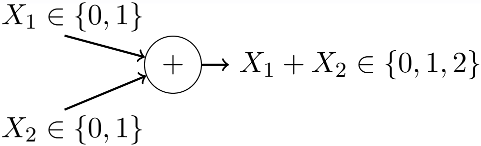
A VC-Dimension-Based Outer Bound on the Zero-Error Capacity of the Binary Adder Channel

Or Ordentlich
Joint work with Ofer Shayevitz

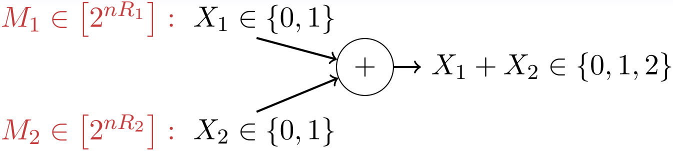
ISIT 2015, Hong Kong

June 19, 2015

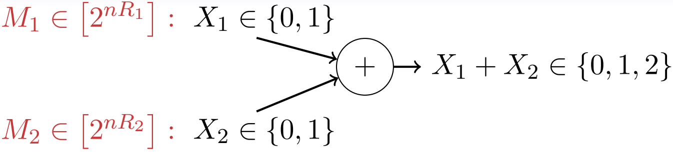
The Binary Adder Channel



The Binary Adder Channel

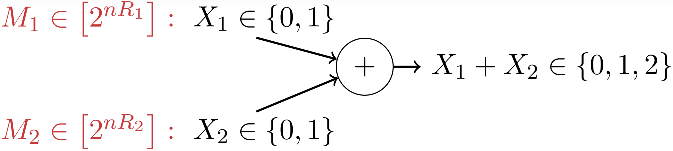


The Binary Adder Channel



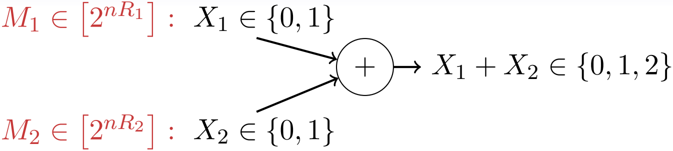
- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$

The Binary Adder Channel



- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$
- Error $\Leftrightarrow$ $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{c}_1' + \mathbf{c}_2'$ for $\mathbf{c}_1, \mathbf{c}_1' \in \mathcal{C}_1,\ \mathbf{c}_2, \mathbf{c}_2' \in \mathcal{C}_2$

THE BINARY ADDER CHANNEL



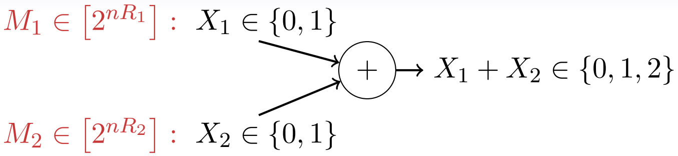
- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$
- Error $\Leftrightarrow$ $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{c}_1' + \mathbf{c}_2'$ for $\mathbf{c}_1, \mathbf{c}_1' \in \mathcal{C}_1,\ \mathbf{c}_2, \mathbf{c}_2' \in \mathcal{C}_2$

Shannon Capacity Region (vanishing error)

- Simple MAC channel... the region is

$$R_1 \leq 1$$
$$R_2 \leq 1$$
$$R_1 + R_2 \leq 1.5$$

The Binary Adder Channel

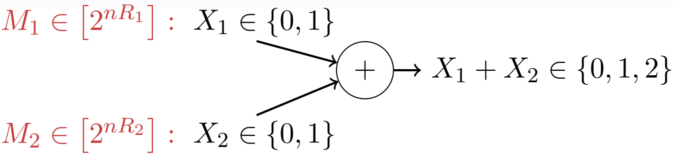


- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$
- Error $\Leftrightarrow$ $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{c}_1' + \mathbf{c}_2'$ for $\mathbf{c}_1, \mathbf{c}_1' \in \mathcal{C}_1, \ \mathbf{c}_2, \mathbf{c}_2' \in \mathcal{C}_2$

Zero-Error Capacity Region

- No errors allowed (no collisions)
- All sums are different

The Binary Adder Channel

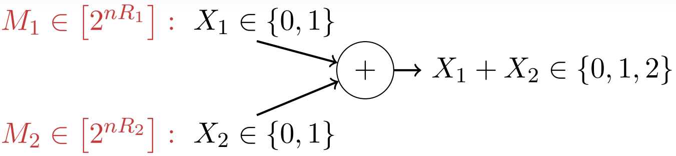


- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$
- Error $\Leftrightarrow$ $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{c}_1' + \mathbf{c}_2'$ for $\mathbf{c}_1, \mathbf{c}_1' \in \mathcal{C}_1,\ \mathbf{c}_2, \mathbf{c}_2' \in \mathcal{C}_2$

Zero-Error Capacity Region

- No errors allowed (no collisions)
- All sums are different
- Capacity region unknown
- Large gap between best inner and outer bounds

The Binary Adder Channel

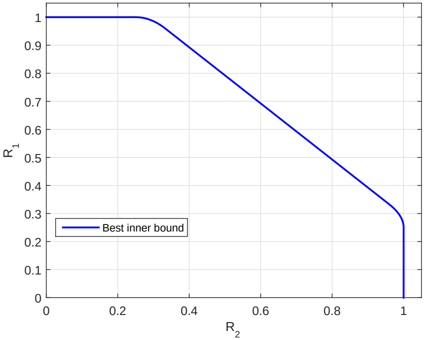


- Codebooks $\mathcal{C}_1, \mathcal{C}_2 \subseteq \{0,1\}^n$ with $|\mathcal{C}_1| = 2^{nR_1}$ and $|\mathcal{C}_2| = 2^{nR_2}$
- Error $\Leftrightarrow$ $\mathbf{c}_1 + \mathbf{c}_2 = \mathbf{c}_1' + \mathbf{c}_2'$ for $\mathbf{c}_1, \mathbf{c}_1' \in \mathcal{C}_1,\ \mathbf{c}_2, \mathbf{c}_2' \in \mathcal{C}_2$

Zero-Error Capacity Region

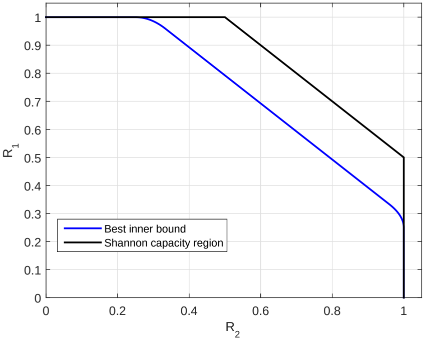
- No errors allowed (no collisions)
- All sums are different
- Capacity region unknown
- Large gap between best inner and outer bounds
- **In this talk: Outer bound improved**

KNOWN BOUNDS

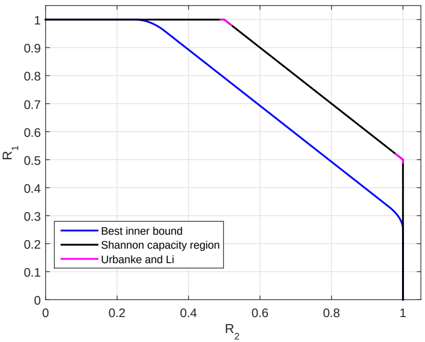


[*Lindström '69*], [*Kasami & Lin '76*], [*Weldon '78*], [*Peterson & Costello '79*], [*Khachatrian '82*], [*van Tilborg '83*], [*Kasami et al '83*], [*van der Braak & van Tilborg '85*], [*Guo & Watanabe '91, '92*], [*Blake '94*], [*Ahlswede & Balakirsky '99*], [*Mattas & Ostergard '05*]

Known Bounds



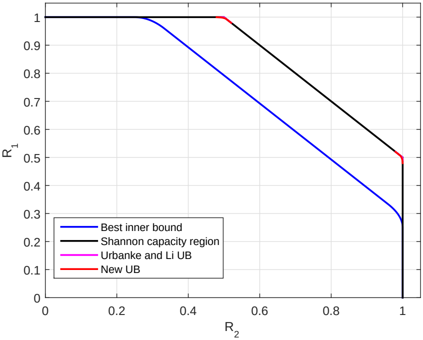
KNOWN BOUNDS



[*Urbanke & Li 1998*]

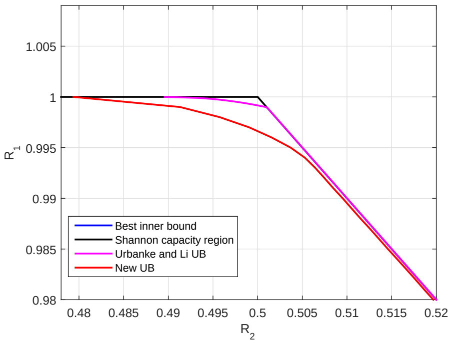
- For $R_1 = 1$: $0.25 \leq R_2 < 0.49216$ [*Kasami et al '83*], [*Urbanke & Li '98*]

Known Bounds



- For $R_1 = 1$: $0.25 \leq R_2 < \sout{0.49216}$ 0.4798 (this talk)

Known Bounds



- For $R_1 = 1$: $0.25 \leq R_2 < \sout{0.49216}$ 0.4798 (this talk)

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1,\ldots,n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1, \ldots, n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S

$$\mathbf{c} = 011101, \; S = \{2,3,5,6\}$$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1,\ldots,n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S

$$\mathbf{c} = 011101,\ S = \{2,3,5,6\} \quad \Rightarrow \quad \mathbf{c}(S) = 1101$$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \overset{\text{def}}{=} \{1, \ldots, n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \overset{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1, \ldots, n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \stackrel{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

- S is *shattered by* $\mathcal{C}$ if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \overset{\text{def}}{=} \{1, \ldots, n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \overset{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

- S is *shattered by* $\mathcal{C}$ if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors

$\mathcal{C} = \{101100, 011101, 100110, 000111\}$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1,\ldots,n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \stackrel{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

- S is *shattered by* $\mathcal{C}$ if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors

$$\mathcal{C} = \{101100, 011101, 100110, 000111\} \Rightarrow \mathcal{S} = \{5,6\} \text{ shattered}$$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1,\ldots,n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \stackrel{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

- S is *shattered by* $\mathcal{C}$ if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors

$\mathcal{C} = \{101100, 011101, 100110, 000111\}$

Projection and Shattering

- Let $\mathbf{c} \in \{0,1\}^n$
- Let $S \subseteq [n] \stackrel{\text{def}}{=} \{1,\ldots,n\}$ be some subset of coordinates
- $\mathbf{c}(S) \in \{0,1\}^{|S|}$ is the *projection* of $\mathbf{c}$ onto S
- The projection of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ onto S is the *multiset*

$$\mathcal{C}(S) \stackrel{\text{def}}{=} \{\mathbf{c}(S) \in \{0,1\}^{|S|} : \mathbf{c} \in \mathcal{C}\} \quad \text{with multiplicities}$$

- S is *shattered by* $\mathcal{C}$ if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors

$\mathcal{C} = \{101100, 011101, 100110, 000111\} \Rightarrow \mathcal{S} = \{1,2\}$ not shattered

Theorem [*Weldon 78*]

Let $(\mathcal{C}_1, \mathcal{C}_2)$ be a pair of zero-error codebooks for the BAC with cardinalities $(2^{nR_1}, 2^{nR_2})$. If $\mathcal{C}_1$ shatters a set of coordinates S with cardinality $|S| = n\alpha$, then

$$R_2 \leq (1-\alpha)\log 3$$

Proof:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \implies 2^{nR_2}$ such S-*complement pairs* exist (at least)

Proof:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \implies 2^{nR_2}$ such S-*complement pairs* exist (at least)
- Their sums should be all distinct on $\bar{S} \stackrel{\text{def}}{=} [n] \setminus S$, hence

$$2^{nR_2} \leq 3^{|\bar{S}|}$$

<u>Proof</u>:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \implies 2^{nR_2}$ such S-*complement pairs* exist (at least)
- Their sums should be all distinct on $\bar{S} \stackrel{\text{def}}{=} [n] \setminus S$, hence

$$2^{nR_2} \leq 3^{n(1-\alpha)}$$

<u>Proof</u>:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \implies 2^{nR_2}$ such S-*complement pairs* exist (at least)
- Their sums should be all distinct on $\bar{S} \overset{\text{def}}{=} [n] \setminus S$, hence

$$2^{nR_2} \leq 3^{n(1-\alpha)} \quad \Rightarrow \quad R_2 \leq (1-\alpha)\log 3 \qquad \square$$

Proof:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \implies 2^{nR_2}$ such S-*complement pairs* exist (at least)
- Their sums should be all distinct on $\bar{S} \stackrel{\text{def}}{=} [n] \setminus S$, hence

$$2^{nR_2} \leq 3^{n(1-\alpha)} \quad \Rightarrow \quad R_2 \leq (1-\alpha)\log 3 \qquad \square$$

- Special case: If $\mathcal{C}_1$ is *systematic* (e.g., linear) it shatters a set S of cardinality nR_1. Thus in this case $R_2 < (1 - R_1)\log 3$

Background & Motivation

<u>Proof</u>:

- Choose any $\mathbf{c}_2 \in \mathcal{C}_2$
- By shatterdness, there exists $\mathbf{c_1} \in \mathcal{C}_1$ such that $\mathbf{c}_1(S) = \overline{\mathbf{c}_2(S)}$, i.e.,

$$(\mathbf{c}_1 + \mathbf{c}_2)(S) = (1 \ldots, 1)$$

- $|\mathcal{C}_2| = 2^{nR_2} \Longrightarrow 2^{nR_2}$ such S-*complement pairs* exist (at least)
- Their sums should be all distinct on $\bar{S} \stackrel{\text{def}}{=} [n] \setminus S$, hence

$$2^{nR_2} \leq 3^{n(1-\alpha)} \quad \Rightarrow \quad R_2 \leq (1-\alpha) \log 3 \qquad \square$$

- Special case: If $\mathcal{C}_1$ is *systematic* (e.g., linear) it shatters a set S of cardinality nR_1. Thus in this case $R_2 < (1 - R_1) \log 3$
- Weldon stopped here, but what can be said in general?

VC Dimension [*Vapnik-Chervonenkis 1971*]

The *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest set shattered by $\mathcal{C}$

Background & Motivation

VC Dimension [*Vapnik-Chervonenkis 1971*]

The *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest set shattered by $\mathcal{C}$

Lemma [*Sauer-Perles-Shelah 1972*]

If the VC dimension of $\mathcal{C}$ is d, then

$$|\mathcal{C}| \leq \sum_{k=0}^{d} \binom{n}{k}$$

VC Dimension [*Vapnik-Chervonenkis 1971*]

The *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest set shattered by $\mathcal{C}$

Lemma [*Sauer-Perles-Shelah 1972*]

If the VC dimension of $\mathcal{C}$ is d, then

$$|\mathcal{C}| \leq \sum_{k=0}^{d} \binom{n}{k}$$

- Remark: The Lemma is tight for a Hamming Ball of radius d

Background & Motivation

VC Dimension [*Vapnik-Chervonenkis 1971*]

The *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest set shattered by $\mathcal{C}$

Lemma [*Sauer-Perles-Shelah 1972*]

If the VC dimension of $\mathcal{C}$ is d, then

$$|\mathcal{C}| \leq \sum_{k=0}^{d} \binom{n}{k} \approx 2^{nh\left(\frac{d}{n}\right)}$$

- Remark: The Lemma is tight for a Hamming Ball of radius d
- $h(p) = -p\log p - (1-p)\log(1-p)$

Background & Motivation

VC Dimension [*Vapnik-Chervonenkis 1971*]

The *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest set shattered by $\mathcal{C}$

Lemma [*Sauer-Perles-Shelah 1972*]

If the VC dimension of $\mathcal{C}$ is d, then

$$|\mathcal{C}| \leq \sum_{k=0}^{d} \binom{n}{k} \approx 2^{nh\left(\frac{d}{n}\right)}$$

- Remark: The Lemma is tight for a Hamming Ball of radius d
- $h(p) = -p \log p - (1-p) \log (1-p)$

Corollary

If $|\mathcal{C}| = 2^{n(R+\varepsilon)}$ then there is a shattered set S with $|S| \geq nh^{-1}(R)$.

Background & Motivation

- Plugging this into Weldon's theorem gives

- Plugging this into Weldon's theorem gives

Corollary

If (R_1, R_2) is achievable then

$$R_2 \leq (1 - h^{-1}(R_1)) \log 3$$

Background & Motivation

- Plugging this into Weldon's theorem gives

Corollary

If (R_1, R_2) is achievable then

$$R_2 \leq (1 - h^{-1}(R_1)) \log 3$$

- Unfortunately, for any $R_1 \in [0, 1]$

$$R_1 + (1 - h^{-1}(R_1)) \log 3 > 1.5$$

- Plugging this into Weldon's theorem gives

Corollary

If (R_1, R_2) is achievable then

$$R_2 \leq (1 - h^{-1}(R_1)) \log 3$$

- Unfortunately, for any $R_1 \in [0, 1]$

$$R_1 + (1 - h^{-1}(R_1)) \log 3 > 1.5$$

- Weaknesses:
  - We assumed only one S-complement for each $\mathbf{c}_2 \in \mathcal{C}_2$
    Weak lower bound on # of S-complement pairs (2^{nR_2})
  - We disregarded the sumset structure outside S
    Weak upper bound on # of S-complement pairs ($3^{|\bar{S}|}$)

HIGHER ORDER VC DIMENSION

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

$\mathcal{C} = \{101100, 011101, 100110, 000111\}$

Higher Order VC Dimension

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

$\mathcal{C} = \{101100, 011101, 100110, 000111\}$, $\mathcal{S} = \{6\}$ 2-shattered

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

$\mathcal{C} = \{101100, 011101, 100110, 000111\}$

Higher Order VC Dimension

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

$$\mathcal{C} = \{101100, 011101, 100110, 000111\}\ , \quad \mathcal{S} = \{2\} \text{ 1-shattered}$$

Higher Order VC Dimension

k-shattering

$S \subseteq [n]$ is *k-shattered by* $\mathcal{C} \subseteq \{0,1\}^n$, if $\mathcal{C}(S)$ contains all $2^{|S|}$ possible vectors, each with multiplicity at least k

$$\mathcal{C} = \{101100, 011101, 100110, 000111\}\ , \quad \mathcal{S} = \{2\} \quad \text{1-shattered}$$

kth-order VC dimension

The kth-order *VC dimension* of a codebook $\mathcal{C} \subseteq \{0,1\}^n$ is the cardinality of the largest subset k-shattered by $\mathcal{C}$

Higher Order VC Dimension

Lemma ("soft" Sauer-Perles-Shelah lemma)

If the kth-order VC dimension of $\mathcal{C} \subseteq \{0,1\}^n$ is $d-1$, then

$$|\mathcal{C}| \le \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^{n} \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

where t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \ge k$ if such an integer exists, and $t^* = n$ otherwise.

Higher Order VC Dimension

Lemma ("soft" Sauer-Perles-Shelah lemma)

If the kth-order VC dimension of $\mathcal{C} \subseteq \{0,1\}^n$ is $d-1$, then

$$|\mathcal{C}| \leq \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^{n} \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

where t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \geq k$ if such an integer exists, and $t^* = n$ otherwise.

- $\mathcal{O}(n/d)$-tight for a Hamming Ball of radius t^*

Higher Order VC Dimension

Lemma ("soft" Sauer-Perles-Shelah lemma)

If the kth-order VC dimension of $\mathcal{C} \subseteq \{0,1\}^n$ is $d-1$, then

$$|\mathcal{C}| \leq \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^{n} \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

where t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \geq k$ if such an integer exists, and $t^* = n$ otherwise.

- $\mathcal{O}(n/d)$-tight for a Hamming Ball of radius t^*

Corollary

If $|\mathcal{C}| = 2^{n(R+\varepsilon)}$ then for any $0 \leq \alpha \leq h^{-1}(R)$ there exists S with $|S| \geq n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}$, where

$$\beta = (1-\alpha) \cdot h\left(\frac{h^{-1}(R) - \alpha}{1-\alpha}\right)$$

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$

NUMBER OF S-COMPLEMENT PAIRS

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq$ # of S-complement pairs $\leq 3^{n(1-\alpha)}$

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq$ # of S-complement pairs $\leq 3^{n(1-\alpha)}$

$$R_2 < (1-\alpha)\log 3 - \beta$$

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?

NUMBER OF S-COMPLEMENT PAIRS

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq$ # of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes

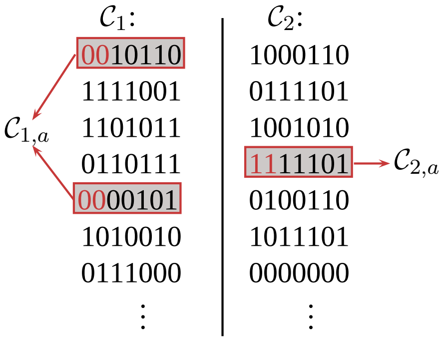
Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$

$\mathcal{C}_1$:	$\mathcal{C}_2$:
0010110	1000110
1111001	0111101
1101011	1001010
0110111	1111101
0000101	0100110
1010010	1011101
0111000	0000000
⋮	⋮

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$



Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$

$\mathcal{C}_1$:	$\mathcal{C}_2$:
0010110 ($\in \mathcal{C}_{1,a}$)	1000110
1111001	0111101
1101011	1001010
0110111	1111101 ($\in \mathcal{C}_{2,a}$)
0000101 ($\in \mathcal{C}_{1,a}$)	0100110
1010010	1011101
0111000	0000000
⋮	⋮

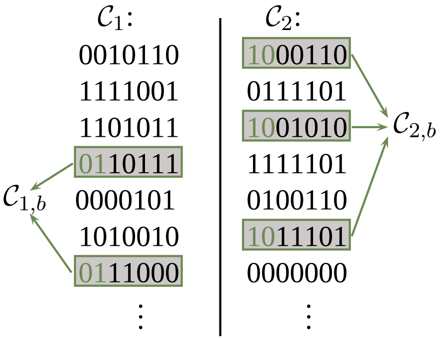
$\forall \mathbf{c}_{1,a} \in \mathcal{C}_{1,a}, \mathbf{c}_{2,a} \in \mathcal{C}_{2,a}$:

```
  00*****
+ 11*****
---------
  11*****
```

In addition: $|\mathcal{C}_{1,a}| \geq 2^{n\beta}$

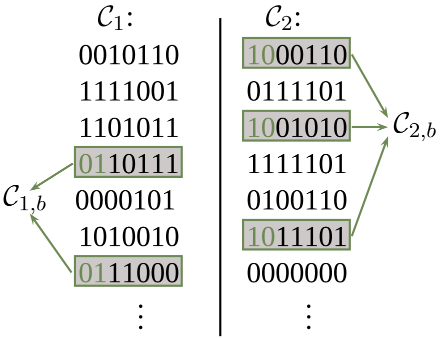
Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$



Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$



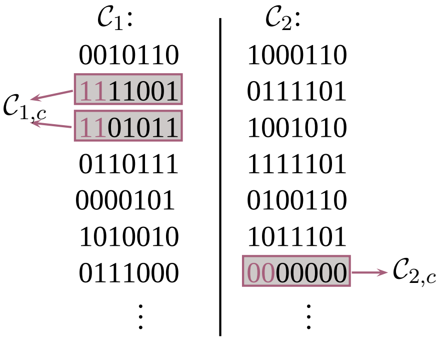
$\forall \mathbf{c}_{1,b} \in \mathcal{C}_{1,b}, \mathbf{c}_{2,b} \in \mathcal{C}_{2,b}$:

$$\begin{array}{r} 01{*}{*}{*}{*}{*} \\ +\;10{*}{*}{*}{*}{*} \\ \hline 11{*}{*}{*}{*}{*} \end{array}$$

In addition: $|\mathcal{C}_{1,b}| \geq 2^{n\beta}$

Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$



Number of S-Complement Pairs

- Assume $(\mathcal{C}_1, \mathcal{C}_2)$ are zero-error
- By the soft lemma, there exists a subset S with cardinality $|S| = n\alpha$ that is $2^{n\beta}$-shattered by $\mathcal{C}_1$
- $2^{n(R_2+\beta)} \leq \#$ of S-complement pairs $\leq$?
- Partition $(\mathcal{C}_1, \mathcal{C}_2)$ to disjoint pairs $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ of subcodes
- Example: $S = \{1, 2\}$

	$\mathcal{C}_1$:	$\mathcal{C}_2$:	
	0010110	1000110	
$\mathcal{C}_{1,c}$	1111001	0111101	
$\mathcal{C}_{1,c}$	1101011	1001010	
	0110111	1111101	
	0000101	0100110	
	1010010	1011101	
	0111000	0000000	$\mathcal{C}_{2,b}$
	⋮	⋮	

$\forall \mathbf{c}_{1,c} \in \mathcal{C}_{1,c}, \mathbf{c}_{2,c} \in \mathcal{C}_{2,c}$:

$$\begin{array}{r} 11{*}{*}{*}{*}{*} \\ +\,00{*}{*}{*}{*}{*} \\ \hline 11{*}{*}{*}{*}{*} \end{array}$$

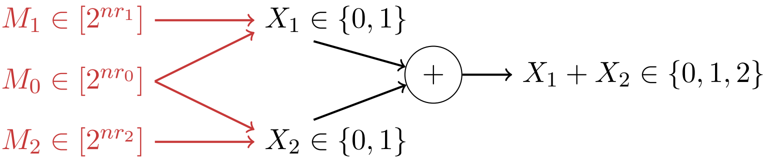
In addition: $|\mathcal{C}_{1,c}| \geq 2^{n\beta}$

Number of S-Complement Pairs

- We get $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ with $|\mathcal{C}_{1,i}| = 2^{n\beta}$ and $|\mathcal{C}_{2,i}| \approx 2^{n(R_2-\alpha)}$ for every i

NUMBER OF S-COMPLEMENT PAIRS

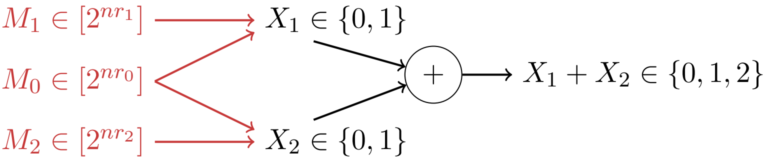
- We get $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ with $|\mathcal{C}_{1,i}| = 2^{n\beta}$ and $|\mathcal{C}_{2,i}| \approx 2^{n(R_2-\alpha)}$ for every i
- Induces a zero-error scheme for BAC with common message



- Send $\mathcal{C}_{1,M_0}(M_1)$ and $\mathcal{C}_{2,M_0}(M_2)$

Number of S-Complement Pairs

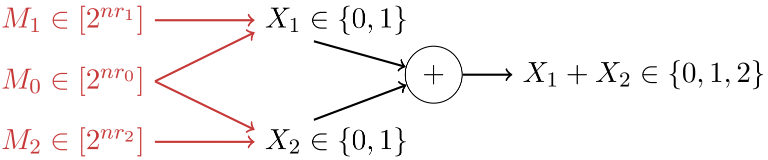
- We get $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ with $|\mathcal{C}_{1,i}| = 2^{n\beta}$ and $|\mathcal{C}_{2,i}| \approx 2^{n(R_2-\alpha)}$ for every i
- Induces a zero-error scheme for BAC with common message



- Send $\mathcal{C}_{1,M_0}(M_1)$ and $\mathcal{C}_{2,M_0}(M_2)$

$$r_0 = \alpha \qquad r_1 = \beta \qquad r_2 = R_2 - \alpha$$

- We get $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ with $|\mathcal{C}_{1,i}| = 2^{n\beta}$ and $|\mathcal{C}_{2,i}| \approx 2^{n(R_2-\alpha)}$ for every i
- Induces a zero-error scheme for BAC with common message



- Send $\mathcal{C}_{1,M_0}(M_1)$ and $\mathcal{C}_{2,M_0}(M_2)$

$$r_0 = \alpha \qquad r_1 = \beta \qquad r_2 = R_2 - \alpha$$

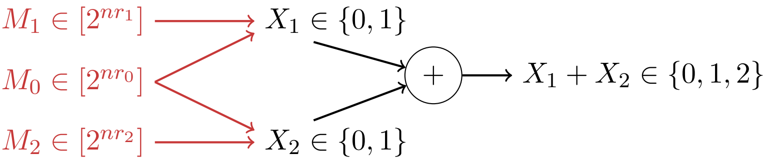
- For each $\mathbf{c}_{1,i} \in \mathcal{C}_{1,i}, \mathbf{c}_{2,i} \in \mathcal{C}_{2,i}$ we have

$$(\mathbf{c}_{1,i} + \mathbf{c}_{2,i})(S) = (1, \ldots, 1)$$

- The $n\alpha$ coordinates in S can be discarded!

Number of S-Complement Pairs

- We get $\{\mathcal{C}_{1,i}, \mathcal{C}_{2,i}\}_{i=1}^{2^{n\alpha}}$ with $|\mathcal{C}_{1,i}| = 2^{n\beta}$ and $|\mathcal{C}_{2,i}| \approx 2^{n(R_2-\alpha)}$ for every i
- Induces a zero-error scheme for BAC with common message



- Send $\mathcal{C}_{1,M_0}(M_1)$ and $\mathcal{C}_{2,M_0}(M_2)$

$$r_0 = \frac{\alpha}{1-\alpha} \quad r_1 = \frac{\beta}{1-\alpha} \quad r_2 = \frac{R_2-\alpha}{1-\alpha}$$

- For each $\mathbf{c}_{1,i} \in \mathcal{C}_{1,i}, \mathbf{c}_{2,i} \in \mathcal{C}_{2,i}$ we have

$$(\mathbf{c}_{1,i} + \mathbf{c}_{2,i})(S) = (1, \ldots, 1)$$

- The $n\alpha$ coordinates in S can be discarded!

The BAC with a Common Message

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_2 = \frac{R_2 - \alpha}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

The BAC with a Common Message

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

$$R_2 < (1-\alpha) r_\Sigma - \beta(\alpha, R_1)$$

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

$$R_2 < (1-\alpha) r_\Sigma - \beta(\alpha, R_1)$$

- **New goal:** Upper bound r_Σ under the above constraints on r_0, r_1

The BAC with a Common Message

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

$$R_2 < (1-\alpha) r_\Sigma - \beta(\alpha, R_1)$$

- **New goal:** Upper bound r_Σ under the above constraints on r_0, r_1
- Trivial bound: $r_\Sigma \leq \log 3$

The BAC with a Common Message

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the zero-error capacity region of the BAC with common message.

$$R_2 < (1-\alpha)\log 3 - \beta(\alpha, R_1)$$

- **New goal:** Upper bound r_Σ under the above constraints on r_0, r_1
- Trivial bound: $r_\Sigma \leq \log 3$

The BAC with a Common Message

A reduction lemma

If (R_1, R_2) are in the BAC zero-error capacity region, then for any $0 < \alpha < h^{-1}(R_1)$

$$r_0 = \frac{\alpha}{1-\alpha}, \quad r_1 = \frac{\beta(\alpha, R_1)}{1-\alpha}, \quad r_\Sigma = \frac{R_2 + \beta(\alpha, R_1)}{1-\alpha}$$

is in the ~~zero-error~~ capacity region of the BAC with common message.

$$R_2 < (1-\alpha) r_\Sigma - \beta(\alpha, R_1)$$

- **New goal:** Upper bound r_Σ under the above constraints on r_0, r_1
- Trivial bound: $r_\Sigma \leq \log 3$

The Binary Adder With a Common Message

Theorem [*Slepian-Wolf 1973*], [*Willems 1982*]

The Shannon capacity region of the BAC with a common message, is the closure of the union of all rate triplets satisfying

$$
\begin{aligned}
r_1 &\leq H(X_1|U) \\
r_2 &\leq H(X_2|U) \\
r_1 + r_2 &\leq H(X_1 + X_2|U) \\
r_\Sigma = r_0 + r_1 + r_2 &\leq H(X_1 + X_2)
\end{aligned}
$$

for some $P_U P_{X_1|U} P_{X_2|U}$, where $|\mathcal{U}| \leq 4$.

The Binary Adder With a Common Message

Theorem [*Slepian-Wolf 1973*], [*Willems 1982*]

The Shannon capacity region of the BAC with a common message, is the closure of the union of all rate triplets satisfying

$$
\begin{aligned}
r_1 &\le H(X_1|U) \\
r_2 &\le H(X_2|U) \\
r_1 + r_2 &\le H(X_1 + X_2|U) \\
r_\Sigma = r_0 + r_1 + r_2 &\le H(X_1 + X_2)
\end{aligned}
$$

for some $P_U P_{X_1|U} P_{X_2|U}$, where $|\mathcal{U}| \le 3$.

The Binary Adder With a Common Message

Theorem [*Slepian-Wolf 1973*], [*Willems 1982*]

The Shannon capacity region of the BAC with a common message, is the closure of the union of all rate triplets satisfying

$$\begin{aligned} r_1 &\leq H(X_1|U) \\ \sout{r_2 \leq H(X_2|U)} \\ r_1 + r_2 &\leq H(X_1 + X_2|U) \\ r_\Sigma = r_0 + r_1 + r_2 &\leq H(X_1 + X_2) \end{aligned}$$

for some $P_U P_{X_1|U} P_{X_2|U}$, where $|\mathcal{U}| \leq 3$.

- Still difficult - 7 parameters to optimize...
- Need to upper bound $r_\Sigma(r_0, r_1)$ analytically!

Lemma (Sum-Rate Bound)

If (r_0, r_1, r_2) is achievable then there is some $\eta \in [0, \frac{1}{2}]$ s.t.

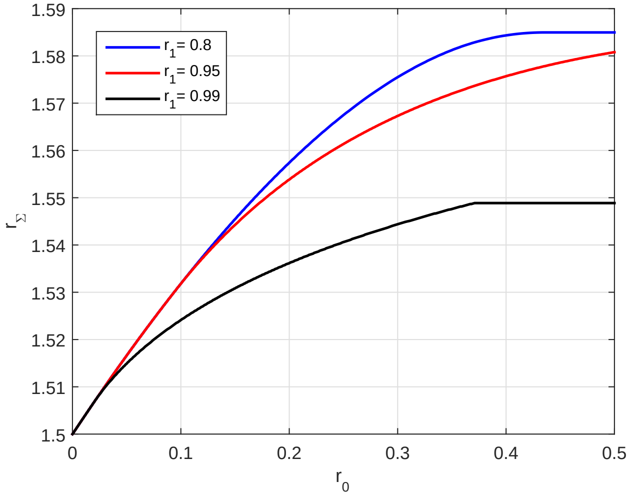
$$r_\Sigma \leq \max_{h^{-1}(r_1) \leq \eta \leq \frac{1}{2}} \min\left(L(\eta), J(h^{-1}(r_1), \eta) + r_0\right)$$

where

$$L(\eta) \stackrel{\text{def}}{=} h(\eta) + 1 - \eta$$

$$J(p, \eta) \stackrel{\text{def}}{=} \begin{cases} 2h\left(\frac{1}{2}\left(1 - \sqrt{1 - 2\eta}\right)\right) - \eta & \eta \geq p \star p \\ 2h\left(\frac{1}{2}\left(1 - \frac{1-\eta-p\star p}{\sqrt{1-2(p\star p)}}\right)\right) \\ \quad -\frac{1}{2}\left(1 - \frac{(1-\eta-p\star p)^2}{1-2(p\star p)}\right) & \eta < p \star p \end{cases}$$

The Binary Adder With a Common Message



Tying the Loose Ends

Theorem (Outer bound for the Zero-error Capacity Region)

Let

$$r_\Sigma(r_0, r_1) \triangleq \max_{h^{-1}(r_1) \le \eta \le \frac{1}{2}} \min\{L(\eta),\ J(h^{-1}(r_1), \eta) + r_0\}$$

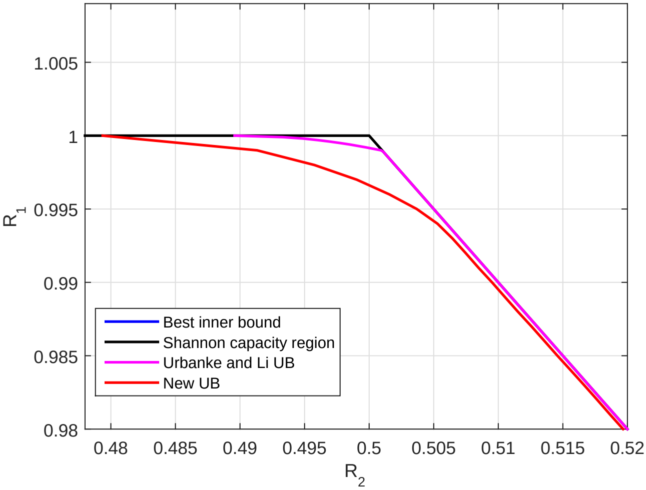
Then any zero-error achievable rate pair (R_1, R_2) satisfies

$$R_2 < \min_{0 \le \alpha \le h^{-1}(R_1)} (1-\alpha)\left(r_\Sigma\left(\frac{\alpha}{1-\alpha}, \Gamma(R_1, \alpha)\right) - \Gamma(R_1, \alpha)\right)$$

where

$$\Gamma(R_1, \alpha) \triangleq h\left(\frac{h^{-1}(R_1) - \alpha}{1-\alpha}\right)$$

Tying the Loose Ends



Summary and Discussion

- New outer bound on BAC zero-error capacity region
- We introduced the notion of kth order VC-dimension and proved an analog of Sauer's Lemma
- Our bounding technique combined this combinatorial notion with network information theoretic arguments

- Weaknesses of our bound
  - The lower bound on $\#$ of S-complement pairs is valid for any pair $(\mathcal{C}_1, \mathcal{C}_2)$ (not just zero-error pairs)
  - We lower bounded the number of S-complement pairs for *any* k-shattered set in $\mathcal{C}_1$, but there are *many such sets*.
- Our technique may be applicable to other zero-error problems