

# Low Complexity Schemes for the Random Access Gaussian Channel

Or Ordentlich (Hebrew University of Jerusalem)  
Joint work with Yury Polyanskiy (MIT)

NSF Workshop on Low-Latency Wireless Random-Access,  
MIT,  
November 2, 2017

## Massive Connectivity

**Key challenge for next generation wireless networks:  
Providing multiple-access to massive number of infrequently  
**UNCOORDINATED** communicating devices**

# Massive Connectivity

**Key challenge for next generation wireless networks:  
Providing multiple-access to massive number of infrequently  
**UNCOORDINATED** communicating devices**

Typical scenario:

- Very large number of users, say  $K_{\text{tot}} \approx 10^6 - 10^7$
- Much smaller, but still large, number of them active within each communication block, say  $K_a \approx 50 - 500$
- Message of each active user is short, say  $k = 100$  bits
- Blocklength is  $n \approx 10^4 - 10^5$
- $\frac{k}{n} \ll 1$ , but the total spectral efficiency  $\rho = \frac{K_a \cdot k}{n}$  is moderate, say 1 bit per channel use

# Massive Connectivity

**Key challenge for next generation wireless networks:**

**Providing multiple-access to massive number of infrequently  
UNCOORDINATED communicating devices**

Typical scenario:

- Very large number of users, say  $K_{\text{tot}} \approx 10^6 - 10^7$
- Much smaller, but still large, number of them active within each communication block, say  $K_a \approx 50 - 500$
- Message of each active user is short, say  $k = 100$  bits
- Blocklength is  $n \approx 10^4 - 10^5$
- $\frac{k}{n} \ll 1$ , but the total spectral efficiency  $\rho = \frac{K_a \cdot k}{n}$  is moderate, say 1 bit per channel use

The goal is to communicate with the smallest possible  
energy-per-bit

# Gaussian Random Access Channel

$$\mathbf{y} = \sum_{i=1}^{K_{\text{tot}}} s_i \mathbf{x}_i + \mathbf{z},$$

- $K_{\text{tot}}$  possible users,  $K_a$  of them are active
- $(s_1, \dots, s_{K_{\text{tot}}}) \in \{0, 1\}^{K_{\text{tot}}}$  with Hamming weight  $K_a$ , **unknown**
- $\mathbf{z} \sim \mathcal{N}(0, \mathbf{I})$ ,  $\mathbf{x}_i \in \mathbb{R}^n$ ,  $\|\mathbf{x}_i\|^2 \leq nP$
- Each active user has a  $k$ -bit message  $M_i$

# Gaussian Random Access Channel

$$\mathbf{y} = \sum_{i=1}^{K_{\text{tot}}} s_i \mathbf{x}_i + \mathbf{z},$$

- $K_{\text{tot}}$  possible users,  $K_a$  of them are active
- $(s_1, \dots, s_{K_{\text{tot}}}) \in \{0, 1\}^{K_{\text{tot}}}$  with Hamming weight  $K_a$ , **unknown**
- $\mathbf{z} \sim \mathcal{N}(0, \mathbf{I})$ ,  $\mathbf{x}_i \in \mathbb{R}^n$ ,  $\|\mathbf{x}_i\|^2 \leq nP$
- Each active user has a  $k$ -bit message  $M_i$

**Decoder's job: Output an unordered list  $\mathcal{L}(\mathbf{y})$  of  $K_a$  messages that contains most messages that were transmitted**  
user identification handled in higher layers

# Gaussian Random Access Channel

$$\mathbf{y} = \sum_{i=1}^{K_{\text{tot}}} s_i \mathbf{x}_i + \mathbf{z},$$

- $K_{\text{tot}}$  possible users,  $K_a$  of them are active
- $(s_1, \dots, s_{K_{\text{tot}}}) \in \{0, 1\}^{K_{\text{tot}}}$  with Hamming weight  $K_a$ , **unknown**
- $\mathbf{z} \sim \mathcal{N}(0, \mathbf{I})$ ,  $\mathbf{x}_i \in \mathbb{R}^n$ ,  $\|\mathbf{x}_i\|^2 \leq nP$
- Each active user has a  $k$ -bit message  $M_i$

**Decoder's job: Output an unordered list  $\mathcal{L}(\mathbf{y})$  of  $K_a$  messages that contains most messages that were transmitted**  
user identification handled in higher layers

$$P_e = \max_{|(s_1, \dots, s_{K_{\text{tot}}})|=K_a} \frac{1}{K_a} \sum_{i=1}^{K_{\text{tot}}} s_i \cdot \Pr(M_i \notin \mathcal{L}(\mathbf{y}))$$

# Gaussian Random Access Channel

$$\mathbf{y} = \sum_{i=1}^{K_{\text{tot}}} s_i \mathbf{x}_i + \mathbf{z},$$

- $K_{\text{tot}}$  possible users,  $K_a$  of them are active
- $(s_1, \dots, s_{K_{\text{tot}}}) \in \{0, 1\}^{K_{\text{tot}}}$  with Hamming weight  $K_a$ , **unknown**
- $\mathbf{z} \sim \mathcal{N}(0, \mathbf{I})$ ,  $\mathbf{x}_i \in \mathbb{R}^n$ ,  $\|\mathbf{x}_i\|^2 \leq nP$
- Each active user has a  $k$ -bit message  $M_i$

**Decoder's job: Output an unordered list  $\mathcal{L}(\mathbf{y})$  of  $K_a$  messages that contains most messages that were transmitted**  
user identification handled in higher layers

$$P_e = \max_{|(s_1, \dots, s_{K_{\text{tot}}})|=K_a} \frac{1}{K_a} \sum_{i=1}^{K_{\text{tot}}} s_i \cdot \Pr(M_i \notin \mathcal{L}(\mathbf{y}))$$

Formulation does not become trivial for  $K_{\text{tot}} = \infty$



# Gaussian Random Access Channel

$$\mathbf{y} = \sum_{i=1}^{K_{\text{tot}}} s_i \mathbf{x}_i + \mathbf{z},$$

- $K_{\text{tot}}$  possible users,  $K_a$  of them are active
- $(s_1, \dots, s_{K_{\text{tot}}}) \in \{0, 1\}^{K_{\text{tot}}}$  with Hamming weight  $K_a$ , **unknown**
- $\mathbf{z} \sim \mathcal{N}(0, \mathbf{I})$ ,  $\mathbf{x}_i \in \mathbb{R}^n$ ,  $\|\mathbf{x}_i\|^2 \leq nP$
- Each active user has a  $k$ -bit message  $M_i$

**Decoder's job: Output an unordered list  $\mathcal{L}(\mathbf{y})$  of  $K_a$  messages that contains most messages that were transmitted**  
user identification handled in higher layers

$$P_e = \max_{|(s_1, \dots, s_{K_{\text{tot}}})|=K_a} \frac{1}{K_a} \sum_{i=1}^{K_{\text{tot}}} s_i \cdot \Pr(M_i \notin \mathcal{L}(\mathbf{y}))$$

**Goal: For given  $(n, k, K_a, P_e)$  minimize  $\frac{E_b}{N_0} \triangleq \frac{nP}{2k}$**

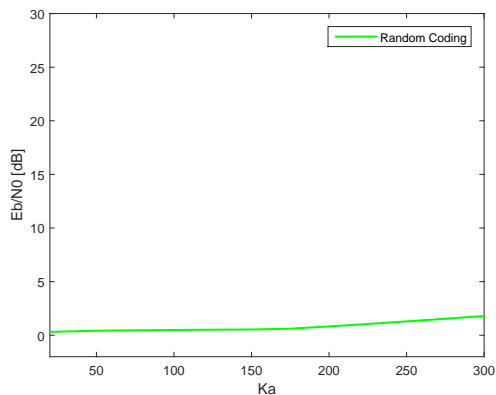
## Potential Coding Schemes

Natural approach is to use the same codebook for all transmitters

# Potential Coding Schemes

Natural approach is to use the same codebook for all transmitters

Random coding achievability bound (Polyanskiy, ISIT'17)



$$n = 30,000, k = 100, P_e = 0.05$$

# Potential Coding Schemes

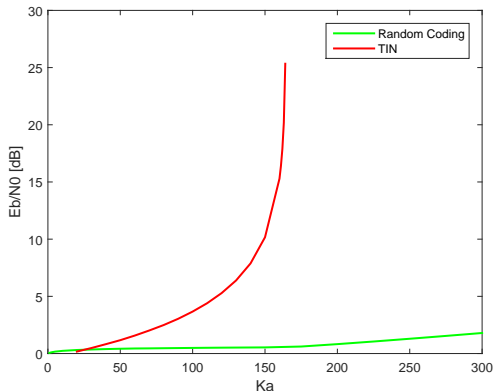
What about more practical solutions?

# Potential Coding Schemes

What about more practical solutions?

Option I - treat interference as noise (un-coordinated CDMA)

Total spectral efficiency is limited  $\rho \triangleq \frac{K_a \cdot k}{n} < \frac{\log(e)}{2} \frac{\text{bits}}{\text{channel use}}$



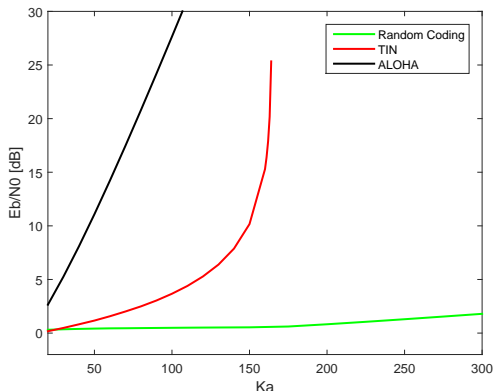
$n = 30,000, k = 100, P_e = 0.05$

# Potential Coding Schemes

What about more practical solutions?

Option II - slotted-ALOHA

Works well for  $P_e \geq 1 - \frac{1}{e}$ . Otherwise, to keep collision probability below  $P_e$  the fraction of utilized slots is  $\approx \ln \frac{1}{1-P_e}$



$n = 30,000, k = 100, P_e = 0.05$

# Potential Coding Schemes

Not quite practical, but getting closer...

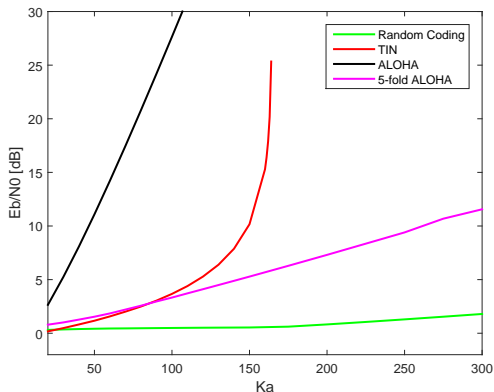
# Potential Coding Schemes

Not quite practical, but getting closer...

T-fold ALOHA : ALOHA with good channel codes for T-user MAC

Collisions of  $\leq T$  users can be resolved

$\implies$  fraction of utilized slots increases



$$n = 30,000, k = 100, P_e = 0.05$$



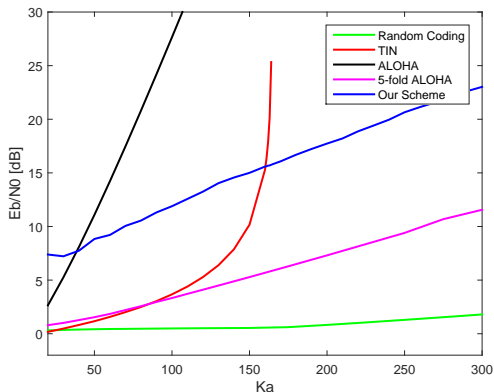
# Potential Coding Schemes

This work: a practical realization of this idea

# Potential Coding Schemes

This work: a practical realization of this idea

Low-complexity (suboptimal) code design for the  $T$ -user MAC with same codebook for all users, combined with  $T$ -fold ALOHA



$n = 30,000$ ,  $k = 100$ ,  $P_e = 0.05$

# High-Level Overview of Scheme

Split the  $n$  channel uses to  $V$  sub-blocks

## High-Level Overview of Scheme

Split the  $n$  channel uses to  $V$  sub-blocks

All users encode their messages using the same codebook  $\mathcal{C} \in \mathbb{R}^{n/V}$

## High-Level Overview of Scheme

Split the  $n$  channel uses to  $V$  sub-blocks

All users encode their messages using the same codebook  $\mathcal{C} \in \mathbb{R}^{n/V}$

Each active user maps its message to a codeword in  $\mathcal{C}$ , and transmits it over one sub-block chosen uniformly over  $[V]$

## High-Level Overview of Scheme

Split the  $n$  channel uses to  $V$  sub-blocks

All users encode their messages using the same codebook  $\mathcal{C} \in \mathbb{R}^{n/V}$

Each active user maps its message to a codeword in  $\mathcal{C}$ , and transmits it over one sub-block chosen uniformly over  $[V]$

If  $L > T$  users transmitted during a sub-block, all their messages are **not delivered**.

Otherwise, the decoder attempts to recover the  $L$  messages and add them to its list

# High-Level Overview of Scheme

Split the  $n$  channel uses to  $V$  sub-blocks

All users encode their messages using the same codebook  $\mathcal{C} \in \mathbb{R}^{n/V}$

Each active user maps its message to a codeword in  $\mathcal{C}$ , and transmits it over one sub-block chosen uniformly over  $[V]$

If  $L > T$  users transmitted during a sub-block, all their messages are **not delivered**.

Otherwise, the decoder attempts to recover the  $L$  messages and add them to its list

**Coding task: design a codebook  $\mathcal{C}$  with efficient encoding/decoding algorithms and good performance for  $T$ -user MAC**

# High-Level Overview of Scheme

We will use a **concatenated code**:

Inner code will deal with noise (*CoF phase*)

Outer code with interaction between codewords (*BAC phase*)



## High-Level Overview of Scheme

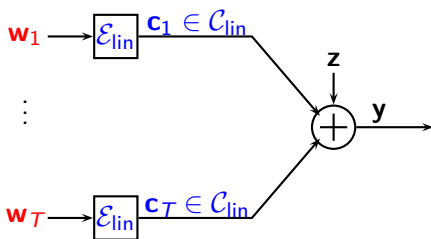
Inner code  $\mathcal{C}_{\text{lin}}$  converts the  $T$ -user Gaussian MAC into a modulo- $p$  noiseless adder MAC.

This is done via compute-and-forward [Nazer-Gastpar'11]

# High-Level Overview of Scheme

Inner code  $\mathcal{C}_{\text{lin}}$  converts the  $T$ -user Gaussian MAC into a modulo- $p$  noiseless adder MAC.

This is done via compute-and-forward [Nazer-Gastpar'11]



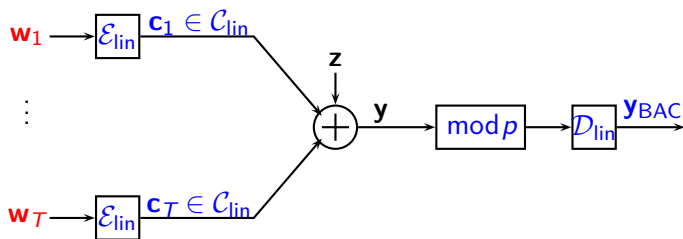
$\mathbf{w}_1, \dots, \mathbf{w}_T$  are vectors in  $\mathbb{Z}_p$

$\mathcal{C}_{\text{lin}}$  is linear code over  $\mathbb{Z}_p$

# High-Level Overview of Scheme

Inner code  $\mathcal{C}_{\text{lin}}$  converts the  $T$ -user Gaussian MAC into a modulo- $p$  noiseless adder MAC.

This is done via compute-and-forward [Nazer-Gastpar'11]



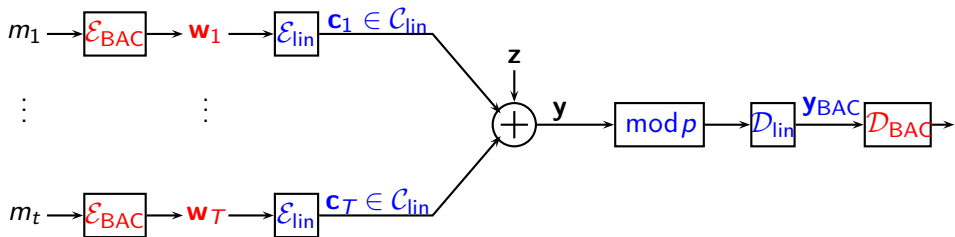
$\mathbf{w}_1, \dots, \mathbf{w}_T$  are vectors in  $\mathbb{Z}_p$

$\mathcal{C}_{\text{lin}}$  is linear code over  $\mathbb{Z}_p$

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \text{mod } p$$

# High-Level Overview of Scheme

Outer code  $\mathcal{C}_{\text{BAC}}$  is designed for the  $T$ -user modulo- $p$  adder MAC



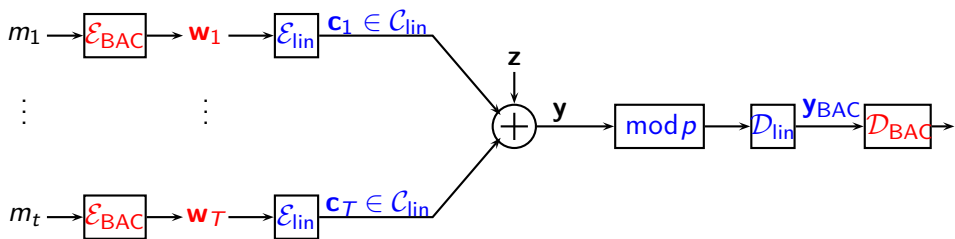
$\mathbf{w}_1, \dots, \mathbf{w}_T$  are vectors in  $\mathbb{Z}_p$

$\mathcal{C}_{\text{lin}}$  is linear code over  $\mathbb{Z}_p$

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \bmod p$$

# High-Level Overview of Scheme

The most practical choice is  $p = 2$  and this is our focus



$\mathbf{w}_1, \dots, \mathbf{w}_T$  are vectors in  $\mathbb{Z}_p$

$\mathcal{C}_{\text{lin}}$  is linear code over  $\mathbb{Z}_p$

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \text{mod } p$$

## Related Work

Most of the ideas we use appeared before in various contexts. Their combination to a coding scheme for the Gaussian random access channel is new.

- Compute-and-forward [Nazer-Gastpar'11]
- Explicit codes for the modulo-2 binary adder channel [Lindström'69, Bar-David et al.'93]
- Concatenation of codes with good minimum distance and codes for the BAC [Ericson-Levenshtein'94]
- Concatenation of CoF inner codes with syndrome decoding for compressed sensing [Lee-Hong'16]

## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint

## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint
- Receiver sees  $\mathbf{y} = \sum_{i=1}^T \mathbf{x}_i + \mathbf{z}$ , after shifting and scaling  $\mathbf{y}$ , and reducing modulo-2, we get

$$\mathbf{y}_{\text{CoF}} = [\mathbf{x} + \mathbf{z}] \bmod 2$$

where  $\mathbf{x} = [\sum_i \mathbf{x}_i] \bmod 2 \in \mathcal{C}_{\text{lin}}$



## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint
- Receiver sees  $\mathbf{y} = \sum_{i=1}^T \mathbf{x}_i + \mathbf{z}$ , after shifting and scaling  $\mathbf{y}$ , and reducing modulo-2, we get

$$\mathbf{y}_{\text{CoF}} = [\mathbf{x} + \mathbf{z}] \bmod 2$$

where  $\mathbf{x} = [\sum_i \mathbf{x}_i] \bmod 2 \in \mathcal{C}_{\text{lin}}$

- The channel from  $\mathbf{x}$  to  $\mathbf{y}_{\text{CoF}}$  is a BMS  
 $\implies$  Designing  $\mathcal{C}_{\text{lin}}$  is a standard coding task

## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint
- Receiver sees  $\mathbf{y} = \sum_{i=1}^T \mathbf{x}_i + \mathbf{z}$ , after shifting and scaling  $\mathbf{y}$ , and reducing modulo-2, we get

$$\mathbf{y}_{\text{CoF}} = [\mathbf{x} + \mathbf{z}] \bmod 2$$

where  $\mathbf{x} = [\sum_i \mathbf{x}_i] \bmod 2 \in \mathcal{C}_{\text{lin}}$

- The channel from  $\mathbf{x}$  to  $\mathbf{y}_{\text{CoF}}$  is a BMS  
 $\implies$  Designing  $\mathcal{C}_{\text{lin}}$  is a standard coding task

**What is lost in the conversion  $\mathbf{y} \mapsto \mathbf{y}_{\text{CoF}}$ ?**

## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint
- Receiver sees  $\mathbf{y} = \sum_{i=1}^T \mathbf{x}_i + \mathbf{z}$ , after shifting and scaling  $\mathbf{y}$ , and reducing modulo-2, we get

$$\mathbf{y}_{\text{CoF}} = [\mathbf{x} + \mathbf{z}] \bmod 2$$

where  $\mathbf{x} = [\sum_i \mathbf{x}_i] \bmod 2 \in \mathcal{C}_{\text{lin}}$

- The channel from  $\mathbf{x}$  to  $\mathbf{y}_{\text{CoF}}$  is a BMS  
 $\implies$  Designing  $\mathcal{C}_{\text{lin}}$  is a standard coding task

**What is lost in the conversion  $\mathbf{y} \mapsto \mathbf{y}_{\text{CoF}}$ ?**

Sum-capacity of  $\mathbf{y}$  grows like  $\log(T \cdot P)$

Capacity of  $\mathbf{y}_{\text{CoF}}$  only grows like  $\log(P)$

## More on the CoF phase

- We construct  $\mathcal{C}_{\text{lin}}$  from a binary linear code, shifted and scaled to meet the power constraint
- Receiver sees  $\mathbf{y} = \sum_{i=1}^T \mathbf{x}_i + \mathbf{z}$ , after shifting and scaling  $\mathbf{y}$ , and reducing modulo-2, we get

$$\mathbf{y}_{\text{CoF}} = [\mathbf{x} + \mathbf{z}] \bmod 2$$

where  $\mathbf{x} = [\sum_i \mathbf{x}_i] \bmod 2 \in \mathcal{C}_{\text{lin}}$

- The channel from  $\mathbf{x}$  to  $\mathbf{y}_{\text{CoF}}$  is a BMS  
 $\implies$  Designing  $\mathcal{C}_{\text{lin}}$  is a standard coding task

**What is lost in the conversion  $\mathbf{y} \mapsto \mathbf{y}_{\text{CoF}}$ ?**

Sum-capacity of  $\mathbf{y}$  grows like  $\log(T \cdot P)$

Capacity of  $\mathbf{y}_{\text{CoF}}$  only grows like  $\log(P)$

**$T$ -fold ALOHA reduces “power-loss” to  $1/T$  instead of  $1/K_a$**

## More on the BAC Phase

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \text{ mod } 2, \quad \mathbf{w}_1, \dots, \mathbf{w}_T \in \mathcal{C}_{\text{BAC}}$$

Need to decode a list  $\{\mathbf{w}_1, \dots, \mathbf{w}_T\}$

## More on the BAC Phase

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \bmod 2, \quad \mathbf{w}_1, \dots, \mathbf{w}_T \in \mathcal{C}_{\text{BAC}}$$

Need to decode a list  $\{\mathbf{w}_1, \dots, \mathbf{w}_T\}$

The symmetric-capacity of this MAC is  $1/T$  bits/channel use

## More on the BAC Phase

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \bmod 2, \quad \mathbf{w}_1, \dots, \mathbf{w}_T \in \mathcal{C}_{\text{BAC}}$$

### How to construct explicit codes?

- Let  $H = [\mathbf{h}_1 | \dots | \mathbf{h}_n]$  be the parity-check matrix of a  $[n, k]$  binary  $T$ -error correcting code
- All linear combinations of at most  $T$  columns are distinct
- The code  $\mathcal{C}_{\text{BAC}} = \{\mathbf{h}_1, \dots, \mathbf{h}_n\}$  is (almost) zero-error for the  $T$ -user mod-2 adder MAC
- $R_{\text{BAC}} = \frac{\log n}{n-k}$

## More on the BAC Phase

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \bmod 2, \quad \mathbf{w}_1, \dots, \mathbf{w}_T \in \mathcal{C}_{\text{BAC}}$$

### How to construct explicit codes?

- Let  $H = [\mathbf{h}_1 | \dots | \mathbf{h}_n]$  be the parity-check matrix of a  $[n, k]$  binary  $T$ -error correcting code
- All linear combinations of at most  $T$  columns are distinct
- The code  $\mathcal{C}_{\text{BAC}} = \{\mathbf{h}_1, \dots, \mathbf{h}_n\}$  is (almost) zero-error for the  $T$ -user mod-2 adder MAC
- $R_{\text{BAC}} = \frac{\log n}{n-k}$

$\forall r \geq 3, \exists [n = 2^r - 1, n - k = rT, d \geq 2T + 1]$  binary BCH code  
Rate of induced  $\mathcal{C}_{\text{BAC}}$  is  $R_{\text{BAC}} = \frac{\log 2^r - 1}{rT} \approx \frac{1}{T}$



## More on the BAC Phase

$$\mathbf{y}_{\text{BAC}} = \left[ \sum_{i=1}^T \mathbf{w}_i \right] \bmod 2, \quad \mathbf{w}_1, \dots, \mathbf{w}_T \in \mathcal{C}_{\text{BAC}}$$

### How to construct explicit codes?

- Let  $H = [\mathbf{h}_1 | \dots | \mathbf{h}_n]$  be the parity-check matrix of a  $[n, k]$  binary  $T$ -error correcting code
- All linear combinations of at most  $T$  columns are distinct
- The code  $\mathcal{C}_{\text{BAC}} = \{\mathbf{h}_1, \dots, \mathbf{h}_n\}$  is (almost) zero-error for the  $T$ -user mod-2 adder MAC
- $R_{\text{BAC}} = \frac{\log n}{n-k}$

$\forall r \geq 3, \exists [n = 2^r - 1, n - k = rT, d \geq 2T + 1]$  binary BCH code  
Rate of induced  $\mathcal{C}_{\text{BAC}}$  is  $R_{\text{BAC}} = \frac{\log 2^r - 1}{rT} \approx \frac{1}{T}$

**Problem: decoding complexity of BCH linear in  $n = 2^r - 1$**

## More on the BAC Phase - Encoding & Decoding

Encoding:

Each column of  $H$  is of the form  $[\alpha, \alpha^3, \dots, \alpha^{2T-1}]$ , for  $\alpha \in GF(2^k) \setminus \{0\}$

To encode, just map messages to elements of  $GF(2^k) \setminus \{0\}$  and compute first  $T$  odd powers

## More on the BAC Phase - Encoding & Decoding

Decoding:

Modified GPZ algorithm, almost the same as Bar-David et al.'93

- *Syndrome computation*: odd syndromes given “for free” from  $\mathbf{y}_{\text{BAC}}$ . Computing even syndromes from them is easy
- *Construction of error locator polynomial*: Berlekamp-Massey algorithm gives

$$\sigma(X) = 1 + \sum_{t=1}^L \sigma_t X^t = \prod_{i=1}^T (1 + \alpha_i X)$$

where  $\alpha_1, \dots, \alpha_T$  correspond to the messages

- *Finding the roots of  $\sigma(X)$* : Rabin's probabilistic algorithm [Rabin'80] finds  $\alpha_1^{-1}, \dots, \alpha_T^{-1}$
- *Inversion of the roots*: using the identity  $\alpha^{-1} = \alpha^{2^k} - 1$

Total complexity:  $\mathcal{O}(kT^2 \log^2(T) \log \log(T))$  operations in  $GF(2^k)$

# Spectral Efficiency $> 1$

The spectral efficiency  $\rho = \frac{K_a \cdot k}{n}$  of our scheme is at most  $R_{\text{lin}}$   
What if  $\rho > 1$ ?

Option I - work with  $p > 2$

- CoF phase requires good linear codes over  $\mathbb{F}_p$
- BAC phase can be implemented using  $H = [\mathbf{h}_1 | \dots | \mathbf{h}_n]$  of a  $[n = p^s - 1, n - k = 2T]$  Reed-Solomon code over  $\mathbb{F}_{p^s}$  with

$$\mathcal{C}_{\text{BAC}} = \{\alpha \mathbf{h}_i : \alpha \in \mathbb{F}_{p^s} \setminus \{0\}, i = 1, \dots, p^s - 1\}$$

- Can also use a nested lattice code to achieve the 1.53dB shaping gain

# Spectral Efficiency $> 1$

The spectral efficiency  $\rho = \frac{K_a \cdot k}{n}$  of our scheme is at most  $R_{\text{lin}}$   
What if  $\rho > 1$ ?

Option I - work with  $p > 2$

- CoF phase requires good linear codes over  $\mathbb{F}_p$
- BAC phase can be implemented using  $H = [\mathbf{h}_1 | \dots | \mathbf{h}_n]$  of a  $[[n = p^s - 1, n - k = 2T]]$  Reed-Solomon code over  $\mathbb{F}_{p^s}$  with

$$\mathcal{C}_{\text{BAC}} = \{\alpha \mathbf{h}_i : \alpha \in \mathbb{F}_{p^s} \setminus \{0\}, i = 1, \dots, p^s - 1\}$$

- Can also use a nested lattice code to achieve the 1.53dB shaping gain

But encoders in our setup must be extremely simple  
 $\implies$  binary codes are preferable

## Spectral Efficiency $> 1$

The spectral efficiency  $\rho = \frac{K_a \cdot k}{n}$  of our scheme is at most  $R_{lin}$   
What if  $\rho > 1$ ?

Option II - use a multilevel code based on binary codes

- Allows to increase  $R_{lin}$  above 1
- Requires some overhead in order to “pair” messages from different layers

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .



## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

$$\Delta = \left(\frac{E_b}{N_0}\right) \text{ dB} - \left(\frac{E_b}{N_0}\right)^* \text{ dB}$$

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

$$\Delta = \left(\frac{E_b}{N_0}\right) \text{ dB} - \left(\frac{E_b}{N_0}\right)^* \text{ dB}$$
$$\approx 6\rho \frac{1-\alpha}{\alpha} + 10 \log_{10}(\alpha)$$

T-Collision avoidance loss due to a  $1/\alpha$  increase in spectral efficiency

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

$$\begin{aligned}\Delta &= \left(\frac{E_b}{N_0}\right) \text{dB} - \left(\frac{E_b}{N_0}\right)^* \text{dB} \\ &\approx 6\rho \frac{1-\alpha}{\alpha} + 10 \log_{10}(\alpha) + 10 \log_{10}(T)\end{aligned}$$

CoF loss from the reduction  $\mathbf{y} \mapsto \mathbf{y}_{\text{CoF}}$

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

$$\begin{aligned}\Delta &= \left(\frac{E_b}{N_0}\right) \text{dB} - \left(\frac{E_b}{N_0}\right)^* \text{dB} \\ &\approx 6\rho \frac{1-\alpha}{\alpha} + 10 \log_{10}(\alpha) + 10 \log_{10}(T) - 10 \log_{10}(1 - 2^{-2\rho})\end{aligned}$$

Loss of +1 in computation rate

## Approximate performance

A TDMA scheme with infinite blocklength and fixed  $K_a$  can achieve  $\left(\frac{E_b}{N_0}\right)^* = \frac{2^{2\rho}-1}{2\rho}$  where  $\rho = \frac{K_a \cdot k}{n}$ .

How far are we from  $\left(\frac{E_b}{N_0}\right)^*$ ?

Fix  $T$  and set the number of sub-blocks to  $V = \frac{K_a}{\alpha T}$  for  $\alpha \in (0, 1]$ .

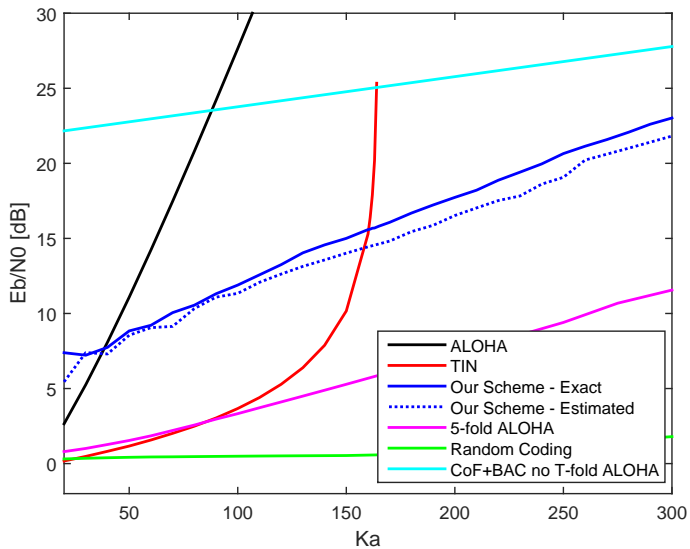
The  $T$ -collision probability is  $\Pr\left(\text{Binomial}\left(K_a - 1, \frac{\alpha T}{K_a}\right) \geq T\right)$

Linear code required to have rate  $R_{\text{lin}} = \frac{\rho}{\alpha}$

$$\begin{aligned}\Delta &= \left(\frac{E_b}{N_0}\right) \text{dB} - \left(\frac{E_b}{N_0}\right)^* \text{dB} \\ &\approx 6\rho \frac{1-\alpha}{\alpha} + 10 \log_{10}(\alpha) + 10 \log_{10}(T) - 10 \log_{10}(1 - 2^{-2\rho}) + 1.53\end{aligned}$$

Shaping loss

# Approximate performance





## Summary and Conclusions

- We considered T-fold ALOHA (MPR) as a candidate coding scheme for the Gaussian random access channel
- We constructed a practical variant of T-fold ALOHA based on concatenation of CoF codes and BAC codes
- Our scheme is far from optimal, but significantly outperforms competing low-complexity schemes in regimes of practical interest