Approximate Support Recovery: Bounds

Лизюра Дмитрий[1]
Руководитель: Фролов Алексей Андреевич[2]

[1]Московский физико-технический институт

[2]Сколковский институт науки и технологий (Сколтех)

22 апреля 2025 года

Постановка задачи

Неформально

Имеется сервер и N пользователей, но в каждый момент времени не более $K_\alpha << N$ пользователей активно. Активные пользователи посылают серверу сообщения, однако они "склеиваются", а ещё к ним добавляется шум. Задача сервера — расшифровать исходные сообщения. Наша задача — минимизировать длину кодовых слов.

Постановка задачи

В частном случае

Пусть:

- M — количество кодовых слов, n — длина сообщения,
- ε — вероятность ошибки,
- $W_1, \dots, W_{K_\alpha} \sim U[M]$ — посылаемые пользователями сообщения,
- $c_1, \dots, c_M \in \mathbb{R}^n$ — кодовые слова,
- $Y = \sum_{j=1}^{K_\alpha} c_{W_j} + Z$, $Z \sim \mathcal{N}(0, I_n)$ — сообщение, полученное сервером,
- $g : \mathbb{R}^n \to \binom{[M]}{K_\alpha}$ — декодировщик,
- $E_j = \{W_j \notin g(Y))\} \cup \{W_j = W_i \text{ для } i \neq j\}$ — событие ошибки j–ого пользователя.

Схема кодирования называется (N, M, n, ε)*–кодом с произвольным доступом*, если выполнено

$$\frac{1}{K_\alpha} \sum_{j=1}^{K_\alpha} \mathbb{P}[E_j] \leq \varepsilon.$$

Альтернативная формулировка

Вместо $c_1, \ldots, c_M$ фиксируем матрицу

$$X = \begin{bmatrix} | & | & & | \\ c_1 & c_2 & \ldots & c_M \\ | & | & & | \end{bmatrix}$$

и сопоставляем сообщениям $W_1, \ldots, W_{K_\alpha}$ вектор $\beta \in \{0,1\}^M$, такой что

$$\beta_i = \begin{cases} 1, & i \in \{W_1, \ldots, W_{K_\alpha}\} \\ 0, & \text{иначе} \end{cases}.$$

Тогда $Y = X\beta$.

Дополнительное ограничение

Рассмотрим коды с ограниченной *энергией*: существует константа P, такая что все $\|c_j\|_2^2 \leq nP$.
Удельной энергией кода называется величина $\mathcal{E} = \frac{nP}{2\log_2 M}$.
Задача — получить оценку на $\inf\{\mathcal{E}\}$ по всем $(N, M, \varepsilon, \mathcal{E}, K_\alpha)$–кодам с произвольным доступом при фиксированных N, M, ε, K_α.

Первая оценка [1]

Theorem 1. *Fix $P' < P$. There exists an (M, n, ϵ) random-access code for K_a-user GMAC satisfying power-constraint P and*

$$\epsilon \le \sum_{t=1}^{K_a} \frac{t}{K_a} \min(p_t, q_t) + p_0 \,, \tag{3}$$

where

$$p_0 = \frac{\binom{K_a}{2}}{M} + K_a \mathbb{P}\left[\frac{1}{n}\sum_{j=1}^{n} Z_j^2 > \frac{P}{P'}\right] , \tag{4}$$

$$p_t = e^{-nE(t)}, \tag{5}$$

$$E(t) = \max_{0 \le \rho, \rho_1 \le 1} -\rho\rho_1 t R_1 - \rho_1 R_2 + E_0(\rho, \rho_1)$$

$$E_0 = \rho_1 a + \frac{1}{2}\log(1 - 2b\rho_1)$$

$$a = \frac{\rho}{2}\log(1 + 2P't\lambda) + \frac{1}{2}\log(1 + 2P't\mu) \tag{6}$$

$$b = \rho\lambda - \frac{\mu}{1 + 2P't\mu}, \quad \mu = \frac{\rho\lambda}{1 + 2P't\lambda} \tag{7}$$

$$\lambda = \frac{P't - 1 + \sqrt{D}}{4(1 + \rho_1\rho)P't}, \tag{8}$$

$$D = (P't - 1)^2 + 4P't\frac{1 + \rho\rho_1}{1 + \rho}$$

$$R_1 = \frac{1}{n}\log M - \frac{1}{nt}\log(t!) \tag{9}$$

$$R_2 = \frac{1}{n}\log\binom{K_a}{t} \tag{10}$$

$$q_t = \inf_{\gamma} \mathbb{P}[I_t \le \gamma] + \exp\{n(tR_1 + R_2) - \gamma\}$$

Идея доказательства:

- Взять $c_1, \ldots, c_M \sim \mathcal{N}(0, P' I_n)$.
- $g(Y) = \arg\min_{S \subset [M]} \left\| \sum_{j \in S} c_j - Y \right\|_2$.

Первая оценка [1]

Theorem 1. *Fix $P' < P$. There exists an (M, n, ϵ) random-access code for K_a-user GMAC satisfying power-constraint P and*

$$\epsilon \le \sum_{t=1}^{K_a} \frac{t}{K_a} \min(p_t, q_t) + p_0 \,, \tag{3}$$

where

$$p_0 = \frac{\binom{K_a}{2}}{M} + K_a \mathbb{P}\left[\frac{1}{n}\sum_{j=1}^{n} Z_j^2 > \frac{P}{P'}\right], \tag{4}$$

$$p_t = e^{-nE(t)}, \tag{5}$$

$$E(t) = \max_{0 \le \rho, \rho_1 \le 1} -\rho\rho_1 t R_1 - \rho_1 R_2 + E_0(\rho, \rho_1)$$

$$E_0 = \rho_1 a + \frac{1}{2}\log(1 - 2b\rho_1)$$

$$a = \frac{\rho}{2}\log(1 + 2P' t\lambda) + \frac{1}{2}\log(1 + 2P' t\mu) \tag{6}$$

$$b = \rho\lambda - \frac{\mu}{1 + 2P' t\mu}, \quad \mu = \frac{\rho\lambda}{1 + 2P' t\lambda} \tag{7}$$

$$\lambda = \frac{P' t - 1 + \sqrt{D}}{4(1 + \rho_1\rho)P' t}, \tag{8}$$

$$D = (P' t - 1)^2 + 4P' t \frac{1 + \rho\rho_1}{1 + \rho}$$

$$R_1 = \frac{1}{n}\log M - \frac{1}{nt}\log(t!) \tag{9}$$

$$R_2 = \frac{1}{n}\log\binom{K_a}{t} \tag{10}$$

$$q_t = \inf_{\gamma} \mathbb{P}[I_t \le \gamma] + \exp\{n(tR_1 + R_2) - \gamma\}$$

Идея доказательства:

- Взять $c_1, \ldots, c_M \sim \mathcal{N}(0, P' I_n)$.
- $g(Y) = \arg\min_{S \subset [M]} \left\| \sum_{j \in S} c_j - Y \right\|_2$.
- Или $g(Y) = \arg\min_{\beta \in \{0,1\}^M} \|X\beta - Y\|_2$.

Вторая оценка [2]

Зафиксируем $\mu = \frac{K_\alpha}{N}$ и определим

$$\mathcal{E}^*(M, \mu, \varepsilon) = \lim_{N\to\infty} \inf\{\mathcal{E} \mid \text{Существует } (N, M, \varepsilon, \mathcal{E}, \mu N) \text{ код}\}.$$

Тогда

Theorem 3 (Bound-MAC). *Fix M, μ and ϵ. Then*

$$\mathcal{E}^*(M, \mu, \epsilon) \le \inf \frac{b^2}{2\log_2 M},$$

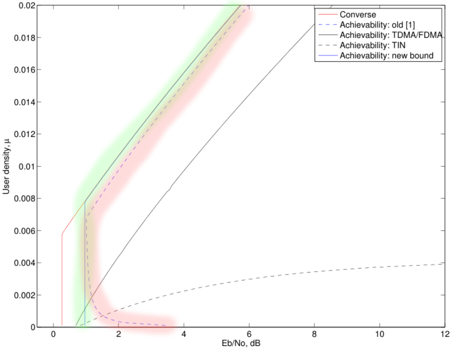
where infimum is over all $b > 0$ such that for all $\theta \in [\epsilon, 1]$ it holds that

$$\theta\mu \ln M + \mu h(\theta) < \max_{\lambda \ge 0}\{\frac{1}{2}\ln(1 + 2b^2\theta\mu\lambda) + \lambda\frac{\psi(b, \theta, \mu)^2}{1 + 2b^2\theta\mu\lambda} - \lambda\}, \quad (13)$$

where ψ is defined in (12).

Сравнение оценок

Оценки на $\mathcal{E}^*$ для разных μ при $M = 2^{100}$ и $\varepsilon = 10^{-3}$ [2].



Зелёным помечена оценка [2], красным — [1].

Задача — придумать неасимптотический аналог оценки [2].

Неравенство Гордона

В доказательстве [1] используется неравенство Чернова, а в [2] добавляется неравенство Гордона (теорема A из [3]):

Теорема

Пусть $\{X_{ij}\}$, $\{Y_{ij}\}$ *— два центрированных гауссовских процесса, удовлетворяющие следующим свойствам:*

- *Для всех* i, j, k *выполнено* $\mathbb{E}|X_{ij} - X_{ik}|^2 \leq \mathbb{E}|Y_{ij} - Y_{ik}|^2$.
- *Для* $i \neq l$ *выполнено* $\mathbb{E}|X_{ij} - X_{lk}|^2 \geq \mathbb{E}|Y_{ij} - Y_{lk}|^2$.

Тогда $\mathbb{E} \min_i \max_j X_{ij} \leq \mathbb{E} \min_i \max_j Y_{ij}$.

Неравенство Гордона

В доказательстве [1] используется неравенство Чернова, а в [2] добавляется неравенство Гордона (теорема A из [3]):

Теорема

Пусть $\{X_{ij}\}$, $\{Y_{ij}\}$ — два центрированных гауссовских процесса, удовлетворяющие следующим свойствам:

- *Для всех i, j, k выполнено $\mathbb{E}|X_{ij} - X_{ik}|^2 \leq \mathbb{E}|Y_{ij} - Y_{ik}|^2$.*
- *Для $i \neq l$ выполнено $\mathbb{E}|X_{ij} - X_{lk}|^2 \geq \mathbb{E}|Y_{ij} - Y_{lk}|^2$.*

Тогда $\mathbb{E} \min_i \max_j X_{ij} \leq \mathbb{E} \min_i \max_j Y_{ij}$.

В альтернативной формулировке все элементы X имеют распределение $\mathcal{N}(0, \sigma^2)$, поэтому $\{(X\beta)_i\}_{\beta \in \{0,1\}^M, i \in [n]}$ — это гауссовский процесс.

Промежуточные результаты

Оценка №1

Пусть $\chi_n(\tau)$ — нецентрированное хи–распределение с параметром τ порядка n и зафиксируем $b > 0$.

Теорема

Пусть $\varepsilon_1 \in (0, 1)$, *а* z — *это* $(1 - \varepsilon_1)$*–квантиль распределения* $\chi_n(\frac{\sqrt{n}}{b\sqrt{K_\alpha}})$. *Если* $\frac{n}{\sqrt{n+1}} - \frac{\sqrt{M}}{2\sqrt{K_\alpha}} - \frac{n}{b\sqrt{K_\alpha}} - z > 0$, *то существует схема кодирования с вероятностью ошибки не более*

$$\varepsilon_1 + \exp\left(-\frac{1}{2}\left(\frac{n}{\sqrt{n+1}} - \frac{\sqrt{M}}{2\sqrt{K_\alpha}} - \frac{n}{b\sqrt{K_a}} - z\right)^2\right)$$

и удельной энергией $\mathcal{E} = \frac{b^2}{2\log_2 M}$.

Промежуточные результаты

Оценка №2

Теорема

Пусть E — математическое ожидание величины распределения $\chi_n(\frac{\sqrt{n}}{b\sqrt{K_a}})$. Если

$$E - \sqrt{n} - \frac{\sqrt{M}}{2\sqrt{K_a}} - \frac{n}{b\sqrt{K_a}} > 0,$$

то существует схема кодирования с вероятностью ошибки не более

$$\exp\left(-\frac{1}{8}\left(E - \sqrt{n} - \frac{\sqrt{M}}{2\sqrt{K_a}} - \frac{n}{b\sqrt{K_a}}\right)^2\right)$$

и удельной энергией $\mathcal{E} = \frac{b^2}{2\log_2 M}$.

Различие оценок

Первая:

$$\frac{n}{\sqrt{n+1}} - \frac{\sqrt{M}}{2\sqrt{K_\alpha}} - \frac{n}{b\sqrt{K_\alpha}} - z > 0$$

— работает, если $\chi_n(\frac{\sqrt{n}}{b\sqrt{K_\alpha}})$ принимает маленькие значения.

Вторая:

$$E - \sqrt{n} - \frac{\sqrt{M}}{2\sqrt{K_\alpha}} - \frac{n}{b\sqrt{K_\alpha}} > 0$$

— работает, если $\chi_n(\frac{\sqrt{n}}{b\sqrt{K_\alpha}})$ принимает большие значения.

Промежуточные результаты

Оценка №3

Теорема

Положим $\tau = \frac{nb}{\sqrt{n+1}}\sqrt{2t} - b\sqrt{M} - 2n$ *и*

$$q_t = \begin{cases} \exp\left(-\frac{1}{2}\tau^2\right), & \tau > 0, \\ 1, & \textit{иначе} \end{cases}.$$

Тогда существует схема кодирования с вероятностью ошибки не более

$$\frac{1}{K_a}\sum_{t=1}^{K_a} q_t$$

и удельной энергией $\mathcal{E} = \frac{b^2}{2\log_2 M}$.

Ссылки

- Y. Polyanskiy, "A perspective on massive random-access," *IEEE Information Theory (ISIT), 2017.*
- I. Zadik, Y. Polyanskiy, and C. Thrampoulidis, "Improved bounds on Gaussian MAC and sparse regression via Gaussian inequalities," *IEEE International Symposium on Information Theory (ISIT), 2019.*
- Gordon, Y. (1988). On Milman's inequality and random subspaces which escape through a mesh in $\mathbb{R}^n$. In: Lindenstrauss, J., Milman, V.D. (eds) Geometric Aspects of Functional Analysis. Lecture Notes in Mathematics, vol 1317. Springer, Berlin, Heidelberg.