Remarks on massive random access

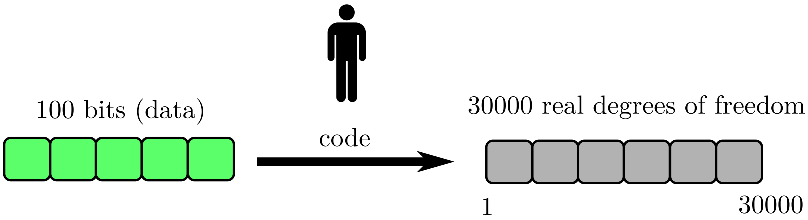
Yury Polyanskiy

Department of EECS
MIT

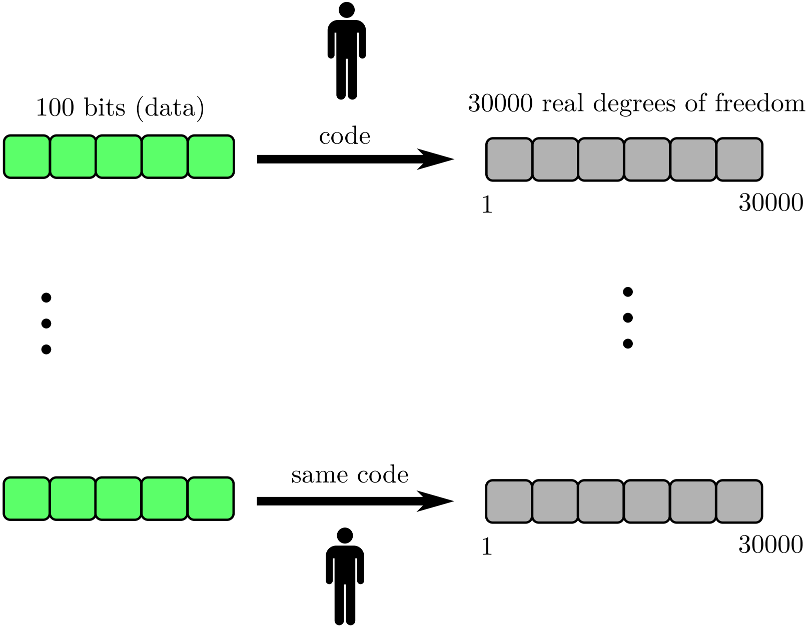
yp@mit.edu

DLR-MIT-TUM Workshop, Munich, Feb. 2020

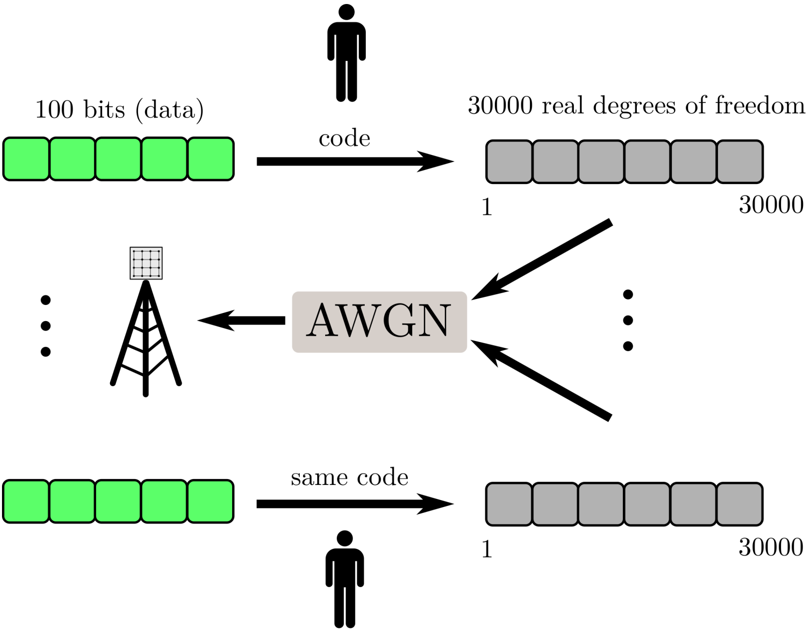
Preview: what this talk is about?



Preview: what this talk is about?



Preview: what this talk is about?



Who cares about this model?

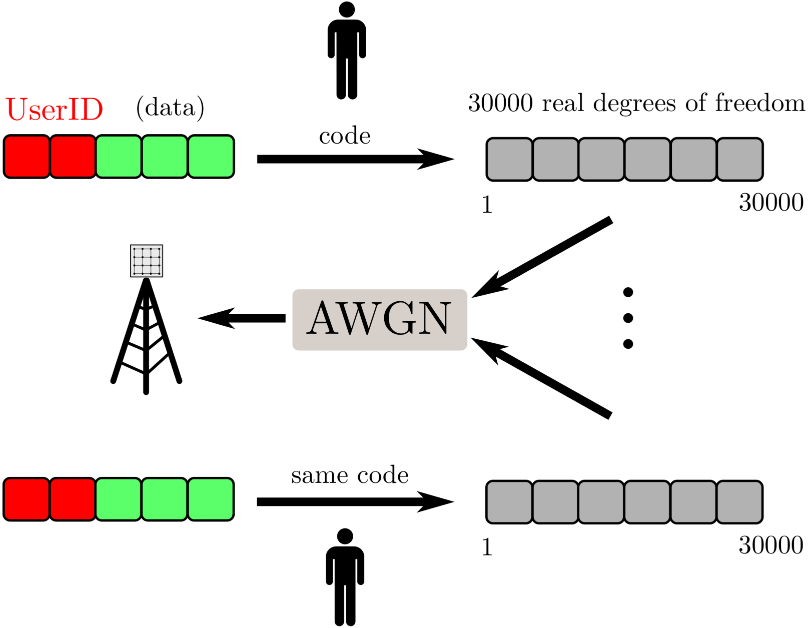
LoRa

sigfox

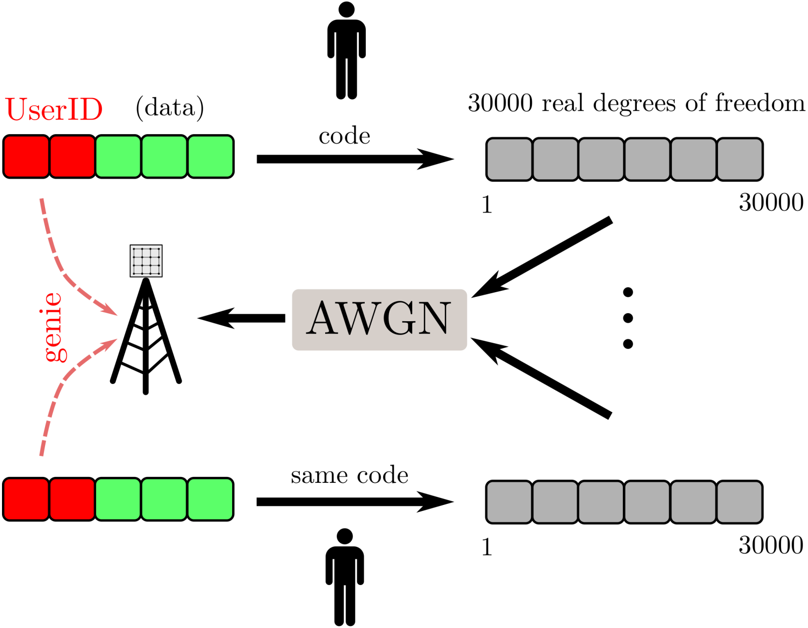
amazon sidewalk

ICARUS
Global Monitoring with Animals

Random-Access vs MAC



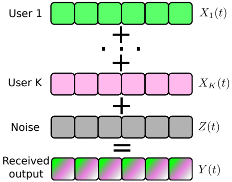
Random-Access vs MAC



Plan

- Question 1: Is there a useful asymptotics to study?
- Question 2: What sparsification is more useful? (IDMA vs. Slotted ALOHA)
- Question 3: Limitations of linear codes.

Key definition: random-access (same codebook) code



Definition (P.'17)

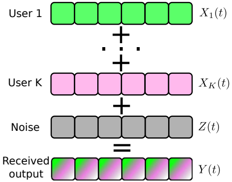
$f : [M] \to \mathbb{R}^n$ is a (n, M, K_a, ϵ) random-access code if $\exists$ list-K_a decoder g s.t.

$$\mathbb{P}[W_j \notin g(f(W_1) + \cdots + f(W_{K_a}) + Z)] \le \epsilon \qquad \forall j \in [K_a]$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$. Fundamental limit ($E_b/N_0$):

$$E_b^*(n, M, K_a, \epsilon) = \frac{1}{2\log_2 M} \min_f \sup_{j \in [M]} \|f(j)\|_2^2$$

Key definition: random-access (same codebook) code



Definition (P.'17)

$f : [M] \to \mathbb{R}^n$ is a (n, M, K_a, ϵ) random-access code if $\exists$ list-K_a decoder g s.t.

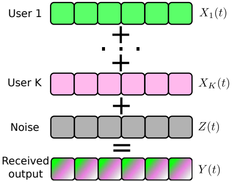
$$\mathbb{P}[W_j \notin g(f(W_1) + \cdots + f(W_{K_a}) + Z)] \le \epsilon \qquad \forall j \in [K_a]$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$. Fundamental limit ($E_b/N_0$):

$$E_b^*(n, M, K_a, \epsilon) = \frac{1}{2\log_2 M} \min_f \sup_{j \in [M]} \|f(j)\|_2^2$$

How to do asymptotics?

Key definition: random-access (same codebook) code



Definition (P.'17)

$f : [M] \to \mathbb{R}^n$ is a (n, M, K_a, ϵ) random-access code if $\exists$ list-K_a decoder g s.t.

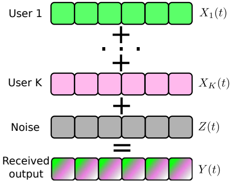
$$\mathbb{P}[W_j \notin g(f(W_1) + \cdots + f(W_{K_a}) + Z)] \le \epsilon \qquad \forall j \in [K_a]$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$. Fundamental limit (E_b/N_0):

$$E_b^*(n, M, K_a, \epsilon) = \frac{1}{2 \log_2 M} \min_f \sup_{j \in [M]} \|f(j)\|_2^2$$

How to do asymptotics? Fixed K_a and $n \to \infty$ is useless.

Key definition: random-access (same codebook) code



Definition (P.'17)

$f : [M] \to \mathbb{R}^n$ is a (n, M, K_a, ϵ) random-access code if $\exists$ list-K_a decoder g s.t.

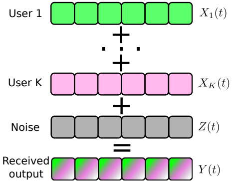
$$\mathbb{P}[W_j \notin g(f(W_1) + \cdots + f(W_{K_a}) + Z)] \le \epsilon \qquad \forall j \in [K_a]$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$. Fundamental limit ($E_b/N_0$):

$$E_b^*(n, M, K_a, \epsilon) = \frac{1}{2\log_2 M} \min_f \sup_{j \in [M]} \|f(j)\|_2^2$$

How to do asymptotics? $K_a = \mu n$ is impossible: $K_a \gg M$

Key definition: random-access (same codebook) code



Definition (P.'17)

$f : [M] \to \mathbb{R}^n$ is a (n, M, K_a, ϵ) random-access code if $\exists$ list-K_a decoder g s.t.

$$\mathbb{P}[W_j \notin g(f(W_1) + \cdots + f(W_{K_a}) + Z)] \le \epsilon \qquad \forall j \in [K_a]$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$. Fundamental limit ($E_b/N_0$):

$$E_b^*(n, M, K_a, \epsilon) = \frac{1}{2\log_2 M} \min_f \sup_{j \in [M]} \|f(j)\|_2^2$$

How to do asymptotics? Solution: $K_a = \mu n$ and $M = 2^k K_a$

Same-codebook codes = compressed sensing

- random-access = all users share same codebook
- ... obviously decoding is upto permutation of users
- Equivalent to compressed-sensing [Jin-Kim-Rao'11]

Same-codebook codes = compressed sensing

- random-access = all users share same codebook
- ... obviously decoding is upto permutation of users
- Equivalent to compressed-sensing [Jin-Kim-Rao'11]
- Let same-codebook (column) vectors be $c_1, \ldots c_j$.

$$X = \left(c_1 \quad \middle| \quad \cdots \quad \middle| \quad c_M\right)$$

- Let $\beta \in \{0,1\}^M$ with $\beta_j = 1$ if codeword j was transmitted
- Then the problem is:

$$Y = X\beta + Z, \qquad \text{Goal: } \mathbb{E}[\|\beta - \hat{\beta}(Y)\|] \to \min$$

(linear regression with sparsity $\|\beta\|_0 = K_a$ aka comp.sensing).
- PUPE requirement translates to false-discovery rate (FDR) requirement: $\|\hat{\beta}\|_0 \le K_a$.

Same-codebook codes = compressed sensing

- random-access = all users share same codebook
- ... obviously decoding is upto permutation of users
- Equivalent to compressed-sensing [Jin-Kim-Rao'11]
- Let same-codebook (column) vectors be $c_1, \ldots c_j$.

$$X = \left(c_1 \quad | \quad \cdots \quad | \quad c_M\right)$$

- Let $\beta \in \{0,1\}^M$ with $\beta_j = 1$ if codeword j was transmitted
- Then the problem is:

$$Y = X\beta + Z, \qquad \text{Goal: } \mathbb{E}[\|\beta - \hat{\beta}(Y)\|] \to \min$$

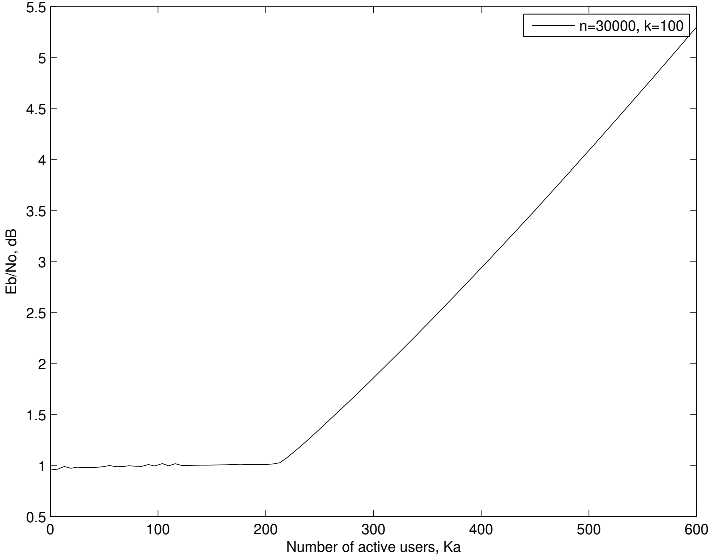
(linear regression with sparsity $\|\beta\|_0 = K_a$ aka comp.sensing).
- PUPE requirement translates to false-discovery rate (FDR) requirement: $\|\hat{\beta}\|_0 \le K_a$.
- Regime of $K_a = \mu n$, $M = 2^k K_a$ and $n \to \infty$: CS with fixed-aspect ratio sensing matrix.

- In [P.'ISIT-2017] a random-coding achievability bound was shown:

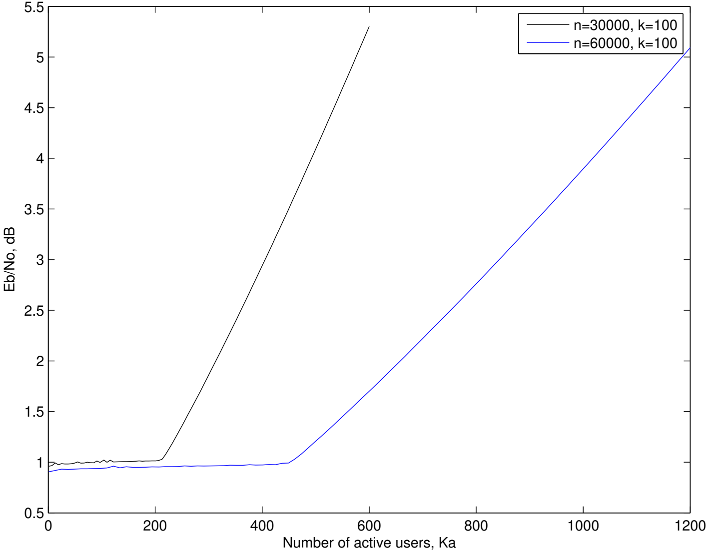
$$E_b^*(n, M, K_a, \epsilon) \leq E_{rc}(n, M, K_a, \epsilon)$$

- The bound is messy, but let us study it numerically.
  - Frame length $n = 30000, 60000, 120000$ (real d.o.f.)
  - User payload: $k = 100$ bits
  - Active users: $K_a = 1 \ldots 1500$ (variable)
  - Target error PUPE = 10^{-3}

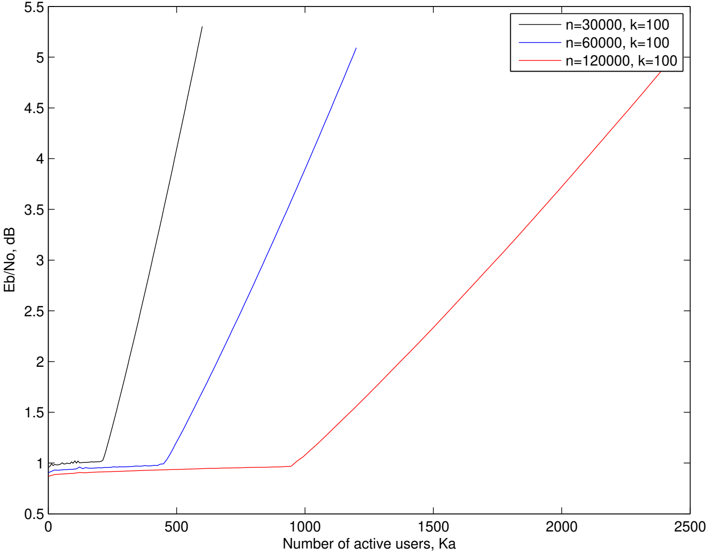
Comparing random coding bound at different n



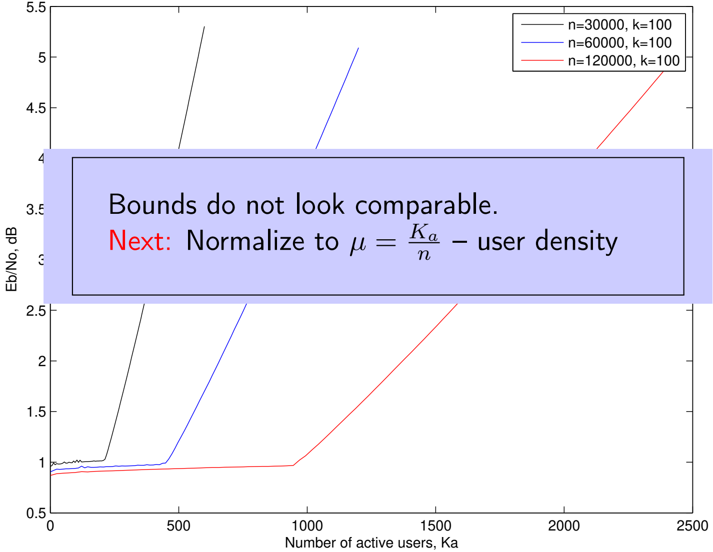
Comparing random coding bound at different n



Comparing random coding bound at different n

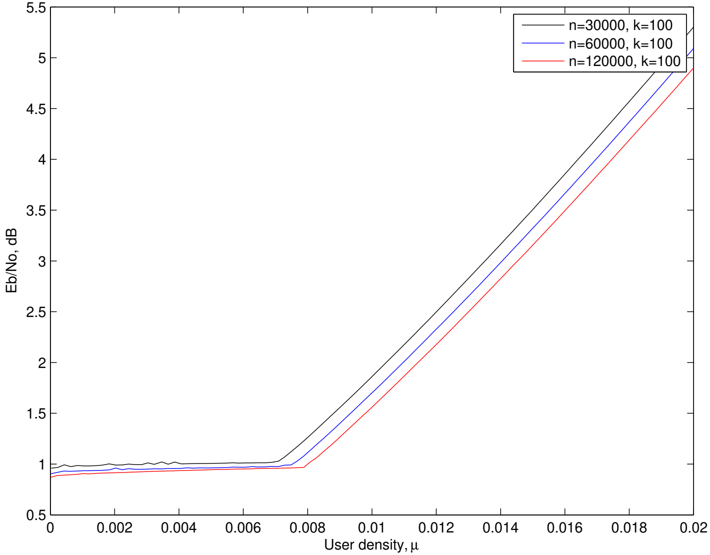


Comparing random coding bound at different n

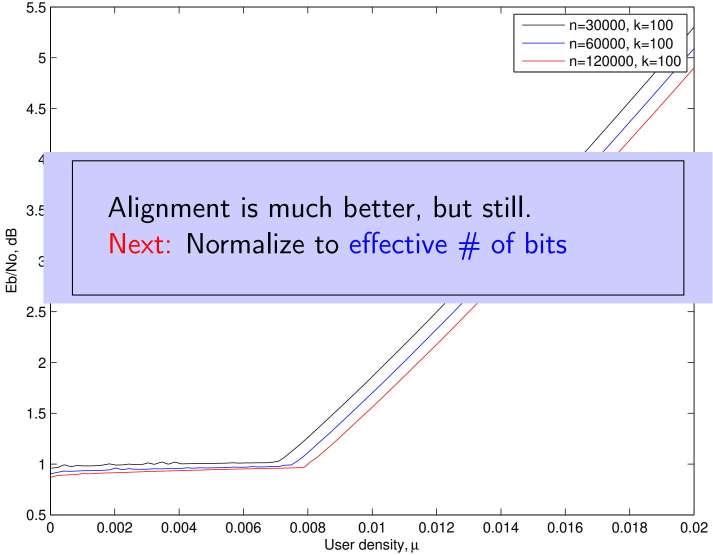


Bounds do not look comparable.
Next: Normalize to $\mu = \frac{K_a}{n}$ – user density

Comparing random coding bound at different n (user density)



Comparing random coding bound at different n (user density)



Alignment is much better, but still.
Next: Normalize to effective # of bits

Effective number of bits

- Problem: Consider two values of blocklength $n_1 < n_2$.
- ... with the same k and μ we have $K_{a,1} = \mu n_1 < K_{a,2} = \mu n_2$.
- ... So comparison of E_b/N_0 is not quite fair.

Effective number of bits

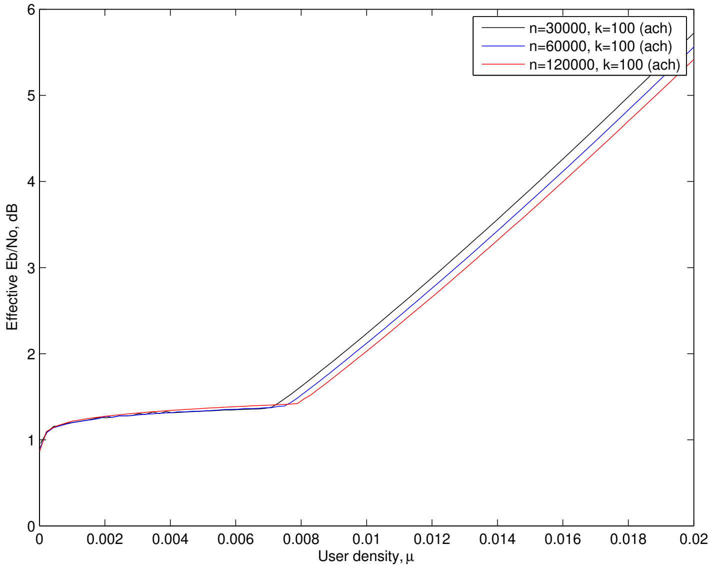
- Problem: Consider two values of blocklength $n_1 < n_2$.
- ... with the same k and μ we have $K_{a,1} = \mu n_1 < K_{a,2} = \mu n_2$.
- ... So comparison of E_b/N_0 is not quite fair.
- Let us introduce effective number of bits as

$$k_{eff} = \log_2 \frac{M}{K_a}$$

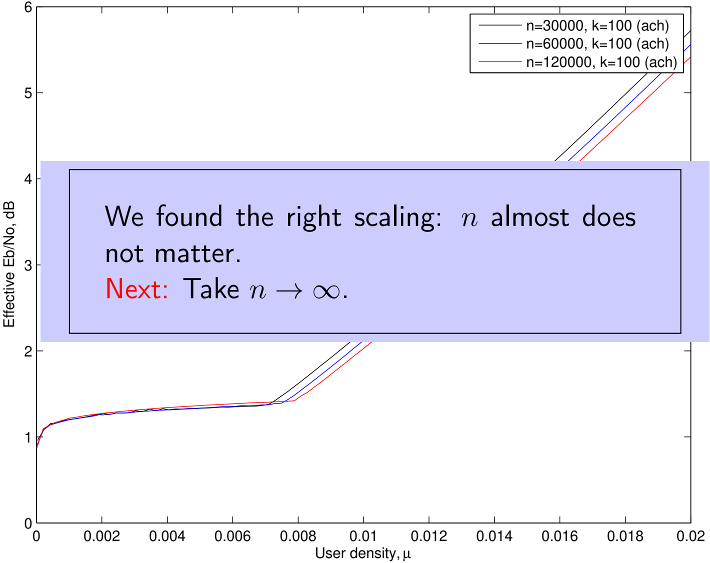
- ... and then effective E_b/N_0 becomes

$$\left(\frac{E_b}{N_0}\right)_{eff} = \frac{1}{2k_{eff}} \sup_{j\in[M]} \|f(j)\|_2^2$$

Comparing bounds at different n (effective E_b/N_0)



Comparing bounds at different n (effective E_b/N_0)



We found the right scaling: n almost does not matter.
Next: Take $n \to \infty$.

Asymptotics of random-access

- We say that $\mathcal{E}$ is asymptotically achievable effective E_b/N_0 at (M_{eff}, μ, ϵ) if $\exists(n, M, K_a, \epsilon)$ RA-code with $M = M_{eff} K_a$, $K_a = \mu n$ and codewords of energy

$$\|c\|_2^2 \leq 2\mathcal{E} \log_2 M_{eff}$$

  for all $n \to \infty$.

- Asymptotic fundamental limit: minimal achievable $\mathcal{E}$, i.e.

$$E_\infty^*(M_{eff}, \mu, \epsilon) = \limsup_{n\to\infty} \frac{\log_2 M}{\log M_{eff}} E_b^*(n, M, K_a, \epsilon)$$

Asymptotics of RA and CS

- Recall connection to the compressed sensing.
- Call $E > 0$ feasible at a given ratio p/n and sparsity π if:

$$Y = \sqrt{E} X\beta + Z, \qquad Z \sim \mathcal{N}(0, I_n), \beta \in R^p$$

  - Columns of X are of unit energy
  - $\beta \in \{0,1\}^p$ and $\|\beta\|_0 = \pi p$,
  - $\exists \hat{\beta}(Y, X)$ such that

$$\begin{aligned} \|\hat{\beta}\|_0 &\le \mu n \qquad \text{(FDR)} \\ \|\hat{\beta} - \beta\|_0 &\le 2\epsilon \|\beta\|_0 \end{aligned}$$

- Then we have $E^*_\infty = \min \frac{E}{2 \log_2 M_{eff}}$

Asymptotics of RA and CS

- Recall connection to the compressed sensing.
- Call $E > 0$ feasible at a given ratio p/n and sparsity π if:

$$Y = \sqrt{E} X\beta + Z, \qquad Z \sim \mathcal{N}(0, I_n), \beta \in R^p$$

  - Columns of X are of unit energy
  - $\beta \in \{0,1\}^p$ and $\|\beta\|_0 = \pi p$,
  - $\exists \hat{\beta}(Y, X)$ such that

$$\begin{aligned} \|\hat{\beta}\|_0 &\leq \mu n \qquad (\text{FDR}) \\ \|\hat{\beta} - \beta\|_0 &\leq 2\epsilon \|\beta\|_0 \end{aligned}$$

- Then we have $E^*_\infty = \min \frac{E}{2 \log_2 M_{eff}}$
- When $X \overset{iid}{\sim} \mathcal{N}(0, 1/n)$ this is well studied in stat. physics.

Replica method prediction

- Consider a scalar problem:

$$B = \sqrt{E_1} A + N\,, \qquad A \sim \mathrm{Ber}(\pi) \perp\!\!\!\perp N \sim \mathcal{N}(0,1)$$

- Define $I_1(E_1) = I(A; B)$ and

$$p^*(E_1, \pi) = \min_{\hat{A}} \left\{ \mathbb{P}[A = 0 | \hat{A} = 1] : \mathbb{P}[\hat{A} = 1] = \pi \right\}$$

- It can be seen that p^* is a solution of

$$\sqrt{E_1} = Q^{-1}(p^*) + Q^{-1}\left(\frac{\pi p^*}{1-\pi}\right) .$$

Replica method prediction

- Consider a scalar problem:

$$B = \sqrt{E_1} A + N\,, \qquad A \sim \mathrm{Ber}(\pi) \perp\!\!\!\perp N \sim \mathcal{N}(0,1)$$

- Define $I_1(E_1) = I(A;B)$ and

$$p^*(E_1,\pi) = \min_{\hat{A}} \left\{ \mathbb{P}[A = 0 | \hat{A} = 1] : \mathbb{P}[\hat{A} = 1] = \pi \right\}$$

- It can be seen that p^* is a solution of

$$\sqrt{E_1} = Q^{-1}(p^*) + Q^{-1}\left(\frac{\pi p^*}{1-\pi}\right) .$$

- Stat. physics predicts that inference in

$$Y = \sqrt{E} X\beta + Z, \qquad X \overset{iid}{\sim} \mathcal{N}(0, 1/n), \beta \sim \mathrm{Ber}^{\otimes p}(\pi)$$

  is asymptotically equivalent to a scalar problem with $E_1 = E\eta$
- $\eta \in [0,1]$ (the multi-user efficiency) is given as a solution of

$$\eta = \operatorname*{argmin}_x \left[\frac{p}{n} I_1(xE) + \frac{1}{2}(x - 1 - \ln x) \right]$$

$$B = \sqrt{\eta E} A + N, \qquad A \sim \mathrm{Ber}(\pi) \perp\!\!\!\perp N \sim \mathcal{N}(0,1)$$

$$Y = \sqrt{E} X\beta + Z, \qquad X \overset{iid}{\sim} \mathcal{N}(0, 1/n), \beta \sim \mathrm{Ber}^{\otimes p}(\pi)$$

Theorem (Replica formula exact for binary β)

Consider a sequence of random variables

$$V_n = \mathbb{P}[\beta_1 = 1 | Y, X] \in [0,1]$$

as $p, n \to \infty$ with $p/n = \mathrm{const}$. Then

$$V_n \overset{(d)}{\to} \mathbb{P}[A = 1 | B] .$$

$$B = \sqrt{\eta E} A + N, \qquad A \sim \mathrm{Ber}(\pi) \perp\!\!\!\perp N \sim \mathcal{N}(0,1)$$

$$Y = \sqrt{E} X\beta + Z, \qquad X \overset{iid}{\sim} \mathcal{N}(0, 1/n), \beta \sim \mathrm{Ber}^{\otimes p}(\pi)$$

Theorem (Replica formula exact for binary β)

Consider a sequence of random variables

$$V_n = \mathbb{P}[\beta_1 = 1 | Y, X] \in [0,1]$$

as $p, n \to \infty$ with $p/n = \mathrm{const}$. Then

$$V_n \overset{(d)}{\to} \mathbb{P}[A = 1 | B] \,.$$

- Pfister-Reeves and Barbier-Macris have shown that

$$\mathrm{Var}[\beta_1 | Y, X] \to \mathrm{Var}[A|B]$$

- This is not enough to conclude the proof.

$$B = \sqrt{\eta E} A + N, \qquad A \sim \mathrm{Ber}(\pi) \perp\!\!\!\perp N \sim \mathcal{N}(0,1)$$

$$Y = \sqrt{E} X\beta + Z, \qquad X \overset{iid}{\sim} \mathcal{N}(0, 1/n), \beta \sim \mathrm{Ber}^{\otimes p}(\pi)$$

Theorem (Replica formula exact for binary β)

Consider a sequence of random variables

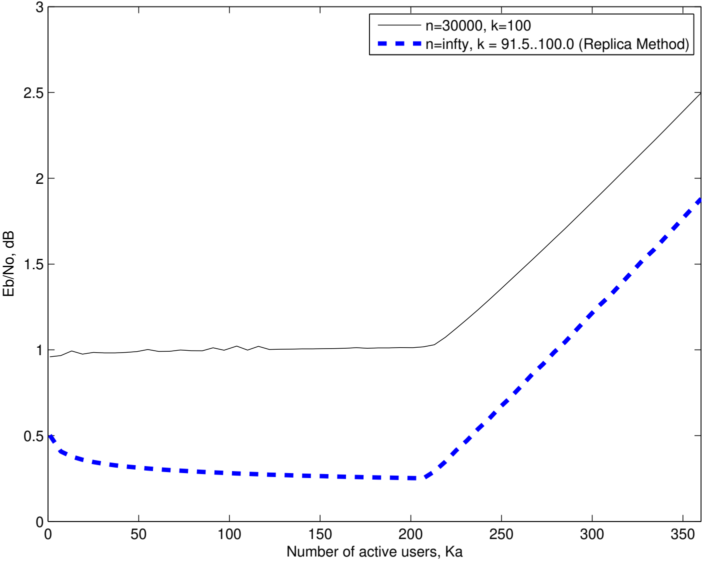
$$V_n = \mathbb{P}[\beta_1 = 1 | Y, X] \in [0,1]$$

as $p, n \to \infty$ with $p/n = \mathrm{const}$. Then

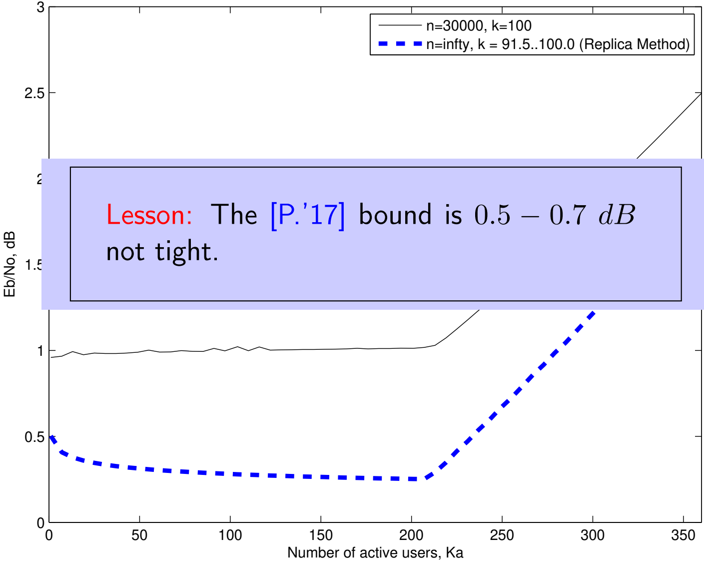
$$V_n \overset{(d)}{\to} \mathbb{P}[A = 1 | B] \,.$$

- Possible to argue indirectly for binary β **only**.
- If we have some sequence $G_n = G_n(Y, X) \in [0,1]$ s.t.
  $\mathbb{E}[(G_n - \beta_1)^2] \to \mathrm{Var}[\beta_1 | Y, X]$ then $G_n \overset{(d)}{\to} \mathbb{E}[\beta_1 | Y, X]$.
  For binary, this is $= \mathbb{P}[\beta_1 = 1 | X, Y]$.
- AMP started at true β yields such a G_n. The law of G_n is known to converge to $\mathbb{P}[A = 1 | B]$.

Finite blocklength bound vs. $n = \infty$ asymptotics

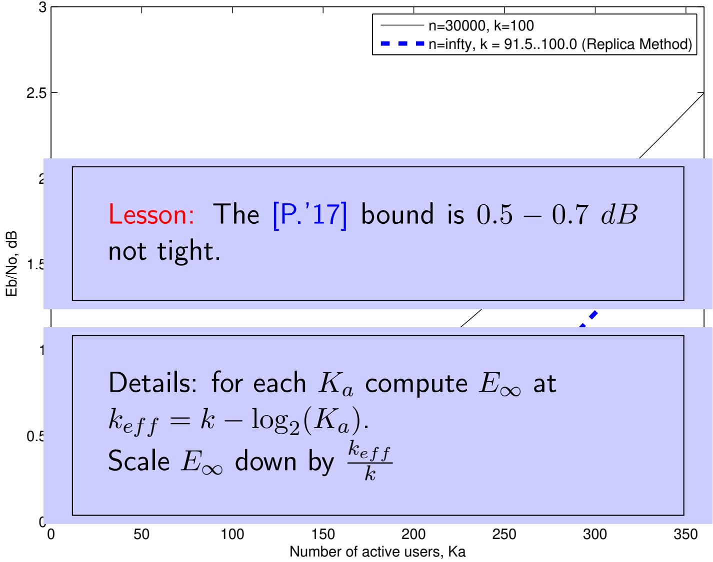


Finite blocklength bound vs. $n = \infty$ asymptotics



Lesson: The [P.'17] bound is $0.5 - 0.7\ dB$ not tight.

Finite blocklength bound vs. $n = \infty$ asymptotics



Lesson: The [P.'17] bound is $0.5 - 0.7\ dB$ not tight.

Details: for each K_a compute E_∞ at $k_{eff} = k - \log_2(K_a)$.
Scale E_∞ down by $\frac{k_{eff}}{k}$

Issue with the asymptotics

- Existence of (n, M, K_a, ϵ) does not imply existence of (Ln, LM, LK_a, ϵ) code (with the same effective E_b/N_0).
- However, existence of $(n, M, \mathrm{Poi}(K_a), \epsilon)$-code does imply the above as $L \to \infty$.
- Let us give a formal definition.

RA-codes for random K_a

Channel model:

$$Y = f(W_1) + \cdots + f(W_T) + Z, \qquad Z \sim \mathcal{N}(0, I_n), T \sim \mathrm{Poi}(K_a)$$

where $W_i \overset{iid}{\sim} \mathrm{Unif}[M]$.

Definition

$f : [M] \to \mathbb{R}^n$ is a $(n, M, \mathrm{Poi}(K_a), \epsilon)$ random-access code if $\exists$ list-decoder g s.t.

$$\begin{aligned} \mathbb{E}[\#\{j : W_j \notin g(Y)\}] &\leq \epsilon \mathbb{E}[T] \\ \mathbb{E}[|g(Y)|] &\leq \mathbb{E}[T] \end{aligned}$$

Open question: There is no random coding bound at present.

Comparing T-fold ALOHA vs. IDMA

- Both T-fold Slotted ALOHA and IDMA try to sparsify collisions.
- T-SA partitions n as $n = Ln_1$ where $L = K_a/T$. Collisions are in n_1-blocks
- Asymptotic fundamental limit of T-SA is the minimal (effective) E_b/N_0 of a $(T/\mu, M_{eff}, \mathrm{Poi}(T), \epsilon)$-codes.

Comparing T-fold ALOHA vs. IDMA

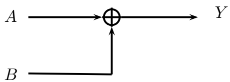
- Both T-fold Slotted ALOHA and IDMA try to sparsify collisions.
- T-SA partitions n as $n = Ln_1$ where $L = K_a/T$. Collisions are in n_1-blocks
- Asymptotic fundamental limit of T-SA is the minimal (effective) E_b/N_0 of a $(T/\mu, M_{eff}, \mathrm{Poi}(T), \epsilon)$-codes.
- Asymptotic fundamental limit of IDMA: Need to solve a (new?) sparse-design compressed sensing problem:

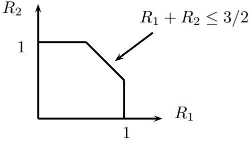
$$Y = \sqrt{E} X\beta + Z$$

  - $X \in \mathbb{R}^{n\times p}$ has unit-energy columns.
  - X has constant $s = M_{eff}T$ non-zeros per-row!
  - $p/n = \mathrm{const}$, $E = \mathrm{const}$, $n \to \infty$.
  - **Open question:** Replica/AMP for $X \overset{iid}{\sim} \frac{c}{p}\mathcal{N}(0, c') + (1 - \frac{c}{p})\delta_0$

Limitations of linear codes

Binary Adder Channel (BAC)

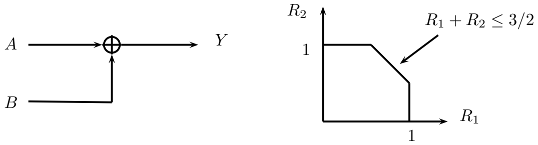




$$Y = A + B \qquad A, B \in \{0,1\}, Y \in \{0,1,2\}$$

- Maximal symmetric rate: $C_{sym} = \frac{1}{2}\max_{A,B} I(A,B;Y) = \frac{1}{2}\max H(A+B) = \frac{3}{4}$
- Maximal same-codebook rate: $C_{same} = \frac{3}{4}$
- Maximal 0-error same-codebook rate: $C_{0,same} \leq 0.5753$ [Cohen-Litsyn-Zemor'01]
- Maximal 0-error symmetric rate: $C_{0,sym} \geq 0.659$ [Bross-Blake'98]

Binary Adder Channel (BAC)



$$Y = A + B \qquad A, B \in \{0, 1\}, Y \in \{0, 1, 2\}$$

- Maximal symmetric rate:
  $C_{sym} = \frac{1}{2} \max_{A,B} I(A, B; Y) = \frac{1}{2} \max H(A + B) = \frac{3}{4}$
- Maximal same-codebook rate: $C_{same} = \frac{3}{4}$
- Maximal 0-error same-codebook rate: $C_{0,same} \leq 0.5753$
  [Cohen-Litsyn-Zemor'01]
- Maximal 0-error symmetric rate: $C_{0,sym} \geq 0.659$ [Bross-Blake'98]
- Thus, for low error-rate there **is** a penalty due to random access.

Limitations of linear codes

Theorem (P.'19, unpublished)

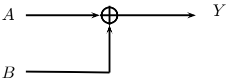
For any same-codebook $\mathcal{C} \subset \{0,1\}^n$ with $|\mathcal{C}| = 2^k$, which is $\mathbb{F}_2$-affine. Then

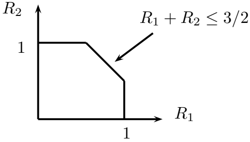
$$P_e \geq \frac{1}{2}\left(1 - \frac{n}{2k-2}\right)$$

Thus, maximal achievable rate via such codes is $\leq \frac{1}{2}$.

- WLOG, assume no constant coordinates. Then average codeword weight $= \frac{n}{2}$.
- Consider two codewords $c_1, c_2 \in \mathcal{C}$. Let $S = \{j : c_{1,j} = c_{2,j}\}$.
- If $|S| < k$ then $\exists 0 \neq c \in \mathcal{C}$ with $c|_S = 0$.
  (since we have $n - k + |S| < n$ equations on c).
- Then $c_1 \oplus c$, $c_2 \oplus c$ is a confusing pair: it has the same real-sum.
- Bound $\mathbb{P}[|S| < k] = \mathbb{P}[|c_1 \oplus c_2|_H > n - k]$ via Chebyshev.

Adder MAC: open issues

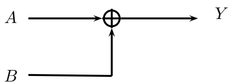


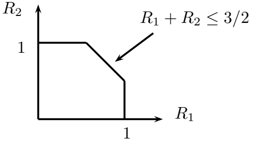


$$Y = A + B \qquad A, B \in \{0, 1\}, Y \in \{0, 1, 2\}$$

- **Challenge:** Find same-codebook code beating $1/2$ barrier.

Adder MAC: open issues

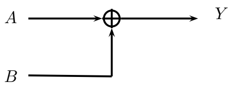


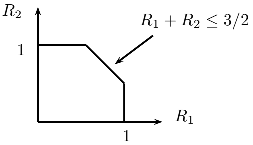


$$Y = A + B \qquad A, B \in \{0,1\}, Y \in \{0,1,2\}$$

- **Challenge:** Find same-codebook code beating $1/2$ barrier.
- Note: two-phase schemes are not allowed
  - use first k_1 data bits (out of $k = nR \gg 1$) to select a permutation matrix for each user.
  - Encode k_1 via any low-rate code into first n_1 coordinates.
  - Then use non-same LDPC codes on the rest $n - n_1$ coordinates.
- Why not allow? e.g. the first k_1 bits have degree $\Omega(n)$ (i.e. affect all coded bits). Bad!

Adder MAC: open issues





$$Y = A + B \qquad A, B \in \{0,1\}, Y \in \{0,1,2\}$$

- **Challenge:** Find same-codebook code beating $1/2$ barrier.
- Note: two-phase schemes are not allowed
  - use first k_1 data bits (out of $k = nR \gg 1$) to select a permutation matrix for each user.
  - Encode k_1 via any low-rate code into first n_1 coordinates.
  - Then use non-same LDPC codes on the rest $n - n_1$ coordinates.
- Why not allow? e.g. the first k_1 bits have degree $\Omega(n)$ (i.e. affect all coded bits). Bad!
- **Challenge:** How to decode sparse-graph same-codebook codes?
- Note: the local beliefs about bits are useless. Need to introduce global "super nodes".

Outline

- Question 1: Is there a useful asymptotics to study?
  A: Yes $K_a = \mu n$, $M = 2^{k_{eff}} K_a$, $n \to \infty$.
- Question 2: What sparsification is more useful? (IDMA vs. T-SA)
  A: Need to solve $\mathrm{Poi}(K_a)$ problem. Need to solve sparse-design CS.
- Question 3: Limitations of linear codes.
  A: Non-capacity achieving. **Challenge:** Find alternatives.

Outline

- Question 1: Is there a useful asymptotics to study?
  A: Yes $K_a = \mu n$, $M = 2^{k_{eff}} K_a$, $n \to \infty$.
- Question 2: What sparsification is more useful? (IDMA vs. T-SA)
  A: Need to solve $\mathrm{Poi}(K_a)$ problem. Need to solve sparse-design CS.
- Question 3: Limitations of linear codes.
  A: Non-capacity achieving. **Challenge:** Find alternatives.

Thank you!