Space-Time Reed-Muller Codes

Alexei Ashikhmin
Bell Labs.

- Grassmannian Packings: Formulation of the Problem and Motivation
- Space-Time Reed-Muller Packings
  - Extraspecial Group and Quantum Stabilizer Codes
  - Reed-Muller Codes and Boolean Function
  - Generalization of Quantum Stabilizer Codes with the Help of Boolean Functions
- Properties of Space-Time Reed-Muller Codes
- Decoding of Space-Time Reed-Muller Codes
- Simulation Results

Joint work with A. R. Calderbank

Notation

- Q_i is an M-dimensional subspace of $\mathbb{C}^T$;
- U_i is an orthonormal basis of Q_i;
- P_i is the orthogonal projection operator on Q_i, i.e.
  - $P_i\mathbf{v} = \mathbf{v}, \mathbf{v} \in Q_i,\ P_i\mathbf{w} = 0, \mathbf{w} \perp Q_i,\ \mathrm{Tr}\,(P_i) = M$
  - P_i is Hermitian and idempotent $P_iP_i = P_i$

$$\mathbf{v} = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_T \end{pmatrix}, \quad \mathbf{v}^\dagger = (v_0^*, v_1^*, \ldots, v_T^*)$$

Grassmannian Packings

The Grassmannian space $G(M,T)$ is the set of all M-dimensional linear subspaces of the space $\mathbb{C}^T$

A packing C in $G(M,T)$ is a set of subspaces $Q_1, Q_2, \ldots, Q_L$

- $\theta_1, \ldots, \theta_t$ are principal angles between Q and Q'.
- P and P' are orthogonal projections on Q and Q' respectively.

The chordal distance between Q and Q' is

$$d(Q,Q')^2 = \sin^2\theta_1 + \ldots + \sin^2\theta_t = M - \mathrm{Tr}\,(PP')$$

Formulation of the Problem

Construct a packing $C = \{Q_1, Q_2, \ldots, Q_L\}$ such that

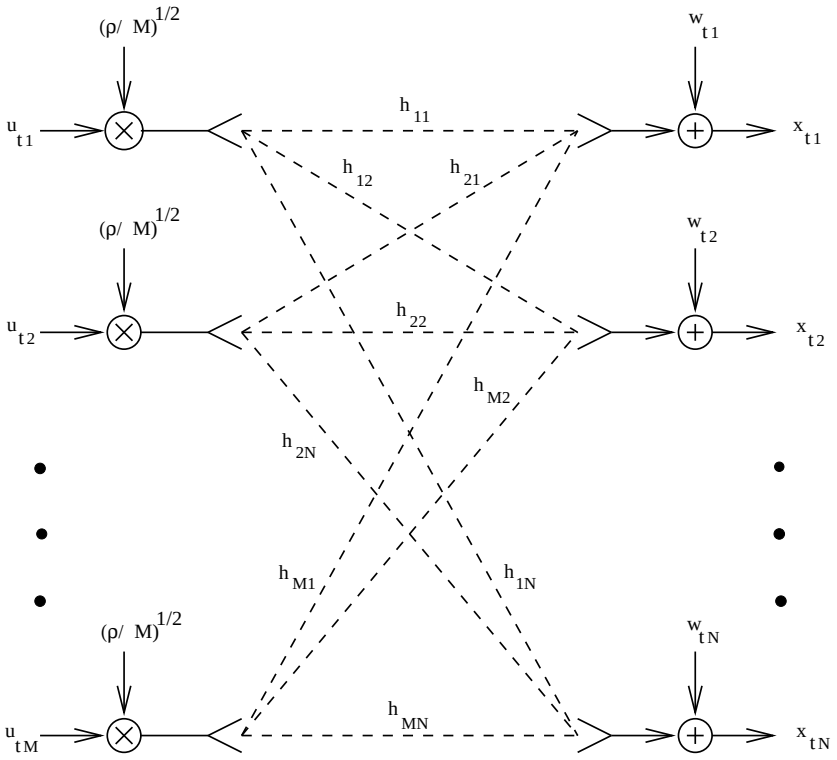
- The size $|C| = L$ is large
- The minimum chordal distance

  $$d(Q_i, Q_j)^2 = M - \mathrm{Tr}\,(P_i, P_j), Q_i, Q_j \in C$$

  is large
- C affords a simple and efficient decoding

Motivation

Noncoherent MIMO Information Transmission



U_i is an orthonormal basis of $Q_i \in C$, i.e. U_i is a $T \times M$ unitary matrix

We transmit

$$U_i = \begin{bmatrix} u_{1,1} & \cdots & u_{1,M} \\ u_{2,1} & \cdots & u_{2,M} \\ u_{3,1} & \cdots & u_{3,M} \\ \vdots & \vdots & \vdots \\ u_{T,1} & \cdots & u_{T,M} \end{bmatrix}$$

and receive

$$X = \sqrt{\frac{\rho}{M}} U_i H + W,$$

where entries of H and W are $\mathcal{CN}(0,1)$

H remains constant for T symbol period, $T \geqslant 2M$, ρ is SNR.

Maximum likelihood decoding (B. Hochwald and T. Marzetta):

$$\arg\max_i \mathrm{Tr}\,(X^\dagger U_i U_i^\dagger X) = \arg\max_i \mathrm{Tr}\,(\underbrace{U_i U_i^\dagger}_{P_i} XX^\dagger) = \arg\max_i \mathrm{Tr}\,(P_i XX^\dagger)$$

The probability of ML detection (B. Hochwald and T. Marzetta)

$$P_e = \sum_j \mathrm{Res}_{\omega=ia_j} \left\{ -\frac{1}{\omega + i/2} \prod_{m=1, d_m>0}^{M} \left[\frac{1+\rho TM}{(\rho T/M)^2 d_m^2 (\omega^2 + a_m^2)} \right]^N \right\},$$

where

$$a_m = \sqrt{\frac{1}{4} + \frac{1+\rho TM}{(\rho T/M)^2 d_m^2}},\ i = \sqrt{-1},$$

and $1 - d_i^2$ are the singular values of the matrix $U_1^\dagger U_2$

For achieving small probability of error P_e

- High SNR:
  - the rank of $U_1^\dagger U_2$ should be large
  - $\prod_j d_j$ should be large
- Low SNR: it is more important how large is

$$d(Q_1, Q_2)^2 = \sum_j d_j^2 = M - \mathsf{Tr}\,(P_1 P_2)$$

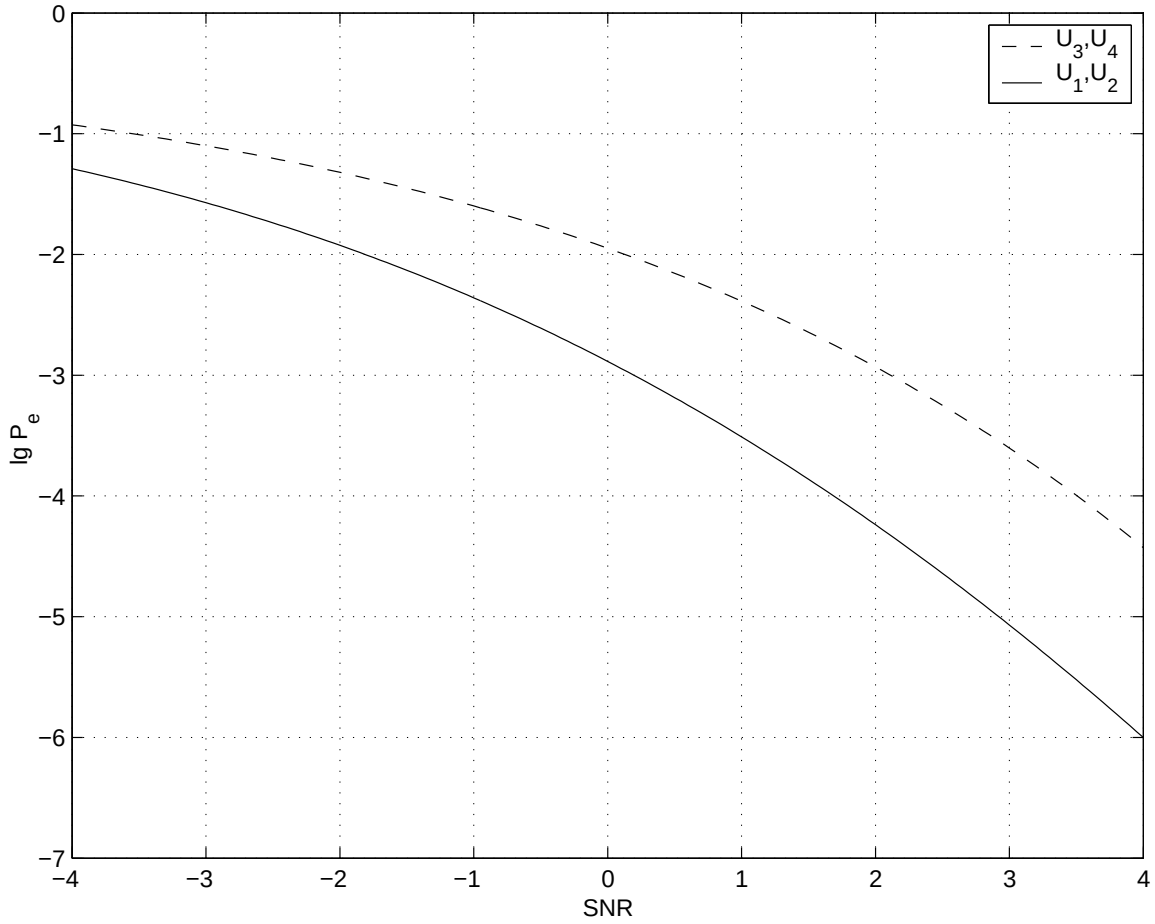
Example 1 $M = N = 8,\ T = 16$

- U_1 *and* U_2*:* $d_1 = 1, d_2 = 1, d_3 = 0, \ldots, d_8 = 0$

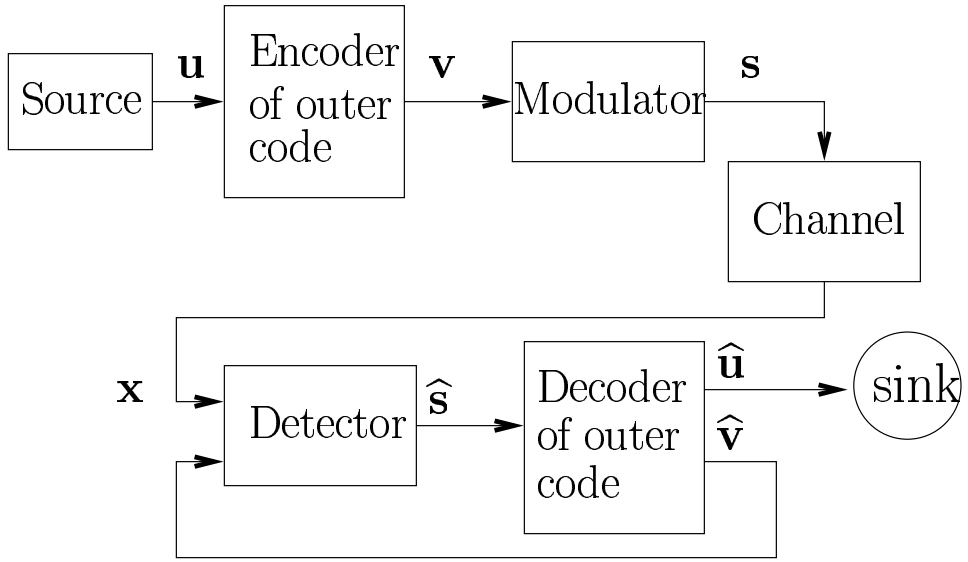
$$\mathsf{rank}\,(U_1 U_2) = 6, \quad \prod_j d_j = 0, \quad \sum_j d_j^2 = 2$$

- U_3 *and* U_4*:* $d_i = 1/8$

$$\mathsf{rank}\,(U_1 U_2) = 8, \quad \prod_j d_j = (1/8)^8, \quad \sum_j d_j^2 = 1/8$$


0
−1
−2
−3
−4
−5
−6
−7
lg P_e
−4
−3
−2
−1
0
1
2
3
4
SNR
U_3,U_4
U_1,U_2

Concatenation of a Space-Time Code with an outer code



If $I(s, \hat{s})$ is close to the channel capacity then a specifically designed LDPC code allows operate near the capacity

S. ten Brink, G. Kramer, A. Ashikhmin, "Detection and Decoding of Multi-Antenna Signals with Low-Density Parity-Check Codes," *IEEE Trans. on Comm. Theory,* 2004.

Space-Time Reed-Muller Codes

We are going to use technique from the theory of quantum error correcting codes

Def. 1 *An* $((n, K))$ *quantum code is a* K*-dimensional subspace of* $\mathbb{C}^{2^n}$.

Let us construct many quantum codes and use then to form a Grassmannian packing.

Extraspecial Group

Pauli matrices:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}.$$

The extraspecial group:

$$\mathcal{E}_2 = \{\xi I_2, \xi\sigma_x, \xi\sigma_z, \xi\sigma_y\},\ \xi \in \{\pm 1, \pm i\}, i = \sqrt{-1},\ |\mathcal{E}_2| = 16$$

The center of the group $\mathcal{Z} = \{I_2, -I_2, iI_2, -iI_2\}$

$\overline{\mathcal{E}} = \mathcal{E}/\mathcal{Z}$ is isomorphic to $\mathbb{F}_2^2$

$$\begin{aligned} \xi I_2 &\longleftrightarrow 00 \\ \xi\sigma_x &\longleftrightarrow 10 \\ \xi\sigma_z &\longleftrightarrow 01 \\ \xi\sigma_y &\longleftrightarrow 11 \end{aligned}$$

$\mathbf{v} = (a_1, \ldots, a_m | b_1, \ldots, b_m) \Rightarrow E_{\mathbf{v}} = e_1 \otimes \ldots \otimes e_n$, where

$$e_i = \begin{cases} I_2, & a_i = 0, b_i = 0, \\ \sigma_x, & a_i = 1, b_i = 0, \\ \sigma_z, & a_i = 0, b_i = 1, \\ \sigma_y, & a_i = 1, b_i = 1, \end{cases}$$

$$\mathbf{v} = (1, 0, |0, 0) \Rightarrow E_{\mathbf{v}} = \sigma_x \otimes I_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Lemma 1 *The operator*

$$P_{\mathbf{v}} = \frac{1}{2} \left(I_{2^m} + \lambda E_{\mathbf{v}} \right), \lambda = \pm 1,$$

is an orthogonal projection and

$$\dim(Q_{\mathbf{v}}) = \mathrm{Tr}\left(P_{\mathbf{v}}\right) = 2^{m-1}.$$

Def. 2 *Vectors* $(\mathbf{a}|\mathbf{b})$ *and* $(\mathbf{a}'|\mathbf{b}')$ *are called orthogonal if the symplectic inner product*

$$(\mathbf{a}|\mathbf{b}) * (\mathbf{a}'|\mathbf{b}') \equiv \mathbf{a}\cdot\mathbf{b}' \oplus \mathbf{b}\cdot\mathbf{a}' = 0; \;\; (\; \textit{here}\; \mathbf{a}\cdot\mathbf{b}' = \sum_i a_i b_i' \;)$$

$\mathcal{G} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{m-k}\}$ is a set of pairwise orthogonal and independent vectors, i.e.

$$\mathbf{v}_i * \mathbf{v}_j = 0, \mathbf{v}_i \in \mathbb{F}_2^{2m}$$

Def. 3 *A quantum stabilizer code is a subspace with the orthogonal projection operator*

$$P = P_{\mathbf{v}_1} \cdot \ldots \cdot P_{\mathbf{v}_{m-k}}, \;\; \mathrm{Tr}\,(P) = 2^k.$$

Binary Reed-Muller Codes

$f(x_1, x_2, x_3) = x_1x_2 \oplus x_1 \oplus x_3$ is a Boolean function of degree 2

We associate with the Boolean function the vector with 2^3 entries

$$\begin{array}{rcccccccc} x_3: & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ x_2: & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ x_1: & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ f: & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1, \end{array} \quad \mathrm{wt}(f) = 4$$

Def. 4 *The r-th order Reed-Muller code $RM(r, m)$ is the set of vectors corresponding to Boolean functions $f(x_1, \ldots, x_m)$ of degree at most r.*

For two commuting projector operators P and P' we define the operation

$$P \oplus P' \equiv P + P' - 2PP'.$$

Lemma 2 *For commuting projection operators the operation* $\oplus$ *is commutative and associative.*

Generalization of Boolean Functions

- $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{F}_2^{2m}$ is a set of orthogonal vectors
- $P_{\mathbf{v}_i} = \frac{1}{2}(I_{2^m} + \lambda E_{\mathbf{v}_i}), \lambda = \pm 1$
- For a Boolean function $f(x_1, \ldots, x_m)$ we define $f(P_1, \ldots, P_m)$, where

$$\begin{array}{rll} x_i x_j & \text{is replaced by} & P_{\mathbf{v}_i} P_{\mathbf{v}_j} \\ x_i \oplus x_j & \text{is replaced by} & P_{\mathbf{v}_i} \oplus P_{\mathbf{v}_j} \end{array}$$

Example 2

$$\mathbf{v}_1 = (1,0,0|0,1,0), \mathbf{v}_2 = (0,1,1|1,1,0), \mathbf{v}_3 = (0,0,1|0,1,1)$$

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 \oplus x_3$$

$$f(P_{\mathbf{v}_1}, P_{\mathbf{v}_2}, P_{\mathbf{v}_3}) = P_{\mathbf{v}_1} P_{\mathbf{v}_2} \oplus P_{\mathbf{v}_1} \oplus P_{\mathbf{v}_3}$$

$$= \frac{1}{4} \begin{bmatrix} 2 & i & -1 & 0 & 0 & -i & 1 & 0 \\ -i & 2 & 0 & 1 & i & 0 & 0 & -1 \\ -1 & 0 & 2 & -i & -1 & 0 & 0 & -i \\ 0 & 1 & i & 2 & 0 & 1 & i & 0 \\ 0 & -i & -1 & 0 & 2 & i & 1 & 0 \\ i & 0 & 0 & 1 & -i & 2 & 0 & -1 \\ 1 & 0 & 0 & -i & 1 & 0 & 2 & -i \\ 0 & -1 & i & 0 & 0 & -1 & i & 2 \end{bmatrix}.$$

Theorem 3 *The operator*

$$P_f = f(P_{\mathbf{v}_1}, \ldots, P_{\mathbf{v}_m})$$

is an orthogonal projection on a subspace of dimension

$$\mathsf{Tr}\,(P_f) = \mathsf{wt}\,(f).$$

($\mathsf{wt}\,(f)$ *is the Hamming weight of the vector* f*)*

Construction of ST-$RM(r, m, M)$ space-time codes

- $\mathcal{S}_m$ is the set of all sets of m pairwise orthogonal linearly independent binary vectors;
- Take all Boolean functions $f(x_1, \ldots, x_m)$:

$$\deg f \leqslant r, \mathsf{wt}\,(f) = M$$

- For all $\mathcal{G} = (\mathbf{v}_1, \ldots, \mathbf{v}_m) \in \mathcal{S}_m$ compute P_f;
- The projectors P_f define subspaces of dimension M in $\mathbb{C}^{2^m}$, i.e. $T = 2^m$; these subspaces form ST-$RM(r, m, M)$.

Properties of $ST\text{-}RM(r, m, M)$

The minimum distance of the binary Reed-Muller code $RM(r, m)$ is

$$d = 2^{m-r}.$$

We can prove similar result for space-time Reed-Muller codes:

Theorem 4 *If* $Q_i, Q_j \in ST\text{-}RM(r, m, M)$ *then*

$$d(Q_1, Q_2)^2 = M - \mathsf{Tr}\,(P_i, P_j) \geqslant 2^{m-r-1}.$$

Theorem 5 *$U_i \in ST\text{-}RM(r,m)$ can be chosen such that their entries belong to $\{0,1,-1,i,-i\}$.*
In other words U_i can be transmitted with the help of QPSK modulation.

Example 3 *$ST\text{-}RM(1,2,2)$, i.e. $T = 2^2 = 4, M = 2$. Let $f(x_1,x_2) = x_1$ and $\mathbf{v}_1 = (0,1|1,1)$. Then*

$$P_{\mathbf{v}_1} = \frac{1}{2}\begin{bmatrix} 1 & i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & i & 1 \end{bmatrix}.$$

An orthonormal basis of the corresponding subspace

$$\mathbf{u}_1^\top = \frac{1}{2}(1,-i,1,i),\ \mathbf{u}_2^\top = \frac{1}{2}(1,-i,-1,-i).$$

If $\mathbf{v} \in RM(r,m)$ then wt $(\mathbf{v})$ is even and

$$\text{wt}\,(\mathbf{v}) \in [2^{m-r}, 2^m - 2^{m-r}]$$

Thus we can choose the number of transmitting antennas

$$2^{m-r} \leqslant M \leqslant 2^m - 2^{m-r},\ M \text{ is even}$$

Decoding

$$\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{2^{2m}-1}$$

are all vectors from $\mathbb{F}_2^{2m}$ ordered lexicographically

For any $P \in ST\text{-}RM(r,m)$ we form the vector

$$\mathbf{w} = (w_0, \ldots, w_{2^{2m}-1}),\ w_i = \mathrm{Tr}\,(E_{\mathbf{v}_i} P)$$

Let $H_{2^{2m}}$ be the Hadamard matrix of order 2^{2m} given by

$$H_{2^{2m}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Theorem 6

$$\mathbf{z} = \frac{1}{2^m} H_{2^{2m}} \mathbf{w} \in RM(r, 2m).$$

Example 4 $f(x_1, x_2) = x_1$ *and* $\mathbf{v}_1 = (0, 1|1, 1)$. *Then*

$$P_{\mathbf{v}_1} = \frac{1}{2}\begin{bmatrix} 1 & i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & i & 1 \end{bmatrix}$$

$$\mathbf{u}_1^\top = \frac{1}{2}(1, -i, 1, i),\ \mathbf{u}_2^\top = \frac{1}{2}(1, -i, -1, -i).$$

If there are no errors

$$\begin{aligned} \mathbf{w} &= (2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0),\ \textit{and} \\ \mathbf{z} &= (1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0) \in RM(1,4). \end{aligned}$$

If there are channel errors $\mathbf{z}$ *will be a corrupted version of a codeword of* $RM(1,4)$.

We transmit U_i ($P_i = U_i^\dagger U_i$) and receive

$$X = \sqrt{\frac{\rho}{M}} U_i H + W,$$

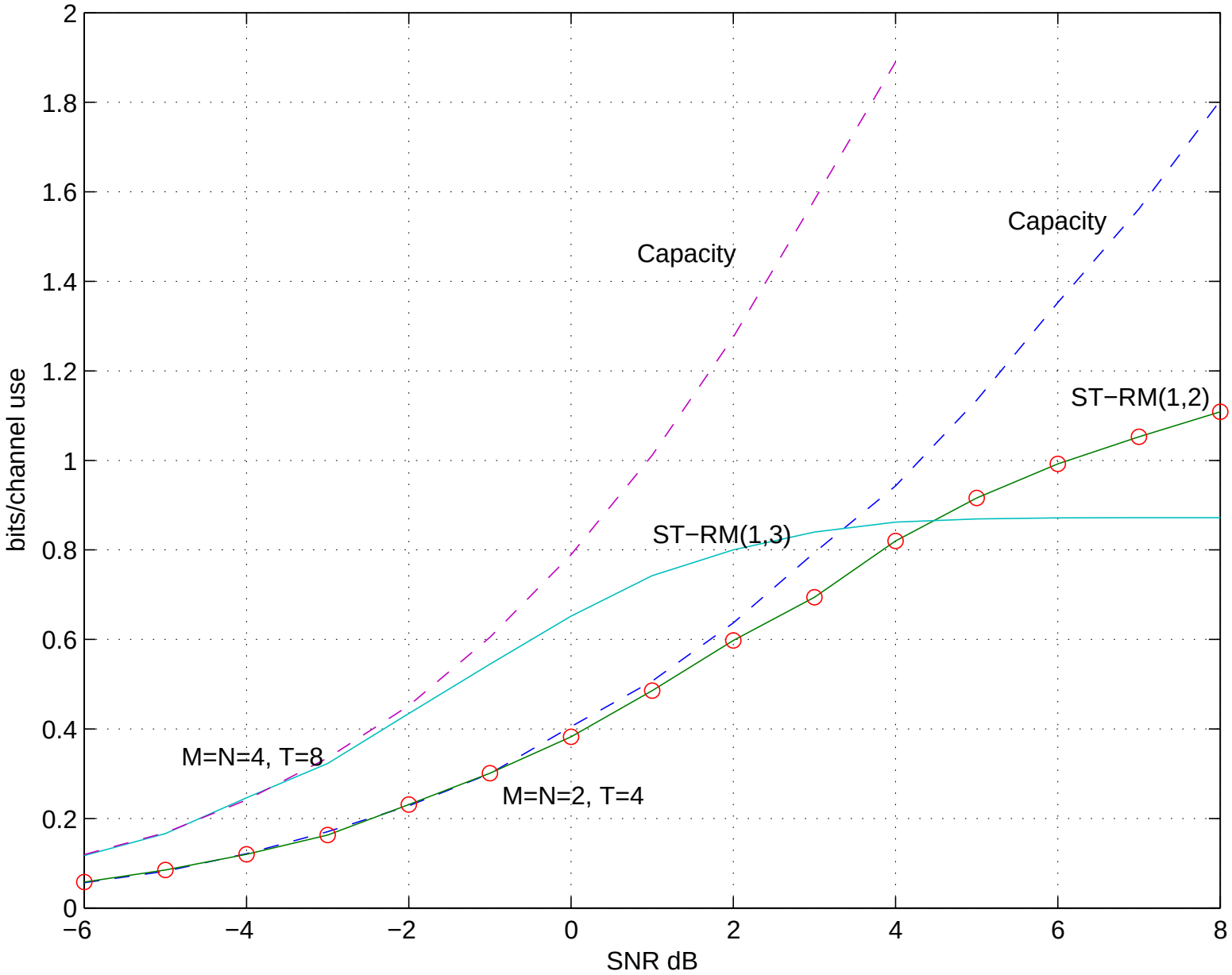
Decoding of $ST\text{-}RM(r,m)$

1. Compute $P_X = \mathbf{X}\mathbf{X}^\dagger$;
2. Compute $\mathbf{w} = (w_0, w_1, \ldots, w_{2^{2m}-1})^\top$, where $w_i = \mathsf{Tr}\,(E_{\mathbf{v}_i} P_X)$;
3. Compute $\mathbf{z} = \frac{1}{2^m} H_{2^{2m}} \mathbf{w}$;
4. Decode $\mathbf{z}$ with the help of any decoder of $RM(r, 2m)$.

There are many efficient decoding algorithms of the Reed-Muller codes, e.g.

I. Dumer, "Recursive decoding and its performance for low-rate Reed-Muller codes", *IEEE Trans. on Inform. Theory*, **50**, (2004)

A. Ashikhmin and S. Litsyn, "Fast MAP Decoding of First Order Reed-Muller and Hamming Codes", *IEEE Trans. on Inform.Theory,* **50**, (2004)


bits/channel use
SNR dB
Capacity
Capacity
ST−RM(1,2)
ST−RM(1,3)
M=N=4, T=8
M=N=2, T=4
2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
−6
−4
−2
0
2
4
6
8

$$R = \frac{\log_2 |C|}{T}$$

$$M = 2,\ T = 4$$

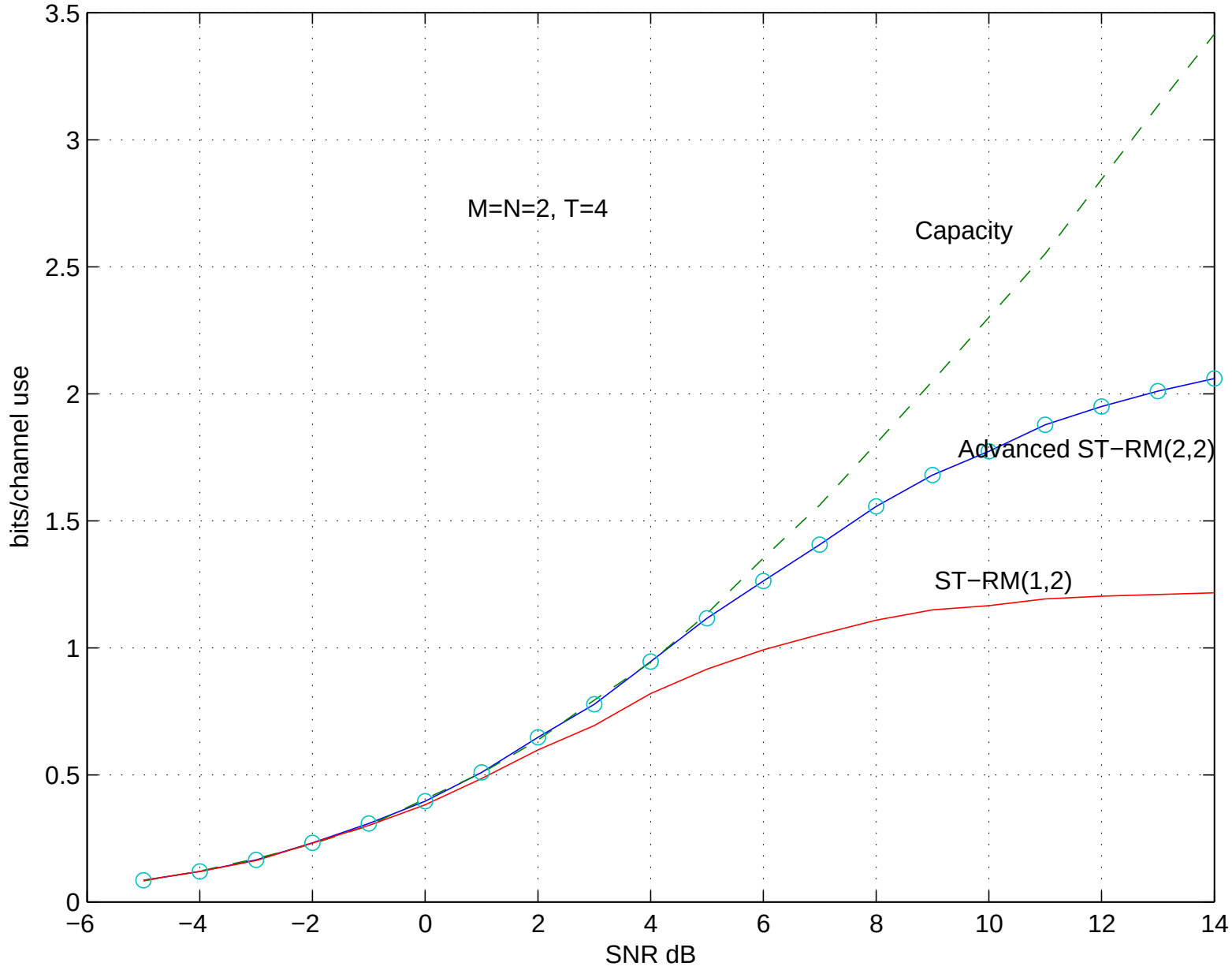
$$r = 1,\ \ |C| = 30,\quad d(Q_i, Q_j)^2 \geqslant 2,\ \ R \approx 1.23$$
$$r = 2,\ \ |C| = 390,\ \ d(Q_i, Q_j)^2 \geqslant 1,\ \ R \approx 2.15$$

$$M = 4,\ T = 8$$

$$r = 1,\ \ |C| = 126,\quad d(Q_i, Q_j)^2 \geqslant 4,\ \ R \approx 0.87$$
$$r = 2,\ \ |C| = 866880,\ \ d(Q_i, Q_j)^2 \geqslant 2,\ \ R \approx 2.46$$

$$M = 8,\ T = 16$$

$$r = 1,\quad d(Q_i, Q_j)^2 \geqslant 8,\ \ R \approx 0.87$$
$$r = 2,\quad d(Q_i, Q_j)^2 \geqslant 4,\ \ R \approx 2.46$$


M=N=2, T=4
Capacity
Advanced ST−RM(2,2)
ST−RM(1,2)
bits/channel use
SNR dB
3.5
3
2.5
2
1.5
1
0.5
0
−6
−4
−2
0
2
4
6
8
10
12
14