Multidimensional Reed-Muller Codes as Grassamannian Packings

Alexei Ashikhmin

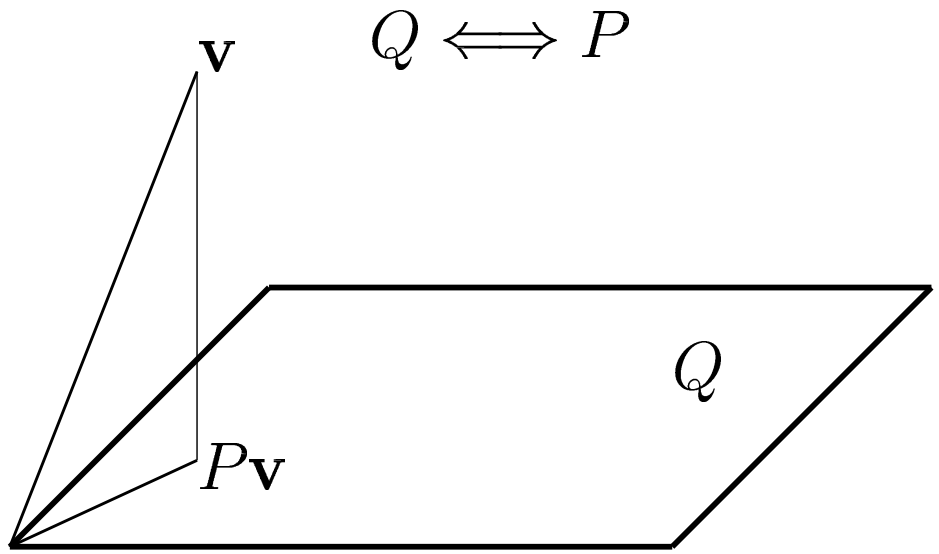
Bell Labs.

- Grassmannian Packings: Formulation of the Problem
- Application to Noncoherent MIMO Transmission
- Construction Based on a Generalization of Boolean Functions
- Construction Derived from Representation Theory
- Simulation Results for Noncoherent MIMO Channel

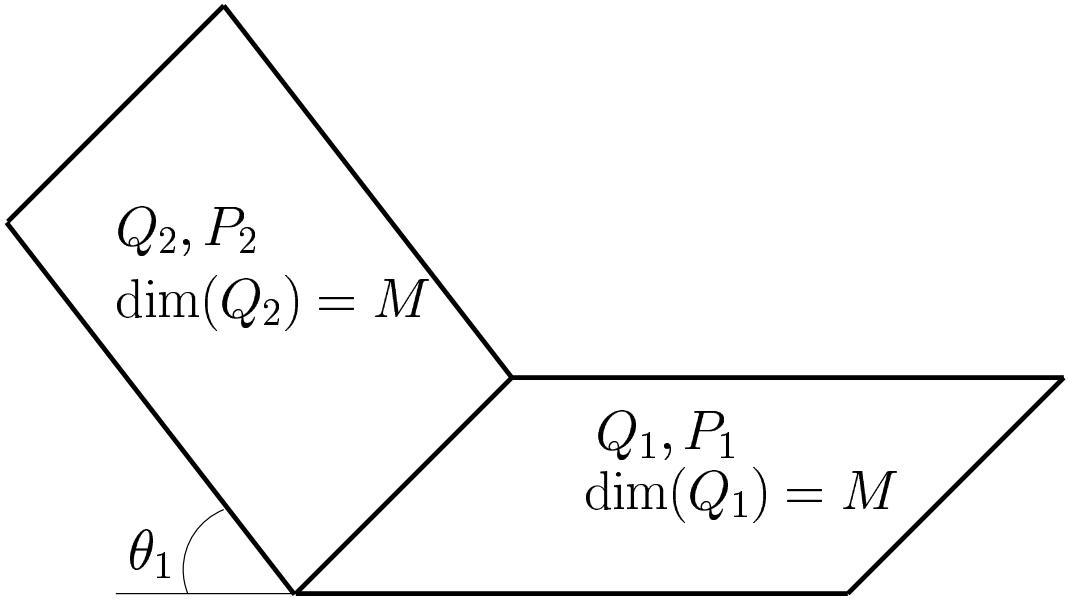
Joint work with A. R. Calderbank and W. Kevlin

Orthogonal Projectors

- Q is a subspace of $\mathbb{C}^T$
- Q can be defined with the help of its orthogonal projector P
- $\dim(Q) = \mathrm{Tr}\,(P)$
- P is an orthogonal projector iff $P^\dagger = P,\ PP = P$



The Chordal Distance



$$\text{dist}\,(Q_1, Q_2) = \text{dist}\,(P_1, P_2) = M - \text{Tr}\,(P_1 P_2) = \sum_{i=1}^{M} \sin^2(\theta_i)$$

- θ_i are principal angles

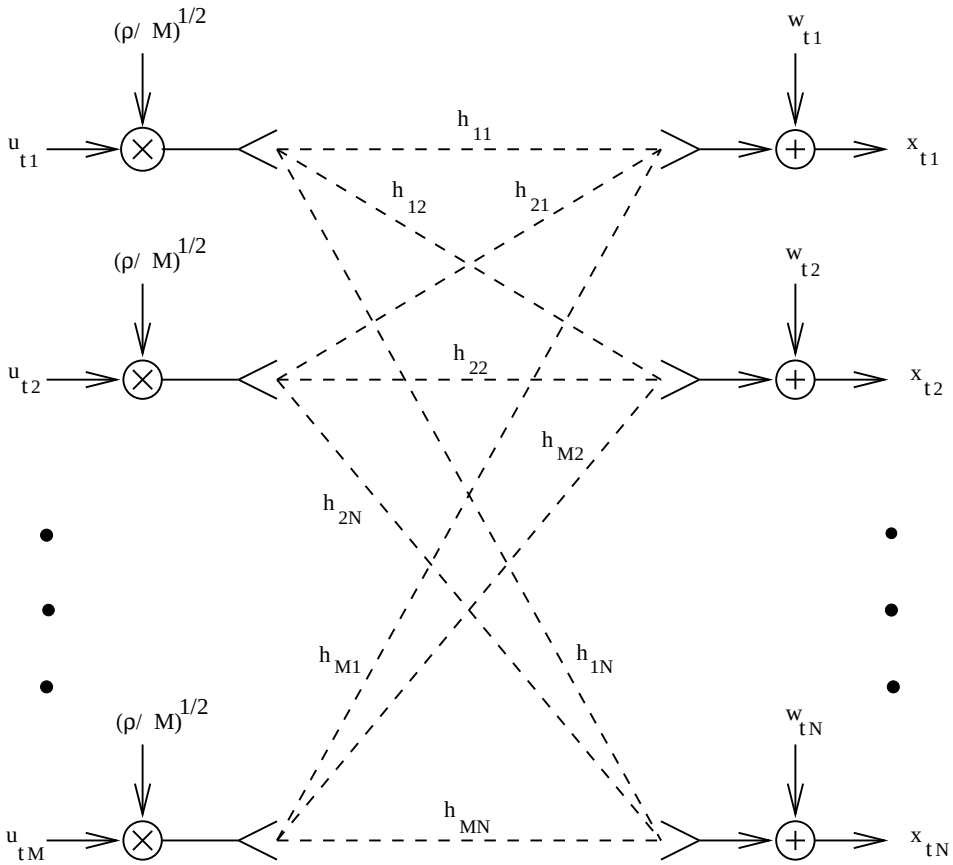
- In this example (assuming $M = 2$) we have : $\theta_1, \theta_2 = 0$

Grassmannian Packings

Construct a set $C = \{P_1, P_2, \ldots, P_L\}$ such that

- $\mathrm{Tr}\,(P_i) = M, i = 1, \ldots, L$
- The number of projectors (subspaces) L is large
- $\mathrm{dist}\,(P_i, P_j) = M - \mathrm{Tr}\,(P_i P_j)$ is large for all $1 \leqslant i < j \leqslant L$
- C affords a simple and efficient decoding

Applications to Noncoherent MIMO Channel



$$C = \{P_1, P_2, \ldots, P_L\}$$

To transmit a message $j, 1 \leqslant j \leqslant L$, we

- take $P_j \Rightarrow Q_j \Rightarrow$ an orthonoramal basis U_j of Q_j

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

- transmit rows of U_j with the help of M antennas
- T is the coherence interval, T is short, typically $T = 2M$

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

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

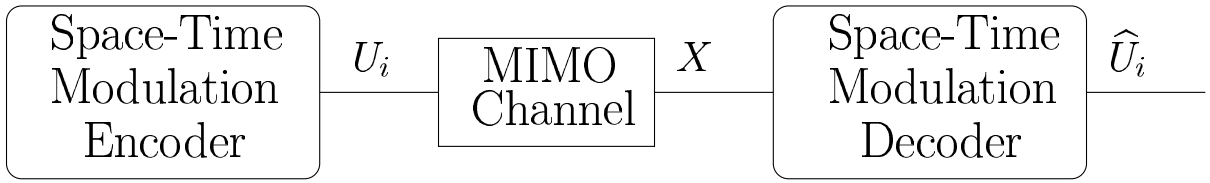
- Typically we optimize space-time codes with respect to

$$\text{dist} = \prod_{i=1}^{m} \sin^2 \theta_i$$

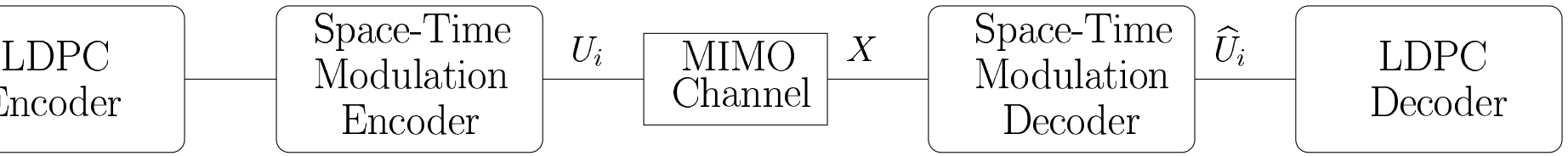
  Wrong criterion

- We optimize them with respect to

$$\text{dist} = M - \text{Tr}\,(P_i P_j) = \sum_{i=1}^{M} \sin^2 \theta_i$$



How close is $I(U_i; \widehat{U}_i)$ to the MIMO channel capacity C?



Constructions

Pauli matrices:

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

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

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

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

$$\mathbf{v} = (a_1, \ldots, a_m | b_1, \ldots, b_m) \Rightarrow E_{\mathbf{v}} \Rightarrow P_{\mathbf{v}} = \frac{1}{2} \left(I_{2^m} + \lambda E_{\mathbf{v}} \right), \lambda = \pm 1,$$

Lemma 1 *The operator $P_{\mathbf{v}}$ is an orthogonal projection and*

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

For commuting operators P and P' we define the operation

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

Lemma 2 *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 (with respect to the symplectic inner product)

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

- For a Boolean function $f(x_1, \ldots, x_m)$ we define $f(P_{\mathbf{v}_1}, \ldots, P_{\mathbf{v}_m})$, where

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

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

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

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

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

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

Example 1

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

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

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

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

$\mathsf{Tr}\,(P_f) = \mathsf{wt}\,(f) = 4,\; P_f P_f = P_f,\; P_f^\dagger = P_f$

Construction of $ST\text{-}RM(r, m, M)$ space-time codes

- Take all sets of m orthogonal binary vectors $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_m} \in \mathbb{F}_2^{2m}$
- $\mathbf{v}_{i_1} \Rightarrow P_{\mathbf{v}_{i_1}}, \ldots, \mathbf{v}_{i_m} \Rightarrow P_{\mathbf{v}_{i_m}}$
- Take all Boolean functions $f(x_1, \ldots, x_m)$:

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

- Projectors $P_f(\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_m}) = f(P_{\mathbf{v}_{i_1}}, \ldots, P_{\mathbf{v}_{i_m}})$ form space-time Reed-Muller codes $ST\text{-}RM(r, m, M)$

- If $P, P' \in ST\text{-}RM(r, m, M)$ then

$$\mathsf{dist}\,(P, P') = M - \mathsf{Tr}\,(PP') \geqslant 2^{m-r-1}$$

Construction Derived from Representation Theory

Pauli matrices:

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

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

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

Let $\mathbf{v}$ be the binary representation of j

To shorten notation we write E_j instead of $E_{\mathbf{v}}$

Operators $\alpha E_{\mathbf{v}}, \alpha = \pm 1, \pm i$, form the extraspecial group

$m = 2$

linear code															
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
E_0	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}	E_{11}	E_{12}	E_{13}	E_{14}	E_{15}
Abelian Group															

its linear characters $\lambda_t(E_j)$ are

	E_0	E_1	E_2	E_3
λ_0 :	1	1	1	1
λ_1 :	1	-1	1	-1
λ_2 :	1	1	-1	-1
λ_3 :	1	-1	-1	1

Representation theory: $P = \frac{1}{4}\sum_{j=0}^{3} \overline{\lambda}_t(E_j)E_j$ is a projector

coset of a linear code

0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
E_0	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}	E_{11}	E_{12}	E_{13}	E_{14}	E_{15}

Can we find a function $f(E_j) \rightarrow \{1, -1\}$ so that

$$P = \frac{1}{2} I_4 + \frac{1}{4} \sum_{j \in \text{coset}} f(E_j) E_j$$

is a projector

Answer - $f(\cdot)$ should be a bent function

Def. 1 *$f(\cdot)$ is a bent function if all coefficients of its Hadamard transform have the same absolute value.*

Example:

$$\begin{pmatrix} 2 \\ -2 \\ 2 \\ 2 \end{pmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

Hence

$$P = \frac{1}{2} I_4 + \frac{1}{4}(E_4 + E_5 - E_6 + E_7)$$

is a projector

We call these packing G-$RM(2, m)$ codes

Decoding

$$\begin{aligned} \mathbf{v}_0 = (0,0,\ldots,0) &\Rightarrow E_{\mathbf{v}_0} \\ \mathbf{v}_1 = (1,0,\ldots,0) &\Rightarrow E_{\mathbf{v}_1} \\ \ldots\ldots\ldots\ldots\ldots &\ldots \quad \ldots \\ \mathbf{v}_{2^{2m}-1} = (1,1,\ldots,1) &\Rightarrow E_{\mathbf{v}_{2^{2m}-1}} \end{aligned}$$

For any $P \in ST\text{-}RM(r,m)$ or $P \in G\text{-}RM(2,m)$ 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

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

Theorem 4

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

We transmit U_i ($P_i = U_i U_i^\dagger$) 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 $RM(r, 2m)$.

The complexity of decoding is about $2T^2 \log_2 T + M \cdot T^2$

Example 2 $f(x_1, x_2) = x_1$ *and* $\mathbf{v}_1 = (0, 1|1, 1)$. *Then*

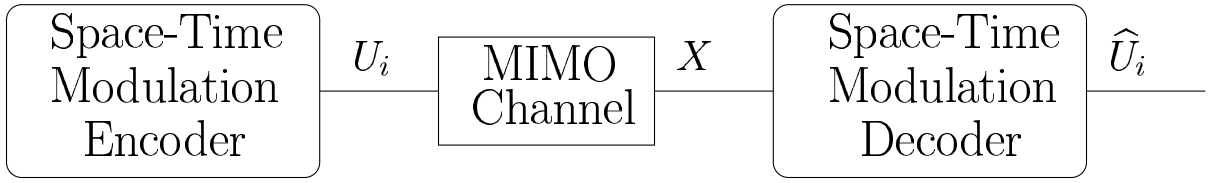
$$P_{\mathbf{v}_1} = \frac{1}{2}\begin{bmatrix} 1 & i & 0 & 0 \\ -i & 1 & 0 & 0 \\ 0 & 0 & 1 & -i \\ 0 & 0 & i & 1 \end{bmatrix}$$

If there are no errors

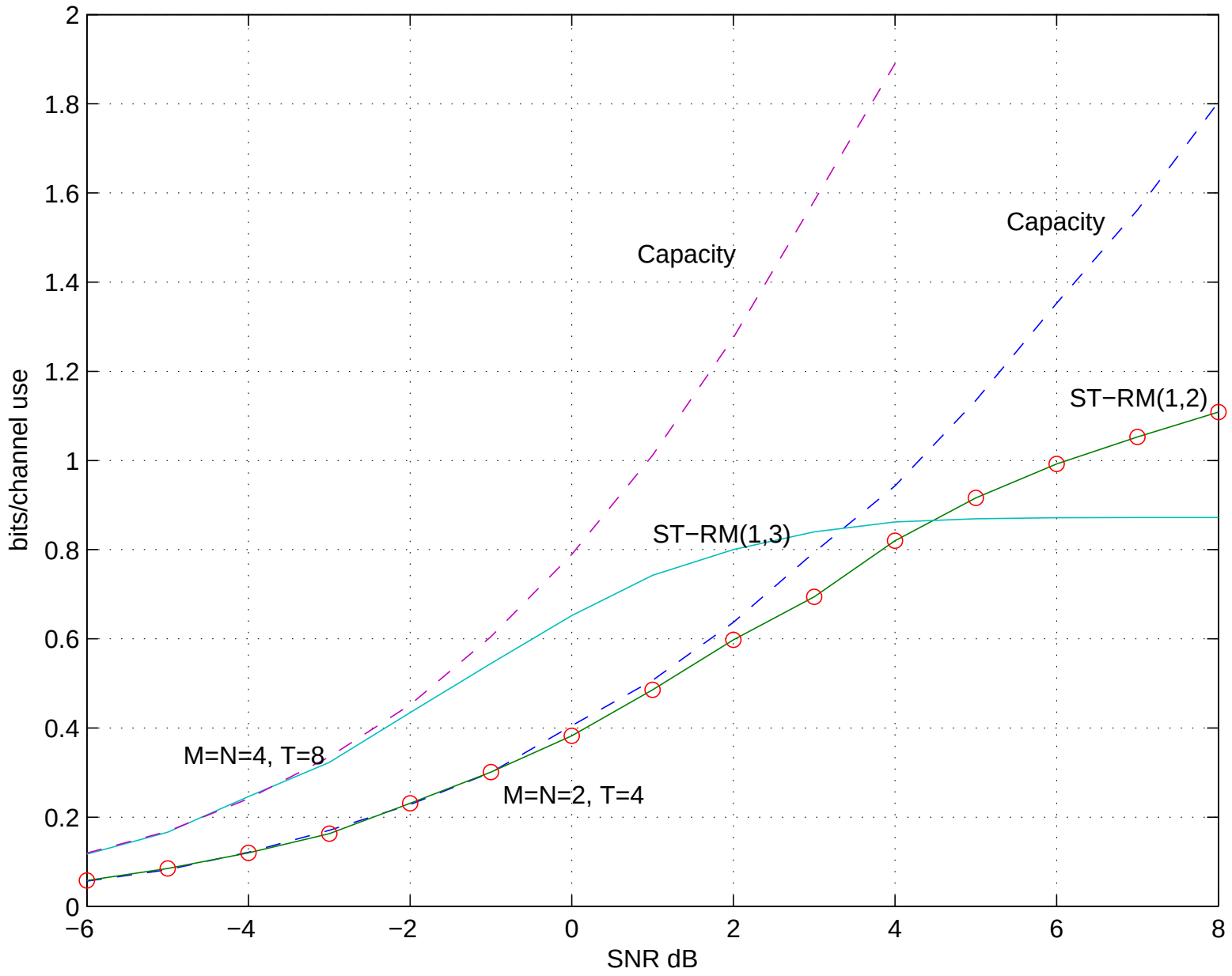
$$\begin{aligned} \mathbf{w} &= (2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0), \text{ and} \\ \mathbf{z} &= (1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0) \in RM(1,4). \end{aligned}$$

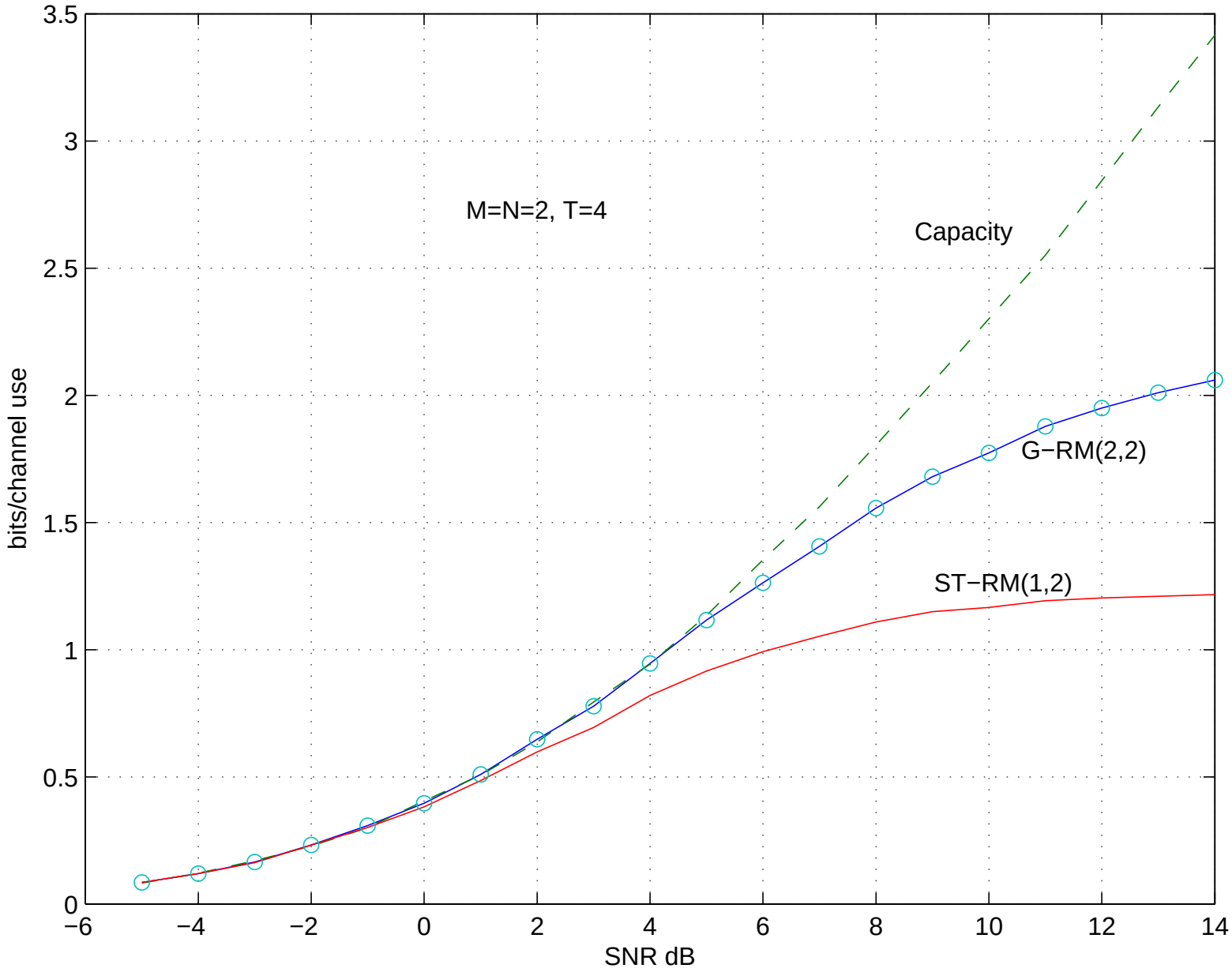
If there are channel errors then $\mathbf{z}$ *will be a corrupted version of a codeword of* $RM(1,4)$.

Simulation Results



With the help of simulation we estimate $I(U_i; \widehat{U}_i)$


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


M=N=2, T=4
Capacity
G−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