Binary Subspace Chirps

A fast multi-user decoding algorithm

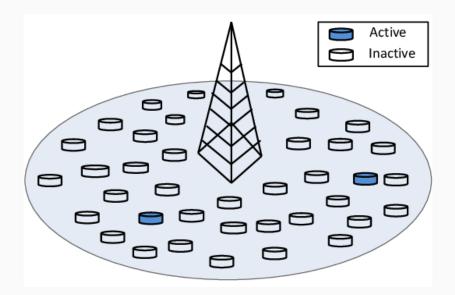
Tefjol Pllaha Joint with R. Calderbank and O. Tirkkonen

Department of Communications and Networking Aalto University, Finland

Massive Machine Type Communications (mMTC)



Random Access in mMTC



- M users, L active users, $L \ll M$.
- Each active user u_{ℓ} transmits signal $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Receiver sees

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} \mathbf{c}_{\ell} \mathbf{s}_{u_{\ell}}\right) + \mathbf{n}, \quad \mathbf{c}_{\ell} \in \mathbb{C}, \mathbf{n} \in \mathbb{C}^{N}.$$

• **Problem:** Determine $\{u_1, \ldots, u_L\}$ given **s**.

- M users, L active users, $L \ll M$.
- Each active user u_{ℓ} transmits signal $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Receiver sees

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} \mathbf{c}_{\ell} \mathbf{s}_{u_{\ell}}\right) + \mathbf{n}, \quad \mathbf{c}_{\ell} \in \mathbb{C}, \mathbf{n} \in \mathbb{C}^{N}.$$

- **Problem:** Determine $\{u_1, \ldots, u_L\}$ given **s**.
- Compressed Sensing Prospective:
 - $\Phi \in \mathbb{C}^{N \times M}, \mathbf{c} \in \mathbb{C}^{M}$.
 - Determine the support of **c** given $\mathbf{s} = \Phi \mathbf{c}$.
 - Design problem: Construct Φ so that support recovery is possible.

Framework

- M users, L active users, $L \ll M$.
- Each active user u_{ℓ} transmits signal $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Receiver sees

$$\mathbf{s} = \left(\sum_{\ell=1}^{L} \mathbf{c}_{\ell} \mathbf{s}_{u_{\ell}}\right) + \mathbf{n}, \ \mathbf{c}_{\ell} \in \mathbb{C}, \mathbf{n} \in \mathbb{C}^{N}.$$

- **Problem:** Determine $\{u_1, \ldots, u_L\}$ given **s**.
- Compressed Sensing Prospective:
 - $\Phi \in \mathbb{C}^{N \times M}, \mathbf{c} \in \mathbb{C}^{M}$.
 - Determine the support of **c** given $\mathbf{s} = \Phi \mathbf{c}$.
 - **Design problem:** Construct Φ so that support recovery is possible.
 - Solution 1: Restricted Isometric Property (RIP).
 - Solution 2: Deterministic sensing matrices.

• Throughout we will use $N = 2^m$.

- Throughout we will use $N = 2^m$.
- Each active user u_{ℓ} transmits its preassigned signature $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.

- Throughout we will use $N = 2^m$.
- Each active user u_{ℓ} transmits its preassigned signature $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Threshold Decoder: Declare user u_{ℓ} active if $|\mathbf{s}^{\dagger}\mathbf{s}_{u_{\ell}}|$ is larger than some threshold.

- Throughout we will use $N = 2^m$.
- Each active user u_{ℓ} transmits its preassigned signature $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Threshold Decoder: Declare user u_{ℓ} active if $|\mathbf{s}^{\dagger}\mathbf{s}_{u_{\ell}}|$ is larger than some threshold.
 - High complexity: Requires *M* measurements!

- Throughout we will use $N = 2^m$.
- Each active user u_{ℓ} transmits its preassigned signature $\mathbf{s}_{u_{\ell}} \in \mathbb{C}^{N}$.
- Threshold Decoder: Declare user u_{ℓ} active if $|\mathbf{s}^{\dagger}\mathbf{s}_{u_{\ell}}|$ is larger than some threshold.
 - High complexity: Requires *M* measurements!
- Key idea: Reed-Muller sequences in C^N can be decoded with log(N) = m measurements.

• Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathrm{t}} \mathbf{S}\mathbf{a} + 2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}}i^{\mathbf{a}^{\mathrm{t}}\mathbf{S}\mathbf{a}+2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

• A binary chirp (BC) is a column $\boldsymbol{U}_{\boldsymbol{S},\boldsymbol{b}}.$

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathrm{t}} \mathbf{S}\mathbf{a} + 2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

- A binary chirp (BC) is a column $U_{S,b}$.
 - There are $2^m \cdot 2^{m(m+1)/2}$ BCs.

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathrm{t}} \mathbf{S}\mathbf{a} + 2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

- A binary chirp (BC) is a column $U_{S,b}$.
 - There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
 - If **S** has zero diagonal then $\mathbf{U}_{\mathbf{S},\mathbf{b}} \in \mathbb{R}^N$.

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathrm{t}} \mathbf{S}\mathbf{a} + 2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

- A binary chirp (BC) is a column $U_{S,b}$.
 - There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
 - If **S** has zero diagonal then $\mathbf{U}_{\mathbf{S},\mathbf{b}} \in \mathbb{R}^N$.
 - There are $2^m \cdot 2^{m(m-1)/2}$ real BCs.

- Fix $m \in \mathbb{N}$ and $\mathbf{S} \in \operatorname{Sym}(m)$ binary symmetric.
- Recall N = 2^m. C^N is indexed with 𝔽^m₂ (all vectors, complex or binary, are column vectors).
- Define a unitary matrix $\boldsymbol{U}_{\boldsymbol{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{N}}i^{\mathbf{a}^{\mathrm{t}}\mathbf{S}\mathbf{a}+2\mathbf{b}^{\mathrm{t}}\mathbf{a} \mod 4}$$

- A binary chirp (BC) is a column $U_{S,b}$.
 - There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
 - If **S** has zero diagonal then $\mathbf{U}_{\mathbf{S},\mathbf{b}} \in \mathbb{R}^N$.
 - There are $2^m \cdot 2^{m(m-1)/2}$ real BCs.
 - BCs can be decoded with m + 1 measurements.

• For $\mathbf{P} \in \mathrm{GL}(m)$, $\mathbf{P}^{-\mathrm{t}}$ denotes the inverse transpose.

- For $\mathbf{P} \in GL(m)$, \mathbf{P}^{-t} denotes the inverse transpose.
- Define a unitary matrix $\mathbf{U}_{\mathbf{P},\mathbf{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{P},\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{2^{r}}} i^{(\mathbf{P}^{-1}\mathbf{a})^{\mathrm{t}}\mathbf{S}(\mathbf{P}^{-1}\mathbf{a}) + 2\mathbf{b}^{\mathrm{t}}(\mathbf{P}^{-1}\mathbf{a}) \mod 4} \cdot f(\mathbf{b},\mathbf{P}^{-1}\mathbf{a},r),$$

where

$$f(\mathbf{x},\mathbf{y},r) = \prod_{i=r+1}^m (1+x_i+y_i).$$

- For $\mathbf{P} \in GL(m)$, \mathbf{P}^{-t} denotes the inverse transpose.
- Define a unitary matrix $\mathbf{U}_{\mathbf{P},\mathbf{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{P},\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{2^r}} i^{(\mathbf{P}^{-1}\mathbf{a})^{\mathrm{t}}\mathbf{S}(\mathbf{P}^{-1}\mathbf{a}) + 2\mathbf{b}^{\mathrm{t}}(\mathbf{P}^{-1}\mathbf{a}) \mod 4} \cdot f(\mathbf{b},\mathbf{P}^{-1}\mathbf{a},r),$$

where

$$f(\mathbf{x},\mathbf{y},r) = \prod_{i=r+1}^m (1+x_i+y_i).$$

• A binary subspace chirp (BSSC) is a column U_{P,S,b}.

- For $\mathbf{P} \in \mathrm{GL}(m)$, $\mathbf{P}^{-\mathrm{t}}$ denotes the inverse transpose.
- Define a unitary matrix $\mathbf{U}_{\mathbf{P},\mathbf{S}} \in \mathbb{C}^{N \times N}$ as

$$\mathbf{U}_{\mathbf{P},\mathbf{S}}(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{2^r}} i^{(\mathbf{P}^{-1}\mathbf{a})^{\mathrm{t}}\mathbf{S}(\mathbf{P}^{-1}\mathbf{a}) + 2\mathbf{b}^{\mathrm{t}}(\mathbf{P}^{-1}\mathbf{a}) \mod 4} \cdot f(\mathbf{b},\mathbf{P}^{-1}\mathbf{a},r),$$

where

$$f(\mathbf{x},\mathbf{y},r) = \prod_{i=r+1}^m (1+x_i+y_i).$$

- A binary subspace chirp (BSSC) is a column **U**_{P,S,b}.
- Note: Not all choices of P, S give different BSSCs.

Parametrization of BSSCs

Theorem

A rank *r* BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \text{Sym}(r)$.

Parametrization of BSSCs

Theorem

A rank r BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \text{Sym}(r)$.

Write H = cs (H_I) where H_I is in CREF and I is the set of pivots. Then put

$$\mathbf{P} = \mathbf{P}_H = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}.$$

Parametrization of BSSCs

Theorem

A rank r BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \text{Sym}(r)$.

Write H = cs (H_I) where H_I is in CREF and I is the set of pivots. Then put

$$\mathbf{P} = \mathbf{P}_{H} = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}.$$

• Note: $\mathbf{P}^{-t} = \begin{bmatrix} \mathbf{I}_{\mathcal{I}} & \widetilde{\mathbf{H}_{\mathcal{I}}} \end{bmatrix}$, where $(\mathbf{H}_{\mathcal{I}})^{t}\widetilde{\mathbf{H}_{\mathcal{I}}} = 0$.

Theorem

A rank r BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \operatorname{Sym}(r)$.

Write H = cs (H_I) where H_I is in CREF and I is the set of pivots. Then put

$$\mathbf{P} = \mathbf{P}_H = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}.$$

- Note: $\mathbf{P}^{-t} = \begin{bmatrix} \mathbf{I}_{\mathcal{I}} & \widetilde{\mathbf{H}_{\mathcal{I}}} \end{bmatrix}$, where $(\mathbf{H}_{\mathcal{I}})^t \widetilde{\mathbf{H}_{\mathcal{I}}} = 0$.
- Sym(r) is embedded in Sym(m) as the upper-left block.

Theorem

A rank r BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \text{Sym}(r)$.

Write H = cs (H_I) where H_I is in CREF and I is the set of pivots. Then put

$$\mathbf{P} = \mathbf{P}_H = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}.$$

- Note: $\mathbf{P}^{-t} = \begin{bmatrix} \mathbf{I}_{\mathcal{I}} & \widetilde{\mathbf{H}_{\mathcal{I}}} \end{bmatrix}$, where $(\mathbf{H}_{\mathcal{I}})^{t}\widetilde{\mathbf{H}_{\mathcal{I}}} = 0$.
- Sym(r) is embedded in Sym(m) as the upper-left block.
- The total number of BSSCs is

$$2^{m} \cdot \sum_{r=0}^{m} 2^{r(r+1)/2} \binom{m}{r}_{2} = 2^{m} \cdot \prod_{r=1}^{m} (2^{r}+1).$$

Theorem

A rank r BSSC is characterized by $H \in \mathcal{G}(m, r)$ and $\mathbf{S}_r \in \text{Sym}(r)$.

Write H = cs (H_I) where H_I is in CREF and I is the set of pivots. Then put

$$\mathbf{P} = \mathbf{P}_H = \begin{bmatrix} \mathbf{H}_{\mathcal{I}} & \mathbf{I}_{\widetilde{\mathcal{I}}} \end{bmatrix}.$$

- Note: $\mathbf{P}^{-t} = \begin{bmatrix} \mathbf{I}_{\mathcal{I}} & \widetilde{\mathbf{H}_{\mathcal{I}}} \end{bmatrix}$, where $(\mathbf{H}_{\mathcal{I}})^{t}\widetilde{\mathbf{H}_{\mathcal{I}}} = 0$.
- Sym(r) is embedded in Sym(m) as the upper-left block.
- The total number of BSSCs is

$$2^{m} \cdot \sum_{r=0}^{m} 2^{r(r+1)/2} \binom{m}{r}_{2} = 2^{m} \cdot \prod_{r=1}^{m} (2^{r}+1).$$

• $|\mathsf{BSSC}|/|\mathsf{BC}| \rightarrow 2.384...$

• The *m*-qubit *Heisenberg-Weyl* group is

 $\mathcal{HW}_{N} = \{i^{k} \mathbf{D}(\mathbf{x}, \mathbf{y}) \mid k = 0, 1, 2, 3, \mathbf{x}, \mathbf{y} \in \mathbb{F}_{2}^{m}\} \subset \mathbb{U}(N)$

where $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{\mathrm{t}}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

• The *m*-qubit *Heisenberg-Weyl* group is

$$\mathcal{HW}_{N} = \{i^{k} \mathbf{D}(\mathbf{x}, \mathbf{y}) \mid k = 0, 1, 2, 3, \mathbf{x}, \mathbf{y} \in \mathbb{F}_{2}^{m}\} \subset \mathbb{U}(N)$$

where $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{t}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

Theorem

(1) There are $\prod_{r=1}^{m} (2^r + 1)$ maximal abelian subgroups if \mathcal{HW}_N .

- (2) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ is the common eigenbase of a unique maximal abelian subgroup of \mathcal{HW}_N .
- (3) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ belongs to the normalizer of \mathcal{HW}_N in $\mathbb{U}(N)$, that is, *Clifford group* Cliff_N .

• The *m*-qubit *Heisenberg-Weyl* group is

$$\mathcal{HW}_{N} = \{i^{k} \mathbf{D}(\mathbf{x}, \mathbf{y}) \mid k = 0, 1, 2, 3, \mathbf{x}, \mathbf{y} \in \mathbb{F}_{2}^{m}\} \subset \mathbb{U}(N)$$

where $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{t}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

Theorem

(1) There are $\prod_{r=1}^{m} (2^r + 1)$ maximal abelian subgroups if \mathcal{HW}_N .

- (2) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ is the common eigenbase of a unique maximal abelian subgroup of \mathcal{HW}_N .
- (3) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ belongs to the normalizer of \mathcal{HW}_N in $\mathbb{U}(N)$, that is, *Clifford group* Cliff_N .

Theorem

Let **w** be a rank *r* BSSCs with on-off pattern determined by $H = cs(\mathbf{H}_{\mathcal{I}})$.

• The *m*-qubit *Heisenberg-Weyl* group is

$$\mathcal{HW}_{N} = \{i^{k} \mathbf{D}(\mathbf{x}, \mathbf{y}) \mid k = 0, 1, 2, 3, \mathbf{x}, \mathbf{y} \in \mathbb{F}_{2}^{m}\} \subset \mathbb{U}(N)$$

where $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{t}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

Theorem

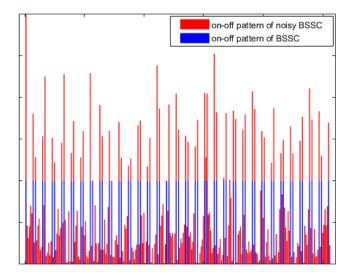
(1) There are $\prod_{r=1}^{m} (2^r + 1)$ maximal abelian subgroups if \mathcal{HW}_N .

- (2) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ is the common eigenbase of a unique maximal abelian subgroup of \mathcal{HW}_N .
- (3) $\mathbf{U}_{\mathbf{P},\mathbf{S},r}$ belongs to the normalizer of \mathcal{HW}_N in $\mathbb{U}(N)$, that is, *Clifford group* Cliff_N .

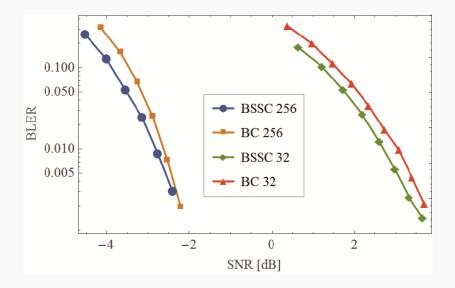
Theorem

Let **w** be a rank *r* BSSCs with on-off pattern determined by $H = \operatorname{cs}(\mathbf{H}_{\mathcal{I}})$. Then $|\mathbf{w}^{\dagger}\mathbf{D}(\mathbf{0}, \mathbf{y})\mathbf{w}| \neq 0$ iff $\mathbf{y}^{t}\mathbf{H}_{\mathcal{I}} = \mathbf{0}$.

BSSC vs Noisy BSSC



Error probability of single transmission



Multi BSSCs (no noise)

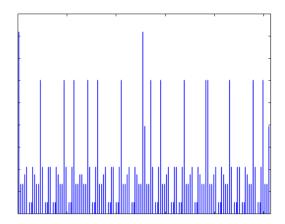
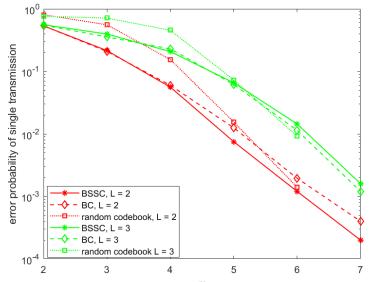


Figure 1: Combination of a rank 2, rank 3, and rank 6 BSSCs in N = 256.

Error probability of multiple transmissions



m



WORK from HOME