スパース重ね合わせ符号と辞書の離散化について

On Sparse Superposition Codes and Discretization of Their Dictionaries

研究集会『情報通信の技術革新のための基礎数理』

九州大学 大学院システム情報科学研究院
武石　啓成

2022年9月15日

九州大学

本講演の目標

- スパース重ね合わせ符号(SS符号)[1,2]の基礎と今後の展望についてご紹介する
  - 辞書の離散化に関する研究[3,4]の紹介

- 誤り訂正符号が専門でない方にもなるべくわかりやすく説明

[1] A. R. Barron and A. Joseph, "Least squares superposition coding of moderate dictionary size, reliable at rates up to channel capacity," *Proc. Int. Symp. Inf. Theory*, Austin, Texas, June 13–18, 2010, pp. 275–279.
[2] A. R. Barron and A. Joseph, "Towards fast reliable communication at rates near capacity with Gaussian noise," *Proc. IEEE. Int. Symp. Inf. Theory*, Austin, Texas, Jun. 13–18, 2010, pp. 315–319.
[3] Y. Takeishi, M. Kawakita, and J. Takeuchi, "Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2737–2750, May 2014.
[4] Y. Takeishi and J. Takeuchi, "An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary," *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.

自己紹介

- 職歴
  - 2013年4月-2021年2月
    三菱電機インフォメーションネットワーク株式会社に勤務
    ネットワーク系システムエンジニアの業務に従事
  - 2022年4月-現在
    九州大学 大学院システム情報科学研究院 助教

- 研究分野

  スパース重ね合わせ符号(2012年～)

  深層学習の原理(2021年～)

  機械学習応用:サイバーセキュリティ, MRI高速化 (2022年～)

1. スパース重ね合わせ符号(SS符号)のレビュー
2. 辞書の離散化
3. 最近の研究動向

1. スパース重ね合わせ符号(SS符号)のレビュー

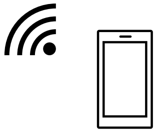
2. 辞書の離散化

3. 最近の研究動向

誤り訂正符号とは

- ノイズのある伝送路を通じて，正しく情報伝送を行うための理論
  - 現代の情報通信社会では欠かすことの出来ない技術

    応用例：携帯電話の無線通信，TVの衛星放送など…
  - 目標：高速で，誤りの少なく，小さい計算量を達成出来る符号を構築したい！



SS符号とは

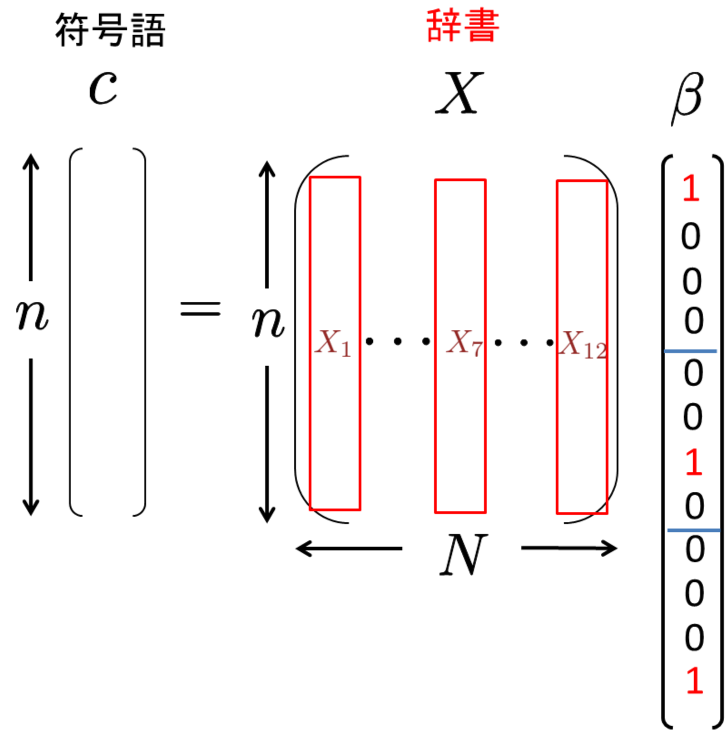
- Sparse Superposition Codes (Sparse Regression Codes とも)
- 通信速度の理論的限界を低計算量で達成できることが証明[5]
  - Polar符号[6], 空間結合LDPC符号[7]に続いて3つめ
  - ガウス通信路(AWGN Channel)に直接適用できるのが特徴

    →現実の通信路に近い設定：変調が不要

[5] A. Joseph and A. R. Barron, “Fast sparse superposition codes have near exponential error probability for R < C. *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 919–942, Feb 2014.
[6] E. Arikan, “Channel polarization,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
[7] S.Kudekar, T. J. Richardson, and R. Urbanke, “Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp.803–834, Feb 2011.

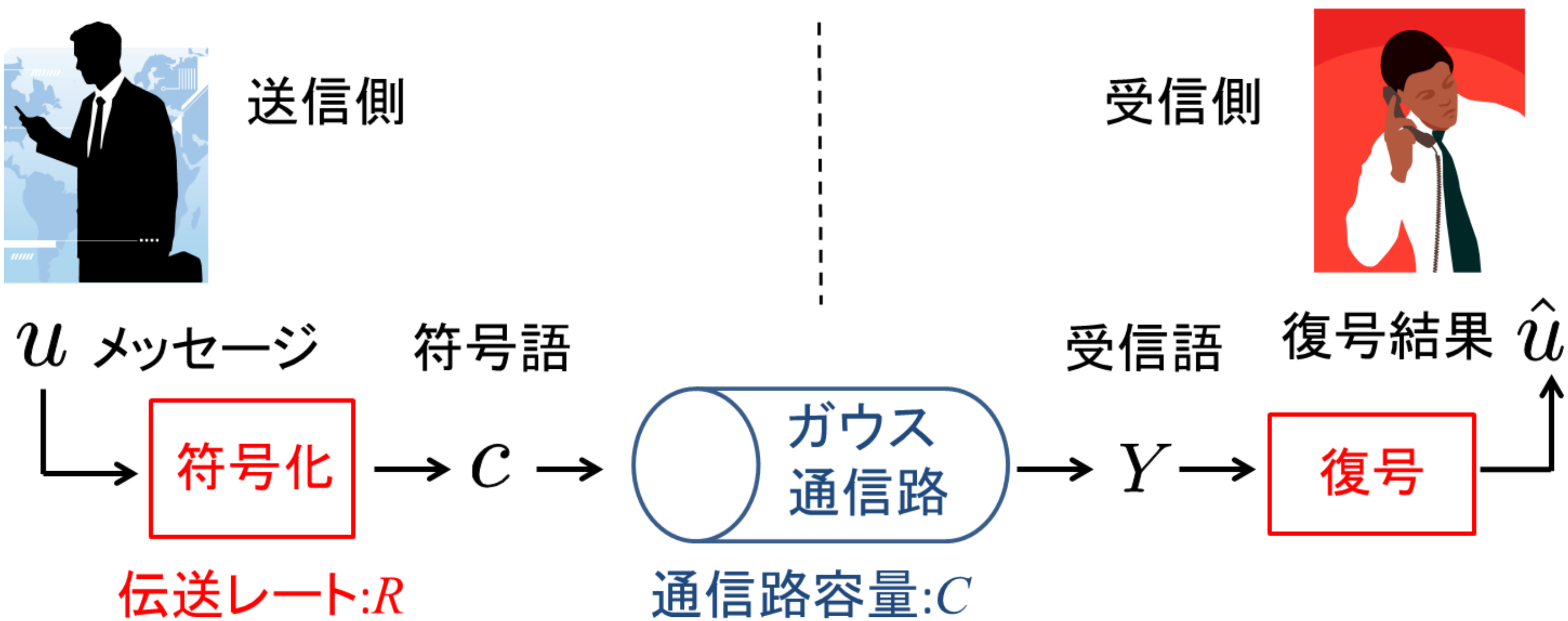
SS符号の特徴

- 非常にシンプルな符号化方法:
  辞書のスパースな足し合わせ
- 圧縮センシング，多重アクセス通信路等，他分野とも密接な関係



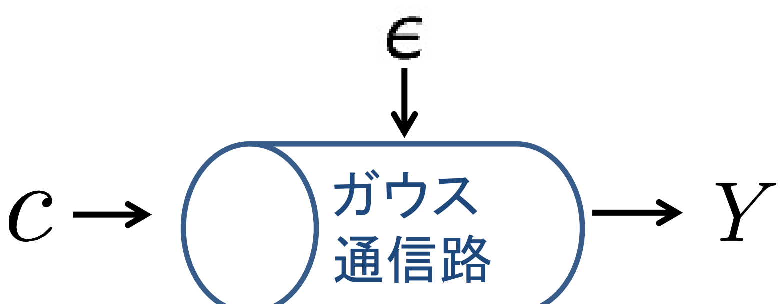
誤り訂正符号の問題設定

- ノイズのある通信路上で送信側から受信側に正しくメッセージを届けたい
- 復号誤り確率 $\Pr\{\hat{u} \neq u\}$ を抑えつつ，なるべく高い伝送レートを達成することが目標



ガウス通信路

- 入力: c,　出力: Y, ノイズ:ϵ　　$c, Y, \epsilon \in \Re^n$
  $Y = c + \epsilon$, $\epsilon_i \sim N(0, \sigma^2)$（各次元は独立）
- c の平均電力を $(1/n)\sum_{i=1}^{n} c_i^2$ で定義
  任意のc の平均電力がP 以下の制約をおく
- K ビットのメッセージ$u \in \{0,1\}^K$ をこの通信路で送信
  (各メッセージの生起確率は$1/2^K$)
  →伝送速度 : $R = K/n$ (bit/transmission)



達成可能レートと通信路容量

- 伝送速度(レート)R において，$\lim_{n\to\infty} \Pr\{\hat{u} \neq u\} = 0$ を満たす符号の列が存在するとき，達成可能(achievable)であると定義する

- すべての達成可能なレートの上限を通信路容量と呼ぶ

- 平均電力制限P でのガウス通信路の通信路容量[7]：

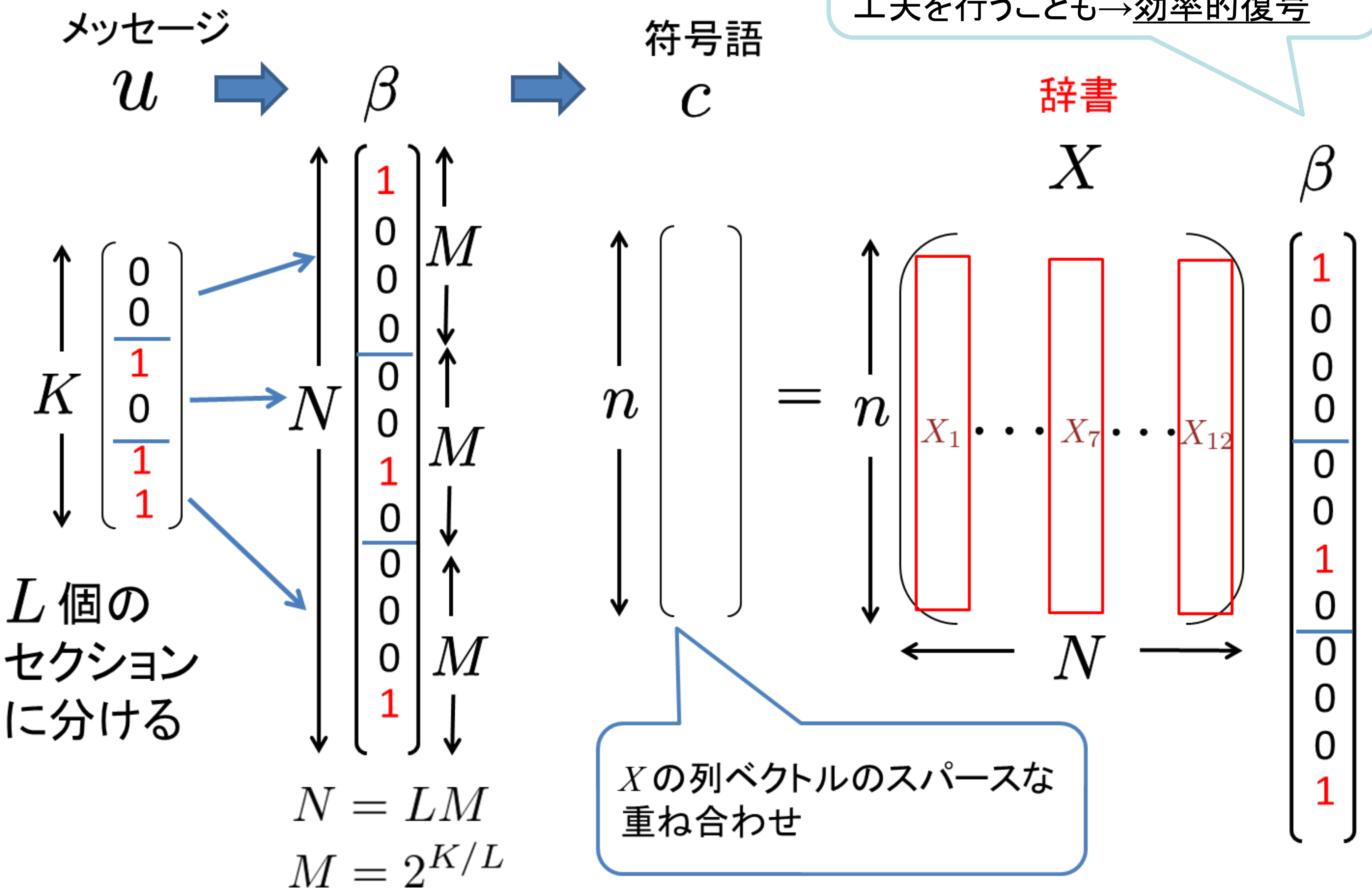
$$C = \max_{p(c_i):\mathbb{E}c_i^2 \le P} I(c_i; Y_i)$$

$$= \frac{1}{2}\log(1+v) \quad (v = P/\sigma^2)$$

[7] C. E. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J.*, vol.27, pp. 379–423, 1948.

SS符号の符号化

非零要素の大きさをセクション毎に変える(指数的に小さくする)工夫を行うことも→効率的復号



辞書Xについて

- $X_{i,j}$ は独立に$N(0, P/L)$ から生成
  $\rightarrow$ このとき符号語の各要素c_i は独立に$N(0, P)$に従う
  この分布は通信路の相互情報量$I(c_i; Y_i)$ を最大化
  ※平均電力$(1/n)\sum_{i=1}^{n} c_i^2$ はP の近くに集中
- 辞書は $n \times N$ 行列
  $\rightarrow M = L^a$ とすることで, N はn に関する多項式オーダーとなる
  (実装可能なサイズ)

$$K = L\log_2 M = aL\log_2 L$$
$$n = (aL\log_2 L)/R$$
$$\Rightarrow$$
$$L = O(n)$$
$$N = LM = L^{a+1} = O(n^{a+1})$$

復号

- $Y = X\beta + \epsilon \quad \epsilon_i \sim N(0, \sigma^2)$

→ 受信語Yと辞書Xが与えられたもとでβを推定

線形回帰と同様の枠組み

本発表の対象

1. 理想的復号(最尤復号): $\hat{\beta} = \underset{\beta \in \mathcal{B}}{\operatorname{argmin}} \|Y - X\beta\|^2$

$\mathcal{B} = \{\beta \in \{0,1\}^N \mid \beta$は各セクションに一つだけ1をもつ$\}$

→計算量的に困難であるが，SS符号の理論的性能限界を知る上で重要

2. 効率的復号：適応的逐次復号アルゴリズム[2]

→計算量は符号長nに対して$O(n)$

[2] A. R. Barron and A. Joseph, “Towards fast reliable communication at rates near capacity with Gaussian noise,” *Proc. IEEE. Int. Symp. Inf. Theory*, Austin, Texas, Jun. 13–18, 2010, pp. 315–319.

準備

復号を誤ったセクションの数

- $\mathcal{E}_{\alpha_0} = \{mistakes \geq \alpha_0 L\}$
  → 復号を誤ったセクションの割合(セクション誤り率)がα_0 以上になる事象

- $$w_v = \frac{v}{[4(1+v)^2]\sqrt{1+(1/4)v^3/(1+v)}}$$

- $$g(x) = \sqrt{1+4x^2} - 1$$

$$\rightarrow \quad g(x) \geq \min\{\sqrt{2}x, x^2\} \quad \text{for all} \quad x \geq 0$$

Theorem 1 [8]

$C - R = \Delta_n = \Omega((\log L)^{1/2}/n^{1/2})$
で n に関して指数的に0に近づく

X は各要素独立に $N(0, P/L)$ から生成する.
$R < C$とし，セクションサイズ率 a は $a \geq a_{v,L}$ を満たすものとする．このとき，$0 \leq \alpha_0 \leq 1$ に対して,

$\Pr[\mathcal{E}_{\alpha_0}] = e^{-nE(\alpha_0, R)}$ が成り立つ．ただし,

$E(\alpha_0, R) \geq h(\alpha_0, C - R) - \ln(2L)/n$

$h(\alpha, \Delta) = \min\left\{\alpha w_v \Delta, \frac{1}{4} g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}$ である.

$h(\alpha_0, C - R) = \Omega((C - R)^2)$

注意：確率変数は，ノイズϵ だけでなく，辞書X も含めて考えている

[8] A. Joseph and A. R. Barron, “Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2541–2557, May 2012.

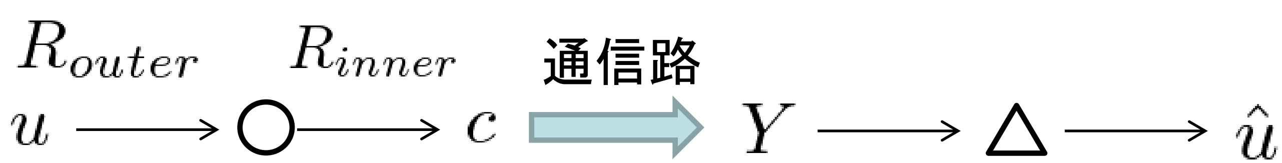
ブロック誤り確率 $\Pr\{\hat{u} \neq u\}$ の評価

- SS符号のセクション誤り率がα_0以下であれば，
  $R_{outer} = 1 - 2\alpha_0$のRS符号[9]により正しく復号できる
  →ブロック誤りが起こらない

$C - R_{inner}$

- 先の定理で$\alpha_0 = \Delta_n$ とおくと，$R_{tot} = (1 - 2\Delta_n)(C - \Delta_n)$
  でブロック誤り確率を $O(\exp\{-nd\Delta_n^2\})$ にできる　d: 正定数

$$R_{tot} = R_{outer} R_{inner}$$



[9] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. SIAM*, vol. 8, pp. 300–304, Jun. 1960.

有限長での実現可能なレート[8]

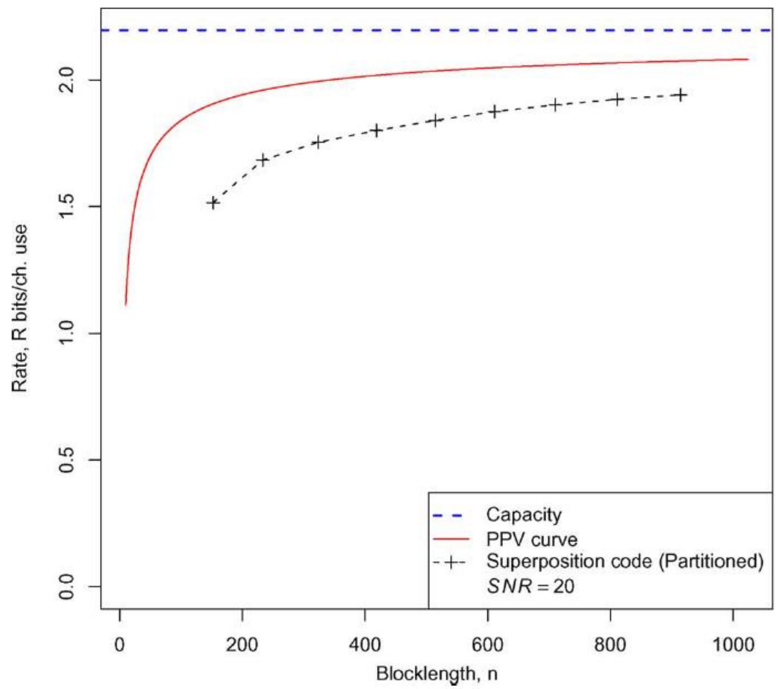
- 各符号長で誤り確率10^{-4}を実現出来る伝送速度をグラフ化
  - PPV curve [10] との比較

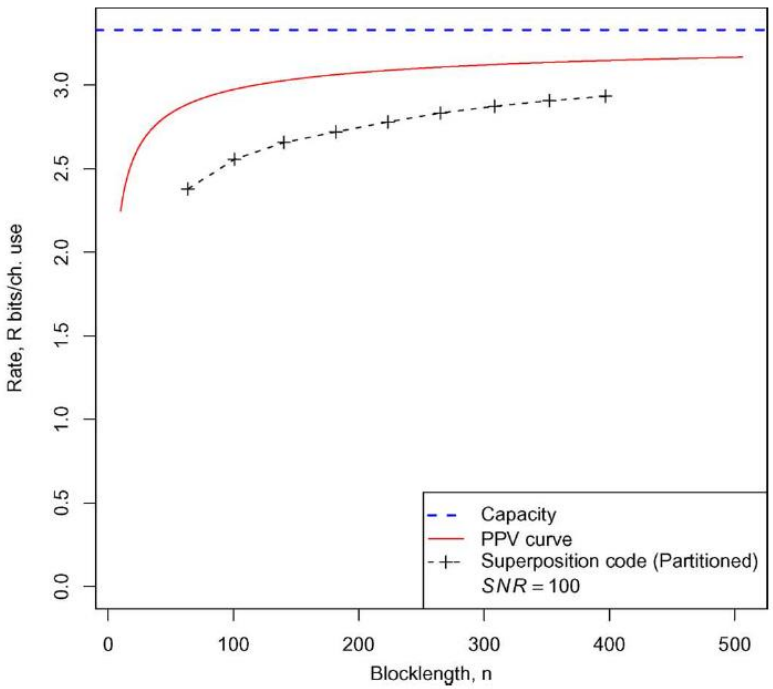
[10] Y. Polyanskiy, H. V. Poor, and S. Verdu, " Channel coding rate in the finite block length regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

$$R \approx C - \sqrt{\frac{V}{n}} Q^{-1}(\epsilon) + \frac{1}{2}\frac{\log n}{n}$$

$V = (v/2)(v+2)\log^2 e/(v+1)^2$

Q^{-1} : inverse normal cumulative distribution function





Theorem 1の証明(概要)

- $\|Y - X\beta\|^2 \leq \|Y - X\beta^*\|^2$となる$\beta$ が存在する確率を評価

- 上記の事象が起きる確率をマルコフの不等式を使って，指数的に小さくなる確率で上から抑える

→$\mathbb{E}_Z[\exp\{T(Z)\}]$の計算が必要

ただし Z は X のいくつかの要素とノイズの線形結合であり,

$T(Z)$はZ の二次関数である

→ Z は正規分布に従うため, この期待値は具体的に計算できる

1. スパース重ね合わせ符号(SS符号)のレビュー
2. 辞書の離散化
3. 最近の研究動向

研究成果概要 [3,4]

$N(0, P/L)$

- オリジナルのSS符号では，辞書の各要素を正規分布から生成
  →厳密には実装出来ない問題あり
- 正規分布の代わりに，2値のみを取るベルヌーイ分布で生成
  →確率1/2で$\sqrt{P/L}$，確率1/2で$-\sqrt{P/L}$をとる

乱数生成が大幅に簡略化

- Barron and Josephの予想：
  $L \to \infty$ で符号語の分布はオリジナルと同じ正規分布に近づくため，この場合もCを達成すると予想

→本研究：最尤復号において，Cを達成することを証明

[3] Y. Takeishi, M. Kawakita, and J. Takeuchi, “Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity,” *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2737–2750, May 2014.
[4] Y. Takeishi and J. Takeuchi, “An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary,” *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.

Theorem 2 [4]

X は各要素独立に前ページのベルヌーイ分布から生成する.
$R < C$とし，セクションサイズ率 a は $a \geq a_{v,L}$ を満たすものとする．このとき，$0 \leq \alpha_0 \leq 1$ に対して,

$\Pr[\mathcal{E}_{\alpha_0}] = e^{-nE(\alpha_0,R)}$ が成り立つ．ただし,

$E(\alpha_0, R) \geq h(\alpha_0, C-R) - \ln(2L)/n - \iota(L)$

$h(\alpha,\Delta) = \min\left\{\alpha w_v \Delta, \frac{1}{4} g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}$ である.

$\iota(L) = O(1/\sqrt{L}) \to 0$

$C - R = \Delta_n = \Omega(1/L^{1/4})$で
n に関して指数的に0に近づく

比較：正規分布の辞書の場合は
$C - R = \Delta_n = \Omega((\log L)^{1/2}/n^{1/2})$
で n に関して指数的に0に近づく

[4] Y. Takeishi and J. Takeuchi, “An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary,” *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.

Theorem 2の証明(概要)

- Theorem 1と基本的に同じ方針で証明
- しかし，この場合の期待値 $\mathbb{E}_Z[\exp\{T(Z)\}]$ は具体的に計算不可 (X の要素の和は二項分布に従う)

- この期待値が，正規分布の場合の値のおよそ1倍で上から抑えられることを示す

$1 + \delta \ (\delta > 0)$

→ これを示すために，以下の二つの補題を利用

Lemma 1 [3]

[3] Y. Takeishi, M. Kawakita, and J. Takeuchi, "Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2737–2750, May 2014.

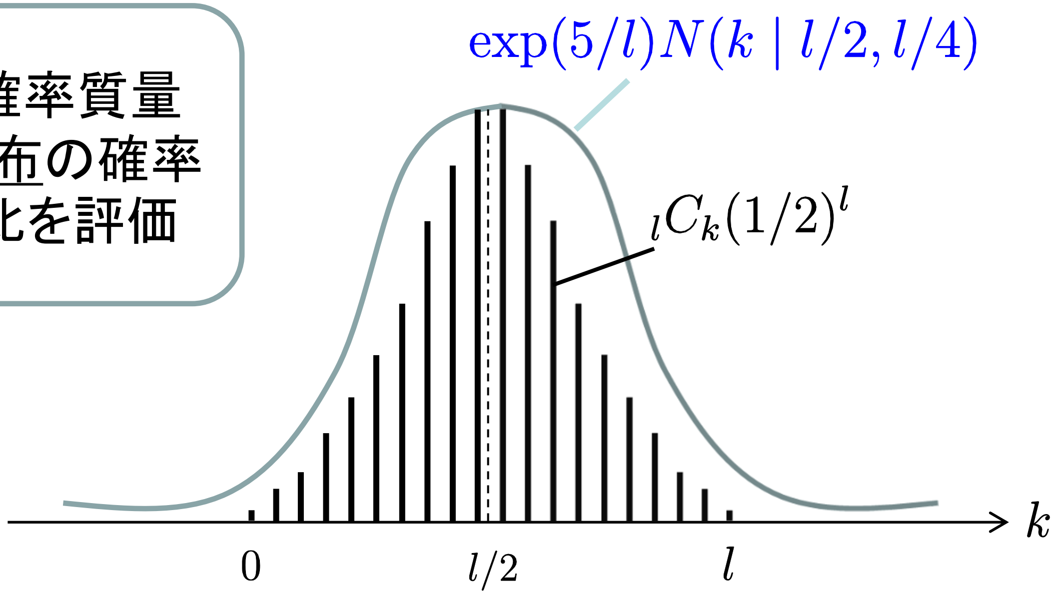
- 1000より大きい自然数 l について，以下が成り立つ

$$\max_{k\in\{0,1,\ldots,l\}} \frac{{}_lC_k(1/2)^l}{N(k\mid l/2, l/4)} \leq \exp(5/l)$$

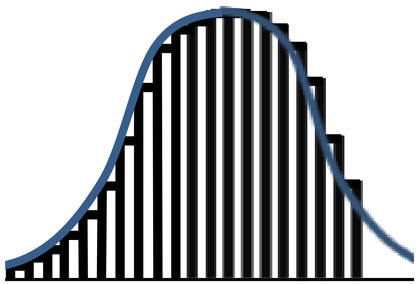
$1+O(1/l)$

$N(x|\mu,\sigma^2)=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$: 正規分布の確率密度関数

二項分布の確率質量関数と正規分布の確率密度関数の比を評価



Lemma 2 [4]



- 自然数l について, $h = 2/\sqrt{l}$,

  $\mathcal{X} = \{h(k - l/2) \mid k = 0,1,\ldots,l\}$ を定義する.

  さらに, $s^2 > 0$, $\mu \in \Re$ について

  $$I_d = h \sum_{x \in \mathcal{X}} \exp\left\{-\frac{s^2}{2}(x-\mu)^2\right\}$$

  $$I_c = \int_{-\infty}^{\infty} \exp\left\{-\frac{s^2}{2}(x-\mu)^2\right\} dx = \sqrt{2\pi/s^2}$$

  を定義する. このとき以下が成り立つ.

  $$I_d \leq (1 + 0.37s^2/l)\, I_c$$

離散分布と連続分布の違いによる, 区分求積の誤差を評価

[4] Y. Takeishi and J. Takeuchi, “An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary,” *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.

Theorem 2の証明(概要)

- Theorem 1と基本的に同じ方針で証明
- しかし，この場合の期待値 $\mathbb{E}_Z[\exp\{T(Z)\}]$ は具体的に計算不可 (X の要素の和は二項分布に従う)

- この期待値が，正規分布の場合の値のおよそ1倍で上から抑えられることを示す

$1 + O(1/l)$
l :二項分布の試行数
→ l について，セクション誤りの数と誤らなかった数の両方を考える必要がある
→$l \geq \sqrt{L}$ のとき上記の評価を行い，それ以外は別の評価を行う

1. スパース重ね合わせ符号(SS符号)のレビュー

2. 辞書の離散化

3. 最近の研究動向

Approximate Message Passing(AMP)による復号

- 圧縮センシングで用いられる効率的アルゴリズム
  – Rushら：SS符号の復号に用いることで，n に関して指数的に小さい誤り確率を達成[11]
  – 波多江ら：残差の推定値の求め方を工夫することで，n が小さい場合にも性能を改善[12]
  – 押川ら，飯田ら：上記のAMPの反復解法に「アンロール」を適用することで性能向上[13,14]

[11] C. Rush, and R. Venkataramanan, “The Error Exponent of Sparse Regression Codes with AMP Decoding,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2478–2482, 2017
[12] 波多江優和, 三村和史, 川喜田雅則, 竹内純一, “スパース重ね合わせ符号のためのBayes 最適AMP 復号器,” 電子情報通信学会技術研究報告, vol. 117, no. 487, IT2017-127, pp. 143-148, 2018 年3月.
[13] 押川祐也, 三村和史, 竹内純一, “スパース重ね合わせ符号のためのTrainable Bayes 最適AMP 復号器, ” 電子情報通信学会技術研究報告, vol. 118, no. 433, IT2018-44, pp. 55-60, 2019 年1月.
[14] 飯田昌澄, 押川祐也, 三村和史, 竹内純一, "深層学習によるスパース重ね合わせ符号の改良," 電子情報通信学会技術研究報告, vol. 119, no. 47, IT2019-13, pp. 67-72, 2019 年5月.

現在私が取り組んでいる研究内容

- ベルヌーイ辞書の場合の誤り確率の評価[4](最尤復号)は二項分布に拡張できる
  - $\tilde{X}$: $n \times (DN)$ 行列

$$\tilde{X}_{ij} = \begin{cases} -\sqrt{P/(DL)} & \text{確率}1/2 \\ \sqrt{P/(DL)} & \text{確率}1/2 \end{cases}$$

  - $X_{ij} = \sum_{k=D(j-1)+1}^{Dj} \tilde{X}_{ik}$

→ X_{ij} は試行数D の二項分布に従う

[4] Y. Takeishi and J. Takeuchi, “An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary,” *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.

Theorem 3 (New)

X は各要素独立に前ページの<u>二項分布</u>から生成する.

$R < C$とし，セクションサイズ率 a は $a \geq a_{v,L}$ を満たすものとする．このとき，$0 \leq \alpha_0 \leq 1$ に対して，

$\Pr\left[\mathcal{E}_{\alpha_0}\right] = e^{-nE(\alpha_0,R)}$ が成り立つ．ただし，

$E(\alpha_0,R) \geq h(\alpha_0, C-R) - \ln(2L)/n - \bar{\iota}(L)$

$h(\alpha,\Delta) = \min\left\{\alpha w_v \Delta, \frac{1}{4} g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\}$である.

$\bar{\iota}(L) = O(1/\sqrt{DL}) \to 0$

$C - R = \Delta_n = \Omega(1/(DL)^{1/4})$で
n に関して指数的に0に近づく

まとめ，今後の展望

- まとめ
  - SS符号はシンプルな符号化でガウス通信路で通信路容量を達成
  - 最尤復号においては，辞書を離散化しても同様に達成
  - 効率的復号においては，現在AMPが高い性能を発揮

- 今後の展望
  - AMPによる復号についても，辞書の離散化の評価
  - SS符号の実用化に向けた性能向上

参考文献(1/2)

[1] A. R. Barron and A. Joseph, “Least squares superposition coding of moderate dictionary size, reliable at rates up to channel capacity,” *Proc. Int. Symp. Inf. Theory*, Austin, Texas, June 13–18, 2010, pp. 275–279.
[2] A. R. Barron and A. Joseph, “Towards fast reliable communication at rates near capacity with Gaussian noise,” *Proc. IEEE. Int. Symp. Inf. Theory*, Austin, Texas, Jun. 13–18, 2010, pp. 315–319.
[3] Y. Takeishi, M. Kawakita, and J. Takeuchi, “Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity,” *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2737–2750, May 2014.
[4] Y. Takeishi and J. Takeuchi, “An Improved Analysis of Least Squares Superposition Codes with Bernoulli Dictionary,” *Japanese Journal of Statistics and Data Science*, 2, pp. 591–613, Sep. 2019.
[5] A. Joseph and A. R. Barron, “Fast sparse superposition codes have near exponential error probability for R < C. *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 919–942, Feb 2014.
[6] E. Arikan, “Channel polarization,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
[7] S.Kudekar, T. J. Richardson, and R. Urbanke, “Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp.803–834, Feb 2011.
[8] A. Joseph and A. R. Barron, “Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2541–2557, May 2012.
[9] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. SIAM*, vol. 8, pp. 300–304, Jun. 1960.

参考文献(2/2)

[10] Y. Polyanskiy, H. V. Poor, and S. Verdu, “ Channel coding rate in the finite block length regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.
[11] C. Rush, and R. Venkataramanan, “The Error Exponent of Sparse Regression Codes with AMP Decoding,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2478–2482, 2017
[12] 波多江優和, 三村和史, 川喜田雅則, 竹内純一, “スパース重ね合わせ符号のためのBayes 最適AMP 復号器,”電子情報通信学会技術研究報告, vol. 117, no. 487, IT2017-127, pp. 143-148, 2018 年3月.
[13] 押川祐也, 三村和史, 竹内純一, “スパース重ね合わせ符号のためのTrainable Bayes 最適AMP 復号器, ” 電子情報通信学会技術研究報告, vol. 118, no. 433, IT2018-44, pp. 55-60, 2019 年1月.
[14] 飯田昌澄, 押川祐也, 三村和史, 竹内純一, "深層学習によるスパース重ね合わせ符号の改良," 電子情報通信学会技術研究報告, vol. 119, no. 47, IT2019-13, pp. 67-72, 2019 年5月.