E2 205: Error-Control Coding

Chapter 5: Bounds on the Parameters of Codes

Navin Kashyap

Indian Institute of Science

The Sphere-Packing Bound

This extends the Hamming bound to arbitrary block codes.

Theorem (The sphere-packing bound)

For any (n, M, d) block code over an alphabet $\mathbb{F}$ of size q, we have

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq \frac{1}{M} \, q^n.$$

The Sphere-Packing Bound

This extends the Hamming bound to arbitrary block codes.

Theorem (The sphere-packing bound)

For any (n, M, d) block code over an alphabet $\mathbb{F}$ of size q, we have

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq \frac{1}{M} q^n.$$

- For a given blocklength n and minimum distance d, this yields an upper bound on M:

$$M \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}.$$

- The Hamming bound for an $[n, k, d]$ linear code is a special case of this bound, obtained by setting $M = q^k$.

Proof of the Sphere-Packing Bound

- Recall that the Hamming balls $B(\mathbf{c}, t)$ of radius $t = \lfloor \frac{d-1}{2} \rfloor$ centered at the codewords $\mathbf{c}$ of an (n, M, d) block code must be disjoint.
- Each such Hamming ball contains $\sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ words from $\mathbb{F}_q{}^n$:
  - $\mathbf{y} \in B(\mathbf{c}, t) \iff w_H(\mathbf{y} - \mathbf{c}) \leq t$
  - So, $|B(\mathbf{c}, t)| = \#$ vectors $\mathbf{e}\,(= \mathbf{y} - \mathbf{c})$ such that $w_H(\mathbf{e}) \leq t$
- Then, the union of all the M balls $B(\mathbf{c}, t)$, $\mathbf{c} \in \mathcal{C}$, contains $M \cdot \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$ words from $\mathbb{F}_q{}^n$. This cannot exceed the total number of words in $\mathbb{F}_q{}^n$, yielding

$$M \cdot \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \;\leq\; q^n. \quad \square$$

Example

What is the largest possible number of codewords in a single-error-correcting binary block code of length 6?

(Not necessarily linear)

Example

What is the largest possible number of codewords in a single-error-correcting binary block code of length 6? (Not necessarily linear)

- Single-error-correcting $\implies$ $d \geq 3$
- By the sphere-packing bound, a single-error-correcting $(6, M, d \geq 3)$ binary block code must satisfy

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{6}{i} \leq \frac{1}{M} 2^6,$$

which implies that $\binom{6}{0} + \binom{6}{1} \leq \frac{64}{M}$, and hence, $M \leq \lfloor 64/7 \rfloor = 9$.

Example

What is the largest possible number of codewords in a single-error-correcting binary block code of length 6? (Not necessarily linear)

- Single-error-correcting $\implies$ $d \geq 3$
- By the sphere-packing bound, a single-error-correcting $(6, M, d \geq 3)$ binary block code must satisfy

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{6}{i} \leq \frac{1}{M} 2^6,$$

  which implies that $\binom{6}{0} + \binom{6}{1} \leq \frac{64}{M}$, and hence, $M \leq \lfloor 64/7 \rfloor = 9$.

- But does there exist a $(6, 9, d \geq 3)$ binary block code?

The Johnson Bound

An improvement to the sphere-packing bound ...

Theorem (The Johnson bound)

For a binary (n, M, d) block code, with $t = \lfloor \frac{d-1}{2} \rfloor$, we have

$$\sum_{i=0}^{t} \binom{n}{i} + \binom{n}{t} \cdot \left(\frac{\frac{n-t}{t+1} - \lfloor \frac{n-t}{t+1} \rfloor}{\lfloor \frac{n}{t+1} \rfloor} \right) \leq \frac{1}{M} 2^n.$$

- For $n = 6$ and $t = 1$, as in the last example, we obtain $M \leq 8$.

Example (cont'd)

What is the largest possible number of codewords in a single-error-correcting binary block code of length 6?

- By the Johnson bound, such a code can have at most 8 codewords.

Example (cont'd)

What is the largest possible number of codewords in a single-error-correcting binary block code of length 6?

- By the Johnson bound, such a code can have at most 8 codewords.
- Indeed, such a code with 8 codewords is possible — for example, the $[6, 3, 3]$ binary linear code with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The Singleton Bound

Theorem (The Singleton bound)

For any (n, M, d) block code over $\mathbb{F}_q$, we have

$$d \leq n - \lceil \log_q M \rceil + 1.$$

The Singleton Bound

Theorem (The Singleton bound)

For any (n, M, d) block code over $\mathbb{F}_q$, we have

$$d \leq n - \lceil \log_q M \rceil + 1.$$

Proof: Set $\ell = \lceil \log_q M \rceil - 1$. Then, $\ell < \log_q M$, i.e., $q^\ell < M$.

- Consider the first ℓ coordinates of a codeword. There are q^ℓ possible ways of filling the first ℓ coords with symbols from $\mathbb{F}_q$.
- Since there are $M > q^\ell$ codewords, by the pigeonhole principle, some pair of codewords, say $\mathbf{c}$ and $\mathbf{c}'$, must agree in their first ℓ coordinates.
- Then, $\mathbf{c}$ and $\mathbf{c}'$ can *differ* in at most $n - \ell$ coordinates

$$\begin{aligned} &\Longrightarrow \quad d_H(\mathbf{c}, \mathbf{c}') \ \leq \ n - \ell \\ &\Longrightarrow \quad d_{\min} \ \leq \ n - \ell. \end{aligned}$$

$\square$

The Singleton Bound

Corollary: For any $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq n - k + 1.$$

Proof: Set $M = q^k$ in the previous theorem. $\square$

The Singleton Bound

Corollary: For any $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq n - k + 1.$$

Proof: Set $M = q^k$ in the previous theorem. $\square$

Alt. Proof: Let H be a parity-check matrix of an $[n, k]$ linear code. Then,

$$\begin{aligned}
&\mathrm{rank}(H) = n - k \\
&\implies \text{any set of } n-k+1 \text{ columns of } H \text{ is linearly dependent} \\
&\implies \text{there exists some codeword of weight } \leq n-k+1 \\
&\implies d_{\min} \ \leq \ n - k + 1.
\end{aligned}$$

$\square$

The Singleton Bound

Corollary: For any $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq n - k + 1.$$

Proof: Set $M = q^k$ in the previous theorem. $\square$

Alt. Proof: Let H be a parity-check matrix of an $[n, k]$ linear code. Then,

$$\begin{aligned} & \text{rank}(H) = n - k \\ \implies & \text{ any set of } n-k+1 \text{ columns of } H \text{ is linearly dependent} \\ \implies & \text{ there exists some codeword of weight } \leq n-k+1 \\ \implies & \; d_{\min} \;\leq\; n-k+1. \end{aligned}$$ $\square$

Definition: An $[n, k, d]$ linear code that satisfies $d = n - k + 1$ is called a maximum distance separable (MDS) code.

Examples of MDS Codes

The following are all examples of MDS codes, over any field $\mathbb{F}$:

- $\mathbb{F}^n$, which is an $[n, n, 1]$ code
- the single parity-check code, defined by the parity-check matrix $H = [1\ 1\ \ldots\ 1]$ — this is an $[n, n-1, 2]$ code
- the $[n, 1, n]$ repetition code, generated by $G = [1\ 1\ \ldots\ 1]$

Examples of MDS Codes

The following are all examples of MDS codes, over any field $\mathbb{F}$:

- $\mathbb{F}^n$, which is an $[n, n, 1]$ code
- the single parity-check code, defined by the parity-check matrix $H = [1\ 1\ \ldots\ 1]$ — this is an $[n, n-1, 2]$ code
- the $[n, 1, n]$ repetition code, generated by $G = [1\ 1\ \ldots\ 1]$

The above are, in fact, the only MDS codes possible when $\mathbb{F} = \mathbb{F}_2$.

Over non-binary fields, we have a wide variety of other examples; a particularly important one is the family of Reed-Solomon codes.

Examples of MDS Codes

The following are all examples of MDS codes, over any field $\mathbb{F}$:

- $\mathbb{F}^n$, which is an $[n, n, 1]$ code
- the single parity-check code, defined by the parity-check matrix $H = [1\ 1\ \ldots\ 1]$ — this is an $[n, n-1, 2]$ code
- the $[n, 1, n]$ repetition code, generated by $G = [1\ 1\ \ldots\ 1]$

The above are, in fact, the <u>only</u> MDS codes possible when $\mathbb{F} = \mathbb{F}_2$.

Over non-binary fields, we have a wide variety of other examples; a particularly important one is the family of Reed-Solomon codes.

MDS codes have some interesting properties. For example,

- $\mathcal{C}$ is MDS iff $\mathcal{C}^\perp$ is MDS.

The Gilbert-Varshamov (GV) Bound

The inequalities relating the parameters $[n, k, d]_q$ or $(n, M, d)_q$ given so far provide necessary conditions for codes with those parameters to exist.

We next give an important sufficient condition on code parameters that guarantees the existence of a linear code with those parameters.

The Gilbert-Varshamov (GV) Bound

The inequalities relating the parameters $[n, k, d]_q$ or $(n, M, d)_q$ given so far provide necessary conditions for codes with those parameters to exist.

We next give an important sufficient condition on code parameters that guarantees the existence of a linear code with those parameters.

Theorem (The Gilbert-Varshamov bound)

Let $\mathbb{F}_q$ be a finite field, and let n, k and d be positive integers such that

$$\sum_{\ell=0}^{d-2} \binom{n-1}{\ell} (q-1)^{\ell} \; < \; q^{n-k}.$$

Then, there exists an $[n, k]$ linear code over $\mathbb{F}_q$, with $d_{\min} \geq d$.

Proof of GV Bound

The idea is to construct an $(n-k) \times n$ parity-check matrix H with the property that no $d-1$ (or fewer) columns are linearly dependent over $\mathbb{F}_q$.

The construction is recursive:

- Pick the first column $\mathbf{h}_1$ to be any non-zero vector in ${\mathbb{F}_q}^{n-k}$.
- Suppose that, for some $i \geq 2$, we have picked the first $i-1$ columns $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}$.

  We then pick $\mathbf{h}_i$ so that it cannot be obtained as a linear combination of any $d-2$ (or fewer) columns from $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}$.

Proof of GV Bound

The idea is to construct an $(n-k) \times n$ parity-check matrix H with the property that no $d-1$ (or fewer) columns are linearly dependent over $\mathbb{F}_q$.

The construction is recursive:

- Pick the first column $\mathbf{h}_1$ to be any non-zero vector in ${\mathbb{F}_q}^{n-k}$.
- Suppose that, for some $i \geq 2$, we have picked the first $i-1$ columns $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}$.

  We then pick $\mathbf{h}_i$ so that it cannot be obtained as a linear combination of any $d-2$ (or fewer) columns from $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}$.
- The number of linear combinations that can be formed from $\leq d-2$ of the columns $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}$ is

$$V_i \triangleq \sum_{\ell=0}^{d-2} \binom{i-1}{\ell} (q-1)^{\ell}.$$

- So, if $V_i < q^{n-k}$, there exists a vector in ${\mathbb{F}_q}^{n-k}$ that is not expressible as a linear combination of $d-2$ or fewer columns from $\mathbf{h}_i, \ldots, \mathbf{h}_{i-1}$. This vector can be taken to be $\mathbf{h}_i$.

Proof of GV Bound

- Note that $V_1 \leq V_2 \leq \cdots \leq V_n$, and the hypothesis of the theorem asserts that $V_n < q^{n-k}$.
- Hence, for each $i \in \{1, 2, \ldots, n\}$, we have $V_i < q^{n-k}$ being satisfied, and we can pick a column $\mathbf{h}_i$ as desired.
- The required $(n-k) \times n$ parity-check matrix H can thus be constructed. $\square$

Using the GV Bound

We often want to know the answer to the following question:

> *Given integers n and d, what is the largest (linear) code over $\mathbb{F}_q$ having blocklength n and $d_{\mathsf{min}} \geq d$?*

The GV bound gives us a means of showing the existence of linear codes with large dimension:

> For the given values of n and d, find the largest k for which the GV bound is satisfied.

Using the GV Bound

We often want to know the answer to the following question:

> *Given integers n and d, what is the largest (linear) code over $\mathbb{F}_q$ having blocklength n and $d_{\mathsf{min}} \geq d$?*

The GV bound gives us a means of showing the existence of linear codes with large dimension:

> For the given values of n and d, find the largest k for which the GV bound is satisfied.

However, the proof is non-constructive, meaning that it does not give a practical algorithm for code construction.

Examples

- $q = 2$, $n = 6$, $d = 3$. LHS of GV bound is 6.

  The largest k such that $6 < 2^{6-k}$ is $k = 3$.
  So, a $[6, 3, 3]$ binary linear code exists.

Examples

- $q = 2$, $n = 6$, $d = 3$. LHS of GV bound is 6.

  The largest k such that $6 < 2^{6-k}$ is $k = 3$.
  So, a $[6, 3, 3]$ binary linear code exists.

  Of course, we already know how to construct such a code: use the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Examples

- $q = 2$, $n = 6$, $d = 3$. LHS of GV bound is 6.

  The largest k such that $6 < 2^{6-k}$ is $k = 3$.
  So, a $[6, 3, 3]$ binary linear code exists.

  Of course, we already know how to construct such a code: use the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

- $q = 2$, $n = 1000$, $d = 201$.
  i.e., a 100-error-correcting binary linear code of length 1000.

  The largest value of k satisfying the inequality in the GV bound is 280; so a $[1000, 280, d_{\min} \geq 201]$ code over $\mathbb{F}_2$ exists.

Estimates of Sums

Evaluating a sum of the form $\sum_{\ell=0}^{d-2} \binom{n-1}{\ell} (q-1)^\ell$ is not easy for large n, d; so we give some useful bounds on such sums.

Define the *q*-ary entropy function

$$h_q(x) \triangleq -x \log_q x - (1-x)\log_q(1-x) + x\log_q(q-1), \quad \text{for } 0 \le x \le 1.$$

Lemma:

(a) For $0 \le m/n \le 1 - 1/q$,

$$\sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^\ell \le q^{nh_q(m/n)}.$$

(b) For $0 \le m/n \le 1$,

$$\sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^\ell \ge \binom{n}{m} (q-1)^m \ge \frac{1}{\sqrt{8m(1-m/n)}} q^{nh_q(m/n)}.$$

Hence, for $0 \le \frac{m}{n} \le 1 - \frac{1}{q}$, $\quad \sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^\ell = q^{nh_q(m/n)+O(\log n)}$.

Proof Sketch of Lemma

(a) Let $\theta = \frac{m}{n}$. We then have

$$
\begin{aligned}
& q^{-nh_q(\theta)} \sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^{\ell} \\
&= \theta^m (1-\theta)^{n-m} (q-1)^{-m} \sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^{\ell} \\
&\leq \theta^m (1-\theta)^{n-m} (q-1)^{-m} \sum_{\ell=0}^{m} \binom{n}{\ell} (q-1)^{\ell} \underbrace{\left[\frac{\theta}{(1-\theta)(q-1)}\right]}_{\substack{\text{this is } \leq 1 \\ \text{for } \theta \leq 1-\frac{1}{q}}}^{\ell-m} \\
&\leq \theta^m (1-\theta)^{n-m} (q-1)^{-m} \sum_{\ell=0}^{n} \binom{n}{\ell} (q-1)^{\ell} \left[\frac{\theta}{(1-\theta)(q-1)}\right]^{\ell-m} \\
&= \sum_{\ell=0}^{n} \binom{n}{\ell} \theta^{\ell} (1-\theta)^{n-\ell} \quad = \quad [\theta + (1-\theta)]^n \quad = \quad 1.
\end{aligned}
$$

(b) follows from Stirling's formula.

Example

$q = 2$, $n = 1000$, $d = 201$.
i.e., a 100-error-correcting binary linear code of length 1000.

- To apply the GV bound, we need to evaluate (or estimate) the sum $\sum_{\ell=0}^{199} \binom{999}{\ell}$.
- By part (a) of the prev. lemma, $\sum_{\ell=0}^{199} \binom{999}{\ell} \leq 2^{999 \cdot h_2(199/999)}$.
- So, if k is such that $2^{999 \cdot h_2(199/999)} < 2^{1000-k}$, then the inequality $\sum_{\ell=0}^{199} \binom{999}{\ell} < 2^{1000-k}$ in the GV bound would also be satisfied.
- Hence, for any $k < 1000 - 999 \cdot h_2(199/999) \approx 280.4$, the inequality in the GV bound would be satisfied.
- In particular, the GV bound is satisfied for $k = 280$, showing that a $[1000, 280, d_{\min} \geq 201]$ binary linear code exists.

The Plotkin Bound for Linear Codes

Theorem: For an $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq \frac{n\,(q^k - q^{k-1})}{q^k - 1}.$$

- For $q = 2$, this reduces to $d \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$.

The Plotkin Bound for Linear Codes

Theorem: For an $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq \frac{n\,(q^k - q^{k-1})}{q^k - 1}.$$

- For $q = 2$, this reduces to $d \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$.
- Asymptotics: As $n \to \infty$, if k also goes to ∞, then

$$\delta \;=\; \frac{d}{n} \;\leq\; \frac{q^k - q^{k-1}}{q^k - 1} \;=\; 1 - \frac{1}{q} + o(1).$$

In particular, for binary linear codes, $\delta \;\leq\; \frac{1}{2} + o(1)$.

The Plotkin Bound for Linear Codes

Theorem: For an $[n, k, d]$ linear code over $\mathbb{F}_q$, we have

$$d \leq \frac{n\,(q^k - q^{k-1})}{q^k - 1}.$$

- For $q = 2$, this reduces to $d \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$.
- Asymptotics: As $n \to \infty$, if k also goes to ∞, then

$$\delta \;=\; \frac{d}{n} \;\leq\; \frac{q^k - q^{k-1}}{q^k - 1} \;=\; 1 - \frac{1}{q} + o(1).$$

  In particular, for binary linear codes, $\delta \;\leq\; \frac{1}{2} + o(1)$.
- An alternative view of this: As $n \to \infty$,

$$\text{either} \quad R = \frac{k}{n} \longrightarrow 0 \quad \text{or} \quad \delta = \frac{d}{n} \leq 1 - \frac{1}{q} + o(1).$$

Proof of Plotkin Bound for Linear Codes

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$.

We count in two different ways the sum of the Hamming weights of all the codewords:

$$W := \sum_{\mathbf{c} \in \mathcal{C}} w_H(\mathbf{c})$$

Proof of Plotkin Bound for Linear Codes

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$.

We count in two different ways the sum of the Hamming weights of all the codewords:

$$W := \sum_{\mathbf{c} \in \mathcal{C}} w_H(\mathbf{c})$$

- On the one hand, since $w_H(\mathbf{c}) \geq d$ for all codewords $\mathbf{c} \neq \mathbf{0}$, we have

$$W \geq (|\mathcal{C}| - 1)d = (q^k - 1)d.$$

Proof of Plotkin Bound for Linear Codes

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$.

We count in two different ways the sum of the Hamming weights of all the codewords:

$$W := \sum_{\mathbf{c} \in \mathcal{C}} w_H(\mathbf{c})$$

- On the one hand, since $w_H(\mathbf{c}) \geq d$ for all codewords $\mathbf{c} \neq \mathbf{0}$, we have
$$W \geq (|\mathcal{C}| - 1)d = (q^k - 1)d.$$
- For another way of evaluating W, we list out the q^k codewords in the rows of an $q^k \times n$ array.

$$\begin{array}{|ccc|}
\hline
\text{———} & \text{codeword } 1 & \text{———} \\
\text{———} & \text{codeword } 2 & \text{———} \\
 & \vdots & \\
\text{———} & \text{codeword } q^k & \text{———} \\
\hline
\end{array}$$

W is equal to the number of non-zero symbols in the array.

Proof of Plotkin Bound for Linear Codes

- Consider the ith column of this array (for any $i \in \{1, \ldots, n\}$).
  - There are q^k entries in this column, of which some are 0s.
  - The number of 0 entries in this column is equal to the number of codewords in the subcode

$$\mathcal{C}' = \{(c_1, c_2, \ldots, c_n) \in \mathcal{C} : \; c_i = 0\}.$$

  - $\mathcal{C}'$ is a linear code with dimension at least $k - 1$.

    This can be seen by noting that a parity-check matrix, H', for $\mathcal{C}'$ can be obtained by appending an extra row to a parity-check matrix H for $\mathcal{C}$:

$$H' = \begin{bmatrix} & & & H & & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

Proof of Plotkin Bound for Linear Codes

- Consider the ith column of this array (for any $i \in \{1, \ldots, n\}$).
  - There are q^k entries in this column, of which some are 0s.
  - The number of 0 entries in this column is equal to the number of codewords in the subcode

$$\mathcal{C}' = \{(c_1, c_2, \ldots, c_n) \in \mathcal{C} : \ c_i = 0\}.$$

  - $\mathcal{C}'$ is a linear code with dimension at least $k - 1$.

    This can be seen by noting that a parity-check matrix, H', for $\mathcal{C}'$ can be obtained by appending an extra row to a parity-check matrix H for $\mathcal{C}$:

$$H' = \begin{bmatrix} & & & H & & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

$$\dim(\mathcal{C}') = n - \operatorname{rank}(H') \geq n - (\operatorname{rank}(H) + 1) = k - 1.$$

Proof of Plotkin Bound for Linear Codes

- Thus, the number of 0 entries in the ith column of the array is $|\mathcal{C}'| \geq q^{k-1}$.
- Consequently, the number of non-zero entries in the ith column is *at most* $q^k - q^{k-1}$.

Proof of Plotkin Bound for Linear Codes

- Thus, the number of 0 entries in the ith column of the array is $|\mathcal{C}'| \geq q^{k-1}$.
- Consequently, the number of non-zero entries in the ith column is *at most* $q^k - q^{k-1}$.
- Therefore, the total number of non-zero symbols across all n columns of the array is

$$W \;\leq\; n\,(q^k - q^{k-1})$$

Proof of Plotkin Bound for Linear Codes

- Thus, the number of 0 entries in the ith column of the array is $|\mathcal{C}'| \geq q^{k-1}$.
- Consequently, the number of non-zero entries in the ith column is *at most* $q^k - q^{k-1}$.
- Therefore, the total number of non-zero symbols across all n columns of the array is

$$W \;\leq\; n\,(q^k - q^{k-1})$$

- Combining this with the lower bound $W \geq (q^k - 1)\,d$, we get

$$(q^k - 1)\,d \;\leq\; n\,(q^k - q^{k-1})$$

from which the bound on d follows. $\square$

The Plotkin Bound for Block Codes

Theorem: For an (n, M, d) block code over $\mathbb{F}_q$, we have

$$M \leq \frac{d}{d - \theta n} \quad \text{for } d > \theta n,$$

where $\theta := 1 - \frac{1}{q}$.

- Equivalently, setting $\delta = d/n$,

$$M \leq \frac{\delta}{\delta - \theta} \quad \text{for } \delta > \theta.$$

- Thus, again, either

$$\delta \leq \theta = 1 - \frac{1}{q},$$

  or M is bounded by $\frac{\delta}{\delta - \theta}$, so that

$$R = \frac{1}{n} \log_q M \longrightarrow 0 \text{ as } n \to \infty.$$

Proof of Plotkin Bound for Block Codes

Let $\mathcal{C}$ be an (n, M, d) block code over $\mathbb{F}_q$.

We count in two different ways the sum

$$S \;:=\; \sum_{\mathbf{u}\in\mathcal{C}} \sum_{\substack{\mathbf{v}\in\mathcal{C} \\ \mathbf{u}\neq\mathbf{v}}} d_H(\mathbf{u}, \mathbf{v})$$

- Since $d_H(\mathbf{u}, \mathbf{v}) \geq d$ for all pairs of distinct codewords $\mathbf{u}$ and $\mathbf{v}$, we have

$$S \;\geq\; M(M-1)d.$$

Proof of Plotkin Bound for Block Codes

Let $\mathcal{C}$ be an (n, M, d) block code over $\mathbb{F}_q$.

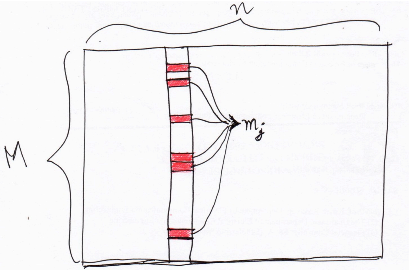
We count in two different ways the sum

$$S \;:=\; \sum_{\substack{\mathbf{u}\in\mathcal{C} \\ \mathbf{u}\neq\mathbf{v}}} \sum_{\mathbf{v}\in\mathcal{C}} d_H(\mathbf{u},\mathbf{v})$$

- Since $d_H(\mathbf{u},\mathbf{v}) \geq d$ for all pairs of distinct codewords $\mathbf{u}$ and $\mathbf{v}$, we have
$$S \;\geq\; M(M-1)d.$$
- For another way of evaluating the sum S, we list out the M codewords in the rows of an $M \times n$ array.

$$\boxed{\begin{array}{c} \text{——— codeword 1 ———} \\ \text{——— codeword 2 ———} \\ \vdots \\ \text{——— codeword } M \text{ ———} \end{array}}$$

Proof of Plotkin Bound for Block Codes



- Consider any particular column of this array.
  - Suppose that symbol $j \in \mathbb{F}_q$ occurs m_j times in this column.
  - The other $M - m_j$ entries in this column are distinct from symbol j; each $(j, \text{not-}j)$ pair contributes 1 to the sum S.
  - So, the total contribution to S from this particular column is

$$\sum_{j \in \mathbb{F}_q} m_j(M - m_j) \;=\; M \cdot \sum_j m_j - \sum_j m_j^2 \;=\; M^2 - \sum_j m_j^2 .$$

Proof of Plotkin Bound for Block Codes

- Consider any particular column of this array.
  - The total contribution to S from this particular column is

$$\sum_{j \in \mathbb{F}_q} m_j(M - m_j) \; = \; M \cdot \sum_j m_j - \sum_j m_j^2 \; = \; M^2 - \sum_j m_j^2.$$

  - Under the restriction that $\sum_j m_j = M$, the term $\sum_j m_j^2$ is minimized by taking $m_j = M/q$ for all j. Hence,

$$M^2 - \sum_j m_j^2 \; \leq \; M^2 - \sum_j (M/q)^2 \; = \; M^2 - M^2/q \; = \; M^2\theta.$$

  - In summary, the contribution to S from this column is $\leq M^2\theta$.

Proof of Plotkin Bound for Block Codes

- Therefore, accounting for the contributions from all n columns, we have
$$S \;\leq\; nM^2\theta.$$
- Combining this with the lower bound $S \geq M(M-1)d$, we obtain
$$M(M-1)d \;\leq\; nM^2\theta.$$
- Solving for M, we find that
$$M \leq \frac{d}{d-\theta n} \quad \text{for } d > \theta n. \quad \square$$