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 $\{u_1, \ldots, u_k\}$ given s.

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

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

- Problem: Determine $\{u_1, \ldots, u_k\}$ given s.
- Compressed Sensing Prospective:
	- $\bullet \ \Phi \in \mathbb{C}^{N \times M}, \mathbf{c} \in \mathbb{C}^{M}.$
	- Determine the support of **c** given $s = \Phi c$.
	- 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

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

- Problem: Determine $\{u_1, \ldots, u_k\}$ given s.
- Compressed Sensing Prospective:
	- $\bullet \ \Phi \in \mathbb{C}^{N \times M}, \mathbf{c} \in \mathbb{C}^{M}.$
	- Determine the support of **c** given $s = \Phi c$.
	- 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.
	- \bullet 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.
	- \bullet High complexity: Requires M measurements!
- Key idea: Reed-Muller sequences in \mathbb{C}^N can be decoded with $log(N) = m$ measurements.

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

- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

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

- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

- A binary chirp (BC) is a column $\mathbf{U}_{\mathbf{S},\mathbf{b}}$.
	- There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

- A binary chirp (BC) is a column $U_{S,h}$.
	- There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
	- $\bullet\;$ If $\mathsf S$ has zero diagonal then $\mathsf{U}_{\mathsf{S},\mathsf{b}}\in\mathbb R^N$.
- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

- A *binary chirp* (BC) is a column $U_{S,b}$.
	- There are $2^m \cdot 2^{m(m+1)/2}$ BCs.
	- $\bullet\;$ If $\mathsf S$ has zero diagonal then $\mathsf{U}_{\mathsf{S},\mathsf{b}}\in\mathbb R^N$.
	- There are $2^m \cdot 2^{m(m-1)/2}$ real BCs.
- Fix $m \in \mathbb{N}$ and $S \in \text{Sym}(m)$ binary symmetric.
- Recall $N = 2^m$. \mathbb{C}^N is indexed with \mathbb{F}_2^m (all vectors, complex or binary, are column vectors).
- \bullet Define a unitary matrix $\mathbf{U}_\mathbf{S} \in \mathbb{C}^{N \times N}$ as

$$
U_S(a,b)=\frac{1}{\sqrt{N}}\mathit{j}^{a^tSa+2b^ta \bmod 4}.
$$

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

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

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

$$
U_{P,S}(a,b)=\frac{1}{\sqrt{2^r}}\mathit{j}^{(P^{-1}a)^{t}S(P^{-1}a)+2b^{t}(P^{-1}a) \bmod 4}\cdot\mathit{f}\big(b,P^{-1}a,r\big),
$$

where

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

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

$$
U_{P,S}(a,b) = \frac{1}{\sqrt{2^r}} i^{(P^{-1}a)^{t}S(P^{-1}a) + 2b^{t}(P^{-1}a) \bmod 4} \cdot f(b, P^{-1}a, r),
$$

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 $\mathbf{U}_{\text{P.S.b.}}$

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

$$
U_{P,S}(a,b) = \frac{1}{\sqrt{2^r}} i^{(P^{-1}a)^{t}S(P^{-1}a) + 2b^{t}(P^{-1}a) \bmod 4} \cdot f(b, P^{-1}a, r),
$$

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 $\mathbf{U}_{\text{P.S.b.}}$
- 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 $\mathbf{S}_r \in \text{Sym}(r)$.

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

• Write $H = \text{cs}(\mathbf{H}_{\mathcal{I}})$ where $\mathbf{H}_{\mathcal{I}}$ is in CREF and \mathcal{I} is the set of pivots. Then put

$$
\mathsf{P} = \mathsf{P}_H = [\mathsf{H}_{\mathcal{I}} \ \mathsf{I}_{\widetilde{\mathcal{I}}}].
$$

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

• Write $H = \text{cs}(\mathbf{H}_{\mathcal{I}})$ where $\mathbf{H}_{\mathcal{I}}$ is in CREF and \mathcal{I} is the set of pivots. Then put

$$
\mathsf{P}=\mathsf{P}_{H}=[\mathsf{H}_{\mathcal{I}}\ \mathsf{I}_{\widetilde{\mathcal{I}}}].
$$

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

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

• Write $H = \text{cs}(\mathbf{H}_T)$ where \mathbf{H}_T is in CREF and $\mathcal I$ is the set of pivots. Then put

$$
\mathbf{P} = \mathbf{P}_H = [\mathbf{H}_{\mathcal{I}} \ \mathbf{I}_{\widetilde{\mathcal{I}}}].
$$

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

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

• Write $H = \text{cs}(\mathbf{H}_T)$ where \mathbf{H}_T is in CREF and $\mathcal I$ is the set of pivots. Then put

$$
\mathsf{P}=\mathsf{P}_H=\big[\mathsf{H}_{\mathcal{I}}\;\; \mathsf{I}_{\widetilde{\mathcal{I}}}\big].
$$

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

$$
2^m \cdot \sum_{r=0}^m 2^{r(r+1)/2} \binom{m}{r}_2 = 2^m \cdot \prod_{r=1}^m (2^r + 1).
$$

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

• Write $H = \text{cs}(\mathbf{H}_T)$ where \mathbf{H}_T is in CREF and $\mathcal I$ is the set of pivots. Then put

$$
\mathbf{P} = \mathbf{P}_H = [\mathbf{H}_{\mathcal{I}} \ \mathbf{I}_{\widetilde{\mathcal{I}}}].
$$

- Note: $\mathbf{P}^{-t} = [\mathbf{I}_{\mathcal{I}} \ \widetilde{\mathbf{H}_{\mathcal{I}}}],$ 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

$$
2^m \cdot \sum_{r=0}^m 2^{r(r+1)/2} \binom{m}{r}_2 = 2^m \cdot \prod_{r=1}^m (2^r + 1).
$$

• ∣BSSC∣/∣BC∣ → 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 $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{\mathrm{t}}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

Theorem

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

- (2) ${\sf U}_{{\sf P},{\sf S},r}$ 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 $\mathbf{D}(\mathbf{x}, \mathbf{y}) : \mathbf{e}_{\mathbf{v}} \longmapsto (-1)^{\mathbf{v}\mathbf{y}^{\mathrm{t}}} \mathbf{e}_{\mathbf{v}+\mathbf{x}}$.

Theorem

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

- (2) ${\sf U}_{{\sf P},{\sf S},r}$ 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 $H = \text{cs}(\mathbf{H}\tau)$.

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

Theorem

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

- (2) ${\sf U}_{{\sf P},{\sf S},r}$ 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 $H = \text{cs}(\mathbf{H}_{\mathcal{I}})$. Then $|\mathbf{w}^{\dagger} \mathbf{D}(\mathbf{0}, \mathbf{y}) \mathbf{w}| \neq 0$ iff $\mathbf{y}^{\dagger} \mathbf{H}_{\mathcal{I}} = \mathbf{0}$.

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