Tightened Upper Bounds on the ML Decoding Error Probability of Binary Linear Block Codes and Applications

Moshe Twitto

Department of Electrical Engineering
Technion-Israel Institute of Technology

An M.Sc. Thesis
supervisor: Dr. Igal Sason

March 30, 2006

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Background

- The error performance of coded communication systems rarely admits exact expressions $\Rightarrow$ Tight analytical bounds emerge as a useful tool for assessing performance.

- The union bound is useless at rates above the cutoff rate of the channel $\Rightarrow$ Improved upper bounds which are not subject to the cutoff rate limitations are needed.

Background (Cont.)

- The discovery of turbo-like codes has increased the motivation for deriving and applying tight performance bounds.
- Turbo-like codes are usually decoded by practical, sub-optimal decoding. However, the derivation of bounds on the ML decoding is of interest, as it provides an ultimate indication on the system performance.

Background (Cont.)

- The fine structure of efficient codes is usually not available! $\Rightarrow$ Useful ML bounds rely only on *basic* features, such as the *distance spectrum* of the codes.

- Efficient bounding techniques desirably encompass both *specific* codes as well as *ensembles* of structured codes.

General Concept for the Derivation of Improved Upper Bounds

- The general concept of the improved bounding technique, as introduced by Fano (1960), is based on the inequality

  $$\text{Pr}(\text{word error} \mid \mathbf{c}_0) \leq \text{Pr}(\text{word error},\ \mathbf{y} \in \mathcal{R} \mid \mathbf{c}_0) + \text{Pr}(\mathbf{y} \notin \mathcal{R} \mid \mathbf{c}_0)$$

  $\mathbf{c_0}$–The transmitted codeword (linear code).
  $\mathbf{y}$–The received vector at the output of the channel.
  $\mathcal{R}$–An arbitrary geometrical region.
- The idea is to apply the union bound to the first term in the RHS of the above inequality.
- Special case: $\mathcal{R}$ is the whole n-dimensional space ⇒ The union bound.

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Tangential-Sphere Bound (TSB)

- Introduced by Poltyrev in 1994.
- Consider the transmission of a binary linear code over an AWGN channel, using an equi-energy modulation.
- For the TSB, the region $\mathcal{R}$ is a circular, N dimensional cone, with a half angle θ, and a radius r. Denote it by $C_N(\theta)$.

Tangential-Sphere Bound (Cont.)

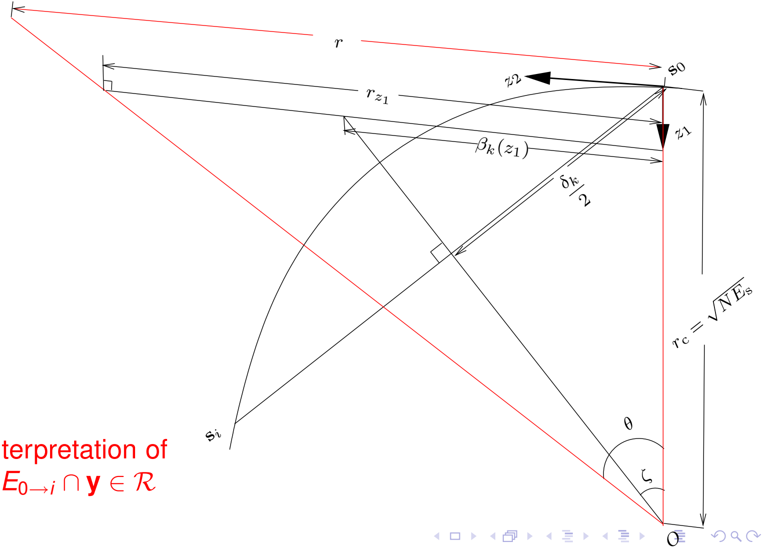
$$\Pr(\text{word error} \mid \mathbf{c}_0) \leq \Pr(\text{word error}, \ \mathbf{y} \in \mathcal{R} \mid \mathbf{c}_0) + \Pr(\mathbf{y} \notin \mathcal{R} \mid \mathbf{c}_0) \tag{1}$$

For the TSB:

- The union bound is applied on the first term in the RHS of (1), which gives:

$$\Pr\left(E|\mathbf{c}_0\right) \leq \sum_{i=1}^{M} \Pr\left(E_{0\to i}, \mathbf{y} \in C_N(\theta) \mid \mathbf{c}_0\right) + \Pr(\mathbf{y} \notin C_N(\theta) \mid \mathbf{c}_0)$$

$E_{0\to i}$–The event of deciding on $\mathbf{c}_i$ rather than $\mathbf{c}_0$.



Geometrical interpretation of the joint event $E_{0 \to i} \cap \mathbf{y} \in \mathcal{R}$

Tangential-Sphere Bound (Cont.)

The optimization is carried over r (r and θ are related).

Two special cases

1. $r \rightarrow \infty$: Particularizes to the union bound.
2. $r = 0$: Equals to 1.

- Shown to be the optimal volume among all the volumes $\mathcal{R}$ which posses some symmetry properties (Yousefi and Khandani).
- One of the tightest upper bounds on the ML-decoding error probability of block codes.

Tangential-Sphere Bound (Cont.)

The optimization is carried over r (r and θ are related).

Two special cases

1. $r \rightarrow \infty$: Particularizes to the union bound.
2. $r = 0$: Equals to 1.

- Shown to be the optimal volume among all the volumes $\mathcal{R}$ which posses some symmetry properties (Yousefi and Khandani).
- One of the tightest upper bounds on the ML-decoding error probability of block codes.

Tangential-Sphere Bound (Cont.)

The final version of the bound is

$$P_e \leq \int_{-\infty}^{\infty} \frac{dz_1}{\sqrt{2\pi}\sigma} e^{-\frac{z_1^2}{2\sigma^2}} \left\{ \begin{array}{l} \displaystyle\sum_{k:\, \frac{\delta_k}{2} \leq \alpha_k} \left\{ A_k \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{z_2^2}{2\sigma^2}} \bar{\gamma}\left(\frac{N-2}{2}, \frac{r_{z_1}^2 - z_2^2}{2\sigma^2}\right) dz_2 \right\} \\ +1 - \bar{\gamma}\left(\frac{N-1}{2}, \frac{r_{z_1}^2}{2\sigma^2}\right) \end{array} \right\}$$

where

$$\bar{\gamma}(a, x) \triangleq \frac{1}{\Gamma(a)} \int_0^x t^{a-1} e^{-t} dt, \quad a, x > 0$$

and A_k denotes the distance spectrum of the code.

Tangential-Sphere Bound (Cont.)

The optimal radius is obtain by the following optimization equation:

$$\begin{cases} \displaystyle\sum_{k:\,\frac{\delta_k}{2}<\alpha_k} A_k \int_0^{\theta_k} \sin^{N-3}\phi \; d\phi = \frac{\sqrt{\pi}\;\Gamma(\frac{N-2}{2})}{\Gamma(\frac{N-1}{2})} \\ \theta_k = \cos^{-1}\left(\frac{\delta_k}{2r}\frac{1}{\sqrt{1-\frac{\delta_k^2}{4NE_s}}}\right) \end{cases}.$$

Notes:

1. The optimal radius is independent of the SNR.
2. There exists a unique solution for the above equation (Sason and Shamai).

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Improvements on the TSB

Reminder:

The TSB is based on the inequality

$$\Pr(\text{word error} \mid \mathbf{c}) \le \Pr(\text{word error}, \ \mathbf{y} \in \mathcal{R} \mid \mathbf{c}) + \Pr(\mathbf{y} \notin \mathcal{R} \mid \mathbf{c}) \tag{2}$$

where the union bound is applied on the first term in the RHS of (2).

Improvement:

Yousefi and Khandani suggest to improve the TSB by applying Hunter's bound rather than the union bound.

Improvements on the TSB

Reminder:

The TSB is based on the inequality

$$\Pr(\text{word error} \mid \mathbf{c}) \leq \Pr(\text{word error},\ \mathbf{y} \in \mathcal{R} \mid \mathbf{c}) + \Pr(\mathbf{y} \notin \mathcal{R} \mid \mathbf{c}) \tag{2}$$

where the union bound is applied on the first term in the RHS of (2).

Improvement:

Yousefi and Khandani suggest to improve the TSB by applying Hunter's bound rather than the union bound.

Improvements on the TSB

Hunter's Bound

Let $\{E_i\}, i = 1, \ldots, M$ designate a set of M events, and E_i^c designates the complementary event of E_i. Then

$$\Pr\left(\bigcup_{i=1}^{M} E_i\right) = \Pr(E_1) + \Pr(E_2 \cap E_1^c) + \ldots + \Pr(E_M \cap E_{M-1}^c \ldots \cap E_1^c)$$

$$\leq \Pr(E_{\pi_1}) + \sum_{i=2}^{M} \Pr(E_{\pi_i} \cap E_{\lambda_i}^c).$$

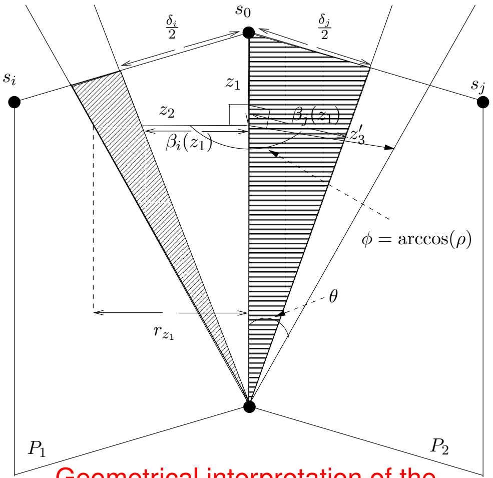
where $\{\pi_1, \ldots, \pi_M\}$ is an arbitrary permutation of the set $\{1, \ldots, M\}$, and $\{\lambda_2, \ldots, \lambda_M\}$ designates an arbitrary sequence of integers where $\lambda_i \in \{\pi_1, \ldots, \pi_{i-1}\}$.

Improvements on the TSB (Cont.)

Applying Hunter's bound yields

$$\Pr\left(\bigcup_{i=1}^{M-1} E_{0\to i}, \mathbf{y} \in C_n(\theta) \mid z_1\right) \leq \min_{\Pi,\Lambda}\Bigg\{\Pr(E_{0\to\pi_1}, \mathbf{y} \in C_n(\theta) \mid z_1) + \sum_{i=2}^{M-1} \Pr(E_{0\to\pi_i}, E^{\mathrm{c}}_{0\to\lambda_i}, \mathbf{y} \in C_n(\theta) \mid z_1)\Bigg\}$$

where $E_{0\to j}$ designates the pairwise error event where the decoder decides on codeword $\mathbf{c}_j$ rather than the transmitted codeword $\mathbf{c}_0$.



Geometrical interpretation of the joint event $E_{0\to i} \cap E^c_{0\to j} \cap \mathbf{y} \in C_N(\theta)$

Improvements on the TSB (Cont.)

Problems:

- The problem of finding the optimal ordering of the events is prohibitively complex.
- The bound depends on the global geometrical properties of the code.

Important fact

The probabilities $\Pr\left(E_{0\rightarrow i}, E^{c}_{0\rightarrow j}\right)$ are monotonic decreasing functions of the correlation coefficients between $\mathbf{c_i}$ and $\mathbf{c}_j$.

Improved Versions of the TSB (Cont.)

- Yousefi et al. derived two versions of improved tangential-sphere bounds. These new bounds (ITSB and AHP bounds) were exemplified to outperform the TSB for short linear block codes.
- In the following, we compare the error exponents associated with the TSB and its improved versions.

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Error Exponents of Improved TSB

Theorem

The upper bounds ITSB, AHP and the TSB have the same error exponent, which is

$$E(c) = \min_{0 \le \delta \le 1} \left\{ \frac{1}{2} \ln \left(1 - \gamma + \gamma e^{-2r(\delta)} \right) + \frac{\gamma \Delta^2 c}{1 + \gamma \Delta^2} \right\}$$

where

$$\gamma = \gamma(\delta) \triangleq \frac{1-\delta}{\delta} \left[\sqrt{\frac{c}{c_0(\delta)} + (1+c)^2 - 1} - (1+c) \right]$$

and

$$c_0(\delta) \triangleq \left(1 - e^{-2r(\delta)} \right) \frac{1-\delta}{2\delta}, \quad r(\delta) = \frac{\ln(A_l)}{N}, \ \Delta = \sqrt{\frac{\delta}{1-\delta}}, \ c \triangleq \frac{E_s}{N_0}.$$

Error Exponents of Improved TSB (Cont.)

Proof's Outline

- Lemma: The ITSB is at least as tight as the TSB for *specific* codes. ⇒ It is at least as tight as the TSB for ensembles of codes.
- Lemma: *Asymptotically*, the AHP is at least as tight as the TSB.
- Lemma: Both the ITSB and the AHP are lower bounded by a certain function $\psi(\mathcal{C})$.
- We use the Chernoff bounding technique to show that the exponential versions of $\psi(\mathcal{C})$ and the TSB are identical.
- ⇒ The error exponents of the TSB, ITSB and AHP bounds are all identical.

Error Exponents of Improved TSB (Cont.)

Proof's Outline

- Lemma: The ITSB is at least as tight as the TSB for *specific* codes. ⇒ It is at least as tight as the TSB for ensembles of codes.
- Lemma: *Asymptotically*, the AHP is at least as tight as the TSB.
- Lemma: Both the ITSB and the AHP are lower bounded by a certain function $\psi(\mathcal{C})$.
- We use the Chernoff bounding technique to show that the exponential versions of $\psi(\mathcal{C})$ and the TSB are identical.
- ⇒ The error exponents of the TSB, ITSB and AHP bounds are all identical.

Error Exponents of Improved TSB (Cont.)

Proof's Outline

- Lemma: The ITSB is at least as tight as the TSB for *specific* codes. $\Rightarrow$ It is at least as tight as the TSB for ensembles of codes.
- Lemma: *Asymptotically*, the AHP is at least as tight as the TSB.
- Lemma: Both the ITSB and the AHP are lower bounded by a certain function $\psi(\mathcal{C})$.
- We use the Chernoff bounding technique to show that the exponential versions of $\psi(\mathcal{C})$ and the TSB are identical.
- $\Rightarrow$ The error exponents of the TSB, ITSB and AHP bounds are all identical.

Error Exponents of Improved TSB (Cont.)

Proof's Outline

- Lemma: The ITSB is at least as tight as the TSB for *specific* codes. $\Rightarrow$ It is at least as tight as the TSB for ensembles of codes.
- Lemma: *Asymptotically*, the AHP is at least as tight as the TSB.
- Lemma: Both the ITSB and the AHP are lower bounded by a certain function $\psi(\mathcal{C})$.
- We use the Chernoff bounding technique to show that the exponential versions of $\psi(\mathcal{C})$ and the TSB are identical.
- $\Rightarrow$ The error exponents of the TSB, ITSB and AHP bounds are all identical.

Outline

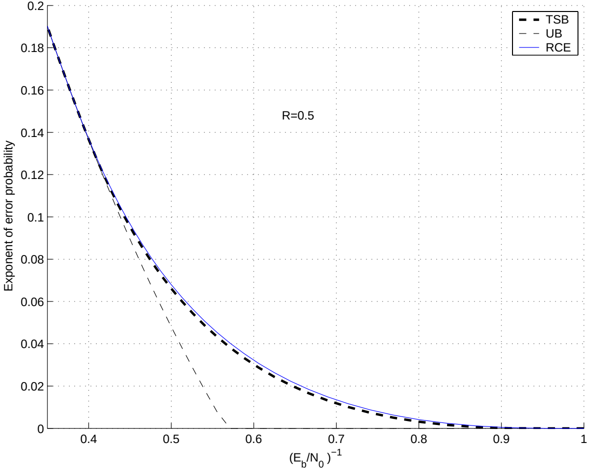
1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Error Exponents of Some Bounds

RCE–Gallager's random coding exponent.

TSB–The error exponent of the tangential-sphere bound.

UB–The error exponent of the union bound.

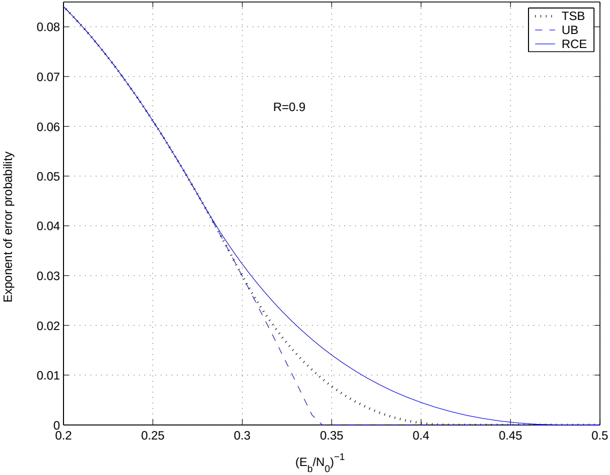


Error Exponents of Some Bounds

RCE–Gallager's random coding exponent.

TSB–The error exponent of the tangential-sphere bound.

UB–The error exponent of the union bound.



Conclusion

- The TSB and its improved versions do not achieve capacity for the ensemble of random linear block codes.
- Tight analytical bounds for structured codes are required, especially for high-rate codes where the weakness of the TSB is more pronounced.

An Overview on the Continuation of this Talk

- In the continuation, we first introduce Gallager's 1965 bound which in general is impractical to evaluate for specific codes.
- The generalization of Duman and Salehi bound by Sason and Shamai is then introduced as an alternative bounding technique which is suitable for both specific codes and ensembles, based on the calculation of their distance spectra.
- Next, the Shulman and Feder bound is obtained as a special case of the DS2 bound (Sason & Shamai, IT 2002) whose alternative derivation is completely different from its original derivation (Shulman & Feder, IT 1999).
- The tightened upper bounds, introduced in this work, are derived by following the alternative derivation of the Shulman and Feder bound as a particular case of the DS2 bound.

The Gallager (1965) Bound

Fixed Codes–Maximum Likelihood (ML) decoding:

$$P_{e|m} \leq \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m) \left(\sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$\lambda, \rho \geq 0$$

- $P_{e|m}$–block error probability conditioned on the transmitted codeword $\mathbf{c}_m$ $(m = 1, 2, \ldots, M)$.
- $\mathbf{c}_m$–the transmitted length-N codeword.
- $\mathbf{y}$–the observation vector (N components).
- $p_N(\mathbf{y}|\mathbf{c})$–the channel transition probability measure (for a block of length N).

The Gallager (1965) Bound

Fixed Codes–Maximum Likelihood (ML) decoding:

$$P_{e|m} \leq \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m) \left(\sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$\lambda, \rho \geq 0$$

Example

- $\rho = 1, \ \lambda = 1/2 \Rightarrow$ Bhattacharyya-Union bound.
- The substitution $\lambda = \frac{1}{1+\rho}$ and optimization over $0 \leq \rho \leq 1$ gives a *tight* bound for orthogonal codes.

- Usually **impractical** to evaluate in terms of distance spectrum of the codes.

The Gallager (1965) Bound

Fixed Codes–Maximum Likelihood (ML) decoding:

$$P_{e|m} \leq \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m) \left(\sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$\lambda, \rho \geq 0$$

Example

- $\rho = 1, \ \lambda = 1/2 \Rightarrow$ Bhattacharyya-Union bound.
- The substitution $\lambda = \frac{1}{1+\rho}$ and optimization over $0 \leq \rho \leq 1$ gives a *tight* bound for orthogonal codes.

- Usually **impractical** to evaluate in terms of distance spectrum of the codes.

Gallager '65 Bound: Random Codes

- Memoryless channel: $p_N(\mathbf{y}|\mathbf{x}) = \prod_{l=1}^{N} p(y_l|x_l)$
- Memoryless input-distribution: $q_N(\mathbf{x}) = \prod_{l=1}^{N} q(x_l)$

The 1965 Gallager Random Coding Bound

$$P_e \leq 2^{-NE_r(R)}$$

where

$$E_r(R) = \max_{0 \leq \rho, q \leq 1} \left(E_0(\rho, q) - \rho R\right)$$

$$E_0(\rho, q) \triangleq -\log_2 \left\{ \sum_{\mathbf{y}} \left(\sum_{\mathbf{x}} q_N(\mathbf{x}) p_N(\mathbf{y}|\mathbf{x})^{\frac{1}{1+\rho}} \right)^{1+\rho} \right\}.$$

Gallager '65 Bound: Random Codes

- Memoryless channel: $p_N(\mathbf{y}|\mathbf{x}) = \prod_{l=1}^{N} p(y_l|x_l)$
- Memoryless input-distribution: $q_N(\mathbf{x}) = \prod_{l=1}^{N} q(x_l)$

The 1965 Gallager Random Coding Bound

$$P_{\mathrm{e}} \le 2^{-NE_{\mathrm{r}}(R)}$$

where

$$E_{\mathrm{r}}(R) = \max_{0 \le \rho, q \le 1} \left(E_0(\rho, q) - \rho R\right)$$

$$E_0(\rho, q) \triangleq -\log_2 \left\{ \sum_{\mathbf{y}} \left(\sum_{\mathbf{x}} q_N(\mathbf{x}) p_N(\mathbf{y}|\mathbf{x})^{\frac{1}{1+\rho}} \right)^{1+\rho} \right\}.$$

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

The second version of Duman and Salehi Bound

- Suggested by Sason and Shamai as a generalization of the Duman and Salehi bound which originally derived for the AWGN channel (Duman Ph.D. dissertation 1998).
- Let $\psi_N^m(\mathbf{y})$ be a measure (may depend on $\mathbf{c}_m$).

The second version of Duman and Salehi Bound (Cont.)

$$P_{e|m} \leq \sum_{\mathbf{y}} \psi_N^m(\mathbf{y})\ \psi_N^m(\mathbf{y})^{-1}\ p_N(\mathbf{y}|\mathbf{c}_m) \left(\sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$= \sum_{\mathbf{y}} \psi_N^m(\mathbf{y}) \left(\psi_N^m(\mathbf{y})^{-\frac{1}{\rho}}\ p_N(\mathbf{y}|\mathbf{c}_m)^{\frac{1}{\rho}} \sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$\lambda, \rho \geq 0.$$

$$\underset{\text{Jensen}}{\leq} \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m)^{\frac{1}{\rho}}\ \psi_N^m(\mathbf{y})^{1-\frac{1}{\rho}} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$0 \leq \rho \leq 1,\ \lambda \geq 0.$$

The second version of Duman and Salehi Bound (Cont.)

$$P_{e|m} \leq \sum_{\mathbf{y}} \psi_N^m(\mathbf{y})\, \psi_N^m(\mathbf{y})^{-1}\, p_N(\mathbf{y}|\mathbf{c}_m) \left(\sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$= \sum_{\mathbf{y}} \psi_N^m(\mathbf{y}) \left(\psi_N^m(\mathbf{y})^{-\frac{1}{\rho}}\, p_N(\mathbf{y}|\mathbf{c}_m)^{\frac{1}{\rho}} \sum_{m' \neq m} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$\lambda, \rho \geq 0.$$

$$\underset{\text{Jensen}}{\leq} \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m)^{\frac{1}{\rho}}\, \psi_N^m(\mathbf{y})^{1-\frac{1}{\rho}} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho}$$

$$0 \leq \rho \leq 1, \;\; \lambda \geq 0.$$

The second version of Duman and Salehi Bound (Cont.)

Let

$$\psi_N^m(\mathbf{y}) = \frac{G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)}{\sum_{\mathbf{y}} G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)}$$

$\Rightarrow$

$$P_{e|m} \le \left(\sum_{\mathbf{y}} G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)\right)^{1-\rho}$$

$$\cdot \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m)\; G_N^m(\mathbf{y})^{1-\frac{1}{\rho}} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)}\right)^{\lambda}\right)^{\rho},$$

$$0 \le \rho \le 1, \quad \lambda \ge 0.$$

The second version of Duman and Salehi Bound (Cont.)

Let

$$\psi_N^m(\mathbf{y}) = \frac{G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)}{\sum_{\mathbf{y}} G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)}$$

$\Rightarrow$

$$P_{e|m} \leq \left(\sum_{\mathbf{y}} G_N^m(\mathbf{y})\; p_N(\mathbf{y}|\mathbf{c}_m)\right)^{1-\rho} \cdot \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m)\; G_N^m(\mathbf{y})^{1-\frac{1}{\rho}} \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)}\right)^{\lambda}\right)^{\rho},$$

$$0 \leq \rho \leq 1, \quad \lambda \geq 0.$$

Advantages

- Gives results in term of basic code features (such as distance spectrum) to structured codes and ensembles.
- Achieve capacity for the ensemble of random codes.
- Many upper bounds are particular cases of this bound.

Drawback

Computationally Hard to compute.

Advantages

- Gives results in term of basic code features (such as distance spectrum) to structured codes and ensembles.
- Achieve capacity for the ensemble of random codes.
- Many upper bounds are particular cases of this bound.

Drawback

Computationally Hard to compute.

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

The Shulman and Feder Bound (SFB)

- Adaption of the random-coding bound to structured ensembles of block codes.
- For a binary linear block code (or ensemble), $\mathcal{C}$, with distance spectrum $\{A_l\}$ the SFB reads

$$P_\mathrm{e} \leq 2^{-NE_\mathrm{r}\left(R+\frac{\log \alpha(\mathcal{C})}{N}\right)}$$

where

$$\alpha(\mathcal{C}) \triangleq \max_{1\leq l\leq N} \frac{A_l}{2^{-N(1-R)} \binom{N}{l}}$$

and E_r is the random coding error exponent.

The Shulman and Feder Bound (Cont.)

Advantage

Clearly, the SFB reproduces the random coding bound for the ensemble of random linear block codes.

Drawback

Depends on the *maximal* ratio between the distance spectrum of the code and the binomial distribution $\Rightarrow$ May not be tight for some efficient codes.

The SFB can be reproduced as a particular case of the DS2 bound [Sason & Shamai].

Alternative proof for the SFB Sason&Shamai.

- Assume that the transmission takes place over an arbitrary memoryless binary-input output-symmetric (MBIOS) channel. So
$$p_N(\mathbf{y}|\mathbf{c}_m) = \prod_{i=1}^{N} p(y_i|c_{m,i}).$$
- Let $G_N^0(\mathbf{y}) = \prod_{i=1}^{N} g(y_i)$.

Alternative proof for the SFB (Cont.)

The DS2 gives

$$
\begin{aligned}
P_{\mathrm{e}} &= P_{\mathrm{e}|0} \\
&\leq \left(\sum_y g(y)\, p(y|0)\right)^{N(1-\rho)} \qquad \begin{array}{c}\lambda \geq 0, \\ 0 \leq \rho \leq 1\end{array} \\
&\quad \cdot \left\{ \sum_{l=1}^{N} A_l \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)\right)^{N-l} \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)^{1-\lambda} p(y|1)^{\lambda}\right)^{l} \right\}^{\rho} \\
&\leq \left(\max_{0<l\leq N} \frac{A_l}{2^{-N(1-R)}\binom{N}{l}}\right)^{\rho} \left(\sum_y g(y)\, p(y|0)\right)^{N(1-\rho)} \quad 2^{-N(1-R)\rho} \\
&\quad \cdot \left\{ \sum_y g(y)^{1-\frac{1}{\rho}} p(y|0) + \sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)^{1-\lambda} p(y|1)^{\lambda} \right\}^{N\rho} .
\end{aligned}
$$

Alternative proof for the SFB (Cont.)

By setting

$$g(y) = \left[\frac{1}{2}p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2}p(y|1)^{\frac{1}{1+\rho}}\right]^{\rho} p(y|0)^{-\frac{\rho}{1+\rho}}$$

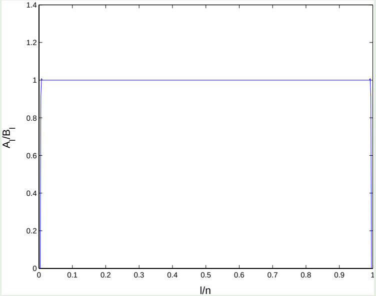
and using the symmetry of the channel (where $p(y|0) = p(-y|1)$), the SFB follows readily.

Distance Spectra of Turbo-Like Ensembles

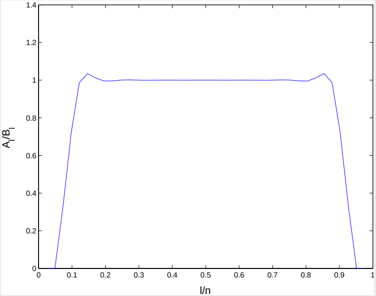
- Let $B_l \triangleq 2^{-N(1-R)}\binom{N}{l} \qquad l = 0, 1, \ldots, N$ designate the average distance spectrum of random code.
- The tightness of the SFB depends on the *maximal* ratio between the spectrum of the code (ensemble) and the average spectrum of random code of the same rate and length.

Distance Spectrums of Turbo-Like Ensembles (Cont.)

Example: Turbo-Hamming codes.



Turbo-Hamming, R=0.965 bits/Sym



Multiple Turbo-Hamming, R=0.634 bits/Sym

Partitioning of $\mathcal{C}$ into two subcodes

Observation:

For a relatively large portion of the Hamming weights, the distance spectrum of the code resembles the binomial distribution of random codes.

Suggestion (Miller & Burshtein):

- Partition the original code into two subcodes, $\mathcal{C}'$ and $\mathcal{C}''$; $\mathcal{C}'$ contains all the codewords with Hamming weight $l \in \mathcal{U} \subseteq \{1, 2, \ldots, N\}$, while $\mathcal{C}''$ contains the other codewords. Both subcodes contain the all-zero codeword.
- The union bound provides $P_\mathrm{e} = P_{\mathrm{e}|0} \leq P_{\mathrm{e}|0}(\mathcal{C}') + P_{\mathrm{e}|0}(\mathcal{C}'')$.
- Use the SFB as an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}')$, and apply the UB on $P_{\mathrm{e}|0}(\mathcal{C}'')$.

Partitioning of $\mathcal{C}$ into two subcodes

Observation:

For a relatively large portion of the Hamming weights, the distance spectrum of the code resembles the binomial distribution of random codes.

Suggestion (Miller & Burshtein):

- Partition the original code into two subcodes, $\mathcal{C}'$ and $\mathcal{C}''$; $\mathcal{C}'$ contains all the codewords with Hamming weight $l \in \mathcal{U} \subseteq \{1, 2, \ldots, N\}$, while $\mathcal{C}''$ contains the other codewords. Both subcodes contain the all-zero codeword.
- The union bound provides $P_{\mathrm{e}} = P_{\mathrm{e}|0} \leq P_{\mathrm{e}|0}(\mathcal{C}') + P_{\mathrm{e}|0}(\mathcal{C}'')$.
- Use the SFB as an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}')$, and apply the UB on $P_{\mathrm{e}|0}(\mathcal{C}'')$.

Partitioning...

The problem of finding the optimal partitioning is very complex. In our work, we suggest a certain partitioning which depends on the ratio between the distance spectrum of the code and the binomial distribution (where the latter characterizes the distance spectra of the ensemble of fully random block codes).

Outline

1. Background
2. The Tangential-Sphere Bound and Improved Versions
   - Tangential-Sphere Bound (TSB)
   - Improvements on the TSB
   - Error Exponents of Improved TSB
   - Numerical Results for Error Exponents
3. Gallager (1965) Bound
   - DS2 Bound
   - Shulman and Feder Bound.
4. Tightened Upper Bounds
   - Upper Bounds on the Block/Bit Error Probability
   - Expurgation
5. Applications

Upper Bound on the Block Error Probability

Theorem (Modified Shulman and Feder Bound).

Let $\mathcal{C}$ be partitioned into two subcodes $\mathcal{C}'$ and $\mathcal{C}''$, as mentioned. Then, for an MBIOS channel:

$$P_{\mathrm{e}} \leq P_{\mathrm{e}|0}(\mathcal{C}') + P_{\mathrm{e}|0}(\mathcal{C}'')$$

where

$$P_{\mathrm{e}|0}(\mathcal{C}') \leq \mathrm{SFB}(\rho) \cdot \left[\sum_{l \in \mathcal{U}} \binom{N}{l} \left(\frac{A(\rho)}{A(\rho)+B(\rho)} \right)^{l} \left(\frac{B(\rho)}{A(\rho)+B(\rho)} \right)^{N-l} \right]^{\rho}, \quad 0 \leq \rho \leq 1$$

$$A(\rho) \triangleq \sum_{y} \left\{ [p(y|0)p(y|1)]^{\frac{1}{1+\rho}} \left[\frac{1}{2} p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2} p(y|1)^{\frac{1}{1+\rho}} \right]^{\rho-1} \right\}$$

$$B(\rho) \triangleq \sum_{y} \left\{ p(y|0)^{\frac{2}{1+\rho}} \left[\frac{1}{2} p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2} p(y|1)^{\frac{1}{1+\rho}} \right]^{\rho-1} \right\}.$$

Upper Bound on the Block Error Probability

The Essence of the Proof.

Instead

$$P_{e|0}(\mathcal{C}') \le \left(\max_{l\in\mathcal{U}} \frac{A_l}{2^{-N(1-R)}\binom{N}{l}}\right)^{\rho} \left(\sum_y g(y)\; p(y|0)\right)^{N(1-\rho)} \qquad 2^{-N(1-R)\rho}$$

$$\cdot \left\{\sum_{l=1}^{N}\binom{N}{l}\left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)\right)^{N-l}\left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)^{1-\lambda} p(y|1)^{\lambda}\right)^{l}\right\}^{\rho}.$$

Note

Since typically $\mathcal{C}''$ contains only a small fraction of the codewords in $\mathcal{C}$, we use the simple UB as an upper bound on $P_{e|0}(\mathcal{C}'')$.

Upper Bound on the Block Error Probability

The Essence of the Proof.

We start the derivation of the bound by writing

$$P_{\mathrm{e}|0}(\mathcal{C}') \leq \left(\max_{l \in \mathcal{U}} \frac{A_l}{2^{-N(1-R)} \binom{N}{l}} \right)^{\rho} \left(\sum_y g(y)\; p(y|0) \right)^{N(1-\rho)} \qquad 2^{-N(1-R)\rho}$$

$$\cdot \left\{ {\color{red}\sum_{l \in \mathcal{U}}} \binom{N}{l} \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0) \right)^{N-l} \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)^{1-\lambda} p(y|1)^{\lambda} \right)^{l} \right\}^{\rho} .$$

and rely on the symmetry properties of the MBIOS channel.

Note

Since typically $\mathcal{C}''$ contains only a small fraction of the codewords in $\mathcal{C}$, we use the simple UB as an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}'')$.

Upper Bound on the Block Error Probability

The Essence of the Proof.

We start the derivation of the bound by writing

$$P_{e|0}(\mathcal{C}') \le \left(\max_{l\in\mathcal{U}} \frac{A_l}{2^{-N(1-R)}\binom{N}{l}}\right)^{\rho} \left(\sum_y g(y)\; p(y|0)\right)^{N(1-\rho)} \quad 2^{-N(1-R)\rho}$$

$$\cdot \left\{ \sum_{l\in\mathcal{U}} \binom{N}{l} \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)\right)^{N-l} \left(\sum_y g(y)^{1-\frac{1}{\rho}} p(y|0)^{1-\lambda} p(y|1)^{\lambda}\right)^{l} \right\}^{\rho}.$$

and rely on the symmetry properties of the MBIOS channel.

Note

Since typically $\mathcal{C}''$ contains only a small fraction of the codewords in $\mathcal{C}$, we use the simple UB as an upper bound on $P_{e|0}(\mathcal{C}'')$.

Upper Bounds on the BER

- The original SFB was derived as an upper bound on the **block** error probability.
- Sason and Shamai derived the bit-error version of the DS2 for fully interleaved fading channels with perfect channel state information at the receiver.
- We generalize the result of Sason and Shamai to arbitrary MBIOS channels.

The SFB on the BER

Theorem. (The SFB Version on the BER)

- Let $\mathcal{C}$ be an (N, K) binary linear block code.
- Assume an MBIOS channel.
- Let $A_{w,l}$ designate the number of codewords in $\mathcal{C}$ which are encoded by information bits whose Hamming weight is w and their Hamming weight after encoding is l.
- The BER is upper bound by

$$P_{\mathrm{b}} \leq 2^{-NE_{\mathrm{r}}\left(R+\frac{\log \alpha_{\mathrm{b}}(\mathcal{C})}{N}\right)}$$

where

$$\alpha_{\mathrm{b}}(\mathcal{C}) \triangleq \max_{0<l\leq N} \frac{A'_l}{2^{-N(1-R)}\binom{N}{l}}, \qquad A'_l \triangleq \sum_{w=1}^{K} \left(\frac{w}{K}\right) A_{w,l}.$$

Partitioning.

- Partitioning of the code may further improve the tightness of the SFB on the BER.
- The threshold in the partitioning algorithm suggested above is now slightly above $\frac{1}{2}$ (instead of 1).
- By the union bound

$$P_{\mathrm{b}} = P_{\mathrm{b}|0} \leq P_{\mathrm{b}|0}(\mathcal{C}') + P_{\mathrm{b}|0}(\mathcal{C}'').$$

Partitioning (Cont.)

- The conditional SFB on the BER of $\mathcal{C}'$ is

$$P_{\mathrm{b}|0}(\mathcal{C}') \leq 2^{-NE_{\mathrm{r}}\left(R+\frac{\log \alpha_{\mathrm{b}}(\mathcal{C}')}{N}\right)}$$

where

$$\alpha_{\mathrm{b}}(\mathcal{C}') \triangleq \max_{l \in \mathcal{U}} \frac{A'_l}{B_l}.$$

- We use the bit-error version of the UB as an upper bound on $P_{\mathrm{b}|0}(\mathcal{C}'')$.

Modified SFB on the Bit Error Probability

In order to tighten the resulting bound, we obtain the bit-error version of the modified SFB.

Modified SFB on the Bit Error Probability

The bit error probability of a binary linear block code transmitted over an MBIOS channel is upper bounded by

$$P_{\mathrm{b}} \leq P_{\mathrm{b}|0}(\mathcal{C}') + P_{\mathrm{b}|0}(\mathcal{C}'')$$

where

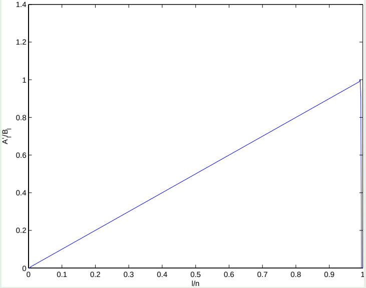
$$P_{\mathrm{b}|0}(\mathcal{C}') \leq 2^{-N\left(E_0(\rho)-\rho\left(R+\frac{\log\left(\alpha_{\mathrm{b}}(\mathcal{C}')\right)}{N}\right)\right)}\left[\sum_{l\in\mathcal{U}}\binom{N}{l}\left(\frac{A(\rho)}{A(\rho)+B(\rho)}\right)^{l}\left(\frac{B(\rho)}{A(\rho)+B(\rho)}\right)^{N-l}\right]^{\rho}$$

$$0 \leq \rho \leq 1.$$

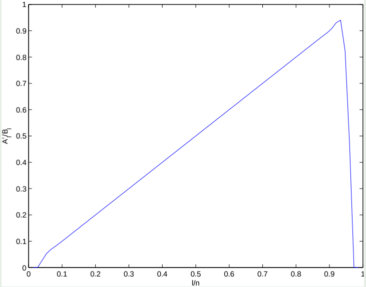
The Simplified DS2 Bound.

The terms $\frac{A'_l}{B_l}$ changes considerably with l.

Example: $\frac{A'_l}{B_l}$ for some ensembles of turbo-like codes.



Turbo-Hamming, R=0.965 bits/Sym



Multiple Turbo-Hamming, R=0.76 bits/Sym

The Simplified DS2 Bound (Cont.)

- The terms $\frac{A_l}{B_l}$ varying slowly over a large range of Hamming weights $\Rightarrow$ Taking out the maximal value of $\frac{A_l}{B_l}$ from the summation does not expect to lessening the bound on the *block* error probability.
- The values of $\frac{A'_l}{B_l}$ change considerably with l.
  $\Rightarrow$ Taking out the maximal value of $\frac{A_l}{B_l}$ is expected to significantly reduce the tightness of the bound on the *bit* error probability.
- A tighter upper bound on the BER is needed.

Theorem. Simplified DS2 Bound

- Let $\mathcal{C}$ be a binary linear block code of length N and rate R, and assume the communication takes place over an MBIOS channel.
- Let
$$A_l{}'(\mathcal{C}') \triangleq \begin{cases} \sum_{w=1}^{NR} \left(\frac{w}{NR}\right) A_{w,l} & \text{if } l \in \mathcal{U} \\ 0 & \text{otherwise} \end{cases} .$$
- The bit error probability is upper bounded by
$$P_{\mathrm{b}} \leq P_{\mathrm{b}|0}(\mathcal{C}') + P_{\mathrm{b}|0}(\mathcal{C}'')$$

where

$$P_{\mathrm{b}|0}(\mathcal{C}') \leq 2^{-N\left(E_0(\rho) - \rho\left(R + \frac{\log \bar{\alpha}_\rho(\mathcal{C}')}{N}\right)\right)}, \quad 0 \leq \rho \leq 1$$

$$\bar{\alpha}_\rho(\mathcal{C}') \triangleq \sum_{l=0}^{N} \left\{ \frac{A_l'(\mathcal{C}')}{2^{-N(1-R)} \binom{N}{l}} \cdot \binom{N}{l} \left(\frac{A(\rho)}{A(\rho)+B(\rho)}\right)^l \left(\frac{B(\rho)}{A(\rho)+B(\rho)}\right)^{N-l} \right\}.$$

The Simplified DS2 Bound (Cont.)

Notes:

- The same bound can be applied to *block* error probability, with the replacement of $A'_l(\mathcal{C}')$ with $A'_l(\mathcal{C}')$.
- Depends on the *average* ratio of $\frac{A'_l}{B_l}$ (instead of the *maximal* ratio) ⇒ yields a tighter bounding technique than the SFB.

Outline

1 Background

2 The Tangential-Sphere Bound and Improved Versions
- Tangential-Sphere Bound (TSB)
- Improvements on the TSB
- Error Exponents of Improved TSB
- Numerical Results for Error Exponents

3 Gallager (1965) Bound
- DS2 Bound
- Shulman and Feder Bound.

4 Tightened Upper Bounds
- Upper Bounds on the Block/Bit Error Probability
- Expurgation

5 Applications

Expurgation

Definition (Voronoi region).

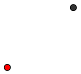
Let $\mathcal{C}$ be a code which is transmitted over an AWGN channel, and let $\mathbf{c}_0$ be a codeword of $\mathcal{C}$. The Voronoi region of $\mathbf{c}_0$ is the set of vectors in $\mathbb{R}^N$ that are closest to $\mathbf{c}_0$.

Definition (Voronoi neighbor).

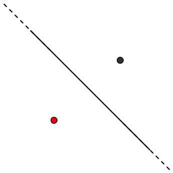
The minimal set of codewords that determine the Voronoi region of $\mathbf{c}_0$ forms the set of Voronoi neighbors of $\mathbf{c}_0$.

Expurgation–example.

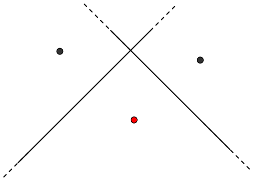
Expurgation–example.



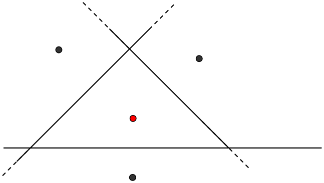
Expurgation–example.



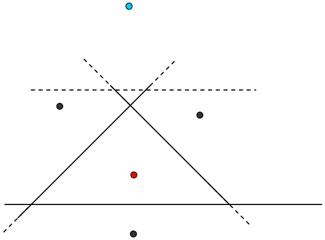
Expurgation–example.



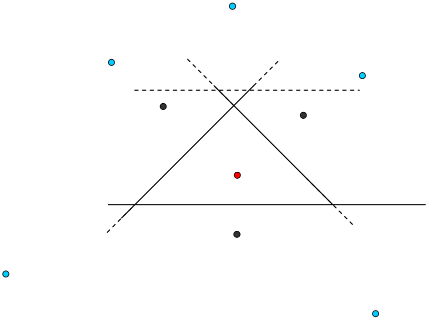
Expurgation–example.



Expurgation–example.



Expurgation–example.



🔴 - Transmitted vector.

● - Voronoi neighbor.

🔵 - Non-neighbor.

Expurgation (Cont.)

- Let $\mathcal{C}$ be a linear block code.
- Let $\mathcal{C}^{\text{ex}}$ denote the *expurgated code* which contains all the Voronoi neighbors of $\mathbf{c}_0$.
- Then
$$P_{\text{e}}(\mathcal{C}) = P_{\text{e}|0}(\mathcal{C}) = P_{\text{e}|0}(\mathcal{C}^{\text{ex}}).$$
- Any upper bound which solely depends on the distance spectrum of the code can be tightened by replacing the distance spectrum with the expurgated spectrum (the weight spectrum of $\mathcal{C}^{\text{ex}}$).

Expurgation (Cont.)

Theorem (Agrell)

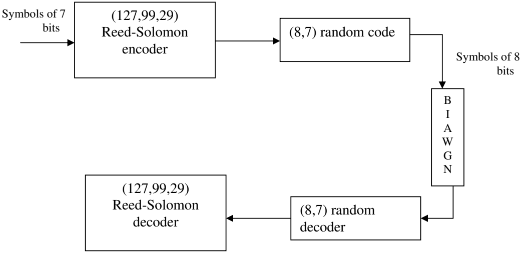
For any binary linear block code with rate R and length N

- All the codeword with Hamming weight less than $2d_{\min}$ are Voronoi neighbors of the all-zero codeword.
- All the codewords with Hamming weight larger than $N(1-R)+1$ are *not* Voronoi neighbors of the all-zero codeword.

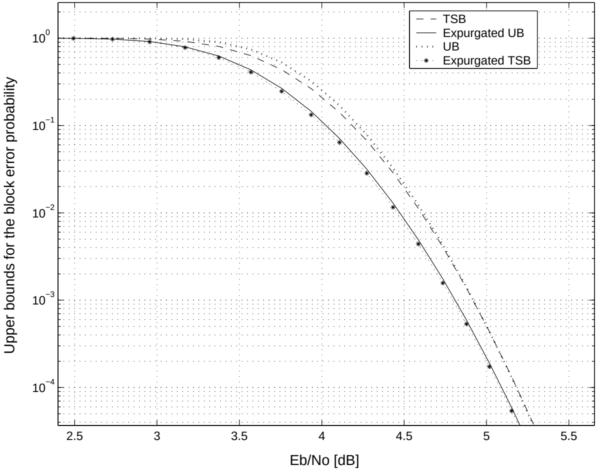
Corollary

A trivial expurgation can be achieved by expurgating all the codeword with Hamming weight larger than $N(1-R)+1$.

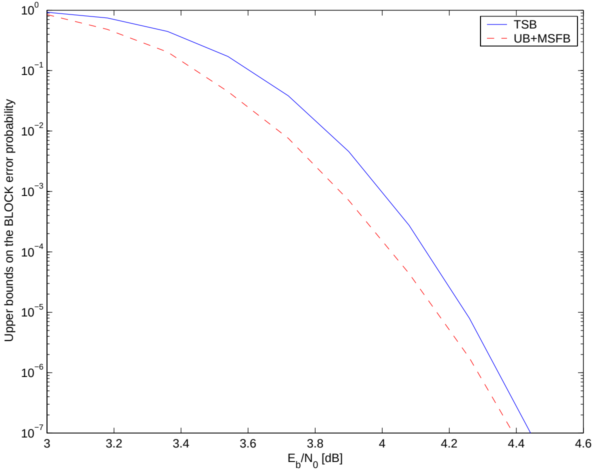
Applications: Serially Concatenated Codes



Applications: Serially Concatenated Codes

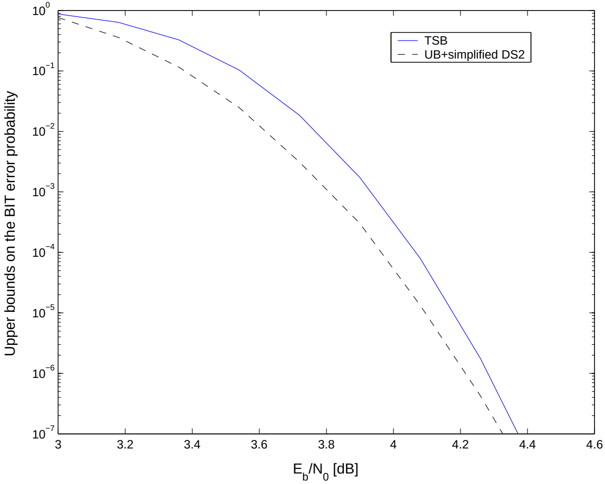


Applications: Random Turbo-Block Codes



$N = 1072$, $R = 0.932$bits/Sym

Applications: Random Turbo-Block Codes



$N = 1072$, $R = 0.932$bits/Sym

Summary

- The TSB and its improved versions do not achieve capacity, and possess the same error exponent.
- Tightened versions of the Shulman and Feder bound were derived based on the general concept of the DS2 bounding technique, and by revisiting the alternative proof for reproducing the Shulman and Feder bound as a particular case of the DS2 bound.
- An expurgation of the distance spectrum of the code further tightens the resulting upper bounds.
- The tightened upper bounds derived in this work were demonstrated to outperform the TSB in some cases, especially for ensembles of turbo-like codes of high rate.

Further Reading

- M. Twitto, I. Sason and S. Shamai, “Tightened upper bounds on the ML decoding error probability of binary linear codes,” submitted to the *IEEE Trans. on Information Theory*, February 2006.
- M. Twitto and I. Sason, “On the Error Exponents of Some Improved Tangential-Sphere Bounds,” submitted to the *IEEE Trans. on Information Theory*, March 2006.
- I. Sason and S. Shamai, “Performance analysis of linear codes under maximum-likelihood decoding: a tutorial,” an *invited monograph* (247 pages), accepted to *Foundations and Trends in Communications and Information Theory*, NOW Publishers, Delft, the Netherlands, March 2006.
- Papers can be found at http://www.ee.technion.ac.il/people/sason/

Thank you!