Binary Subspace Chirps

Tefjol Pllaha

School of Electrical Engineering
Aalto University

Universität Zürich
November 27, 2019

*Joint with R. Calderbank and O. Tirkkonen

Motivation/Applications

- Machine-type wireless communication.
  - Signature coding.
  - Unsourced random access.
- Compressive Sensing.
  - Construction of deterministic compressive sensing matrices.
  - Fast decoding/reconstruction algorithms.
- Quantum Computing.
  - Clifford Group/Hierarchy.
  - Stabilizer States.
- Coding Theory.
  - Reed-Muller codes.
  - Rank-metric codes.
    - Kerdock codes.
    - Delsarte-Goethals codes.

Binary Chirps

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

$$\mathbf{U_S}(\mathbf{a}, \mathbf{b}) = \frac{1}{\sqrt{N}} i^{\mathbf{a}^{\mathrm{t}} \mathbf{S} \mathbf{a} + 2\mathbf{b}^{\mathrm{t}} \mathbf{a} \bmod 4}.$$

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

Reconstruction Algorithm for BCs[1]

Problem: Assume you are given and unknown BC $\mathbf{w} = \mathbf{U}_{\mathbf{S},\mathbf{b}} \in \mathbb{C}^N$. How to find $\mathbf{S}, \mathbf{b}$?
Solution: "Shift and multiply" technique[1]:

- For a shift $\mathbf{e}$ compute

$$\begin{aligned}\mathbf{w}_{\mathbf{e}} &:= \left[\mathbf{w}(\mathbf{a}+\mathbf{e})\overline{\mathbf{w}(\mathbf{a})}\right]_{\mathbf{a}\in\mathbb{F}_2^m} \in \mathbb{C}^N \\ &= \frac{1}{N} i^{\mathbf{e}^{\mathrm{t}}\mathbf{S}\mathbf{e}+2\mathbf{b}^{\mathrm{t}}\mathbf{e} \bmod 4} \cdot \left[(-1)^{\mathbf{e}^{\mathrm{t}}\mathbf{S}\mathbf{a}}\right]_{\mathbf{a}\in\mathbb{F}_2^m}.\end{aligned}$$

- The Walsh-Hadamard transform is

$$\mathbf{H}_N = \frac{1}{\sqrt{N}}\left[(-1)^{\mathbf{b}^{\mathrm{t}}\mathbf{a}}\right]_{\mathbf{a},\mathbf{b}} = \frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes m}.$$

---

[1] S. D. Howard, A. R. Calderbank, and S. J. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes, 2008 42nd annual conference on information sciences and systems, 2008March, pp. 11–15.

Reconstruction Algorithm for BCs Continued

- For a basis vector $\mathbf{e}_i$ one has

$$|(\mathbf{H}_N \mathbf{w}_{\mathbf{e}_i})(\mathbf{a})| = \begin{cases} 1, & \text{if } \mathbf{a} = \mathbf{S}\mathbf{e}_i, \\ 0, & \text{else.} \end{cases}$$

- After m shifts one recovers $\mathbf{S}$.
- To recover $\mathbf{b}$ one computes

$$[\mathbf{w}(\mathbf{a})\overline{\mathbf{U}_{\mathbf{S},\mathbf{0}}(\mathbf{a})}]_{\mathbf{a}\in\mathbb{F}_2^m},$$

and then applies $\mathbf{H}_N$.

Reconstruction Algorithm for BCs: Example

- Let $m = 3$ and consider $\mathbf{S} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ and $\mathbf{b} = \mathbf{0}$.
- Corresponding BC $\mathbf{w} = \mathbf{w}_{\mathbf{S},\mathbf{0}}$ is $+++-+---$.
- The three shifted version $\mathbf{w}_i$, and their Walsh-Hadamard transform are, the rows/columns of $\mathbf{S}$ are

$\mathbf{w}_i$	$\mathbf{H}_8\mathbf{w}_i$	$\mathbf{S}_i$
$++-+-+--$	00010000	$4 = 011$
$+-++--+-$	00000100	$6 = 101$
$+---+++-$	00000010	$7 = 110$

- Minor problems arise if $\mathbf{S}$ has equal rows/columns.
- Algorithm works even in presence of noise.

Multiple BC scenario

- **Problem:** What if you are given a linear combination of multiple BCs
$$\mathbf{w} = \sum_{l=1}^{L} c_l \mathbf{w}_l, c_l \in \mathbb{C},$$
where L is small. How to find $\mathbf{S}_l, \mathbf{b}_l$?
- **Compressive sensing prospective:** Concatenate all matrices $\mathbf{U_S}$ to a long $2^m \times 2^m \cdot 2^{m(m+1)/2}$ matrix $\mathbf{\Phi}$. Given
$$\mathbf{y} = \mathbf{\Phi x},$$
where $\mathbf{x}$ is sparse, how to find $\mathbf{x}$?

Binary Subspace Chirps

- Fix a rank $0 \le r \le m$ and $\mathbf{P} \in \mathrm{GL}(m)$.
- $\mathbf{P}^{-\mathrm{t}}$ denotes the inverse transpose.
- Define a unitary matrix $\mathbf{U}_{\mathbf{P},\mathbf{S}} \in \mathbb{C}^{N \times N}$ as

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

  where

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

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

Parametrization of BSCs

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

- Write $H = \mathrm{cs}\,(\mathbf{H}_{\mathcal{I}})$ where $\mathbf{H}_{\mathcal{I}}$ 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:** $\mathbf{P}^{-\mathrm{t}} = [\mathbf{I}_{\mathcal{I}} \;\; \widetilde{\mathbf{H}_{\mathcal{I}}}]$, where $(\mathbf{H}_{\mathcal{I}})^{\mathrm{t}}\widetilde{\mathbf{H}_{\mathcal{I}}} = 0$.
- For $\mathbf{S}_r \in \mathrm{Sym}(r)$ we will denote

$$\widetilde{\mathbf{S}_r} = \begin{bmatrix} \mathbf{S}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

Example $m = 5, r = 3$

$$\mathbf{P} = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right], \mathbf{P}^{-\mathrm{t}} = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\widetilde{\mathbf{S}}_3 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \mathbf{P}^{-\mathrm{t}}\widetilde{\mathbf{S}}_3\mathbf{P}^{-1} = \begin{bmatrix} 0 & \mathbf{0} & 1 & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 1 & \mathbf{0} & 0 & 1 & \mathbf{0} \\ 1 & \mathbf{0} & 1 & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$$

Example $m = 5, r = 1$

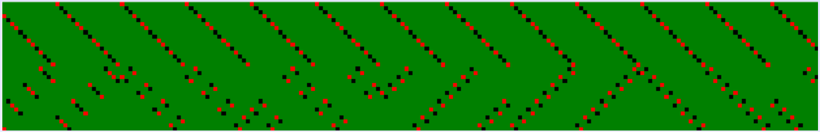

Figure: Rank 1 Real BCs: 1 Red, -1 Black, 0 Green.

Properties of BSCs

- A rank r BSC has 2^r nonzero entries.
- The nonzero entries are precisely the BCs in the respective dimensions.
- The total number of BSCs is

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

- $|\mathrm{BSC}|/|\mathrm{BC}| \to 2.384\ldots$

Reconstruction algorithm for BSC

- **Problem:** How to recover $r, H, \mathbf{S}_r$ for an unknown BSC $\mathbf{w}$?
- First recover r and H: $\mathbf{H}_N[\mathbf{w}(\mathbf{a})\overline{\mathbf{w}(\mathbf{a})}]_{\mathbf{a}} \neq 0$ iff

$$\mathbf{a} \in \left\{ \mathbf{I}_{\widetilde{\mathcal{I}}} \mathbf{b}_{m-r} + \mathbf{H}_{\mathcal{I}} \mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{F}_2^r \right\}.$$

- To recover rows $\mathbf{S}_r$ use "shift and multiply" where instead of shifting with the masis vectors $\mathbf{e}_i$ one shifts with columns of $\mathbf{H}_{\mathcal{I}}$.
- The column $\mathbf{b}$ is recovered exactly as for BCs.
- Complexity $\mathcal{O}(N \log N)$ (same as for BC reconstruction!).

Algebraic structure of BSCs

- *Pauli matrices*

$$\mathbf{I}_2, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

- m-qubit *Pauli group*

$$\mathcal{P}_m = \langle e_1 \otimes \cdots \otimes e_m \mid e_i \text{ Pauli matrix} \rangle \subset \mathbb{U}(N).$$

- The m-qubit *Clifford group* is the normalizer of $\mathcal{P}_m$ in $\mathbb{U}(N)$.
- BSCs are columns of Clifford matrices, also known as *stabilizer states*.

MRD codes

- Fix a BC $\mathbf{w}$ which is a column of $\mathbf{U_S}$. If $\mathbf{v}$ is another BC that runs though the columns of $\mathbf{U_{S'}}$, then

$$|\langle \mathbf{v} | \mathbf{w} \rangle|^2 = \begin{cases} 1/2^\ell, & 2^\ell \text{ times}, \\ 0, & 2^m - 2^\ell \text{ times}, \end{cases}$$

  where $\ell = \operatorname{rank}(\mathbf{S} + \mathbf{S'})$.
  - If $\ell = m$, $\mathbf{v}$ and $\mathbf{w}$ are called *mutually unbiased*.
- A vector space of invertible matrices contains at most 2^m matrices.
  - **Corollary:** This can be used show that there exist precisely $2^m + 1$ *mutually unbiased bases* in 2^m dimensions.
- $\mathrm{Sym}(m)$ is a disjoint union of $2^{m(m-1)/2}$ MRD (of type $[2^m, m]$) codes.

Thank You!