Space Time Coding for Secure Wireless Networks

Alfred O. Hero

Dept. EECS

University of Michigan - Ann Arbor

hero@eecs.umich.edu

http://www.eecs.umich.edu/~hero

Outline

1. Wireless network models
2. Performance metrics: capacity vs security
3. Unconstrained information rates
4. Maximum LPD-constrained information rates
5. Maximum LPI-constrained information rates
6. Tradeoff study

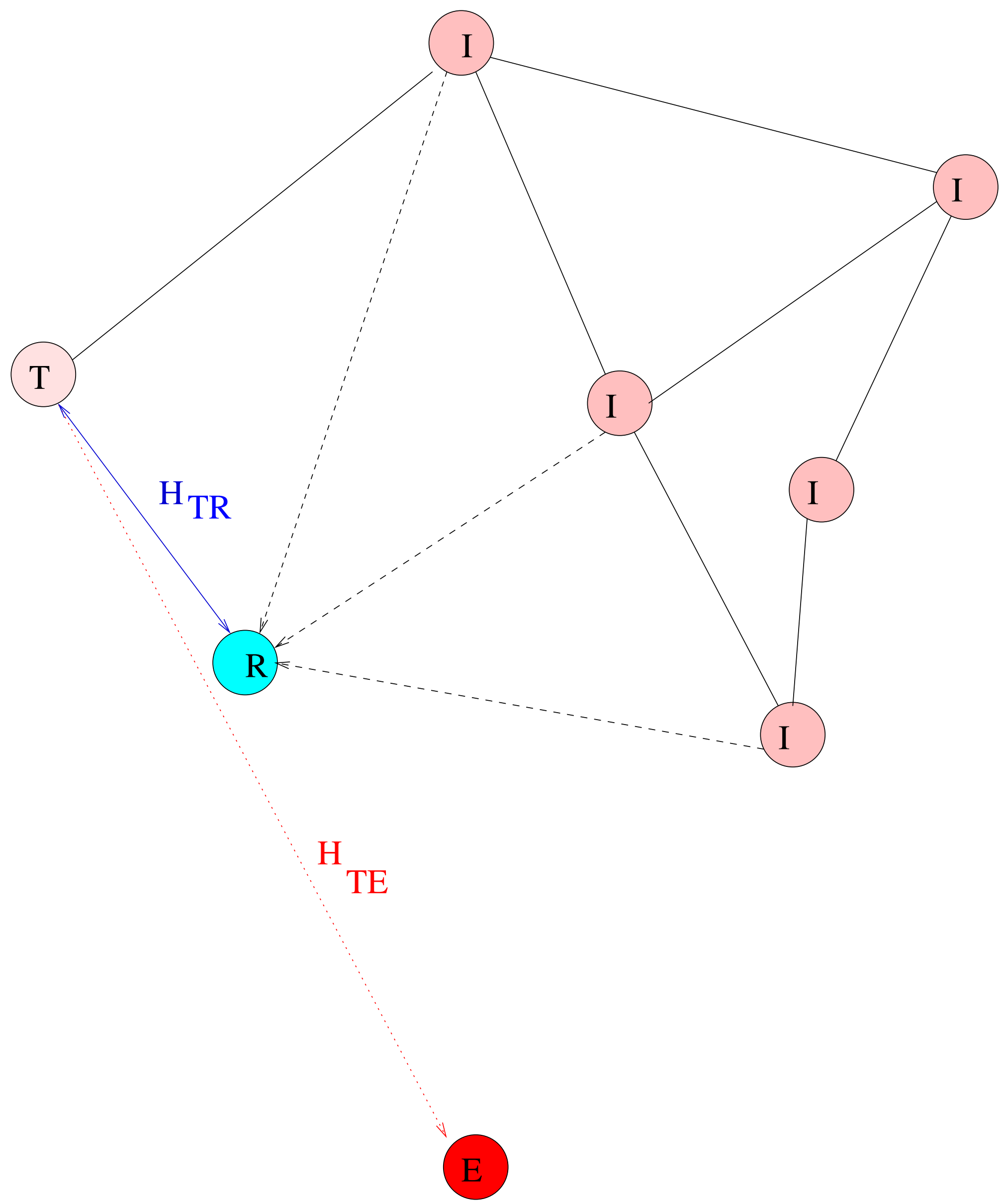
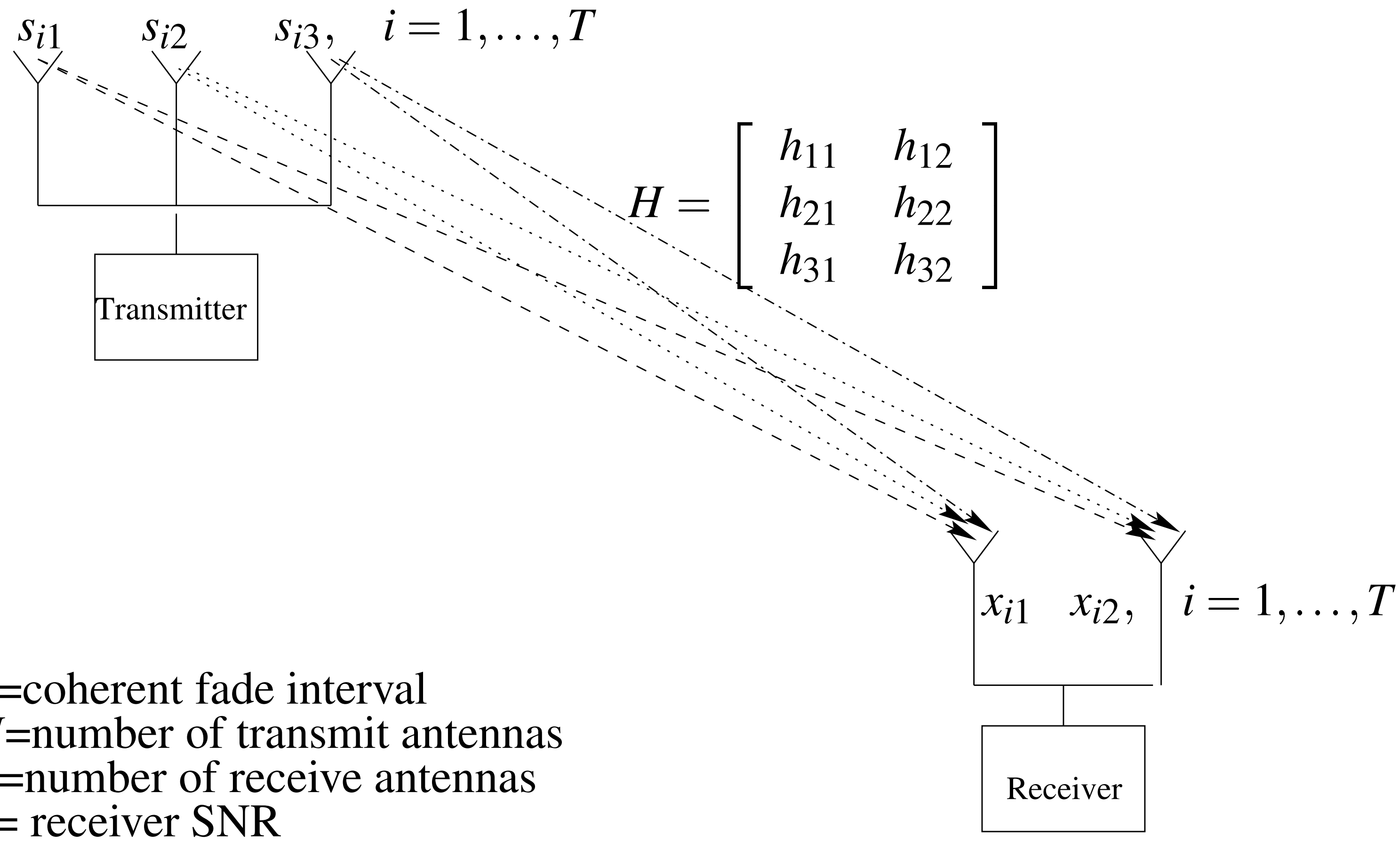


Figure 1. *Wireless network with eavesdropper*



T=coherent fade interval
M=number of transmit antennas
N=number of receive antennas
η= receiver SNR

$$X_{TR} = \sqrt{\eta} SH + W, \; (T \times N)$$

Figure 2. Space-Time channel ($M = 3$, $N = 2$)

Single User System

Received signal in l-th frame $(t = 1, \ldots, T)$

$$[x_{t1}^l, \ldots, x_{tn}^l] = \sqrt{\eta}[s_{t1}^l, \ldots, s_{tm}^l] \begin{bmatrix} h_{11}^l & \cdots & h_{1n}^l \\ \vdots & \vdots & \vdots \\ h_{m1}^l & \cdots & h_{mn}^l \end{bmatrix} + [w_{t1}^l, \ldots, w_{tn}^l],$$

or, equivalently

$$X^l = \sqrt{\eta} S^l H^l + W^l$$

- X^l: $T \times N$ received signal matrices
- S^l: $T \times M$ transmitted signal matrices
- H^l: i.i.d. $M \times N$ channel matrices $\sim \mathcal{CN}(0, I_M \bigotimes I_N)$
- W^l: i.i.d. $T \times N$ noise matrices $\sim \mathcal{CN}(0, I_T \bigotimes I_N)$

Code Construction

Block coding: string L codewords over L frames

$$| \; S^1 \; | \; S^2 \; | \; \cdots \; | \; S^L \; |$$

where S^l's are selected from a symbol alphabet $\mathcal{S}$

Random Block Coding: select S^l at random from $\mathcal{S}$ according to probability distribution $P \in \mathcal{P}$.

- Objective: Find optimal distribution $P(S)$ over $\mathcal{P}$ to:
  - maximize avg. information rate (achieve capacity)
  - maximize guaranteed rate (achieve outage capacity)
  - maximize random coding error exponent (achieve minimum P_e)
  - maximize sequentially-decodable rate (achieve cut-off rate)
- Transmitter constraints:

- average power constraint: $E[\|S\|^2] = \int \|S\|^2 dP \leq TM$
- peak power constraint: $\|S\|^2 \leq TM$, for all $S \in \mathcal{S}$

where

$$\|S\|^2 = \mathrm{tr}\{S^H S\}$$

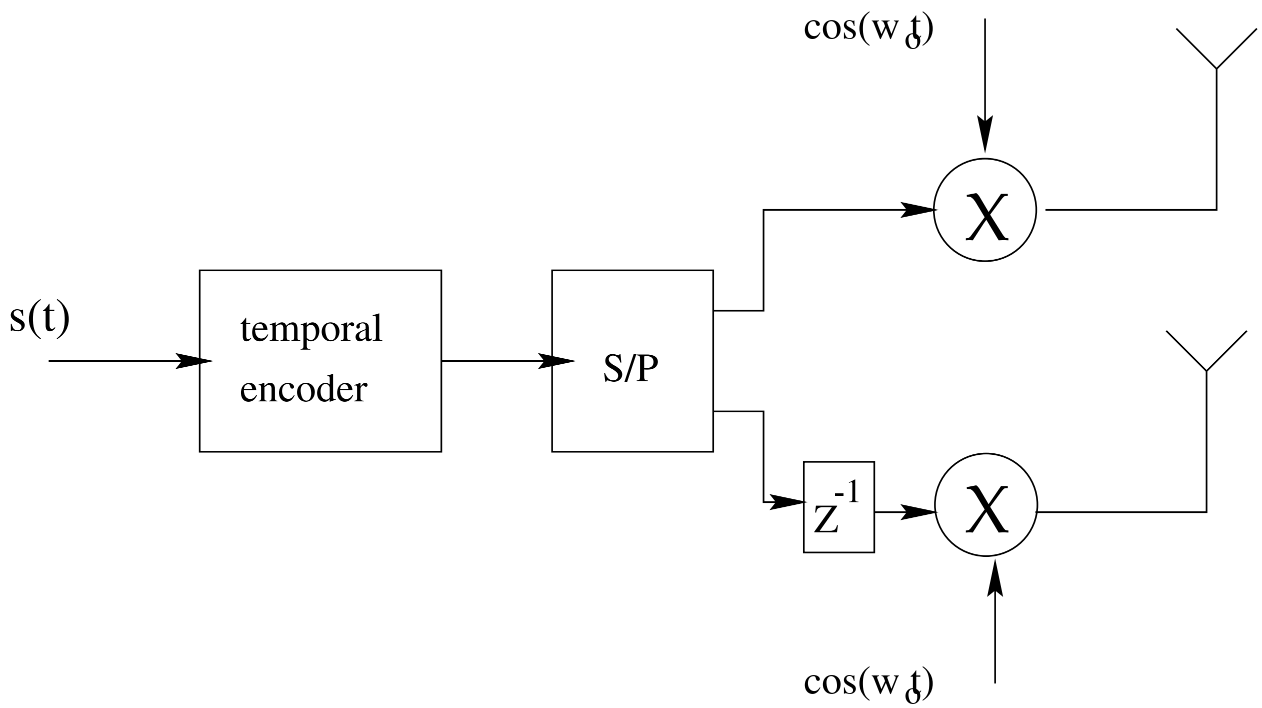


Figure 3. First generation space-time coding: Seshadri&Winters FDD transmitter with delay diversity (1994)

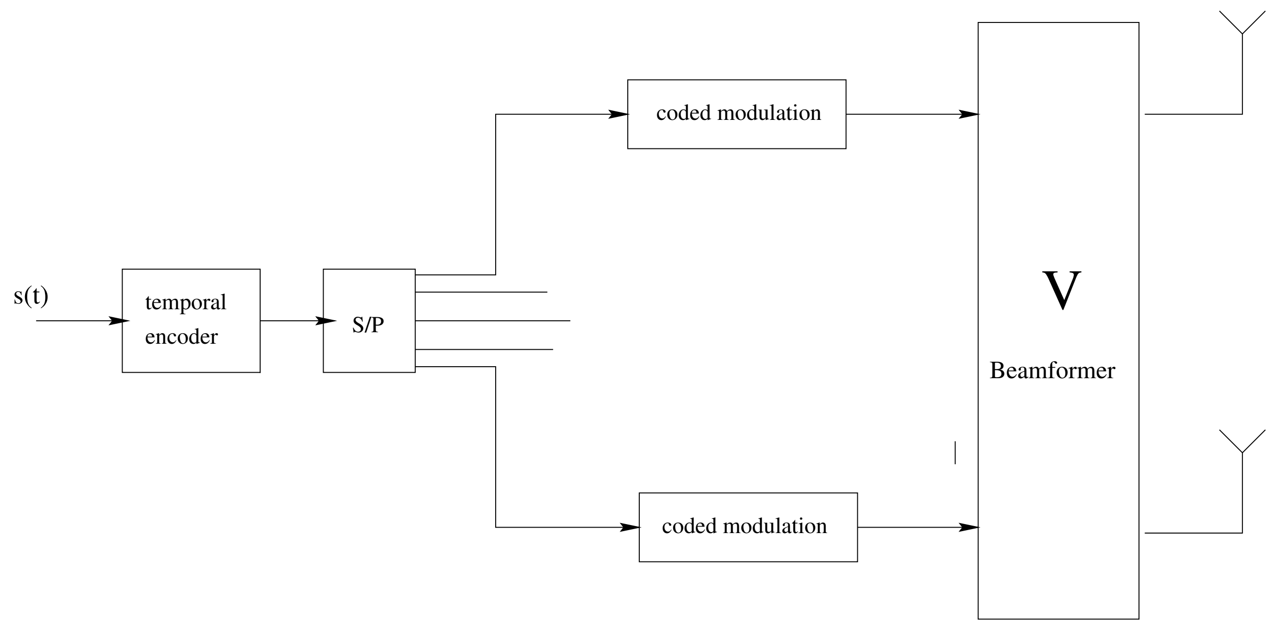


Figure 4. Second generation space-time coding (Foschini:96,Tarokh&etal:98)

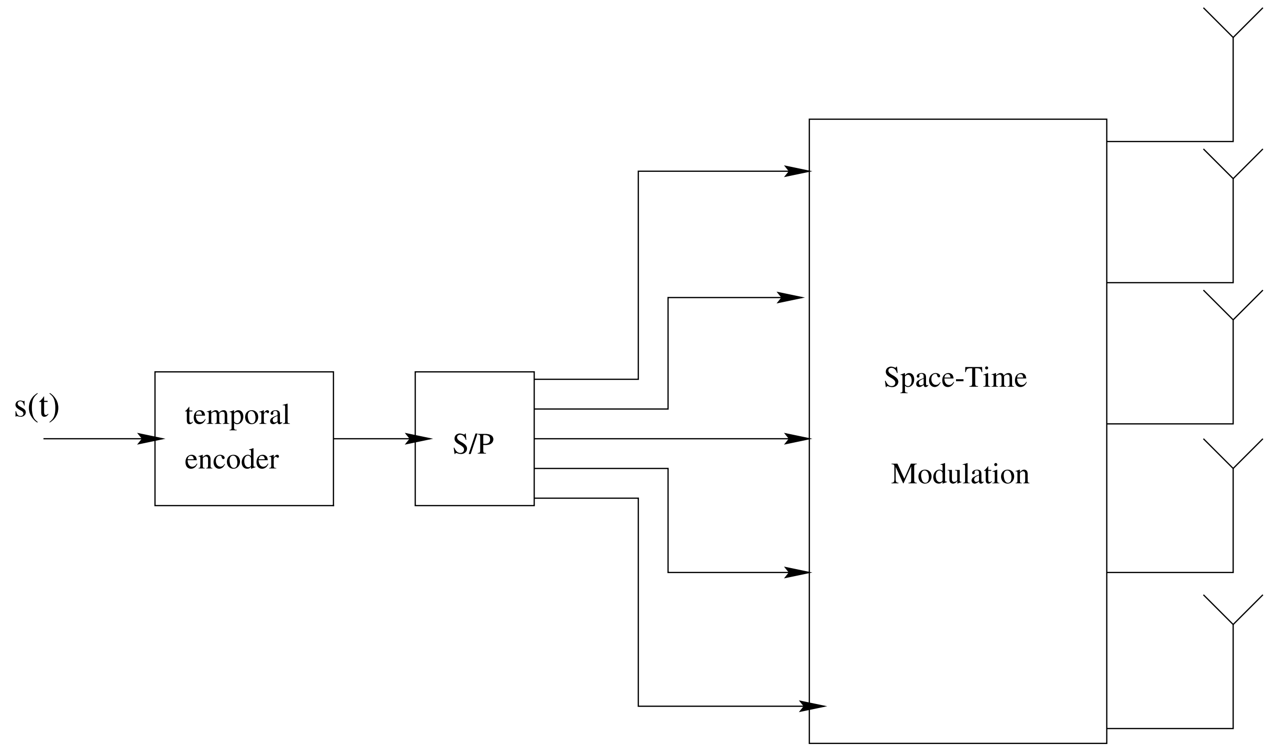


Figure 5. Third generation space-time coding (Hochwald&etal:98)

Multi-user Rayleigh Fading Receiver Model

Received signal over L symbol blocks is sequence of $T \times N$ matrices

$$
\begin{aligned}
\mathbf{X}(t) &= \sum_{i=1}^{K} \mathbf{S}_k(t;\theta_k)\mathbf{H}_k(t) + \mathbf{N}(t) \\
&= \overbrace{[\mathbf{S}_1(t;\theta_1),\ldots,\mathbf{S}_K(t;\theta_K)]}^{T\times KM} \underbrace{\begin{bmatrix} \mathbf{H}_1(t) \\ \vdots \\ \mathbf{H}_K(t) \end{bmatrix}}_{KM\times N} + \mathbf{N}(t) \\
&= \mathcal{S}_K(t;\underline{\theta}_K)\mathcal{H}_K(t) + \mathbf{N}(t) \\
&= \mathbf{S}_K(t;\theta_K)\mathbf{H}_K(t) + \underbrace{\mathcal{S}_{K-1}(t;\underline{\theta}_{K-1})\mathcal{H}_{K-1}(t)}_{MUI} + \mathbf{N}(t) \quad t = 1,\ldots,L
\end{aligned}
$$

General Model Parameters

1. $\mathbf{S}_k(t;\theta_k)$: k-th user signature matrix ($T \times M$)
2. $\mathbf{H}_k(t)$: k-th user propagation (channel) matrix ($M \times N$)
3. θ_k: k-th user parameters (b_k, τ_k, ν_k)
4. $\mathbf{N}(t)$: zero mean white complex Gaussian noise matrix ($T \times N$)

Saturated/heavily-loaded MUI approximation

$$\text{MUI} \sim \mathcal{N}(0,\ Q_T \otimes Q_N)$$

Secure network conditions

1. Subscriber links have *informed* transmitters/receivers:
   - H_{TR} is known to both parties over a hop
   - Training may be required to learn channel
   - Feedback is required to inform transmitter of channel
2. Eavesdropper link has *uninformed* transmitter/reciever
   - H_{TE} is unknown to both parties over a hop
   - Training sequences, signal constellations, and other attributes may be known

Network QoS metrics

1. $P_{sde}(K)$: symbol decoding error rate of K-th link

$$P_{sde}(K) = P_{\underline{\theta}}(\hat{\underline{\theta}}_K \neq \underline{\theta}_K)$$

2. $C(K)$: **channel capacity of K-th link**

$$C(K) = \max_{P_{S_K}} I(S_K;X), \quad I(S_K;X) = E_{\underline{\theta}}[\ln f_{X|S_K}(X|S_K)/f_X(X)]$$

3. $R_o(K)$: **channel cutoff-rate of K-th link**

4. $C_{out}(K)$: outage capacity of K-th link

$$P(C(H_K) > C_{out}) \geq 1 - \varepsilon, \quad C(H_K) = \max_{P_{S_K}} I(S_K;X|H_K)$$

5. C_{sum}: sum capacity over all links

$$C_{sum} = \max_{P_{S_1,\ldots,S_K}} \sum_{i=1}^{K} R_i$$

6. C_{min}: min capacity of any link

$$C_{min} = \max_{P_{S_1,\ldots,S_K}} \min_i R_i$$

Eavesdropper metrics

1. $P_F(K), P_M(K) = 1 - P_D(K)$: **eavesdropper error rates for detecting presence of K-th user**

$$P_M = P_{H_0}(\Lambda_K^e > \gamma), \quad P_M = P_{H_1,\underline{\theta}_K}(\Lambda_K^e < \gamma)$$

2. $C^e(K) = \max_{P_{S_K}} I(S_K; X^e)$: **eavesdropper link capacity for K-th user**

3. $P_{sde}^e(K)$: eavesdropper K-th user intercept error rate

$$P_{sde}^e(K) = P_{\underline{\theta}}(\hat{\underline{\theta}}_K^e \neq \underline{\theta}_K)$$

Single Link Capacity: avg power constraint: $\mathrm{tr}(E[SS^{\dagger}]) \leq \sigma$

1. T/R-informed σ-capacity: H known to both T/R

$$C_1 = E[C(H)], \quad (bits/sec/hz)$$

$$\begin{aligned} C(H) &= \max_{P_{S|H}} I(S,X|H) \\ &= T \ln \left| I_M + H\Sigma_S H^{\dagger} \right| \end{aligned}$$

Capacity achieving source (waterpouring is optimal)

$$S \sim \mathcal{N}(0,\, I_T \bigotimes \Sigma_S), \qquad \Sigma_S = \mathrm{diag}\left((\mu - 1/\lambda_i)^+\right)$$

$$\lambda_i = \mathrm{eigs}\left(H(I_N + Q_N)^{-1} H^{\dagger}\right) \qquad \mu \,:\, \mathrm{tr}(\Sigma_S) = \sigma$$

2. R-informed σ-capacity: H known to R only

$$C_2 = \max_{P_S} E[I(X,S|H)]$$

Capacity achieving source

$$S \sim \mathcal{N}(0, I_T \bigotimes I_M)$$

3. Uninformed σ-capacity: H unknown to either T/R

$$C = \max_{P_S} E\left[\log P_{X|S}(X|S)/P_X(X)\right]$$

Capacity achieving source

$$S \sim V\Lambda$$

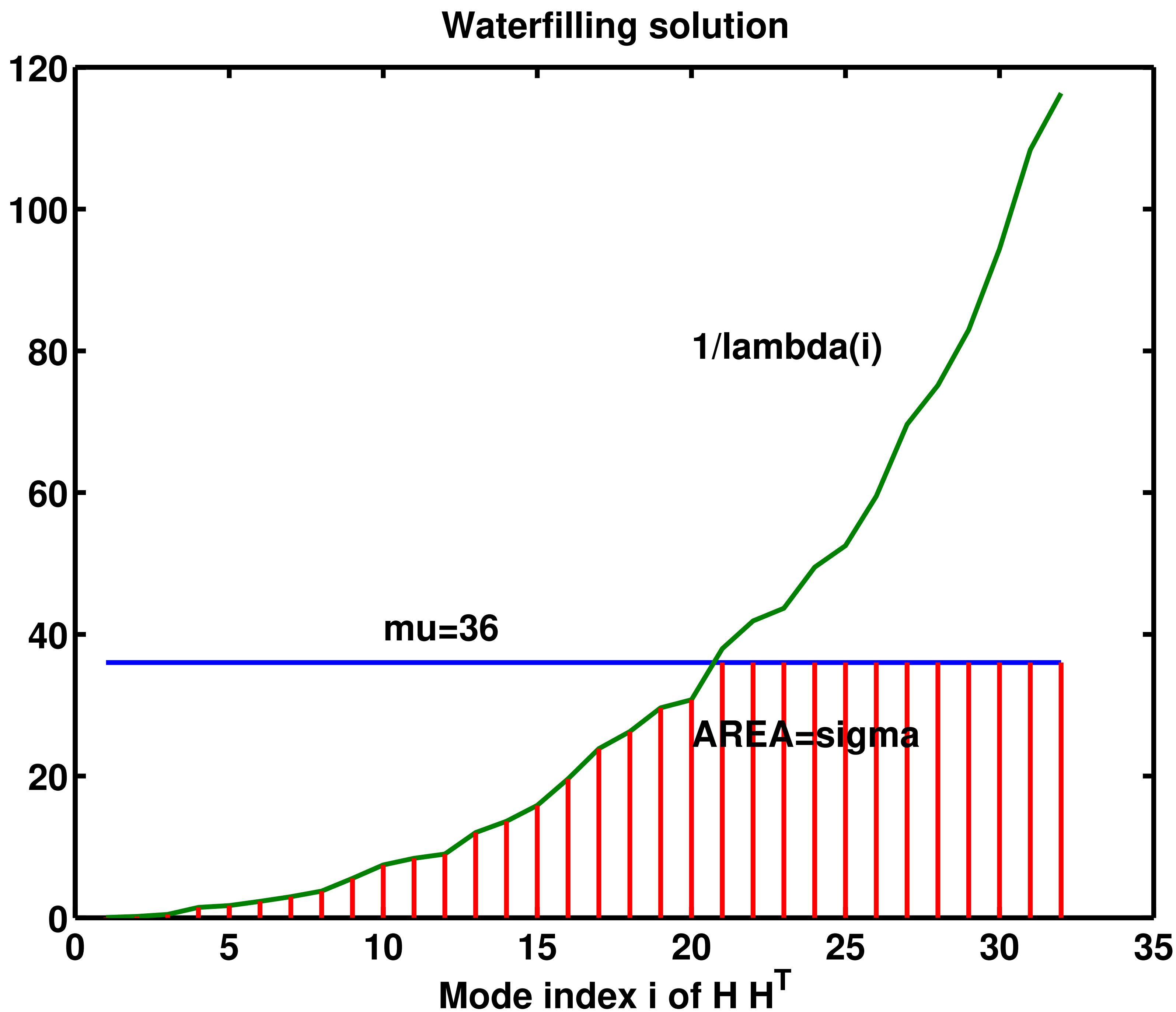


Figure 6. *Waterpouring solution for σ-capacity achieving mode allocation($N = M = 32$)*

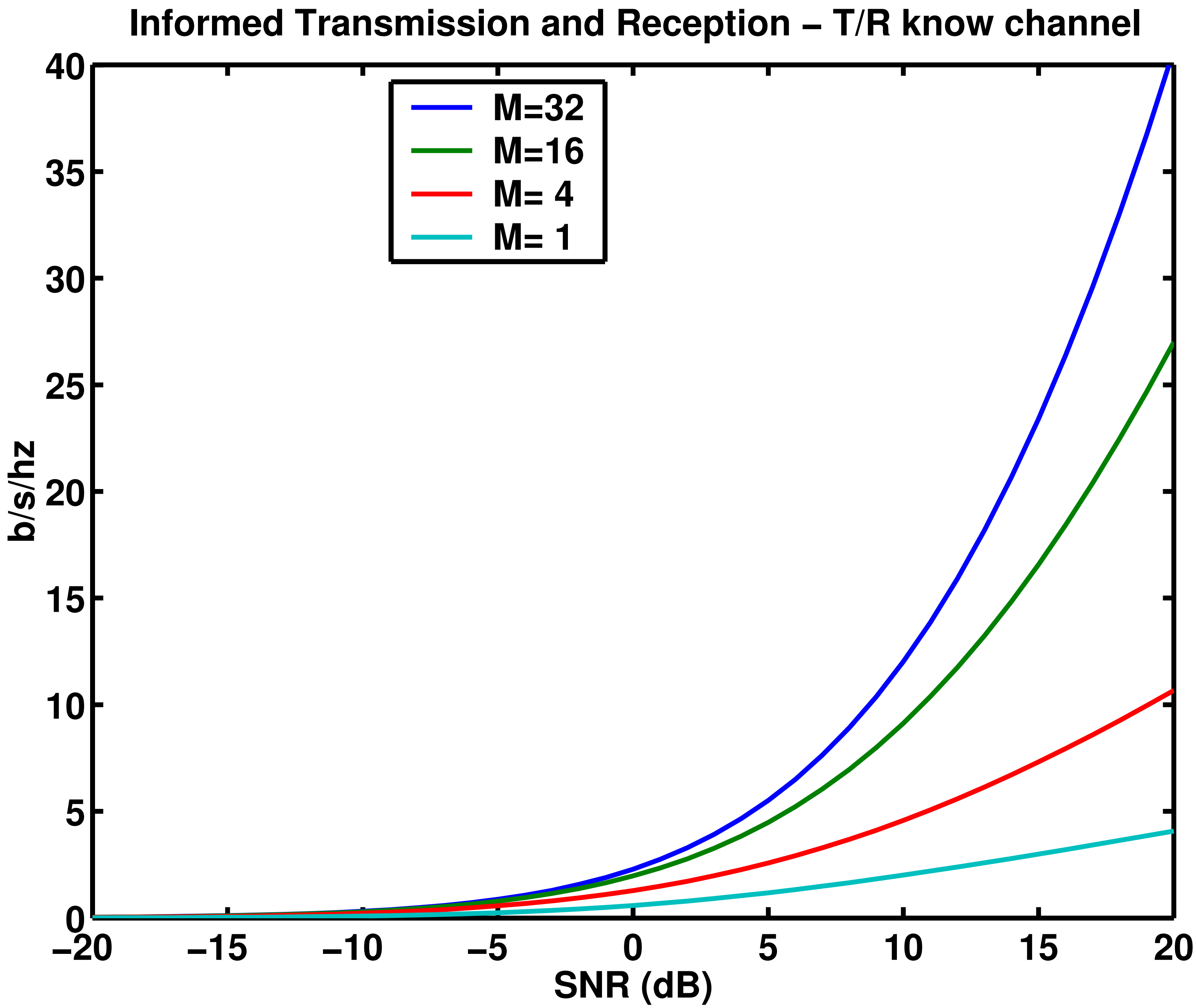


Figure 7. *T/R informed σ-capacity (N = M)*

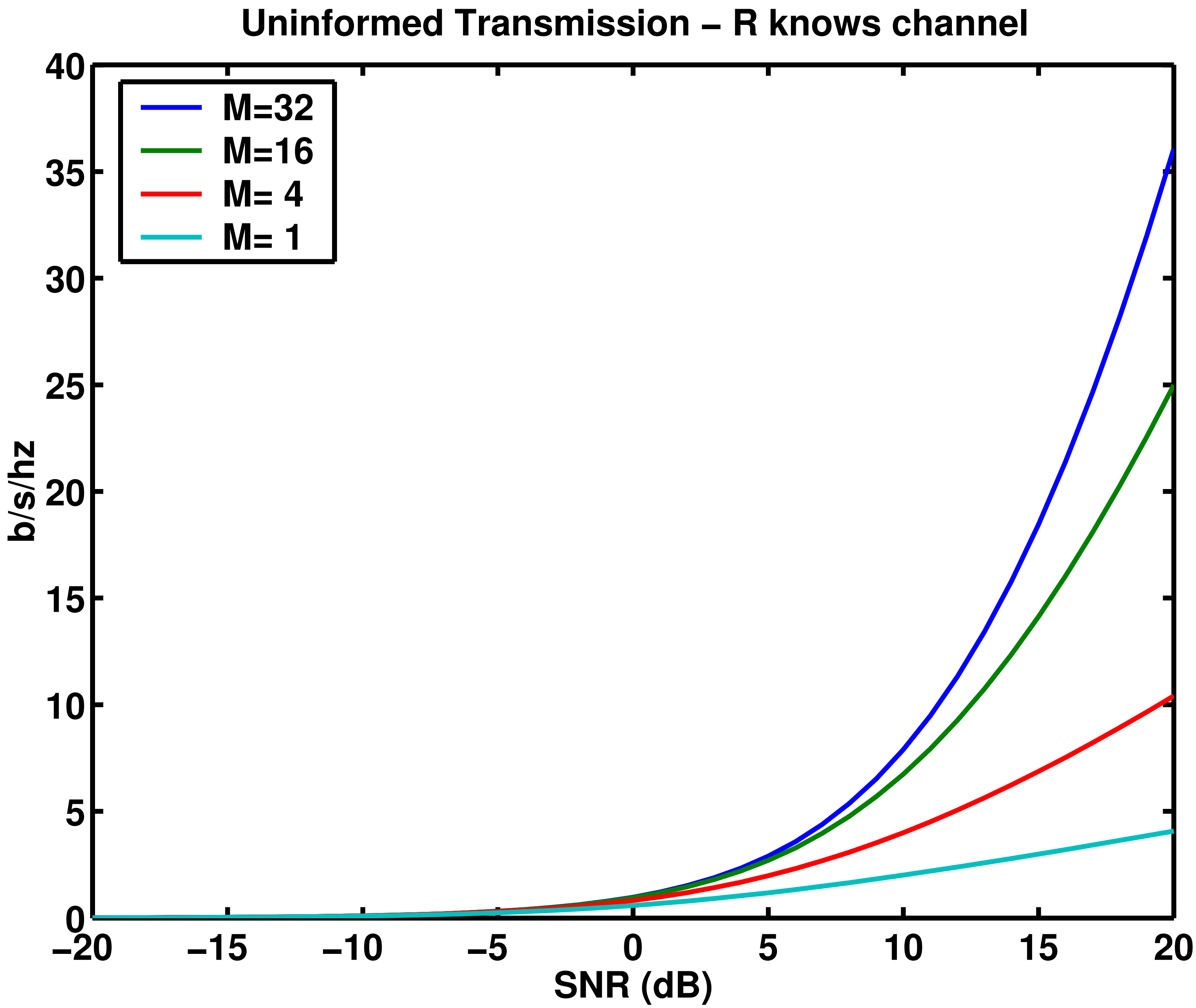


Figure 8. *R informed σ-capacity ($N = M$)*

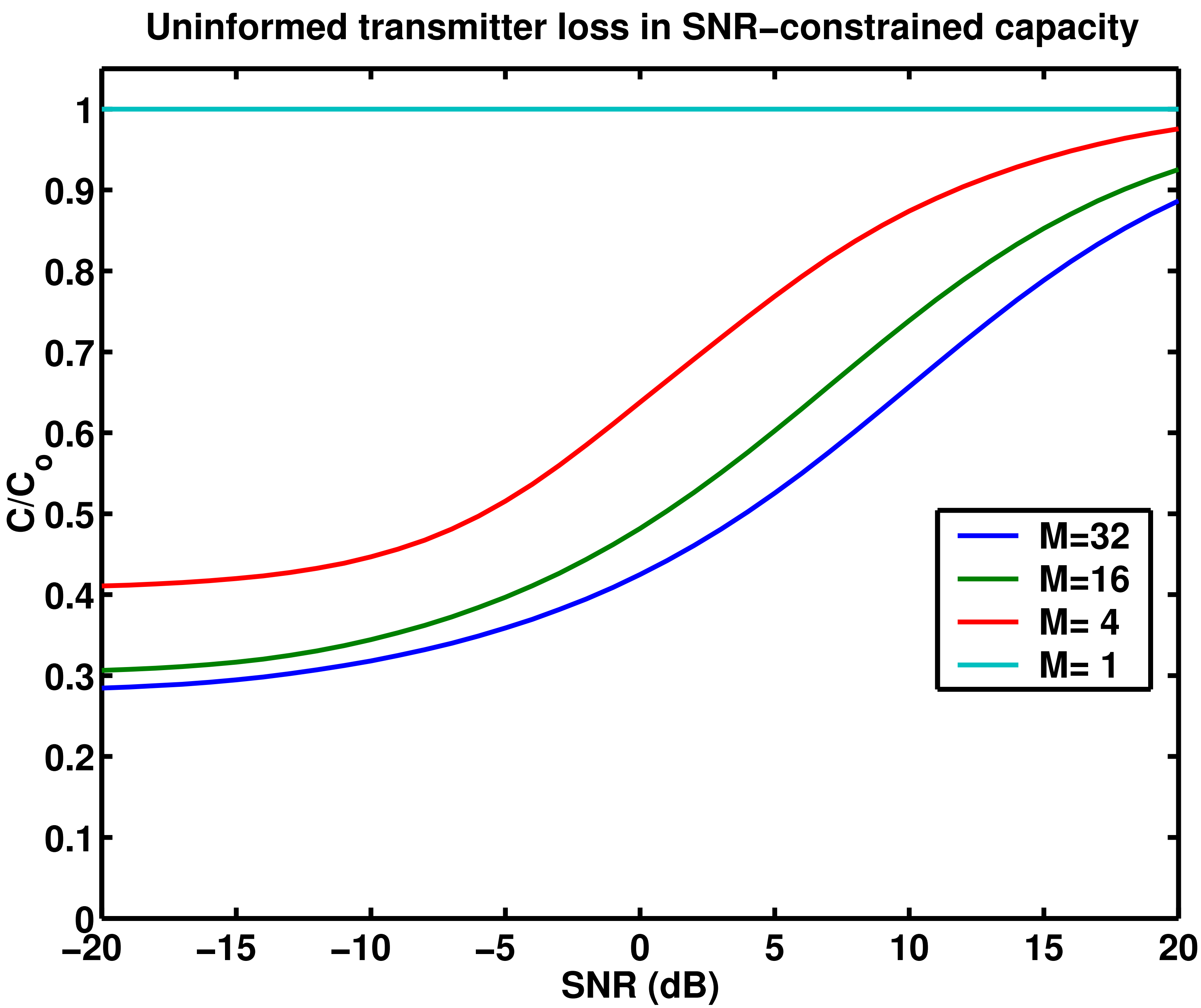


Figure 9. *R informed Capacity loss due to uninformed T (N = M)*

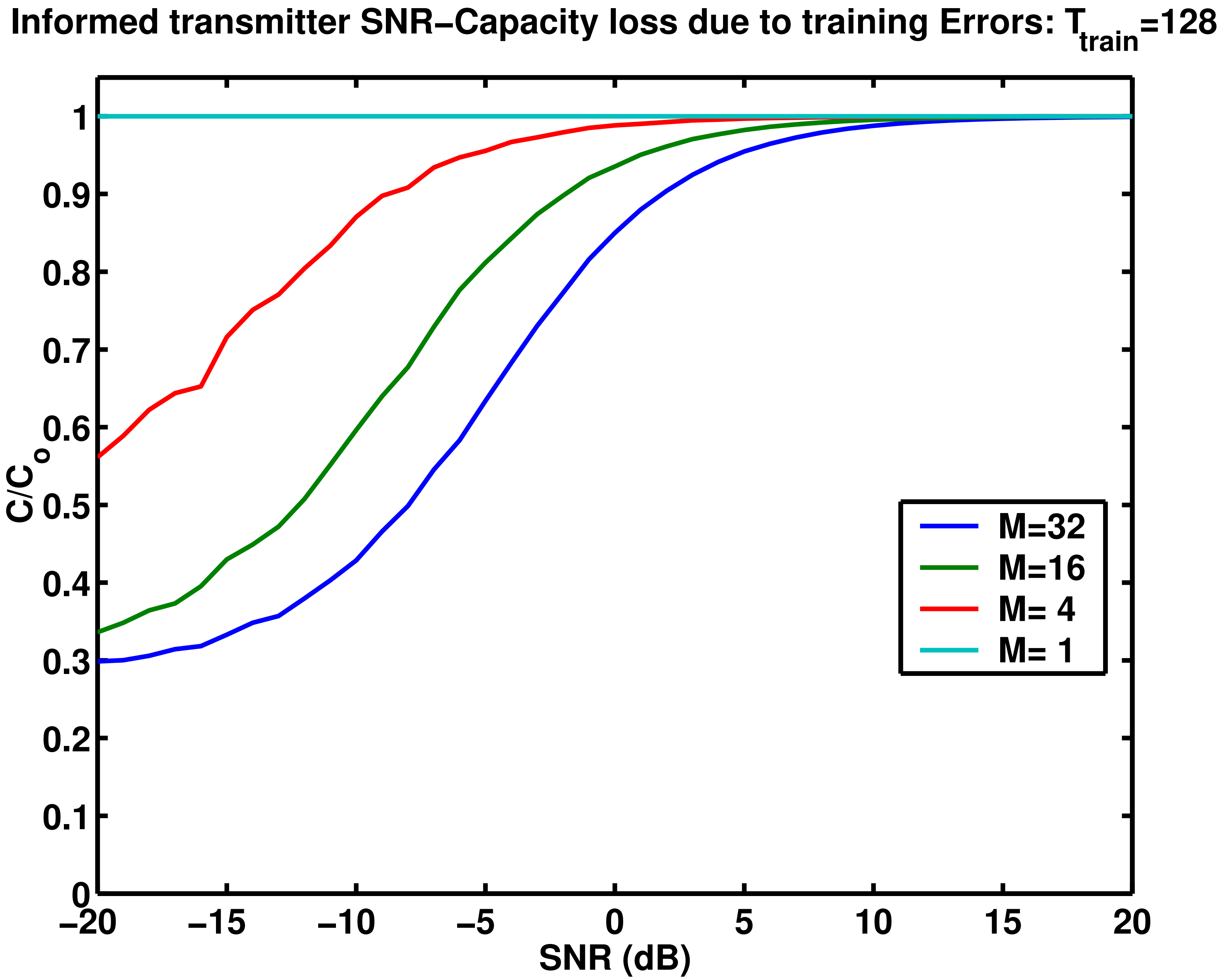


Figure 10. *T/R nformed capacity loss due to training errors (N = M)*

Random Coding Error Exponents

The minimum error probability of any decoder of a block code over L frames satisfies (Fano 61)

$$\min P_e \leq e^{-LE_U(R)}, \quad R < C$$

where

- R: symbol rate (nats/symbol)
- C: channel capacity (nats/symbol)
- $E_U(R)$: error exponent

$$E_U(R) = \max_{\mu\in[0,1]} \max_{P\in\mathcal{P}} \left\{ -\mu R - \ln \int_{X\in\mathcal{X}} \left[\int_{S\in\mathcal{S}} (p(X|S))^{1/(1+\mu)} \, dP(S) \right]^{1+\mu} dX \right\}, \quad \text{nats/sym}$$

$E_U(R)$ has been studied under *avg. power constraint* for

$\Rightarrow$ Known H (Telatar BL TM 96)

$\Rightarrow$ Unknown H (Abou-Faycal & Hochwald BL TM 99)

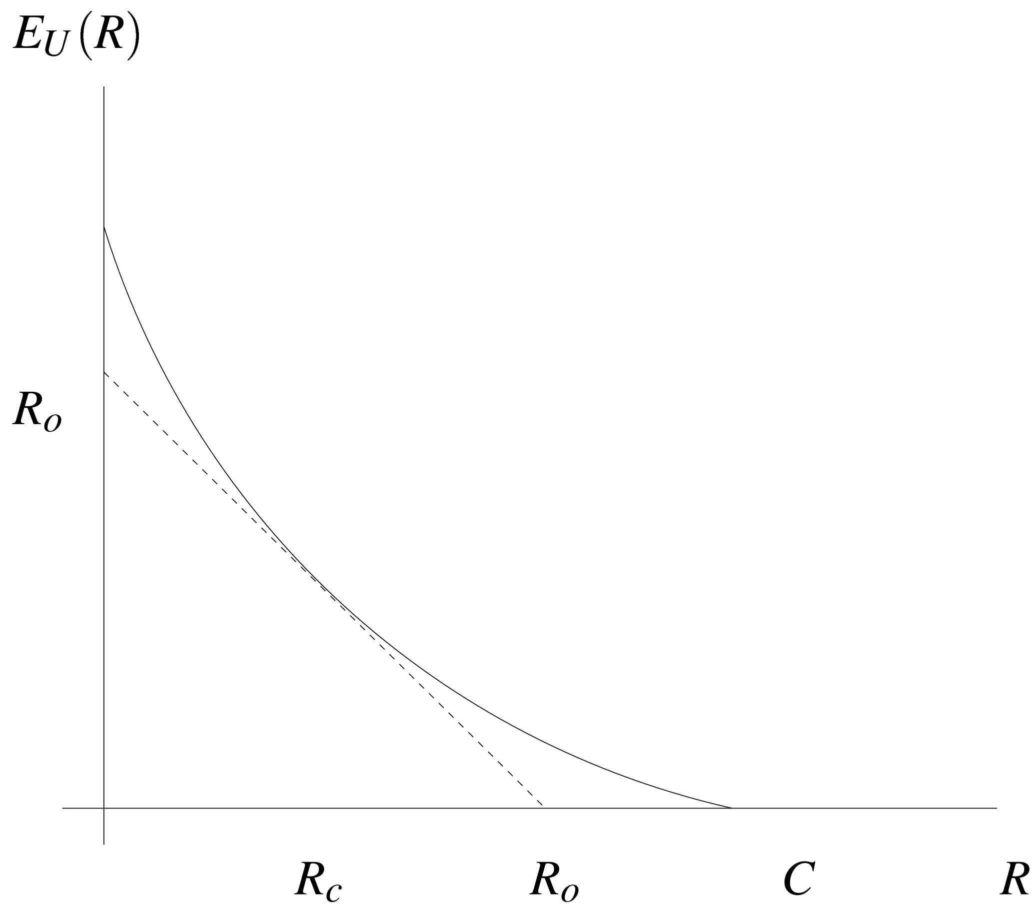


Figure 11. Error exponent $E_U(R)$ and cut-off rate bound $y(R) = R_o - R$.

R_o ***computational cut-off rate*** **lower bound** (Gallager IT 64)

$$E_U(R) \geq R_o - R, \quad R \leq R_o$$

$$R_o = \max_{P \in \mathcal{P}} - \ln \int_{X \in \mathcal{X}} \left[\int_{S \in \mathcal{S}} \sqrt{p(X|S)} dP(S) \right]^2 dX, \quad \text{nats/symbol}$$

where $\mathcal{P}$ are suitably constrained distributions over $\mathcal{C}^{T \times M}$

$\Rightarrow$ Cut-off rate analysis has been used to evaluate

- practical coding limits (Wang&Costello COM 95, Hagenauer&etal IT 96)
- different coding and modulation schemes (Massey 74)
- signal design for optical fiber links (Snyder&Rhodes IT 80)
- signaling over multiple access channels (Narayan&Snyder IT81)

FACTS:

- $R_o \leq C$
- R_o is highest practical rate for sequential decoders (Savage 65)
- $E_U(R) \approx R_o - R$ when $R \approx R_c$, the critical rate
- R_o specifies upper bound on optimal decoder error

$$P_e \leq e^{-L(R_o - R)}, \quad R \leq R_o$$

Single Link Cutoff Rates for Space Time Coding

$$R_o(H) = \max_{P_{S|H}} -\ln \int\int_{S_1,S_2\in \mathbb{C}^{T\times M}} dP_{S|H}(S_1)\,dP_{S|H}(S_2)\ \ e^{-ND(S_1\|S_2)}$$

1. T/R Informed cutoff rate: H known to both T/R

$$D(S_1\|S_2) = \frac{\eta}{4}\,\mathrm{tr}\left(H^\dagger(S_1-S_2)^\dagger(S_1-S_2)H\right)$$

2. R informed cutoff rate: H known to R only

$$D(S_1\|S_2) = \ln\left|I_M + \frac{\eta}{4}\,(S_1-S_2)^\dagger(S_1-S_2)\right|$$

3. Uninformed cutoff rate: H unknown to either T/R

$$D(S_1\|S_2) = \ln \frac{\left|I_T + \frac{\eta}{2}(S_1S_1^\dagger + S_2S_2^\dagger)\right|}{\sqrt{\left|I_T+\eta S_1S_1^\dagger\right|\ \left|I_T+\eta S_2S_2^\dagger\right|}}$$

LPI: Eavesdropper Lockout Capacity

Lock out condition: $R_o^3 = 0$

Note: **lock out** occurs if transmitted signal constellation $\{S_i\}$ satisfies:

$$S_i S_i^\dagger = A, \qquad \forall\, i$$

Examples:

- Doubly unitary codes ($T \geq M$):

$$S_i^\dagger S_i = I_M, \quad S_i S_i^\dagger = \begin{bmatrix} I_M & O \\ O & O \end{bmatrix}$$

  Instances

  - Square unitary codes ($T = M$): $S_i S_i^\dagger = S_i^\dagger S_i = I_M$

– Space time QPSK: Quaternion codes ($T = M = 2$):

$$\mathcal{S} = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix} \right\}$$

- Constant (spatial) modulus (CM) codes $(T = 1)$:

$$S_i = \underline{s}_i^T = [s_{1i}, \cdots, s_{Mi}]$$

$$\underline{s}_i^\dagger \underline{s}_i = \mathrm{tr}\{\underline{s}_i^\dagger \underline{s}_i\} = 1 \;\; \Rightarrow \;\; \text{peak transmit power constraint}$$

Q: What is the channel capacity under lockout constraint?

Let

$$N \geq M, \quad H = U[\Lambda\, O]V$$

$$SO(\mathbb{C}^{TM}) = \{S : SS^\dagger = cI_T\}$$

and define for $c > 0$

$$\mathcal{E} = \{S : S\Lambda^{-2}S^\dagger = cI_T\}$$

Proposition 1 *Eavesdropper lockout capacity for a T/R informed link is* $E[C_{lockout}(H)]$

$$C_{lockout}(H) = -\int dX_1 \mathcal{N}_{TM}(S - X_1) \ln \int_{\mathcal{E}} dP_S^*(S') \mathcal{N}_{TM}(S' - X_1) - TM \ln \pi e$$

where

- $\mathcal{N}_{TM}(x)$ *is density of standard* TM *complex normal rv*
- $T \times M$ *matrix* X_1 *is defined by:* $[X_1, X_2] = XV$
- dP_S^* *is density over* $SO(\mathbb{C}^T M)$ *which makes the RHS independent of S*

Note 1: Optimality of uniform codeword distribution:

Special case: $\Lambda = aI_M$

$\Rightarrow$ Capacity attaining distribution dP_S^* is uniform over the TM*-sphere* $SO(\mathbb{C}^{TM})$

Example: *Equispaced QPSK constellation*

Conjecture: uniform dP_S is optimal for any H for large T and large SNR.

Note 2: Q. How much capacity does lockout cost?

A. Dimensionality analysis $(T = M)$:

Constraint $S_i S_i^\dagger = A$ reduces code dimension by factor

$$\rho = \frac{M(M+1)/2}{M^2} \approx 1/2$$

LPD constraint

Chernoff Bound on eavesdropper's minimum attainable detection error probability

$$\begin{aligned}
\liminf_{L\to\infty} \frac{1}{L} P_e &\leq \rho \\
\rho &= \inf_{\alpha\in[0,1]} \ln \int dP_S(s) \int dX\, f_{X|S}^{1-\alpha}(X|s) f_{X|S}^{\alpha}(X|s=0) \\
&= \inf_{\alpha\in[0,1]} \ln \int dP_S(s) \left(\frac{\|I_T + \eta\, SS^\dagger\|^\alpha}{I_T + \alpha\eta\, SS^\dagger\|} \right)^N
\end{aligned}$$

Low SNR approximation:

$$\rho = -\frac{N\eta^2}{8} \operatorname{tr}\left(E[SS^\dagger SS^\dagger]\right) + o(\eta^2)$$

Conclude: LPD constraint $\rho \geq \rho_o$ is captured by *kurtosis* constraint

$$\operatorname{tr}\left(E[SS^\dagger SS^\dagger]\right) \leq \kappa$$

Kurtosis-constrained Capacity

Proposition 2 *The kurtosis-constrained capacity C_κ^3 for the T/R informed link satisfies the lower bound*

$$C_\kappa^3 \geq E[C_\kappa(H)]$$

$$C_\kappa(H) \quad = \quad T \ln \left| I_M + H \Sigma_S H^\dagger \right|$$

Capacity-bound achieving source: $S \sim \mathcal{N}(0,\, I_T \bigotimes \Sigma_S)$

$$\Sigma_S = \operatorname{diag}\left(\frac{\sqrt{1/\lambda_i^2 + \mu} - 1/\lambda_i}{2} \right), \qquad \lambda_i = \operatorname{eigs}\left(H (I_N + Q_N)^{-1} H^\dagger \right)$$

$$\mu \;:\; 3\left(\operatorname{tr}\{\Sigma_S\}\right)^2 = \kappa$$

Note:

1) σ-optimal waterpouring solution is **not** κ-optimal

2) relation between kurtosis and avg power of S

$$\sqrt{M\,\mathrm{tr}\{E[SS^\dagger SS^\dagger]\}} \geq \mathrm{tr}\left\{E[SS^\dagger]\right\}$$

Conclude: kurtosis constraint also constrains avg power

However: kurtosis constraint produces qualitatively different optimal source distribution.

3) Optimal Kurtosis constrained signal covariance is well approximated at high SNR by

$$\Sigma_S \approx \sqrt{\kappa/M}\;\mathrm{diag}\left(\frac{\lambda_{max}^2 - \lambda_i^2}{\sum_i(\lambda_{max}^2 - \lambda_i^2)}\right)$$

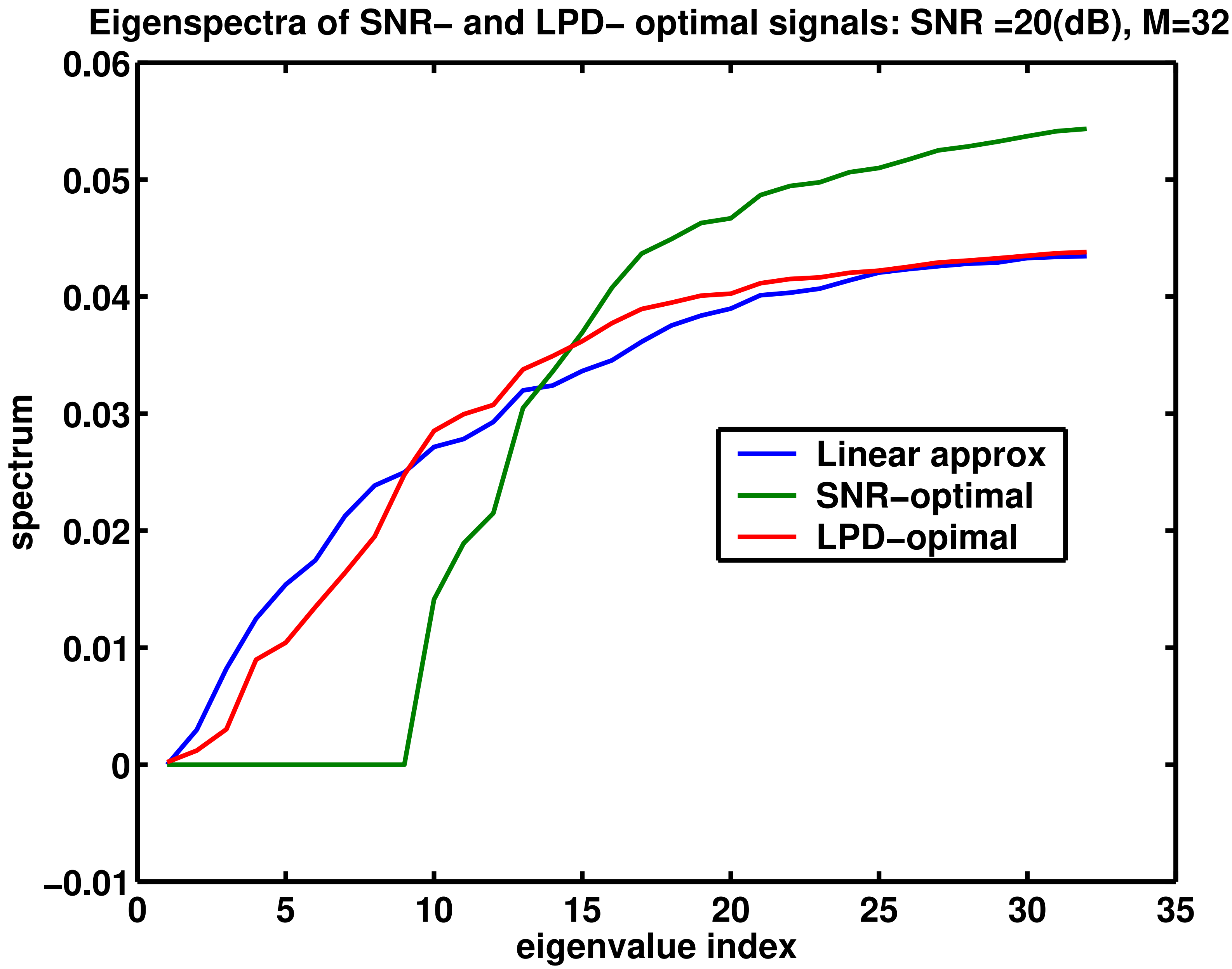


Figure 12. *Spectra of optimal source covariance matrices under LPD and Pavg constraints: SNR* $= 20dB, M = N = 32, Q_T = Q_R = 0$

LPD: Tradeoff Study

1. T/R informed κ-Capacity
2. Loss in σ-capacity due to LPD constraint

$$C_\sigma(dP_\kappa^*)/C_\sigma(dP_\sigma^*)$$

3. Loss in κ-capacity due to Pavg constraint

$$C_\kappa(dP_\sigma^*)/C_\kappa(dP_\kappa^*)$$

4. Loss in κ-capacity due to training errors

$$T = 1024, \quad T_{train} = 128$$

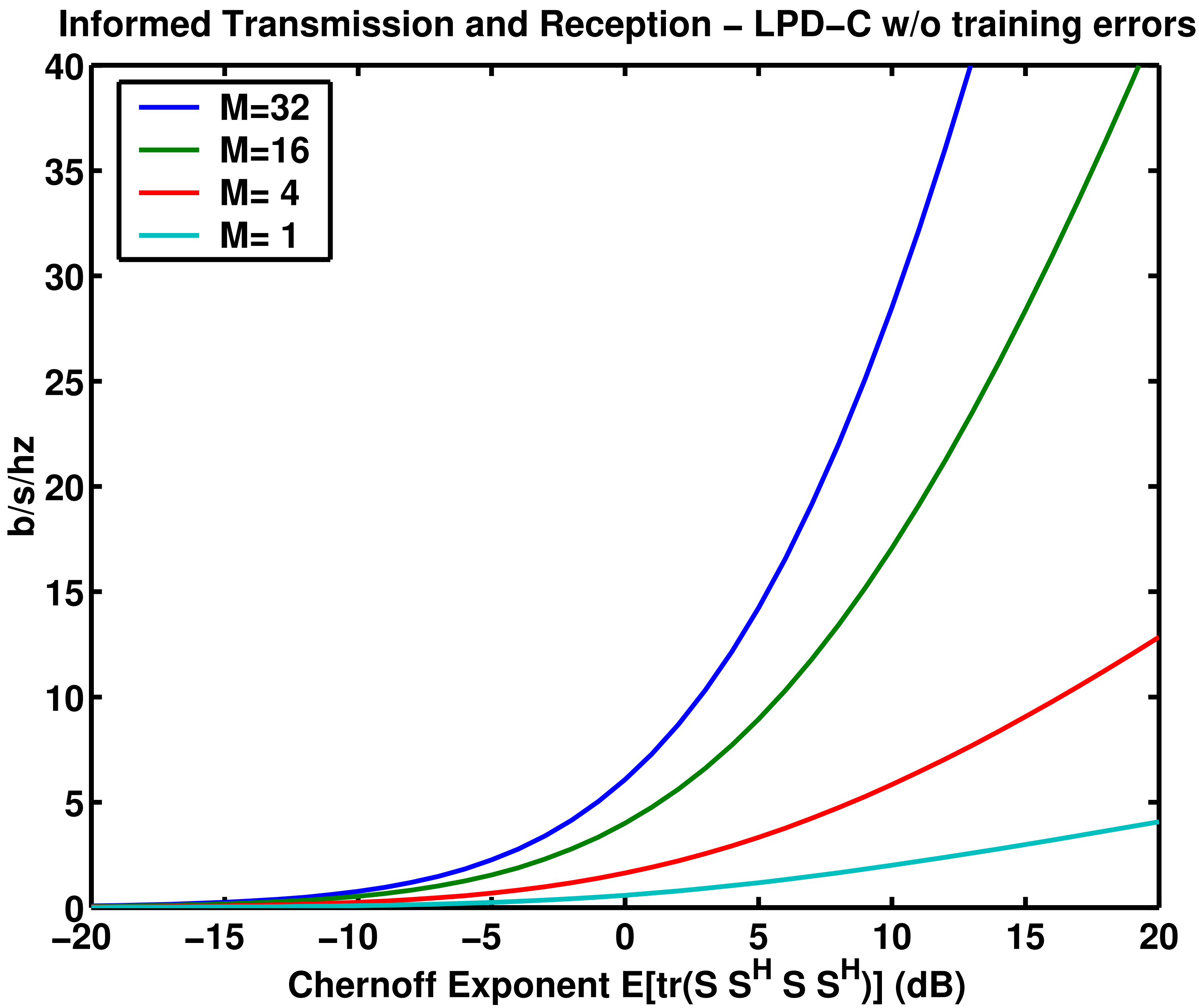


Figure 13. *T/R informed κ-capacity (N = M)*

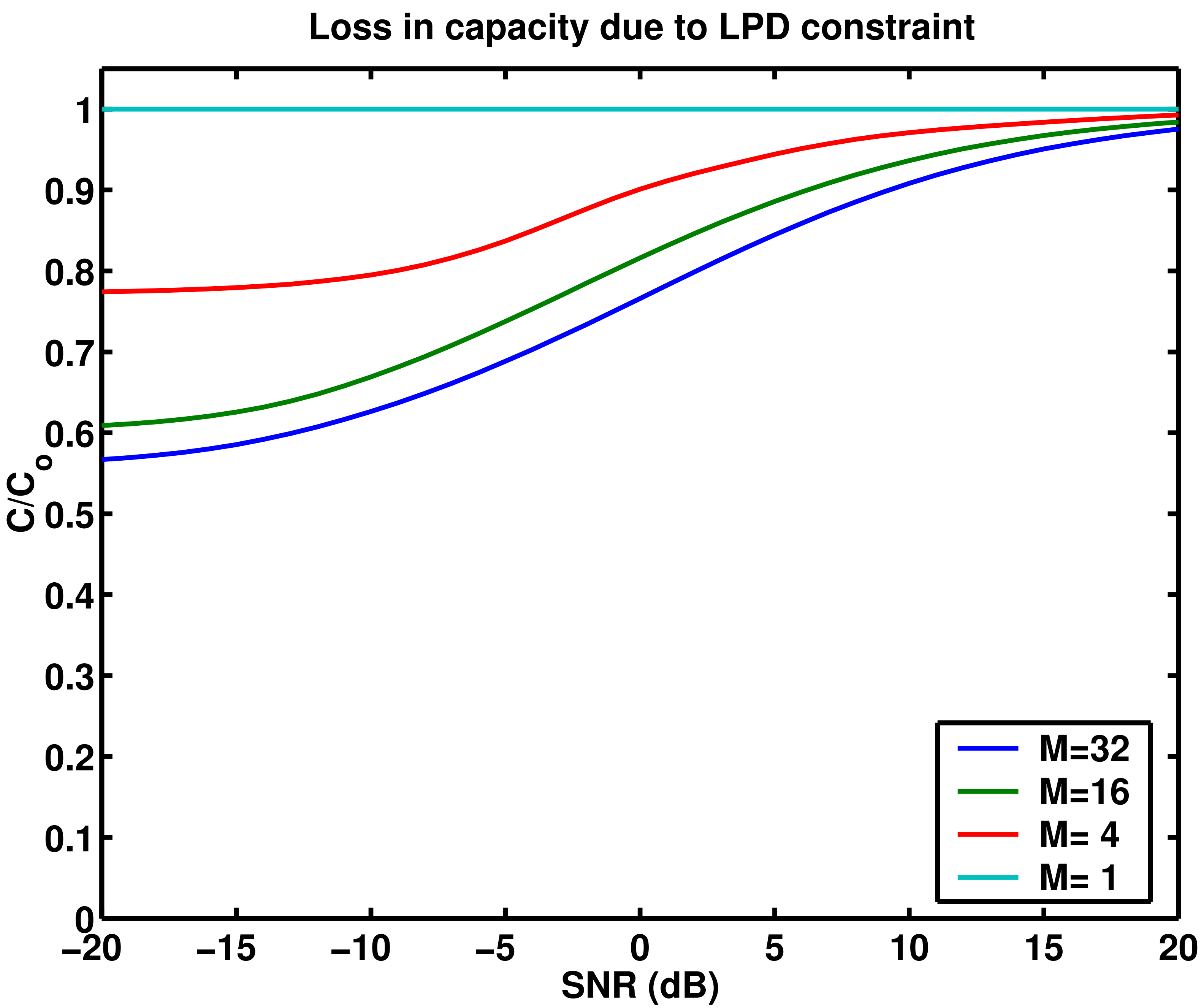


Figure 14. *Loss in σ-capacity due to LPD constraint (N = M)*

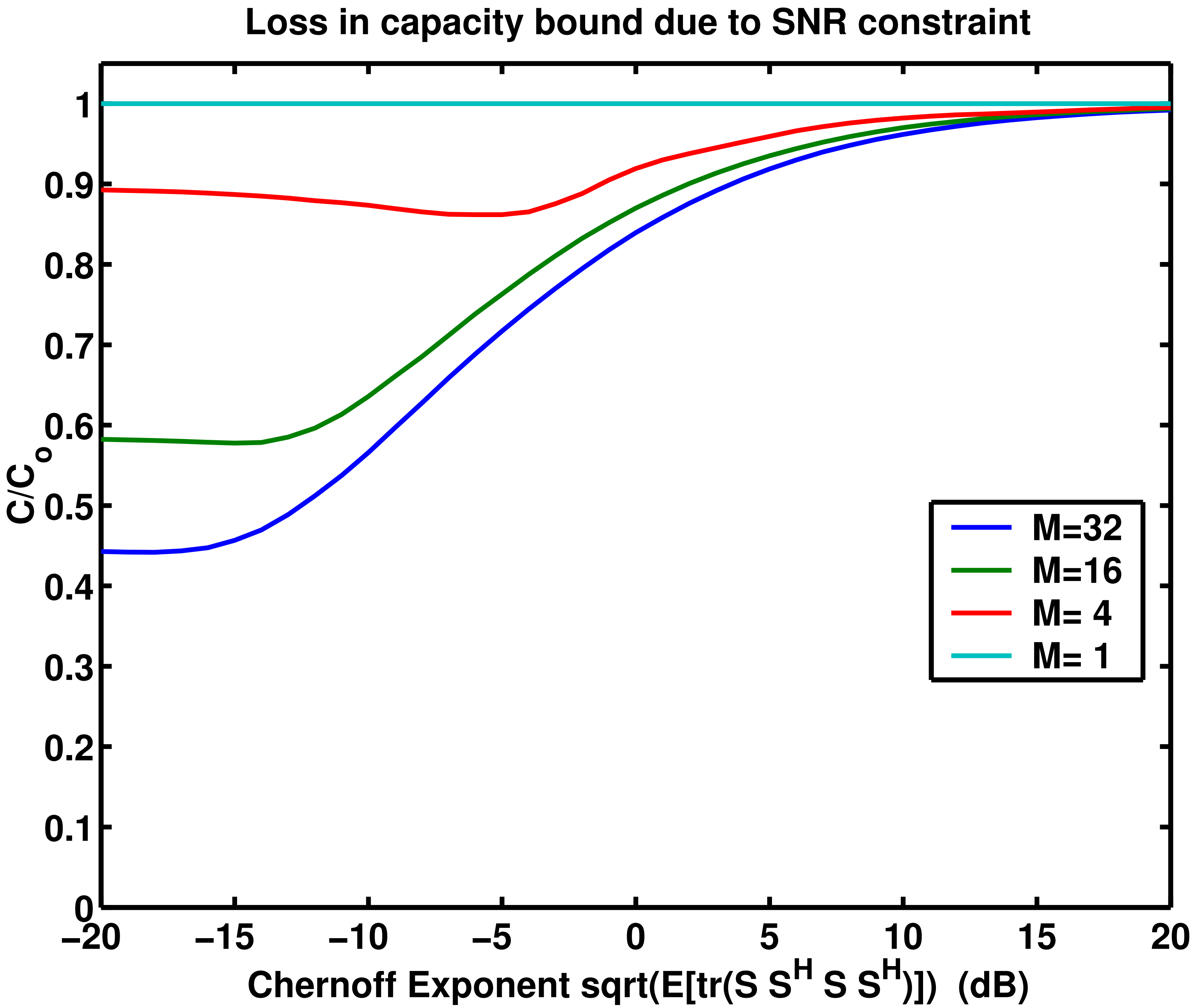


Figure 15. *Loss in κ-capacity due to Pavg constraint (N = M)*

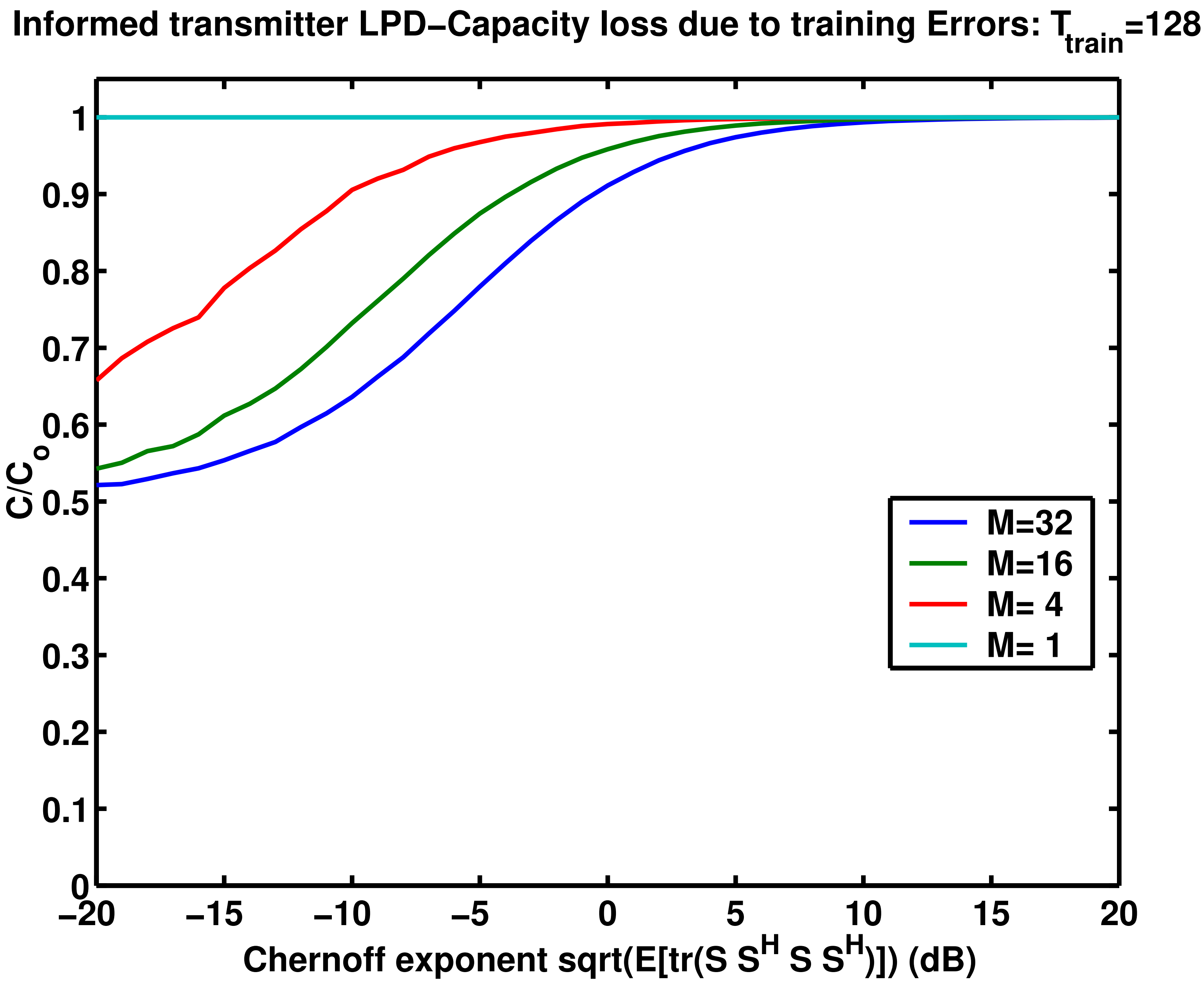


Figure 16. *T/R informed κ-capacity loss due to training errors (N = M)*

Conclusions

1. Capacity and other link level QoS metrics can be analyzed under network security constraints
2. Optimal signalling for LPD- and LPI- constrained *secure* channels is qualitatively different from *open* channels
3. Transmit kurtosis is relevant constraint for ensuring LPD to eavesdropper
4. Smart eavesdropper with info on training sequences can be handled similarly
5. Analogous analysis of R-informed link capacity is of interest
6. Extensions to min and sum capacities will account for network level QoS