルメントの集中化についても言える.

# 加法的通信路符号化での有限長理論 (及び一般化加法的通信路)

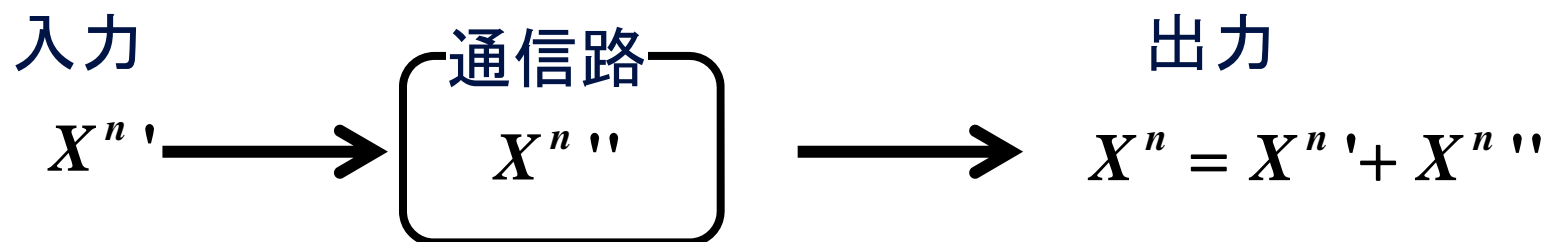
- 2元対称通信路はこのクラスに含まれる.
- ガウス通信路の場合でも, 入力を1,-1に制限すると, 一般化加法的通信路になる.
- したがってかなり重要なクラス
- 入力分布の最適化の必要がない
- 代数的対称性を符号化に要請すれば, 固定長情報源符号化とほとんど変わらない

# 加法的通信路と条件付き加法的通信路

$$\mathcal{X}: \text{加群} \quad \mathcal{X}^n := \underbrace{\mathcal{X} \times \cdots \times \mathcal{X}}_n$$
$$X^n = (X_1, \dots, X_n)$$

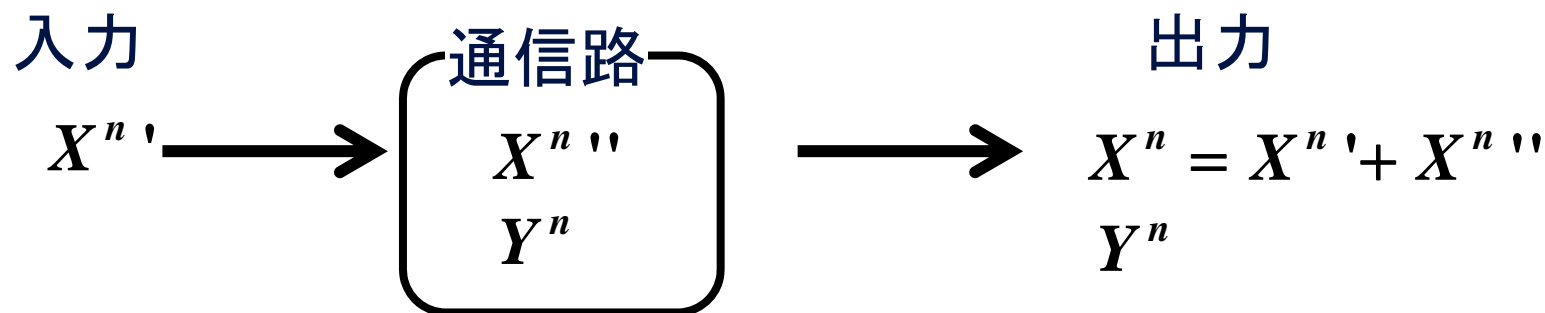
## 加法的通信路

$$W_{X^n|X^n}, (X^n = x^n | X^n' = x^n') := P_{X^n}(x^n' - x^n)$$



## 条件付き加法的通信路

$$W_{X^n, Y^n|X^n}, (X^n = x^n, Y^n = y^n | X^n' = x^n') := P_{X^n, Y^n}(x^n' - x^n, Y^n = y^n)$$



## 定式化(条件付き加法的通信路)

符号化:  $e_n : \mathbb{F}_2^M \rightarrow \mathcal{X}^n$  復号化:  $d_n : \mathcal{X}^n \times \mathcal{Y}^n \rightarrow \mathbb{F}_2^M$  符号:  $\psi_n = (e_n, d_n)$

$$\begin{aligned} \mathbf{P}_{e,n}[\psi_n, P] &:= \sum_{m \in \mathbb{F}_2^M} \frac{1}{2^M} W_{\mathcal{X}^n, \mathcal{Y}^n | \mathcal{X}^n}(\{d_n(x^n, y^n) \neq m\} | X^n = e_n(m)) \\ &= \sum_{m \in \mathbb{F}_2^M} \frac{1}{2^M} P_{XY}^n \{d_n(x^n + e_n(m), y^n) \neq m\} \end{aligned}$$

$$M_{n,\max}(\varepsilon, P) := \max_{\psi=(e,d)} \left\{ S \mid \mathbf{P}_{n,e}[\psi, P] \leq \varepsilon, e : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \right\}$$

$$M_{n,e,\max}(\varepsilon, P) := \max_{\Psi=(E,D)} \left\{ S \mid \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \right\}$$

# 符号化が線形であるとき

符号化  $e$  が線形とする.

情報源圧縮の符号化:  $f : \mathcal{X}^n \rightarrow \mathcal{X}^n / \text{Im } e = \mathbb{F}_2^S \in \mathcal{U}_2$  を考える.

情報源圧縮の復号化:  $g : \mathbb{F}_2^S \times \mathcal{Y}^n \rightarrow \mathcal{X}^n$

通信路符号化の復号化:  $d(x, y) := x - g(f(x), y) : \mathcal{X}^n \times \mathcal{Y}^n \rightarrow \mathcal{X}^n$

$$\begin{aligned} \mathbf{P}_{e,n}[(e, d), P] &= \sum_{m \in \mathbb{F}_2^M} \frac{1}{2^M} P_{XY}^n \{d_n(x^n + e_n(m), y^n) \neq m\} \\ &= P_{XY}^n \{X \neq g(f(X), Y)\} = \mathbf{P}_{n,e}[(f, g), P] \end{aligned}$$

$$\begin{aligned} M_{n,U,\min}(\varepsilon, P) &:= \min_{\Psi=(E,D)} \left\{ M \left| \begin{array}{l} \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, E : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \\ \mathcal{X}^n \rightarrow \mathcal{X}^n / \text{Im } E \in \mathcal{U}_2 \end{array} \right. \right\} \\ M_{n,U,\max}(\varepsilon, P) &:= \max_{\Psi=(E,D)} \left\{ M \left| \begin{array}{l} \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, E : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \\ \mathcal{X}^n \rightarrow \mathcal{X}^n / \text{Im } E \in \mathcal{U}_2 \end{array} \right. \right\} \end{aligned}$$

$$M_{n,U,\min}(\varepsilon, P) \leq M_{n,U,\max}(\varepsilon, P) \leq M_{n,\max}(\varepsilon, P) \leq M_{n,e,\max}(\varepsilon, P)$$

## 定式化(条件付き加法的通信路)

符号化:  $e_n : \mathbb{F}_2^M \rightarrow \mathcal{X}^n$  復号化:  $d_n : \mathcal{X}^n \times \mathcal{Y}^n \rightarrow \mathbb{F}_2^M$  符号:  $\psi_n = (e_n, d_n)$

$$\mathbf{P}_{e,n}[\psi_n, P] := \sum_{m \in \mathbb{F}_2^M} \frac{1}{2^M} W_{\mathcal{X}^n, \mathcal{Y}^n | \mathcal{X}^n}(\{d_n(x^n, y^n) \neq m\} | X^n = e_n(m))$$

$$= \sum_{m \in \mathbb{F}_2^M} \frac{1}{2^M} P_{XY}^n \{d_n(x^n + e_n(m), y^n) \neq m\}$$

$$M_{n,\max}(\varepsilon, P) := \max_{\psi=(e,d)} \left\{ S \mid \mathbf{P}_{n,e}[\psi, P] \leq \varepsilon, e : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \right\}$$

$$M_{n,e,\max}(\varepsilon, P) := \max_{\Psi=(E,D)} \left\{ S \mid \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, F : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \right\}$$

$$M_{n,U,\min}(\varepsilon, P) := \min_{\Psi=(E,D)} \left\{ M \mid \begin{array}{l} \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, E : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \\ \mathcal{X}^n \rightarrow \mathcal{X}^n / \text{Im}E \in U_2 \end{array} \right\}$$

$$M_{n,U,\max}(\varepsilon, P) := \max_{\Psi=(E,D)} \left\{ M \mid \begin{array}{l} \mathbf{P}_{n,e}[\Psi, P] \leq \varepsilon, E : \mathcal{X}^n \rightarrow \mathbb{F}_2^M \\ \mathcal{X}^n \rightarrow \mathcal{X}^n / \text{Im}E \in U_2 \end{array} \right\}$$

$$M_{n,U,\min}(\varepsilon, P) \leq M_{n,U,\max}(\varepsilon, P) \leq M_{n,\max}(\varepsilon, P) \leq M_{n,e,\max}(\varepsilon, P)$$

# 様々な上下限

$M_{n,U,\min}(\varepsilon, P) \leq M_{n,e,\max}(\varepsilon, P)$  について共通の上下限が  
以下のように取れる.

$\bar{M}_{n,s}(\varepsilon, P), \underline{M}_{n,s}(\varepsilon, P)$  : 情報スペクトル形の上下限

$\bar{M}_{n,r}(\varepsilon, P), \underline{M}_{n,e}(\varepsilon, P)$  : 条件付Renyi entropyによる上下限

## 計算量

$\bar{M}_{n,s}(\varepsilon, P), \underline{M}_{n,s}(\varepsilon, P)$  : 対応する確率分布の裾確率から計算できる.

$\bar{M}_{n,r}(\varepsilon, P), \underline{M}_{n,e}(\varepsilon, P)$  :  $n$  に依存しない.  $O(1)$ .



# スペクトル型上下限の具体形

$$\underline{M}_{n,s}(\varepsilon, P)$$

$$:= n \log |\mathcal{X}| - \inf \left\{ S \mid P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) > S \right\} \leq \varepsilon \right\}$$

$$\bar{M}_{n,s}(\varepsilon, P)$$

$$:= n \log |\mathcal{X}|$$

$$- \inf \left\{ S \mid \sup_{\gamma \geq 0} P_{XY}^n \left\{ -\log P_{X|Y}^n(x|y) > \gamma \right\} - 2^{S-\gamma} \geq \varepsilon \right\}$$

# 漸近最適性I

$\bar{M}_{n,s}(\varepsilon, P), \underline{M}_{n,s}(\varepsilon, P)$ : 2次漸近最適性を満たす.

$$\begin{aligned}\underline{M}_{n,s}(\varepsilon, P) &= \bar{M}_{n,s}(\varepsilon, P) + o(\sqrt{n}) \\ &= n(\log |\mathcal{X}| - H_P(X|Y)) - \sqrt{nV_P(X|Y)}\Phi^{-1}(\varepsilon) + o(\sqrt{n})\end{aligned}$$

$\bar{M}_{n,s}(\varepsilon, P), \underline{M}_{n,s}(\varepsilon, P)$ : Moderate deviationについて漸近最適

$$\begin{aligned}\bar{M}_{n,s}(e^{-n^{1-2t}r}, P) &= \underline{M}_{n,s}(e^{-n^{1-2t}r}, P) + o(n^{1-t}) \\ &= n(\log |\mathcal{X}| - H_P(X|Y)) - \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2\end{aligned}$$

$$H_P(X|Y) := -\sum_{x,y} P_{XY}(x,y) \log P_{X|Y}(x|y)$$

$$V_P(X|Y) := \sum_{x,y} P_{XY}(x,y) \left( H_P(X|Y) + \log P_{X|Y}(x|y) \right)^2$$

# 漸近最適性II

$\bar{M}_{n,r}(\varepsilon, P), \underline{M}_{n,e}(\varepsilon, P)$ : Moderate deviationについて漸近最適

$$\bar{M}_{n,r}(e^{-n^{1-2t}r}, P) = \underline{M}_{n,r}(e^{-n^{1-2t}r}, P) + o(n^{1-t})$$

$$= n(\log |X| - H_P(X|Y)) - \sqrt{2V_P(X|Y)}n^{1-t} + o(n^{1-t}), \quad 0 < t < 1/2$$

$\bar{M}_{n,r}(\varepsilon, P), \underline{M}_{n,e}(\varepsilon, P)$ : Large deviationについて漸近最適

$$\bar{M}_{n,r}(e^{-nr}, P) = \underline{M}_{n,r}(e^{-nr}, P) + o(n)$$

$$= n \log |X| - n \inf_{-\frac{1}{2} \leq s \leq 0} H_{1+s|P}^{\uparrow}(X|Y) - \frac{(1+s)r}{s}$$

ただし,  $r$ は臨界指数以下.

# 加法的通信路符号化, 固定長 情報源符号化の有限長理論の課題

- 秘密一様乱数生成と同様に有限長限界が得られた.
- しかし, 復号の計算量は考慮していない.
- そのため, 復号の計算量が大きくなならない符号のクラスについての有限長限界が必要となる.
- 例えば, LDPC符号やPolar符号などのクラスが考えられる.

# Markov 過程への拡張

- One-shot boundは注目する確率変数のキュムラント生成関数から計算可能.
- Markov 過程の場合, キュムラント生成関数は, 漸近的なキュムラント生成関数の $n$ 倍との差分は定数オーダー
- One-shot bound+定数オーダーの差分で有限長限界が得られる.
- 重要な量はすべて, 凸関数となる漸近的なキュムラント生成関数から与えることができる.
- IIDの場合とほぼ同様の漸近最適性を満たす有限長理論が可能.

## 量子系への拡張

- 非可換性のため、情報量の量子拡張が一意に決まらない。
- 単純仮説検定の場合であっても、領域に応じて異なる量子拡張が意味を持つ。
- 秘密一様乱数生成に関しては、量子暗号との関係で重要であるが、large deviation 型の漸近最適レートは得られていない。
- しかし、とりあえず使えそうな有限長限界は存在する。

# References

- MH and SW, **arXiv:1309.7528**
- およびその参考文献



電子情報通信学会ソサイエティ大会：IT 研企画セッション

## 通信路符号化における有限長理論

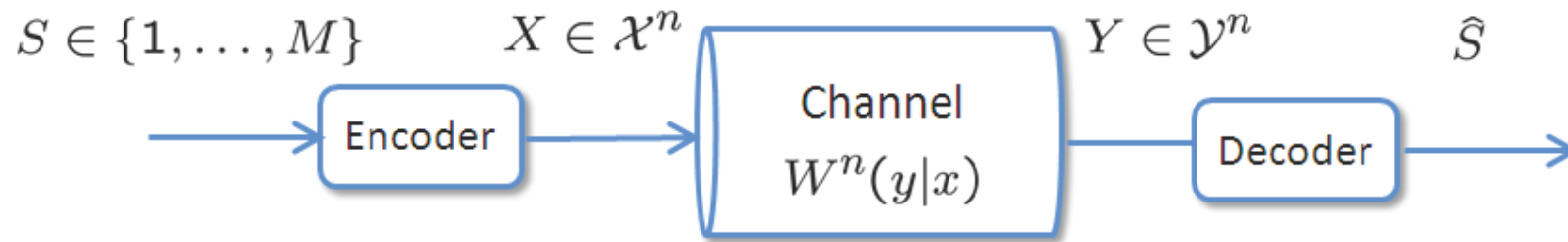
八木 秀樹

電気通信大学

2014.9.25

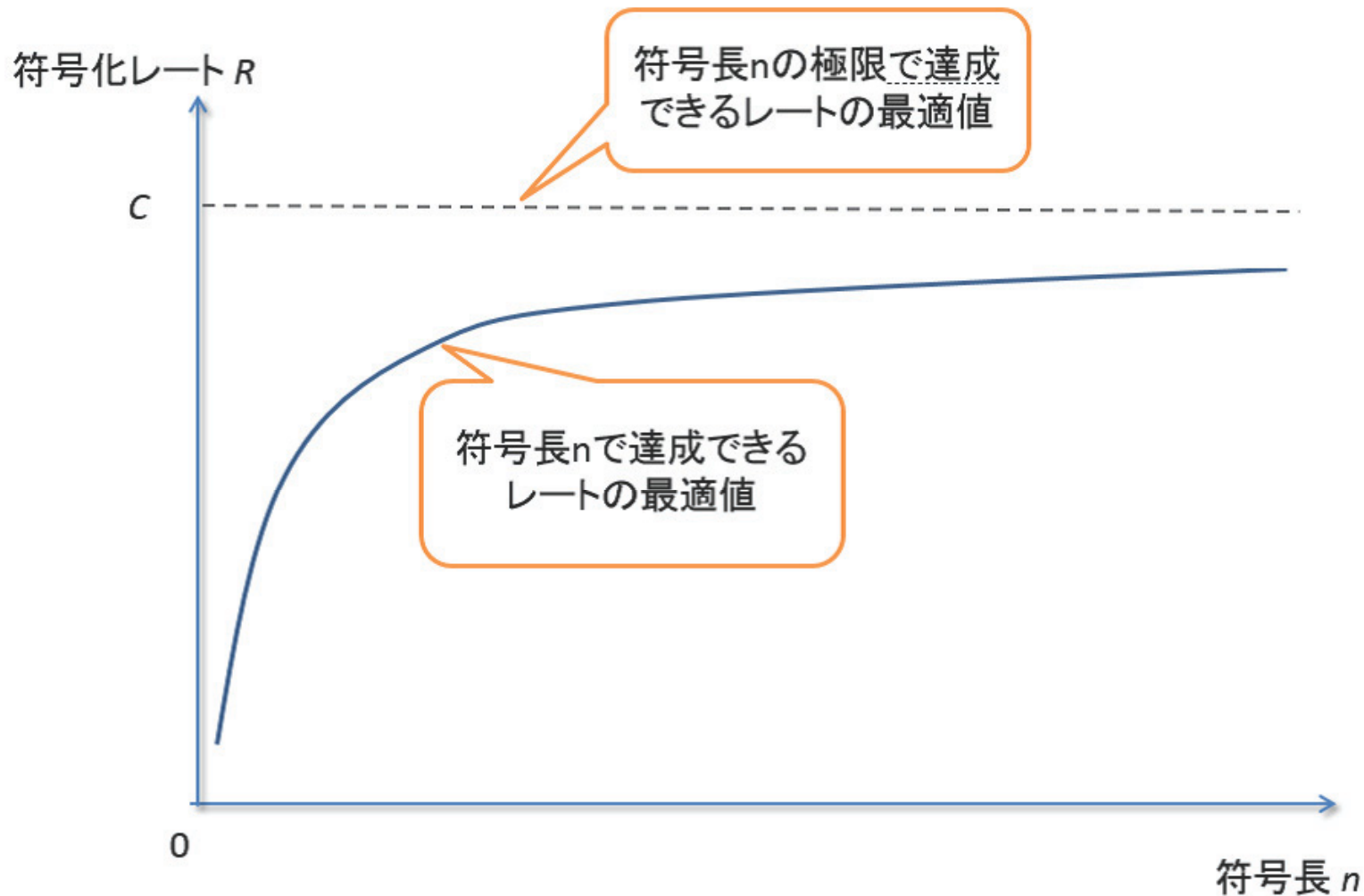


# 通信路符号化における符号化レートの理論限界



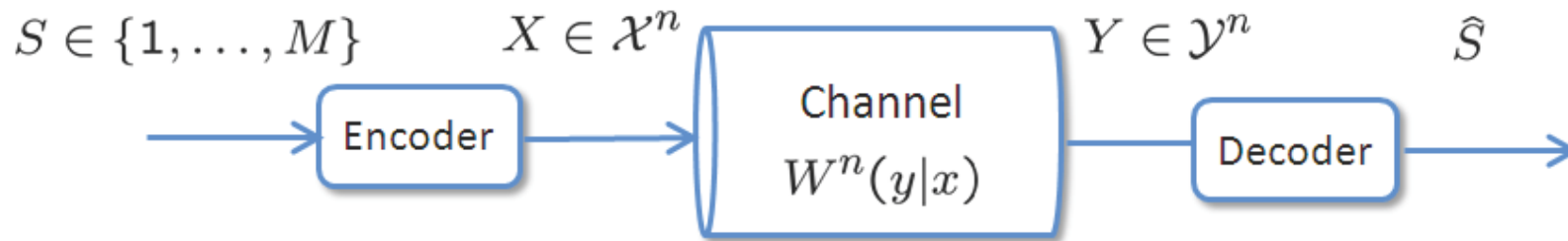
- $M_n$  個のメッセージを通信路  $W^n(y|x)$  を介して送る.
- $\varepsilon$ -通信路容量 : 復号誤り確率が  $\varepsilon$  を達成する**符号列**の最大符号化レート
  - ▶ 離散無記憶通信路 (DMC) :  $C = \max_{P_X} I(X; Y)$
  - ▶ SN 比  $P/N$  の AWGN 通信路 :  $C = \frac{1}{2} \log(1 + P/N)$
- よく行われる符号の評価 : 誤り確率  $\varepsilon$  を固定して, 符号化レートの  $C$  からの差分を図る (  $\implies$  **差分は必ず存在する** )

# 有限長の最大符号化レートの振舞



有限長  $n$  の場合のターゲットを知ることが必要

# 通信路符号化における有限長解析



- $M_n$  個のメッセージを通信路  $W^n(y|x)$  を介して送る.
- 符号長  $n$ , 復号誤り確率  $\varepsilon$  を達成する符号の**最大**符号語数を  $M_{n,\varepsilon}^*$  と表す.

## 本発表における有限長解析

$n, \varepsilon, W^n(y|x)$  が与えられたとき,  $\log M_{n,\varepsilon}^*$  を特徴づけること

# 有限長解析のアプローチ

- $\log M_{n,\varepsilon}^*$  を直接評価する（狭義の有限長解析）  
通信路  $W^n$  に対して、 $\log M_{n,\varepsilon}^*$  の上界式と下界式を評価する
- $\log M_{n,\varepsilon}^*$  の 2 次以下の項を評価する（広義の有限長解析）
  - ▶ シングルーザ通信路に対する 2 次符号化定理 [Strassen'62], [Hayashi'09], [Polyanskiy et al.'10]
  - ▶ DMC に対する 3 次以下の項の解析 [Moulin.'12], [Tomamichel & Tan'14]
  - ▶ 様々な符号化システムにおいて 2 次符号化レート解析が行われている

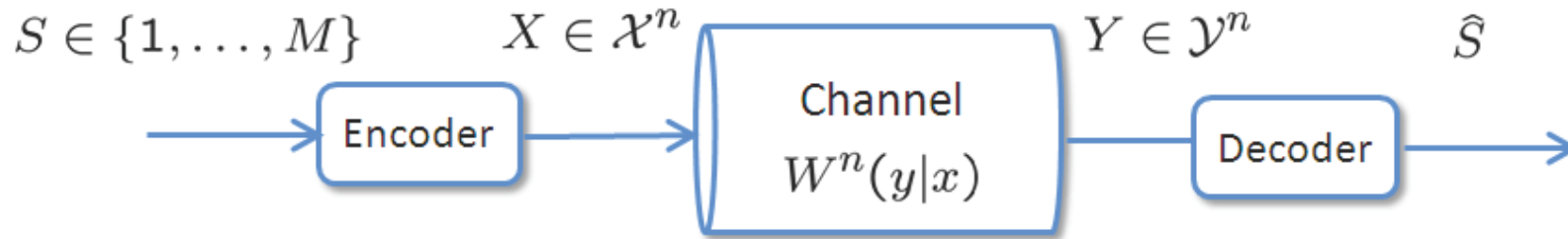
## 本発表の内容

通信路符号化における有限長解析のアプローチの紹介. 主に**仮説検定**と**復号**の類似性を利用した関連研究

# 2次符号化定理

## (広義の有限長解析)

# 一般通信路



- $M_n$  個のメッセージの**一様分布**
- 一般通信路  $W^n(y|x)$
- 通信路入力  $X \in \mathcal{X}^n$
- 通信路出力  $Y \in \mathcal{Y}^n$

簡単のため、全てのアルファベットは離散と仮定する。

以降、任意の  $A \subseteq \mathcal{X}^n \times \mathcal{Y}^n$  に対し、

$$\begin{aligned} P_{XY}(A) &:= \sum_{(x,y) \in A} P_X(x) W^n(y|x) \\ &= \Pr \{ (X, Y) \in A \} \end{aligned}$$

# $(n, M_n, \varepsilon)$ 符号

## 平均誤り確率

符号長  $n$ , メッセージ数  $M_n$  の符号  $C$  と復号法  $\psi : \mathcal{Y}^n \rightarrow \{1, \dots, M_n\}$  に対し,

$$P_e^{(n)} := \frac{1}{M_n} \sum_{m=1}^{M_n} \Pr[\psi(Y) \neq m | m \text{ sent}]$$

## $(n, M_n, \varepsilon)$ 符号

固定した  $\varepsilon \in [0, 1)$  に対し, 符号  $C$  がある復号法のもと

$$P_e^{(n)} \leq \varepsilon$$

を満たすとき, この符号を  $(n, M_n, \varepsilon)$  符号と呼ぶ.

$M_{n,\varepsilon}^*$ :  $(n, M_n, \varepsilon)$  符号の最大符号語数

# DMCにおける2次符号化定理

- 1次符号化定理 (Shannon'48) :

$$\log M_{n,\varepsilon}^* = nC + o(n)$$

$$C = \max_{P_X} \mathbb{E}_{P_X W} \left\{ \log \frac{W(Y|X)}{P_Y(Y)} \right\}$$

- ▶  $C$  は通信路容量 (1次レート) の最大値
- ▶ 大数の法則による解析
- 2次符号化定理 (Strassen'62, Hayashi'09, PPV'10) :

$$\log M_{n,\varepsilon}^* = nC + \sqrt{nV_\varepsilon} G^{-1}(\varepsilon) + O(\log n)$$

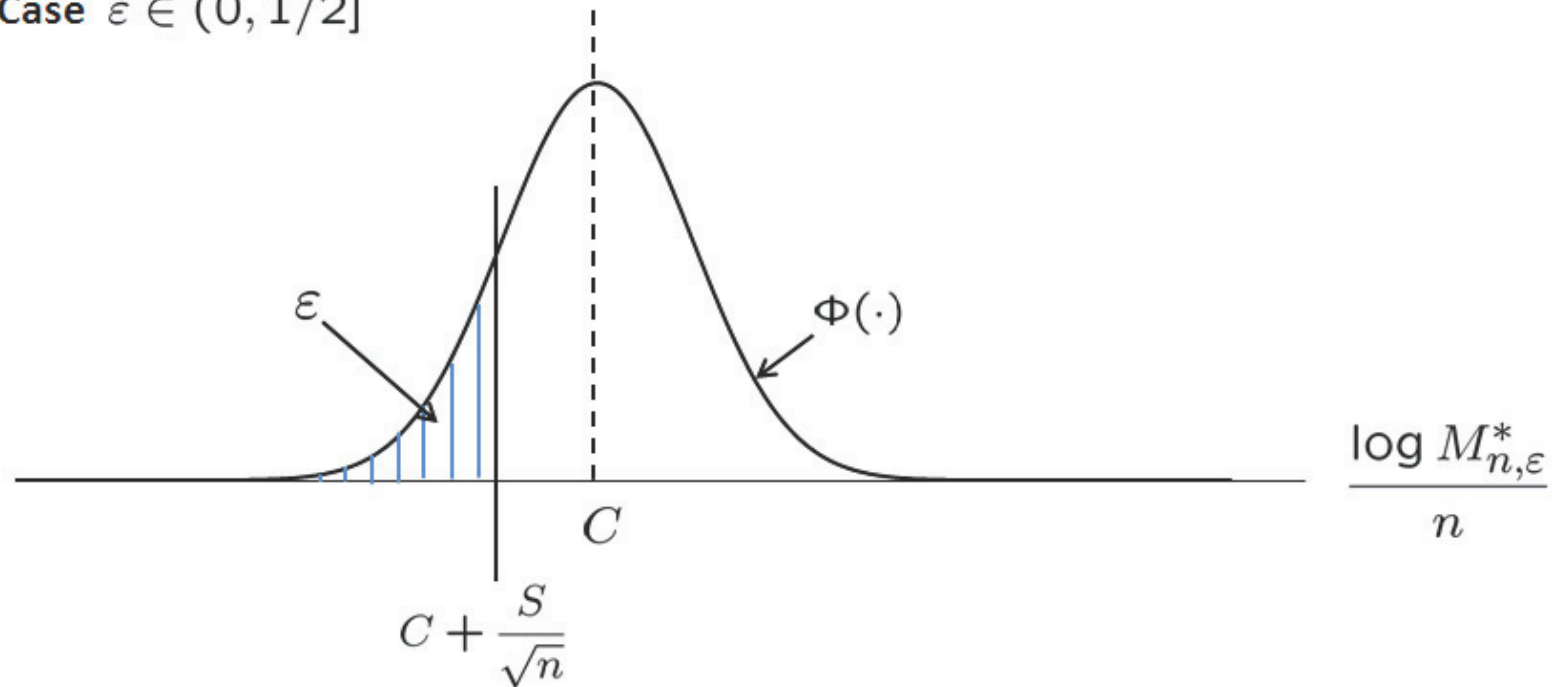
$$V_\varepsilon = \mathbb{V}_{P_X W} \left\{ \log \frac{W(Y|X)}{P_Y(Y)} \right\} \quad \text{with } P_X : I(X; Y) = C$$

- ▶  $G(\cdot)$  は標準正規分布  $\mathcal{N}(0, 1)$  の CDF
- ▶ 中心極限定理 (Berry-Esséen 定理) による解析



# 2次符号化定理のイメージ

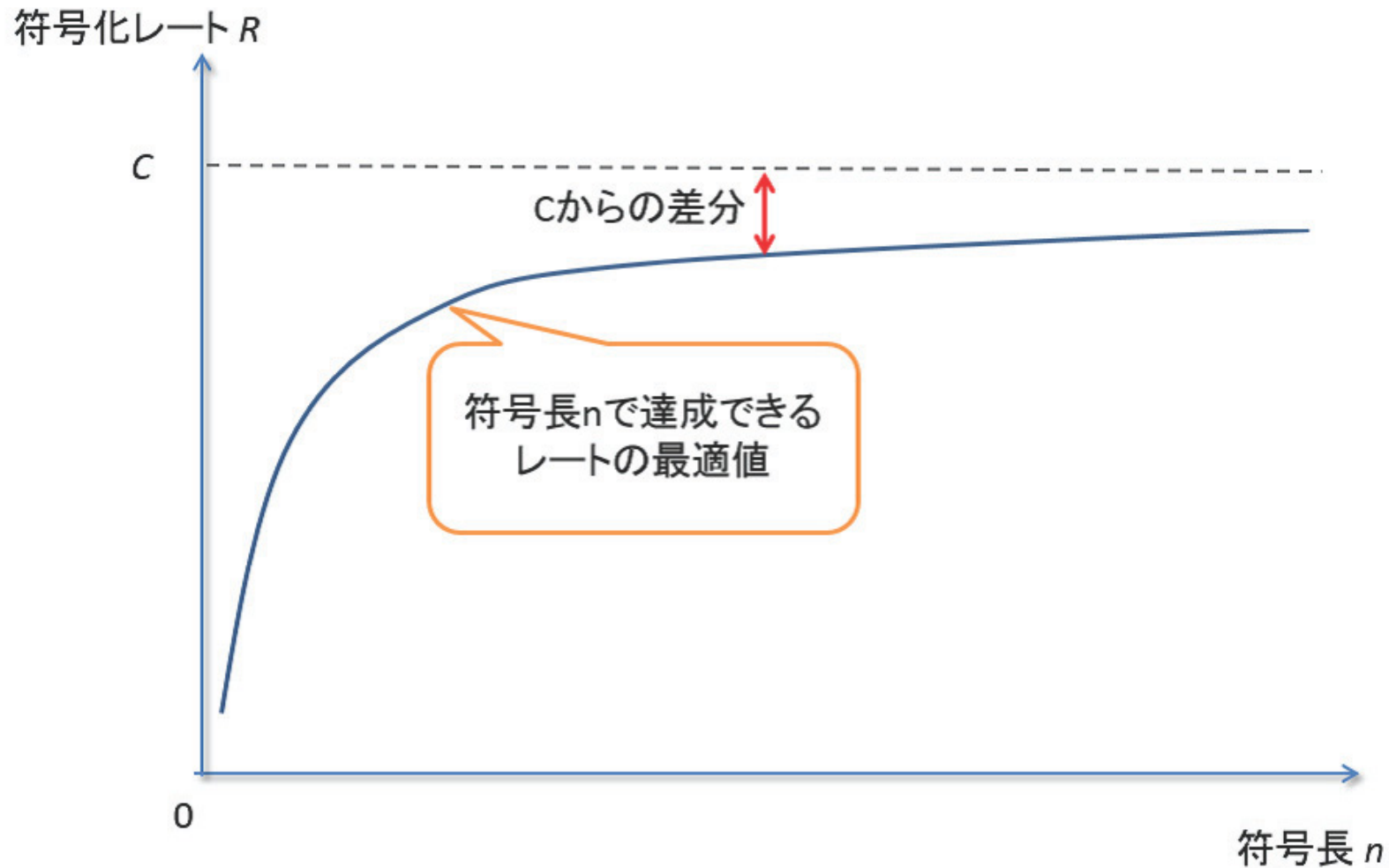
Case  $\varepsilon \in (0, 1/2]$



$\varepsilon \in (0, 1/2)$  の場合の最適符号化レート. 達成可能な2次符号化レートは**負**になる. (分散  $V_\varepsilon$  は小さくなる方向)

$\varepsilon \in [1/2, 1)$  の場合は, 達成可能な2次符号化レートは**非負**になる. (分散  $V_\varepsilon$  は大きくなる方向)

# DMCにおける最大符号化レート of 振舞



最適レートの  $C$  からの差分は  $\frac{1}{\sqrt{n}} V_{\varepsilon} G^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right)$

# DMCにおける2次符号化定理の精密化

## 2次符号化定理 (PPV'10), (Tomamichel & Tan'14)

$$V_\varepsilon = \mathbb{V}_{P_X W} \left\{ \log \frac{W(Y|X)}{P_Y(Y)} \right\} > 0 \quad \text{with } P_X : I(X; Y) = C$$

となる DMC  $W$  に対して,

$$\log M_{n,\varepsilon}^* \leq nC + \sqrt{nV_\varepsilon} G^{-1}(\varepsilon) + \frac{1}{2} \log n + O(1)$$

ここで,  $G(\cdot)$  は標準正規分布  $\mathcal{N}(0, 1)$  の CDF

- 平均誤り率に対する  $M_{n,\varepsilon}^*$  を直接評価する
- reverse dispersion  $\text{Var}[i(X; Y)|Y]$  が正の通信路に対しては, 達成可能性も示されている (Polyanskiy'10)

# AWGN 通信路における 2 次符号化定理

AWGN 通信路 :

$$Y_i = X_i + Z_i \quad Z_i \sim \mathcal{N}(0, N)$$

## 2 次符号化定理 (Hayashi'09), (PPV'10)

平均電力制約  $P$

$$\sum_{i=1}^n x_i^2 \leq nP$$

のある AWGN 通信路において,

$$\log M_{n,\varepsilon}^* = nC + \sqrt{nV_\varepsilon} G^{-1}(\varepsilon) + O(\log n)$$

ここで,  $G(\cdot)$  は標準正規分布  $\mathcal{N}(0, 1)$  の CDF

# 2次符号化定理の関連研究

- 一般通信路に対する最適2次符号化レートの一般公式 (Hayashi'09)
- DMCに対するFeedback (PPV'11), 消失あり復号, リスト復号 (Tan&Moulin'14)
- Gilbert-Elliott 通信路 (PPV'11), 加法的型マルコフ通信路 (Hayashi&Watanabe'13)
- Fading 通信路, 複合 DMC (Polyanskiy'13), Well-Ordered 混合 DMC (Y.&Nomura'14) 等
- マルチユーザ通信路で最適2次符号化レートが決定している例はほとんど見られない。

# 狭義の有限長解析

(2次符号化定理の導出に向けて)

# アプローチ

- 順定理（達成可能性）：

任意の確率分布  $P_X$  について，誤り率の上界 ( $g_u(\cdot)$ )

$$\varepsilon_n \leq g_u(n, M_n | P_X)$$

を満たす  $(n, M_n, \varepsilon_n)$  符号が存在することを示す。

$$\implies M_{n,\varepsilon}^* \geq \sup_{P_X} \max \{ M_n \mid g_u(n, M_n | P_X) \leq \varepsilon \}$$

- 逆定理：

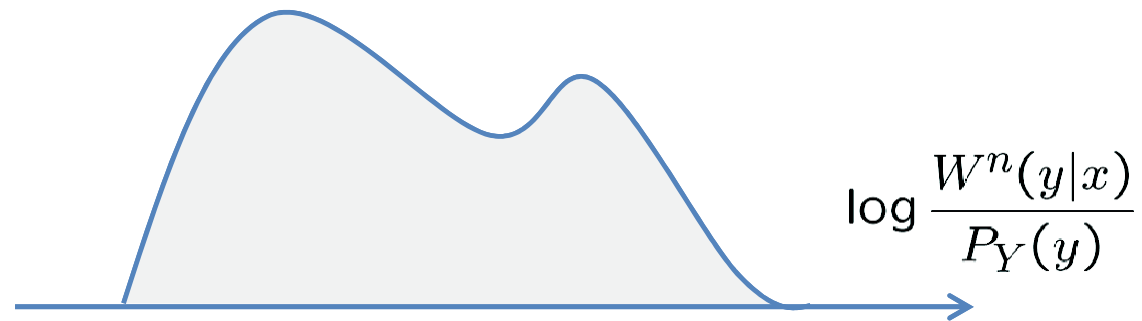
任意の  $(n, M_n, \varepsilon_n)$  符号が満たす誤り率の下界 ( $g_l(\cdot)$ )

$$\varepsilon_n \geq g_l(n, M_n | P_X).$$

を示す。ただし， $P_X$  は符号語の確率分布を表わす。

$$\implies M_{n,\varepsilon}^* \leq \sup_{P_X} \max \{ M_n \mid g_l(n, M_n | P_X) \leq \varepsilon \}$$

# 情報スペクトルの視点



- 情報スペクトル的手法 (Verdú-Han'94, Han'03)
- 尤度比  $\log \frac{W^n(y|x)}{P_Y(y)}$  の分布関数に注目

$$\Pr \left\{ \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log \gamma \right\}$$

- $n \rightarrow \infty$  では,  $\epsilon$ -通信路容量を特徴付ける



# 上界式とベイズ的仮説検定

主に, (Hayashi & Nagaoka'03), (PPV'10)

# しきい値復号スキーム

- 復号領域 :  $\gamma > 0$  に対し,

$$\mathcal{L}(\gamma) = \left\{ (x, y) \in \mathcal{X}^n \times \mathcal{Y}^n \mid \log \frac{W^n(y|x)}{P_Y(y)} > \log \gamma \right\}$$

$(x, y) \in \mathcal{L}$  を満たす  $x$  が一意に定まれば,  $x$  を送信したと推定

- 送信  $X \in \mathcal{X}^n$  に対する復号誤り事象
  - ▶  $\mathcal{E}_1 = \{(X, Y) \notin \mathcal{L}(\gamma)\}$
  - ▶  $\mathcal{E}_2 = \{(\bar{X}, Y) \in \mathcal{L}(\gamma)\}$  ( $\bar{X}$  は他の符号語)

# Feinstein 上界式 [Feinstein'54]

- 任意の  $P_X$  に対し, 次式を満たす  $(n, M_n, \varepsilon_n)$  符号が存在する.

$$\begin{aligned}\varepsilon_n &\leq P_{XY}(\mathcal{L}(\gamma)^c) + M_n/\gamma \\ &= \Pr \left\{ \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log \gamma \right\} + M_n/\gamma \quad \text{Feinstein 上界式}\end{aligned}$$

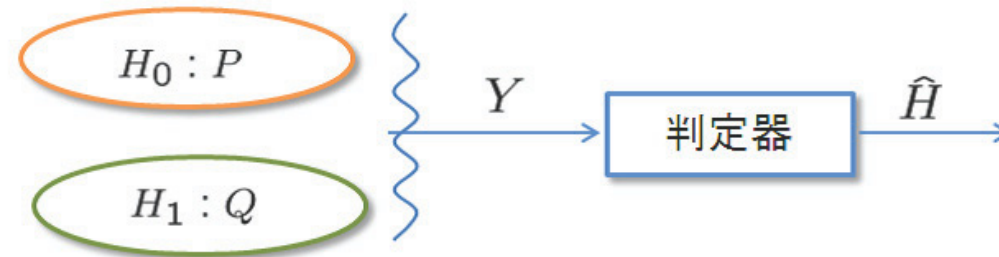
- 別表現 (任意の  $\eta > 0$  に対して  $\gamma := M_n e^{n\eta}$ )

$$\varepsilon_n \leq \Pr \left\{ \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log M_n + n\eta \right\} + e^{-n\eta}$$

- 最適化 :

$$\varepsilon_n \leq \inf_{\gamma > 0} \left\{ \Pr \left\{ \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log \gamma \right\} + M_n/\gamma \right\}$$

# 仮説検定



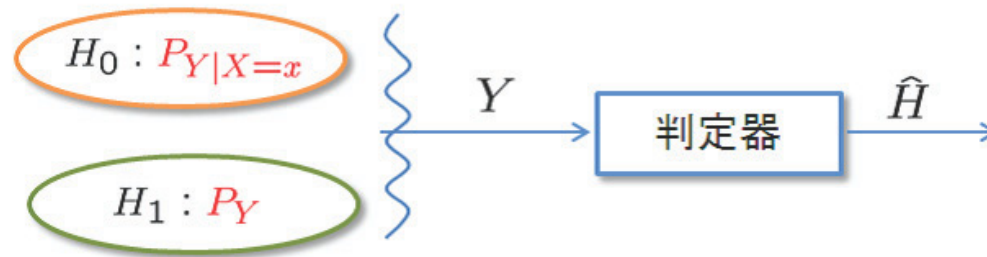
- $Y$  を観測して，仮説  $H_0$  と  $H_1$  のどちらが正しいか判定する

$$H_0: Y \sim P \quad \text{vs.} \quad H_1: Y \sim Q$$

- 誤り率を最小にするのは**尤度比検定**

$$\hat{H} = \begin{cases} H_0 & \text{if } \frac{P(y)}{Q(y)} > \gamma \\ H_1 & \text{otherwise} \end{cases}$$

# 独立性の検定問題



- $Y$  を観測して、仮説  $H_0$  と  $H_1$  のどちらが正しいか判定する

$$H_0: Y \sim P_{Y|X=x} \quad \text{vs.} \quad H_1: Y \sim P_Y$$

- 誤り率を最小にするのは尤度比検定

$$\hat{H} = \begin{cases} H_0 & \text{if } \frac{P_{Y|X}(y|x)}{P_Y(y)} > \gamma \\ H_1 & \text{otherwise} \end{cases}$$

- しきい値復号は、 $Y$  を『 $H_0$  と判定する  $X$  に復号する』動作と見える

⇒ 仮説検定の手法から上界式・下界式をより厳密にできる

# Dependence Testing (DT) 上界式

定理： DT 上界式 (Hayashi & Nagaoka'03), (PPV '10)

任意の  $P_X$  に対し，次式を満たす  $(n, M_n, \varepsilon_n)$  符号が存在する。

$$\varepsilon_n \leq P_{XY}(\mathcal{L}(\gamma)^c) + \frac{M_n - 1}{2} P_{\bar{X}Y}(\mathcal{L}(\gamma)) \quad \text{DT 上界式}$$

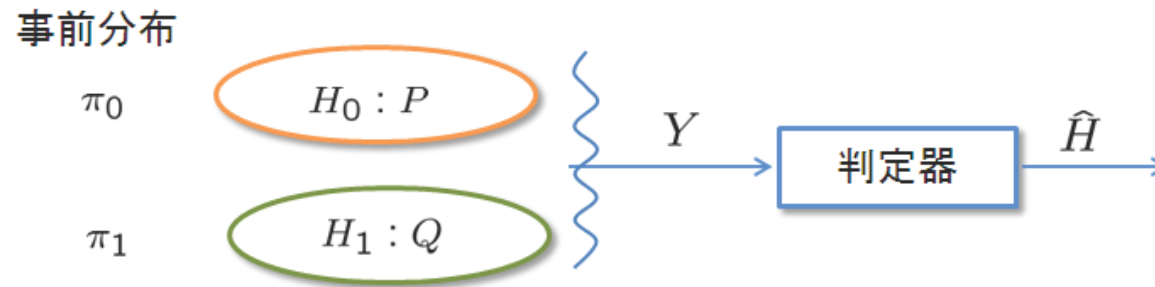
$\bar{X}$  は送信していない符号語に対応 ( $\bar{X} \perp Y$ )

- 証明のスケッチ：  $C = \{\mathbf{x}_1, \dots, \mathbf{x}_{M_n}\}$  を用い，メッセージを小さい順にしきい値判定するとき，誤り率は

$$\begin{aligned} P_e &= \frac{1}{M_n} \sum_m \sum_y W^n(y|\mathbf{x}_m) \mathbf{1} \left\{ (\mathbf{x}_m, y) \notin \mathcal{L}(\gamma) \text{ or } \bigcup_{m' < m} \{(\mathbf{x}_{m'}, y) \in \mathcal{L}(\gamma)\} \right\} \\ &\leq \frac{1}{M_n} \sum_m \sum_y W^n(y|\mathbf{x}_m) \left( \mathbf{1}\{(\mathbf{x}_m, y) \notin \mathcal{L}(\gamma)\} + \sum_{m' < m} \mathbf{1}\{(\mathbf{x}_{m'}, y) \in \mathcal{L}(\gamma)\} \right) \end{aligned}$$

以降，  $P_X$  によるペア毎に独立なランダム符号化を用いる

# ベイズ的仮説検定問題



- 仮説の**事前確率**  $\pi_0, \pi_1 = 1 - \pi_0$  が分かる場合：

$$H_0: Y \sim P(Y) \text{ w.p. } \pi_0 \quad \text{vs.} \quad H_1: Y \sim Q(Y) \text{ w.p. } \pi_1$$

のしきい値  $\gamma > 0$  による誤り率

$$P_e(\gamma) = \pi_0 P \left( \log \frac{P(Y)}{Q(Y)} \leq \log \gamma \right) + \pi_1 Q \left( \log \frac{P(Y)}{Q(Y)} > \log \gamma \right)$$

- 誤り率を最小化する最適しきい値  $\gamma^* = \pi_1 / \pi_0$

# しきい値 $\gamma$ の最適化

- DT 上界式

$$\begin{aligned} P_e^{(n)} &\leq P_{XY} (\mathcal{L}(\gamma)^c) + \frac{M_n-1}{2} P_{\bar{X}Y} (\mathcal{L}(\gamma)) \\ &= \frac{M_n+1}{2} \cdot \left\{ \frac{2}{M_n+1} \cdot P_{XY} \left( \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log \gamma \right) \right. \\ &\quad \left. + \frac{M_n-1}{M_n+1} \cdot P_{\bar{X}Y} \left( \log \frac{W^n(Y|\bar{X})}{P_Y(Y)} > \log \gamma \right) \right\} \end{aligned}$$

ベイズ的検定  $\{P_{XY}$  w.p.  $\frac{2}{M_n+1}$  vs.  $P_{\bar{X}Y}$  w.p.  $\frac{M_n-1}{M_n+1}\}$  の誤り率

- 誤り率を最小化するしきい値  $\gamma^* = \frac{\pi_1}{\pi_0} = \frac{M_n-1}{2}$

c.f. Feinstein 上界式の最適化 :

$$P_e \leq \inf_{\eta>0} \left\{ \Pr \left( \log \frac{W^n(Y|X)}{P_Y(Y)} \leq \log M_n + n\eta \right) + e^{-n\eta} \right\}$$



# Feinstein 上界式との比較

$\gamma > 0$  を固定すると, 第2項同士の比較

$$\begin{aligned} \text{(DT 上界)} \quad \frac{M_n - 1}{2} P_{\bar{X}Y} \left( \log \frac{W^n(Y|\bar{X})}{P_Y(Y)} > \log \gamma \right) \\ &= M_n P_{\bar{X}Y} \left( \frac{P_{XY}(\bar{X}, Y)}{P_{\bar{X}Y}(\bar{X}, Y)} > \gamma \right) \\ &\leq M_n / \gamma \cdot P_{XY} \left( \frac{P_{XY}(X, Y)}{P_{\bar{X}Y}(X, Y)} > \gamma \right) \\ &\leq M_n / \gamma \quad \text{(Feinstein 上界)} \end{aligned}$$

すなわち

DT 上界式  $\leq$  Feinstein 上界式

DT 上界式では, 最適なしきい値が容易に求まる.  
高次符号化レートの詳細な解析にも用いられる.

# DT 上界式の他の符号化問題への拡張

- 情報源・通信路結合符号化 (Tauste Campo et al.'11)
- 相関のある複数の情報源の通信路結合符号化 (Yagi'12)
- 多重アクセス通信路 (MolavianJazi & Laneman'12), (八木, 大濱'12)

# 下界式と Neyman-Pearson 仮説検定

主に (Nagaoka'01), (Hayashi'06) ,(PPV'10),  
& (Vazquez-Vilar et al.'13)

# Neyman-Pearson 定式化

- 仮説検定

$$H_0: Y \sim P(Y) \quad \text{vs.} \quad H_1: Y \sim Q(Y)$$

- 確率  $P_{T|Y} : \mathcal{Y} \rightarrow \{0, 1\}$  を用いて, 確率  $P_{T|Y}(1|y)$  で  $P$  が正しいと判定する

- 2 種類の誤り事象:

- 第 1 種の誤り率

$$P(T = 0) = \sum_y P(y) P_{T|Y}(0|y)$$

- 第 2 種の誤り率

$$Q(T = 1) = \sum_y Q(y) P_{T|Y}(1|y)$$

# Neyman-Pearson 定式化 (2)

- 第1種の誤り率が  $\alpha$  以下になる判定則の集合：

$$\mathcal{P}_\alpha(P) := \left\{ P_{T|Y} \mid \underbrace{\sum_y P(y) P_{T|Y}(0|y)}_{=P(T=0)} \leq \alpha \right\}$$

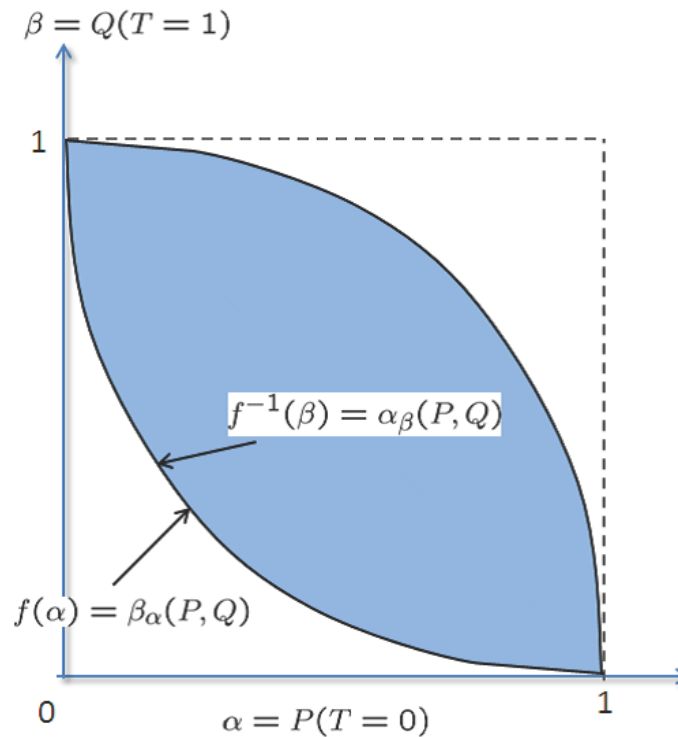
- 第1種の誤り率を  $\alpha$  以下にするもとの、最小の第2種誤り率

$$\beta_\alpha(P, Q) := \min_{P_{T|Y} \in \mathcal{P}_\alpha(P)} \underbrace{\sum_y Q(y) P_{T|Y}(1|y)}_{=Q(T=1)}$$

- 次数零の smooth Rényi ダイバージェンス (Wang et al.'09)：

$$D_0^\alpha(P||Q) := -\log \beta_\alpha(P, Q)$$

# $(\alpha, \beta)$ 領域



達成できる  $\alpha = P(T = 0)$ ,  $\beta = Q(T = 1)$  の領域

- $(\frac{1}{2}, \frac{1}{2})$  に関して対称な凸領域になる
- 下の境界が  $\beta_\alpha(P, Q)$  に対応する
- 逆関数は  $\alpha_\beta(P, Q)$  と表わされる

# Meta Converse 下界式 (レートの上界式)

定理 : meta converse 下界式 (Nagaoka'01), (Hayashi'06), (PPV'10)

誤り率  $P_e^{(n)} = \varepsilon$  を達成する符号は,  $\mathcal{Y}^n$  上の任意の確率測度  $Q_Y$  に対して次式を満たす.

$$\frac{1}{M_n} \geq \beta_\varepsilon(P_{XY}, P_X Q_Y) \quad \text{MC 下界式}$$

$$\varepsilon \geq \alpha_{\frac{1}{M_n}}(P_{XY}, P_X Q_Y) \quad \text{共役形}$$

ただし,  $P_X$  は符号上の一様分布.

- meta converse 下界式は, (PPV'10) において初めて導出されたと広く認識されているが, (Hayashi'06) に同様の限界式が記されている.

# Meta Converse 下界式と従来の下界式の関係

$\beta_\varepsilon(P_{XY}, Q_{XY})$  の上界式と  $Q_{Y|X}$  のおき方を工夫すれば,

meta converse 下界式  $\succeq$   $\left\{ \begin{array}{ll} \text{Hayashi-Nagaoka 下界式} & [\text{Hayashi \& Nagaoka'03}] \\ \text{Verdú-Han 下界式} & [\text{Verdú \& Han'94}] \\ \text{Poor-Verdú 下界式} & [\text{Poor \& Verdú'95}] \end{array} \right.$

が示せる



# Meta Converse 下界式のタイト性

- meta converse 下界式の**共役形**

$$\varepsilon \geq \max_{Q_Y} \alpha_{\frac{1}{M_n}}(P_{XY}, P_X Q_Y)$$

- 現在まで知られている（ほぼ）全ての下界式が meta converse 下界式から導出される  
Arimoto の指数, sphere-packing 指数, etc.

**定理 4: meta converse 下界式のタイト性 (Vazquez-Vilar et al.'13)**

与えられた  $(n, M_n)$  符号の **MAP 復号性能と一致する**

$$\varepsilon_n^{\text{MAP}} = \max_{Q_Y} \alpha_{\frac{1}{M_n}}(P_{XY}, P_X Q_Y)$$

# Meta Converse 式に関連する研究

- Wang らによる真の  $P_Y$  を用いた導出 (Wang et al.'09)
- 複合通信路 (Polyanskiy'13) や記憶のある通信路 (Tomamichel&Tan'13)
- 情報源・通信路結合符号化 (Kostina & Verdú'13), (Vazquez-Vilar et al.'13)
- 多重アクセス通信路 (Huang & Moulin'12), (八木, 大濱'12)
- 干渉通信路 (松田, 植松'13)

# まとめ

- 通信路符号の最適レートの有限長解析
  - ▶ 高次レートの解析 (広義の有限長解析)
  - ▶ 上界式・下界式のギャップを小さくする (狭義の有限長解析)
- 仮説検定問題としきい値復号の関係による one-shot 限界式
  - ▶ DT 上界式 (Bayes 的仮説検定)
  - ▶ meta converse 下界式 (Neyman-Pearson 的仮説検定)
- 多くのマルチユーザ通信路に対しては, 未解決な問題が多い

# 謝辞

本講演のきっかけを頂いた林正人先生，並びに IT 研究専門委員会の皆様に感謝致します。

数値計算のグラフは Yury Polyanskiy 先生にいただきました。

また，有益な情報をくださった大濱靖匡先生，野村亮先生，葛岡成晃先生，松田哲直先生，渡辺峻先生にお礼申し上げます。

# References I

- S. Arimoto, “On the converse to the coding theorem for discrete memoryless channels,” *IEEE Trans. Inf. Theory*, vol. IT-19, no. 3, pp. 357–359, May 1973.
- A. Feinstein, “A new basic theorem of information theory,” *IRE Trans. Inf. Theory*, vol. 4, no. 4, pp. 2–22, Sep. 1954.
- G. D. Forney, “Exponential error bounds for erasure, list, and decision feedback schemes,” *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 206–220, Mar. 1968.
- R. G. Gallager, “A simple derivation of the coding theorem and some applications,” *IEEE Trans. Inf. Theory*, vol. 11, no. 1, pp. 3–18, Jan. 1965.
- T. S. Han, “An information-spectrum approach to capacity theorems for the general multiple-access channel,” *IEEE Trans. on Inf. Theory*, vol. 44, no. 7, pp. 2773–2795, Jan. 1998.
- T. S. Han, *Information-Spectrum Methods in Information Theory*, Springer, 2003.
- M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4947–4966, Nov. 2009.
- M. Hayashi, *Quantum Information: An Introduction*, Springer, 2006.
- M. Hayashi and H. Nagaoka, “General formulas for capacity of classical-quantum channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1753–1768, Jul. 2003.
- M. Hayashi and S. Watanabe, “A unified approach to non-asymptotic and asymptotic analyses of information processing on Markov chains,” preprint available at *arXiv:1309.7528*, Sep. 2013.
- 林 正人, “量子情報理論入門,” SGC ライブラリ 32, サイエンス社, 2004.
- 林 正人, “情報スペクトルによる二次オーダーの情報理論 —一次漸近理論を越えて—,” *IEICE Fundamentals Review*, vol. 6, no. 1, pp. 12–25, July 2012.
- Y.-W. Huang and P. Moulin, “Finite blocklength coding for multiple access channels,” *Proc. IEEE Int. Symp. on Inf. Theory*, Cambridge, MA, USA, July 2012.

# References II

- V. Kostina and S. Verdú, “Lossy joint source-channel coding in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2545–2575, May 2013.
- V. Kostina and S. Verdú, “Channels with cost constraints: strong converse and dispersion,” *Proc. IEEE Int. Symp. on Inf. Theory*, Istanbul, Turkey, July 2013.
- S.-Q. Le, V. Y. F. Tan, M. Motani, “On the dispersions of the discrete memoryless interference channel,” *Proc. IEEE Int. Symp. on Inf. Theory*, Istanbul, Turkey, July 2013.
- 松田 哲直, 植松 友彦, “Smooth Rényi ダイバージェンスによる干渉通信路符号化問題,” 第 8 回シャノン理論ワークショップ予稿集, 2013.
- E. MolavianJazi and J. N. Laneman, “Discrete memoryless multiple access channel in the finite blocklength regime,” *Proc. IEEE Int. Symp. on Inf. Theory*, Cambridge, MA, USA, July 2012.
- P. Moulin, “A new metaconverse and outer region for finite-blocklength MACs,” *Proc. Inf. Theory and Applications Workshop*, San Diego, CA, USA, 2013.
- H. Nagaoka, “Strong converse theorems in quantum information theory,” *Proc. ERATO Conference on Quantum Information Science (EQIS)*, Jul. 2001 (also available in M. Hayashi Ed., *Asymptotic Theory of Quantum Statistical Inference, Selected Papers*, World Scientific Publishing, 2005).
- J. Neyman and E. S. Pearson, “On the problem of the most efficient tests of statistical hypotheses,” *Phil. Trans. Royal Soc. London A*, vol. 231, pp. 289–337, 1933.
- Y. Polyanskiy, *Channel coding: Non-asymptotic fundamental limits*, Ph.D. thesis, Princeton University, 2010.
- Y. Polyanskiy, “Arimoto channel coding converse and Rényi divergence,” *Proc. 48th Annual Allerton Conf.*, Allerton, IL, USA, 2010.
- Y. Polyanskiy, “Saddle point in the minimax converse for channel coding,” *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2576–2595, May 2013.
- Y. Polyanskiy, “On dispersion of compound DMCs,” *Proc. 51th Annual Allerton Conf.*, Allerton, IL, USA, 2013.

# References III

- Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2358, May 2010.
- Y. Polyanskiy, H. V. Poor, and S. Verdú, “Dispersion of the Gilbert-Elliott channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1829–1848, Apr. 2011.
- H. V. Poor, *An Introduction to Signal Detection and Estimation, 2nd Ed.* New York, NY: Springer-Verlag, 1994.
- H. V. Poor and S. Verdú, “A lower bound on the probability of error in multihypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1992–1994, Nov. 1995.
- J. Scarlett and V. Y. F. Tan, “Second-order asymptotics for the Gaussian MAC with degraded message sets,” preprint available at *arXiv:1310.1197*, Oct. 2013.
- C. E. Shannon, “A mathematical theory of communication,” *Bell System Tech. Journal*, vol. 27, pp. 379–423 and 623–656, Oct. 1948.
- C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, “Lower bounds to error probability for coding on discrete memoryless channels, part i and part ii,” *Inform. Contr.*, vol. 10, pp. 65–103, pt. I, 522–552 pt. II, 1967.
- V. Strassen, “Asymptoticische abschatzungen in Shannons informationstheorie,” *Trans. Thrid Prague Conf. Inf. Theory*, pp. 689–723, Prague, 1962.
- V. Y. F. Tan and O. Kosut, “On the dispersions of three network information theory problems,” *Proc. IEEE Int. Symp. on Inf. Theory*, Cambridge, MA, USA, 2012. Extended version is available at *arXiv:1201.3901*, Jan. 2012.
- A. Tauste Campo, G. Vazquez-Vilar, and A. Guillén. i Fàbregas, “Random-coding joint source-channel bounds,” *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, 2011.
- M. Tomamichel and V. Y. F. Tan, “A tight upper bound for the third-order asymptotics for most discrete memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7041–7051, Nov. 2013.
- M. Tomamichel and V. Y. F. Tan, “ $\epsilon$ -Capacities and second-order coding rates for channels with general state,” preprint available at *arXiv:1305.6789*, May 2013.

# References IV

- S. Verdú and T. S. Han, “A general formula for channel capacity,” *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1147–1157, July 1994.
- G. Vazquez-Vilar, A. Tauste Campo, A. Guillén i Fàbregas, and A. Martinez, “The meta-converse bound is tight,” *Proc. IEEE Int. Symp. on Inf. Theory*, Istanbul, Turkey, July 2013.
- L. Wang, R. Colbeck, and R. Renner, “Simple channel coding bounds,” *Proc. IEEE Int. Symp. on Inf. Theory*, Seoul, South Korea, 2009.
- D. Wang, A. Ingber, and Y. Kochman, “The dispersion of joint source-channel coding,” *Proc. 49th Annual Allerton Conf.*, Allerton, IL, USA, 2011. Extended version is available at *arXiv:1109.6310*, Sep. 2011.
- N. A. Warsi, “One-shot bounds for various information theoretic problems using smooth min and max Rényi divergences,” in *Proc. IEEE Inf. Theory Workshop*, Seville, Spain, 2013.
- S. Watanabe, S. Kuzuoka, and V. Y. F. Tan, “Non-asymptotic and second-order achievability bounds for coding with side information,” *arXiv:1301.6467*, Jan. 2013
- J. Wolfowitz, “The coding of messages subject to chance errors,” *Illinois J. Math.*, vol. 1, pp. 591–606, Dec. 1957.
- H. Yagi, “Finite blocklength bounds for multiple access channels with correlated sources,” *Proc. Int. Symp. on Inf. Theory and its Applications*, Honolulu, HI, USA, 2013.
- 八木 秀樹, 大濱 靖匡, “多重アクセス通信路における有限ブロック長解析と複合仮説検定の関係,” 第 35 回情報理論とその応用シンポジウム予稿集, Dec. 2012.
- H. Yagi and R. Nomura, “Channel dispersion for well-ordered mixed channels decomposed into memoryless channels,” to be presented at *Proc. Int. Symp. on Inf. Theory and Its Applications*, Oct. 2014.
- W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, “Quasi-static SIMO fading channels at finite blocklength,” *Proc. IEEE Int. Symp. on Inf. Theory*, Istanbul, Turkey, July 2013.



# 符号長無限大の極限 $N \rightarrow \infty$ より 少し手前に広がる風景

—低密度パリティ検査符号とポーラ符号の漸近解析—

田中利幸

京都大学大学院情報学研究科

2014 年 9 月 25 日

# 目次

- ① 準備
- ② 低密度パリティ検査符号
  - 基礎的事項
  - 復号誤り率
  - スケーリング則
- ③ ポーラ符号
  - 基礎的事項
  - 復号誤り率の上界
  - スケーリング則
  - 拡張
- ④ まとめ

# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ ポーラ符号
- ④ まとめ

# 通信路パラメータ

通信路パラメータ  $\delta$ : 通信路の品質をあらわすパラメータ



具体例:

- 二元消失通信路 (BEC): 消失確率
- 二元対称通信路 (BSC): 反転確率
- 二元入力ガウス通信路 (BIAWGNC): 雑音の分散

# 符号の性能

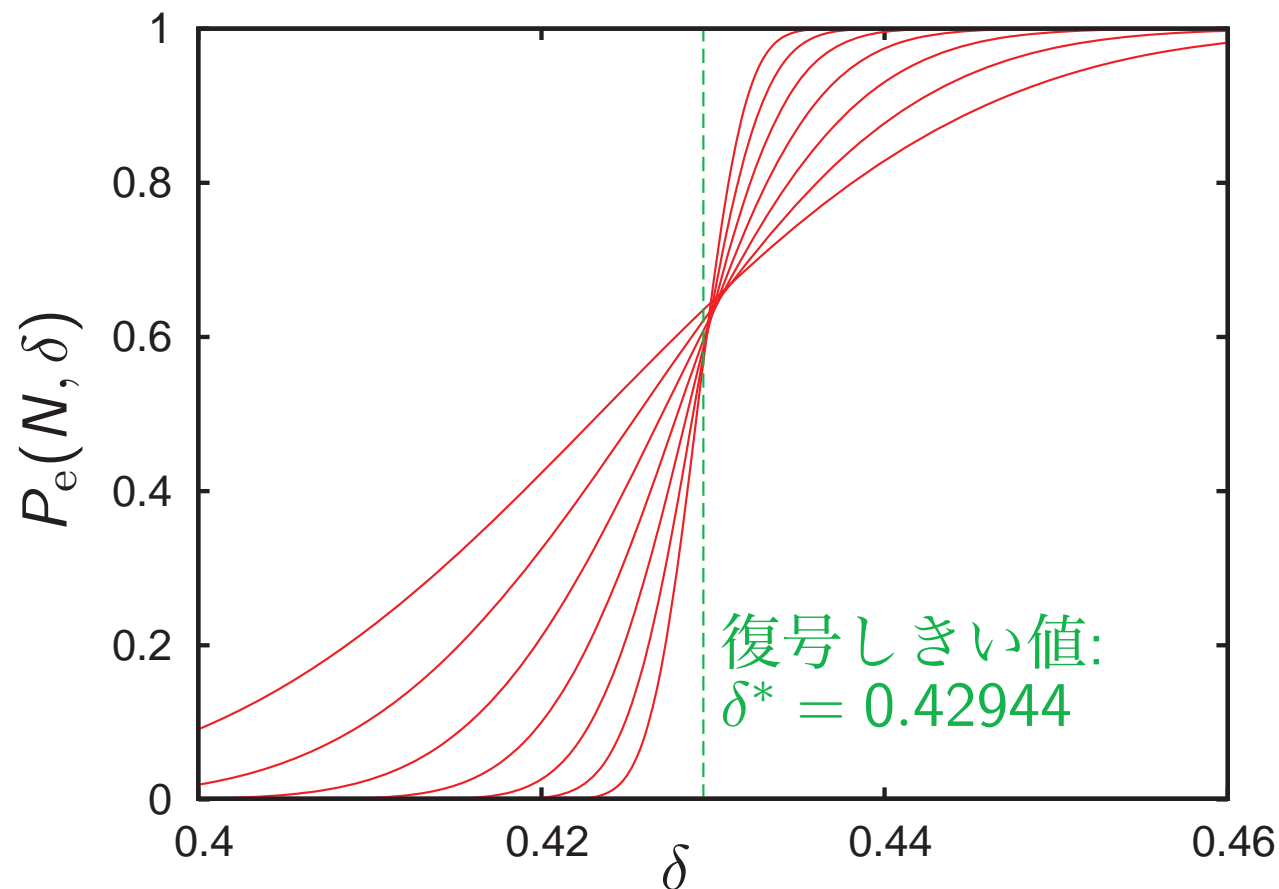
符号化法, 復号法, 符号化率  $R$  を固定.

符号長  $N$ , 通信路パラメータ  $\delta \Rightarrow$  復号誤り率  $P_e(N, \delta)$

通信路パラメータの復号しきい値  $\delta^*$

- $\delta < \delta^*$ :  $\lim_{N \rightarrow \infty} P_e(N, \delta) = 0$
- $\delta > \delta^*$ :  $\lim_{N \rightarrow \infty} P_e(N, \delta) > 0$

# 符号の性能



二元消失通信路における (6, 3)-正則 LDPC 符号, 確率伝搬復号法の性能. 符号長は  $N = 2^n$ ,  $n = 10, 11, \dots, 16$ .

# 通信路符号化定理

## 定理

最適な符号化法，復号法の組に対して， $R < C(\delta)$  であれば

$$\lim_{N \rightarrow \infty} P_e(N, \delta) = 0$$

が成り立つ。

- 存在定理: ランダム符号の平均復号誤り率にもとづく議論。
- 「ほとんどの符号はよい符号。ただし我々が知っている符号は除く。」

*There are few known constructive codes that are good, fewer still that are practical, and none at all that are both practical and very good. It seems to be widely believed that while almost any random linear code is good, codes with structure that allows practical coding are likely to be bad.*

—MacKay, 1999

# 通信路符号化定理

## 定理

最適な符号化法，復号法の組に対して， $R < C(\delta)$  であれば

$$\lim_{N \rightarrow \infty} P_e(N, \delta) = 0$$

が成り立つ。

- 存在定理: ランダム符号の平均復号誤り率にもとづく議論。
- 「ほとんどの符号はよい符号。ただし我々が知っている符号は除く。」

*There are few known constructive codes that are good, fewer still that are practical, and none at all that are both practical and very good. It seems to be widely believed that while almost any random linear code is good, codes with structure that allows practical coding are likely to be bad.*

—MacKay, 1999



# 通信路符号化定理

## 定理

最適な符号化法，復号法の組に対して， $R < C(\delta)$  であれば

$$\lim_{N \rightarrow \infty} P_e(N, \delta) = 0$$

が成り立つ。

- 存在定理: ランダム符号の平均復号誤り率にもとづく議論。
- 「ほとんどの符号はよい符号。ただし我々が知っている符号は除く。」

*There are few known constructive codes that are good, fewer still that are practical, and none at all that are both practical and very good. It seems to be widely believed that while almost any random linear code is good, codes with structure that allows practical coding are likely to be bad.*

—MacKay, 1999

# 目次

- ① 準備
- ② 低密度パリティ検査符号
  - 基礎的事項
  - 復号誤り率
  - スケーリング則
- ③ ポーラ符号
- ④ まとめ

# 目次

- ① 準備
- ② 低密度パリティ検査符号
  - 基礎的事項
  - 復号誤り率
  - スケーリング則
- ③ ポーラ符号
- ④ まとめ

# LDPC 符号

検査行列が疎である線形符号+確率伝搬法による反復軟判定復号法.

## 歴史

- Gallager の学位論文 (1960)
- ターボ符号 (畳み込み符号の並列接続+確率伝搬法による反復軟判定復号法) (Berrou-Glavieux-Thitimajshima, 1993)
- MacKay-Neal (1996); Sipser-Spielman (expander 符号, 1994); etc.
- 密度発展法 (Luby ら, 2001) による性能解析, EXIT 図 (ten Brink, 1999) による符号の設計, ...

# LDPC 符号

確率伝搬法にもとづく復号.

- 局所的に定義される.
- 性能評価も局所的: ビット誤り率にもとづく検討が多い. ( $\Leftrightarrow$  通信路符号化定理はブロック誤り率. )
- 二元消失通信路の場合には厳密な結果が得られている.
- 一般の無記憶通信路に対する結果は限定的.

# 誤り率

## 復号誤り事象

- ブロック誤り  $B$
- ビット誤り  $b_i, i \in \{1, \dots, N\}$

$$B = \bigcup_{i=1}^N b_i$$

## 復号誤り率

- ブロック誤り率  $P_B := P(B)$
- ビット誤り率  $P_b := (1/N) \sum_{i=1}^N P(b_i)$

$$P_b \leq \max_i P(b_i) \leq P_B = P(B) \leq \sum_{i=1}^N P(b_i) = NP_b$$

$$P_b \leq P_B \leq NP_b$$

$P_b = P_B$  となる例

すべてのビットについて一斉に誤る例.



or



$$\Rightarrow P_b = P_B$$

$P_B = NP_b$  となる例

特定のビットについて常に誤る例.

$$\Rightarrow P_b = 1/N, P_B = 1$$

$$P_b \leq P_B \leq NP_b$$

$P_b = P_B$  となる例

すべてのビットについて一斉に誤る例。



or



$$\Rightarrow P_b = P_B$$

$P_B = NP_b$  となる例

特定のビットについて常に誤る例。

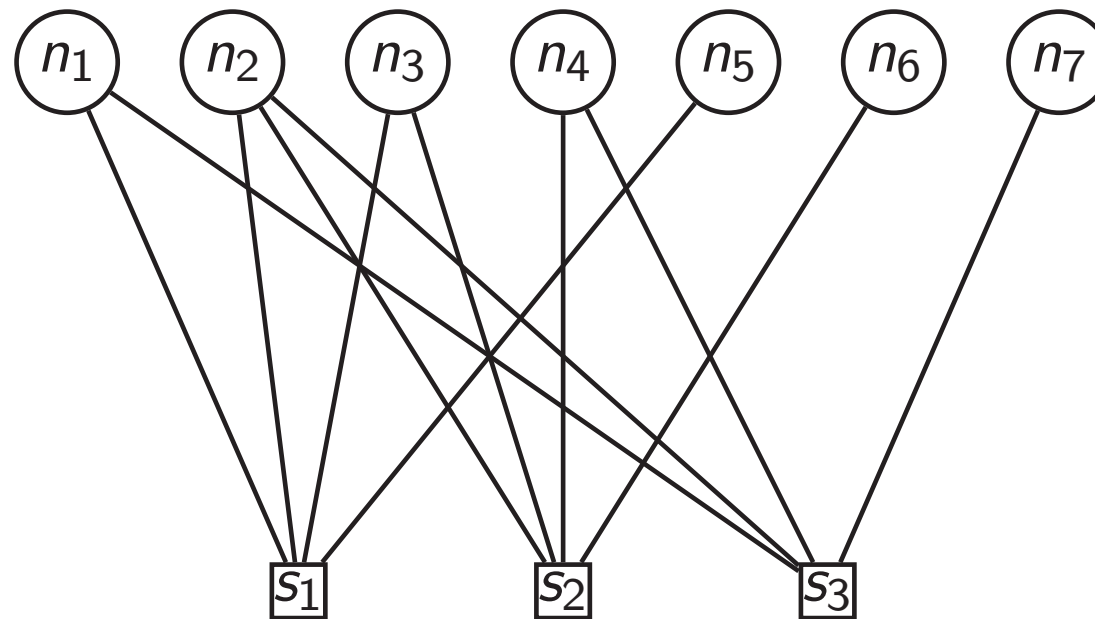
常に誤り



$$\Rightarrow P_b = 1/N, P_B = 1$$

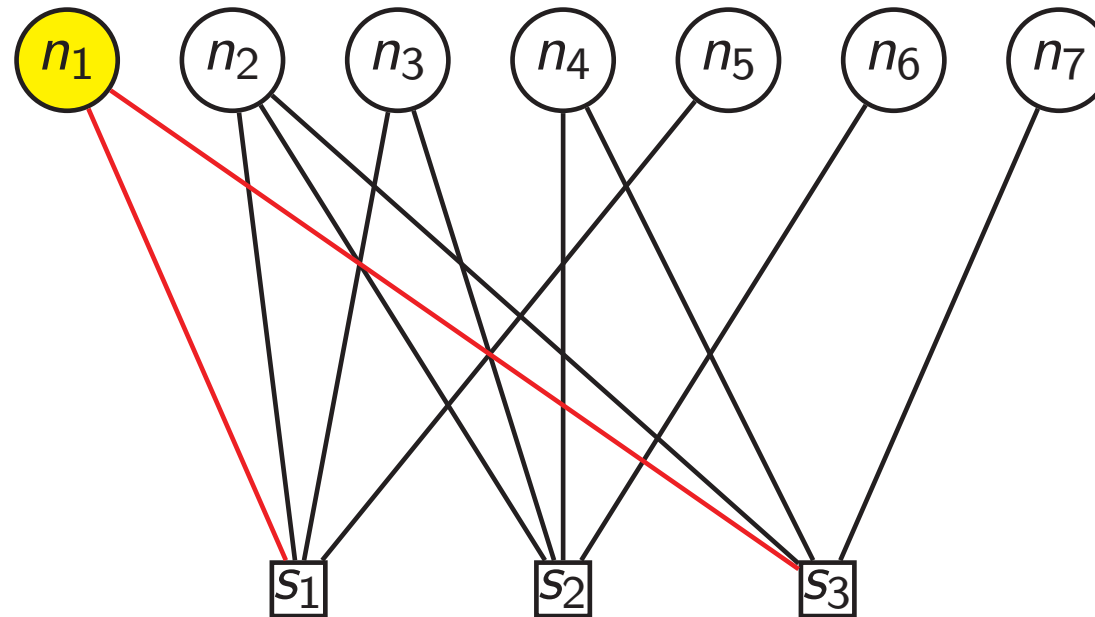


## (7, 4)-ハミング符号の復号グラフ



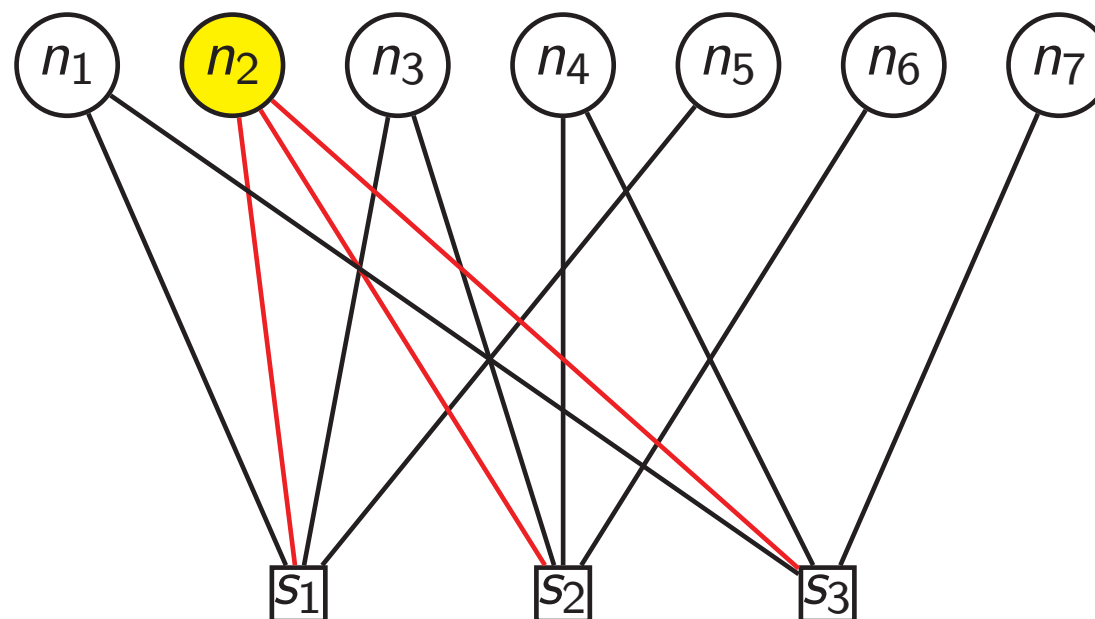
$$s = Hn, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

## (7, 4)-ハミング符号の復号グラフ



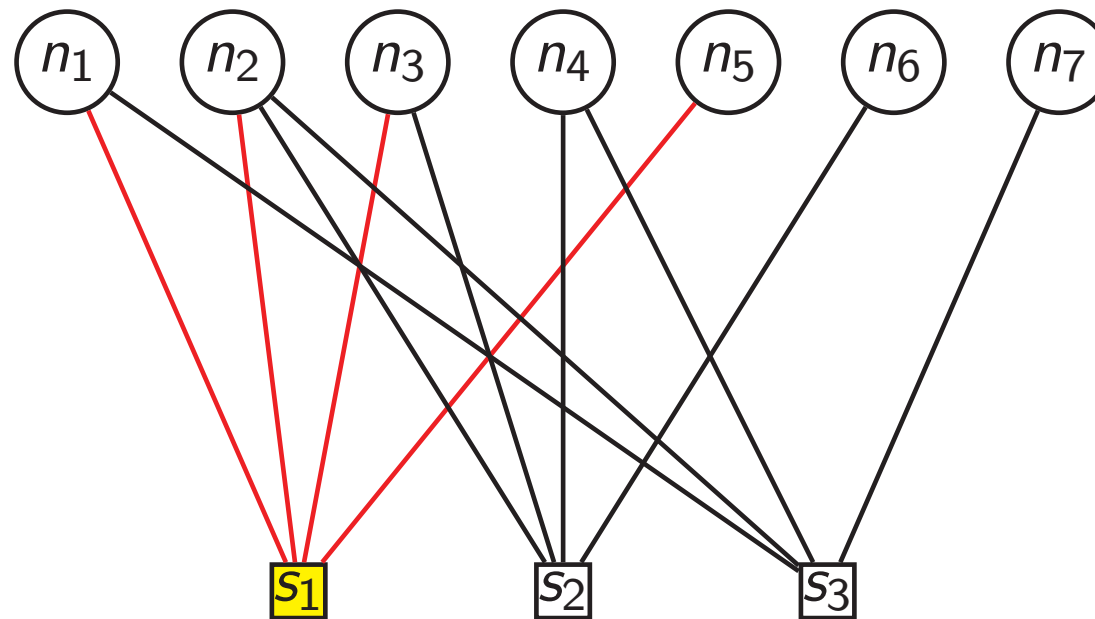
$$\mathbf{s} = \mathbf{H}\mathbf{n}, \quad \mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

## (7, 4)-ハミング符号の復号グラフ



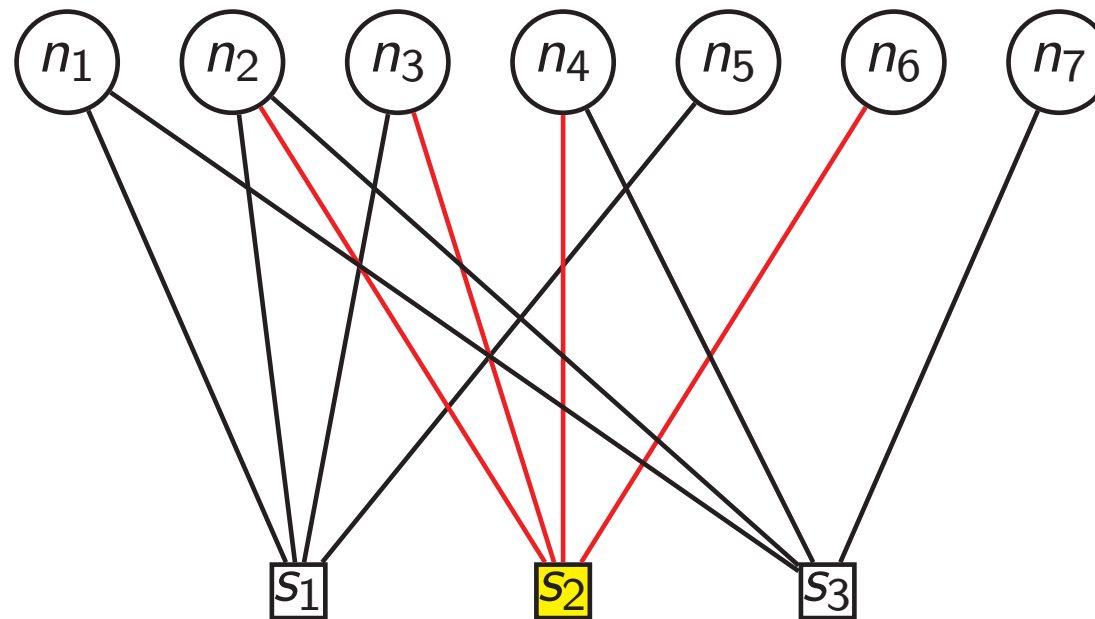
$$s = Hn, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

## (7, 4)-ハミング符号の復号グラフ



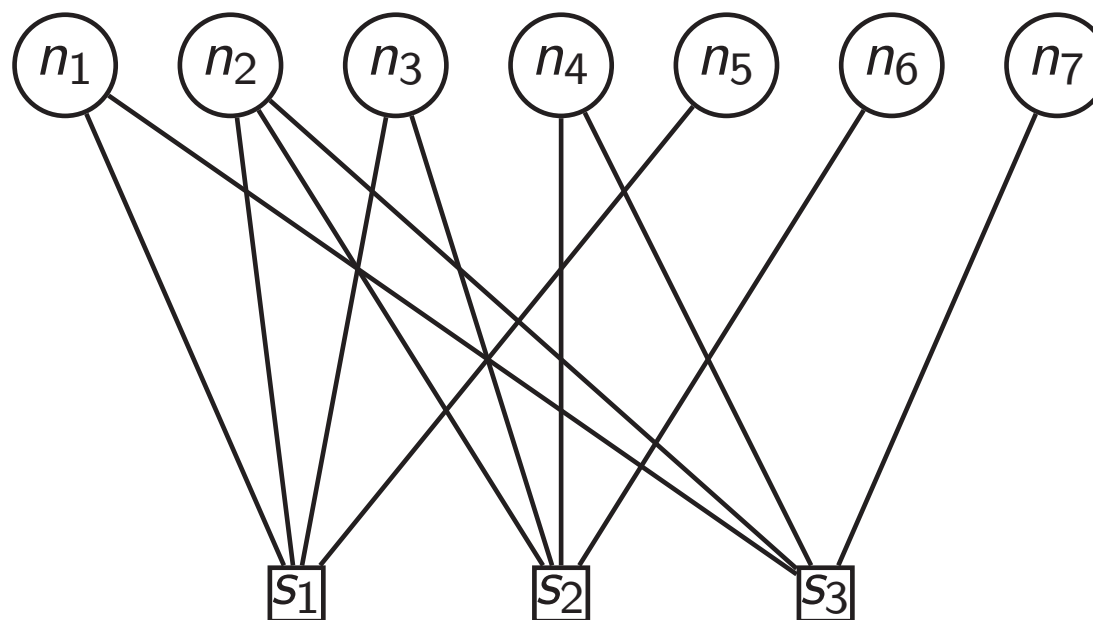
$$s = Hn, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

## (7, 4)-ハミング符号の復号グラフ



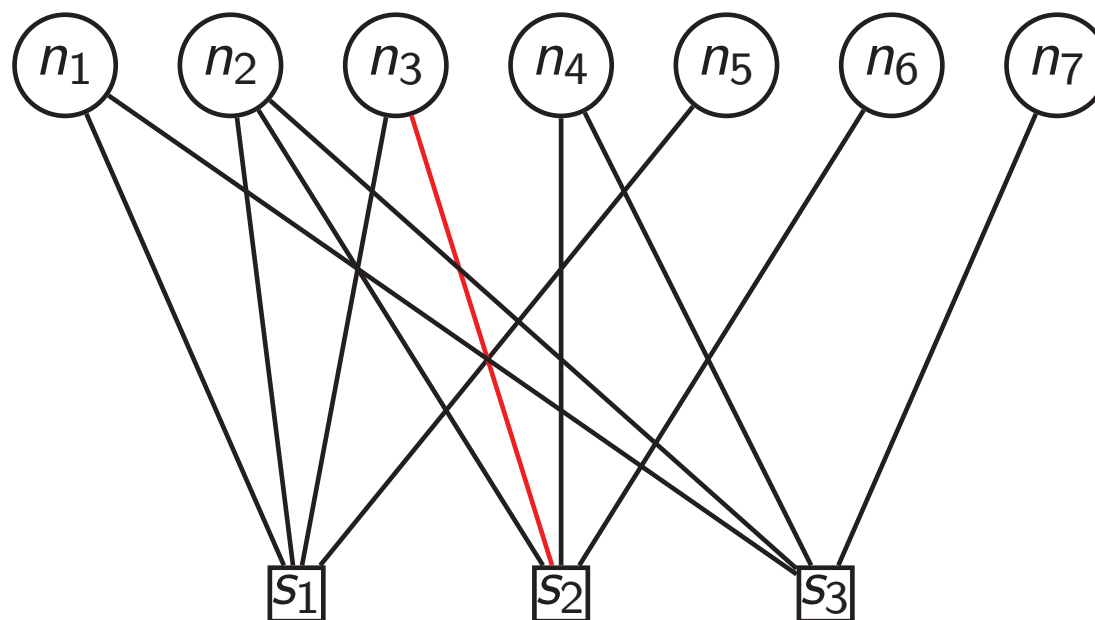
$$s = Hn, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

## 次数



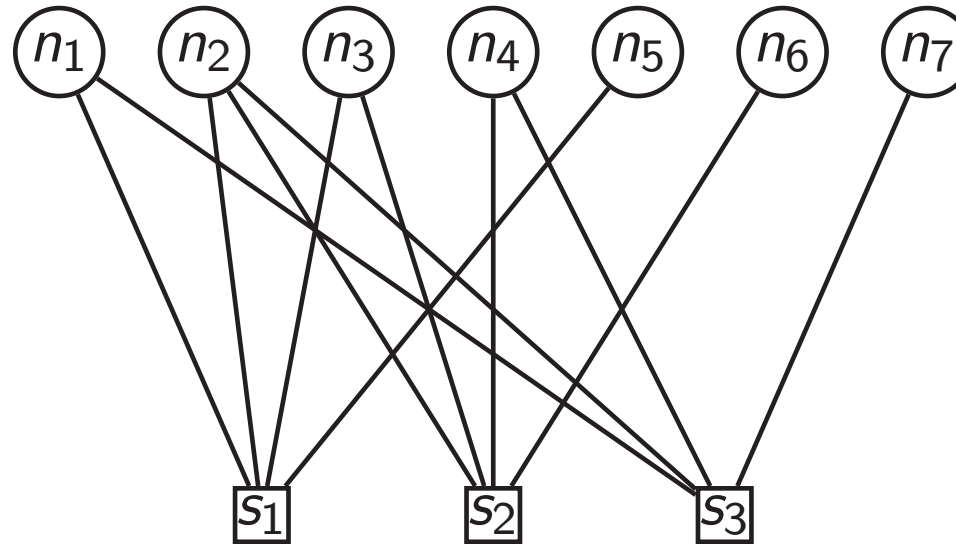
変数ノード次数: 2; チェックノード次数: 4

## 次数



変数ノード次数: 2; チェックノード次数: 4

# 次数多項式



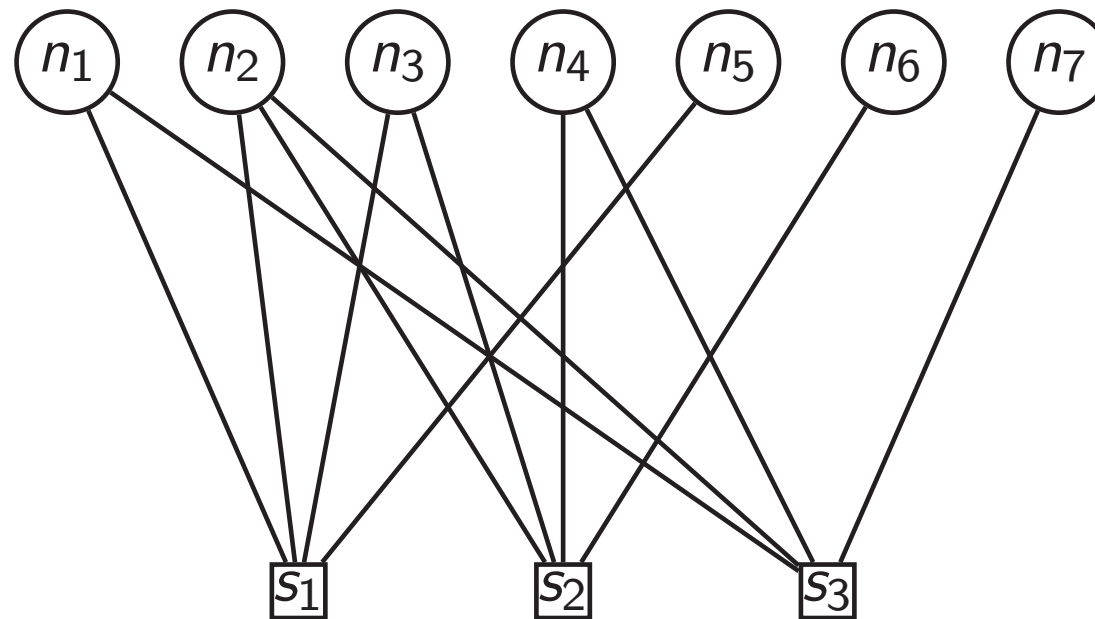
	1	2	3	4
変数ノード次数	3	6	3	0
チェックノード次数	0	0	0	12

次数多項式: 次数分布の母関数

- 辺視点の変数ノード次数多項式:  $\lambda(x) = \frac{1}{12}(3 + 6x + 3x^2)$
- 辺視点のチェックノード次数多項式:  $\rho(x) = \frac{1}{12}(12x^3)$



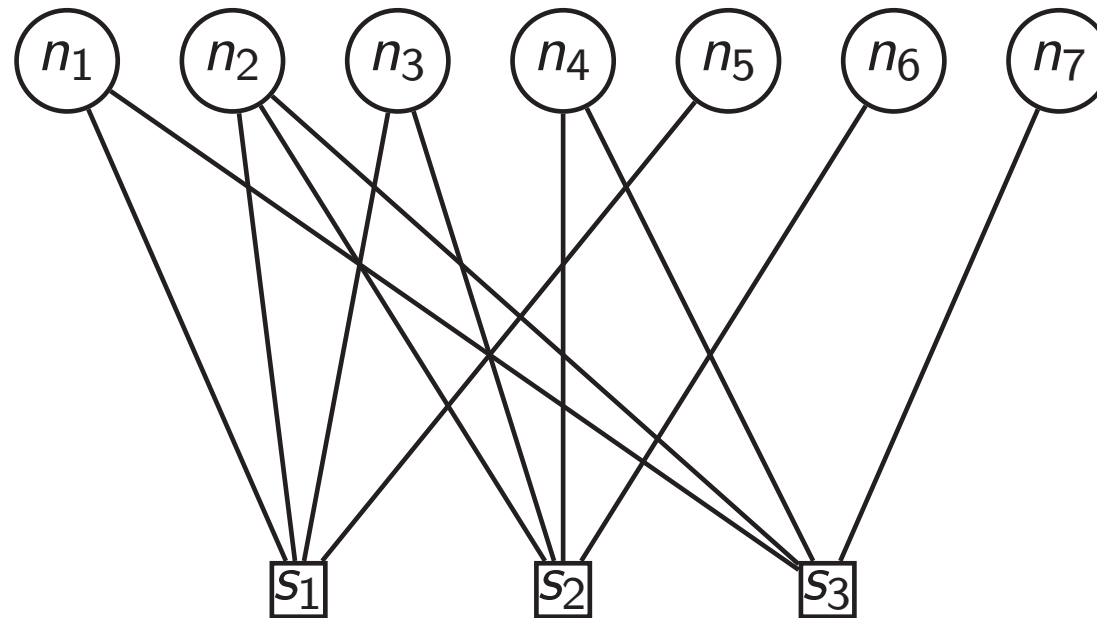
# 次数多項式



## LDPC 符号

検査行列  $H$  が疎行列  $\Rightarrow$  復号グラフが疎 (次数は  $O(N^0)$ ).

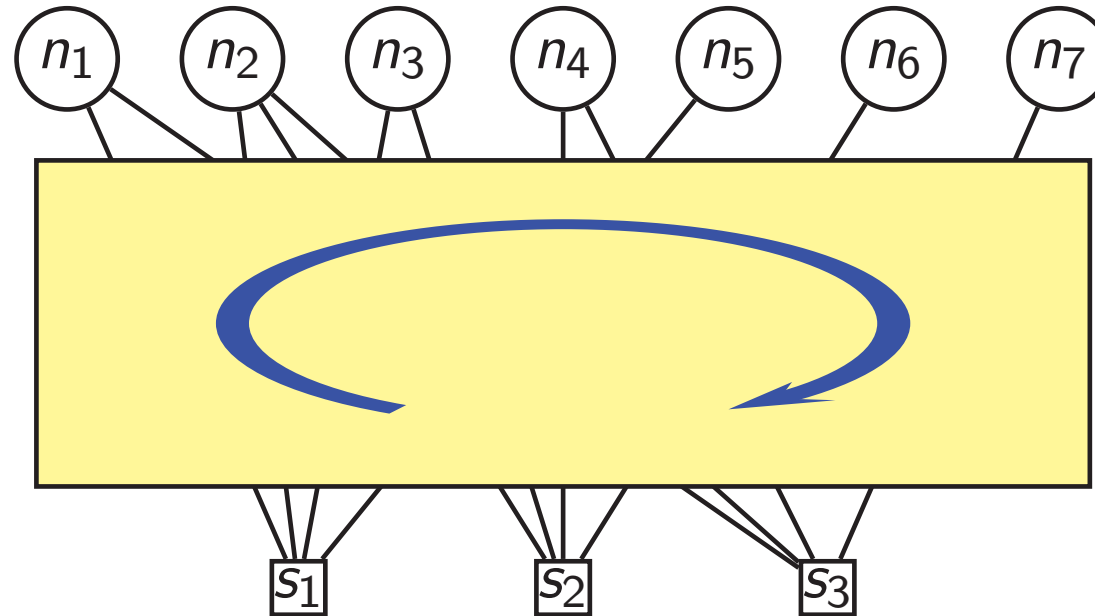
# 符号のランダムアンサンブル



辺のランダムなつながりかえを考えると、次数分布が同一である符号のランダムアンサンブルを定義できる。

- 次数多項式の組  $(\lambda(x), \rho(x))$  によって特徴づけられる。
- ブロック誤り率  $P_e(N, \delta)$  は確率変数。

# 符号のランダムアンサンブル



辺のランダムなつながりかえを考えると、次数分布が同一である符号のランダムアンサンブルを定義できる。

- 次数多項式の組  $(\lambda(x), \rho(x))$  によって特徴づけられる。
- ブロック誤り率  $P_e(N, \delta)$  は確率変数。

# 目次

- ① 準備
- ② 低密度パリティ検査符号
  - 基礎的事項
  - 復号誤り率
  - スケーリング則
- ③ ポーラ符号
- ④ まとめ

# 復号誤り率

二元消失通信路 (BEC) を仮定  $\Rightarrow$  「皮むき」復号による解析が可能, 復号誤り = 残存消失シンボルが停止集合をなす.

- ① ブロック復号誤り率の期待値  $\mathbb{E}[P_e(N, \delta)]$ : 大きい復号誤り率をもつ少数の符号の影響を受ける.

列重みの最小値  $l_{\min}$  が 3 以上であれば,  $\delta < \delta^*$  なら

- $\lim_{N \rightarrow \infty} \mathbb{E}[P_e(N, \delta)] = 0$ .
- $\mathbb{E}[P_e(N, \delta)] = O(N^{1 - \lceil l_{\min}/2 \rceil})$ : 0 への収束は遅い (Orlitzky-Viswanathan-Zhang, 2005).

- ② ランダム符号アンサンブルのなかで典型的な符号は性能がよい (Burshtein-Miller, 2004):  $l_{\min} \geq 3$  の場合, 次数分布や通信路パラメータから計算可能な量  $E \geq 0$  および任意の  $\Delta > 0$  に対して

$$\lim_{N \rightarrow \infty} \Pr \left( -\frac{1}{N} \log P_e(N, \delta) \geq E - \Delta \right) = 1$$

が成り立つ.

# 復号誤り率

二元消失通信路 (BEC) を仮定  $\Rightarrow$  「皮むき」復号による解析が可能, 復号誤り = 残存消失シンボルが停止集合をなす.

- ① ブロック復号誤り率の期待値  $\mathbb{E}[P_e(N, \delta)]$ : 大きい復号誤り率をもつ少数の符号の影響を受ける.  
列重みの最小値  $l_{\min}$  が 3 以上であれば,  $\delta < \delta^*$  なら
  - $\lim_{N \rightarrow \infty} \mathbb{E}[P_e(N, \delta)] = 0$ .
  - $\mathbb{E}[P_e(N, \delta)] = O(N^{1 - \lceil l_{\min}/2 \rceil})$ : 0 への収束は遅い (Orlitzky-Viswanathan-Zhang, 2005).
- ② ランダム符号アンサンブルのなかで典型的な符号は性能がよい (Burshtein-Miller, 2004):  $l_{\min} \geq 3$  の場合, 次数分布や通信路パラメータから計算可能な量  $E \geq 0$  および任意の  $\Delta > 0$  に対して

$$\lim_{N \rightarrow \infty} \Pr \left( -\frac{1}{N} \log P_e(N, \delta) \geq E - \Delta \right) = 1$$

が成り立つ.

# 復号誤り率

二元消失通信路 (BEC) を仮定  $\Rightarrow$  「皮むき」復号による解析が可能, 復号誤り = 残存消失シンボルが停止集合をなす.

- ① ブロック復号誤り率の期待値  $\mathbb{E}[P_e(N, \delta)]$ : 大きい復号誤り率をもつ少数の符号の影響を受ける.  
列重みの最小値  $l_{\min}$  が 3 以上であれば,  $\delta < \delta^*$  なら
  - $\lim_{N \rightarrow \infty} \mathbb{E}[P_e(N, \delta)] = 0$ .
  - $\mathbb{E}[P_e(N, \delta)] = O(N^{1 - \lceil l_{\min}/2 \rceil})$ : 0 への収束は遅い (Orlitzky-Viswanathan-Zhang, 2005).
- ② ランダム符号アンサンブルのなかで典型的な符号は性能がよい (Burshtein-Miller, 2004):  $l_{\min} \geq 3$  の場合, 次数分布や通信路パラメータから計算可能な量  $E \geq 0$  および任意の  $\Delta > 0$  に対して

$$\lim_{N \rightarrow \infty} \Pr \left( -\frac{1}{N} \log P_e(N, \delta) \geq E - \Delta \right) = 1$$

が成り立つ.

# 復号誤り率

二元消失通信路 (BEC) を仮定  $\Rightarrow$  「皮むき」復号による解析が可能, 復号誤り = 残存消失シンボルが停止集合をなす.

- ① ブロック復号誤り率の期待値  $\mathbb{E}[P_e(N, \delta)]$ : 大きい復号誤り率をもつ少数の符号の影響を受ける.  
列重みの最小値  $l_{\min}$  が 3 以上であれば,  $\delta < \delta^*$  なら
  - $\lim_{N \rightarrow \infty} \mathbb{E}[P_e(N, \delta)] = 0$ .
  - $\mathbb{E}[P_e(N, \delta)] = O(N^{1 - \lceil l_{\min}/2 \rceil})$ : 0 への収束は遅い (Orlitzky-Viswanathan-Zhang, 2005).
- ② ランダム符号アンサンブルのなかで典型的な符号は性能がよい (Burshtein-Miller, 2004):  $l_{\min} \geq 3$  の場合, 次数分布や通信路パラメータから計算可能な量  $E \geq 0$  および任意の  $\Delta > 0$  に対して

$$\lim_{N \rightarrow \infty} \Pr \left( -\frac{1}{N} \log P_e(N, \delta) \geq E - \Delta \right) = 1$$

が成り立つ.



# 目次

- ① 準備
- ② 低密度パリティ検査符号
  - 基礎的事項
  - 復号誤り率
  - スケージング則
- ③ ポーラ符号
- ④ まとめ





# スケーリング則

復号しきい値  $\delta = \delta^*$  付近での復号誤り率の漸近的特性: ある定数  $\nu$  およびある非負値関数  $f(z)$  に対して

$$\lim_{N \rightarrow \infty} P_e(N, \delta^* - N^{-1/\nu} z) = f(z)$$

という関係を見出すことが目的.

$\nu$ : スケーリング指数

※ もともとは熱力学, 統計力学において, 相転移の研究に際して導入された概念.

# 簡単な例題: 低密度でないパリティ検査符号

- 検査行列  $H \in \{0, 1\}^{N(1-R) \times N}$ : 各要素を独立に等確率で 0, 1 とする.
- 消失確率  $\delta$  の消失通信路 (BEC), 最尤復号を仮定.  $\delta^* = 1 - R$ .
- $\mathcal{E} \in \{1, \dots, N\}$ : 受信語における消失シンボルの添字集合.

消失シンボルを変数とする検査方程式の係数行列:  $H_{\mathcal{E}}$  ( $\mathcal{E}$  に含まれる添字に対応する列を  $H$  から取り出して構成される行列)

$\Rightarrow$  復号が成功するための必要十分条件は  $\text{rank } H_{\mathcal{E}} = |\mathcal{E}|$ .

$$\Pr(\text{rank } H_{\mathcal{E}} = |\mathcal{E}|) = \begin{cases} 0, & |\mathcal{E}| > N(1-R) \\ \prod_{i=0}^{|\mathcal{E}|-1} (1 - 2^{i-N(1-R)}), & 0 \leq |\mathcal{E}| \leq N(1-R) \end{cases}$$

$$\begin{aligned} \mathbb{E}[P_e(N, \delta)] &= \sum_{|\mathcal{E}|=0}^N \binom{N}{|\mathcal{E}|} \delta^{|\mathcal{E}|} (1 - \delta)^{N-|\mathcal{E}|} [1 - \Pr(\text{rank } H_{\mathcal{E}} = |\mathcal{E}|)] \\ &= Q\left(\frac{\sqrt{N}(\delta^* - \delta)}{\sqrt{\delta^*(1 - \delta^*)}}\right) + O(N^{-1}) \end{aligned}$$

# 簡単な例題: 低密度でないパリティ検査符号

$$\mathbb{E}[P_e(N, \delta)] = Q \left( \frac{\sqrt{N}(\delta^* - \delta)}{\sqrt{\delta^*(1 - \delta^*)}} \right) + O(N^{-1})$$

$$\mathbb{E}[P_e(N, \delta^* - N^{-1/2}z)] = Q \left( \frac{z}{\sqrt{\delta^*(1 - \delta^*)}} \right) + O(N^{-1})$$

スケーリング指数  $\nu = 2$  のスケーリング則に従う。

# LDPC 符号

小さい停止集合をもつ符号を除いた修正 (expurgated) 符号アンサンブルおよび二元消失通信路 (BEC) に対する解析  
(Amraoui-Montanari-Richardson-Urbanke, 2009)

$$\mathbb{E}[P_e(N, \delta^* - N^{-1/2}z)] = Q\left(\frac{z}{\alpha}\right) + o(1)$$

$\alpha$ : 次数多項式  $(\lambda(x), \rho(x))$  から計算できる量.

$(l, r)$ -正則 LDPC 符号 (変数ノード次数がすべて  $l$ , チェックノード次数がすべて  $r$  であるような LDPC 符号のアンサンブル) に対しては

$$\alpha = \delta^* \sqrt{\frac{l-1}{l} \left( \frac{1}{x^*} - \frac{1}{y^*} \right)}$$

$x^*, y^*$ : 以下の密度発展方程式の最大解.

$$x = \delta y^{l-1}$$

$$y = 1 - (1 - x)^{r-1}$$

# LDPC 符号

一般の二元入力無記憶対称通信路に対しても、同様の形

$$\mathbb{E}[P_e(N, \delta^* - N^{-1/2}z)] = Q\left(\frac{z}{\alpha}\right) + o(1)$$

あるいはより詳細な形

$$\mathbb{E}[P_e(N, \delta^* - N^{-1/2}z - \beta N^{-2/3})] = Q\left(\frac{z}{\alpha}\right) + O(N^{-1/3})$$

のスケーリング則が成り立つと予想されている。



# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ **ポーラ符号**
  - 基礎的事項
  - 復号誤り率の上界
  - スケーリング則
  - 拡張
- ④ まとめ

# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ **ポーラ符号**
  - 基礎的事項
  - 復号誤り率の上界
  - スケーリング則
  - 拡張
- ④ まとめ

# ポーラ符号

Arikan (2009) により提案された符号.

- 符号化, 復号の計算量が  $O(N \log N)$ .
- 任意の二元無記憶通信路に対して対称通信路容量 (一様分布に従う入力に対する入出力の相互情報量) を漸近的に達成することが証明されている (非対称通信路に対して通信路容量を達成する方法については, Sutter ら, 2012; 本多-山本, 2013 など).
- 様々な問題に対して最適 (Korada, 2009 ほか).
  - 歪みあり情報源圧縮
  - 付加情報のある情報源圧縮 (Wyner-Ziv 問題)
  - 付加情報のある通信路符号化 (Gelfand-Pinsker 問題)
  - Slepian-Wolf, One-Helper, ...

# 通信路の組み合わせと分解

通信路  $W : \mathcal{X} = \{0, 1\} \mapsto \mathcal{Y}$

通信路の組み合わせと分解:

$$\Phi : W \rightarrow \{W^-, W^+\}$$

$$W^-(y_0, y_1|x_0) = \sum_{x_1 \in \mathcal{X}} \frac{1}{2} W(y_0|(\mathbf{x}G)_0) W(y_1|(\mathbf{x}G)_1)$$

$$W^+(y_0, y_1, x_0|x_1) = \frac{1}{2} W(y_0|(\mathbf{x}G)_0) W(y_1|(\mathbf{x}G)_1), \quad G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$\Phi$  の反復的な適用:

$$\begin{aligned} W &\rightarrow \{W^-, W^+\} \rightarrow \{W^{--}, W^{-+}, W^{+-}, W^{++}\} \\ &\rightarrow \{W^{----}, W^{---+}, W^{-+-}, W^{-++}, \\ &\quad W^{+--}, W^{+-+}, W^{++-}, W^{+++}\} \rightarrow \dots, \end{aligned}$$

# 通信路の組み合わせと分解

通信路  $W : \mathcal{X} = \{0, 1\} \mapsto \mathcal{Y}$

通信路の組み合わせと分解:

$$\Phi : W \rightarrow \{W^-, W^+\}$$

$$W^-(y_0, y_1 | x_0) = \sum_{x_1 \in \mathcal{X}} \frac{1}{2} W(y_0 | (\mathbf{x}G)_0) W(y_1 | (\mathbf{x}G)_1)$$

$$W^+(y_0, y_1, x_0 | x_1) = \frac{1}{2} W(y_0 | (\mathbf{x}G)_0) W(y_1 | (\mathbf{x}G)_1), \quad G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$\Phi$  の反復的な適用:

$$\begin{aligned} W &\rightarrow \{W^-, W^+\} \rightarrow \{W^{--}, W^{-+}, W^{+-}, W^{++}\} \\ &\rightarrow \{W^{---}, W^{--+}, W^{-+-}, W^{-++}, \\ &\quad W^{+--}, W^{+-+}, W^{++-}, W^{+++}\} \rightarrow \dots, \end{aligned}$$

# 通信路の組み合わせと分解

$\Phi$  の反復的な適用:

$$\begin{aligned} W &\rightarrow \{W^-, W^+\} \rightarrow \{W^{--}, W^{-+}, W^{+-}, W^{++}\} \\ &\rightarrow \{W^{---}, W^{--+}, W^{-+-}, W^{-++}, \\ &\quad W^{+--}, W^{+-+}, W^{++-}, W^{+++}\} \rightarrow \dots, \end{aligned}$$

- $I(W)$ : 対称通信路容量
  - 性質:  $I(W^-) + I(W^+) = 2I(W)$
- Byattacharyya パラメータ:

$$Z(W) := \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$$

- 入力用最尤推定の誤り率の上界.
- \* 二元消失通信路 (BEC) では  $Z(W) = 1 - I(W)$ .
- \* 一般の通信路に対しては  $Z(W)$  が 0/1 に近い  $\Leftrightarrow I(W)$  が 1/0 に近い.

# 通信路の組み合わせと分解

$\Phi$  の反復的な適用:

$$\begin{aligned} W &\rightarrow \{W^-, W^+\} \rightarrow \{W^{--}, W^{-+}, W^{+-}, W^{++}\} \\ &\rightarrow \{W^{---}, W^{--+}, W^{-+-}, W^{-++}, \\ &\quad W^{+--}, W^{+-+}, W^{++-}, W^{+++}\} \rightarrow \dots, \end{aligned}$$

- $I(W)$ : 対称通信路容量
  - 性質:  $I(W^-) + I(W^+) = 2I(W)$
- Byattacharyya パラメータ:

$$Z(W) := \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$$

- 入力用最尤推定の誤り率の上界.
- \* 二元消失通信路 (BEC) では  $Z(W) = 1 - I(W)$ .
- \* 一般の通信路に対しては  $Z(W)$  が  $0/1$  に近い  $\Leftrightarrow I(W)$  が  $1/0$  に近い.

# 通信路の組み合わせと分解

$\Phi$  の反復的な適用:

$$\begin{aligned} W &\rightarrow \{W^-, W^+\} \rightarrow \{W^{--}, W^{-+}, W^{+-}, W^{++}\} \\ &\rightarrow \{W^{---}, W^{--+}, W^{-+-}, W^{-++}, \\ &\quad W^{+--}, W^{+-+}, W^{++-}, W^{+++}\} \rightarrow \dots, \end{aligned}$$

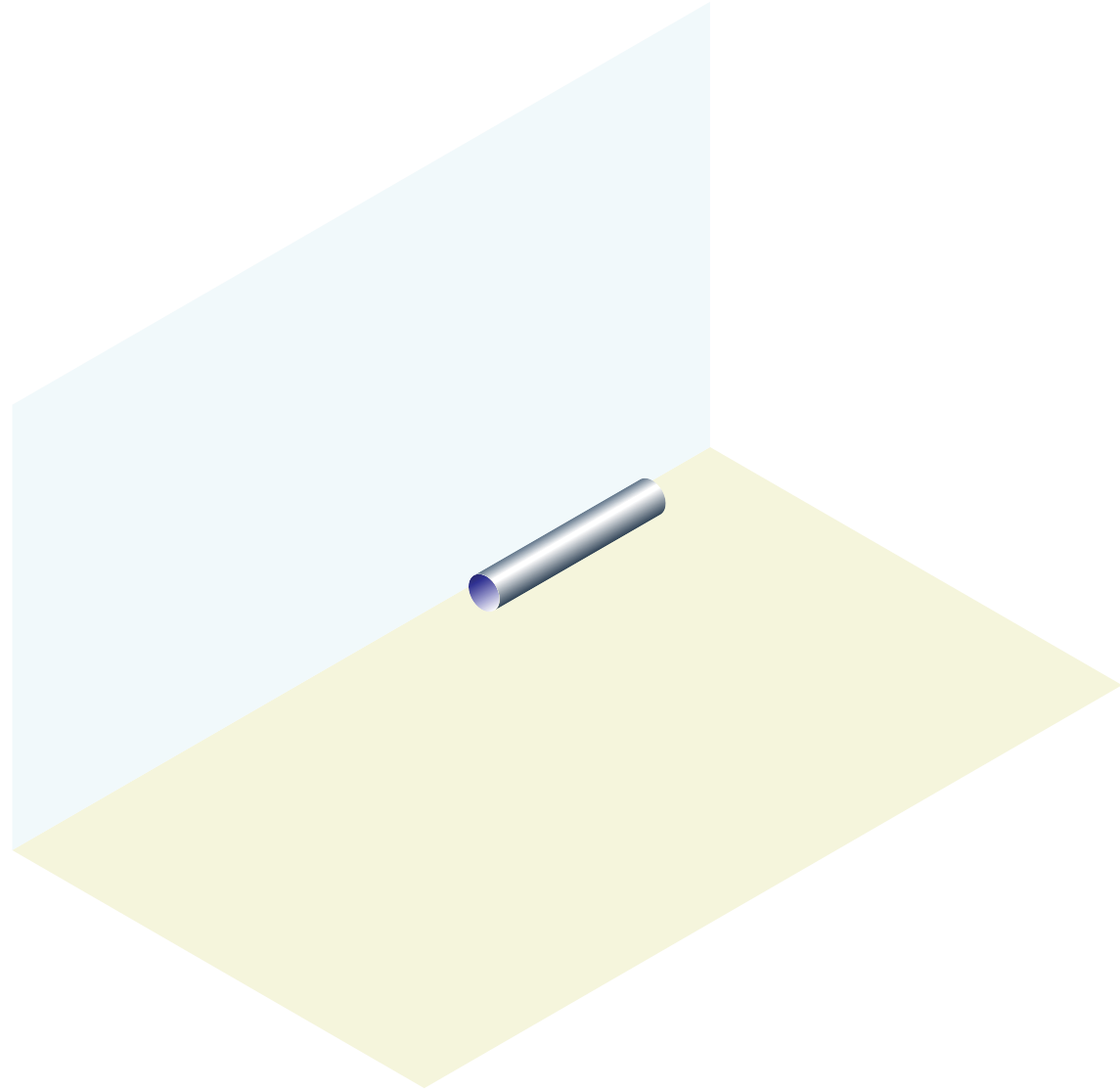
- $I(W)$ : 対称通信路容量
  - 性質:  $I(W^-) + I(W^+) = 2I(W)$
- Byattacharyya パラメータ:

$$Z(W) := \sum_{y \in \mathcal{Y}} \sqrt{W(y|0)W(y|1)}$$

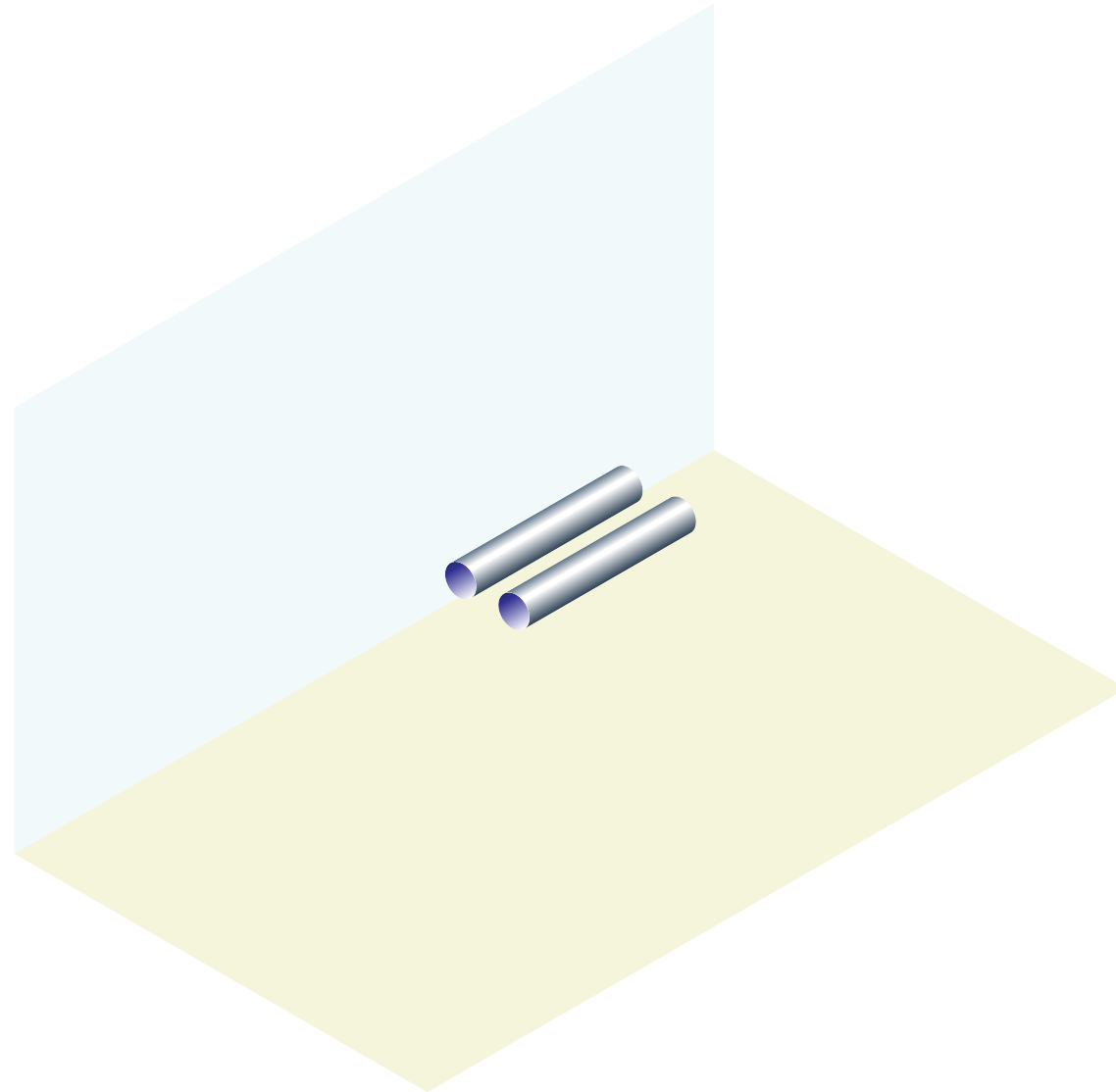
- 入力 of 最尤推定の誤り率の上界.
- \* 二元消失通信路 (BEC) では  $Z(W) = 1 - I(W)$ .
- \* 一般の通信路に対しては  $Z(W)$  が  $0/1$  に近い  $\Leftrightarrow I(W)$  が  $1/0$  に近い.



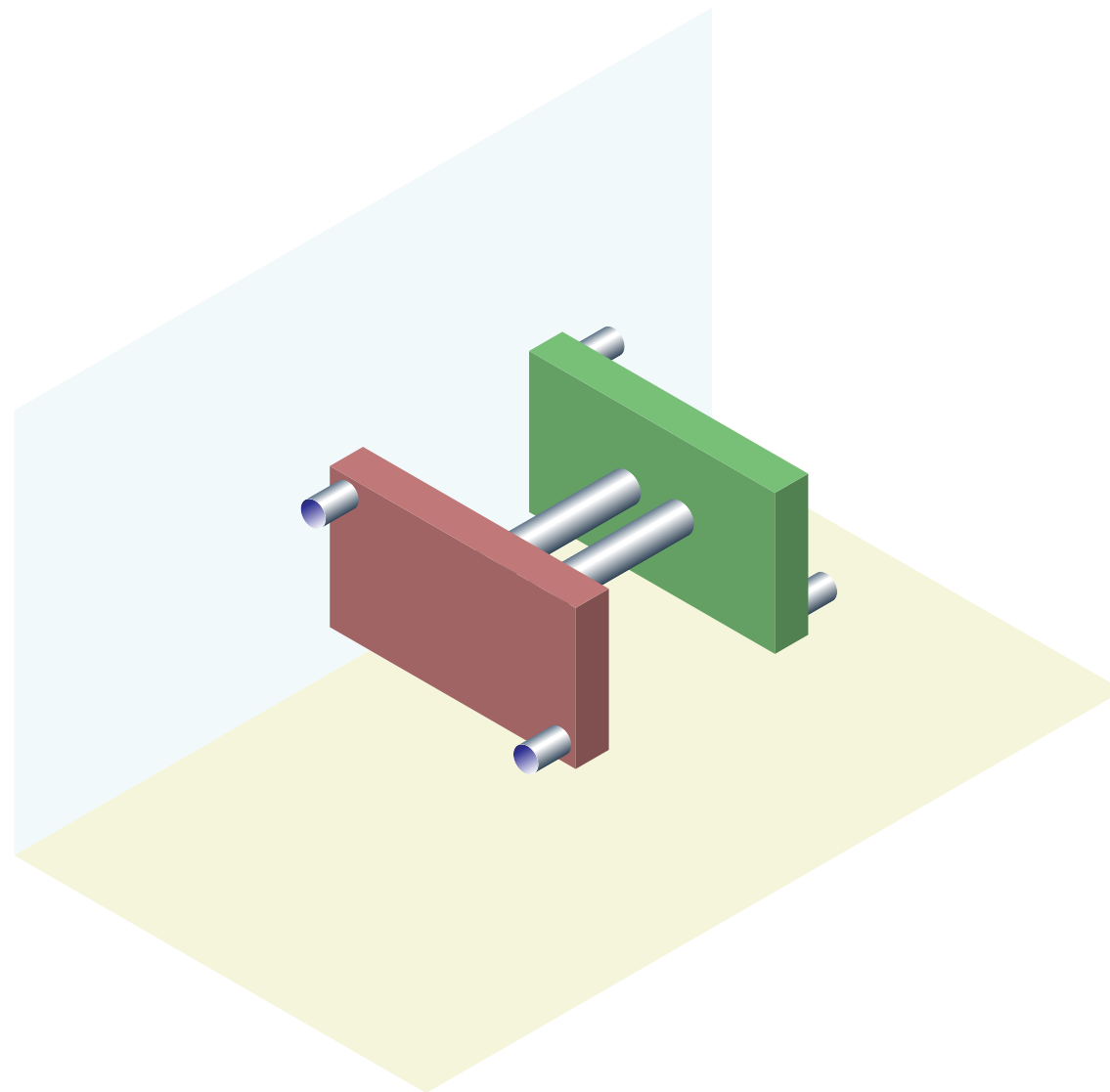
# 通信路の組み合わせと分解



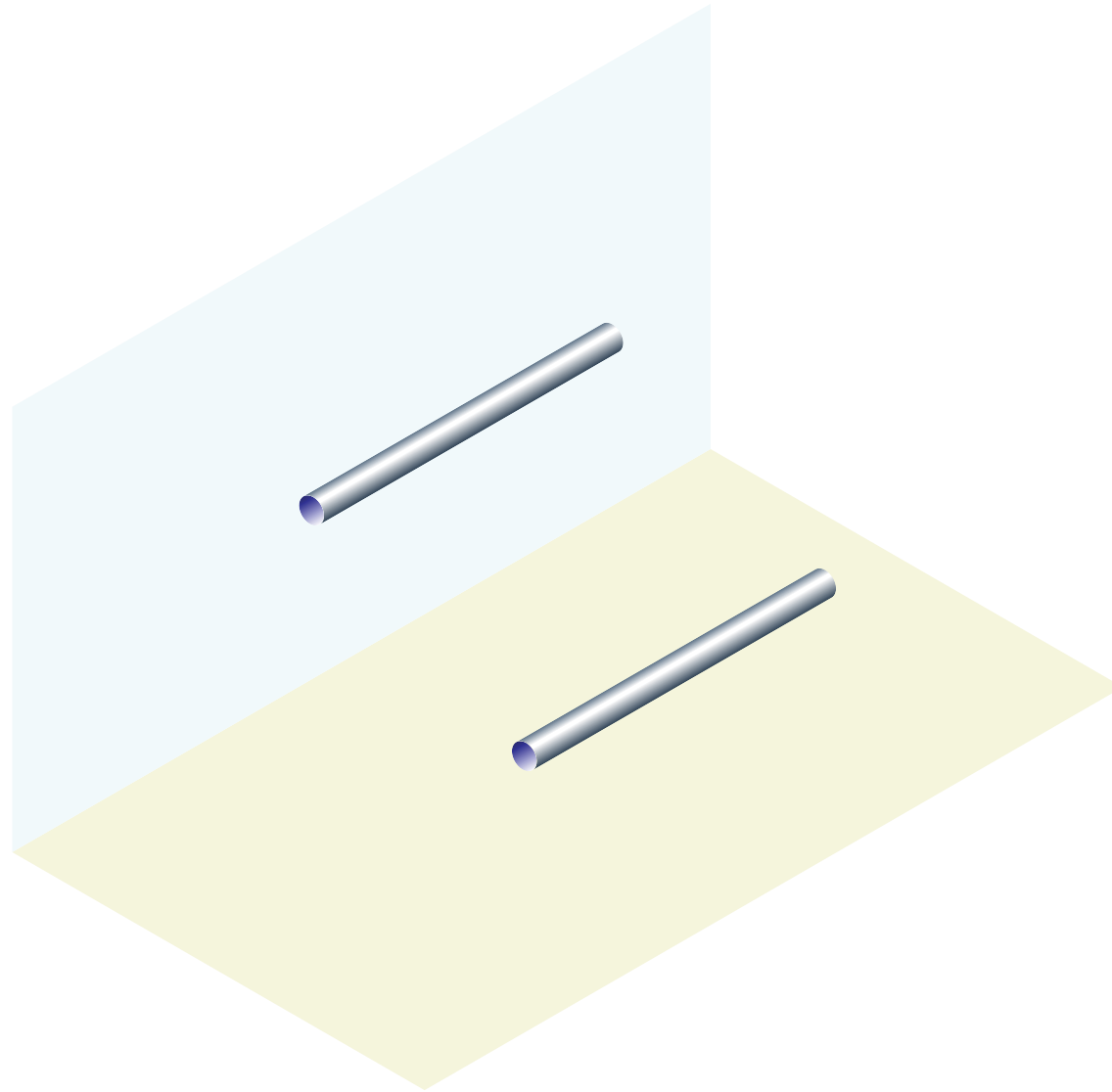
# 通信路の組み合わせと分解



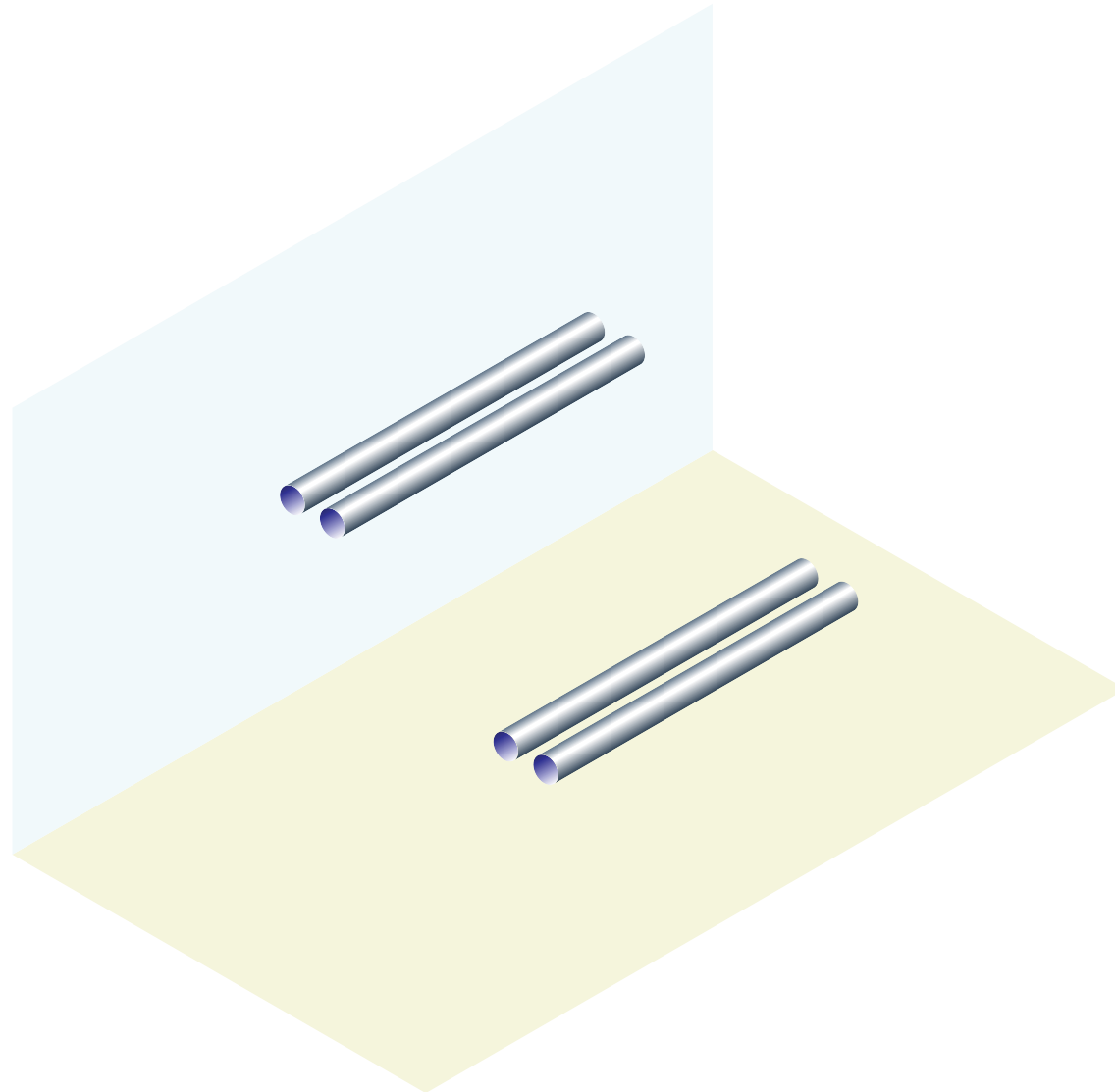
# 通信路の組み合わせと分解



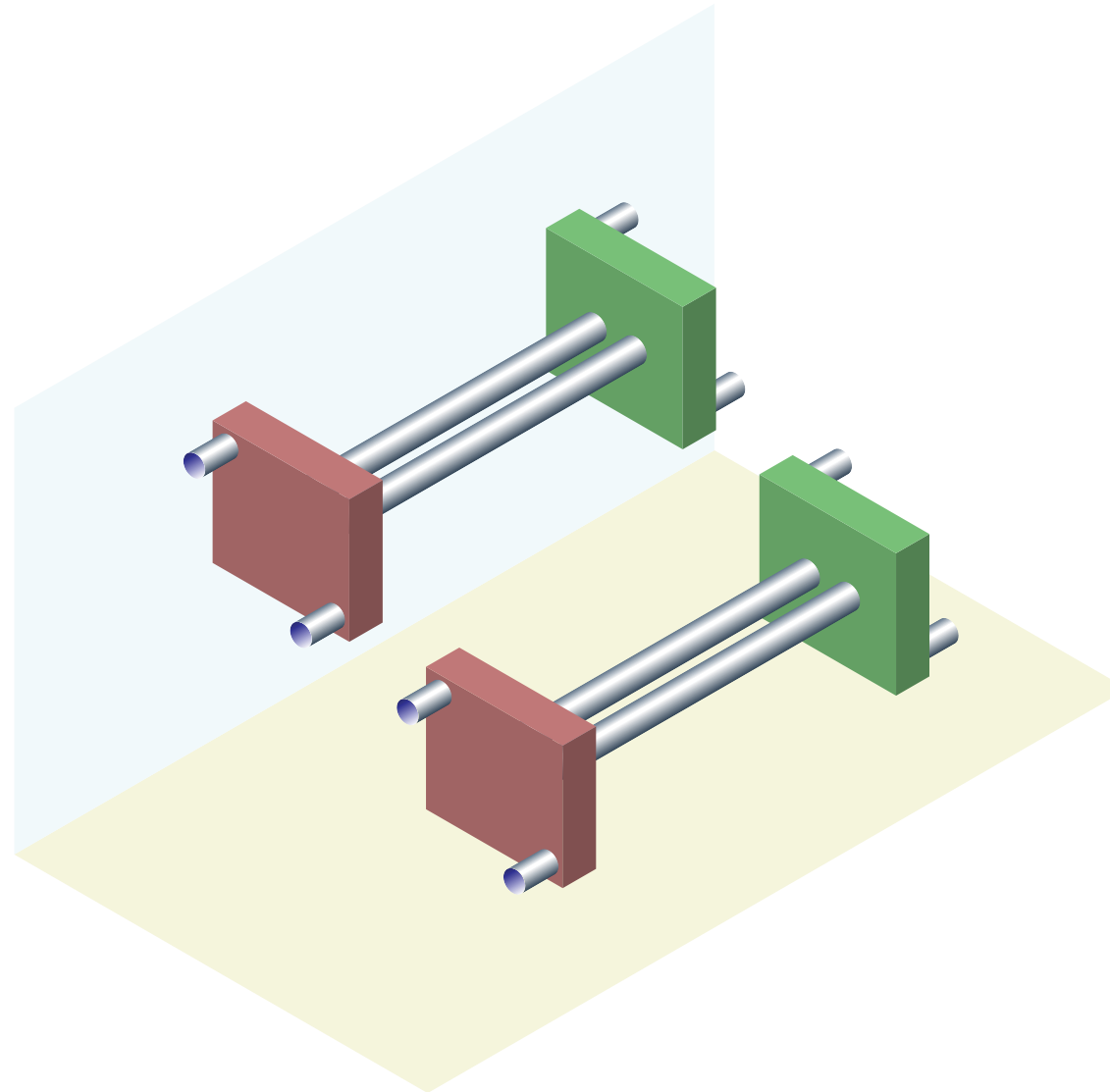
# 通信路の組み合わせと分解



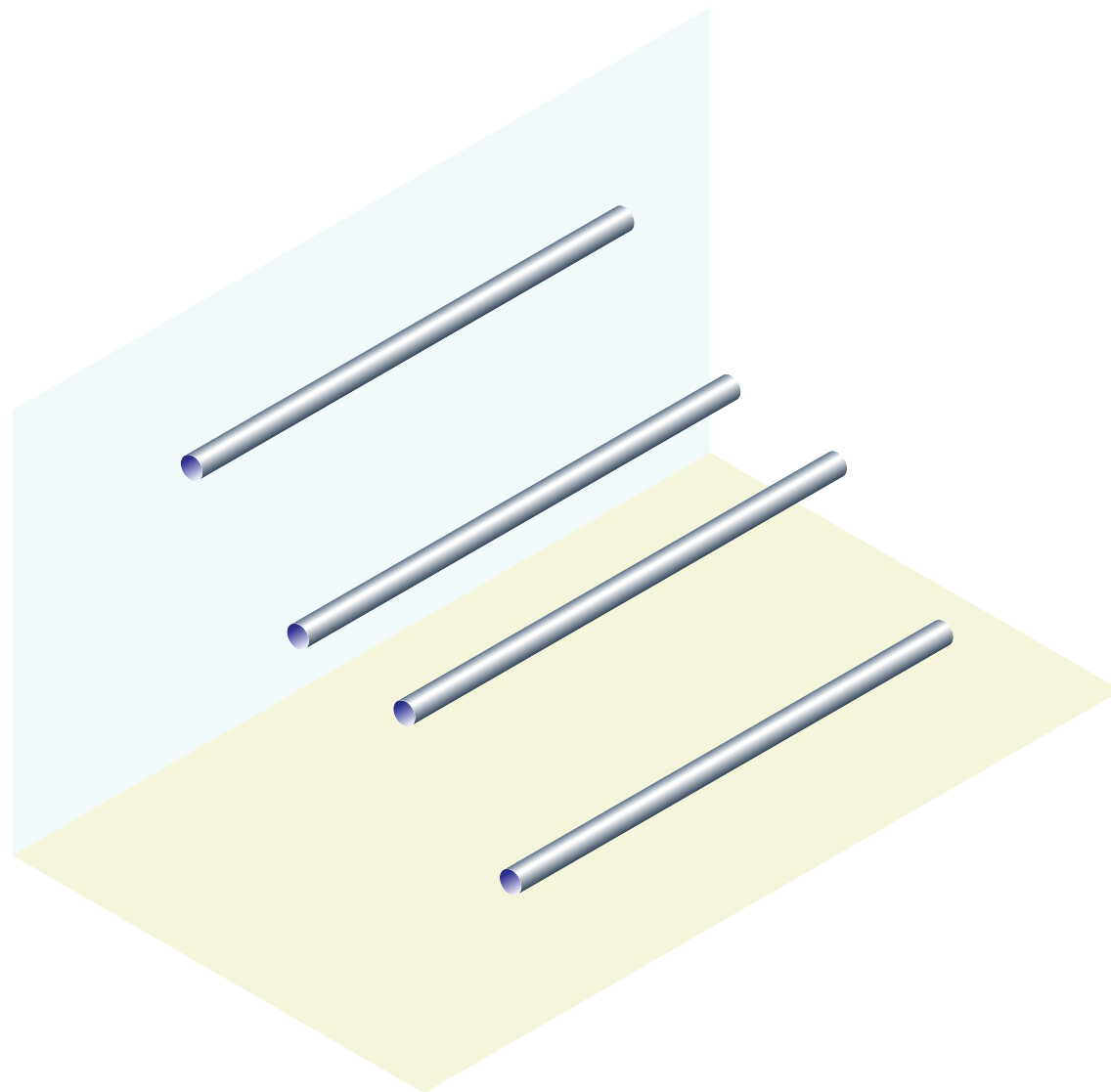
# 通信路の組み合わせと分解



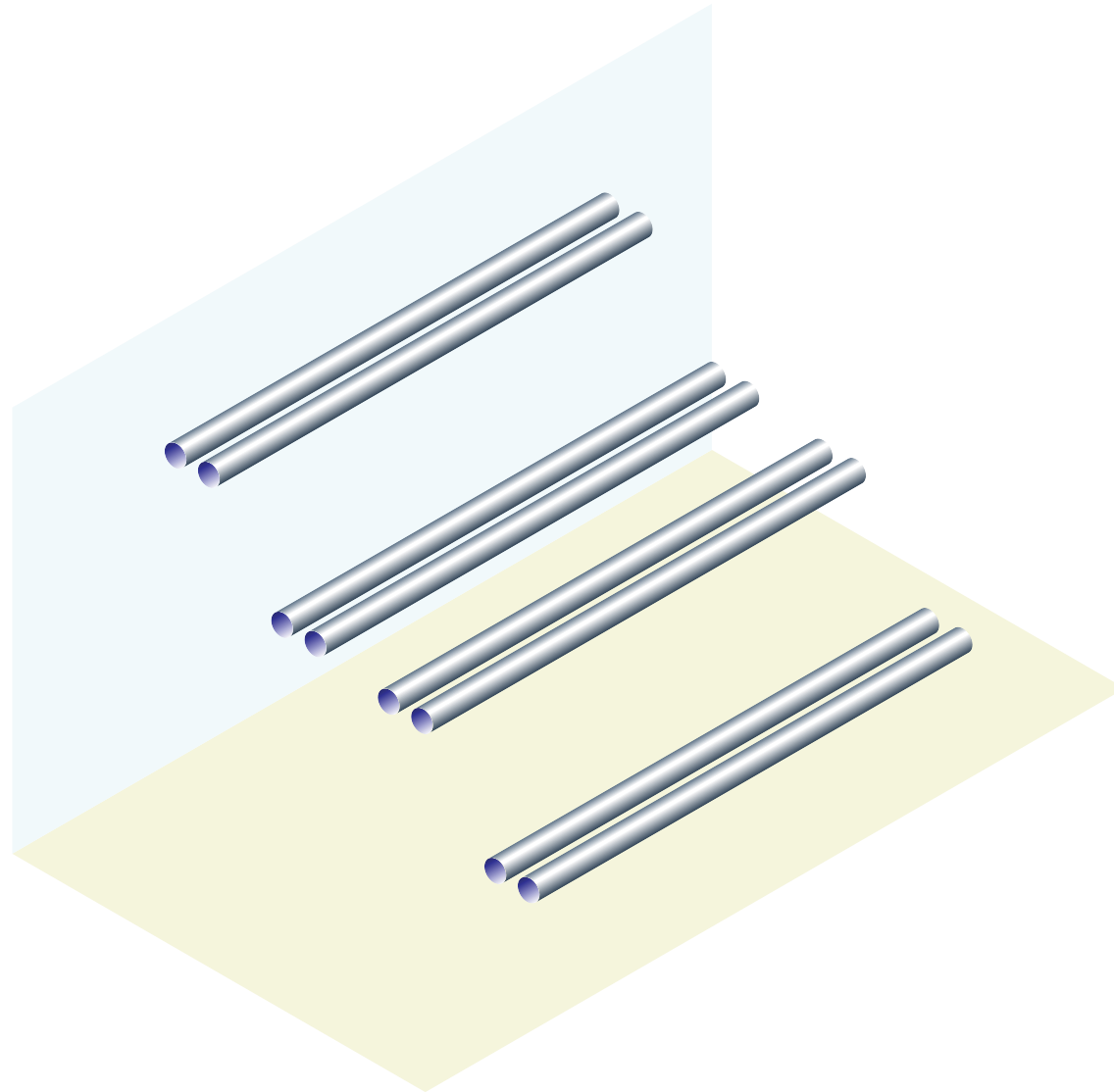
# 通信路の組み合わせと分解



# 通信路の組み合わせと分解

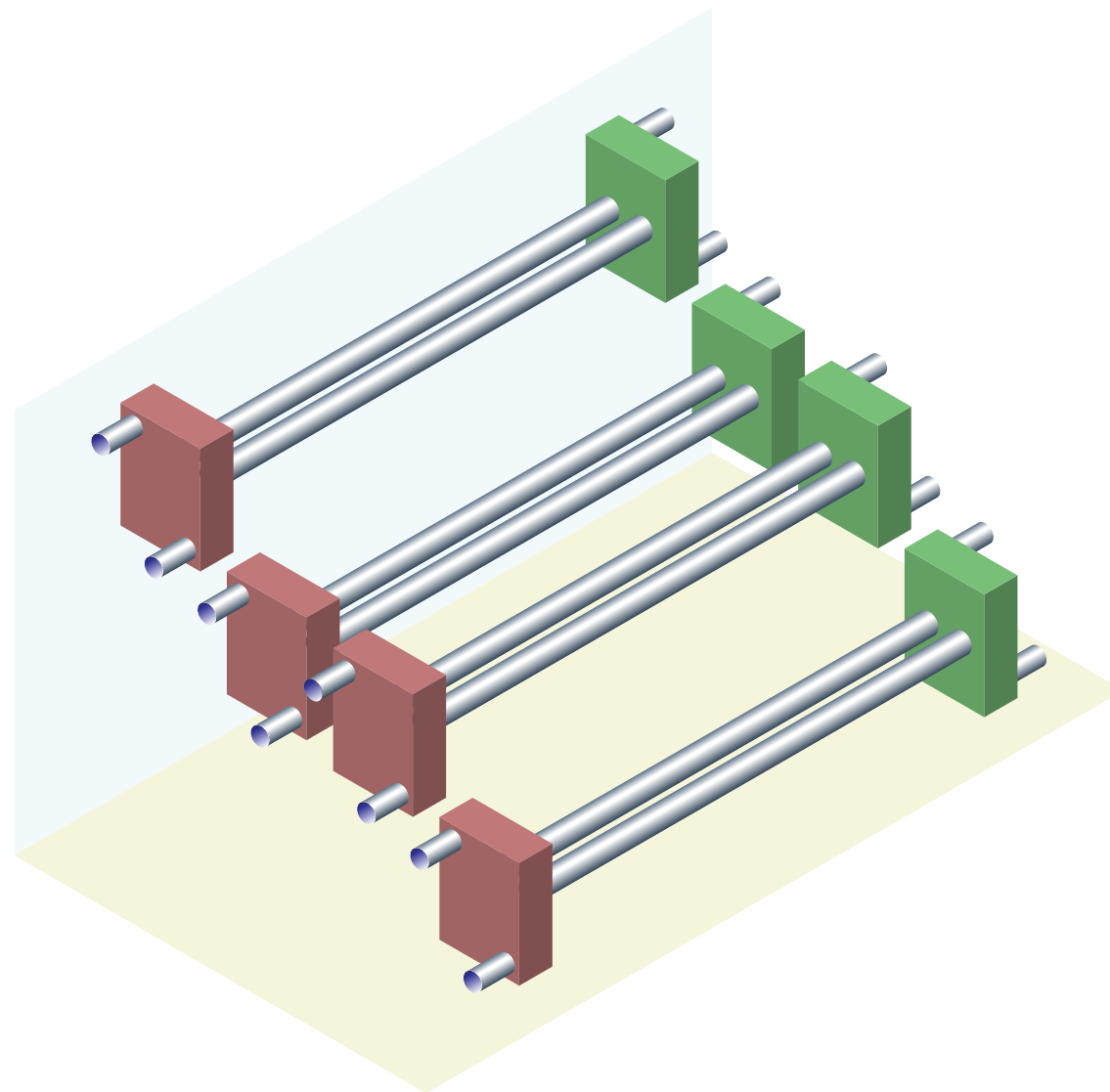


# 通信路の組み合わせと分解

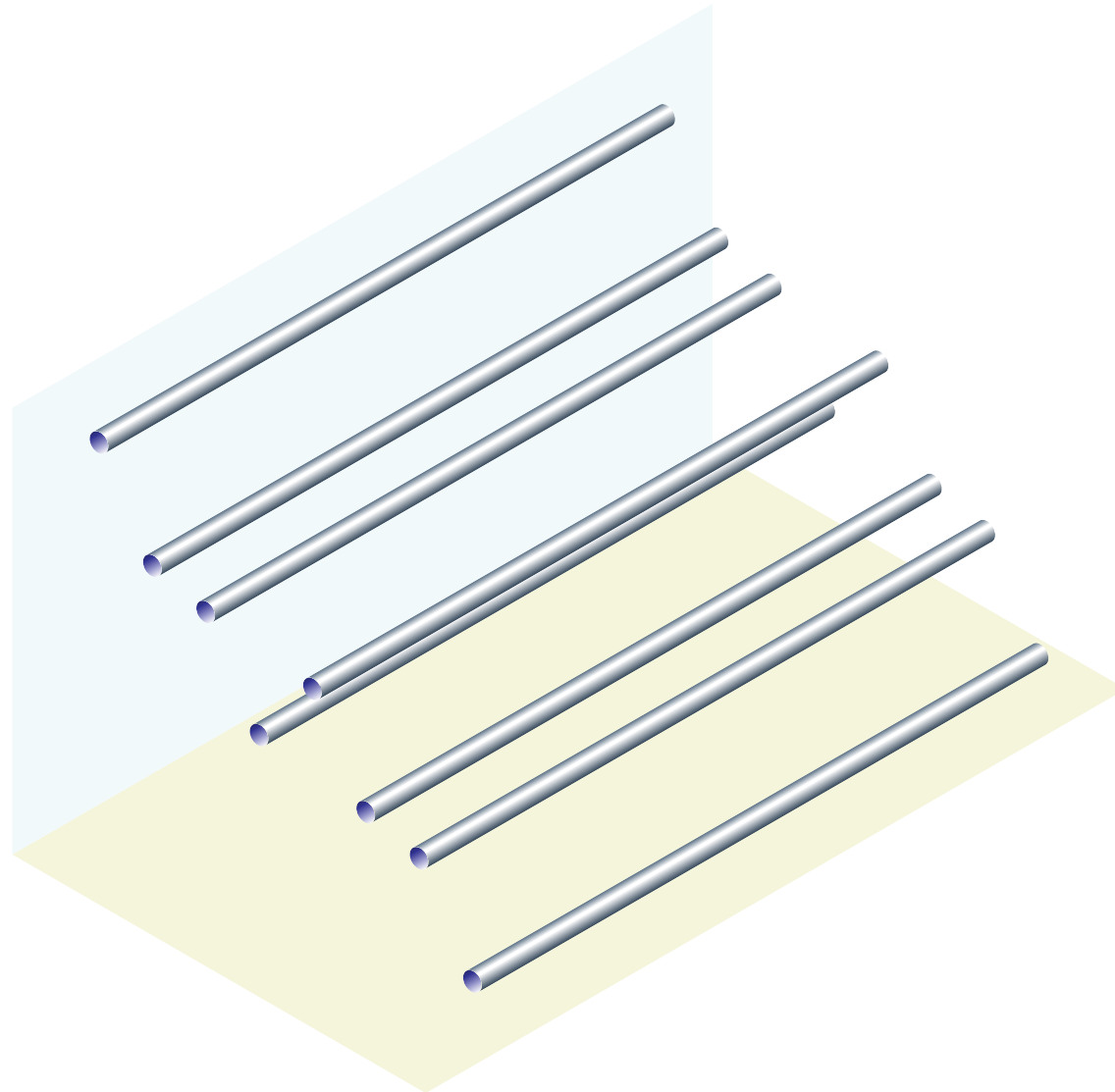




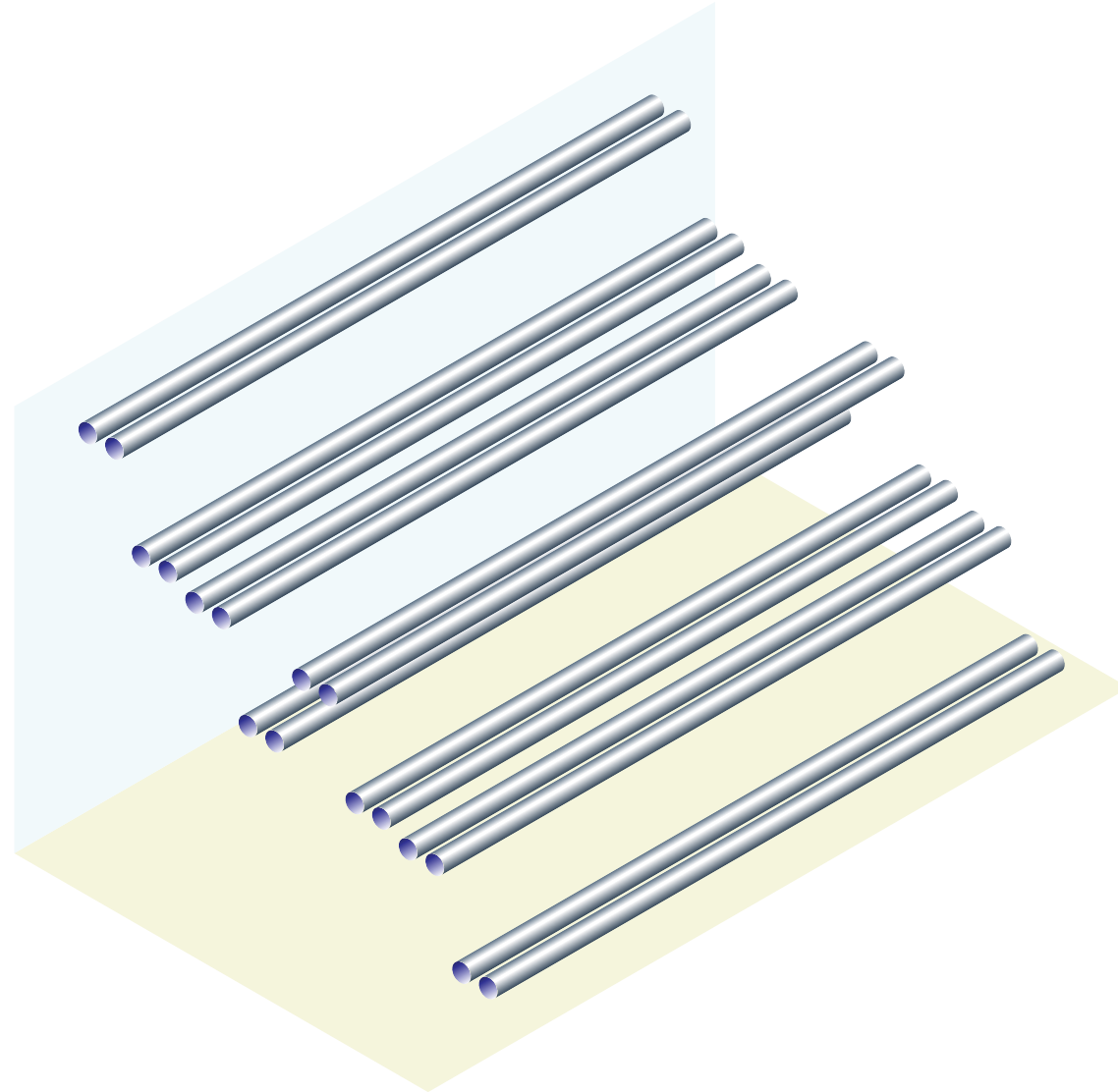
# 通信路の組み合わせと分解



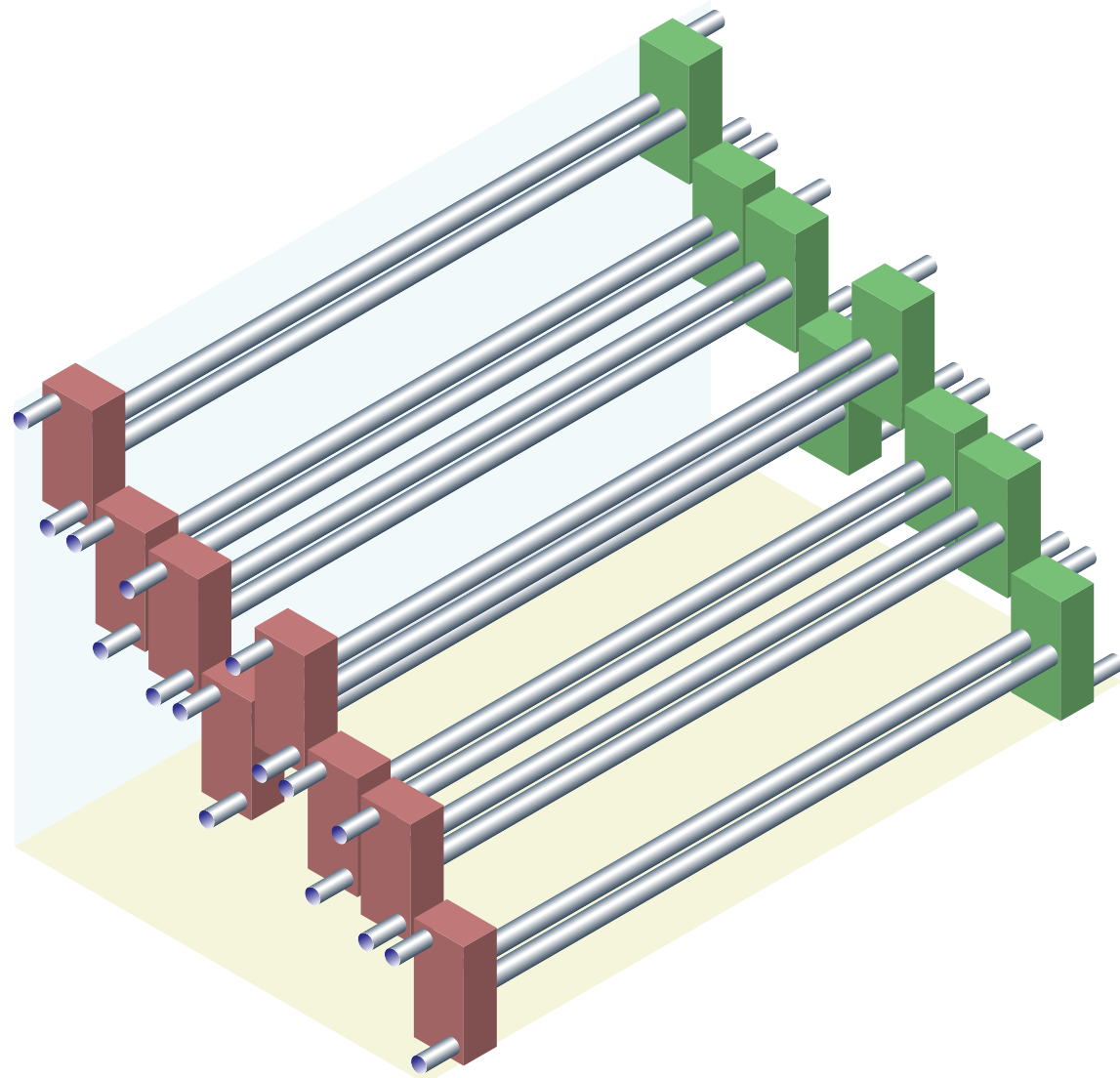
# 通信路の組み合わせと分解



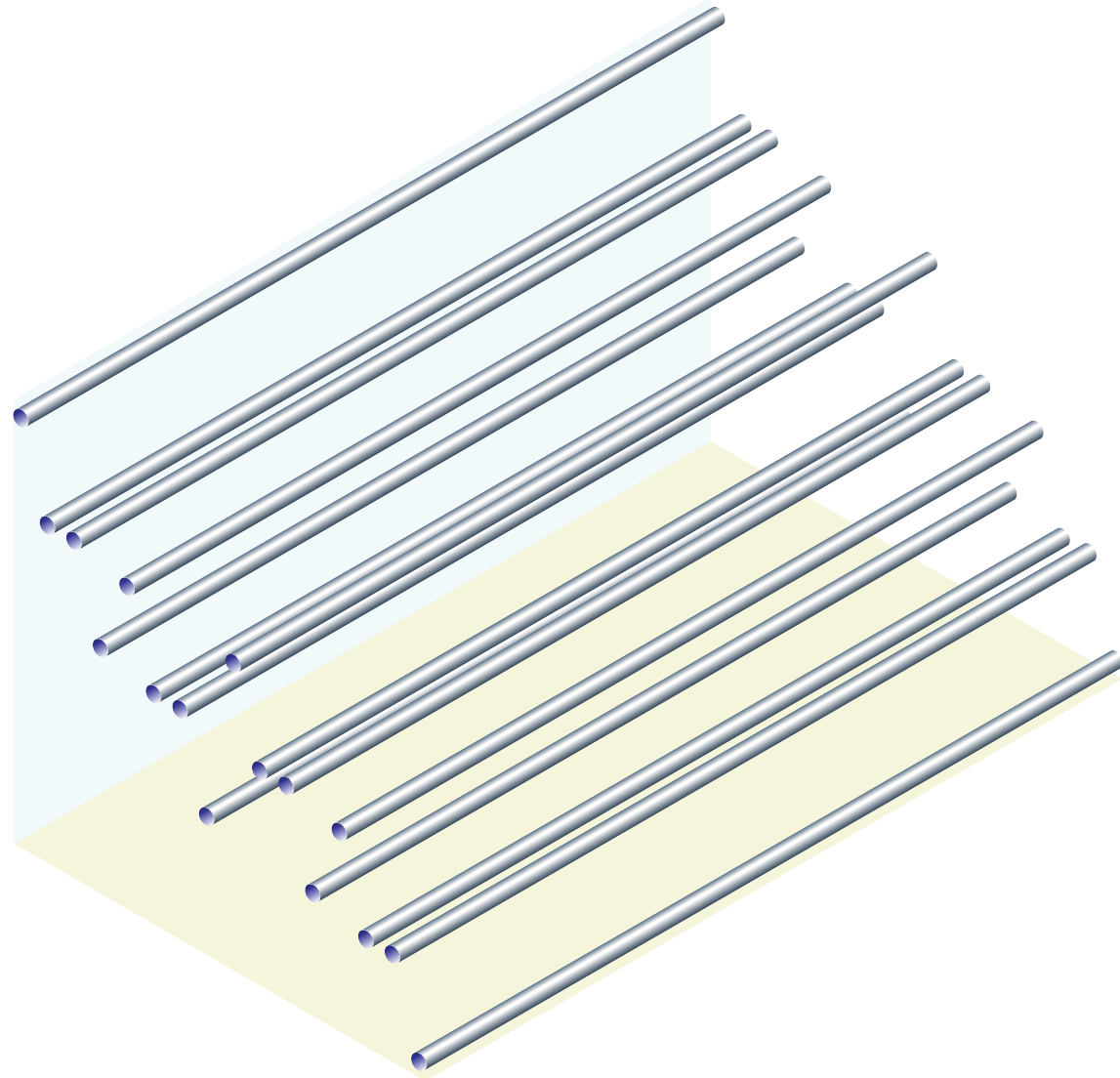
# 通信路の組み合わせと分解



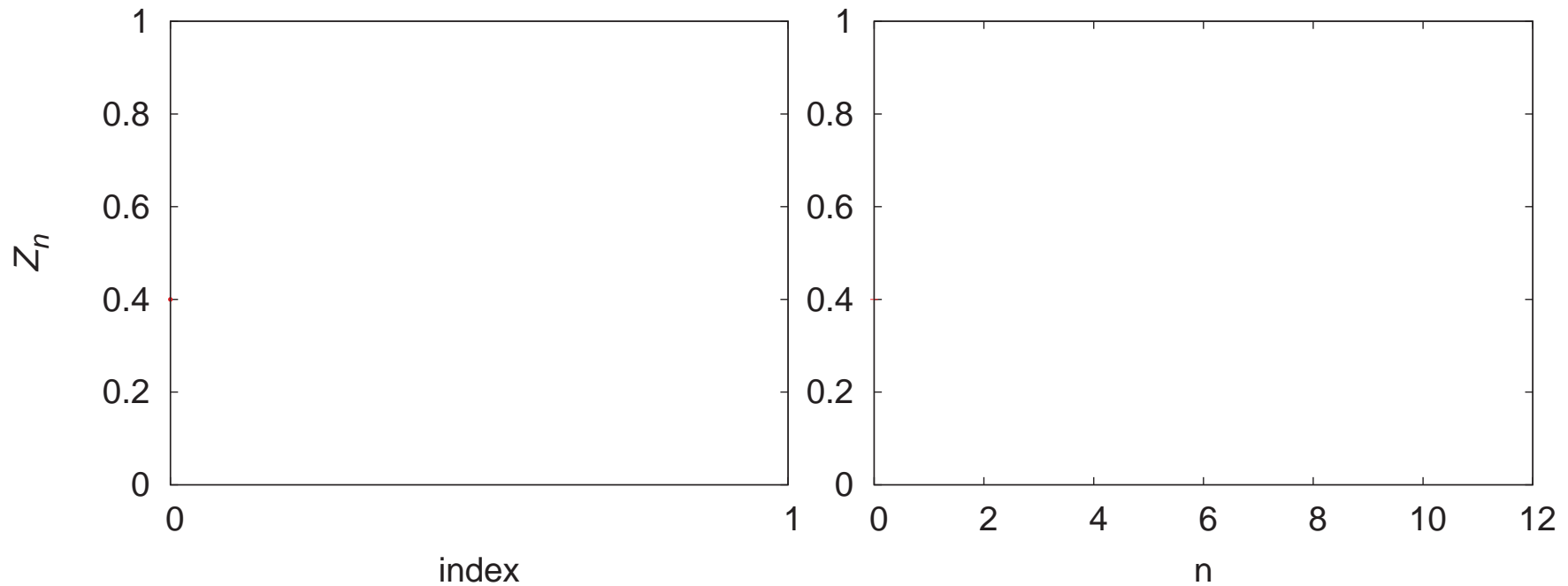
# 通信路の組み合わせと分解



# 通信路の組み合わせと分解

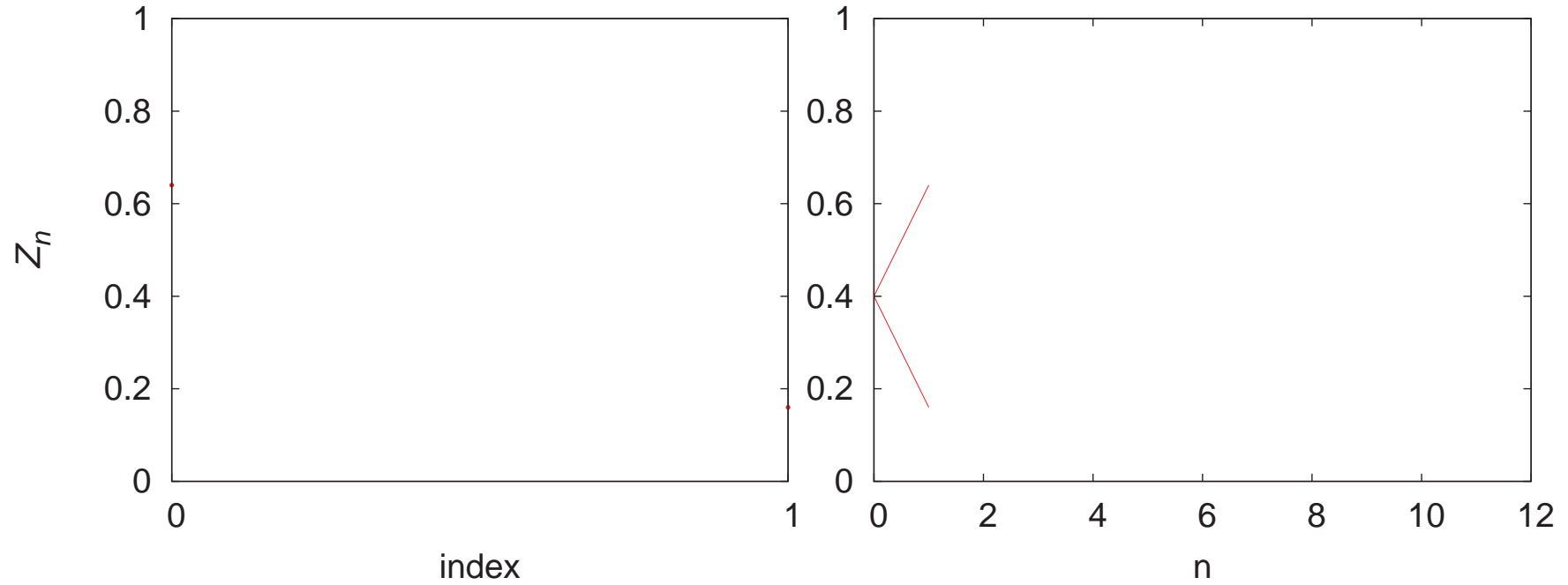


# 数値例 (BEC, 消失確率 0.4)



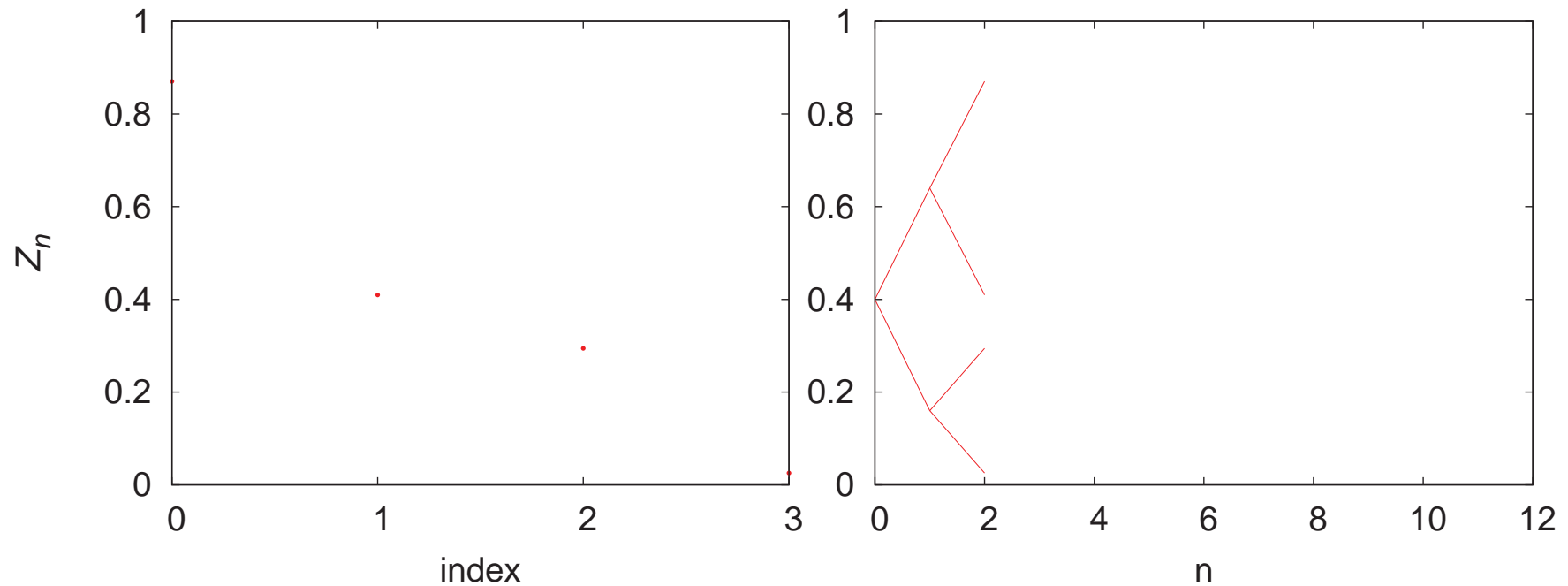
$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

# 数値例 (BEC, 消失確率 0.4)



$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$

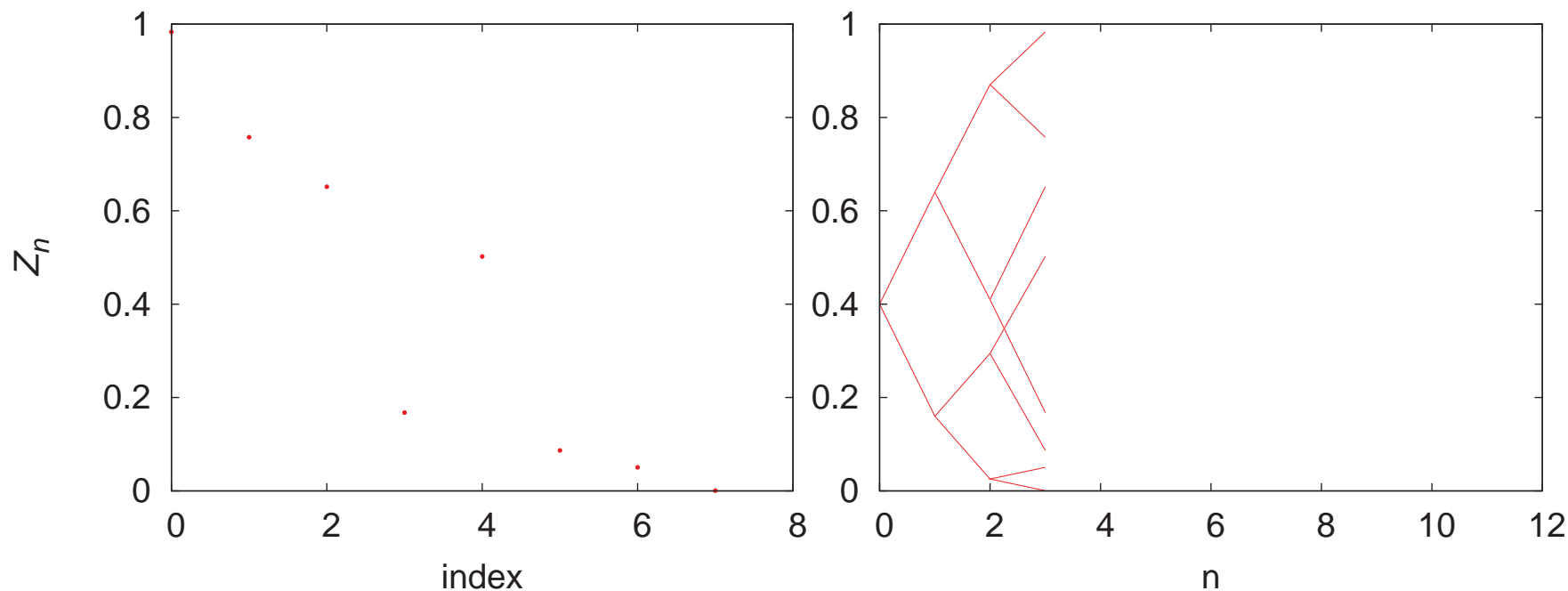
# 数値例 (BEC, 消失確率 0.4)



$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$

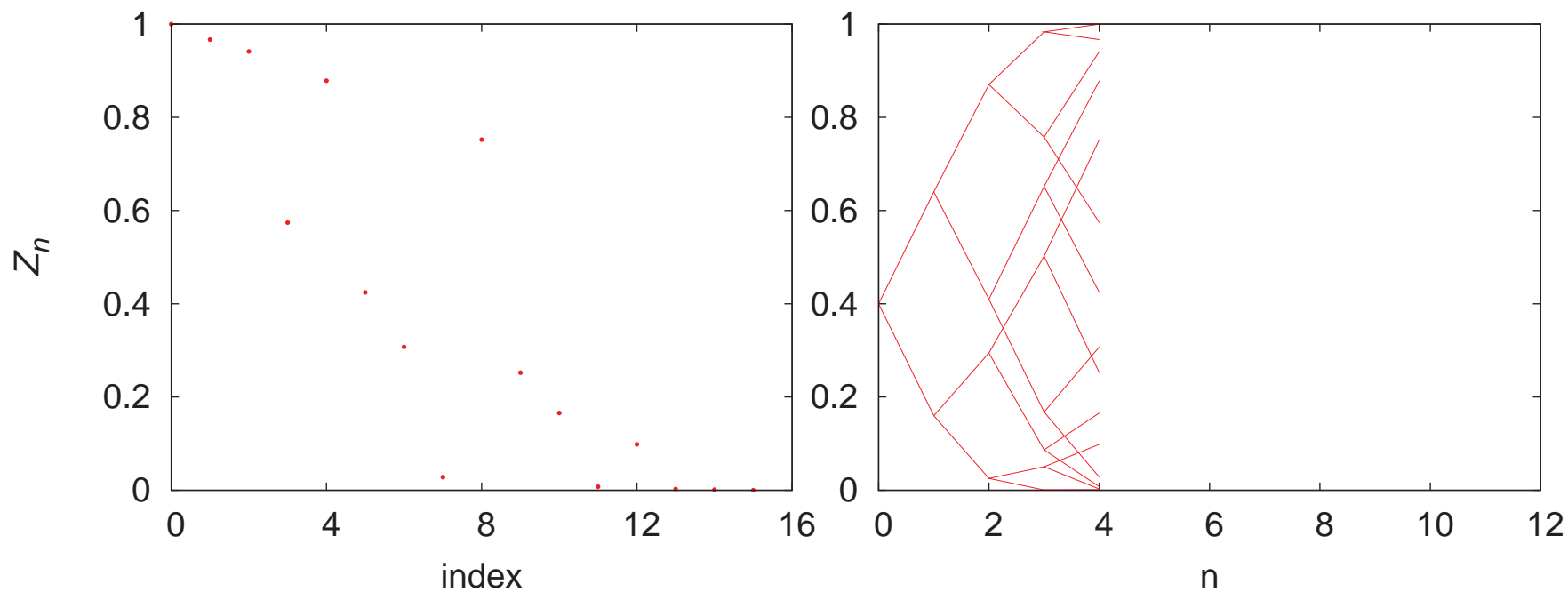


# 数値例 (BEC, 消失確率 0.4)



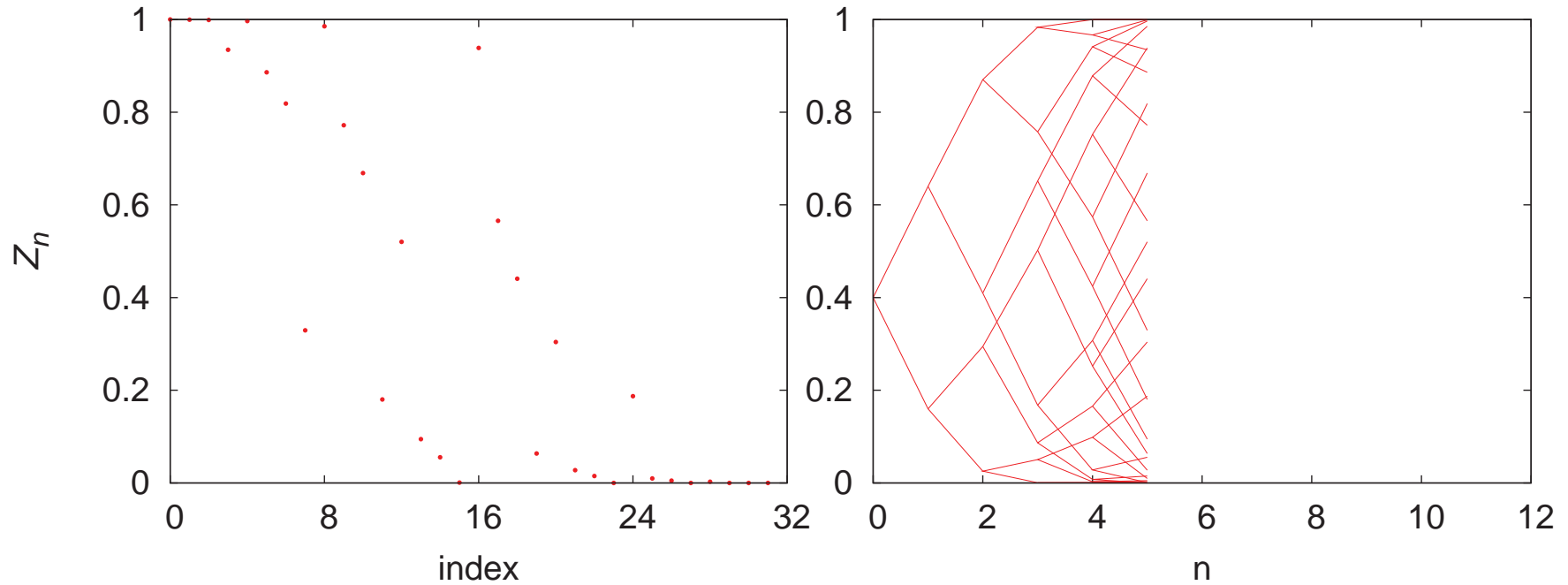
$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$

# 数値例 (BEC, 消失確率 0.4)



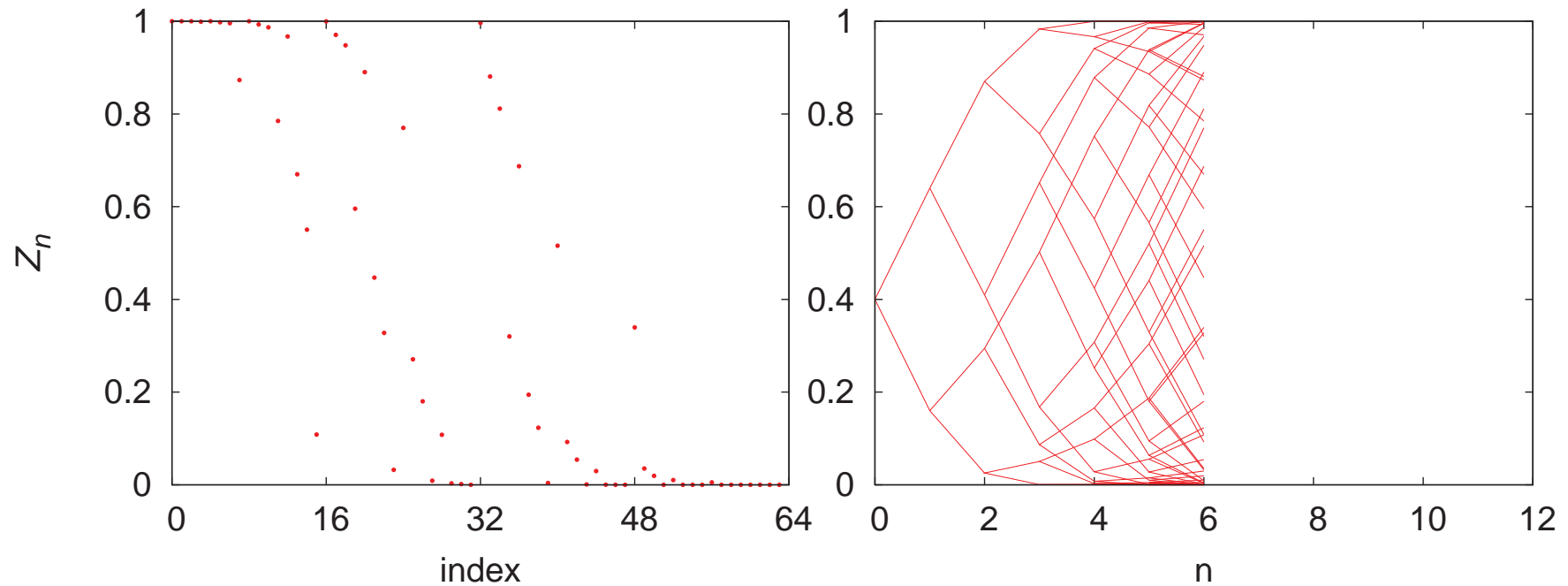
$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

# 数値例 (BEC, 消失確率 0.4)



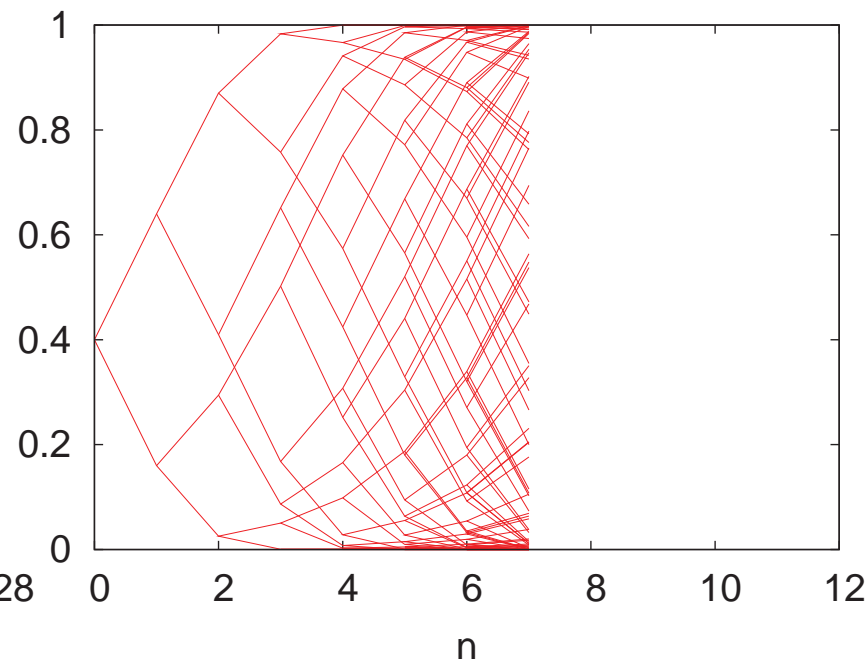
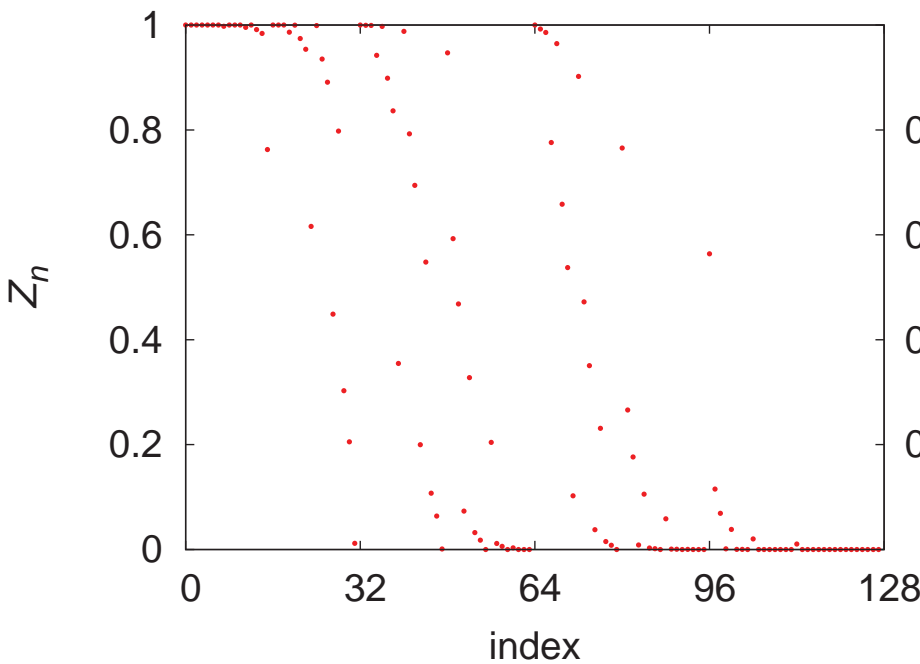
$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

# 数値例 (BEC, 消失確率 0.4)



$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

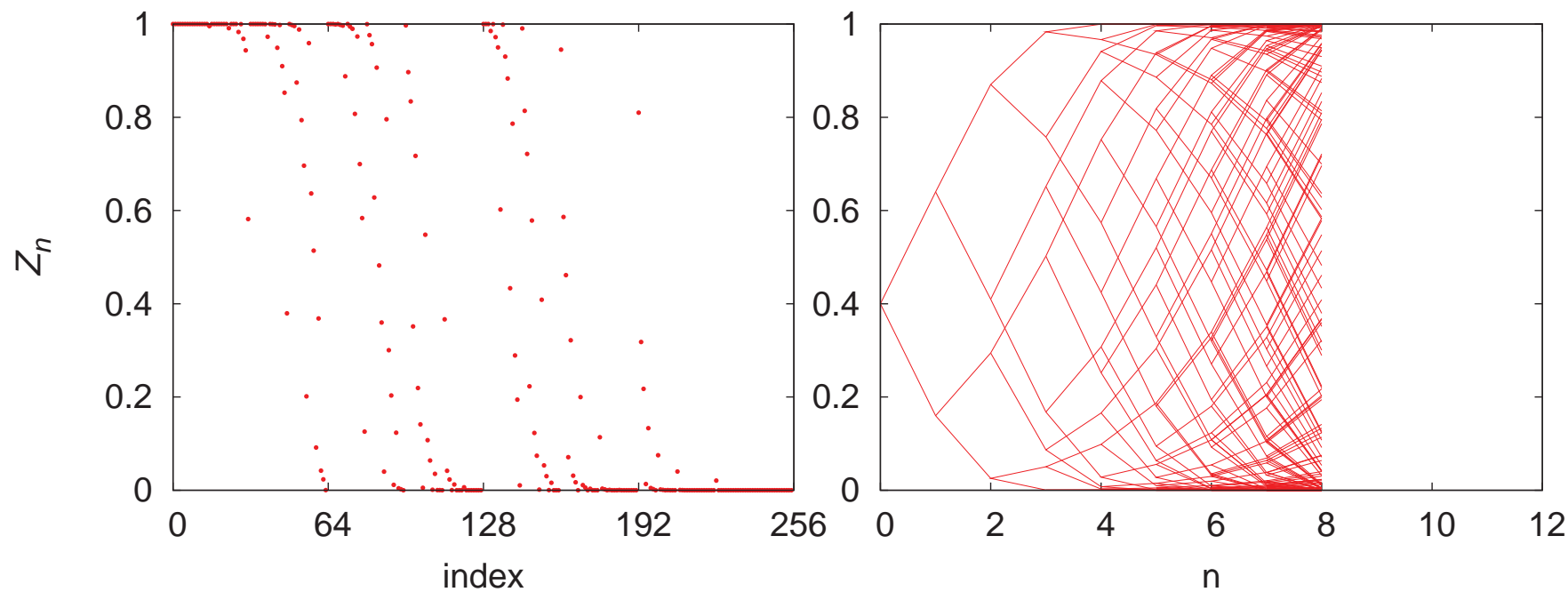
# 数値例 (BEC, 消失確率 0.4)



$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$

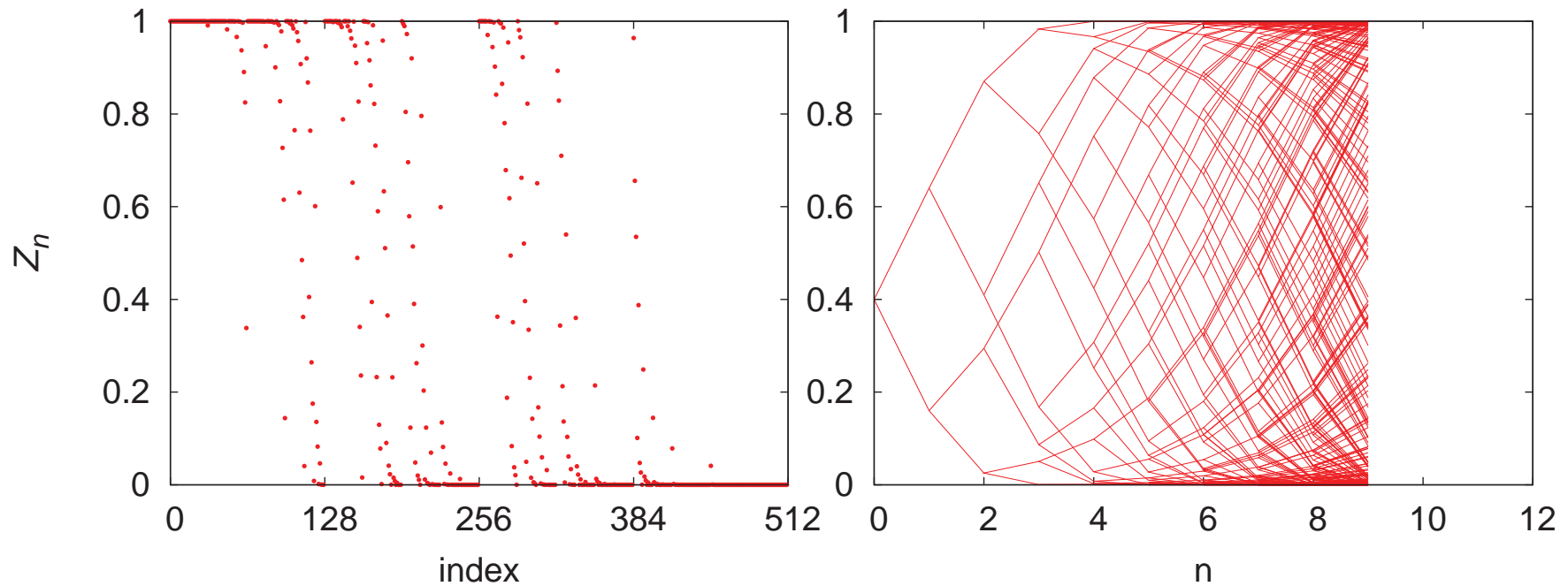


# 数値例 (BEC, 消失確率 0.4)



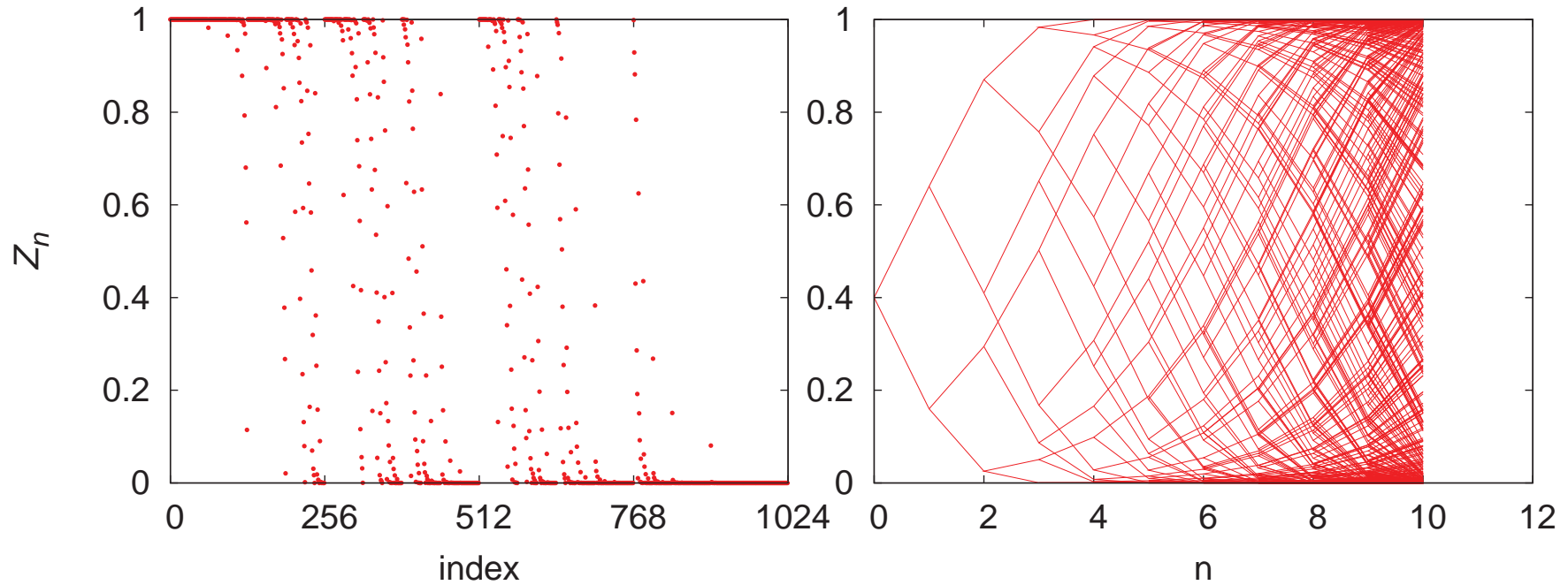
$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

# 数値例 (BEC, 消失確率 0.4)



$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

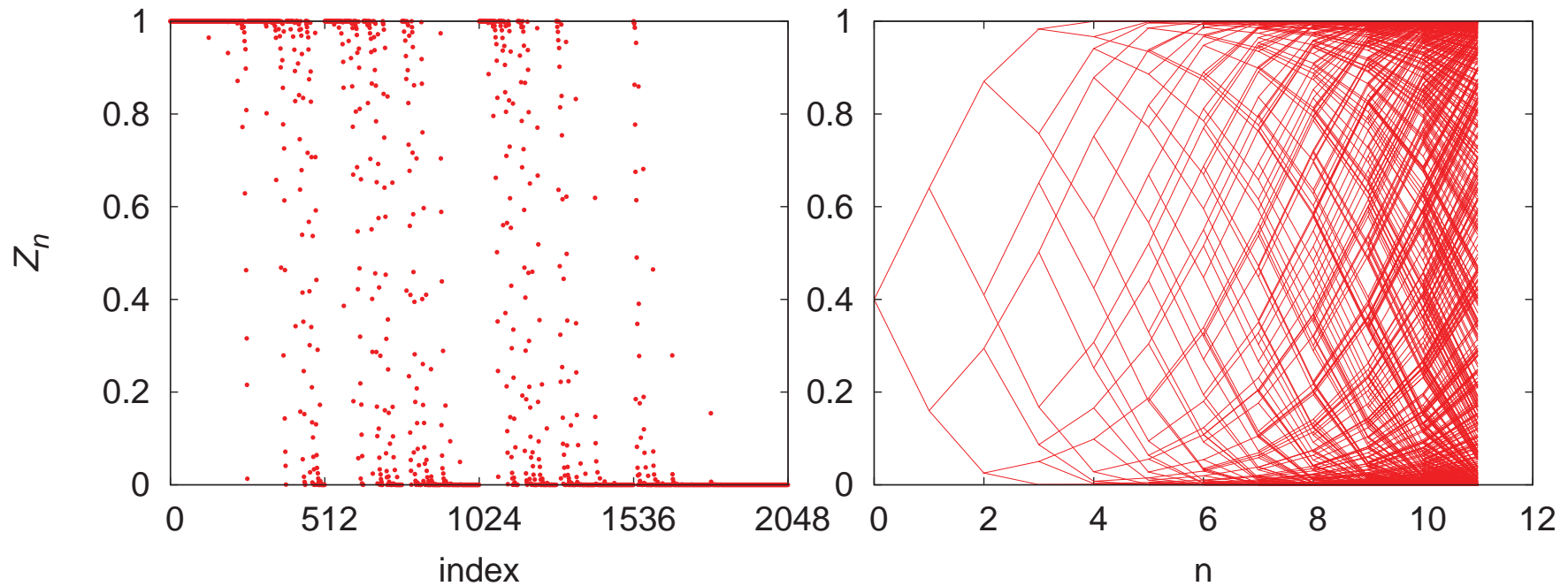
# 数値例 (BEC, 消失確率 0.4)



$B_n \dots B_2 B_1 =$  (添字の二進数表示)

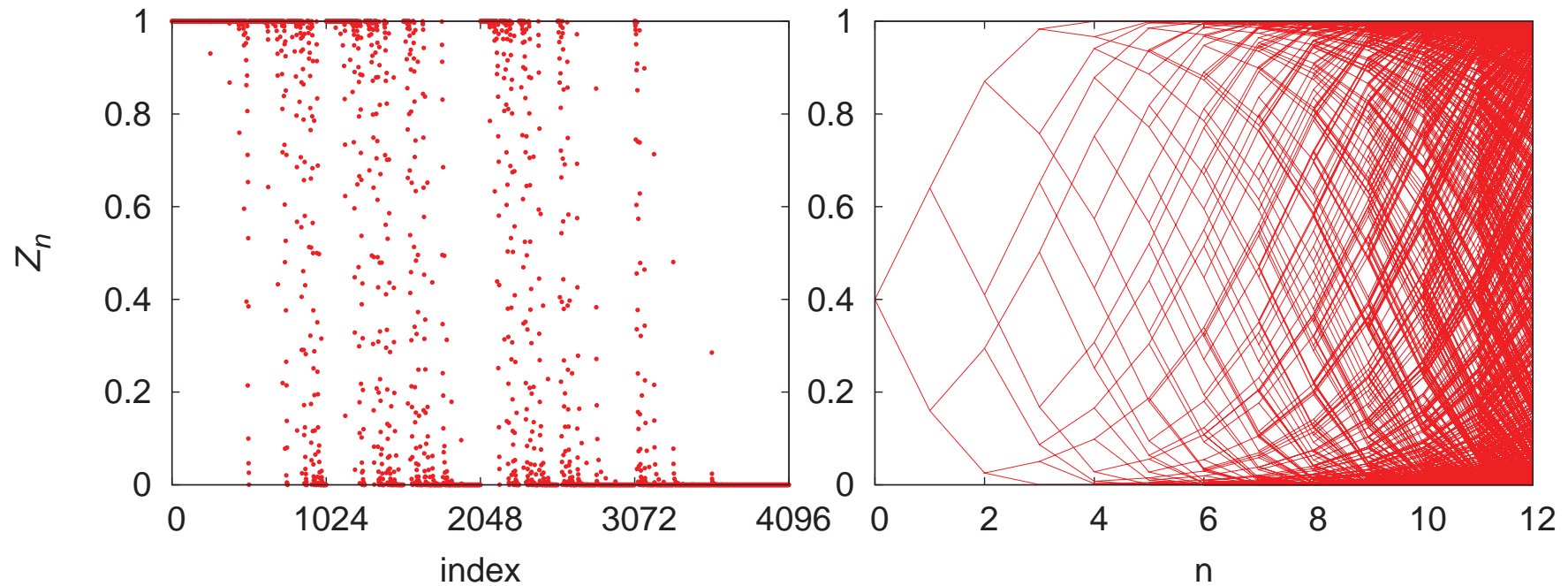


# 数値例 (BEC, 消失確率 0.4)



$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

# 数値例 (BEC, 消失確率 0.4)



$$B_n \dots B_2 B_1 = (\text{添字の二進数表示})$$

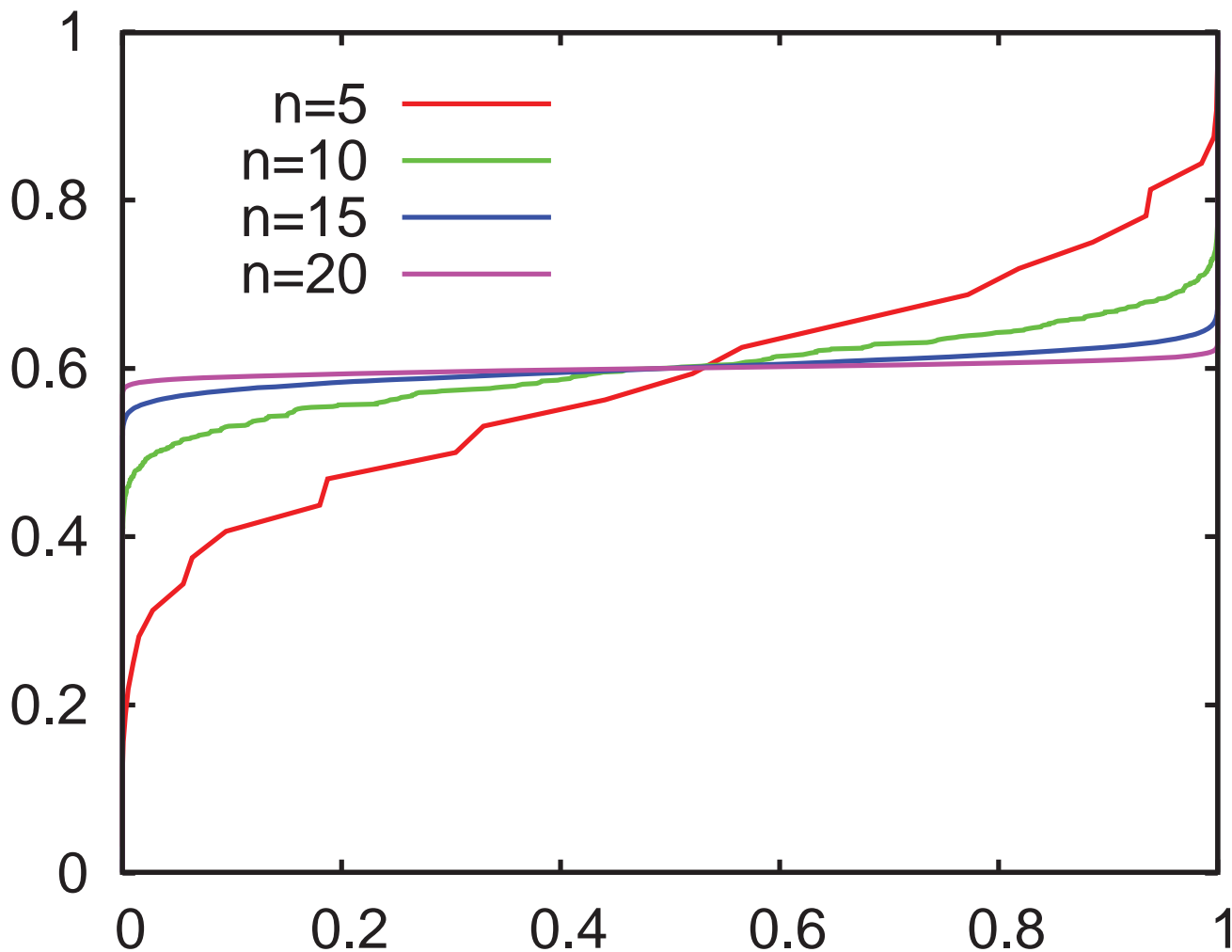
# 分極

## 分極 (Arikan, 2009)

通信路の組み合わせと分解  $\Phi$  を  $n$  回反復して得られる  $2^n$  個の通信路に対し, Bhattacharyya パラメータの値が

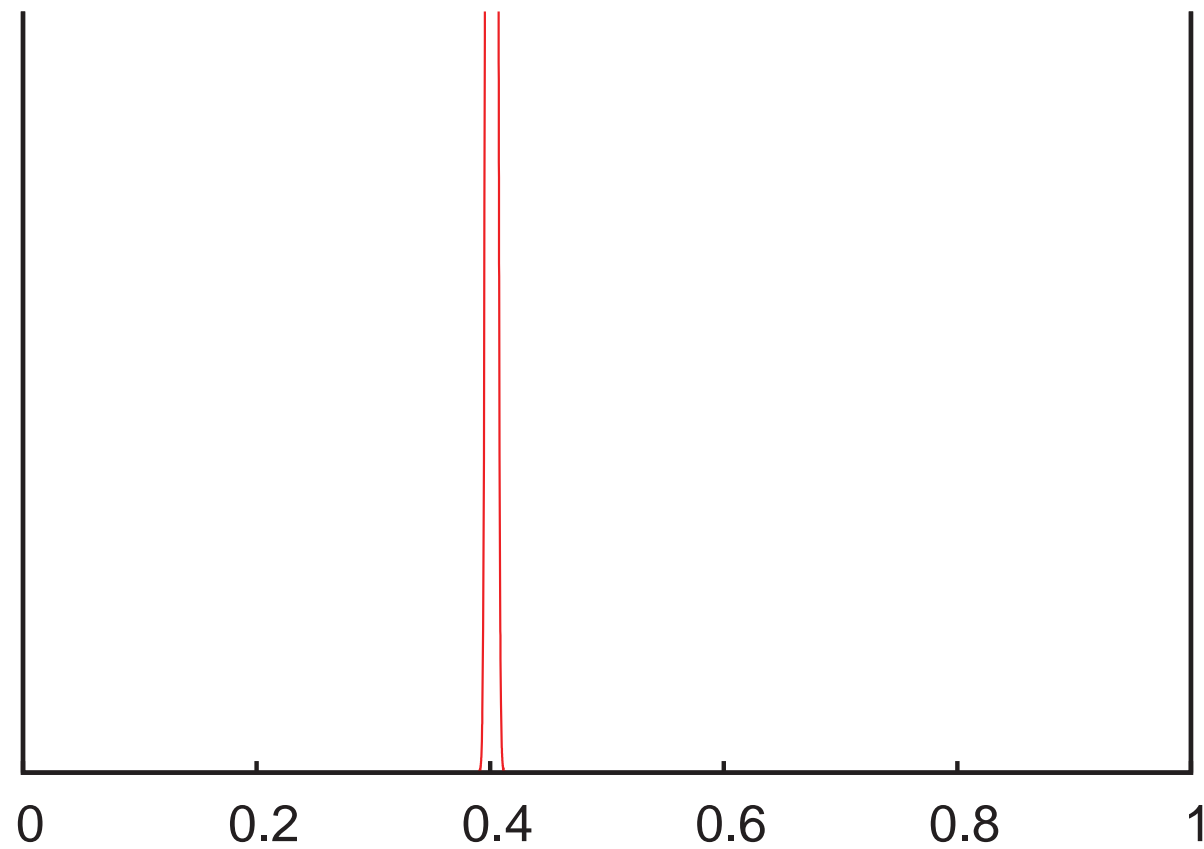
- 0 に近いものの割合は  $I(W)$  に近づく.
- 1 に近いものの割合は  $1 - I(W)$  に近づく.
- 0 にも 1 にも近くないものの割合は 0 に近づく.

# 数値例 (BEC, 消失確率: 0.4)

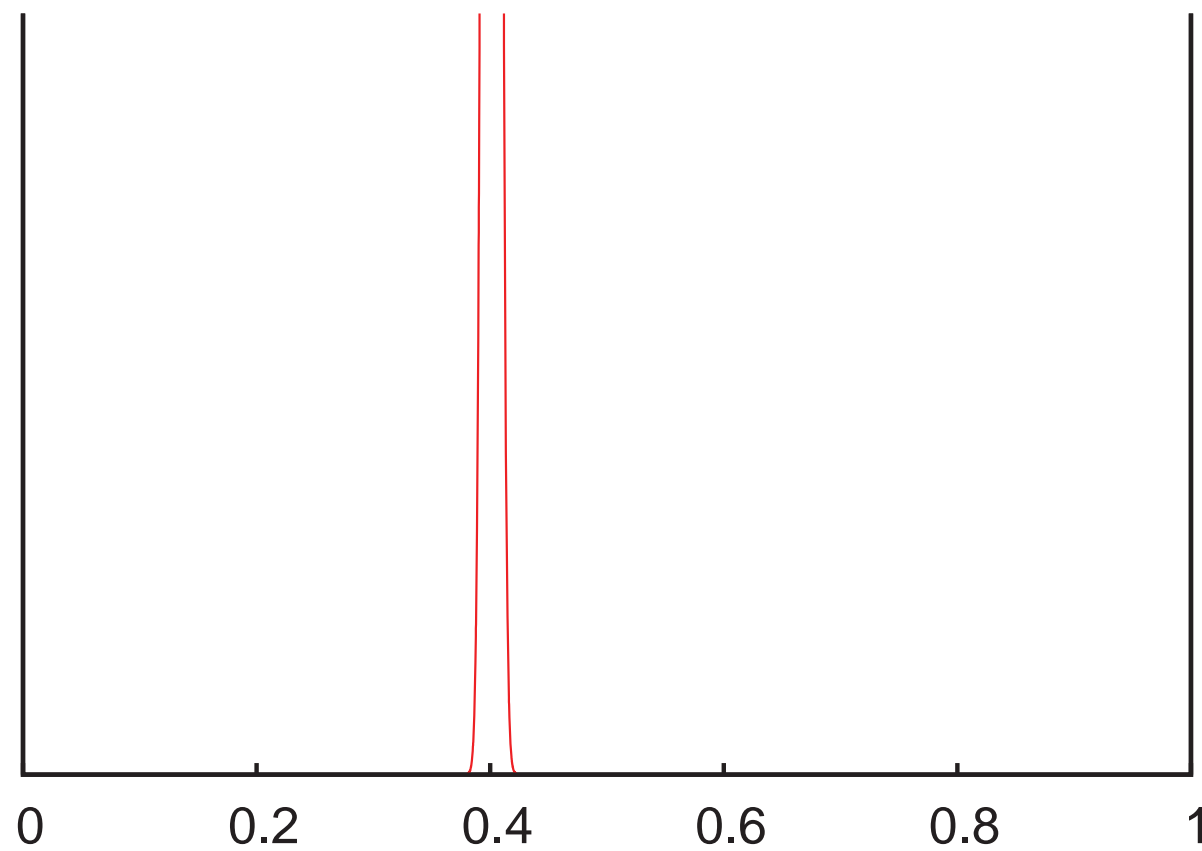


Bhattacharyya パラメータの累積分布  
( $n = 5, 10, 15, 20$ )

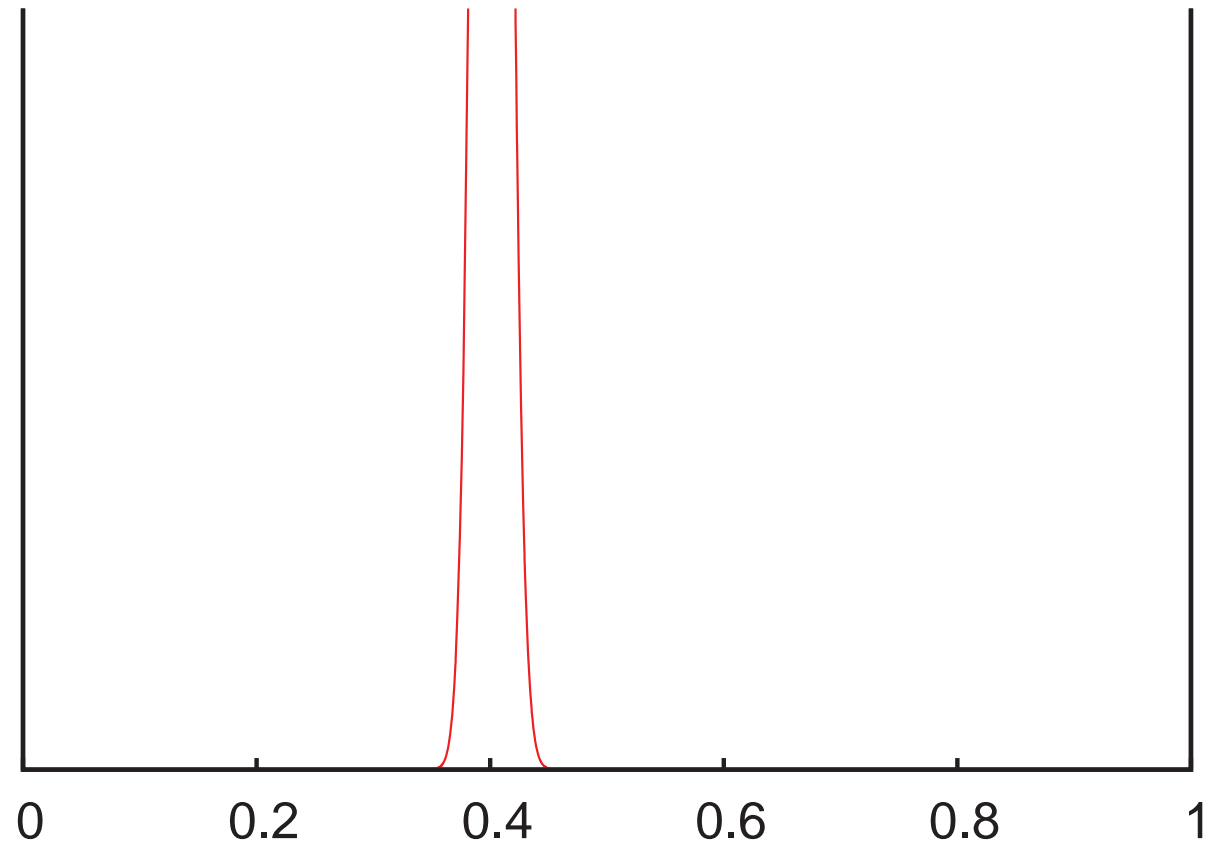
# 直観的には...



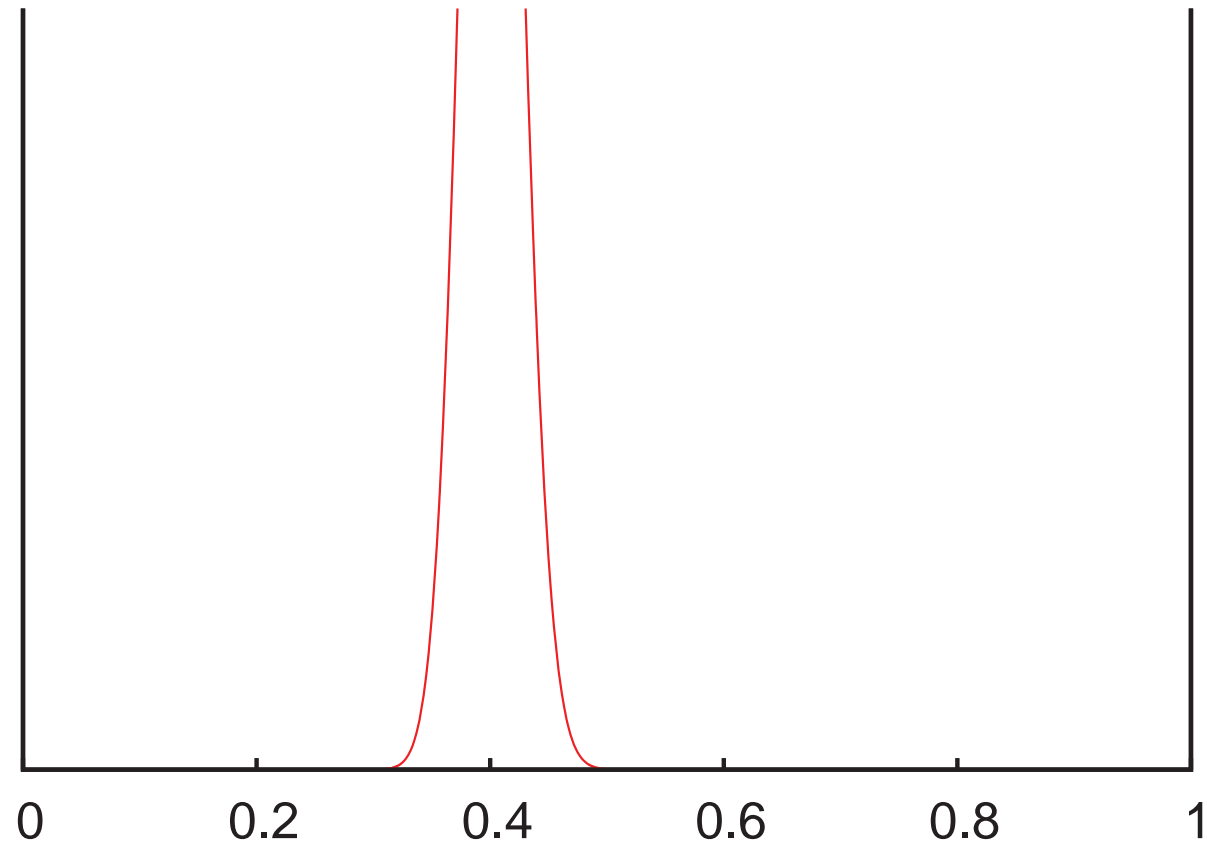
# 直観的には...



# 直観的には...

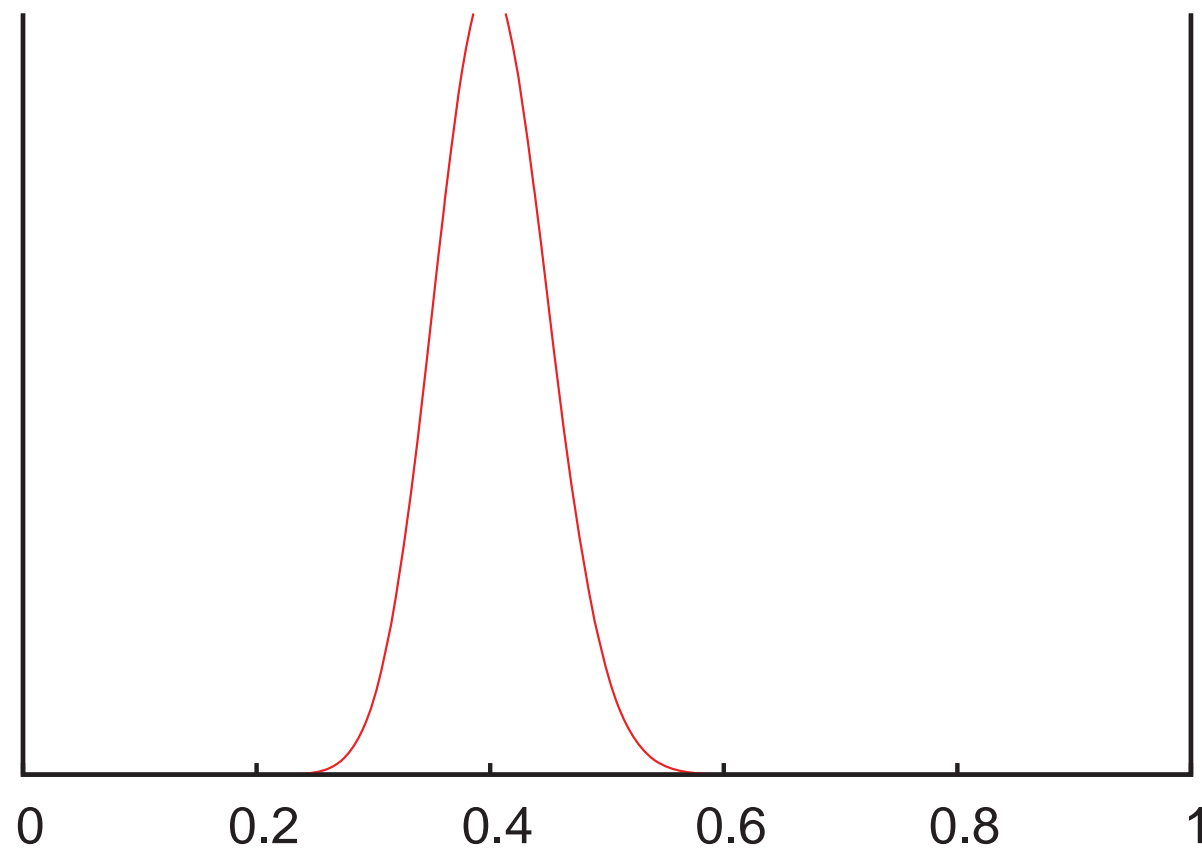


# 直観的には...

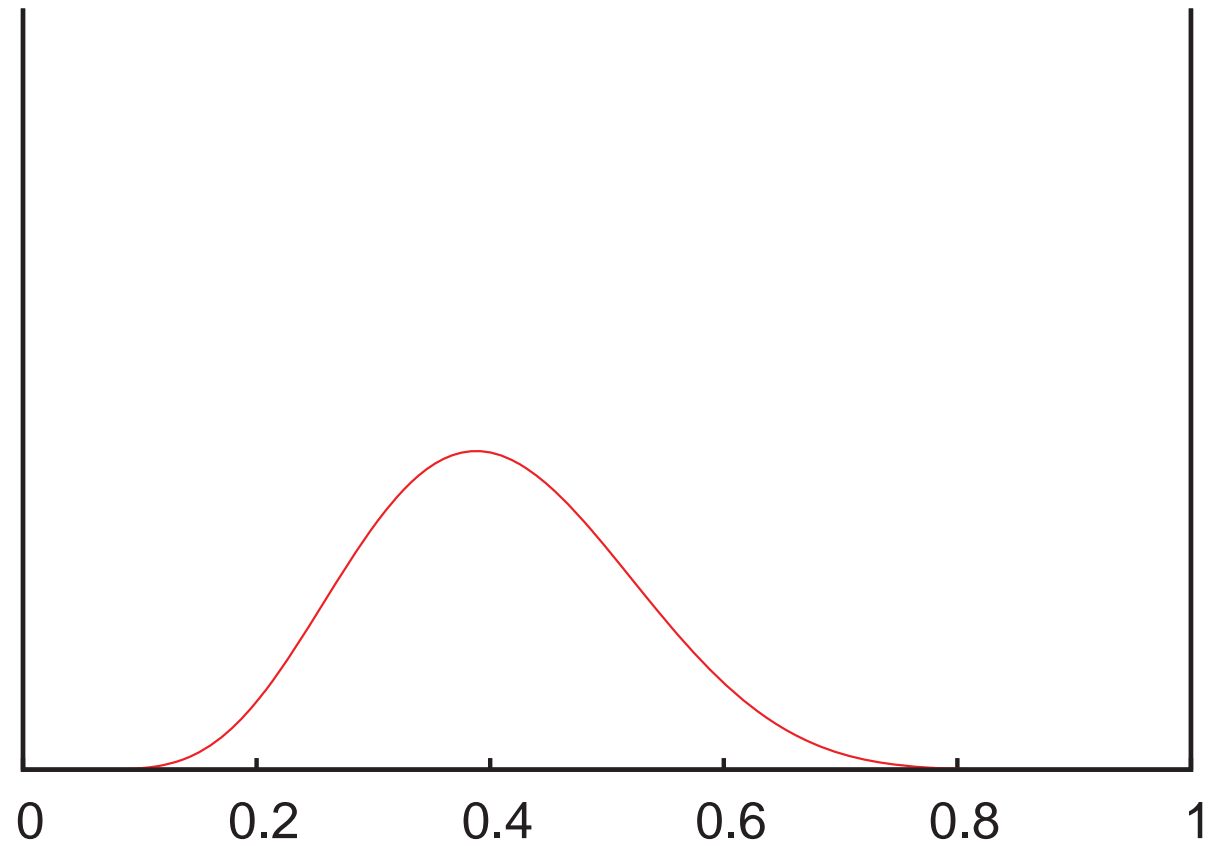




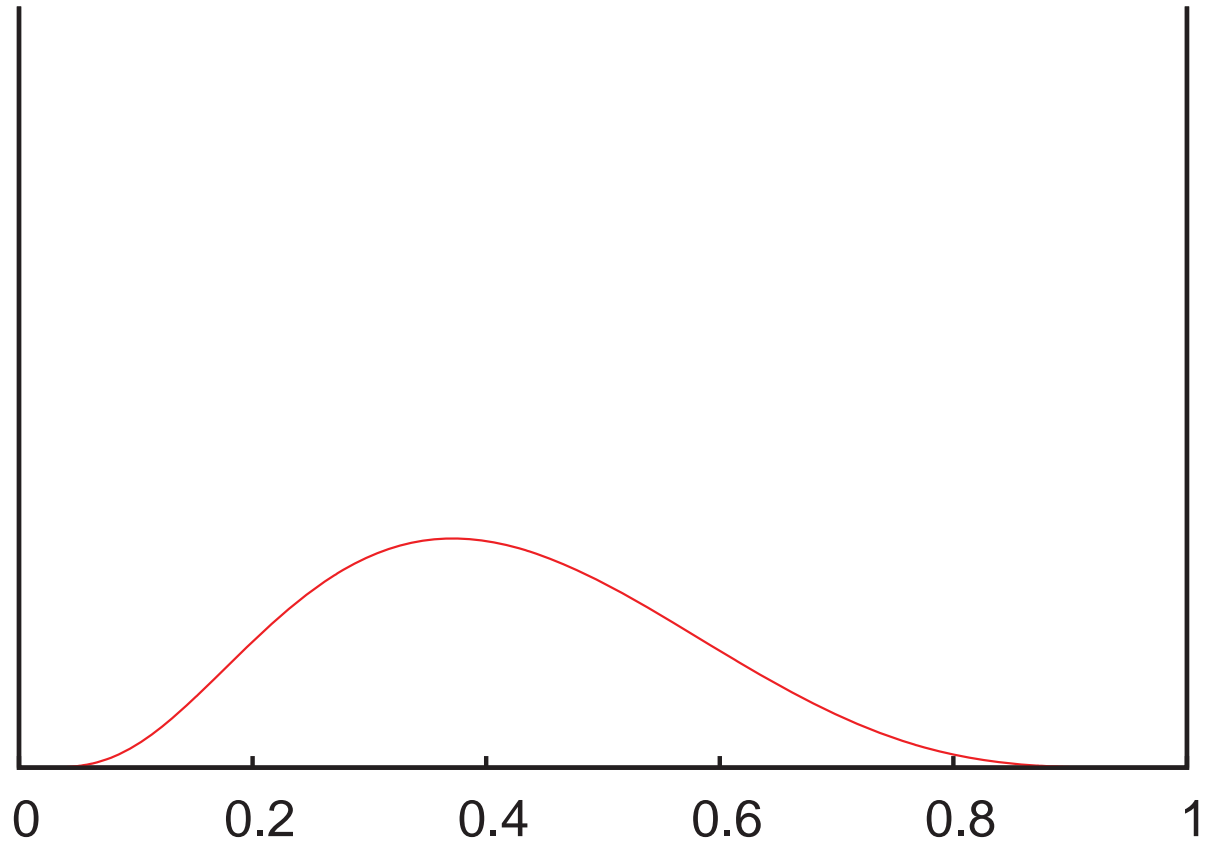
# 直観的には...



# 直観的には...

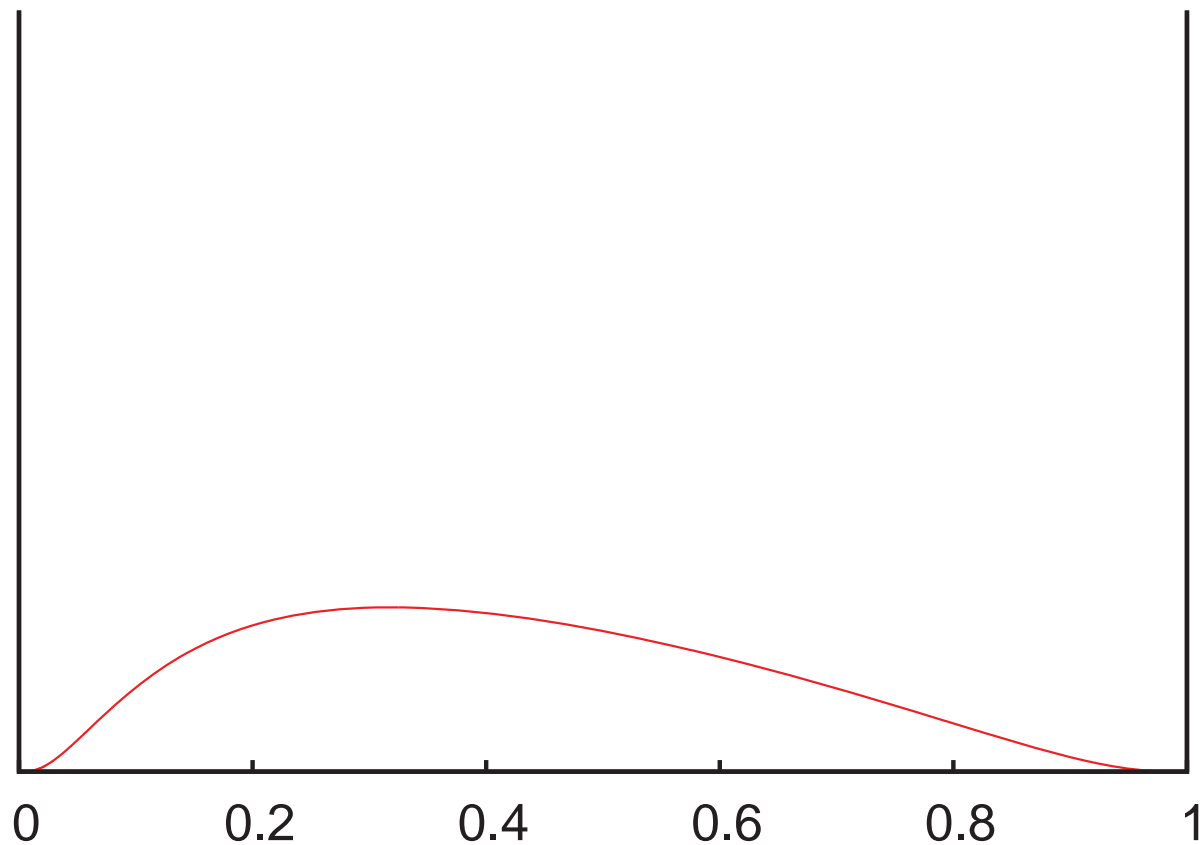


# 直観的には...

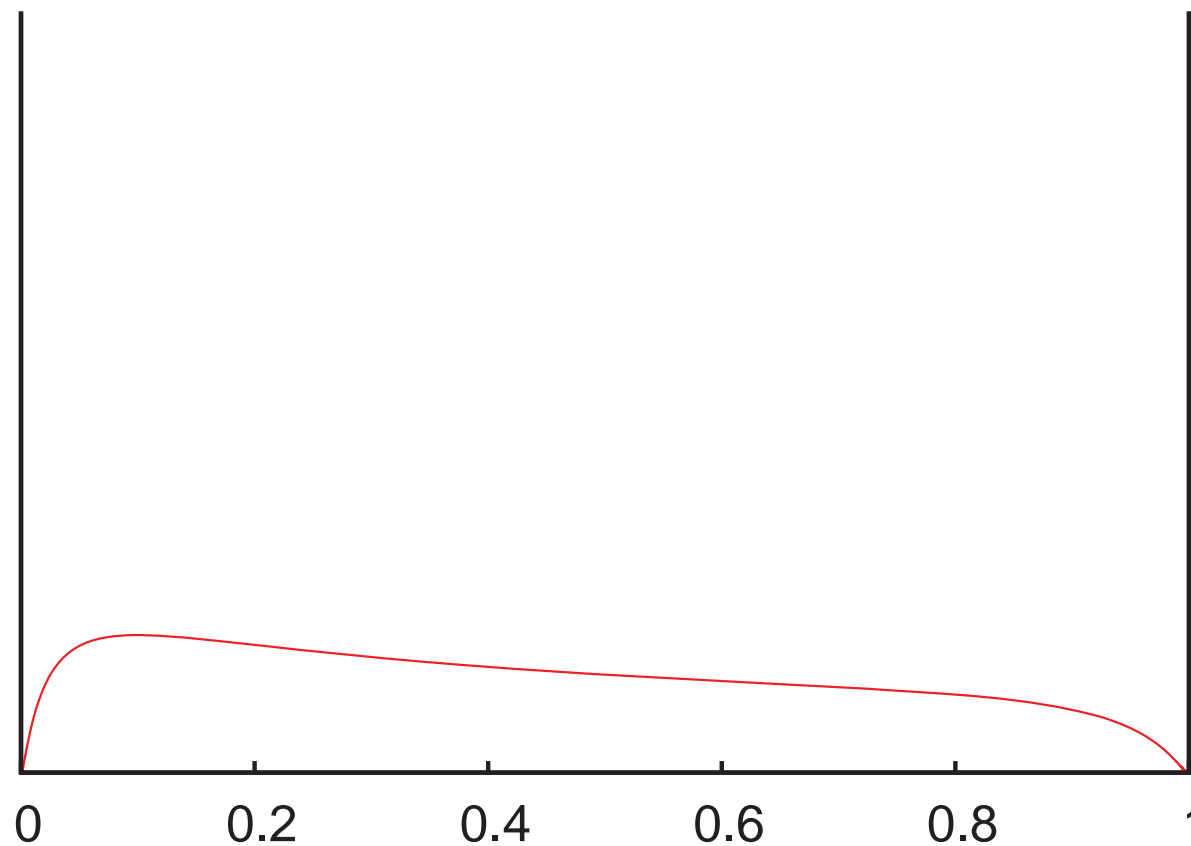


基礎的事項

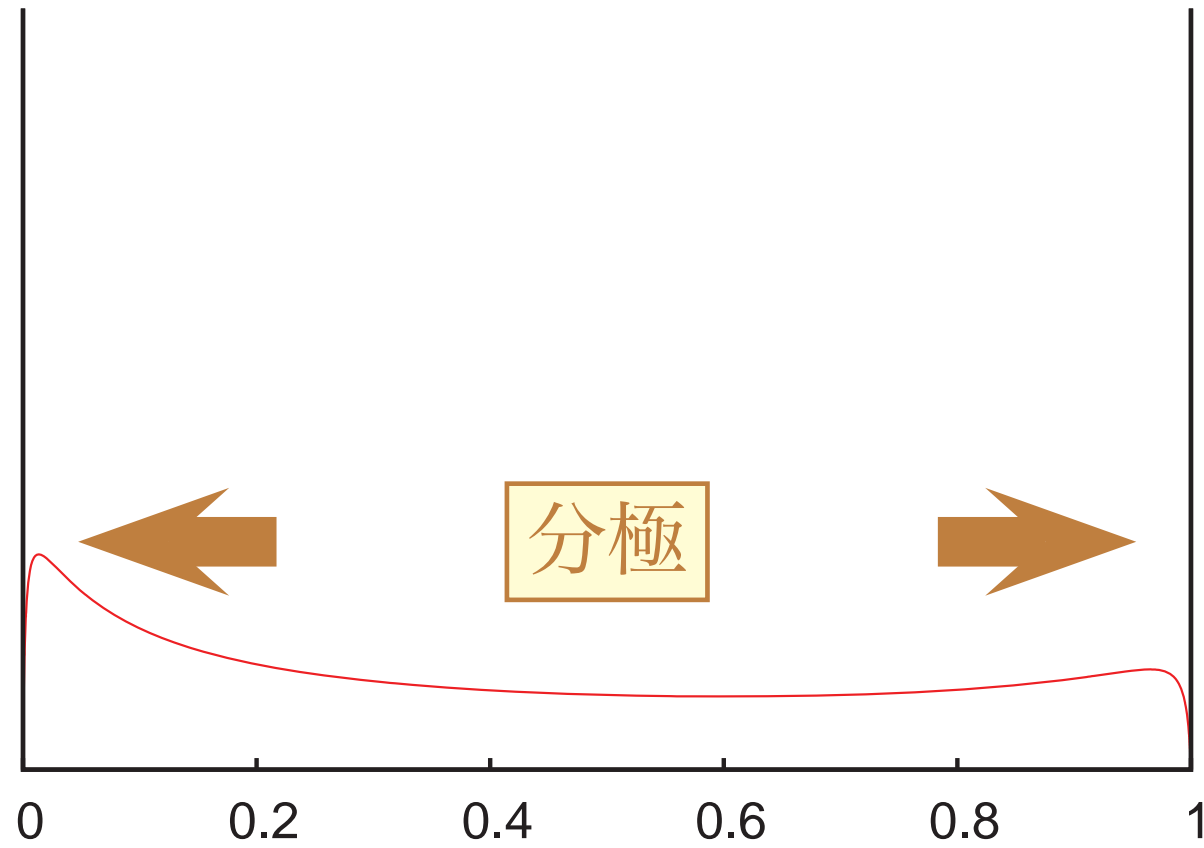
# 直観的には...



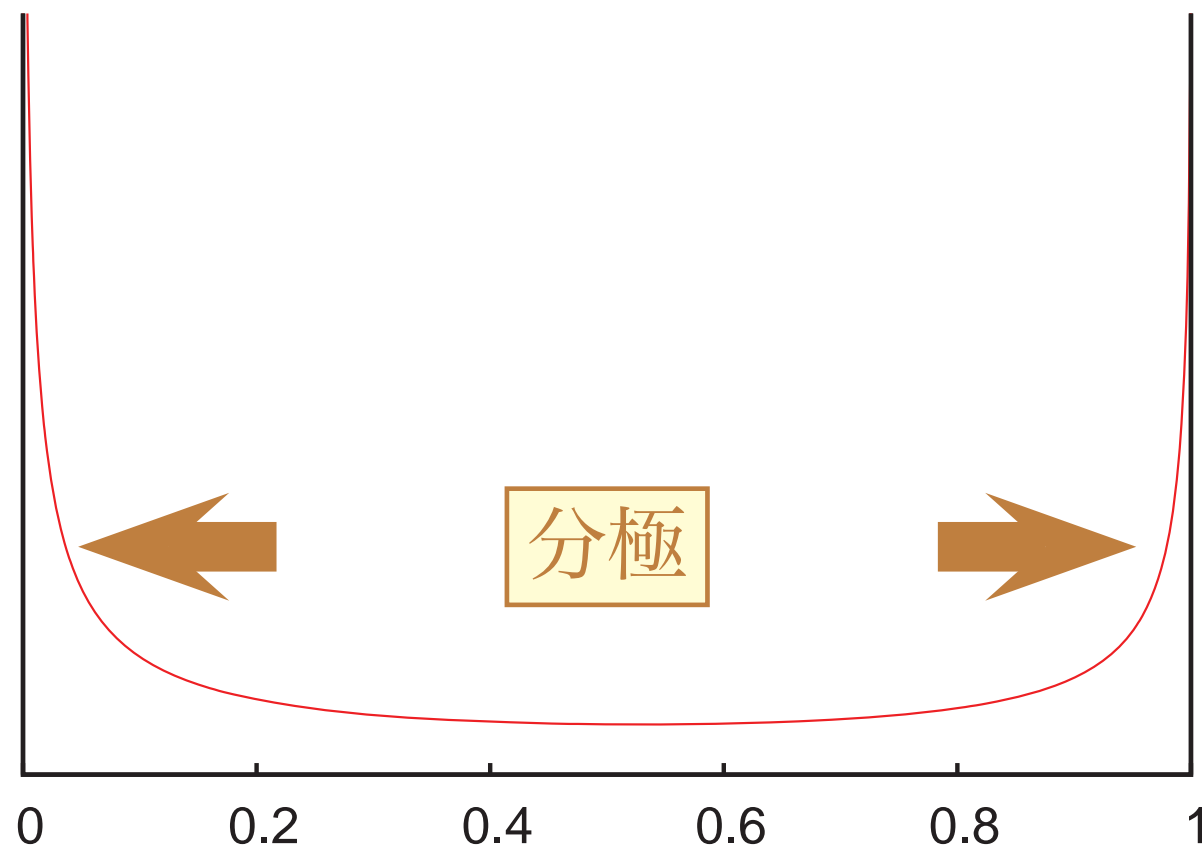
# 直観的には...



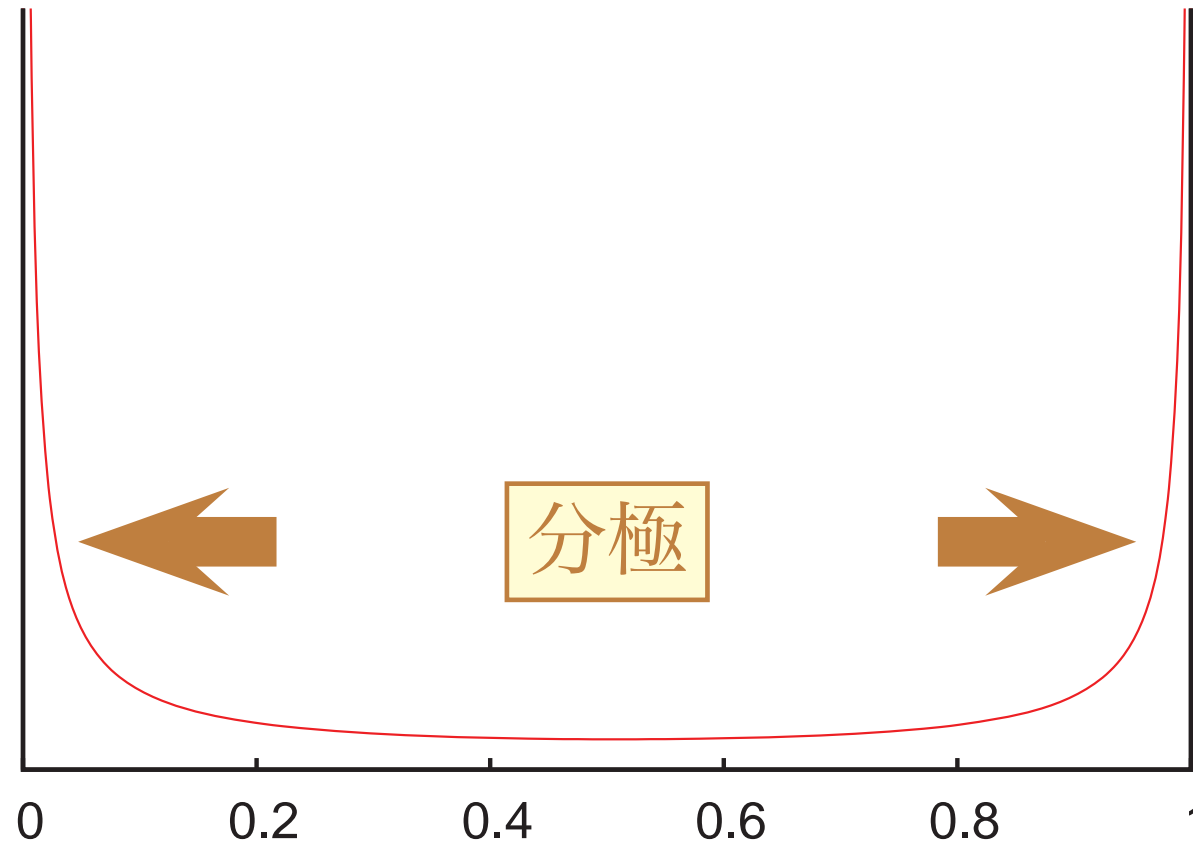
## 直観的には...



# 直観的には...

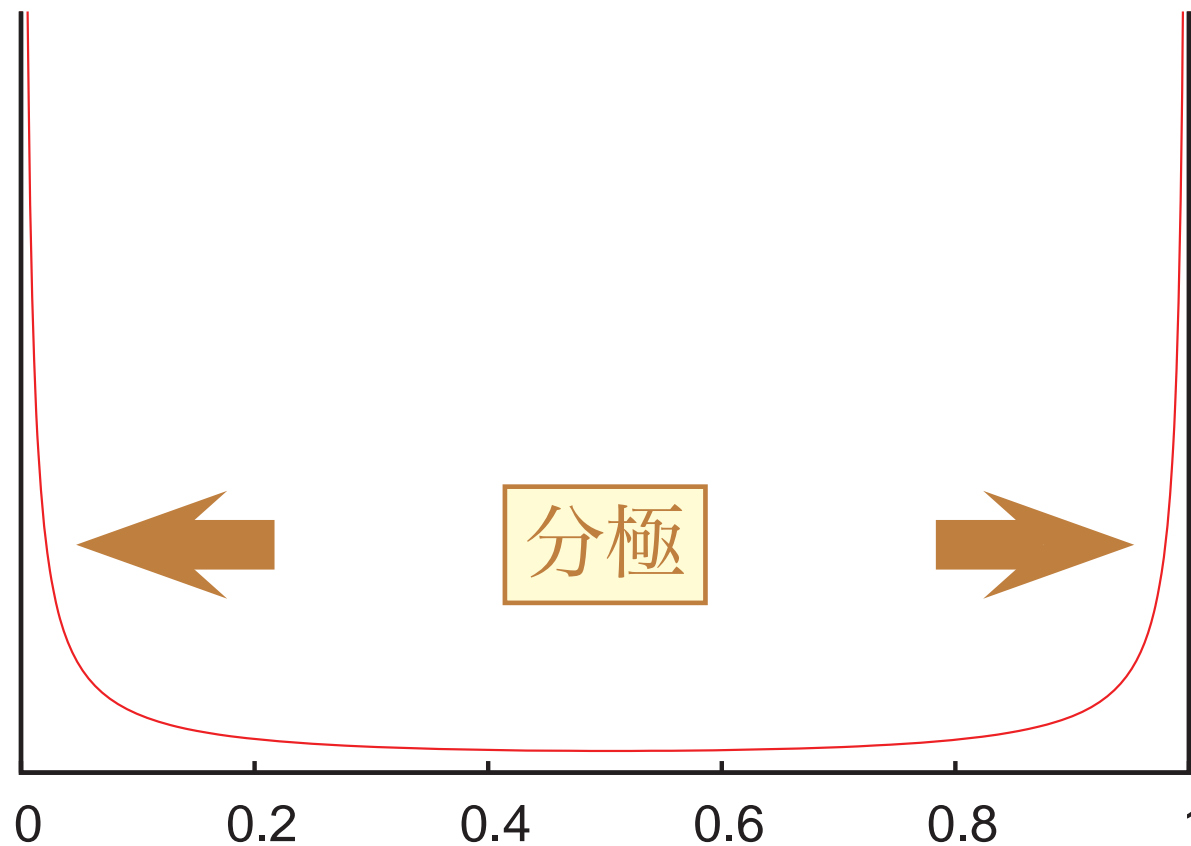


# 直観的には...

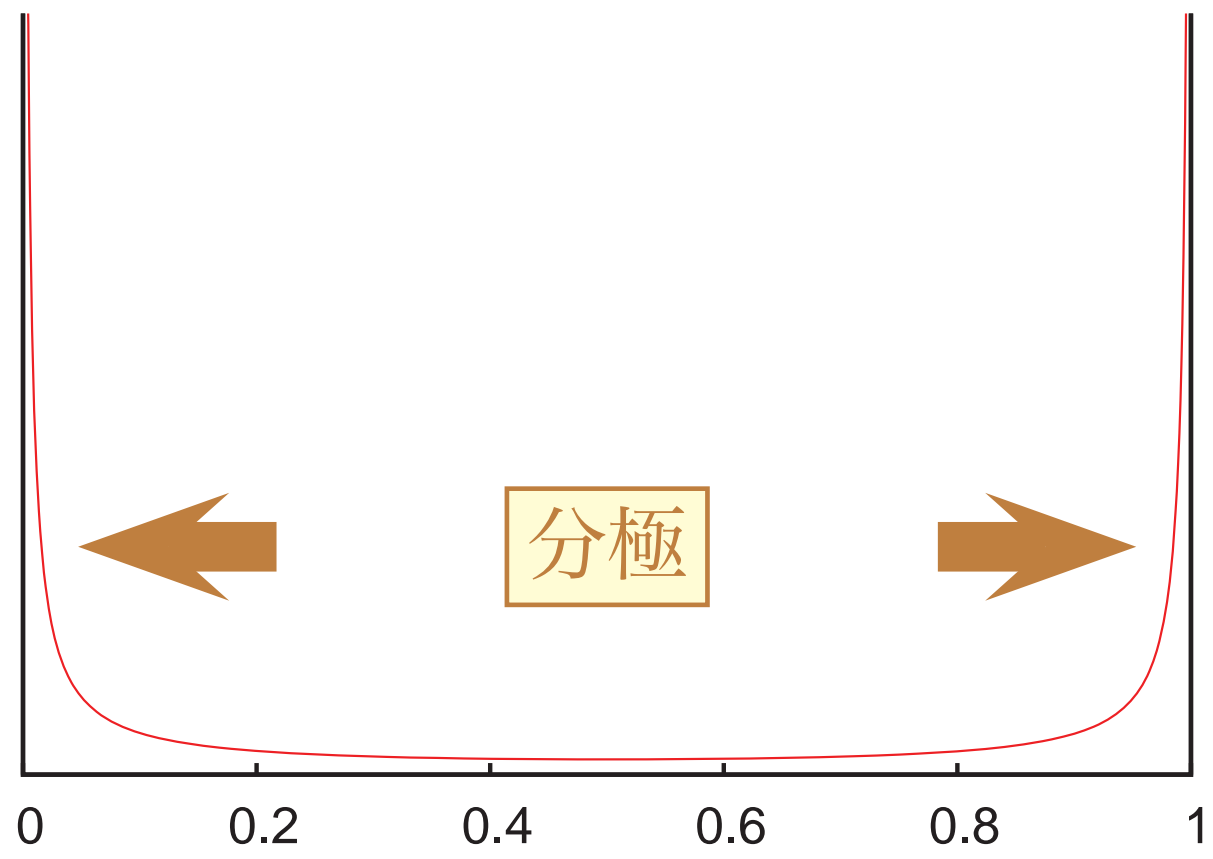




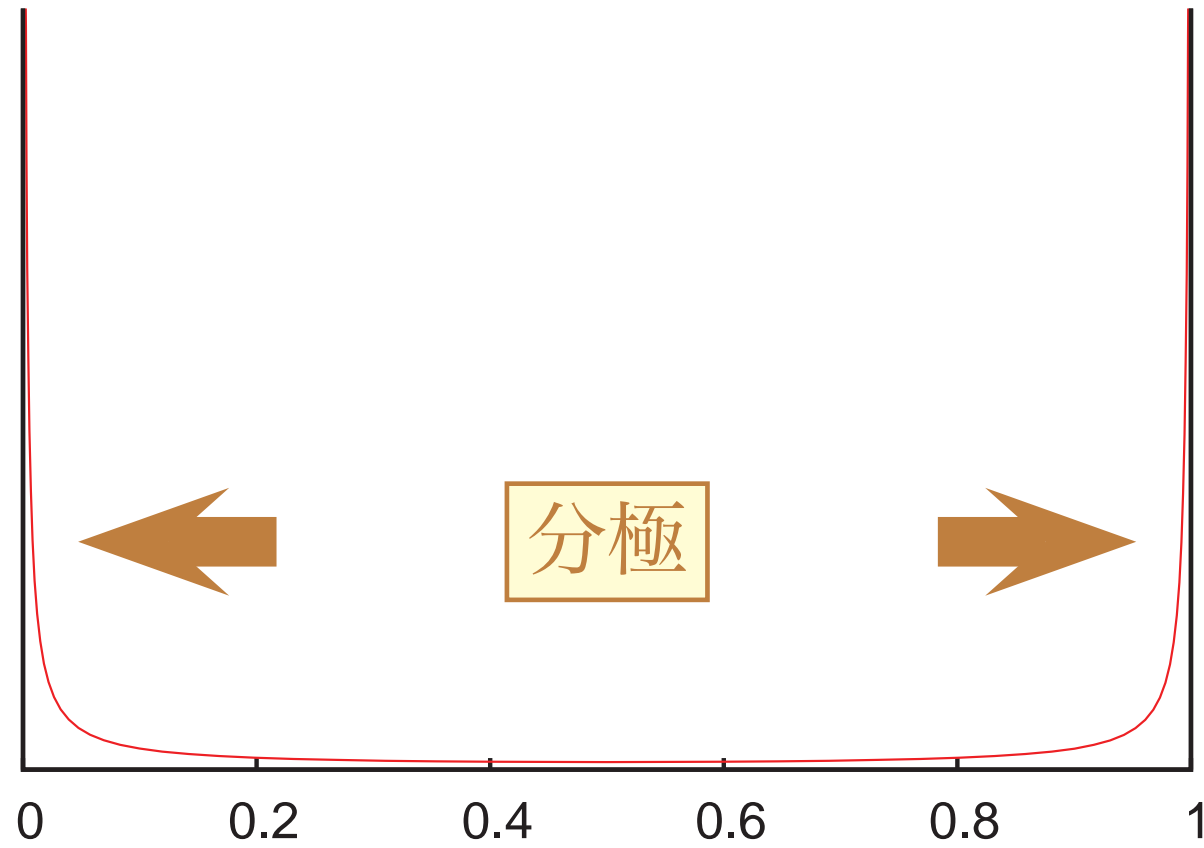
# 直観的には...



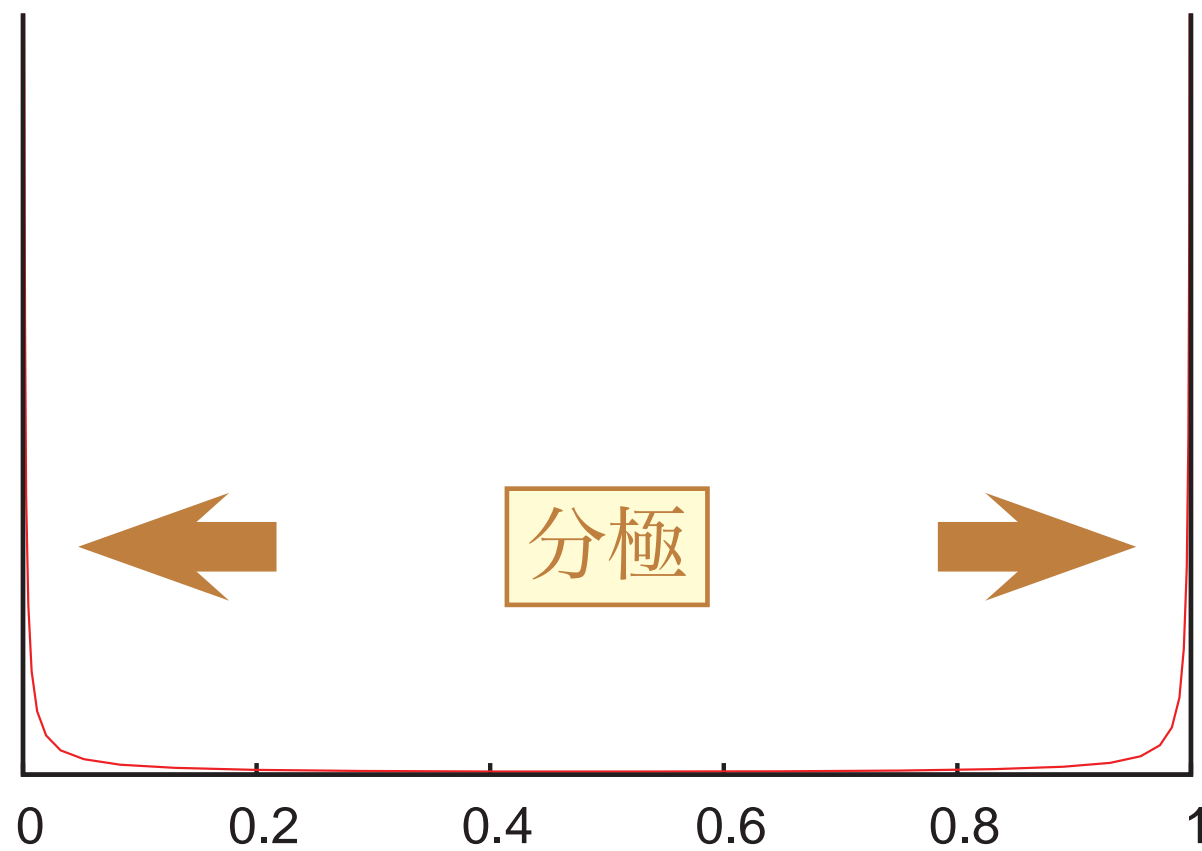
# 直観的には...



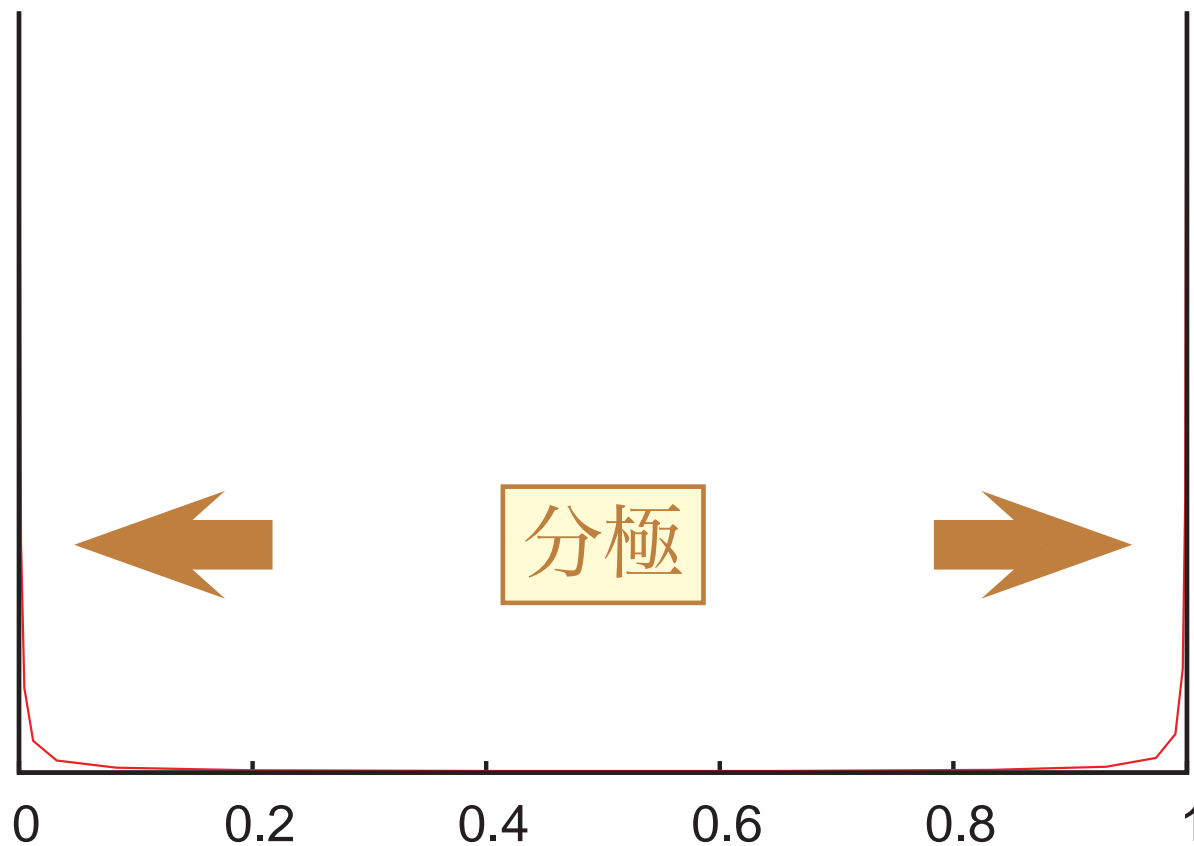
# 直観的には...



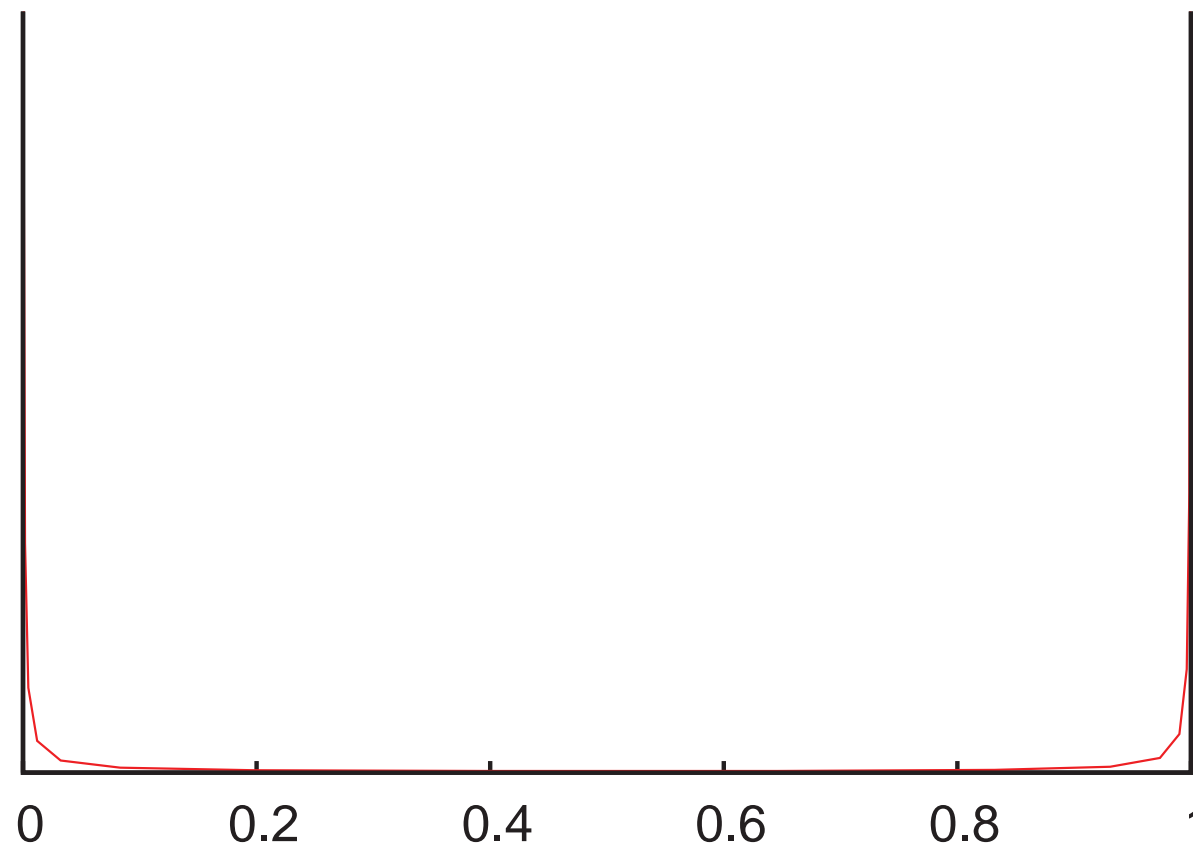
# 直観的には...



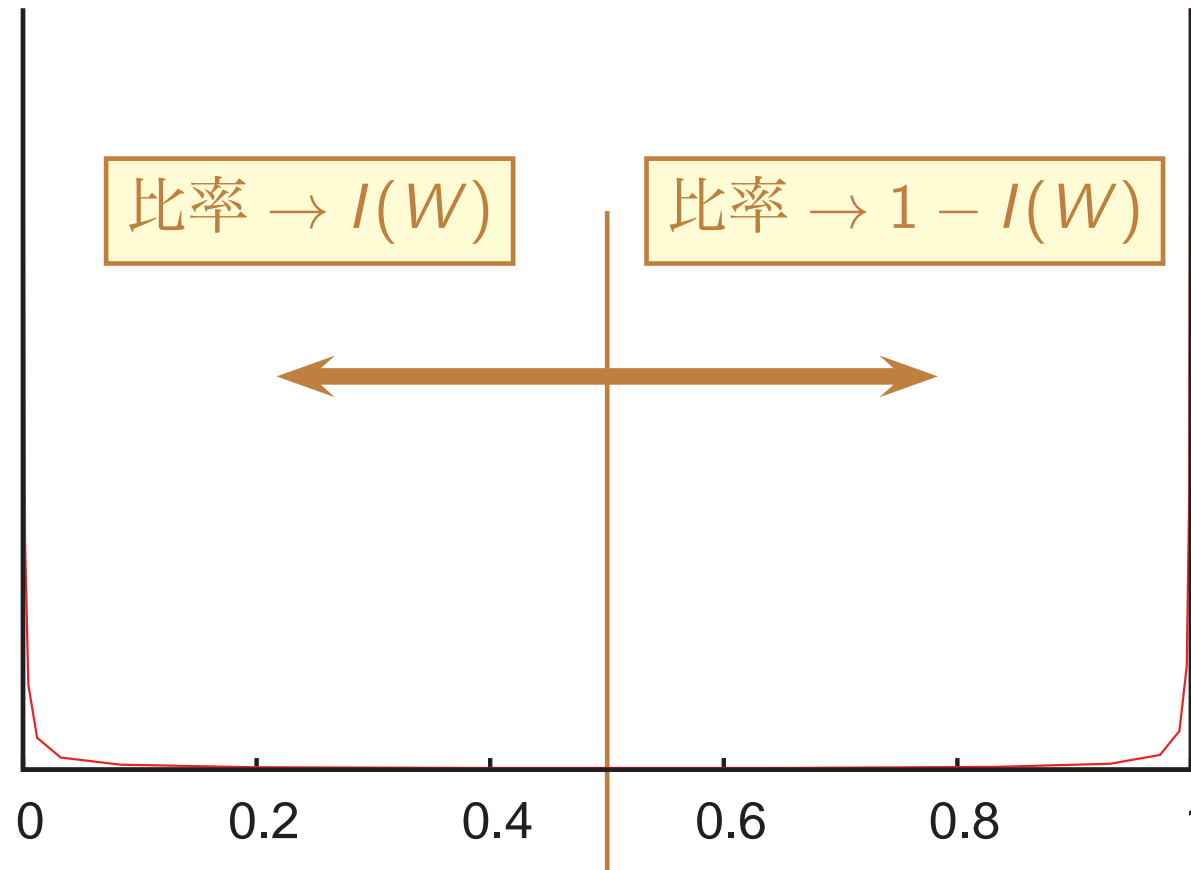
# 直観的には...



# 直観的には...



# 直観的には...



# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ **ポーラ符号**
  - 基礎的事項
  - **復号誤り率の上界**
  - スケーリング則
  - 拡張
- ④ まとめ



# Problem

## 復号誤り率の上界

$\Phi$  を  $n$  回適用して得られる  $2^n$  個の通信路のうち, Bhattacharyya パラメータが  $A$  以下の通信路の比率が  $R \Rightarrow$  符号長  $N = 2^n$ , 符号化率  $R$  で, 逐次除去復号によるブロック誤り率が  $P_B \leq NR \times A$  であるポーラ符号が存在.

## 対称通信路容量の達成および復号誤り率の漸近形

$N \rightarrow \infty$  で,  $A = o(N^{-1})$  に対し Bhattacharyya パラメータが  $A$  以下の通信路の比率が  $I(W) - \epsilon$  以上となることを示す必要がある.

- $A = O(N^{-5/4}) \Rightarrow P_B = O(N^{-1/4})$  (Arıkan, 2009)
- $0 < \beta < 1/2$  をみたす任意の  $\beta$  に対して  $A = o(2^{-2^{\beta n}}) \Rightarrow P_B = o(2^{-2^{\beta n}})$  (Arıkan-Telatar, 2009)

# Problem

## 復号誤り率の上界

$\Phi$  を  $n$  回適用して得られる  $2^n$  個の通信路のうち, Bhattacharyya パラメータが  $A$  以下の通信路の比率が  $R \Rightarrow$  符号長  $N = 2^n$ , 符号化率  $R$  で, 逐次除去復号によるブロック誤り率が  $P_B \leq NR \times A$  であるポーラ符号が存在.

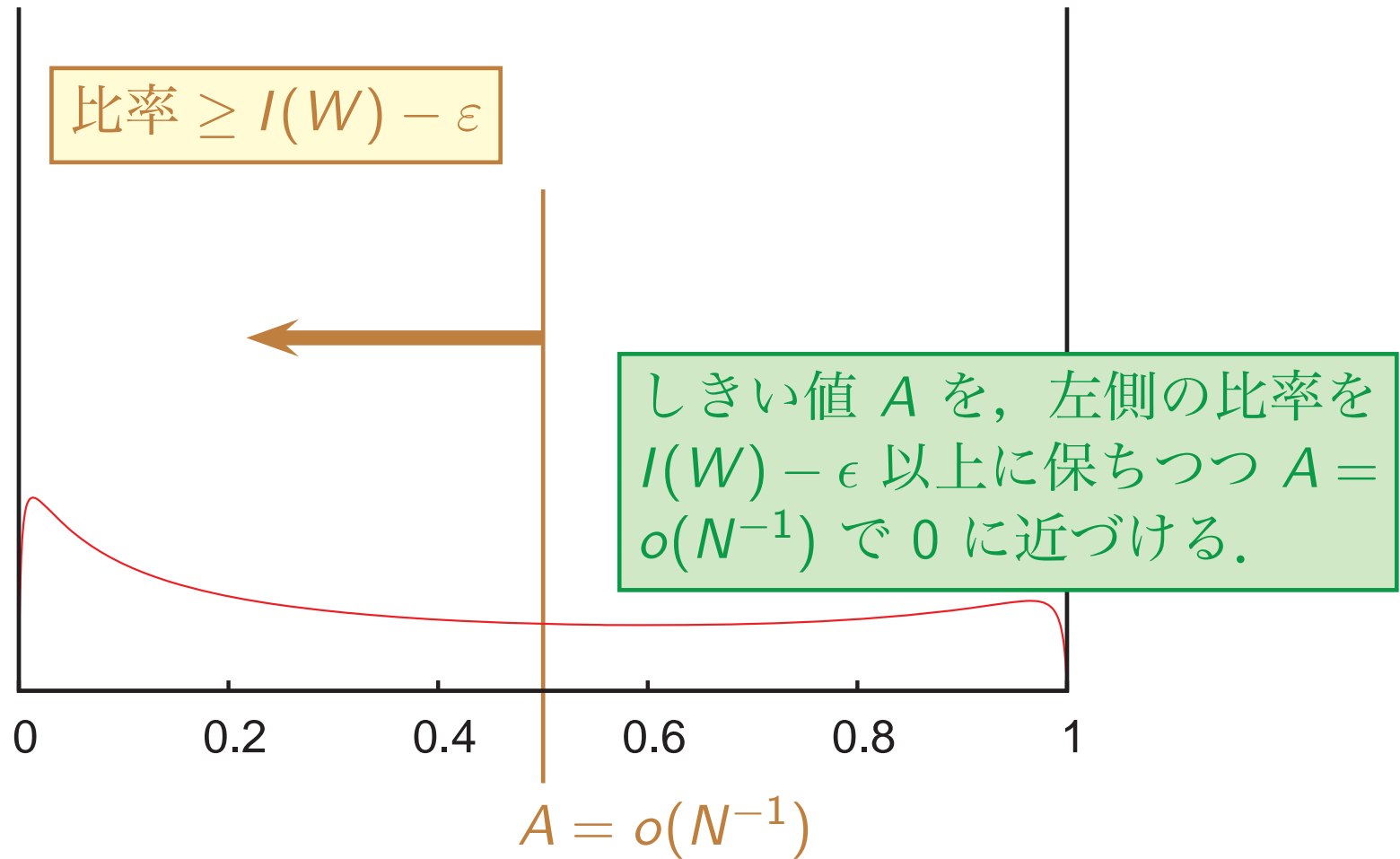
## 対称通信路容量の達成および復号誤り率の漸近形

$N \rightarrow \infty$  で,  $A = o(N^{-1})$  に対し Bhattacharyya パラメータが  $A$  以下の通信路の比率が  $I(W) - \epsilon$  以上となることを示す必要がある.

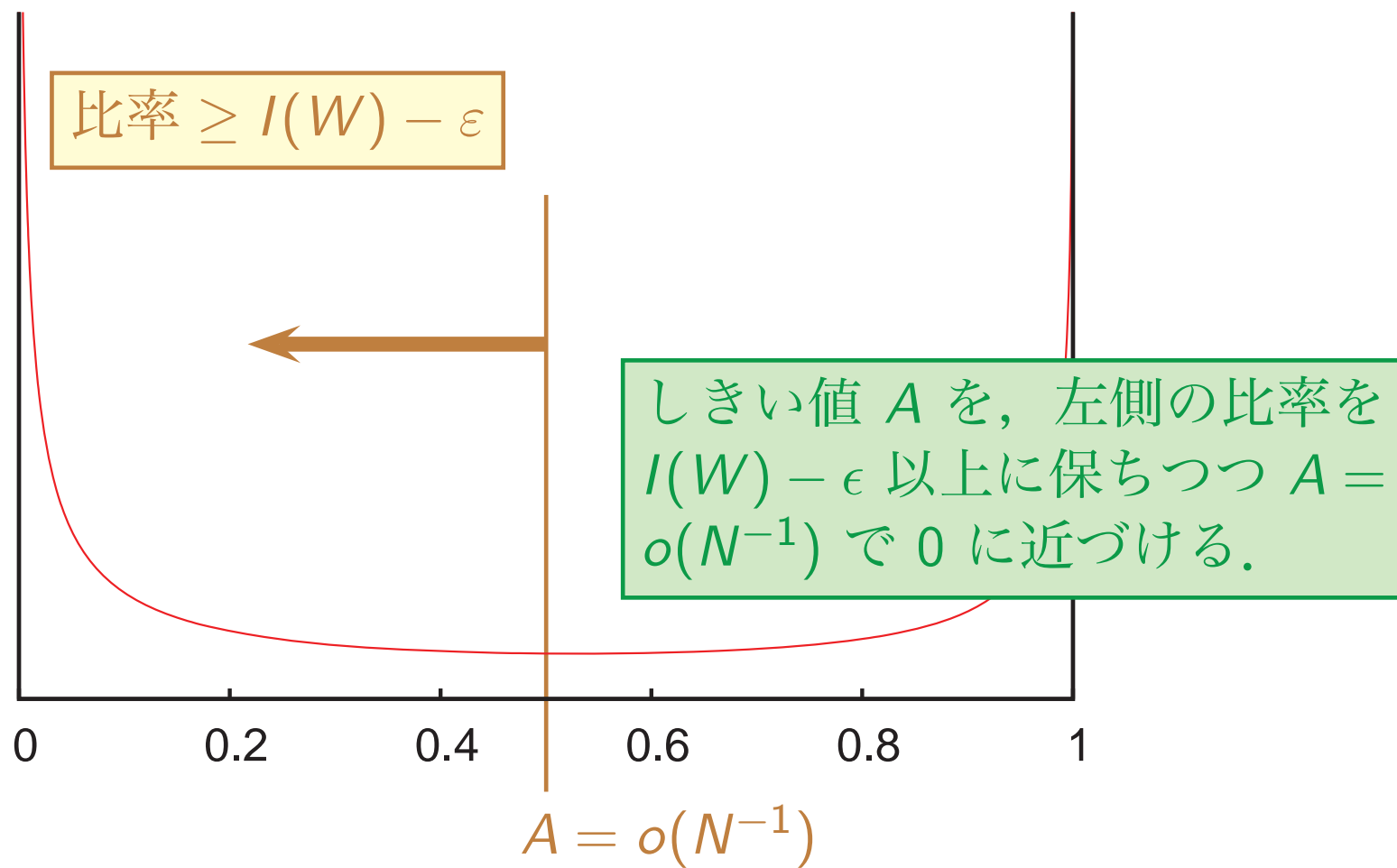
- $A = O(N^{-5/4}) \Rightarrow P_B = O(N^{-1/4})$  (Arıkan, 2009)
- $0 < \beta < 1/2$  をみたく任意の  $\beta$  に対して  $A = o(2^{-2^{\beta n}}) \Rightarrow P_B = o(2^{-2^{\beta n}})$  (Arıkan-Telatar, 2009)



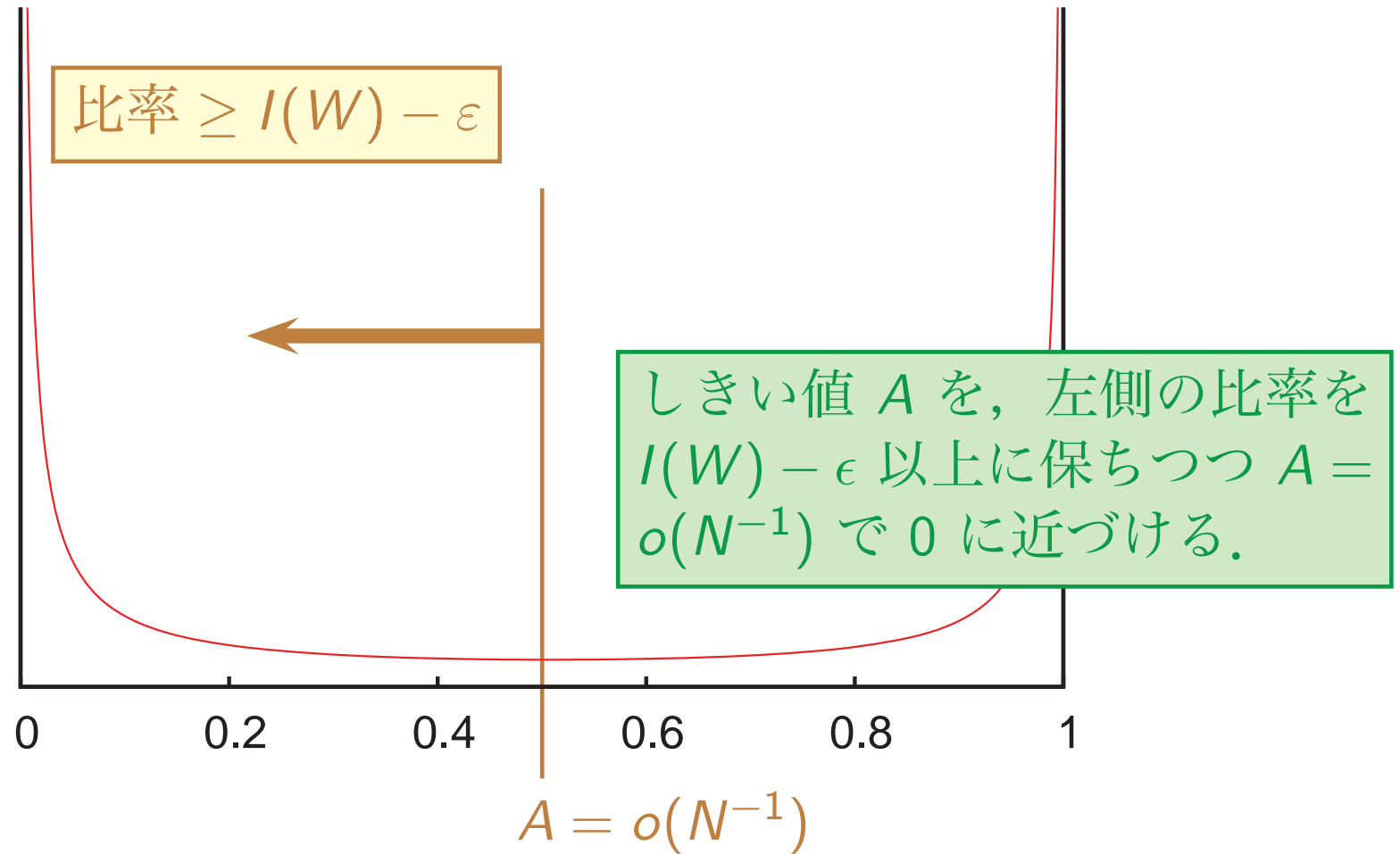
# 直観的には...



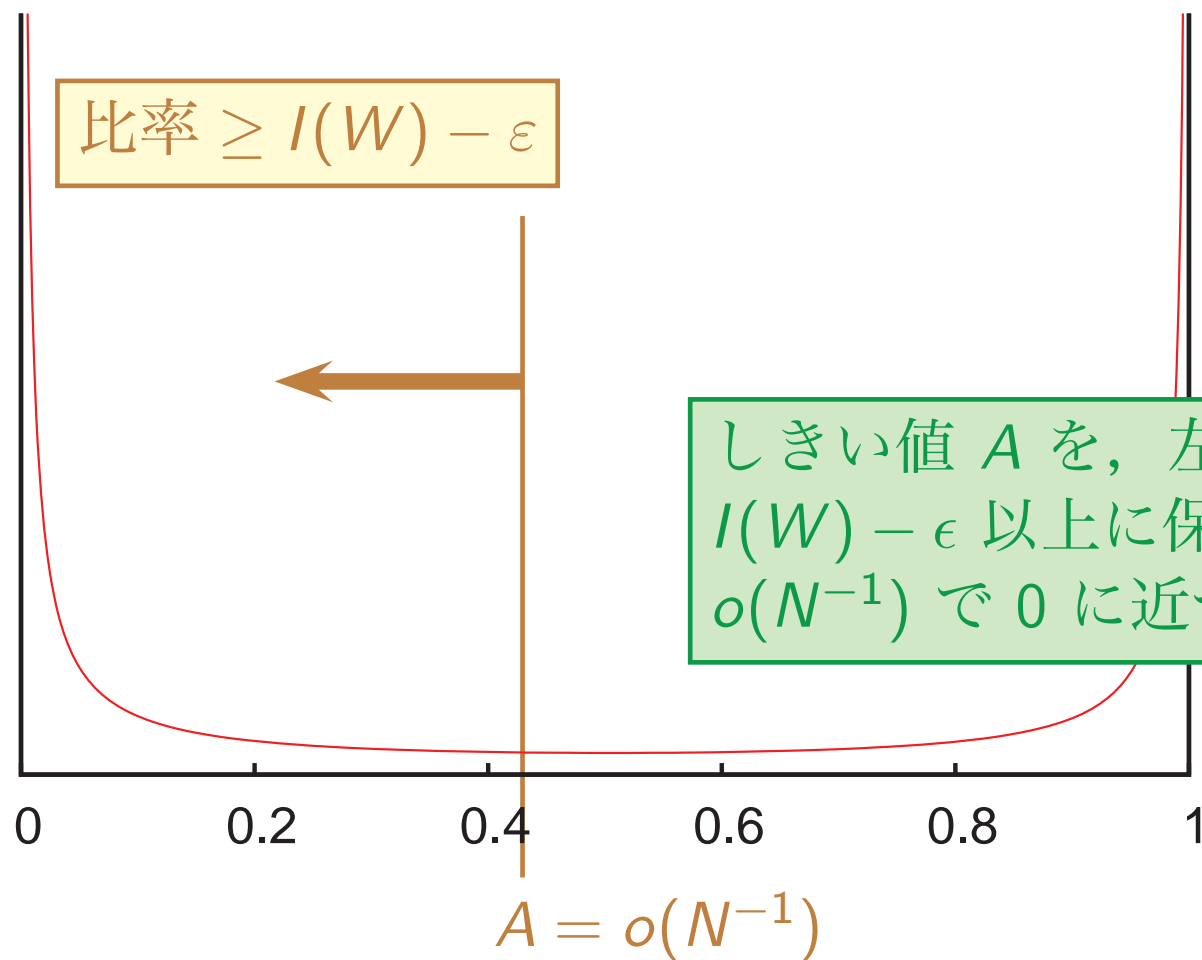
# 直観的には...



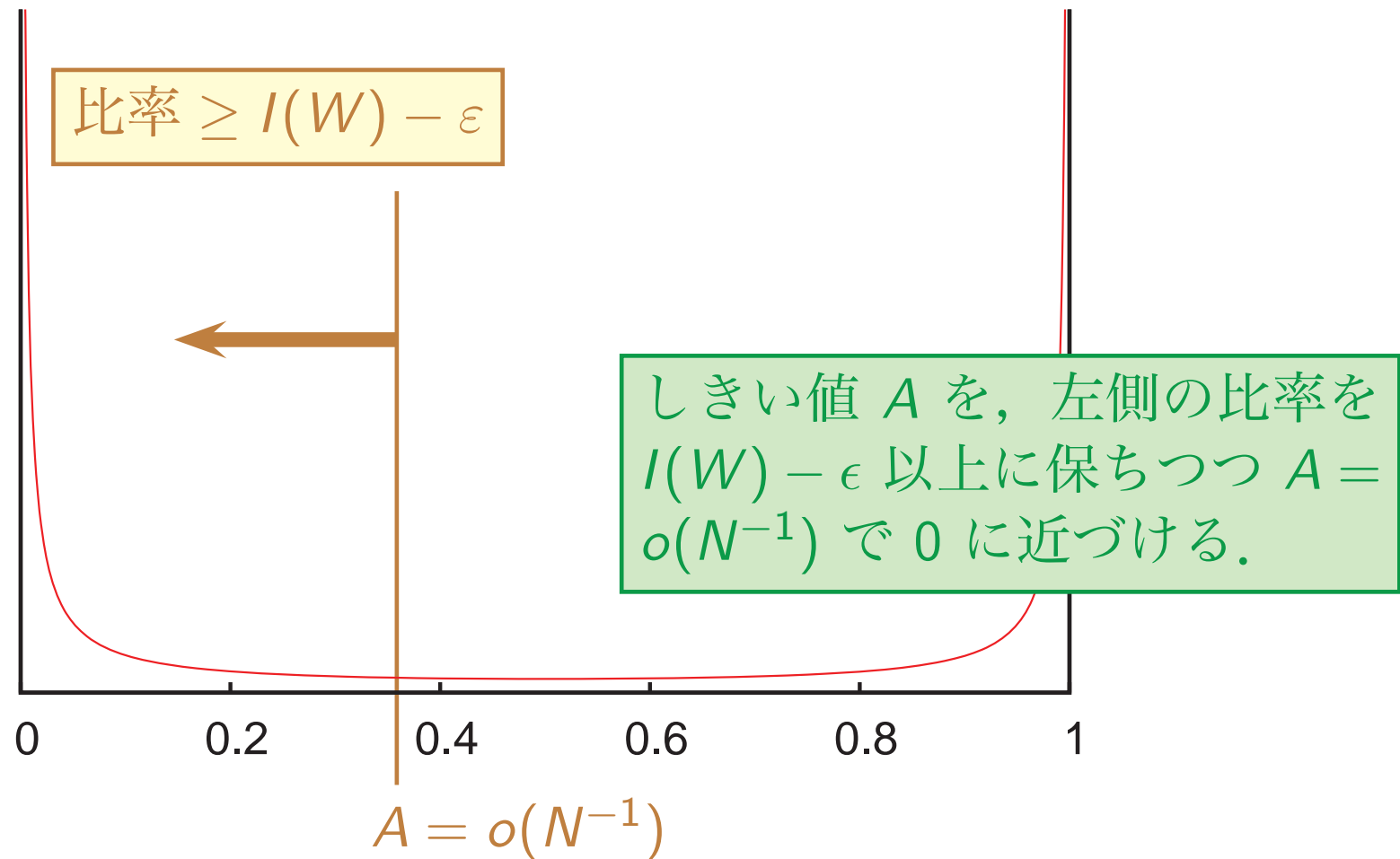
# 直観的には...



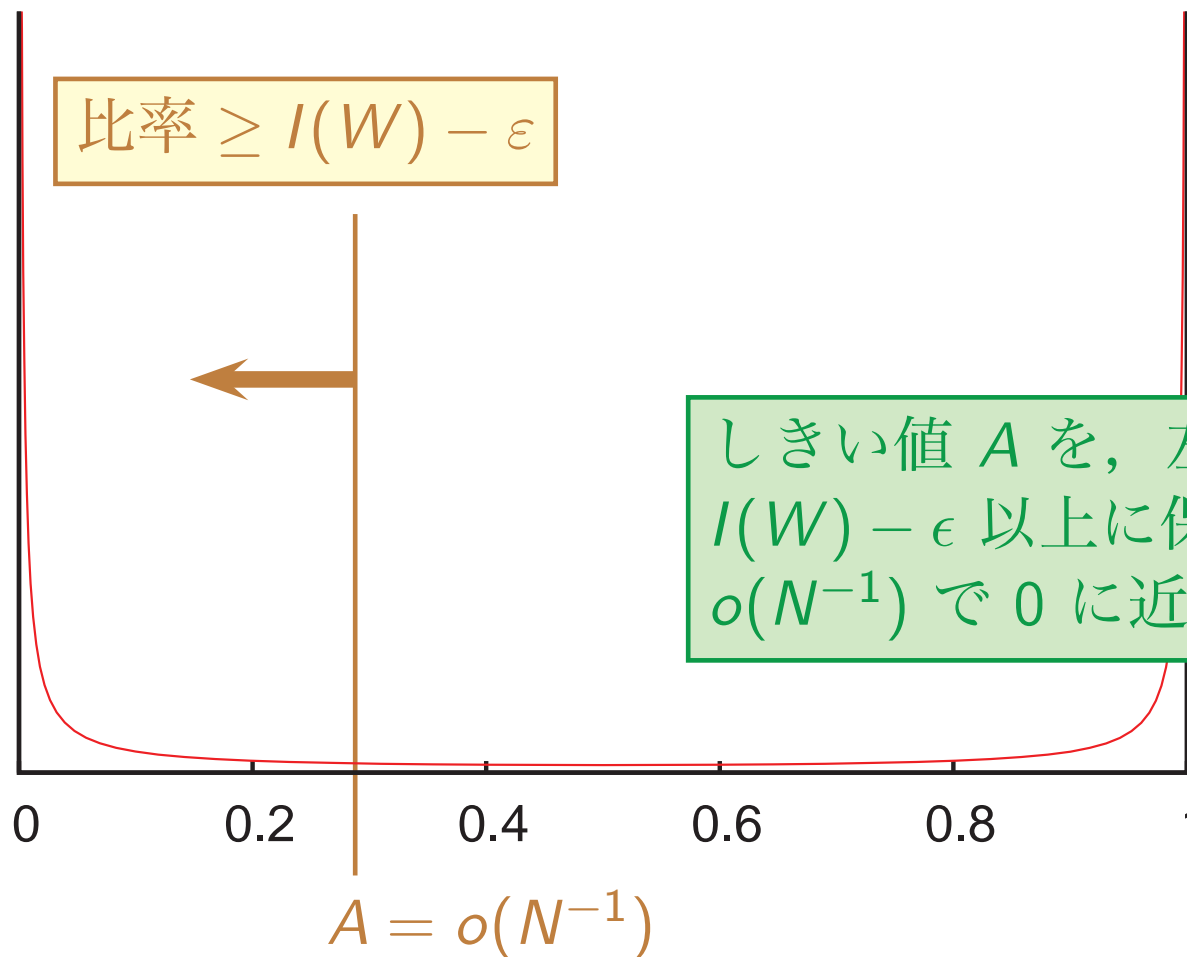
## 直観的には...



## 直観的には...

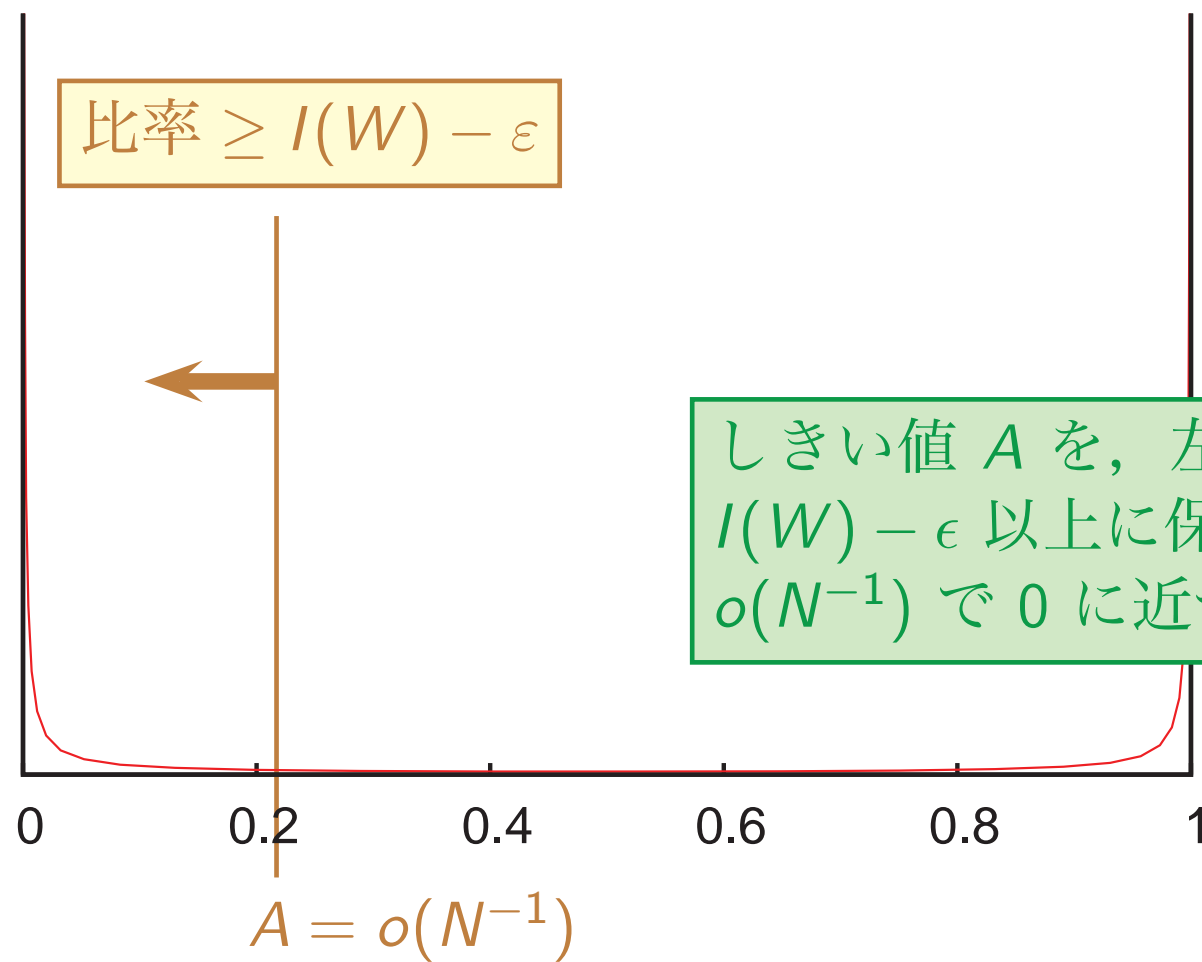


# 直観的には...





# 直観的には...



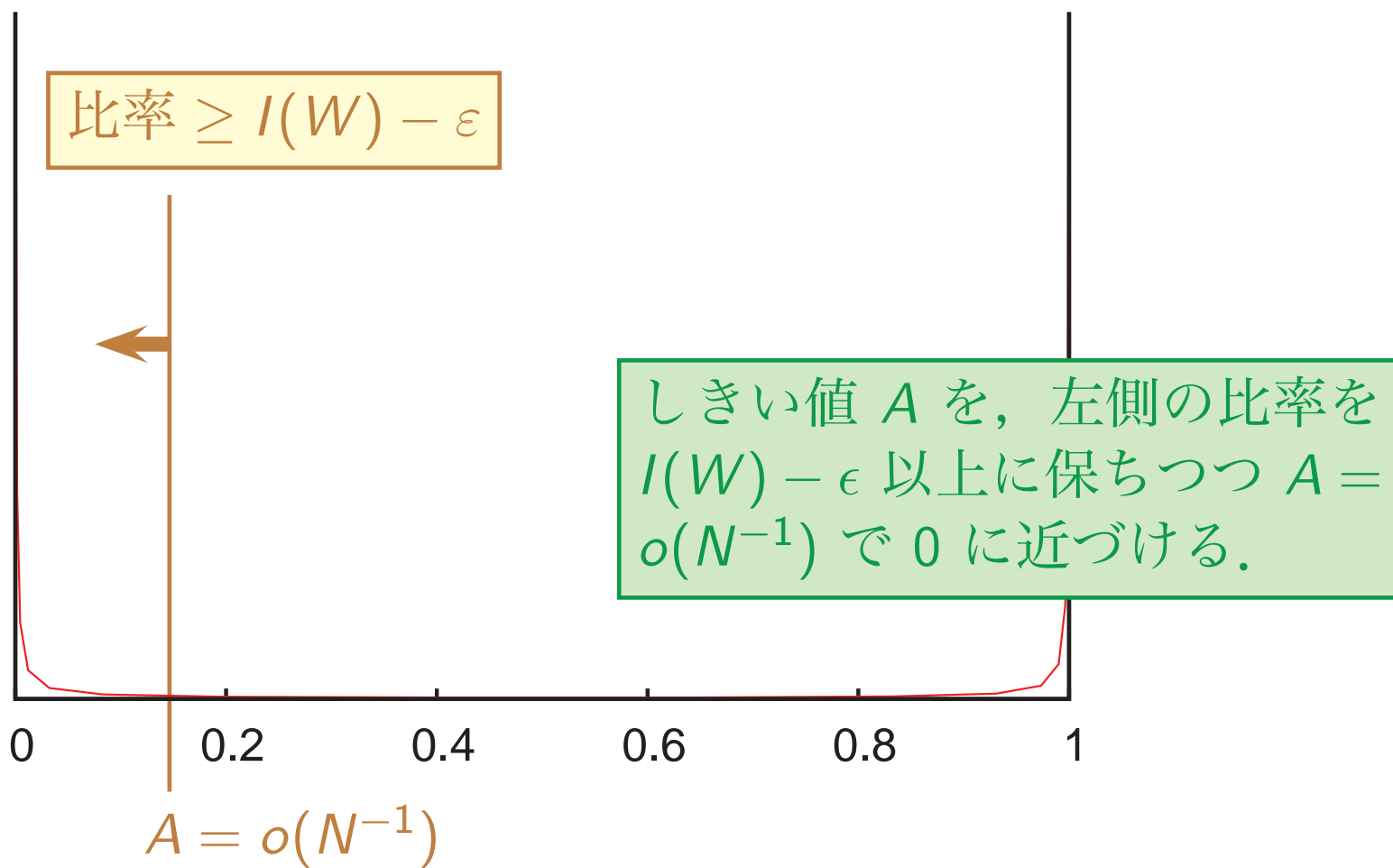
比率  $\geq I(W) - \epsilon$

しきい値  $A$  を, 左側の比率を  $I(W) - \epsilon$  以上に保ちつつ  $A = o(N^{-1})$  で 0 に近づける.

$A = o(N^{-1})$

復号誤り率の上界

# 直観的には...



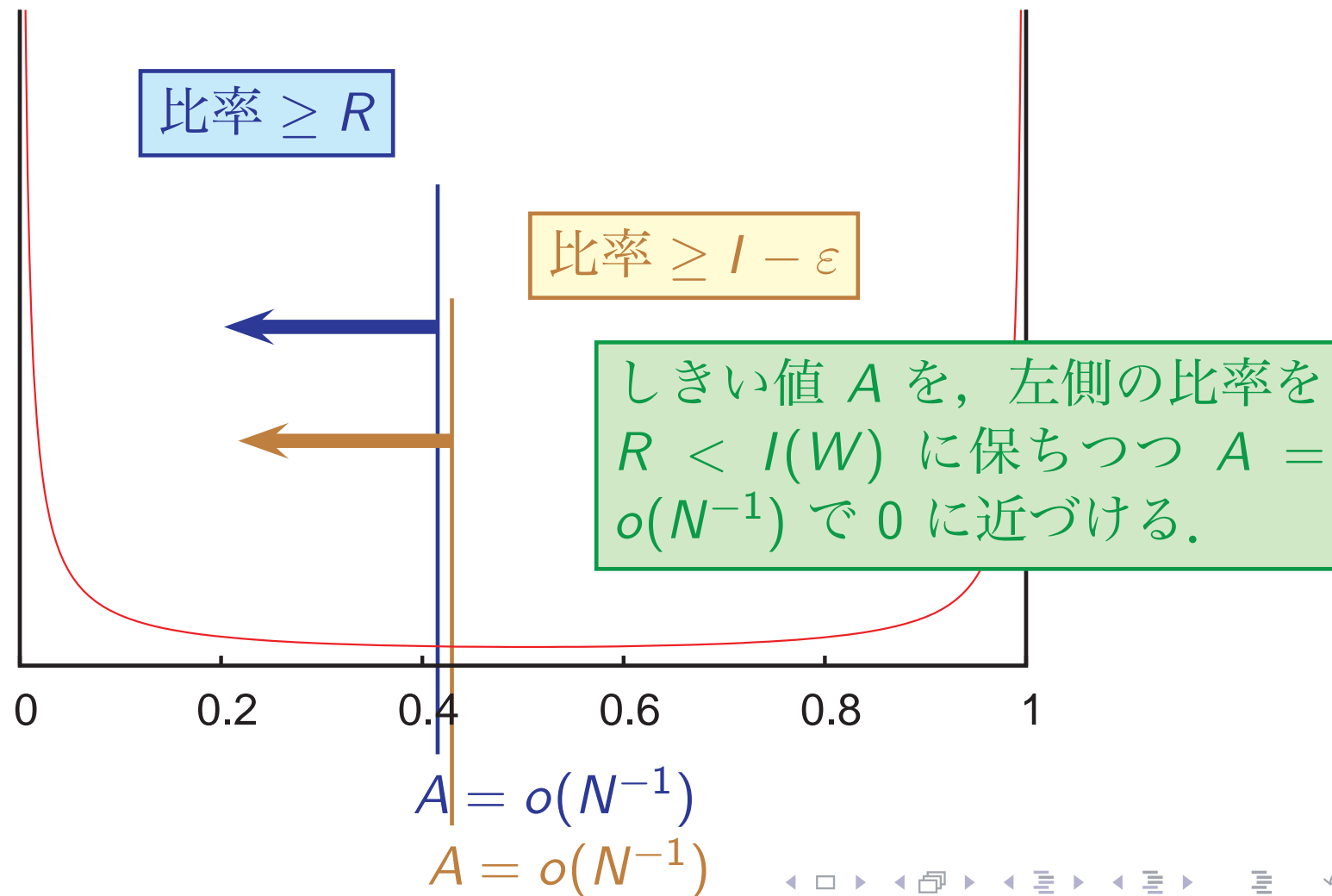
# 符号化率依存の結果

- ここまでに示した結果は符号化率に依存しない:  
 $P_B = o(2^{-2^{\beta n}}), \quad \forall R \in (0, I(W))$
- 符号化率に依存する復号誤り率  $P_B$  の上界?

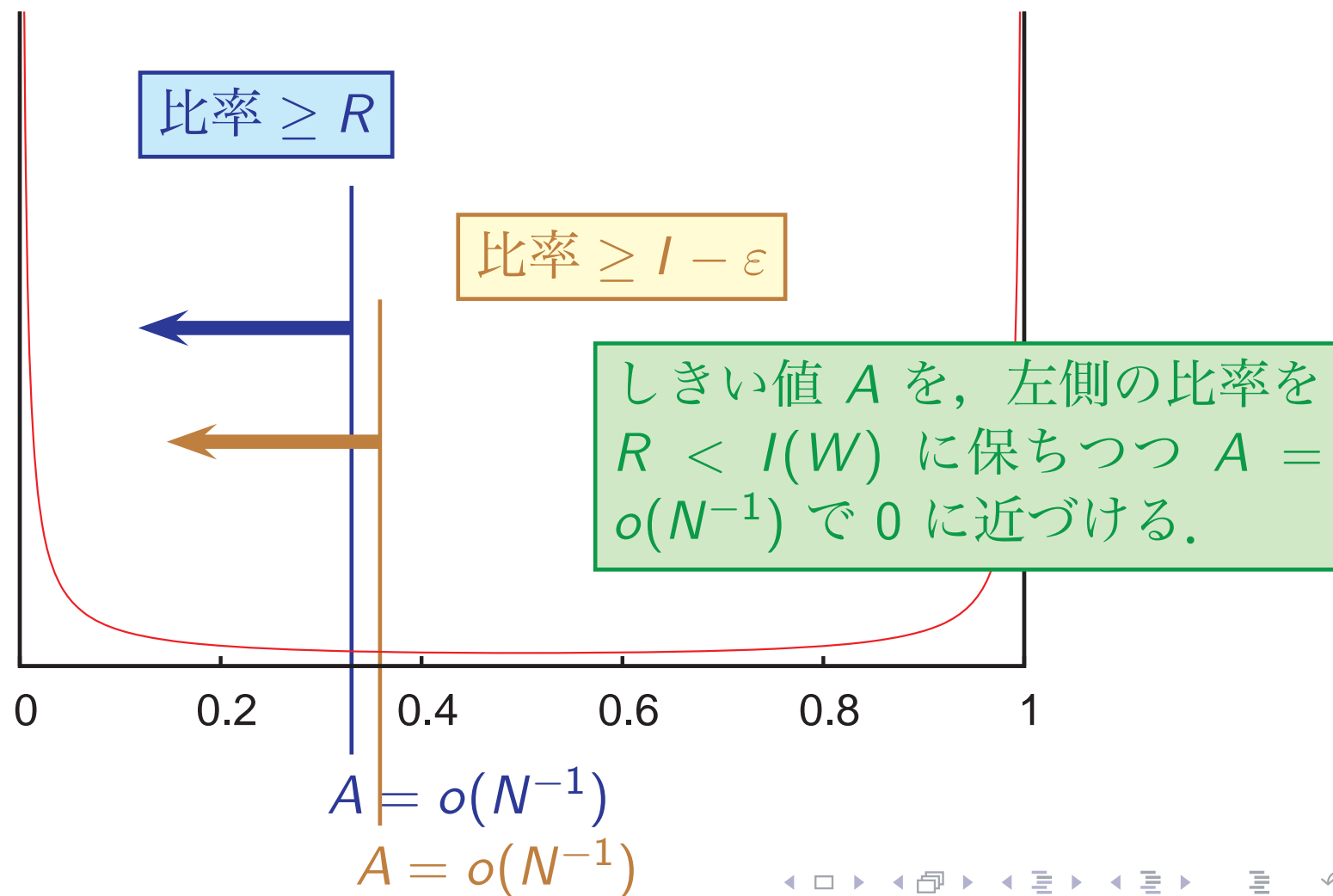
※ 0 に漸近する Bhattacharrya パラメータの値の分布 (漸近的に  
対数正規分布) に対して,

- 大数の法則を適用  $\Rightarrow$  符号化率に依存しない結果.
- 中心極限定理を適用  $\Rightarrow$  符号化率に依存する結果.

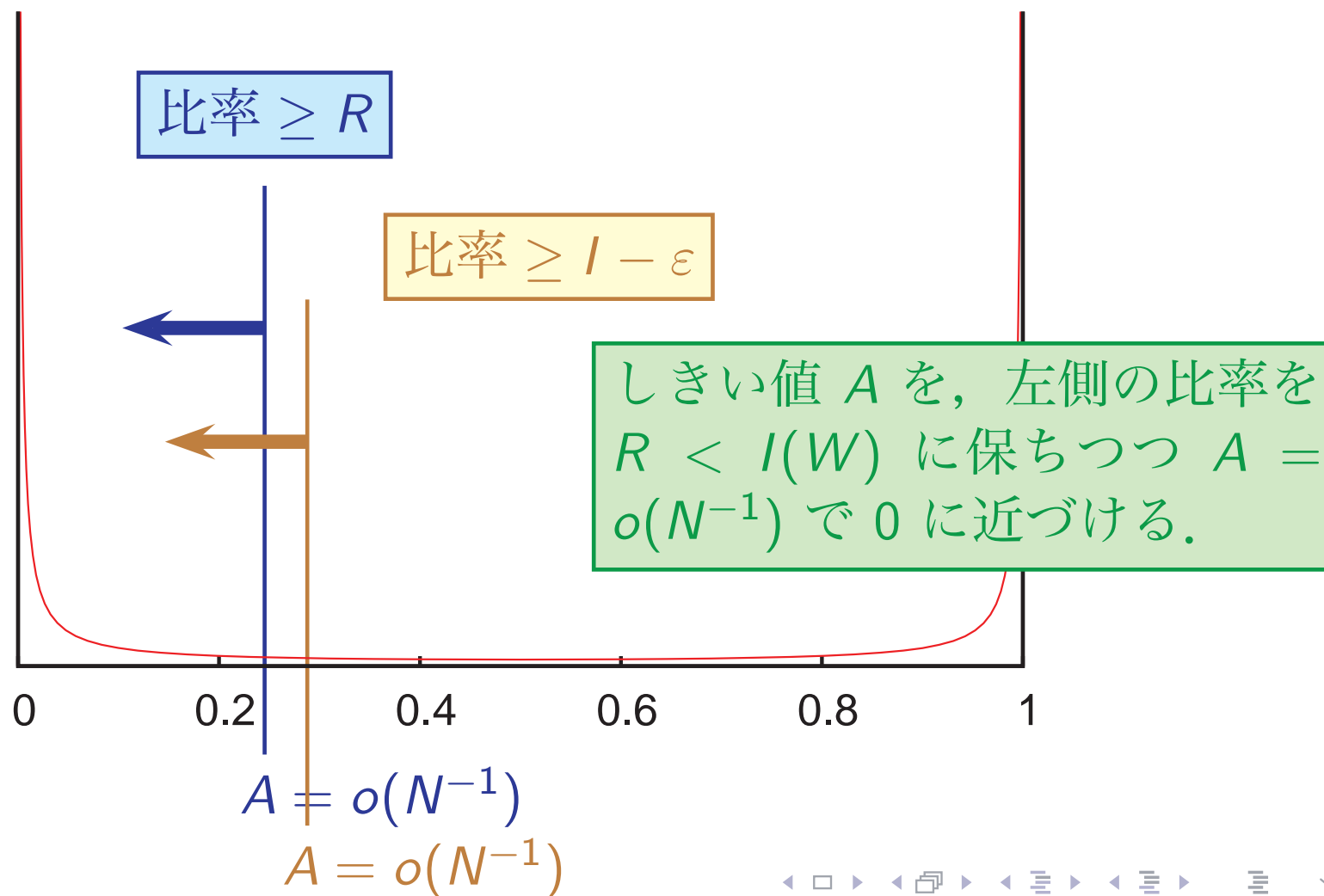
# 直観的には...



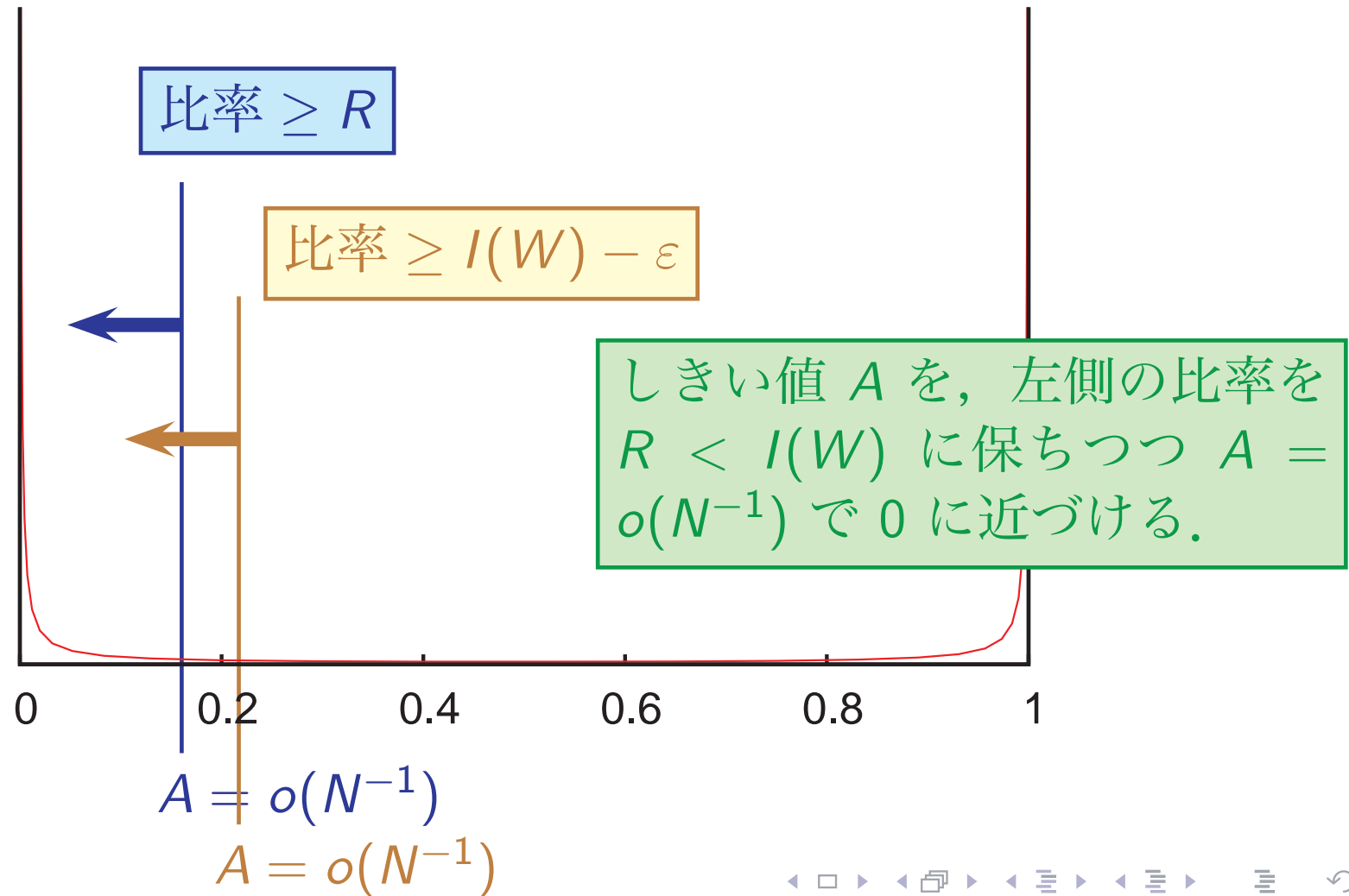
# 直観的には...



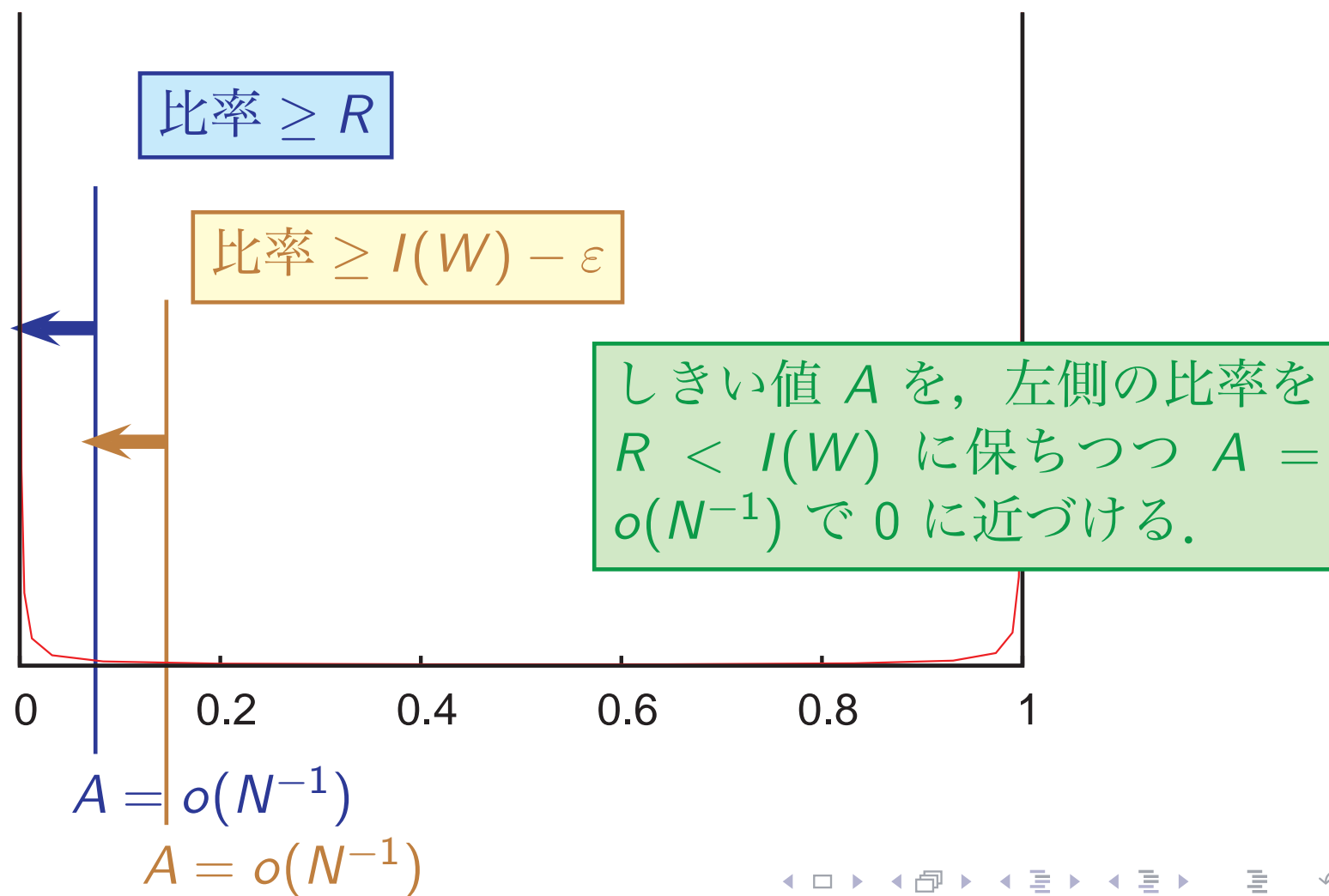
# 直観的には...



## 直観的には...



## 直観的には...





# 符号化率依存の結果

- ここまでに示した結果は符号化率に依存しない:  
 $P_B = o(2^{-2^{\beta n}}), \quad \forall R \in (0, I(W))$
- 符号化率に依存する復号誤り率  $P_B$  の上界?

※ 0 に漸近する Bhattacharrya パラメータの値の分布 (漸近的に  
対数正規分布) に対して,

- 大数の法則を適用  $\Rightarrow$  符号化率に依存しない結果.
- 中心極限定理を適用  $\Rightarrow$  符号化率に依存する結果.

# 符号化率依存の上界 (Hassani-Mori-Tanaka-Urbanke, 2013)

## 符号化率に依存した復号誤り率の上界

$$P_B \leq 2^{-2[n + \sqrt{n}Q^{-1}(R/I(W))]/2 + o(\sqrt{n})}$$

$I(W)$ : 対称通信路容量,  $R$ : 符号化率,  $Q(t) = \int_t^\infty \frac{e^{-z^2/2}}{\sqrt{2\pi}} dz$ .

## 符号化率に依存した漸近形

$$\log_2(-\log_2 P_B) = \frac{n}{2} + \sqrt{n} \frac{Q^{-1}(R/I(W))}{2} + o(\sqrt{n}) \quad (n \rightarrow \infty)$$

# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ **ポーラ符号**
  - 基礎的事項
  - 復号誤り率の上界
  - **スケーリング則**
  - 拡張
- ④ まとめ

# スケーリング則

$$\lim_{N \rightarrow \infty} P_e(N, I(W) - N^{-1/\nu} z) = f(z)$$

スケーリング指数 (Korada-Montanari, Telatar-Urbanke, 2010;  
Goli-Hassani-Urbanke, 2012):

- 二元消失通信路 (BEC):  $\nu \approx 3.6261$
- 二元入力ガウス通信路 (BIAWGNC):  $\nu \approx 4.007$
- 一般の二元入力無記憶対称通信路:  $\nu \geq 3.614$

# 所望の復号誤り率を達成するための符号長

通信路  $W$  を二元入力無記憶対称と仮定し，符号化率を  $R = I(W) - \epsilon$  とする．  $(1/\epsilon)^\nu$  に比例する程度の符号長  $N$  で，

- 復号誤り率が  $N \rightarrow \infty$  で 0 に漸近するポーラ符号が存在し，  $\nu \approx 5.9$  ととれる (Hassani, 2013).
- 復号誤り率が  $2^{-N^{0.49}}$  以下であるようなポーラ符号が存在する (Guruswami-Xia, 2013).

# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ **ポーラ符号**
  - 基礎的事項
  - 復号誤り率の上界
  - スケーリング則
  - **拡張**
- ④ まとめ

# 行列 $G$ の選択

1	0
1	1

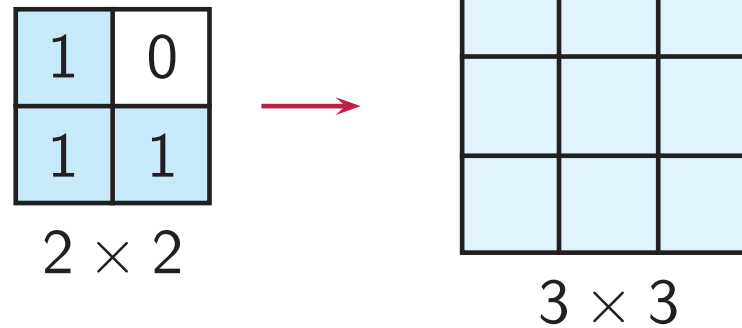
$2 \times 2$

$l \times l$  行列による分極 (Korada-Şaşıoğlu-Urbanke, 2009;  
Hassani-Mori-Tanaka-Urbanke, 2013)

$$P_B \leq 2^{-\ell^{nE(G)+Q^{-1}(R/I(W))\sqrt{nV(G)}+o(\sqrt{n})}}$$

$(E(G), V(G))$ : 行列  $G$  から計算される量.

# 行列 $G$ の選択



$l \times l$  行列による分極 (Korada-Şaşoğlu-Urbanke, 2009;  
Hassani-Mori-Tanaka-Urbanke, 2013)

$$P_B \leq 2^{-\ell^{nE(G)+Q^{-1}(R/I(W))\sqrt{nV(G)}+o(\sqrt{n})}}$$

$(E(G), V(G))$ : 行列  $G$  から計算される量.



行列  $G$  の選択

1	0
1	1

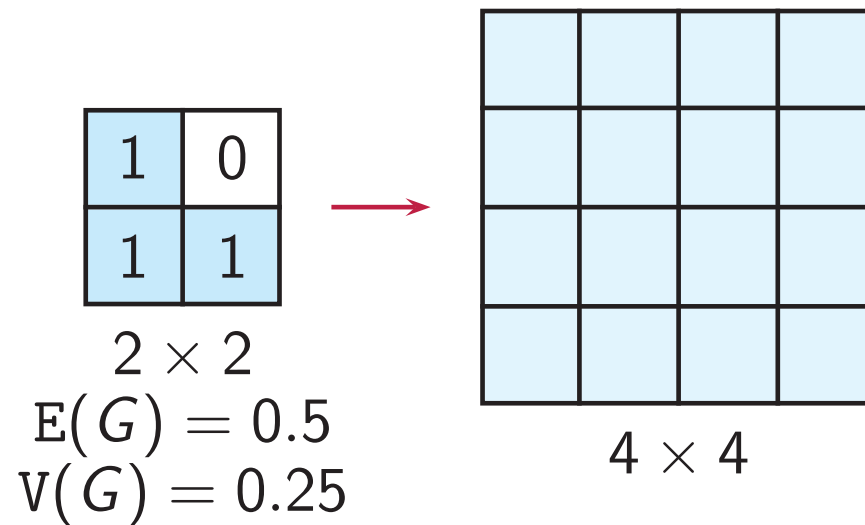
 $2 \times 2$ 


 $4 \times 4$ 

$l \times l$  行列による分極 (Korada-Şaşıođlu-Urbanke, 2009;  
Hassani-Mori-Tanaka-Urbanke, 2013)

$$P_B \leq 2^{-\ell^{nE(G)+Q^{-1}(R/I(W))\sqrt{nV(G)+o(\sqrt{n})}}$$

$(E(G), V(G))$ : 行列  $G$  から計算される量.

行列  $G$  の選択

$l \times l$  行列による分極 (Korada-Şaşoğlu-Urbanke, 2009;  
 Hassani-Mori-Tanaka-Urbanke, 2013)

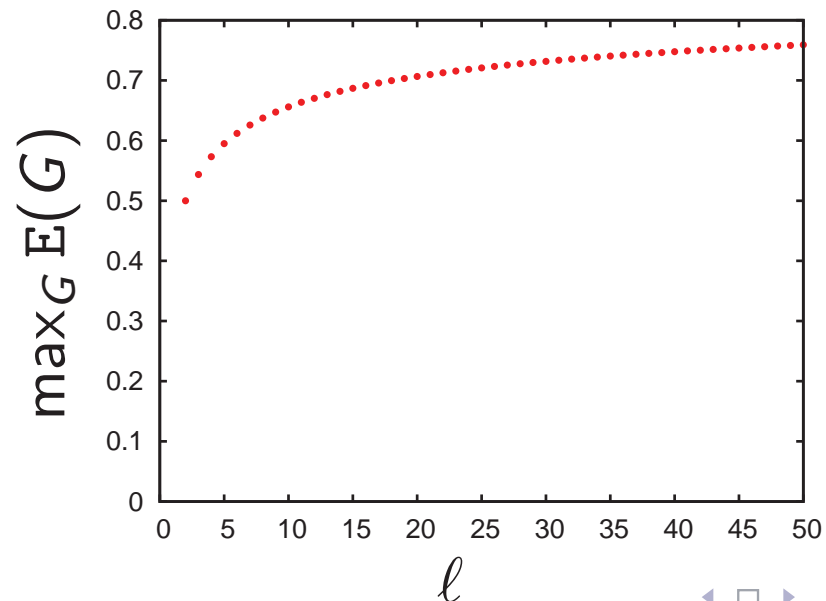
$$P_B \leq 2^{-l^{nE(G)+Q^{-1}(R/I(W))\sqrt{nV(G)+o(\sqrt{n})}}$$

$(E(G), V(G))$ : 行列  $G$  から計算される量。

行列  $G$  の選択

$E(G)$  が大きいほど漸近的には高性能.

- $\mathbb{F}_2$  上の  $l \times l$  行列 (Korada-Şaşođlu-Urbanke, 2009):
  - $\lim_{l \rightarrow \infty} \max_G E(G) = 1$ .
  - $l \leq 15$  では  $E(G) \leq 1/2$ ,  $l = 16$  で  $\max_G E(G) = 0.51828$ .
- $\mathbb{F}_q$  上の  $l \times l$  行列,  $l \leq q$ :  $\max_G E(G) = \frac{\log l!}{l \log l}$  (Mori-Tanaka, 2014).



# RS 符号との接続

外部符号に高符号化率の RS 符号を使う接続符号

(Mardavifar-El-Khamy-Lee-Kang, 2014):

- 内部ポーラ符号の符号長:  $n = N^\epsilon$
- 内部ポーラ符号の復号誤り率:  $P_e = O(2^{-n^{1/2-\epsilon}})$
- 外部 RS 符号の符号長:  $m = N^{1-\epsilon}$
- 外部 RS 符号の符号化率:  $R_o = 1 - 4N^{-\epsilon(1/2-\epsilon)}$
- 外部 RS 符号に対して限界距離復号を適用: 最大で  $\tau = \lfloor (1 - R_o)m/2 \rfloor$  ビットの誤りが訂正可能.

⇒ 接続符号の復号誤り率:

$$\begin{aligned}
 P_e' &= \sum_{i=\tau+1}^m \binom{m}{i} P_e^i (1 - P_e)^{m-i} \leq \binom{m}{\tau+1} P_e^{\tau+1} \\
 &= O\left(2^m \times 2^{-n^{1/2-\epsilon} m(1-R_o)/2}\right) = O\left(2^{N^{1-\epsilon} - 2N^{\epsilon(1/2-\epsilon)+1-\epsilon-\epsilon(1/2-\epsilon)}}\right) \\
 &= O\left(2^{-N^{1-\epsilon}}\right)
 \end{aligned}$$

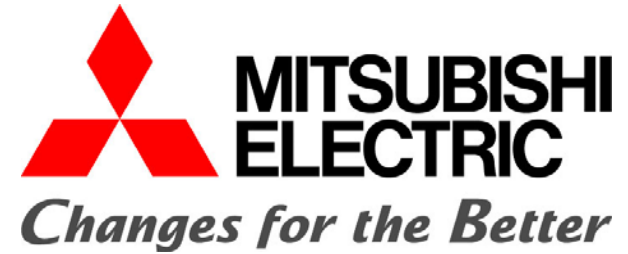
# 目次

- ① 準備
- ② 低密度パリティ検査符号
- ③ ポーラ符号
- ④ まとめ**

# まとめ

LDPC 符号, ポーラ符号の漸近性能に関する最近の研究成果を紹介.

- LDPC 符号:
  - 二元消失通信路 (BEC) の場合について解析が進められている.
    - 典型的な符号の復号誤り率は復号しきい値未満では符号長に対して指数的に減少.
    - 修正アンサンブルのスケーリング指数  $\nu$  は 2.
  - 一般の通信路に対する解析は難しい.
- ポーラ符号:
  - 任意の二元無記憶通信路について対称通信路容量を達成.
  - 復号誤り率が  $O(2^{-N^\beta})$ ,  $\beta < 1$ .
  - $\beta$  を 1 に近づけるための工夫.
  - スケーリング指数は 3.614 以上で, 4 程度と予想されている.
- 話さなかったこと:
  - 符号の設計
  - MAP 復号の性能評価
  - 応用



# 量子暗号における有限長解析

鶴丸豊広（三菱電機株式会社）  
於 電子情報通信学会ソサエティ大会  
2014/9/25

# 量子暗号の特徴

量子論を安全性の根拠とする、原理的に安全な暗号方式

## 現代暗号 vs. 量子暗号

現代暗号 (AES, MISTY, Camellia, RSA暗号など)

高速: 数百Mbps (S/W) ~ 数十Gbps (LSI)

計算量的安全性: 現在の計算機を想定した解読に対しては安全だが、  
新原理の計算機が出現した時に解読される可能性あり。

量子暗号 (BB84方式, B92方式, DPSQKD方式ほか)

低速: 数十kbps ~ 1Mbps

絶対的安全性: **どんなに計算機が進歩しても解読できない。**

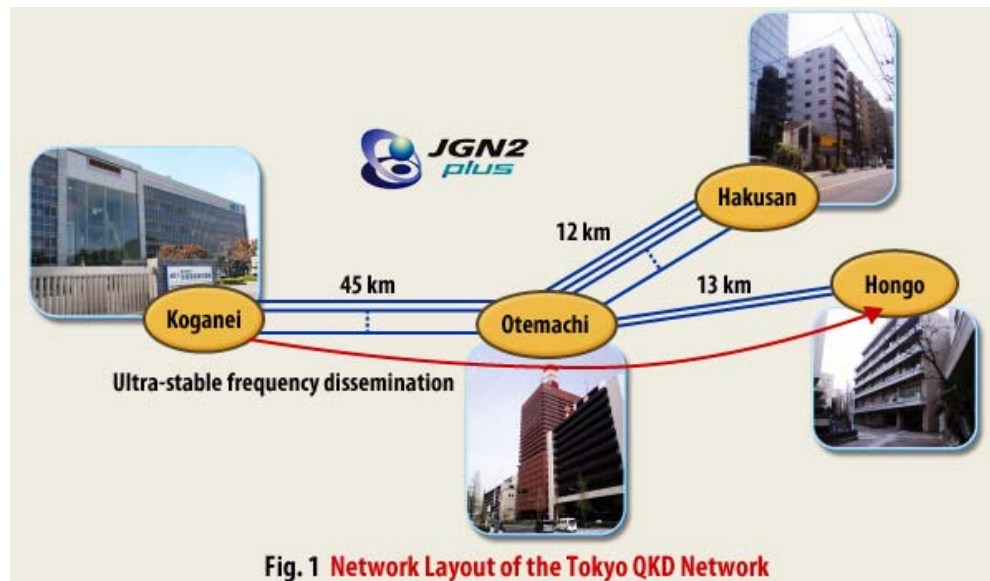
量子力学の公理から出発して、安全性を数学的に証明する

- この講演ではもっぱら量子鍵配送 (quantum key distribution, QKD) の、BB84方式 (Bennett-Brassard 1984 protocol) についてのべる
- とくに線型符号の果たす役割、および装置開発の状況を説明する。



# Tokyo QKD Network

- 2010年、国内外各社の量子暗号装置を接続し、東京都内の既設光ファイバ上に、量子暗号ネットワークを構築
  - 情報通信研究機構(NICT)の呼びかけにより、以下の機関が参加
    - 国内: NEC、三菱電機、NTT、
    - 海外: 東芝欧州研(英)、id Quantique社(スイス)、All Vienna(オーストリア)
  - 4拠点: 大手町、白山、本郷、小金井
  - 古典中継(※)により、総延長200km以上



参考:

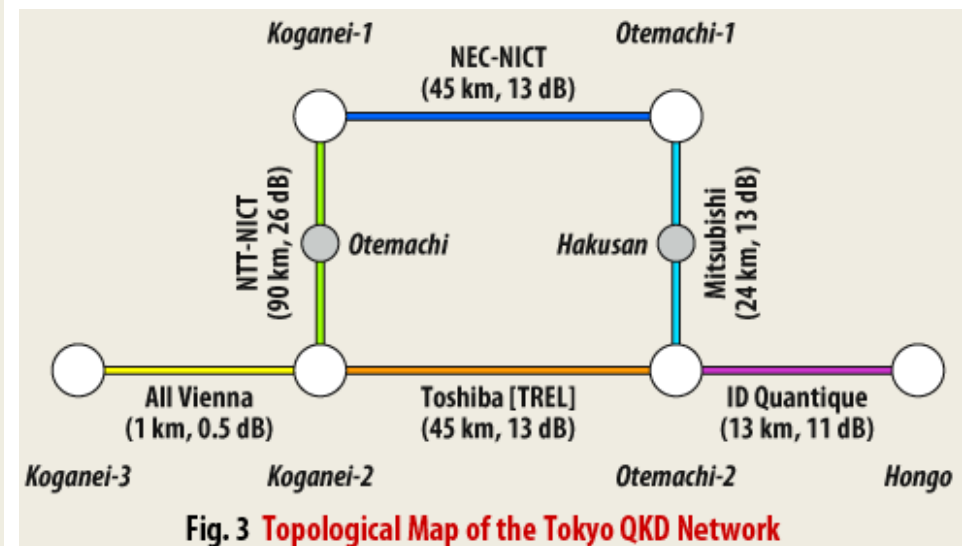
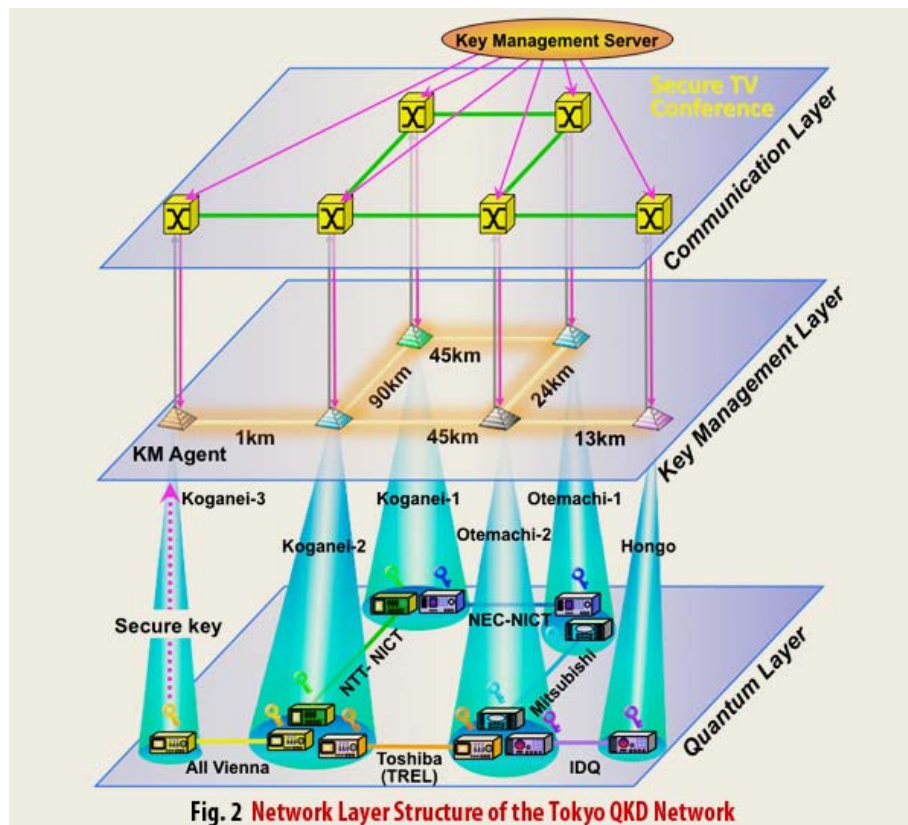
UQCCホームページ

<http://www.uqcc2010.org/>

※各ノードは信頼できるとし  
秘密鍵をリレーした

# Tokyo QKD Network

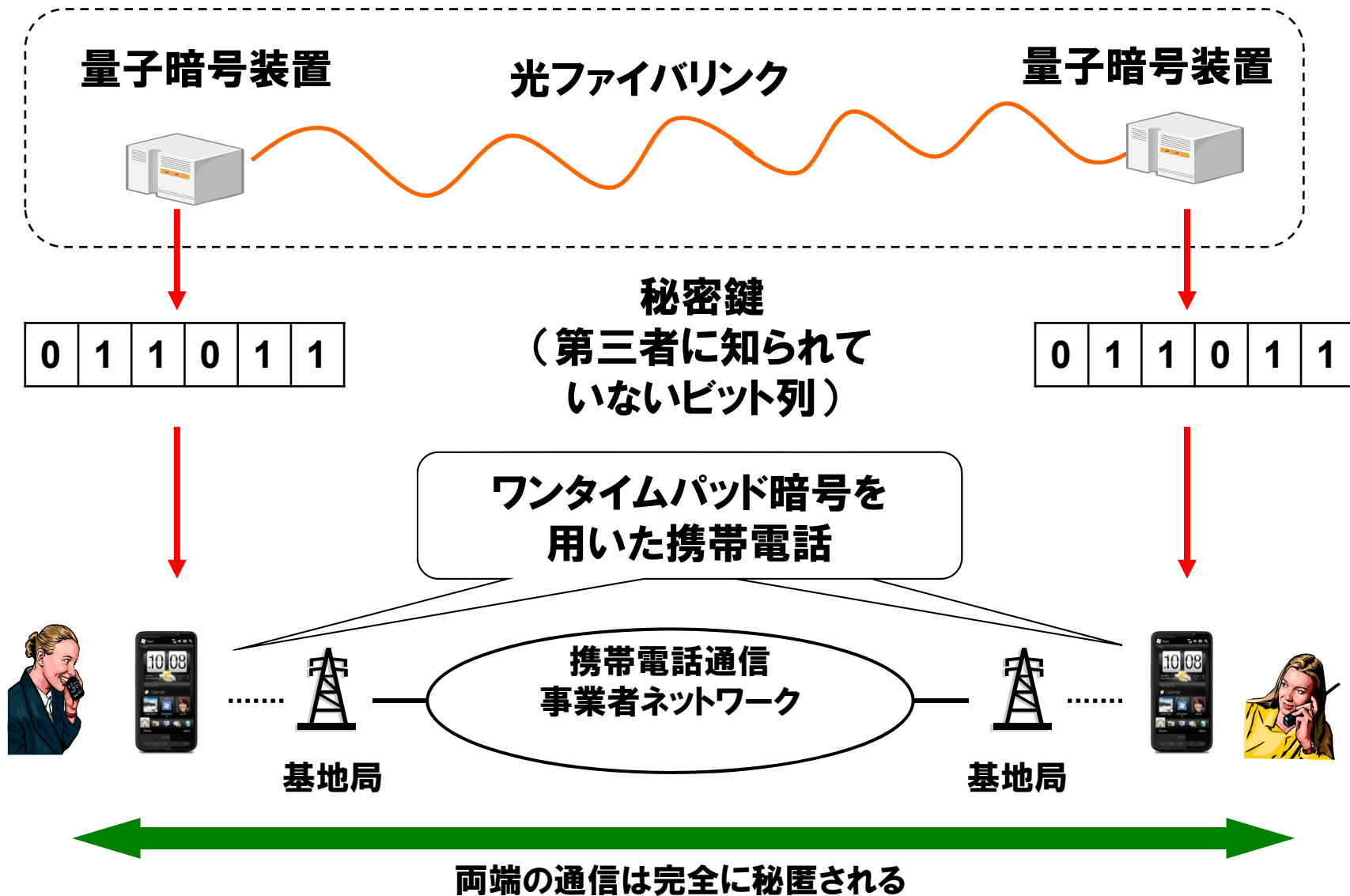
- 量子暗号で共有した鍵で暗号化し、動画配信(テレビ会議)を実施
  - 記者発表、および国際会議UQCCでのデモ(2010年)
- 通信速度: 数kbps~300kbps (通信路により異なる)



UQCCホームページ

<http://www.uqcc2010.org/> より

# 量子暗号の目的は秘密鍵の共有 (秘密鍵を携帯電話の暗号化に使う例)

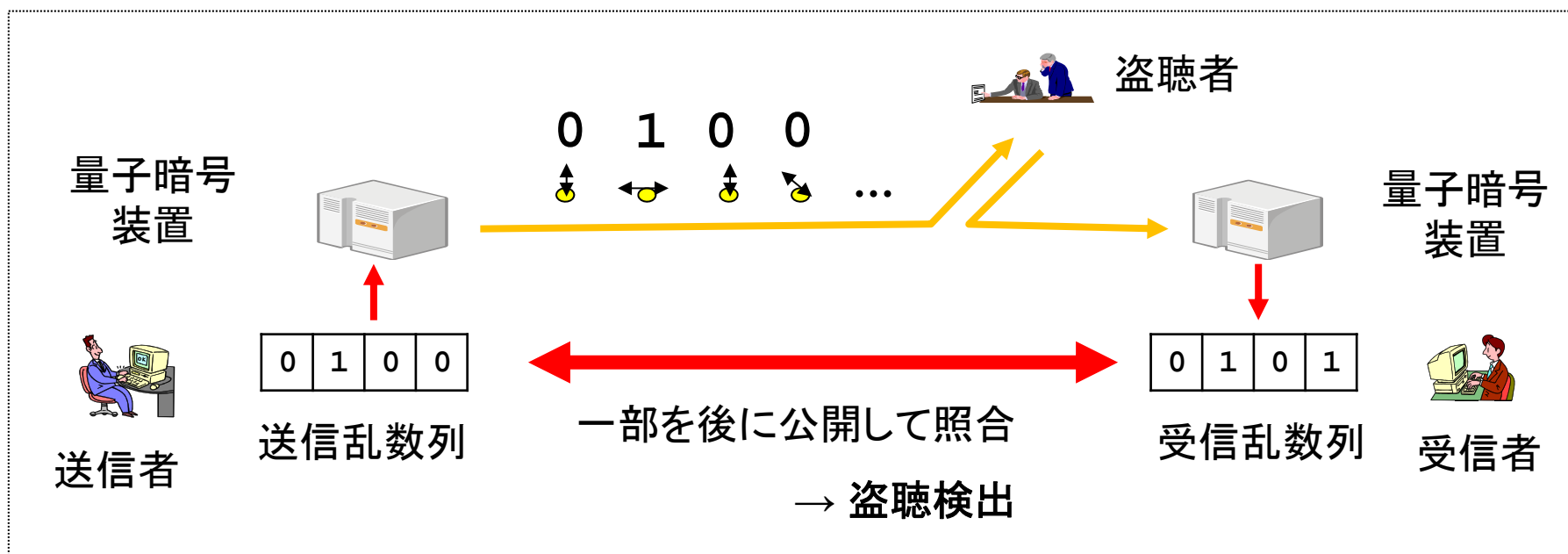


# 量子暗号の無条件安全性（イメージ）

量子暗号では、光の粒子（光子）に0,1の乱数を乗せて送る

この乱数値は「測定すると必ず影響を受けて変化」← 量子論

→ 盗聴があればノイズが増加し、あとで必ず露見する



したがって通信路ノイズには敏感 → 通信距離と安全性に相関がある

- 長距離化 → 通信路ノイズ増加 → 盗聴ノイズとの区別がより困難になる
- 光を強める → 光子の数を増やすことに相当 → コピーが作れて盗聴が容易に
- 中継点での増幅も困難 ... 増幅には測定がともなう

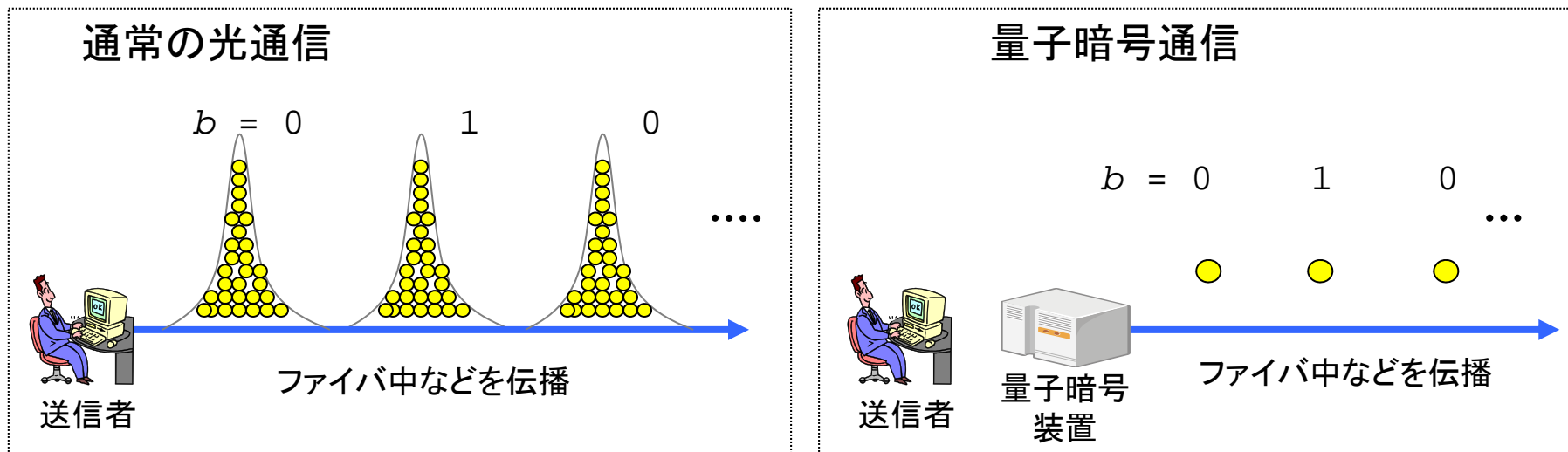
# 「量子」に乱数ビットをのせる

- 量子とは？
  - この世の物質は全て量子であり、波としての性質と、粒子としての性質の両方を併せ持つ
  - 精密測定を行うと、量子としての性質が現れる  
→ **測定によって、状態が乱される**
- この性質から
  - Eveが盗聴を行うと、Bobが受け取る信号に必ず変化がおきる
  - それを送信者と受信者が検出できる。



# 「量子」に乱数をのせる

- 通常用いる量子は「光」
  - 光は粒子である（これを「光子」(photon)と呼ぶ）
  - 我々が通常見ているのは粒々の集まり（粒子の数 ~ エネルギー）
  - 量子暗号では, 粒子ひとつずつに0, 1のデータを乗せる



※ 1パルス辺り $10^7$ 個程度の光子

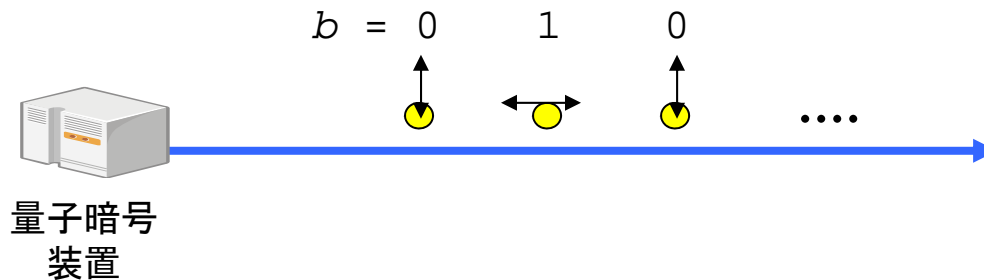
# どうやって光子に乱数をのせるか？

符号化の方法： 偏光変調

- 光は波であり，振動の方向が複数ある



- この偏光を使って，光子ひとつずつに情報をのせる



- 同様に ↗ 偏光, ↘ 偏光もある（装置を45度傾ける）

+ 基底

× 基底

# 盗聴検知 (通信路雑音がない場合)

- 量子暗号では暗号用の乱数を送る
- 2種類の変調方式(×基底、+基底)でスクランブルする
- 盗聴者は基底の選択を知らないので、  
確率的に誤った基底で測定をする →盗聴の痕跡を残す



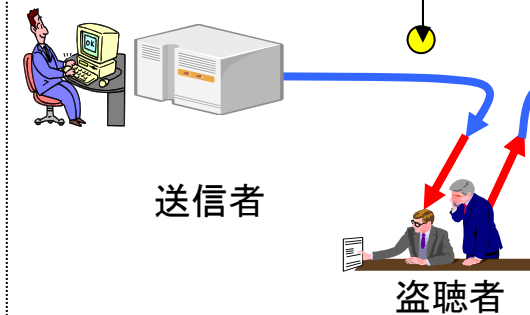
# 基底をランダムにふって光子を送る

	$b=0$	$b=1$
+基底	↕	↔
×基底	↗	↘

基底をランダムに選んで光子を送る

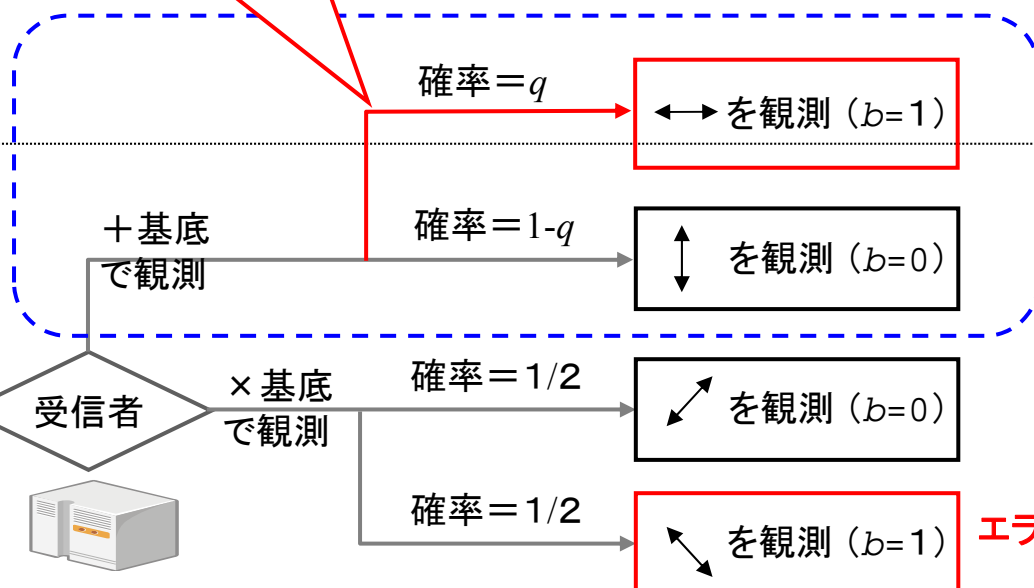
$\left\{ \begin{array}{l} \text{確率 } p \Rightarrow \times \text{基底} \\ \text{確率 } 1-p \Rightarrow + \text{基底} \end{array} \right.$

+基底で  $b = 0$



受信者が正しい基底で観測してもエラーが起こる

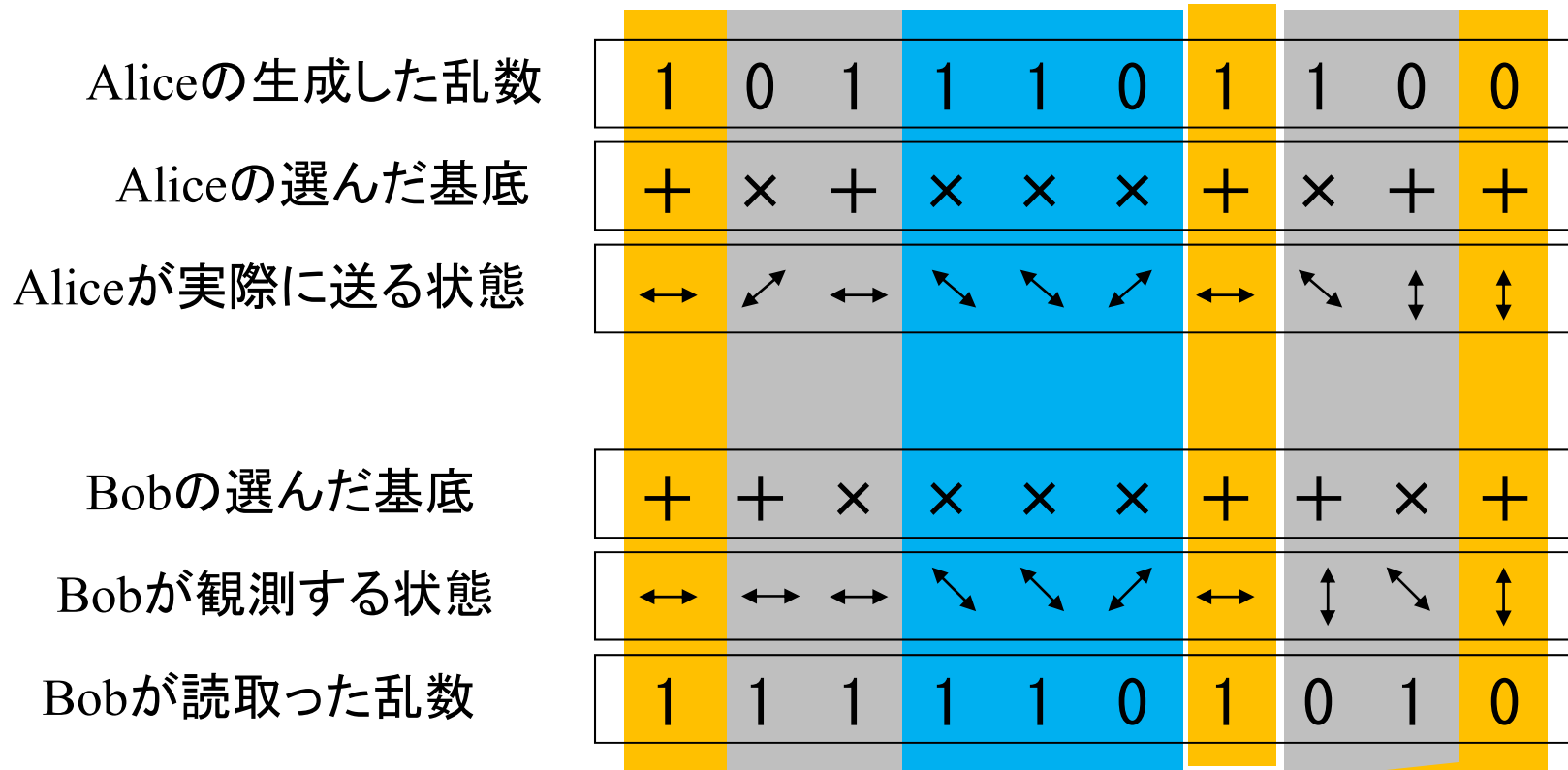
盗聴者検出



盗聴者Eveは基底を知らずに観測  
⇒ 光子の偏光を変えてしまう

# 盗聴者がいない場合の処理の流れ

	b=0	b=1
+基底	↕	↔
×基底	↗	↘



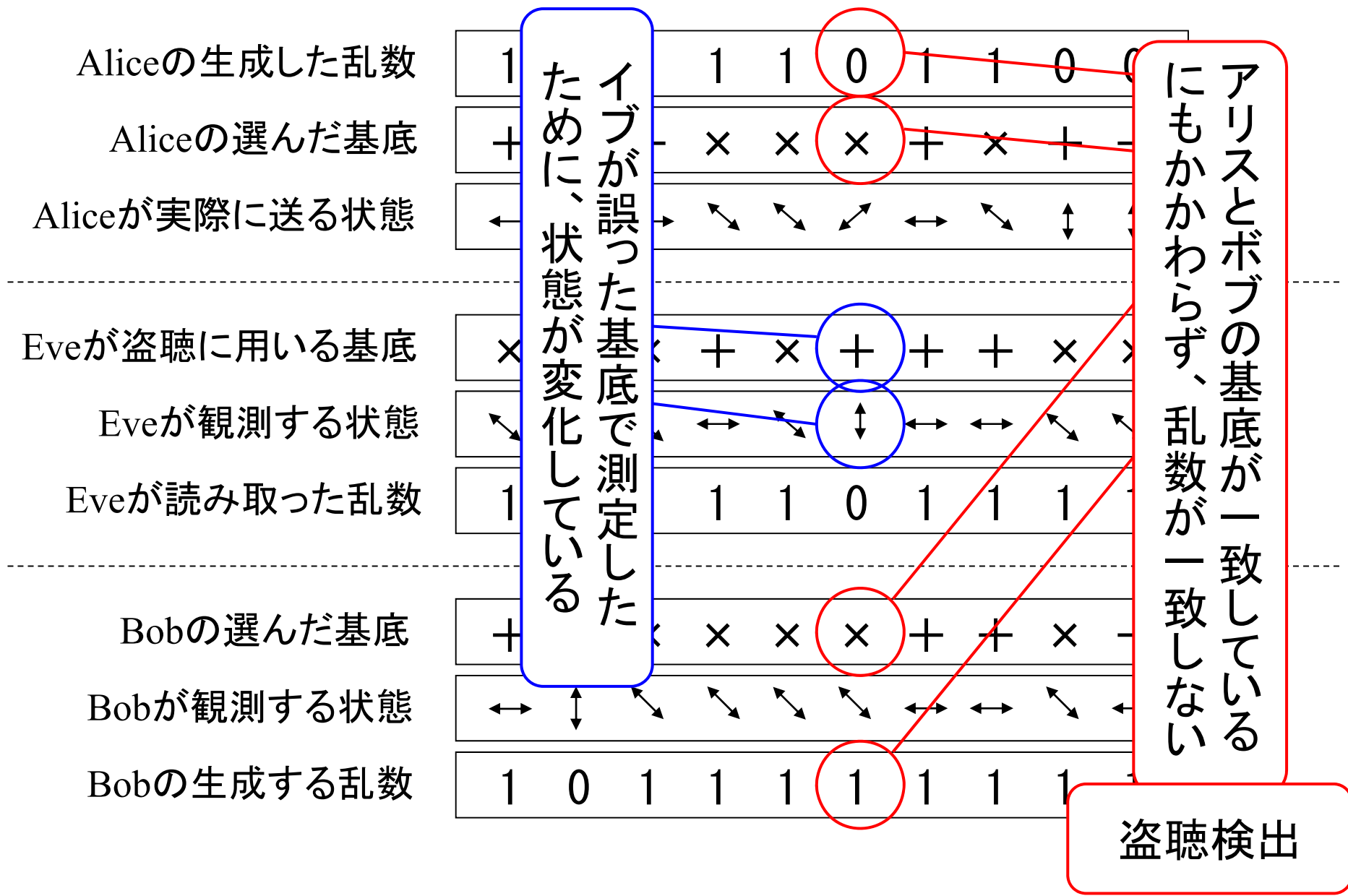
光子の送受信が終わってから  
基底の情報を公開する

+基底で一致した箇所は  
「ふるい鍵」  
→データ処理して秘密鍵に

×基底で一致した箇所は  
「サンプルビット」  
→盗聴検出に使う

基底の一致しない  
箇所は捨てる

# 盗聴者Eveがいる場合 (intercept-resend attack)



以下、基底が一致しない箇所はそもそも  
なかったこととして話を進める

...そもそも送っているのが乱数なので、

安全性に影響なし

	b=0	b=1
+基底	↕	↔
×基底	↗	↘

Aliceの生成した乱数

1	0	1	1	1	0	1	1	0	0
---	---	---	---	---	---	---	---	---	---

Aliceの選んだ基底

+	×	+	×	×	×	+	×	+	+
---	---	---	---	---	---	---	---	---	---

Aliceが実際に送る状態

↔	↗	↔	↘	↘	↗	↔	↘	↕	↕
---	---	---	---	---	---	---	---	---	---

Bobの選んだ基底

+	+	×	×	×	×	+	+	×	+
---	---	---	---	---	---	---	---	---	---

Bobが観測する状態

↔	↔	↔	↘	↘	↗	↔	↕	↘	↕
---	---	---	---	---	---	---	---	---	---

Bobが読取った乱数

1	1	1	1	1	0	1	0	1	0
---	---	---	---	---	---	---	---	---	---

光子の送受信が終わってから  
基底の情報公開する

+基底で一致した箇所は  
「ふりい鍵」  
→データ処理して秘密鍵に

×基底で一致した箇所は  
「サンプルビット」  
→盗聴検出に使う

基底の一致しない  
箇所は捨てる

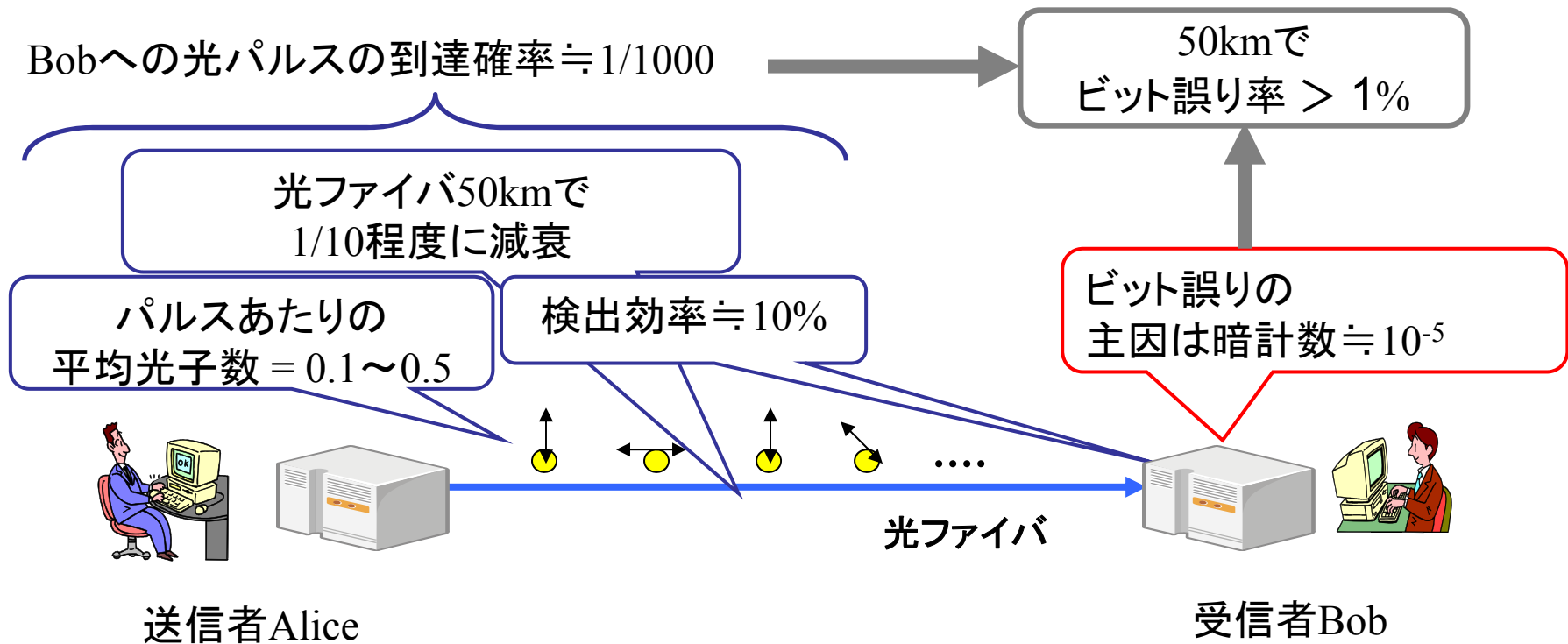
# 通信路雑音がある場合の 安全性の考え方

前ページまでの攻撃の話は、ある特定の例  
(intercept/resend 攻撃)にたよった、直感的な説明にすぎない。  
実際の量子暗号の安全性証明では、攻撃者Eveが、  
量子力学によって許されたあらゆる攻撃を行うと想定する。

さらに現実の装置や通信路では、盗聴者がいなくとも雑音がある

# 現実の通信路にはノイズがある

量子暗号装置は、減衰や雑音の巣窟  
敵がいなくても通信路上でエラーが起こる



※暗計数(dark count) = 信号が来ていないのに、検出器が反応する事象

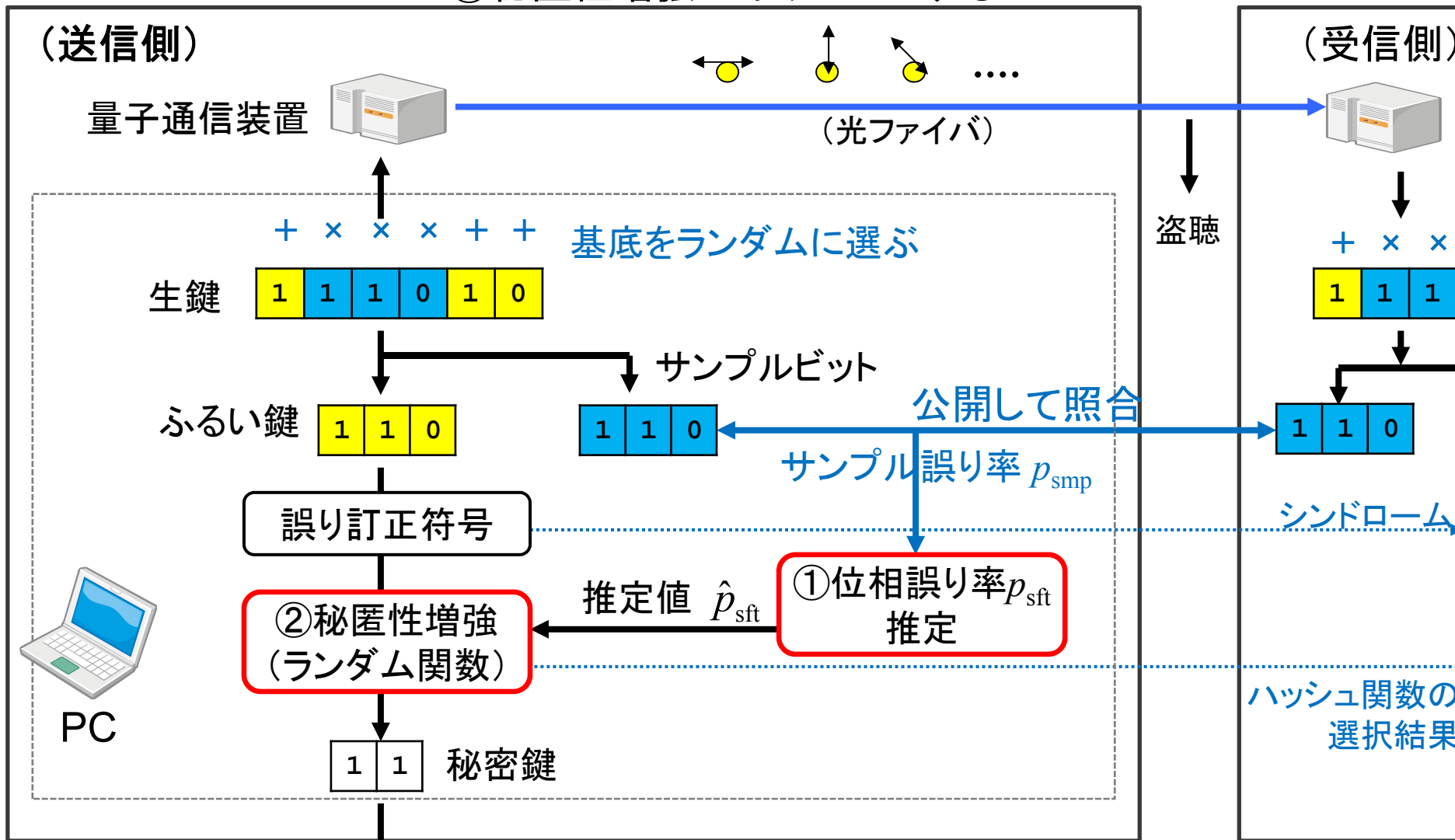
# 安全性証明で示したいこと

このノイズを全て敵によるものと想定する (安全サイドに倒すことに相当)



# 現実のBB84プロトコル

- ① サンプルから盗聴者への漏洩情報量を見積もり
- ② 秘匿性増強でキャンセルする



アプリケーション(携帯電話など)



※青線、青字は公開データ



# 秘匿性増強と位相誤り率推定の概要

秘匿性増強： 「大体安全」な暗号鍵を「完全に安全」にする統計処理

大体安全な鍵



(例: 量子暗号のふるい鍵)

…一部が漏洩しているので  
秘密鍵としては使えない



ランダム関数



完全に安全な鍵



…秘密鍵として使える

■ 盗聴者の知らないビット  
□ 盗聴者に漏洩したビット

※これはあくまでイメージです

位相誤り率推定： 盗聴者に漏洩したビット数の上界を、統計的に推定する

- 盗聴で漏れたビット数 (□ の数)  $\propto h_2(p_{\text{sft}})$ 
  - $h_2$ : binary entropy.
  - 位相誤り率  $p_{\text{sft}} =$  ふるい鍵を  $\times$  基底で測定したときの誤り率
- しかし  $p_{\text{sft}}$  は直接測定できない  $\leftarrow$  サンプルビットの誤り率  $p_{\text{smp}}$  から区間推定

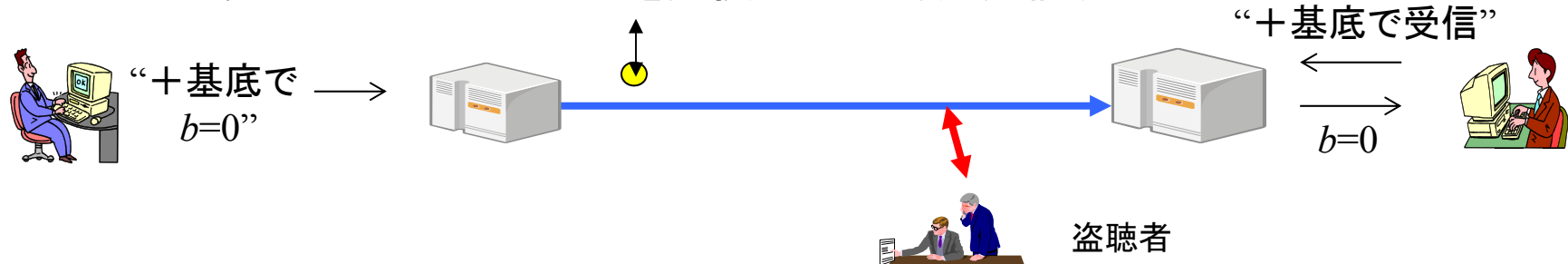
# 簡単なプロトコルへの書き換え(ゲーム変換)

- 安全性証明では、盗聴者の状態と、送信者の秘密鍵状態のみ考察する
- それらを変化させない限り、より簡単なプロトコルに書きかえてよい  
...結果が同じなら、簡単なプロトコルに変換してから解析の方が楽。
- 特にBell状態を用いた書きかえが便利。

• Bell状態とは、もつれあい状態の一種である。  $|\Psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

• これをつかうと、基底選択を後回しにできる。

(ア) 現実のプロトコル: 基底を選択したのち、送受信する



(イ) Bell状態を使った仮想プロトコル

① Bell状態を生成して送る



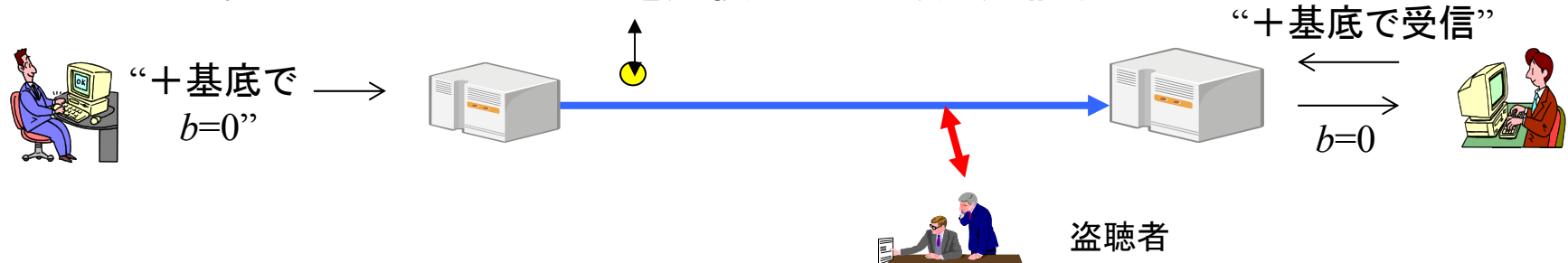
# 簡単なプロトコルへの書き換え(ゲーム変換)

- 安全性証明では、盗聴者の状態と、送信者の秘密鍵状態のみ考察する
- それらを変化させない限り、より簡単なプロトコルに書きかえてよい  
...結果が同じなら、簡単なプロトコルに変換してから解析の方が楽。
- 特にBell状態を用いた書きかえが便利。

• Bell状態とは、もつれあい状態の一種である。  $|\Psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

• これをつかうと、基底選択を後回しにできる。

(ア) 現実のプロトコル: 基底を選択したのち、送受信する



(イ) Bell状態を使った仮想プロトコル

① Bell状態を生成して送る



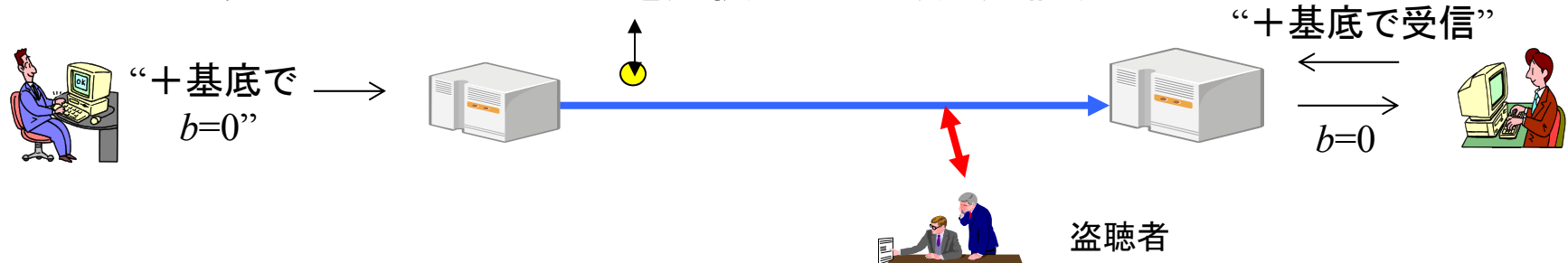
# 簡単なプロトコルへの書き換え(ゲーム変換)

- 安全性証明では、盗聴者の状態と、送信者の秘密鍵状態のみ考察する
- それらを変化させない限り、より簡単なプロトコルに書きかえてよい  
...結果が同じなら、簡単なプロトコルに変換してから解析の方が楽。
- 特にBell状態を用いた書きかえが便利。

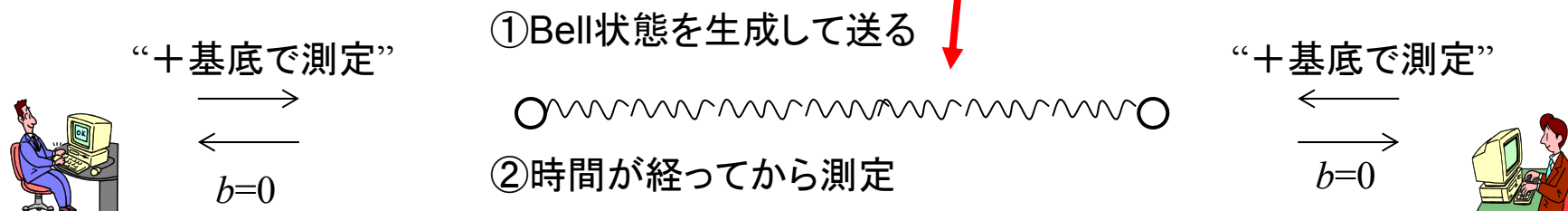
• Bell状態とは、もつれあい状態の一種である。  $|\Psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

• これをつかうと、基底選択を後回しにできる。

(ア) 現実のプロトコル: 基底を選択したのち、送受信する

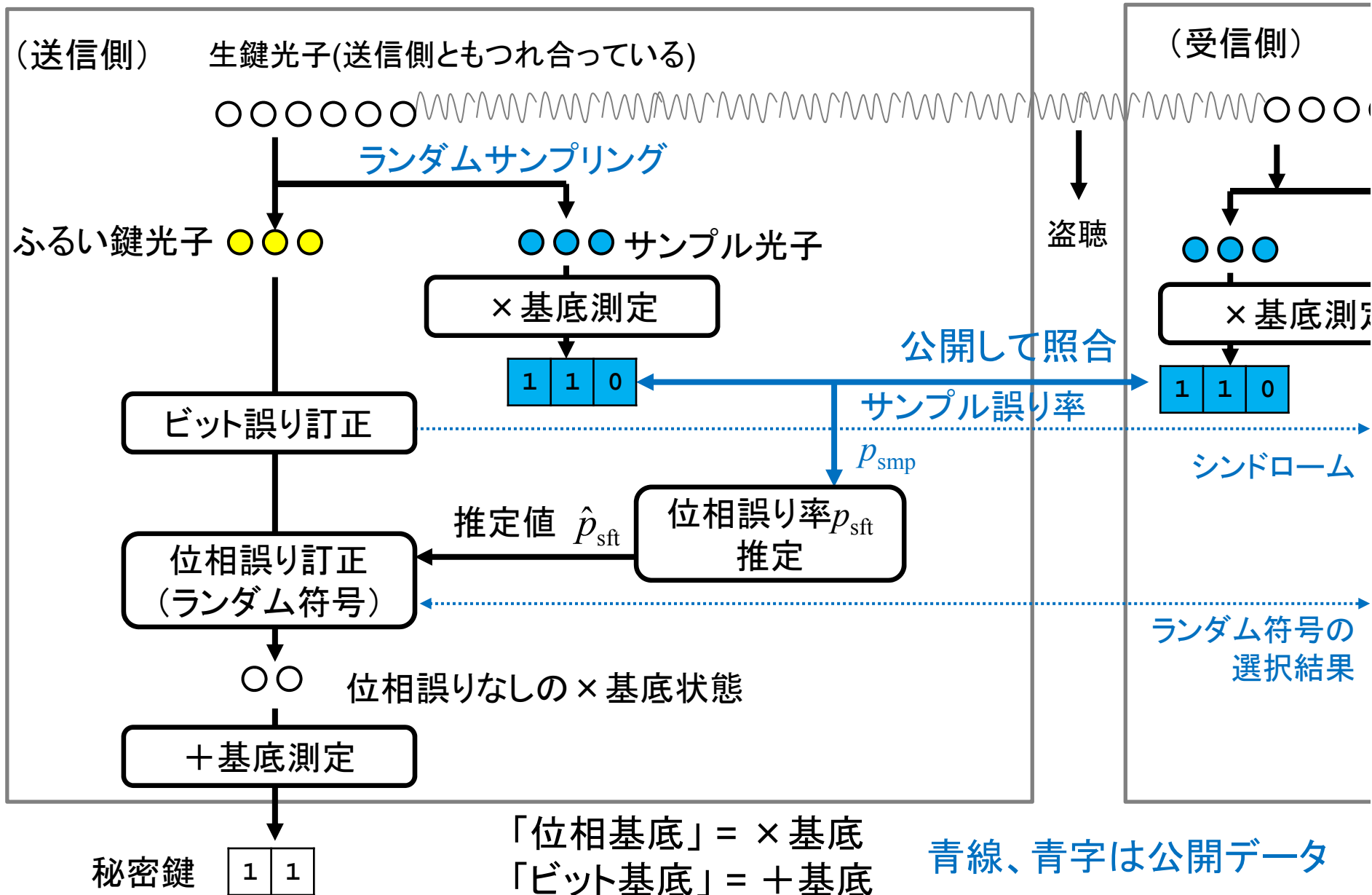


(イ) Bell状態を使った仮想プロトコル



# Bell状態により書き換えた仮想BB84プロトコル

秘匿性増強が、位相誤り訂正におきかわる



# 安全性証明に関するまとめ

- 量子暗号では2種類の変調方式をランダムに使い分け、盗聴行為を検出する

	$b=0$	$b=1$
+基底 (ビット基底)	↑↓	←→
×基底 (位相基底)	↗↘	↖↙

→ ふるい鍵

→ 秘密鍵

→ サンプルビット

→ ふるい鍵の

位相誤り率 $p_{\text{sft}}$ を推定

漏洩情報量に対応

安全性証明では、以下の2つの状況は同じ

現実のBB84プロトコル	仮想プロトコル
単一光子を送信	Bell状態を送信
秘匿性増強	位相誤り訂正
ランダム線形関数	ランダム線形符号



秘密鍵の安全性は、位相誤り訂正の性能で決まる  
(誤り率 $p_{\text{sft}}$ , ランダム線形符号)

# 量子暗号における有限長効果

- 漸近的な場合 (パルス数 $n, l \rightarrow$  無限大)
  - サンプル数 $l \rightarrow$  無限大
    - 位相誤り率は正確に見積もれる:  $\hat{p}_{\text{sft}}(p_{\text{smp}}) = p_{\text{smp}}$
  - ふるい鍵長 $n \rightarrow$  無限大
    - 位相誤り訂正符号の符号化率は  $1 - h_2(p_{\text{smp}})$
    - 秘密鍵は正確に  $n[1 - h_2(p_{\text{smp}})] - s$  ビット
- 現実の装置のパルス数 $n, l$ は有限である。

厳密な解析を行うと、秘密鍵生成率は上記より低くなる。

秘密鍵生成率 = 生成した秘密鍵長 / 通信した光子数

  - たとえば $n, l$ をともに1000とすると、本来の誤り率 $p_{\text{sft}} = 5\%$ に対し
    - 推定値  $\hat{p}_{\text{sft}} \geq 6\%$  (危険率6%) → 秘密鍵生成率低下
  - 秘密鍵生成率を、漸近の場合と遜色ないレベルにするためには、 $n$ を1Mbit以上にすべしという主張もある (Scarani-Renner 2008)
    - この場合、秘匿性増強の処理速度がボトルネックになる

( $s$  = ビット誤り訂正の  
シンドローム長)

# 量子暗号における有限長解析

- 有限長効果を厳密に考慮した安全性証明を行い、なおかつ秘密鍵生成率 $R$ を最大化する。
  - 秘密鍵生成率  $R := \text{生成した秘密鍵長} / \text{通信した光子数}$   
(量子暗号装置の通信速度に相当)
- 以下では下記の論文に基き、限長解析の概要を解説する。  
M. Hayashi and TT, New J. Phys. **14** (2012) 093014  
ここでは(1)鍵生成率 $R$ をサンプル誤り率 $p_{\text{smp}}$ に応じて可変にし、  
(2)位相誤り率の推定方式を改良することによって、  
平均として高い $R$ を実現している
  - 比較対象: [Scarani-Renner 2008], [Tomamichel et al. 2011]



# 秘密鍵の情報理論的な安全性 (統計距離による評価)

- $A, B$  : Alice, Bobの秘密鍵  
 $E$  : 盗聴者Eveの得た情報
- 現実の確率分布:  $P_{AE}$   
理想的な状況:  $U_A \times P_E$  ( $U_A$ は一様分布)
- 安全性の指標 = 上記2つの状況の統計距離:  $d(P_{AE}, U_A \times P_E)$
- 統計距離<sup>†</sup>:  $d(P_X, P_Y) := \frac{1}{2} \sum_a |P_X(a) - P_Y(a)|$
- この安全性の指標はuniversal composabilityを満たす。
- 適用例: extractor, privacy amplification

(<sup>†</sup>variational distance,  $L_1$  distance, Kolmogorov distanceなどとも呼ばれる)

# 量子暗号における秘密鍵の安全性(1/2)

## (トレース距離による評価)

- Alice, Bob, Eveの3者を表す量子状態:  $\rho_{ABE}$
- 現実の確率分布:  $\rho_{AE}$   
理想的な状況:  $\rho_U \otimes \rho_E$  ( $\rho_U$ は一様分布)
- 安全性の指標 = 上記2つの間のトレース距離:  $d(\rho_{AE}, \rho_U \otimes \rho_E)$
- トレース距離  $d(\rho, \sigma) := \text{状態 } \rho - \sigma \text{ のトレースノルム}^\dagger$
- この安全性の指標はuniversal composabilityを満たす。
  - トレース距離が距離の公理を満たす
  - あらゆる量子操作  $\Lambda$  に対して  $d(\Lambda(\rho), \Lambda(\sigma)) \leq d(\rho, \sigma)$

(†トレースノルムの定義は省略)

# 量子暗号における秘密鍵の安全性(2/2)

## (トレース距離による評価)

- 量子暗号の安全性はトレース距離の上界  $\varepsilon$  により定量的に評価する。  
Universally composable security criterion ( $\varepsilon$ -Security):  
(e.g., Ben-Or et al. 2003, Renner-Koenig 2004)

$$\|\rho_{A,E} - \rho_U \otimes \rho_E\| \leq \varepsilon$$

- 上記の  $\varepsilon$  は、位相誤り訂正の失敗率(ブロック誤り率)  $P_{\text{ph}}$  で抑えられる。  
(e.g., Koashi 2005, Hayashi 2007)

$$\|\rho_{A,E} - \rho_U \otimes \rho_E\| \leq 2\sqrt{2}\sqrt{P_{\text{ph}}},$$

$$P_{\text{ph}} = \sum_y P_{\text{pub}}(y) P_{\text{ph}|y} \quad (\text{ただし } y = \text{すべての公開情報})$$

結論として、秘密鍵の安全性はすべて  $P_{\text{ph}}$  で解析できる。

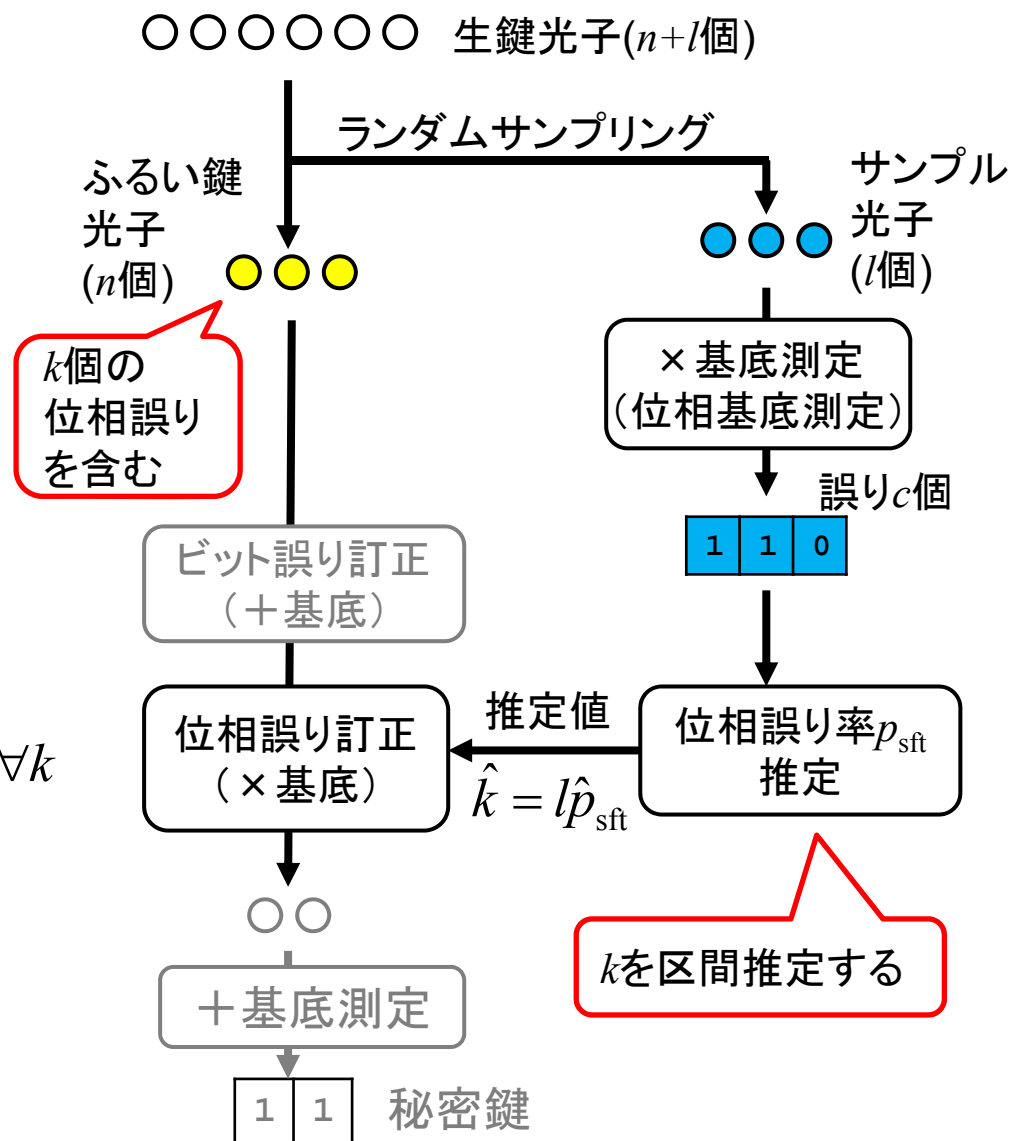
# 位相誤り率の上界の区間推定 (1/2)

- サンプルビットは非復元抽出  
→ 超幾何分布で記述される

$$P_{\text{hg}}(c|k) = \frac{\binom{n}{k-c} \binom{l}{c}}{\binom{n+l}{k}}$$

- 位相誤り率  $p_{\text{sft}}$  の上界を、失敗確率  $\varepsilon_{\text{hg}}$  で推定したい。  
...つまり以下を満たす関数  $\hat{p}_{\text{sft}}(c)$  を決定すればよい

$$\Pr[\hat{p}_{\text{sft}}(c) < p_{\text{sft}}(k, c) | k] \leq \varepsilon_{\text{hg}} \text{ for } \forall k$$



# 位相誤り率の上界の区間推定 (2/2)

これは通常の片側区間推定問題であり、以下の通り解ける。

- 簡単のため、超幾何分布  $P_k(c)$  を正規近似する。

$$\sum_{a=c}^l P_k(a) \cong \Phi\left(\frac{c-\bar{c}}{\sigma(k)}\right), \quad \Phi(y) = \frac{1}{\sqrt{2\pi}} \int_y^{\infty} dx \exp\left(-\frac{x^2}{2}\right).$$

- 危険率 = 推定の失敗確率  $\varepsilon_{\text{hg}}$  となる。  
これを正規分布の中心からのずれ  $s$  であらわす:  $\Phi(s(\varepsilon_{\text{hg}})) = \varepsilon_{\text{hg}}$ .
- このとき推定値  $\hat{p}_{\text{sft}}(c)$  の関数形は以下のとおりになる。

$$\hat{p}_{\text{sft},\varepsilon}(c) = \frac{1}{n} \left( (n+l)\hat{p}_{\varepsilon}(c) - lp_{\text{smp}}(c) \right),$$
$$\hat{p}_{\varepsilon}(c) = \frac{1}{1+4\gamma} \left( p_{\text{smp}} + 2\gamma + 2\sqrt{\gamma \{ p_{\text{smp}}(1-p_{\text{smp}}) + \gamma \}} \right),$$
$$\gamma = \frac{s^2 n}{4l(n+l-1)}$$

# ブロック誤り率 $P_{ph}$ の評価 (1/2)

1. 位相誤り率  $p_{sft}=k/n$  が既知の場合、  
ランダム符号なので結果はシンプル:  
(Gallager限界)

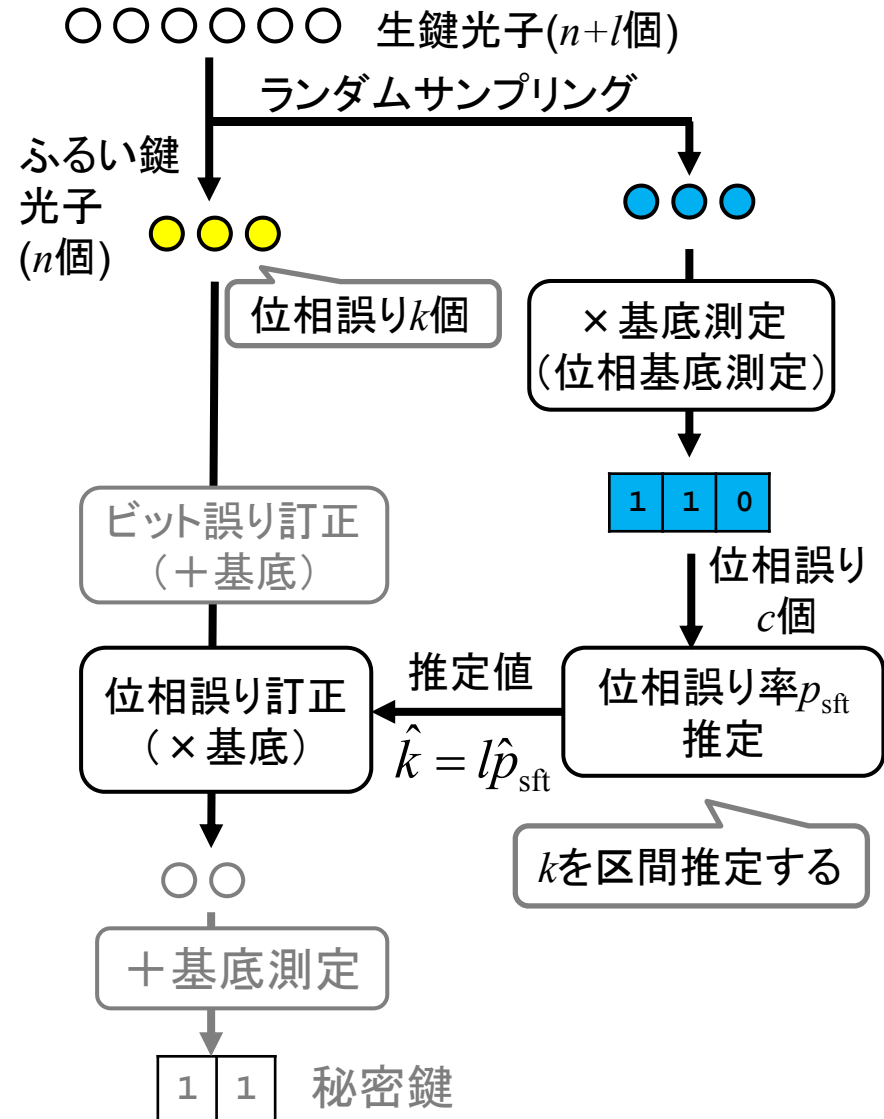
$$S_{pa}(k, c) \leq 2^{\min\{nh(p_{sft}(k, c)) - nh(\hat{p}_{sft}(c)) - D, 0\}}$$

2. 現実には  $p_{sft}=k/n$  は測定できない。  
そこで超幾何分布について平均すると  
 $p_{sft}=k/n$  に依存しない上界が得られる。

$$\begin{aligned} P_{ph} &= \sum_{c=0}^{c_{\max}} Q_{Eve}(k) P_{ph|k} \\ &\leq \sum_k \sum_c Q_{Eve}(k) P_{hg}(c|k) S_{pa}(k, c) \\ &= \sum_k Q_{Eve}(k) S_{av}(k) \leq \max_k S_{av}(k) \end{aligned}$$

$p_{sft}=k/n$  に依存しない上界

ただし  $S_{av}(k) := \sum_{c=0}^{c_{\max}} P_{hg}(c|k) S_{pa}(k, c)$



# ブロック誤り率 $P_{\text{ph}}$ の評価 (2/2)

- $\max_k S_{\text{av}}(k)$  の上界:

$c$  の和を2つの区間に分け、 $P_{\text{hg}}(c|k)$  に正規近似を適用する

$$\begin{aligned}
 S_{\text{av}}(k) &= \sum_{c=0}^{c_{\text{max}}} P_{\text{hg}}(c|k) S_{\text{pa}}(k, c) \\
 &= \sum_{c=0}^{\bar{c}(k) - s\sigma(k)} P_{\text{hg}}(c|k) S_{\text{pa}}(k, c) + \sum_{c=\bar{c}(k) - s\sigma(k) + 1}^{c_{\text{max}}} P_{\text{hg}}(c|k) S_{\text{pa}}(k, c) \\
 &\leq \underbrace{\sum_{c=0}^{\bar{c}(k) - s\sigma(k)} P_{\text{hg}}(c|k)}_{\hat{p}_{\text{sft}}(c) \text{ の定義から、} \leq \varepsilon} + \underbrace{\max_{c \in [\bar{c}(k) - s\sigma(k), c_{\text{max}}]} S_{\text{pa}}(k, c)}_{\leq 2^{-D}}
 \end{aligned}$$

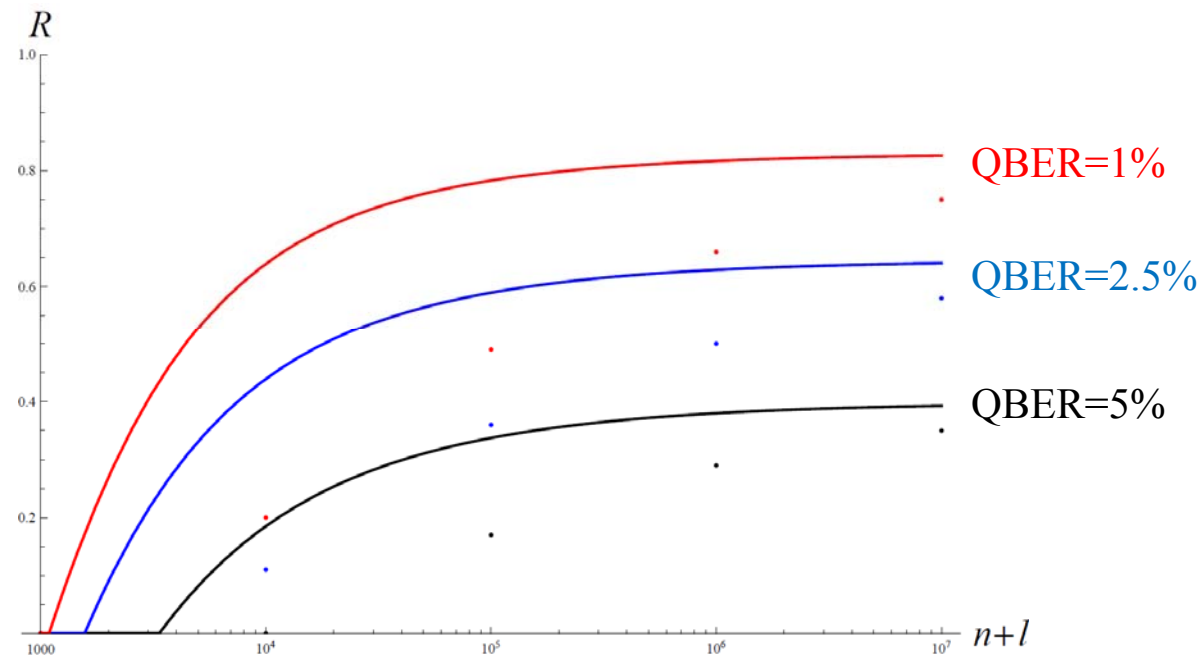
- これが任意の  $k$  について成立するので、トレース距離が抑えられる

$$\|\rho_{A,E} - \rho_U \otimes \rho_E\| \leq 2\sqrt{2}\sqrt{P_{\text{ph}}} \leq 2\sqrt{2}\sqrt{\max_k S_{\text{av}}(k)} \leq 2\sqrt{2}\sqrt{\varepsilon + 2^{-D}}$$

- さらに類似の上界が、**正規近似なし**でも導出できる

# 鍵生成率 $R$ の最適化(数値計算)

- 横軸: ふるい鍵長  $n$  + サンプルビット数  $l$
- 縦軸: 鍵生成レート  $R = \text{秘密鍵長} / n+l$
- 正規近似によらない厳密な評価



M. Hayashi and TT, New J. Phys. **14** (2012) 093014  
(同色の点はTomamichel et al. 2011の結果)

- デコイ法を考慮した解析:  
Masahito Hayashi, Ryota Nakayama, New J. Phys. 16 063009 (2014).



# 有限長解析のまとめ

- 量子暗号の安全性は、位相誤り訂正のブロック誤り率 $P_{\text{ph}}$ の上界の評価に帰着される。
- 現実の装置ではブロック長 $n$ ,  $l$ は有限であるので、有限長解析が必要。同時に秘密鍵生成率  $R := \text{生成した秘密鍵長} / \text{通信した光子数}$  を最適化する。
- 具体的には
  - ふるい鍵の位相誤り $p_{\text{sft}}$ の推定精度
  - ( $p_{\text{sft}}$ が既知の場合の)位相誤り訂正符号のブロック誤り確率を同時に考慮して最終的な $P_{\text{ph}}$ を抑える


# 秘匿性増強の効率化

— (双対)ユニバーサルハッシュ関数 —

# Universal<sub>2</sub> Hash Function

(Carter-Wegman 1979)

A family of functions  $\{f_r\}_{r \in R} = \{f_1, f_2, f_3, \dots\}$ ,  $f_r : A \rightarrow B$  is  $\varepsilon$ -almost universal<sub>2</sub>

  $\Pr[f_R(a_1) = f_R(a_2)] \leq \frac{\varepsilon}{|B|}, \quad \forall a_1 \neq a_2 \in A$

- Probability  $\Pr$  : random distribution  $r \in R$
  - “1-almost universal<sub>2</sub>” is often simply called “universal<sub>2</sub>”
- 
- Weaker condition than the completely random functions.  
ex: the Toeplitz matrix multiplication
  - Still a sufficient condition for many applications;  
information theoretically-secure authentication,  
and PA for QKD (if  $\varepsilon \leq 2$ )

# Examples of Universal<sub>2</sub> Hash Functions

Ex.1:

the Toeplitz matrix

(All diagonals are the same)

$$X_r = \begin{pmatrix} r_{n-t} & r_{n-t+1} & & r_{n-2} & r_{n-1} \\ r_{n-t-1} & r_{n-t} & r_{n-t+1} & & r_{n-2} \\ & r_{n-t-1} & r_{n-t} & r_{n-t+1} & \\ r_2 & & r_{n-t-1} & r_{n-t} & r_{n-t+1} \\ r_1 & r_2 & & r_{n-t-1} & r_{n-t} \end{pmatrix}$$

The multiplication of  $X_r$  and a vector  $v$  yields a universal<sub>2</sub> hash family  
 $y = H_r(v) := X_r v$

Ex. 2: modified Toeplitz matrix

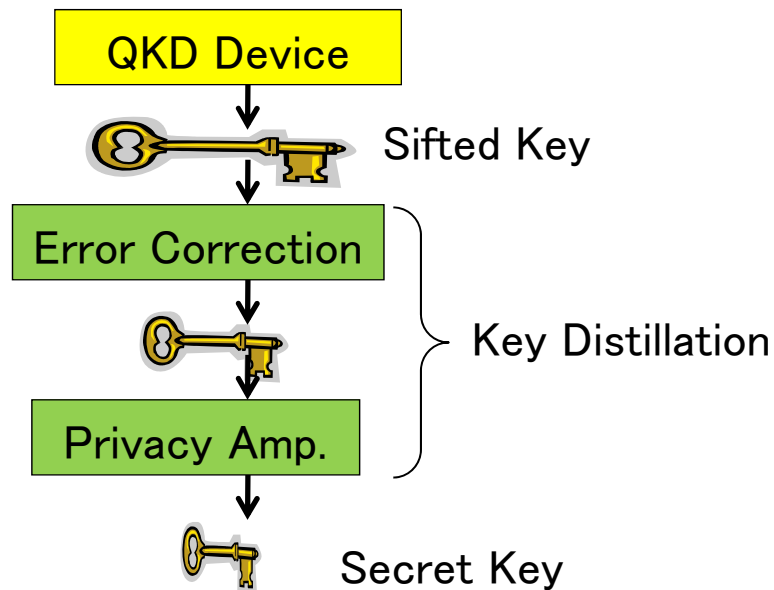
(Hayashi PRA 2009,  
Hayashi arXiv:0904.0308)

A concatenation  $(X_r, I_{n-t})$  of Toeplitz matrix  $X_r$  and the identity  $I_{n-t}$

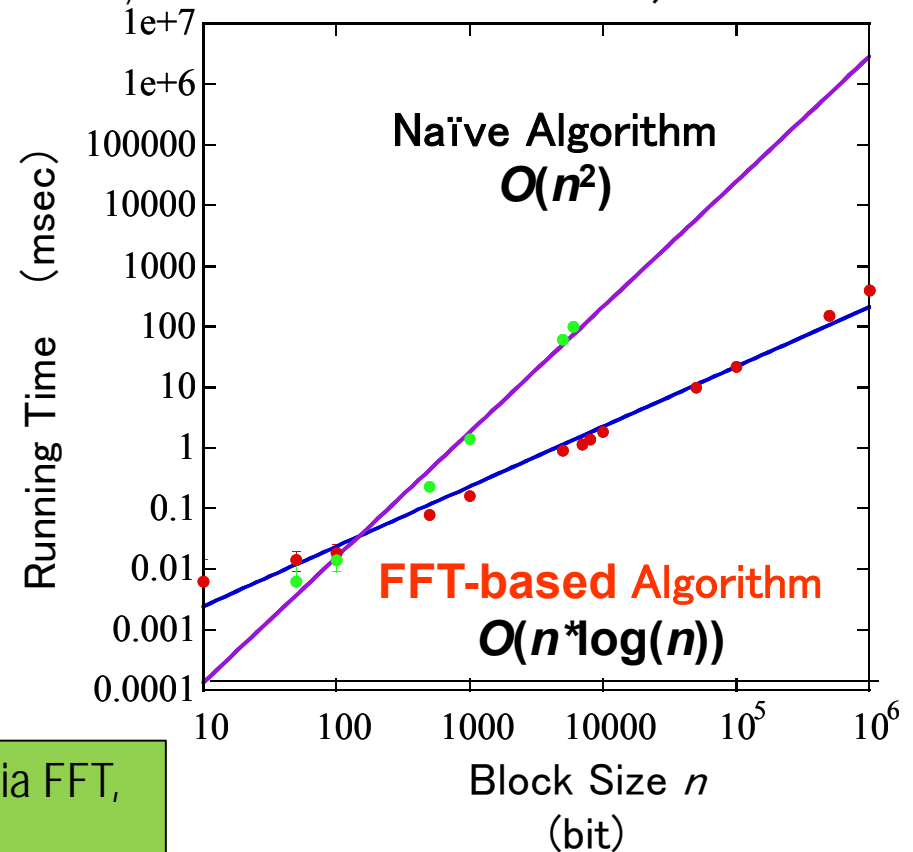
# 高速秘匿性増強アルゴリズム (FFTによるToeplitz行列演算)

As a solution to the finite size effect<sup>†</sup> of key distillation,  
we developed a new efficient algorithm for privacy amplification

<sup>†</sup>Due to statistical fluctuations of phase error, block lengths of privacy amplification must exceed  $10^6$  (Hayashi 2007; Scarani and Renner 2008)



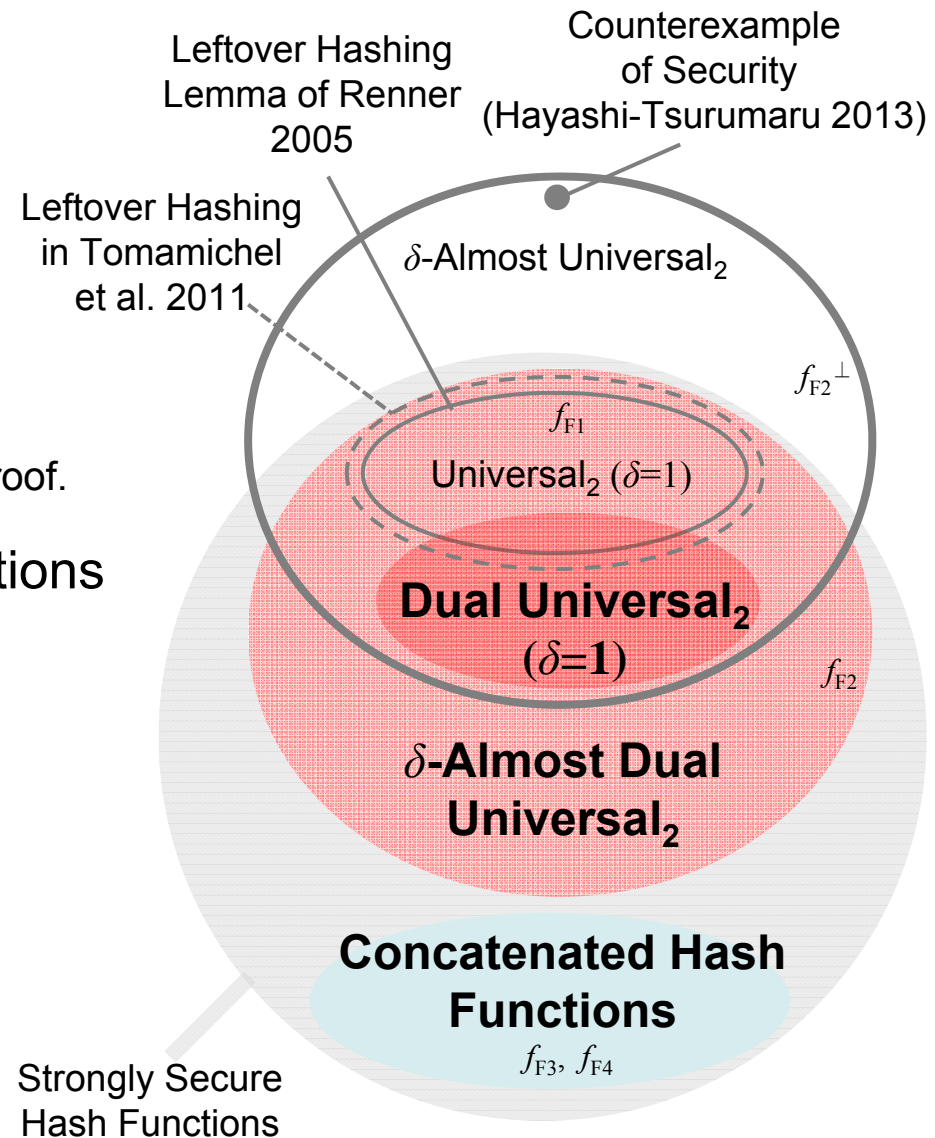
Efficient multiplication algorithm of Toeplitz matrices via FFT,  
with an almost constant running time per bit  
⇒ Privacy amplification on software for block size  $n \gg 10^6$



Running time of PA on software

# Dual Universal<sub>2</sub> Hash Functions

- Introduction of the concept and application to security proofs (T. Tsurumaru and M. Hayashi, IEEE Trans. IT 59, 4700 (2013))
  - Generalization of conventional universal hash functions
  - Allows the use of (dual) universal<sub>2</sub> hash functions in Shor-Preskill-type security proof.
- Improved and practical hash functions (M. Hayashi and T. Tsurumaru, arXiv:1311.5322)
  - Efficiently implementable hash functions with the shortest random seeds ever ( $f_{F1}, f_{F2}, f_{F3}, f_{F4}$  in the figure)
  - General methods for using non-uniform random seeds.



# Dual Universal<sub>2</sub> Hash Functions

We restrict ourselves to linear functions  $f_r$  over  $\mathbf{F}_2$

**Conventional**  $\varepsilon$ -almost universal<sub>2</sub> functions  $\{f_r: \mathbf{F}_2^n \rightarrow \mathbf{F}_2^m \mid r \in I\}$



$$\Pr[f_R(x) = 0] \leq 2^{-m} \varepsilon, \quad \forall x \neq 0 \in \mathbf{F}_2^n$$



$$\Pr[x \in \text{Ker } f_R] \leq 2^{-m} \varepsilon, \quad \forall x \neq 0 \in \mathbf{F}_2^n$$

..., the kernel  $\text{Ker } f_r$  of a linear map  $f_r$

$\varepsilon$ -almost **Dual** universal<sub>2</sub> functions  $\{f_r: \mathbf{F}_2^n \rightarrow \mathbf{F}_2^m \mid r \in I\}$



$$\Pr[x \in (\text{Ker } f_R)^\perp] \leq 2^{m-n} \varepsilon, \quad \forall x \neq 0 \in \mathbf{F}_2^n$$

(TT and M. Hayashi, IEEE Trans. IT 59, 4700 (2013);  
also see Fehr and Schaffner, TCC2008)

# Relation Between Universal<sub>2</sub> Hash Function Family and Its Dual Family

Given a surjective function family  $\{f_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^m \mid r \in I\}$

one can define its dual function family  $\{g_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^{n-m} \mid r \in I\}$

having dual kernel :  $\text{Ker } g_r = (\text{Ker } f_r)^\perp$

## Theorem

If a function family  $\{f_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^m \mid r \in I\}$  is  $\varepsilon$ -almost universal<sub>2</sub>,  
its dual family  $\{g_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^{n-m} \mid r \in I\}$  is  
 $2(1-2^{-m}\varepsilon)+(\varepsilon-1)2^{n-m}$ -almost universal<sub>2</sub>

In particular, a conventional universal hash function (with  $\varepsilon=1$ )  
is always 2-almost dual universal<sub>2</sub>.

(TT and M. Hayashi, IEEE Trans. IT 59, 4700 (2013))



# Duality Relation for Code Families

$\text{Ker } f_r \cong$  vector subspace  $V_r \cong$  linear code  $C_r$

Given a code family  $\mathbf{C} = \{C_r\}_r = \{C_1, C_2, C_3, \dots\}$ ,

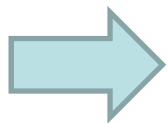
the *dual code family*  $\mathbf{C}^\perp$  of  $\mathbf{C}$  is the set of their dual codes

$$\mathbf{C}^\perp = \{C_r^\perp\}_r = \{C_1^\perp, C_2^\perp, C_3^\perp, \dots\}$$

where  $C^\perp := \{x \in \mathbb{F}_2^n \mid (x, y) = 0 \text{ for } \forall y \in C\}$

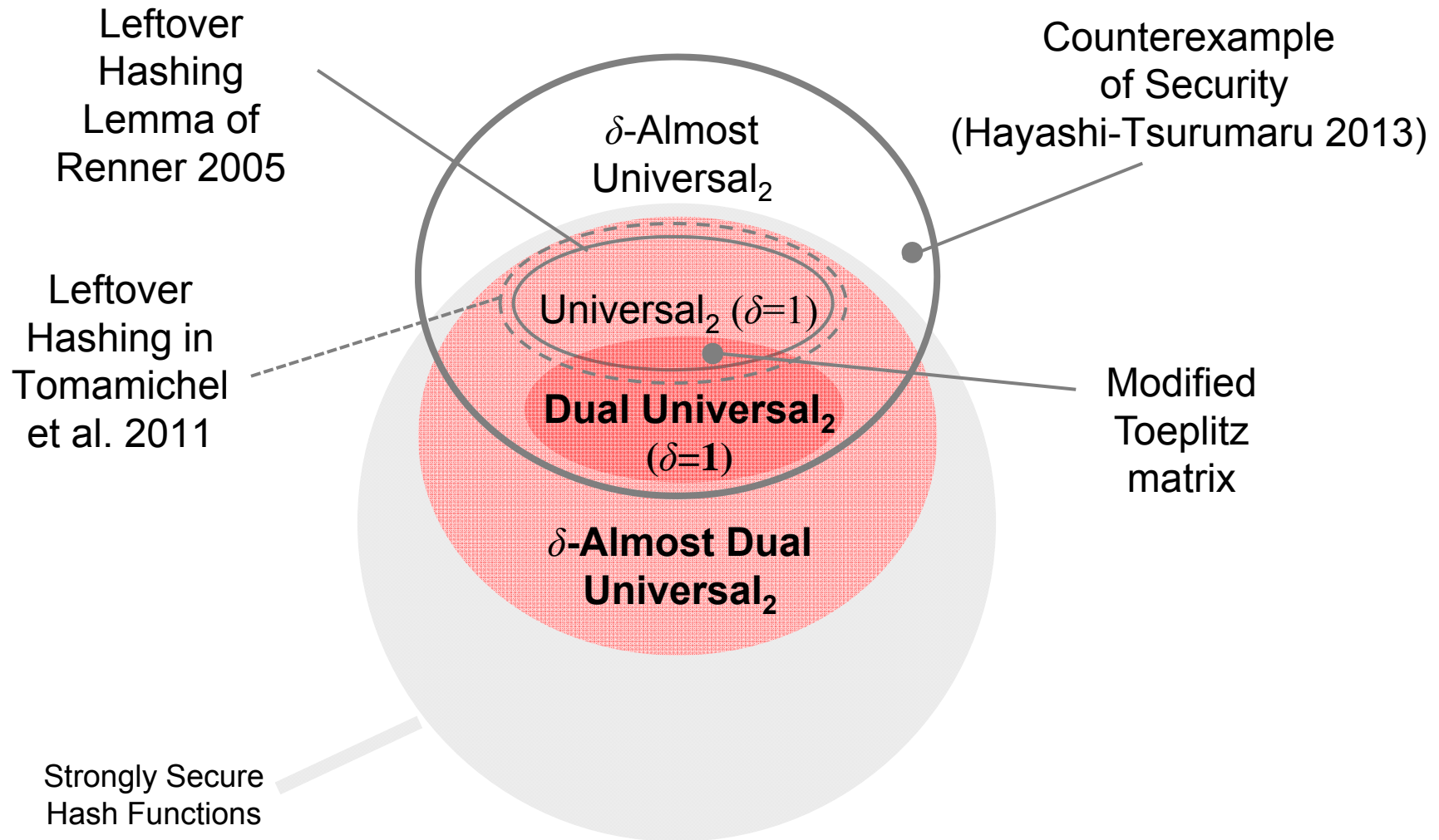
## Theorem

A linear code family  $\mathbf{C} = \{C_r\}_r$  is  $\varepsilon$ -almost universal<sub>2</sub>  
 $(C_r \subset \mathbb{F}_2^n, \dim C_r = t)$



The dual code family  $\mathbf{C}^\perp$  of  $\mathbf{C}$  is  
 $2(1-2^{t-n}\varepsilon)+(\varepsilon-1)2^t$ -almost universal<sub>2</sub>

# Classes of (Dual) Universal<sub>2</sub> Code Families and the Security of QKD



# Security Proof in Terms of Phase Error Correction

# Kernel of an $\varepsilon$ -Almost Universal<sub>2</sub> Hash Function is a Good Error Correcting Code

Any  $\varepsilon$ -almost universal<sub>2</sub> hash function is a projection:

$$f_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n / \text{Ker } f_r$$

→  $C_r \cong \text{Ker } f_r$  is a linear code with the syndrome function  $f_r$

→ Errors are mapped to syndromes uniquely

→ (Random) linear code  $C_r$  achieves the Shannon limit

**Lemma (Gallager bound)**



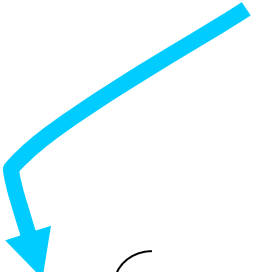
For an  $n$ -tuple use of (i.i.d.) BSC with crossover probability  $p$ , if one uses an  $\varepsilon$ -almost universal<sub>2</sub> code family  $\{C_r \subset \mathbf{F}_2^n\}_r$  of  $nR$  dimension, the ML decoding fails with error prob.  $P_e(C_r)$ , where

$$\mathbf{E}_r P_e(C_r) \leq \min_{0 < s \leq 1} \varepsilon^s 2^{-n[-sR + E_0(s, p)]}$$
$$E_0(s, p) := s - (1 + s) \log \left[ p^{\frac{1}{1+s}} + (1 - p)^{\frac{1}{1+s}} \right]$$

(Also see, e.g., Brassard-Salvail, Eurocrypt '93)

# Security of QKD

PA using  $\varepsilon$ -almost ~~dual~~ universal<sub>2</sub> function  
 $\Rightarrow$  Random code for ~~phase~~ error correction

- Equiv. by def. 
1. PA using an  $\varepsilon$ -almost ~~DUAL~~ univesal<sub>2</sub> function family
  2. PA by projection  $\mathbf{F}_2^n \rightarrow \mathbf{F}_2^n / C_r$   
 with an  $\varepsilon$ -almost ~~DUAL~~ univesal<sub>2</sub> code family  $\{C_r\}_{r \in R}$
  3. Phase error correction using code family  $\{C_r^\perp\}_{r \in R}$   
 with the syndrome function  $f_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n / C_r^\perp$   
 being  ~~$\varepsilon$ -almost univesal<sub>2</sub> function~~
- Equiv. by def. 
- 

• The Instead,  $f_r : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n / C_r$  becomes  $\varepsilon$ -almost universal<sub>2</sub>

$$E_r \chi \leq \eta_n(E_r P_e(C_r^\perp)) \leq \eta_n\left(\min_{0 \leq s \leq 1} \varepsilon^s 2^{-n[-sR + E_0(s,p)]}\right)$$

 Gallager bound

where  $nR$  bits are consumed in PA.  $\eta_n(x) := h(x) + nx$ .

• ~~The security under coherent attacks can be shown similarly.~~

# Comparison with the Conventional Universal Hash Function

(Generalized Leftover Hashing  
Lemma)

# Generalized Quantum Leftover Hashing Lemma

The security of QKD evaluated quantitatively using the trace distance:

$$d_1'(f_R(A) | E | \rho_{A,E}) := \left\| \rho_{A,E} - \rho_{\text{mix},A} \otimes \rho_E \right\|_1$$

- For *Conventional*  $\varepsilon$ -almost universal hash function:

$$\mathbb{E}_R d_1'(f_R(A) | E | \rho_{A,E}) \leq \min 2\eta + \sqrt{\varepsilon - 1 + (1 + \eta^{-2}) 2^{m - H_{\min}(A|E|\rho_{A,E})}}$$

- M. Tomamichel et al.,  
IEEE Trans. IT 57, 5524 (2012)

No security if  $\varepsilon \geq 2$

- For  $\varepsilon$ -almost *Dual* universal hash function:

$$\mathbb{E}_R d_1'(f_R(A) | E | \rho_{A,E}) \leq \sqrt{\varepsilon} 2^{\frac{1}{2}(m - H_{\min}(A|E|\rho_{A,E}))}$$

- TT and M. Hayashi, IEEE Trans. IT 59, 4700 (2013);  
Fehr and Schaffner, TCC2008
- Application to QKD  
M. Hayashi and TT, New J. Phys. 14, 093014 (2012).

Secure even for large  $\varepsilon$

# Explicit Counterexample of a Secure Conventional $\varepsilon$ -Almost Universal<sub>2</sub> Hash Function Family with $\varepsilon \geq 2$

An  $\varepsilon$ -almost universal<sub>2</sub> code family that is NOT  $\varepsilon$ -almost dual universal<sub>2</sub>

- Given a  $t$ -dimensional universal<sub>2</sub> code family  $\mathbf{C} = \{C_r\}_r$  over  $\mathbb{F}_2^n$ , one can construct another code family
$$\mathbf{C}' := \{C'_r\}_r = \{0 \| x \mid x \in C_r\}$$
that is a 2-almost universal<sub>2</sub> code family over  $\mathbb{F}_2^{n+1}$
- One cannot attain strong security by performing privacy amplification using  $\mathbf{C}'$

  $\mathbf{C}'$  is NOT  $\varepsilon$ -almost dual universal<sub>2</sub>.



# 提案方式の概要

(M. Hayashi and TT, arXiv:1311.5322)

Hash function  $f_{\mathbf{F}_2}$  over finite field  $\mathbf{F}_{2^k}$

- Input:  $x = (x_1, \dots, x_l) \in (\mathbf{F}_{2^k})^l$ ,
- Output:  $y = (y_1, \dots, y_{l-1}) \in (\mathbf{F}_{2^k})^{l-1}$ , where  $y_i = x_i + r^i x_l$
- Random seed:  $r \in \mathbf{F}_{2^k}$

This function is in fact a dual function of the well-known (conventional)  $\epsilon$ -almost universal hash function using polynomial.

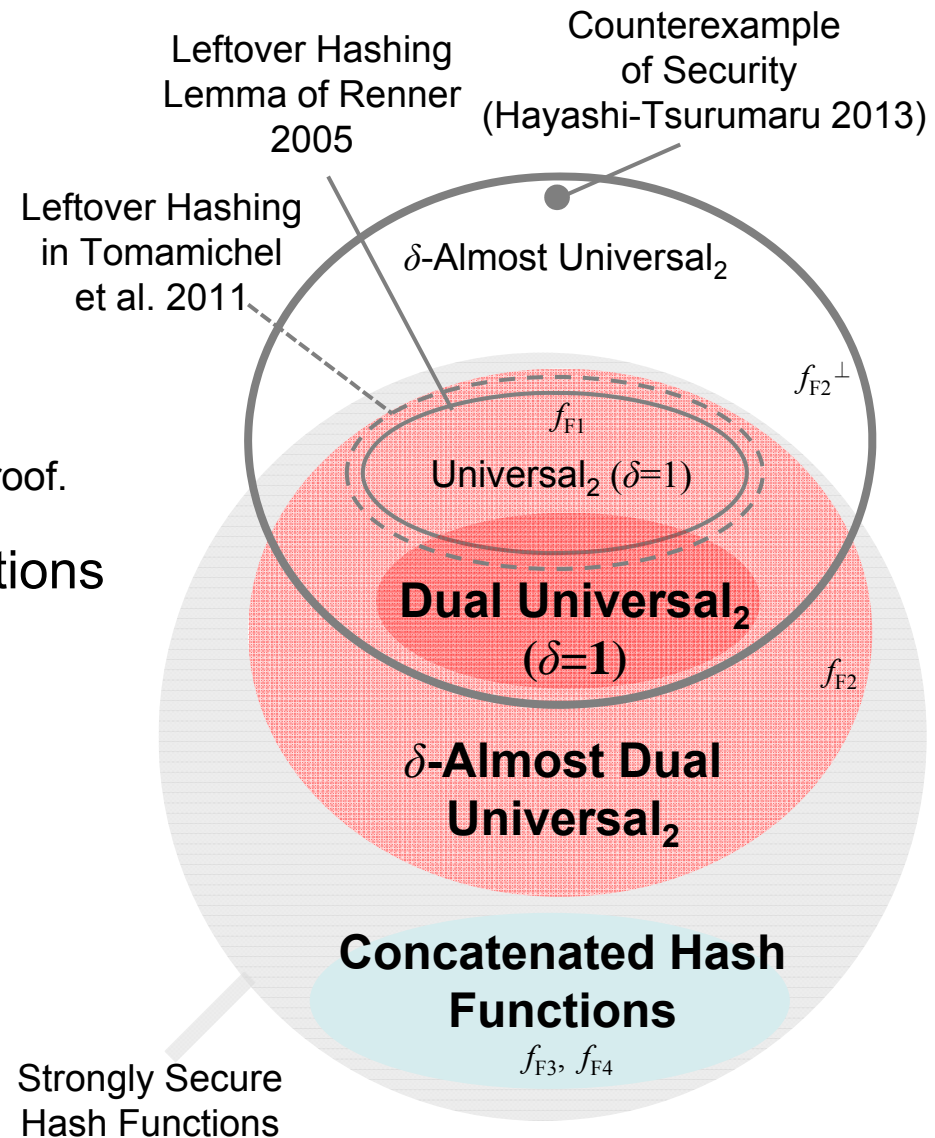
$$\text{i.e., } f_{\mathbf{F}_2, R}^\perp(x_1, \dots, x_{l-1}) = x_1 + rx_2 + r^2x_3 + \dots + r^{l-1}x_l \in \mathbf{F}_{2^k}$$

(D. Stinson, 2002)

Hash function  $f_{\mathbf{F}_3}$ ,  $f_{\mathbf{F}_4}$  are concatenations of  $f_{\mathbf{F}_2}$  and its dual  $f_{\mathbf{F}_2}^\perp$

# Dual Universal<sub>2</sub> Hash Functions

- Introduction of the concept and application to security proofs (T. Tsurumaru and M. Hayashi, IEEE Trans. IT 59, 4700 (2013))
  - Generalization of conventional universal hash functions
  - Allows the use of (dual) universal<sub>2</sub> hash functions in Shor-Preskill-type security proof.
- Improved and practical hash functions (M. Hayashi and T. Tsurumaru, arXiv:1311.5322)
  - Efficiently implementable hash functions with the shortest random seeds ever ( $f_{F1}, f_{F2}, f_{F3}, f_{F4}$  in the figure)
  - General methods for using non-uniform random seeds.



# 全体のまとめ

- 量子暗号では2種類の変調方式をランダムに使い分け、盗聴を検出する。  
直感的には「サンプル誤り率 $p_{\text{smp}}$   $\doteq$  盗聴の行為の強さ」
- 安全性証明のために仮想プロトコルを考えると、秘匿性増強が「位相誤り訂正」に置き換わる。  
→ 「秘密鍵の安全性 = 位相誤り訂正の性能」
- 量子暗号の有限長解析  
現実の量子暗号装置ではブロック長 $n$ ,  $l$ は有限である。  
以下2種類の有限長効果を考慮しつつ秘密鍵の長さを最大化する。
  - ふるい鍵の位相誤り $p_{\text{sft}}$ の推定精度
  - ( $p_{\text{sft}}$ が基地の場合の)位相誤り訂正符号のブロック誤り確率
- ブロック長 $n$ ,  $l$ の絶対値を大きくするには秘匿性増強方式(ハッシュ関数)の改良が有効 → 双対ユニバーサルハッシュ関数