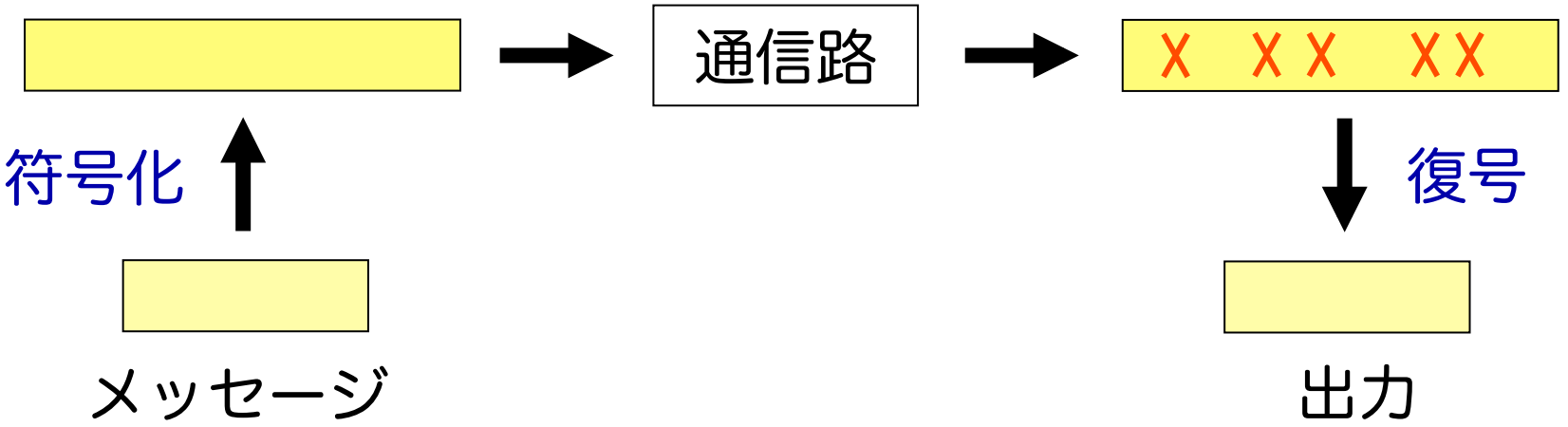
効率的に計算可能な
加法的誤りの訂正可能性

安永 憲司

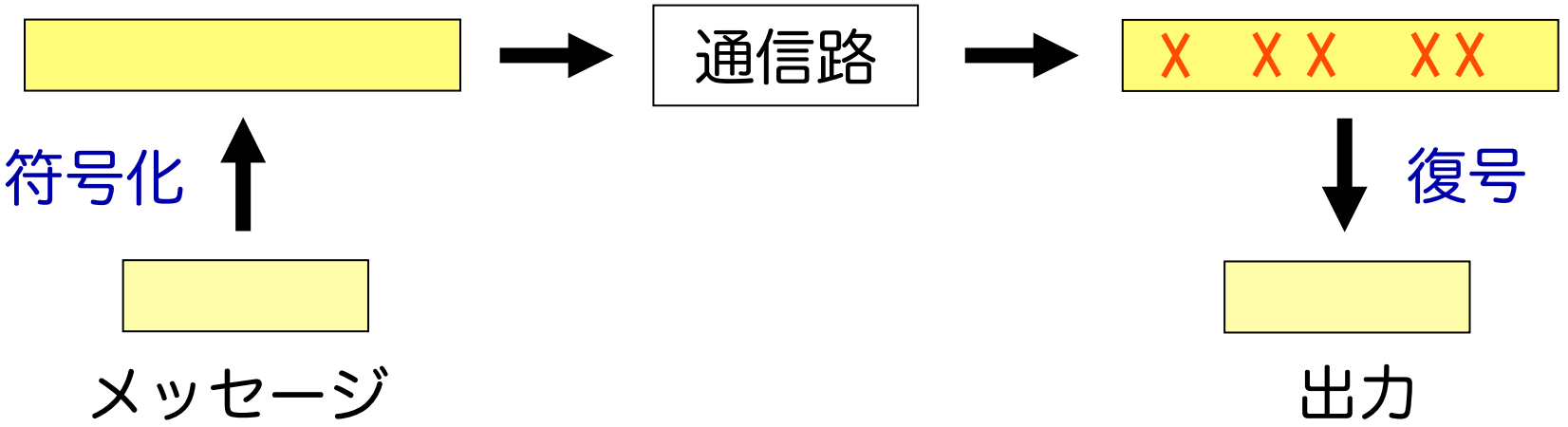
九州先端科学技術研究所

SITA 2012 @ 別府湾ロイヤルホテル 2012.12.14

誤り訂正符号

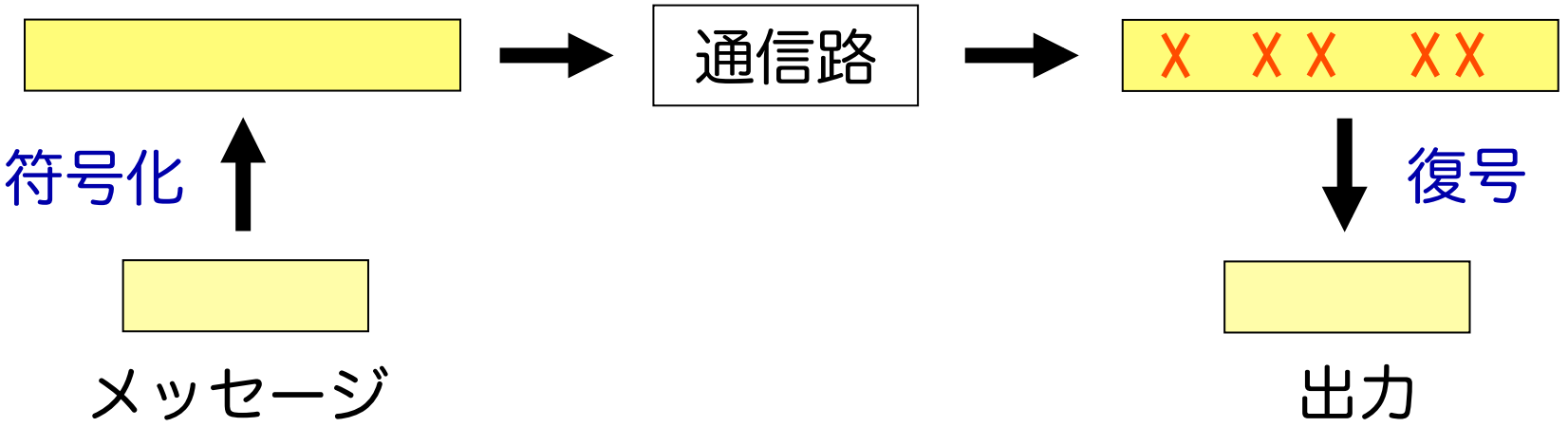


誤り訂正符号



- 多くの誤りを訂正したい
- 多くのメッセージを送りたい（高い符号化レート）

誤り訂正符号



- 多くの誤りを訂正したい
- 多くのメッセージを送りたい（高い符号化レート）

→ その限界は通信路モデルに依存

通信路モデル

通信路モデル

- 確率的通信路（二元対称通信路）
  - 各ビット毎に独立に一定確率で誤りが発生
  - 確率 $p < 1/2$ に対し
    符号化レート $1 - H(p)$ で訂正可能
    - レート $1 - H(p)$ は最適
  - 効率的な符号化・復号法が存在
    - 連接符号・Polar 符号

通信路モデル

- 最悪ケース通信路
  - 符号語に挿入される誤りの数だけを制限
  - 誤り割合 $p < 1/4$ に対し
    符号化レート $1 - H(2p)$ で訂正可能
    - レート $1 - H(2p)$ が最適化かどうかは未解決
    - 明示的な構成法・効率的な復号法の存在も未解決
  - 誤り割合 $p \geq 1/4$ だと訂正不可能
    （符号化レートが 0 でない限り）

通信路モデルのギャップ

- 確率的通信路では、単純な方法で誤りが発生

- 最悪ケース通信路では、
  符号に関する十分な知識・考察から誤りが発生

通信路モデルのギャップ

- 確率的通信路では、単純な方法で誤りが発生

  → 低コスト計算を行う通信路

- 最悪ケース通信路では、
  符号に関する十分な知識・考察から誤りが発生

  → 高コスト計算を行う通信路

計算量制限通信路

- Lipton (STACS ‘94) が導入

- 通信路の計算量は、符号長の多項式時間
  - 確率的/最悪ケース通信路の中間モデル
  - 現実的に存在するすべての通信路を含む

本研究

- 標本可能な加法的誤りの訂正限界の考察
  - 標本可能 ≈ 効率的に計算可能
  - 加法的誤り ≈ 符号語と独立な誤り

$Z : \{0,1\}^n$ 上の標本可能な分布

$$C^Z(x) = x + z,\ z \sim Z$$

以降の発表内容

- 既存の関連研究
  - 確率的/最悪ケース通信路の中間モデル
- 本研究の位置づけ・成果
  - 標本可能な加法的誤りの訂正限界
- 今後の方向性

Lipton (STACS '94)

- 計算量制限通信路 C^{comp} : $\{0,1\}^n \rightarrow \{0,1\}^n$
  - C^{comp} は多項式時間計算アルゴリズム
  - 反転可能な誤りの数は制限

- BSC に対する符号 → C^{comp} に対する符号
  - C^{comp} に秘密の共有乱数を仮定
  - 符号語を擬似ランダムに置換することで、C^{comp} の誤り → ランダム誤りに
  - 一方向性関数の存在を仮定

Micali, Peikert, Sudan, Wilson (TCC '05, IEEE IT '10)

- 計算量制限通信路 C^{comp}
- 公開鍵基盤を仮定
  - 共有乱数は仮定しない

- リスト復号可能符号 → C^{comp} に対する符号
  - 「メッセージ＋カウンター＋署名」を符号化
  - 一方向性関数の存在を仮定
  - 正しい訂正のためには、誤り数の制限が必要

Guruswami, Smith (FOCS '10)

- 共有乱数・公開鍵は仮定しない
- 誤りの数は制限

- 以下の通信路に対する効率的な符号化方式
  - 最悪ケース加法的通信路
    - 最適なレート 1 - H(p) を達成
  - 空間量制限通信路
    - 変転通信路（Arbitrarily Varying Channel）を含む
    - 一意復号ではなくリスト復号を達成

Dey, Jaggi, Langberg, Sarwate (IEEE IT ‘13(?))

- オンライン通信路
  - 符号語を1ビットずつ見て反転するかを決める
  - 誤りの数は制限
  - 共有乱数は仮定しない
  - 通信路の計算能力は制限しない

標本可能な加法的誤り

標本可能な加法的誤り

- 確率分布 Z が標本可能
  ⇔ 確率的多項式時間アルゴリズム S が存在し、
  $S(1^n)$ が Z に従って分布

標本可能な加法的誤り

- 確率分布 Z が標本可能
  ⇔ 確率的多項式時間アルゴリズム S が存在し、
  $S(1^n)$ が Z に従って分布

- 標本可能な分布 Z による
  加法的通信路 $C^Z : \{0,1\}^n \rightarrow \{0,1\}^n$
  - $C^Z(x) = x + z,\ z \sim Z$
  - 発生する誤りの数は制限しない
    - 誤り数がまばらだが規則性のある誤りを含む
  - 符号化方式は C^Z に依存して存在性を議論

標本可能な加法的誤り

- 確率分布 Z が標本可能
  ⇔ 確率的多項式時間アルゴリズム S が存在し、
  $S(1^n)$ が Z に従って分布

- 標本可能な分布 Z による
  加法的通信路 $C^Z : \{0,1\}^n \rightarrow \{0,1\}^n$
  - $C^Z(x) = x + z,\ z \sim Z$
  - 発生する誤りの数は制限しない
    - 誤り数がまばらだが規則性のある誤りを含む
  - 符号化方式は C^Z に依存して存在性を議論

  → どのような Z なら訂正可能か？

訂正可能性に関する考察

訂正可能性に関する考察

- H(Z) = 0 ならば簡単に訂正可能
  - 誤りの系列を知っているので

訂正可能性に関する考察

- H(Z) = 0 ならば簡単に訂正可能
  - 誤りの系列を知っているので
- H(Z) = n ならば訂正不可能
  - 受信系列は乱数

訂正可能性に関する考察

- H(Z) = 0 ならば簡単に訂正可能
  - 誤りの系列を知っているので
- H(Z) = n ならば訂正不可能
  - 受信系列は乱数
- H(Z) = n･H(p) のとき
  レート R > 1 - H(p) では訂正不可能
  - Z = BSC_p を計算できる場合

標本可能な Z の訂正可能性

- $H(Z) \leq n^{\varepsilon}$ で効率的に訂正できない Z が存在
  - 任意の $0 < \varepsilon < 1$

標本可能な Z の訂正可能性

- $H(Z) \leq n^{\varepsilon}$ で効率的に訂正できない Z が存在
  - 任意の $0 < \varepsilon < 1$
- 証明
  - 擬似乱数生成器 $G : \{0,1\}^m \rightarrow \{0,1\}^n$ に対し $Z = G(U_m)$ とする
  - $y = x + G(U_m)$ から x を効率的に復号できると、$G(U_m)$ が擬似ランダムであることに矛盾
  - 一方向性関数の存在を仮定した場合、任意の $0 < \varepsilon < 1$ について $m = n^{\varepsilon}$ とできる

シンドローム復号による訂正可能性

- $H(Z) = \omega(\log n)$ のとき
  レート $R > \Omega((\log n)/n)$ では
  シンドローム復号による効率的な訂正は不可能
  - あるオラクルへのアクセスを許すとき

シンドローム復号による訂正可能性

- $H(Z) = \omega(\log n)$ のとき
  レート $R > \Omega((\log n)/n)$ では
  シンドローム復号による効率的な訂正は不可能
  - あるオラクルへのアクセスを許すとき
- 証明
  - $H(Z) = \omega(\log n)$ で長さ $< n - \Omega(\log n)$ に効率的に圧縮できない標本可能分布が存在 (Wee '04)
    - あるオラクルへのアクスを許すとき
  - レート R で Z をシンドローム復号訂正可能
    $\Leftrightarrow$ Z を長さ $n(1 - R)$ に線形圧縮可能

訂正可能性のまとめ

- 標本可能な Z による加法的誤りの訂正可能性

H(Z)	訂正可能性
0	効率的に訂正可能
$\omega(\log n)$	レート $R > \Omega((\log n)/n)$ で シンドローム復号による 効率的な訂正は不可能
n^{ε} for $0 < \varepsilon < 1$	効率的に訂正不可能
$n \cdot H(p)$ for $0 < p < 1$	レート $R > 1 - H(p)$ では 訂正不可能
n	訂正不可能

今後の研究

- 無損失濃縮器との関係
  - 濃縮器: エントロピーを高くする関数
  - 平坦分布 Z に対する線形無損失濃縮器
    ⇔ 加法的誤り Z を線形関数で訂正可能
    - Cheraghchi (ISIT '09)
    - 復号の効率性は考えていない

  → 標本可能な Z に対する
  無損失濃縮器の存在の可能性を探る

まとめ

- 中間的な通信路モデルとして
  標本可能な加法的誤り通信路
- 訂正限界の考察
- 今後の課題
  - 訂正可能な Z の特徴付け
  - 訂正可能性に関する議論

オラクルアクセスについて

- $H(Z) = \omega(\log n)$ のとき
  レート $R > \Omega((\log n)/n)$ では
  シンドローム復号による効率的な訂正は不可能
  - あるオラクルへのアクセスを許すとき

- (a) から (b) のブラックボックス構成は存在しない

  (a) $H(Z) = \omega(\log n)$ の Z

  (b) Z をシンドローム復号で効率的に訂正する
  レート $R > \Omega((\log n)/n)$ の符号