Gaussian Multiple and Random Access in the Finite Blocklength Regime

Recep Can Yavas

California Institute of Technology

June 21-26, 2020

Joint work with Victoria Kostina and Michelle Effros

ISIT 2020

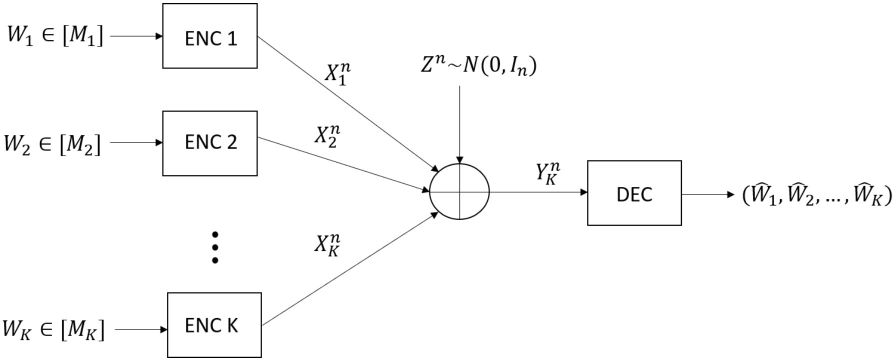
This work was supported in part by the National Science Foundation (NSF) under grant CCF-1817241.

Talk Plan

We present two achievability results for

1. Gaussian Multiple Access Channel (MAC)
2. Gaussian Random Access Channel (RAC)

Gaussian Multiple Access Channel (MAC)



- Maximal power constraint on the codewords: $\|X_k^n\|^2 \leq nP_k$ for $k = 1, \dots, K$
- Notation: $[M] = \{1, \dots, M\}, x_{\mathcal{A}} = (x_a \colon a \in \mathcal{A})$

MAC Code Definition

Definition (K-transmitter MAC)

An $(n, M_1, \ldots, M_K, \epsilon, P_1, \ldots, P_K)$ code for the K-transmitter MAC consists of

- K encoding functions $\mathrm{f}_k : [M_k] \to \mathbb{R}^n, \quad k \in [K]$
- a decoding function $\mathrm{g} : \mathbb{R}^n \to [M_1] \times \cdots \times [M_K]$

with maximal power constraint

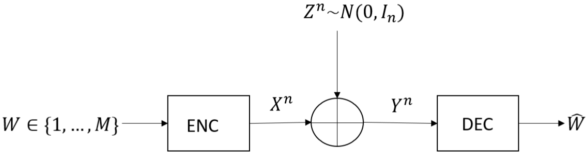
$$\|\mathrm{f}_k(m_k)\|^2 \leq nP_k \text{ for } m_k \in [M_k], k \in [K]$$

and

$$\frac{1}{\prod_{k=1}^{K} M_k} \sum_{m_{[K]} \in [M_1] \times \cdots \times [M_K]} \mathbb{P}\left[\mathrm{g}(Y_K^n) \neq m_{[K]} \mid X_k^n = \mathrm{f}_k(m_k) \, \forall k \in [K]\right] \leq \epsilon$$

average probability of error

- Channel:



- $M^*(n, \epsilon, P) \triangleq \{\max M : \text{ an } (n, M, \epsilon, P) \text{ code exists.}\}$.

$$\log M^*(n, \epsilon, P) = nC(P) - \sqrt{nV(P)}\,Q^{-1}(\epsilon) + \frac{1}{2}\log n + O(1)$$

$C(P) = \frac{1}{2}\log(1+P)$ (capacity) $\quad V(P) = \frac{P(P+2)}{2(1+P)^2}$ (dispersion) $\quad$ third-order term

Achievability ($\geq$): [Tan-Tomamichel 15']
Converse ($\leq$): [Polyanskiy et al. 10']

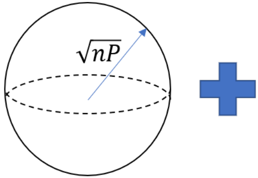
The Lesson from P2P Channel

We can achieve

$$\log M^*(n, \epsilon, P) = nC(P) - \sqrt{nV(P)}Q^{-1}(\epsilon) + \frac{1}{2}\log n + O(1)$$

by using

Uniformly distributed codewords over:



Maximum Likelihood (ML) Decoder

n dim power sphere

(Spherical codebook)

- We are interested in refining the achievable third-order term for the Gaussian MAC in the finite blocklength regime.
- For the point-to-point case, it is known that the third-order term $+1/2 \log n$ is optimal. We want to show that $+1/2 \log n\mathbf{1}$ is achievable for the Gaussian MAC.

Gaussian MAC - Main Result

Theorem

For any $\epsilon \in (0,1)$ and any $P_1, P_2 > 0$, an $(n, M_1, M_2, \epsilon, P_1, P_2)$ code for the two-transmitter Gaussian MAC exists provided that

$$\begin{bmatrix} \log M_1 \\ \log M_2 \\ \log M_1 M_2 \end{bmatrix} \in n\mathbf{C}(P_1, P_2) - \sqrt{n} Q_{\mathrm{inv}}(\mathsf{V}(P_1, P_2), \epsilon) + \frac{1}{2} \log n\mathbf{1} + O(1)\mathbf{1}.$$

- $\mathbf{C}(P_1, P_2) = \begin{bmatrix} C(P_1) \\ C(P_2) \\ C(P_1 + P_2) \end{bmatrix} =$ capacity vector

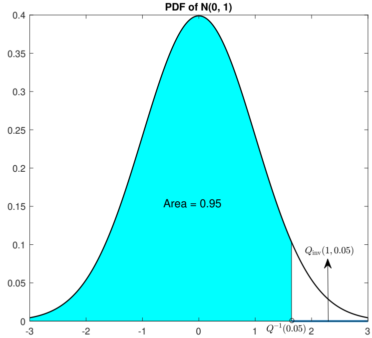
  $\mathsf{V}(P_1, P_2) = 3 \times 3$ positive-definite dispersion matrix
- $Q_{\mathrm{inv}}(\mathsf{V}, \epsilon) =$ multidimensional counterpart of inverse Q-function

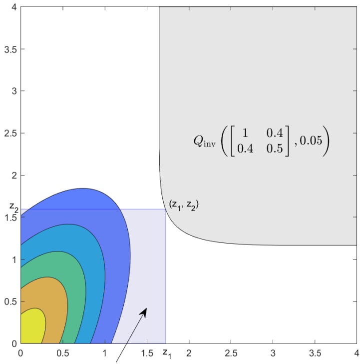
$$Q_{\mathrm{inv}}(\mathsf{V}, \epsilon) \triangleq \left\{ \mathbf{z} \in \mathbb{R}^d : \mathbb{P}[\mathbf{Z} \leq \mathbf{z}] \geq 1 - \epsilon \right\}$$

where $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$ component-wise

What does $Q_{\mathrm{inv}}(\mathsf{V}, \epsilon)$ look like?

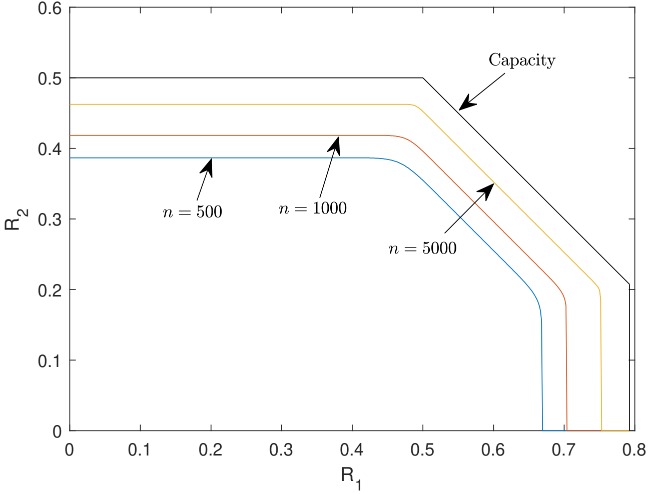
$$Q_{\mathrm{inv}}(1, \epsilon) \triangleq \{x \colon x \geq Q^{-1}(\epsilon)\} \qquad Q_{\mathrm{inv}}(\mathsf{V}, \epsilon) \triangleq \left\{\mathbf{z} \in \mathbb{R}^d : \mathbb{P}[\mathbf{Z} \leq \mathbf{z}] \geq 1 - \epsilon\right\}$$





$$\mathbb{P}\left[\mathcal{N}(0, \mathsf{V}) \leq (z_1, z_2)\right] = 0.95$$

Achievable region for $P_1 = 2, P_2 = 1$ and $\epsilon = 10^{-3}$:



Comparison with the literature

- Our third-order term improves!

$$n\mathbf{C}(P_1, P_2) - \sqrt{n}Q_{\mathrm{inv}}(\mathsf{V}(P_1, P_2), \epsilon) + \frac{1}{2}\log n\mathbf{1} + O(1)\mathbf{1}$$

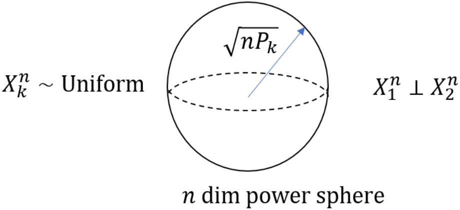
$> O\left(n^{1/4}\right)\mathbf{1}$ [MolavianJazi-Laneman 15']

$> O\left(n^{1/4}\log n\right)\mathbf{1}$ [Scarlett et al. 15']

- Proof techniques:
  - **Our bound**: Spherical codebook + Maximum-likelihood decoder
  - [MolavianJazi-Laneman 15'] : Spherical codebook + threshold decoder
  - [Scarlett et al. 15'] : Constant composition codes + Quantization

Encoding and decoding

- **Encoding**: independently generate M_k codewords for $k = 1, 2$:



(Spherical codebook)

  [Shannon 49'] used spherical codebook to bound error exponent of the P2P Gaussian channel.

- **Decoding**: Mutual information density

$$\imath_{1,2}(x_1^n, x_2^n; y^n) \triangleq \log \frac{P_{Y_2^n|X_1^n,X_2^n}(y^n|x_1^n, x_2^n)}{P_{Y_2^n}(y^n)}$$

  Maximum likelihood (ML) Decoder:

$$\mathsf{g}(y^n) = \arg\max_{m_1,m_2} \imath_{1,2}(\mathsf{f}_1(m_1), \mathsf{f}_2(m_2); y^n)$$

Main Tool: Random-Coding Union (RCU) Bound

P2P case: proved in [Polyanskiy et al. 10']

Using the ML decoder, for a general MAC:

Theorem (New RCU bound for MAC)

For arbitrary input distributions P_{X_1} and P_{X_2}, there exists a (M_1, M_2, ϵ)-MAC code such that

$$\epsilon \leq \mathbb{E}\Big[\min\Big\{1, (M_1-1)\mathbb{P}\left[\imath_1(\bar{X}_1; Y_2|X_2) \geq \imath_1(X_1; Y_2|X_2) \mid X_1, X_2, Y_2\right]$$
$$+ (M_2-1)\mathbb{P}\left[\imath_2(\bar{X}_2; Y_2|X_1) \geq \imath_2(X_2; Y_2|X_1) \mid X_1, X_2, Y_2\right]$$
$$+ (M_1-1)(M_2-1)\mathbb{P}\left[\imath_{1,2}(\bar{X}_1, \bar{X}_2; Y_2) \geq \imath_{1,2}(X_1, X_2; Y_2) \mid X_1, X_2, Y_2\right]\Big\}\Big],$$

where $P_{X_1,\bar{X}_1,X_2,\bar{X}_2,Y_2}(x_1, \bar{x}_1, x_2, \bar{x}_2, y) = P_{X_1}(x_1)P_{X_1}(\bar{x}_1)P_{X_2}(x_2)P_{X_2}(\bar{x}_2)P_{Y_2|X_1X_2}(y|x_1, x_2)$.

- Crucial in refining the third-order term to $\frac{1}{2}\log n$

Key Challenge

Modified mutual information density r.v.:

$$\tilde{\boldsymbol{\imath}}_2 \triangleq \begin{bmatrix} \tilde{\imath}_1(X_1^n; Y_2^n | X_2^n) \\ \tilde{\imath}_2(X_2^n; Y_2^n | X_1^n) \\ \tilde{\imath}_{1,2}(X_1^n, X_2^n; Y_2^n) \end{bmatrix} - n\mathbf{C}(P_1, P_2)$$

$$\tilde{\imath}_{1,2}(x_1^n, x_2^n; y^n) \triangleq \log \frac{P_{Y_2^n | X_1^n, X_2^n}(y^n | x_1^n, x_2^n)}{Q_{Y_2^n}(y^n)} \text{ with } Q_{Y_2^n} \sim \mathcal{N}(\mathbf{0}, (1 + P_1 + P_2)\mathrm{I}_n)$$

Lemma (New Berry-Esséen type bound)

Let $\mathcal{D} \in \mathbb{R}^3$ be a convex, Borel measurable set and $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathrm{V}(\mathrm{P}_1, \mathrm{P}_2))$. Then

$$\left| \mathbb{P}\left[\frac{1}{\sqrt{n}} \tilde{\boldsymbol{\imath}}_2 \in \mathcal{D} \right] - \mathbb{P}\left[\mathbf{Z} \in \mathcal{D} \right] \right| \leq \frac{C_0}{\sqrt{n}}$$

- [MolavianJazi-Laneman 15', Prop. 1] showed a weaker upper bound with $O\left(\frac{1}{n^{1/4}}\right)$ using CLT for functions $\Longrightarrow$ affects the third-order term
- We use a different technique to prove this lemma.

Proof of Lemma

- Problem: We cannot use Berry-Esséen theorem directly since X_1^n and X_2^n are not i.i.d.
- Solution:
  - Conditional dist. $\tilde{\imath}_2 | \langle X_1^n, X_2^n \rangle = q$ is a sum of independent r.v.s
  - Apply the multidimensional Berry-Esséen theorem to that sum of independent vectors after conditioning on the inner product $\langle X_1^n, X_2^n \rangle$.
  - Then integrate the probabilities over q.

Extension to K-transmitter ($P_k = P,\ M_k = M\ \forall\, k \in [K]$)

Theorem

For any $\epsilon \in (0,1)$, and $P > 0$, an $(n, M\mathbf{1}, \epsilon, P\mathbf{1})$-MAC code for the K-transmitter Gaussian MAC exists provided that

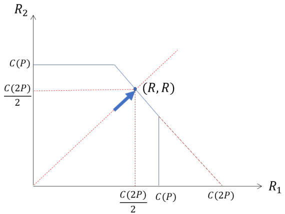
$$K \log M \leq nC(KP) - \sqrt{n(V(KP) + V_{\mathrm{cr}}(K,P))}\,Q^{-1}(\epsilon) + \frac{1}{2}\log n + O(1).$$

$V_{\mathrm{cr}}(K,P)$ is the cross dispersion term

$$V_{\mathrm{cr}}(K,P) = \frac{K(K-1)P^2}{2(1+KP)^2}.$$

Message set size vector:

$$\begin{bmatrix} \log M_1 \\ \log M_2 \\ \vdots \\ \log(M_1 M_2 \cdots M_K) \end{bmatrix} \in \mathbb{R}^{2^K - 1}$$



Talk Plan

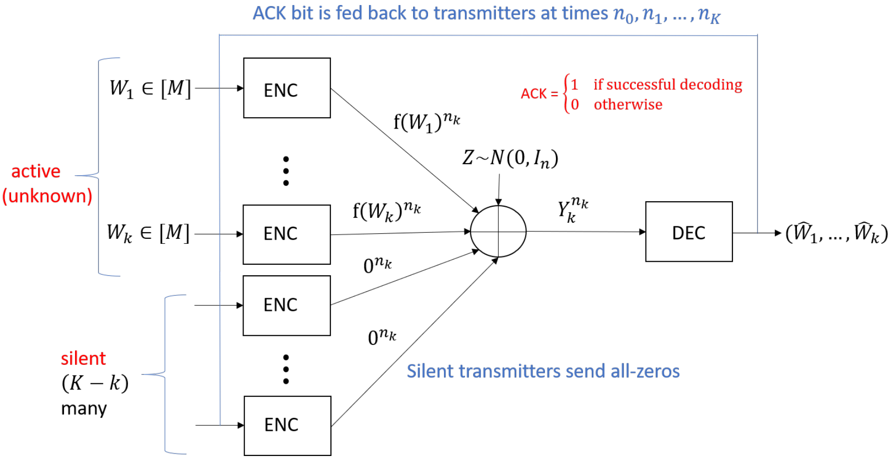
We present two achievability results for

1. Gaussian Multiple Access Channel (MAC)
2. Gaussian Random Access Channel (RAC)

Random access

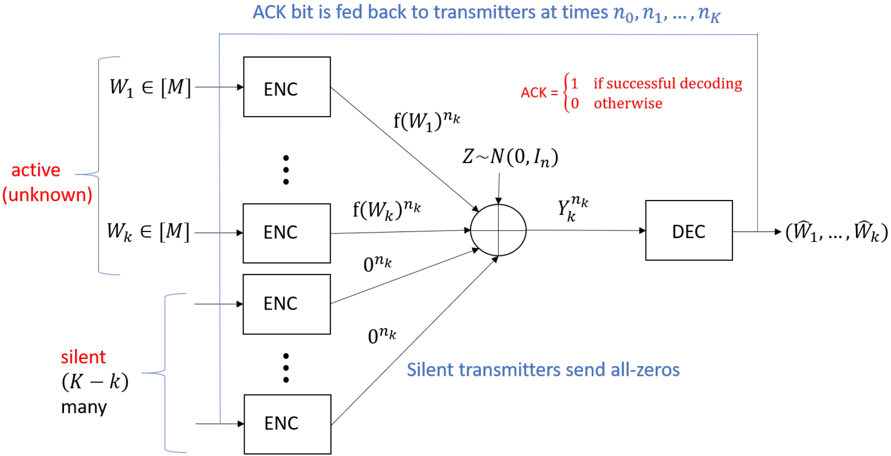
- Random access solutions such as ALOHA, treating interference as noise, or orthogonalization methods (TDMA/FDMA) perform poorly.
- We want to design a random access communication strategy that
  - does not require the knowledge of transmitter activity
  - and still does not cause a performance loss compared to k-MAC.

Rateless Gaussian RAC Communication



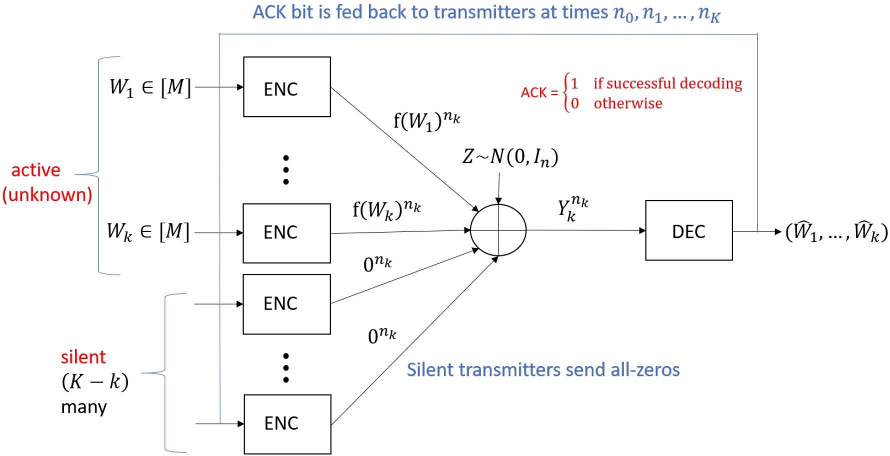
- There are K transmitters in total. A subset of those with size k are active.
- Nobody knows the active transmitters.
- No probability of being active is assigned to transmitters.

Rateless Gaussian RAC Communication



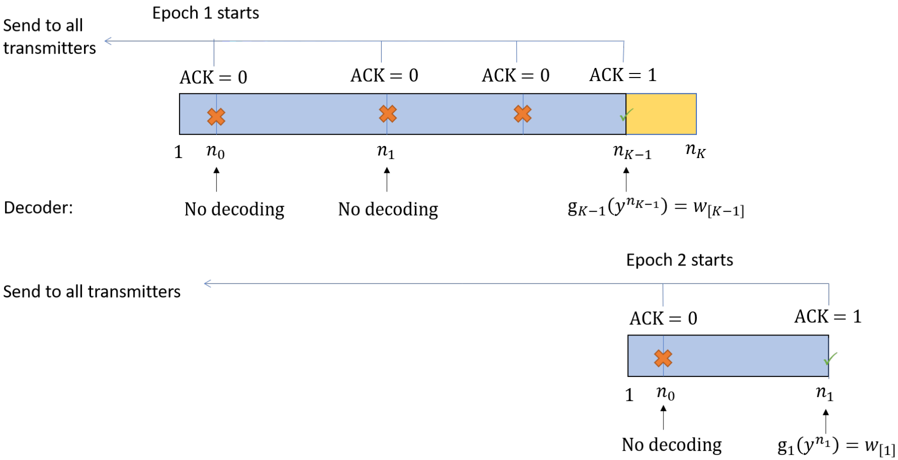
- Identical encoding and list decoding as in [Polyanskiy 17']
- Average probability of error $\leq \epsilon_k$ for $k = 0, \ldots, K$
- New: Gaussian RAC, maximal power constraint: $\|\mathrm{f}(m)^{n_k}\|^2 \leq n_k P$ for all k and m

Rateless Gaussian RAC Communication



- Rateless coding scheme that we defined in the context of DMCs [Effros, Kostina, Yavas, "Random access channel coding in the finite blocklength regime", 18']
- Predetermined decoding times: $n_0, \ldots, n_K$

Communication Process



RAC Code Definition

Definition

An $(\{n_k, \epsilon_k\}_{k=0}^{K}, M, P)$-RAC consists of

- an encoder function f
- decoding functions $\{\mathsf{g}_k\}_{k=0}^{K}$

such that

- Maximal power constraints are satisfied:

$$\|\mathsf{f}(m)^{n_k}\|^2 \leq n_k P \text{ for } m \in \{1, \dots, M\}, k \in \{1, \dots, K\}$$

- and

$$\frac{1}{M^k} \sum_{m_{[k]} \in [M]^k} \mathbb{P}\left[\left\{ \bigcup_{t<k} \{\mathsf{g}_t(Y_k^{n_t}) \neq \mathsf{e}\} \right\} \bigcup \left\{ \mathsf{g}_k(Y_k^{n_k}) \overset{\pi}{\neq} m_{[k]} \right\} \middle| X_{[k]}^{n_k} = \mathsf{f}(m_{[k]})^{n_k} \right] \leq \epsilon_k$$

the average probability of error in decoding k messages at time n_k

Gaussian RAC - Main Result

Theorem

For any $K < \infty$, $\epsilon_k \in (0,1)$ and any $P > 0$, an $(M, \{(n_k, \epsilon_k)\}_{k=0}^{K}, P)$-code for the Gaussian RAC exists provided that

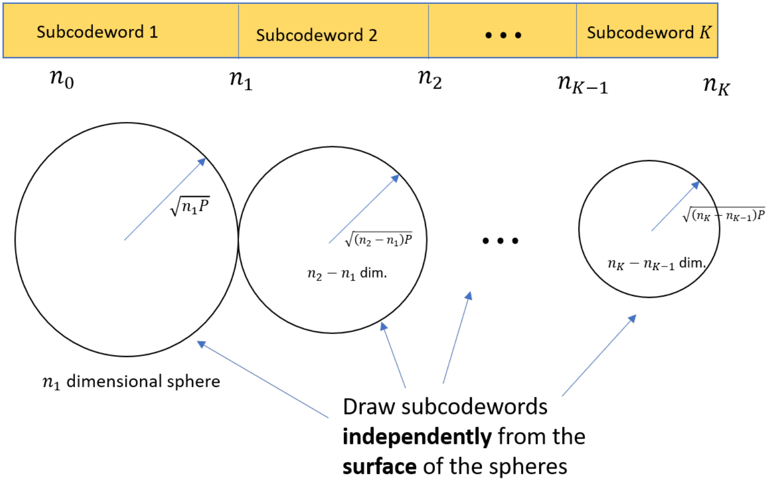
$$k \log M \leq n_k C(kP) - \sqrt{n_k (V(kP) + V_{\text{cr}}(k,P))} Q^{-1}(\epsilon_k) + \frac{1}{2} \log n_k + O(1)$$

for all $k \in [K]$, for some positive constant C.

- The same first, second, and third-order terms as in Gaussian MAC with known number of transmitters!

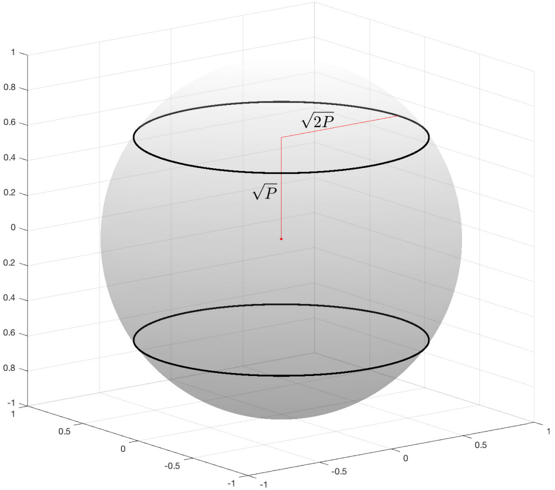
Gaussian RAC - Encoding

- To satisfy the maximal power constraints for all decoding times simultaneously, we set the input distribution as:



Feasible codeword set for Gaussian RAC

- $n_1 = 2, n_2 = 3, P = \frac{1}{3}$:[1]



[1] If we use this input dist. for the Gaussian MAC, we achieve the same first three order terms.

Gaussian RAC - Decoding

- Mutual information density for t transmitters:

$$\imath_{[t]}(x_{[t]}^{n_t}; y^{n_t}) \triangleq \log \frac{P_{Y_t^{n_t}|X_{[t]}^{n_t}}(y^{n_t}|x_{[t]}^{n_t})}{P_{Y_t^{n_t}}(y^{n_t})}$$

- Decoder output at time n_t is

$$\mathrm{g}_t(y^{n_t}) = \begin{cases} \arg\max\limits_{m_{[t]}} \imath_{[t]}(\mathrm{f}(m_{[t]})^{n_t}; y^{n_t}) & \text{if } \left| \frac{1}{n_t} \|y^{n_t}\|^2 - (1 + tP) \right| \leq \lambda_t \\ \mathrm{e} & \text{otherwise} \end{cases}$$

If e, send ACK $= 0$ to request the next subcodeword of length $n_{t+1} - n_t$

Summary of the main theorems

- Gaussian MAC:
  - We refine the achievable third-order term to $1/2 \log n\mathbf{1}$ by using spherical codebook and ML decoder.
  - We derive a Berry-Esséen type bound for the spherical codebook.
- Gaussian RAC:
  - Our proposed rateless code **performs as well in the first-, second-, and third-order terms as the best known communication scheme** when the set of active transmitters is known.

References

1. E. MolavianJazi and J. N. Laneman, "A second-order achievable rate region for Gaussian multi-access channels via a central limit theorem for functions, "IEEE Transactions on Information Theory, vol. 61, no. 12, pp. 6719–6733, Dec. 2015.
2. A. M. Scarlett, and A. G. i Fabregas, "Second-order rate region of constant-composition codes for the multiple-access channel, "IEEE Transactions on Information Theory, vol. 61, no. 1, pp. 157–172, Jan. 2015.
3. Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," IEEE Transactions on Information Theory, vol. 56, no. 5, pp. 2307–2359, May 2010.
4. V. Y. F. Tan and M. Tomamichel, "The third-order term in the normal approximation for the AWGN channel," IEEE Transactions on Information Theory, vol. 61, no. 5, pp. 2430–2438, May 2015.
5. M. Effros, V. Kostina, and R. C. Yavas, "Random access channel coding in the finite blocklength regime," in 2018 IEEE International Symposium on Information Theory (ISIT), June 2018, pp. 1261–1265.
6. Y. Polyanskiy, "A perspective on massive random-access," in Proceedings 2017 IEEE International Symposium on Information Theory, Aachen, Germany, June 2017, pp. 2523–2527.

Thanks

- R. C. Yavas, V. Kostina, and M. Effros, "Gaussian multiple and random access in the finite blocklength regime," ArXiv/2001.03867, 2020. Available at: `https://arxiv.org/abs/2001.03867`