

Codes and Cryptography

Jorge L. Villar

MAMME, Fall 2015

PART V

Outline

- 1 Block Codes and Bounds
- 2 Background on Finite Fields

Block Codes

From now on, we assume:

- An r -ary code \mathcal{C} of constant length n and size K
- A K -ary uniform source (all codewords are equally likely)
- An r -ary symmetric channel with (small) error probability α

Block Codes

From now on, we assume:

- An r -ary code \mathcal{C} of constant length n and size K
- A K -ary uniform source (all codewords are equally likely)
- An r -ary symmetric channel with (small) error probability α

In a **block code** a source stream is split into blocks (of the same size), and each block is encoded independently.

Minimum Distance and Error Correction Capacity

The **minimum distance** of \mathcal{C} is defined as

$$d_{\mathcal{C}} = \min_{x, y \in \mathcal{C}, x \neq y} d(x, y)$$

Minimum Distance and Error Correction Capacity

The **minimum distance** of \mathcal{C} is defined as

$$d_{\mathcal{C}} = \min_{x, y \in \mathcal{C}, x \neq y} d(x, y)$$

- The *nearest codeword* decoding rule always gives the right codeword if they occur at most $t = \lfloor \frac{d_{\mathcal{C}} - 1}{2} \rfloor$ errors.

Minimum Distance and Error Correction Capacity

The **minimum distance** of \mathcal{C} is defined as

$$d_{\mathcal{C}} = \min_{x, y \in \mathcal{C}, x \neq y} d(x, y)$$

- The *nearest codeword* decoding rule always gives the right codeword if they occur at most $t = \lfloor \frac{d_{\mathcal{C}}-1}{2} \rfloor$ errors. t is called the **error correction capability** of \mathcal{C} .

Minimum Distance and Error Correction Capacity

The **minimum distance** of \mathcal{C} is defined as

$$d_{\mathcal{C}} = \min_{x, y \in \mathcal{C}, x \neq y} d(x, y)$$

- The *nearest codeword* decoding rule always gives the right codeword if they occur at most $t = \lfloor \frac{d_{\mathcal{C}} - 1}{2} \rfloor$ errors. t is called the **error correction capability** of \mathcal{C} .
- \mathcal{C} can also correct up to $d_{\mathcal{C}} - 1$ erasures.

Minimum Distance and Error Correction Capacity

The **minimum distance** of \mathcal{C} is defined as

$$d_{\mathcal{C}} = \min_{x, y \in \mathcal{C}, x \neq y} d(x, y)$$

- The *nearest codeword* decoding rule always gives the right codeword if they occur at most $t = \lfloor \frac{d_{\mathcal{C}} - 1}{2} \rfloor$ errors. t is called the **error correction capability** of \mathcal{C} .
- \mathcal{C} can also correct up to $d_{\mathcal{C}} - 1$ erasures.

The **relative minimum distance** is defined as $\delta_{\mathcal{C}} = \frac{d_{\mathcal{C}}}{n}$, where n is the length of \mathcal{C} .

Singleton Bound

If we puncture \mathcal{C} at some position $i \in \{1, \dots, n\}$, and $d = d_{\mathcal{C}} > 1$, we obtain a new code \mathcal{C}' of length $n' = n - 1$, minimum distance $d' \geq d - 1$ and size $|\mathcal{C}'| = |\mathcal{C}|$.

Singleton Bound

If we puncture \mathcal{C} at some position $i \in \{1, \dots, n\}$, and $d = d_{\mathcal{C}} > 1$, we obtain a new code \mathcal{C}' of length $n' = n - 1$, minimum distance $d' \geq d - 1$ and size $|\mathcal{C}'| = |\mathcal{C}|$.

By puncturing \mathcal{C} at $d - 1$ positions we similarly obtain another code of the same size and length $n - d + 1$.

Singleton Bound

If we puncture \mathcal{C} at some position $i \in \{1, \dots, n\}$, and $d = d_{\mathcal{C}} > 1$, we obtain a new code \mathcal{C}' of length $n' = n - 1$, minimum distance $d' \geq d - 1$ and size $|\mathcal{C}'| = |\mathcal{C}|$.

By puncturing \mathcal{C} at $d - 1$ positions we similarly obtain another code of the same size and length $n - d + 1$.

Therefore,

$$|\mathcal{C}| \leq r^{n-d+1}$$

Singleton Bound

If we puncture \mathcal{C} at some position $i \in \{1, \dots, n\}$, and $d = d_{\mathcal{C}} > 1$, we obtain a new code \mathcal{C}' of length $n' = n - 1$, minimum distance $d' \geq d - 1$ and size $|\mathcal{C}'| = |\mathcal{C}|$.

By puncturing \mathcal{C} at $d - 1$ positions we similarly obtain another code of the same size and length $n - d + 1$.

Therefore,

$$|\mathcal{C}| \leq r^{n-d+1}$$

or equivalently, in terms of the code rate,

$$R = \frac{\log_r |\mathcal{C}|}{n} \leq 1 - \delta + \frac{1}{n}$$

MDS Codes

Codes achieving the equality in Singleton bound are called **Maximum Distance Separable** or **MDS**.

MDS Codes

Codes achieving the equality in Singleton bound are called **Maximum Distance Separable** or **MDS**.

Examples of them are

- the trivial code, $\{0, \dots, r-1\}^n$
- the repetition code, $\mathcal{C}_{rep} = \{0^n, \dots, (r-1)^n\}$
- the “hyperplane”
 $\mathcal{C} = \{\mathbf{x} \in \{0, \dots, r-1\}^n \mid x_1 + \dots + x_n = 0\}$
 $|\mathcal{C}| = r^{n-1}$, $d_{\mathcal{C}} = 2$, it corrects up to 1 erasure, but no errors

MDS Codes

Codes achieving the equality in Singleton bound are called **Maximum Distance Separable** or **MDS**.

Examples of them are

- the trivial code, $\{0, \dots, r-1\}^n$
- the repetition code, $\mathcal{C}_{rep} = \{0^n, \dots, (r-1)^n\}$
- the “hyperplane”
 $\mathcal{C} = \{\mathbf{x} \in \{0, \dots, r-1\}^n \mid x_1 + \dots + x_n = 0\}$
 $|\mathcal{C}| = r^{n-1}$, $d_{\mathcal{C}} = 2$, it corrects up to 1 erasure, but no errors

The only MDS codes for $r = 2$ and d odd are the trivial and the repetition codes.

Sphere Packing (Hamming) Bound

Given any code \mathcal{C} of length n and minimum distance $d > 1$, the spheres in $\{0, \dots, r-1\}^n$ of radius $t = \lfloor \frac{d-1}{2} \rfloor$ centered at codewords of \mathcal{C} are disjoint. Therefore,

$$|\mathcal{C}| \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$$

Codes achieving the equality are called **Perfect**.

Sphere Packing (Hamming) Bound

Given any code \mathcal{C} of length n and minimum distance $d > 1$, the spheres in $\{0, \dots, r-1\}^n$ of radius $t = \lfloor \frac{d-1}{2} \rfloor$ centered at codewords of \mathcal{C} are disjoint. Therefore,

$$|\mathcal{C}| \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$$

Codes achieving the equality are called **Perfect**.

If \mathcal{C} is a binary MDS code, $1 + n + \dots + \binom{n}{t} \leq \frac{2^n}{|\mathcal{C}|} = 2^{d-1}$

Sphere Packing (Hamming) Bound

Given any code \mathcal{C} of length n and minimum distance $d > 1$, the spheres in $\{0, \dots, r-1\}^n$ of radius $t = \lfloor \frac{d-1}{2} \rfloor$ centered at codewords of \mathcal{C} are disjoint. Therefore,

$$|\mathcal{C}| \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$$

Codes achieving the equality are called **Perfect**.

If \mathcal{C} is a binary MDS code, $1 + n + \dots + \binom{n}{t} \leq \frac{2^n}{|\mathcal{C}|} = 2^{d-1}$

Using now $n \geq d \geq 2t + 1$,

$$1 + n + \dots + \binom{n}{t} \geq 1 + (2t + 1) + \dots + \binom{2t+1}{t} = 2^{2t}$$

Sphere Packing (Hamming) Bound

Given any code \mathcal{C} of length n and minimum distance $d > 1$, the spheres in $\{0, \dots, r-1\}^n$ of radius $t = \lfloor \frac{d-1}{2} \rfloor$ centered at codewords of \mathcal{C} are disjoint. Therefore,

$$|\mathcal{C}| \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$$

Codes achieving the equality are called **Perfect**.

If \mathcal{C} is a binary MDS code, $1 + n + \dots + \binom{n}{t} \leq \frac{2^n}{|\mathcal{C}|} = 2^{d-1}$

Using now $n \geq d \geq 2t + 1$,

$$1 + n + \dots + \binom{n}{t} \geq 1 + (2t + 1) + \dots + \binom{2t+1}{t} = 2^{2t}$$

If $d \geq 3$ is odd, $d - 1 = 2t$, and then $n = d$, $|\mathcal{C}| = 2$, and \mathcal{C} can only be the repetition code.

Plotkin Bound

For a random $X = (X_1, \dots, X_n) \in \mathcal{C}$, define $p_{i,j} = \Pr(X_i = j)$.

Plotkin Bound

For a random $X = (X_1, \dots, X_n) \in \mathcal{C}$, define $p_{i,j} = \Pr(X_i = j)$.

Now, for two independent random codewords X, Y ,

$$E(d(X, Y)) = \sum_{i=1}^n \Pr(X_i \neq Y_i) = \sum_{i=1}^n \left(1 - \sum_{j=0}^{r-1} p_{i,j}^2 \right) \leq \sum_{i=1}^n \left(1 - \frac{1}{r} \right)$$

where the last inequality comes from $\|\mathbf{v}\|_1^2 \leq r\|\mathbf{v}\|_2^2$, for $\mathbf{v} \in \mathbb{R}^r$.

Plotkin Bound

For a random $X = (X_1, \dots, X_n) \in \mathcal{C}$, define $p_{i,j} = \Pr(X_i = j)$.

Now, for two independent random codewords X, Y ,

$$E(d(X, Y)) = \sum_{i=1}^n \Pr(X_i \neq Y_i) = \sum_{i=1}^n \left(1 - \sum_{j=0}^{r-1} p_{i,j}^2 \right) \leq \sum_{i=1}^n \left(1 - \frac{1}{r} \right)$$

where the last inequality comes from $\|\mathbf{v}\|_1^2 \leq r\|\mathbf{v}\|_2^2$, for $\mathbf{v} \in \mathbb{R}^r$.

Therefore,

$$d_{\mathcal{C}} \left(1 - \frac{1}{|\mathcal{C}|} \right) = d_{\mathcal{C}} \Pr(X \neq Y) \leq E(d(X, Y)) \leq n \left(1 - \frac{1}{r} \right)$$

Plotkin Bound

For a random $X = (X_1, \dots, X_n) \in \mathcal{C}$, define $p_{i,j} = \Pr(X_i = j)$.

Now, for two independent random codewords X, Y ,

$$\mathbb{E}(d(X, Y)) = \sum_{i=1}^n \Pr(X_i \neq Y_i) = \sum_{i=1}^n \left(1 - \sum_{j=0}^{r-1} p_{i,j}^2 \right) \leq \sum_{i=1}^n \left(1 - \frac{1}{r} \right)$$

where the last inequality comes from $\|\mathbf{v}\|_1^2 \leq r\|\mathbf{v}\|_2^2$, for $\mathbf{v} \in \mathbb{R}^r$.

Therefore,

$$d_{\mathcal{C}} \left(1 - \frac{1}{|\mathcal{C}|} \right) = d_{\mathcal{C}} \Pr(X \neq Y) \leq \mathbb{E}(d(X, Y)) \leq n \left(1 - \frac{1}{r} \right)$$

and for any $d_{\mathcal{C}} > \frac{r-1}{r}n$, $|\mathcal{C}| \leq \frac{rd_{\mathcal{C}}}{rd_{\mathcal{C}} - (r-1)n}$

Example

$$\mathcal{C} = \{0000, 0122, 0211, 1012, 1101, 1220, 2021, 2110, 2202\}$$

Example

$$\mathcal{C} = \{0000, 0122, 0211, 1012, 1101, 1220, 2021, 2110, 2202\}$$

- $r = 3$, $n = 4$, $|\mathcal{C}| = 9$, $d = 3$
- \mathcal{C} corrects one error and has a rate $R = 1/2$ (while \mathcal{C}_{rep} with $n = 3$ also corrects one error, but at a rate $1/3$).
- \mathcal{C} is MDS and perfect, since $|\mathcal{C}| = 3^{n-d+1}$ and $|\mathcal{C}| = \frac{3^n}{1+2n}$
- \mathcal{C} satisfies the equality in Plotkin bound, since $|\mathcal{C}| = \frac{3d}{3d-2n}$

Example

$$\mathcal{C} = \{0000, 0122, 0211, 1012, 1101, 1220, 2021, 2110, 2202\}$$

- $r = 3$, $n = 4$, $|\mathcal{C}| = 9$, $d = 3$
- \mathcal{C} corrects one error and has a rate $R = 1/2$ (while \mathcal{C}_{rep} with $n = 3$ also corrects one error, but at a rate $1/3$).
- \mathcal{C} is MDS and perfect, since $|\mathcal{C}| = 3^{n-d+1}$ and $|\mathcal{C}| = \frac{3^n}{1+2n}$
- \mathcal{C} satisfies the equality in Plotkin bound, since $|\mathcal{C}| = \frac{3d}{3d-2n}$

Actually, \mathcal{C} can be seen as a vector subspace in \mathbb{F}_3^4 (so codewords can be added or multiplied by scalars in \mathcal{C}).

Example

$$\mathcal{C} = \{0000, 0122, 0211, 1012, 1101, 1220, 2021, 2110, 2202\}$$

- $r = 3$, $n = 4$, $|\mathcal{C}| = 9$, $d = 3$
- \mathcal{C} corrects one error and has a rate $R = 1/2$ (while \mathcal{C}_{rep} with $n = 3$ also corrects one error, but at a rate $1/3$).
- \mathcal{C} is MDS and perfect, since $|\mathcal{C}| = 3^{n-d+1}$ and $|\mathcal{C}| = \frac{3^n}{1+2n}$
- \mathcal{C} satisfies the equality in Plotkin bound, since $|\mathcal{C}| = \frac{3d}{3d-2n}$

Actually, \mathcal{C} can be seen as a vector subspace in \mathbb{F}_3^4 (so codewords can be added or multiplied by scalars in \mathcal{C}).

Furthermore, it can be seen as the ideal generated by the polynomial $X^2 + 2X + 2$ in the quotient ring $\mathbb{F}_3[X]/(X^4 + 1)$ e.g., the codeword 1012 corresponds to the polynomial $X^3 + X + 2 = (X + 1)(X^2 + 2X + 2)$

Maximal Codes

An r -ary code \mathcal{C} of length n and minimum distance d is called **maximal** if it has the maximum possible size. We denote the size of a maximal code as $A_r(n, d)$.

Maximal Codes

An r -ary code \mathcal{C} of length n and minimum distance d is called **maximal** if it has the maximum possible size. We denote the size of a maximal code as $A_r(n, d)$.

Every of the previous bounds (Singleton, Hamming and Plotkin) are indeed upper bounds for $A_r(n, d)$. Namely

- $A_r(n, d) \leq r^{n-d+1}$
- $A_r(n, d) \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$
- if $d > \frac{r-1}{r}n$ then $A_r(n, d) \leq \frac{rd_{\mathcal{C}}}{rd_{\mathcal{C}} - (r-1)n}$

Maximal Codes

An r -ary code \mathcal{C} of length n and minimum distance d is called **maximal** if it has the maximum possible size. We denote the size of a maximal code as $A_r(n, d)$.

Every of the previous bounds (Singleton, Hamming and Plotkin) are indeed upper bounds for $A_r(n, d)$. Namely

- $A_r(n, d) \leq r^{n-d+1}$
- $A_r(n, d) \leq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{t}(r-1)^t}$
- if $d > \frac{r-1}{r}n$ then $A_r(n, d) \leq \frac{rd_{\mathcal{C}}}{rd_{\mathcal{C}} - (r-1)n}$

On the other hand, every construction of a code gives a lower bound for $A_r(n, d)$. But there is a known non-constructive lower bound.

Gilbert-Varshamov Bound

Given a maximal r -ary code \mathcal{C} of length n and minimum distance d , the spheres in $\{0, \dots, r-1\}^n$ of radius $d-1$ centered at codewords of \mathcal{C} must cover all the space.

Otherwise, any $x \in \{0, \dots, r-1\}^n$ outside all spheres can be added to \mathcal{C} as a new codeword, without decreasing the minimum distance.

Gilbert-Varshamov Bound

Given a maximal r -ary code \mathcal{C} of length n and minimum distance d , the spheres in $\{0, \dots, r-1\}^n$ of radius $d-1$ centered at codewords of \mathcal{C} must cover all the space.

Otherwise, any $x \in \{0, \dots, r-1\}^n$ outside all spheres can be added to \mathcal{C} as a new codeword, without decreasing the minimum distance. Therefore,

$$A_r(n, d) \geq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{d-1}(r-1)^{d-1}}$$

Gilbert-Varshamov Bound

Given a maximal r -ary code \mathcal{C} of length n and minimum distance d , the spheres in $\{0, \dots, r-1\}^n$ of radius $d-1$ centered at codewords of \mathcal{C} must cover all the space.

Otherwise, any $x \in \{0, \dots, r-1\}^n$ outside all spheres can be added to \mathcal{C} as a new codeword, without decreasing the minimum distance. Therefore,

$$A_r(n, d) \geq \frac{r^n}{1 + n(r-1) + \dots + \binom{n}{d-1}(r-1)^{d-1}}$$

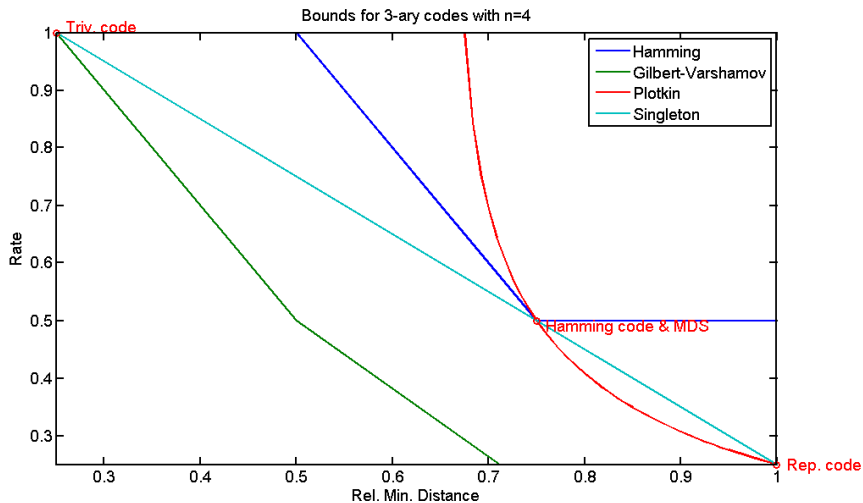
The **covering radius** of a code \mathcal{C} is defined as

$$\rho_{\mathcal{C}} = \max_{x \in \{0, \dots, r-1\}^n \setminus \mathcal{C}} d(x, \mathcal{C})$$

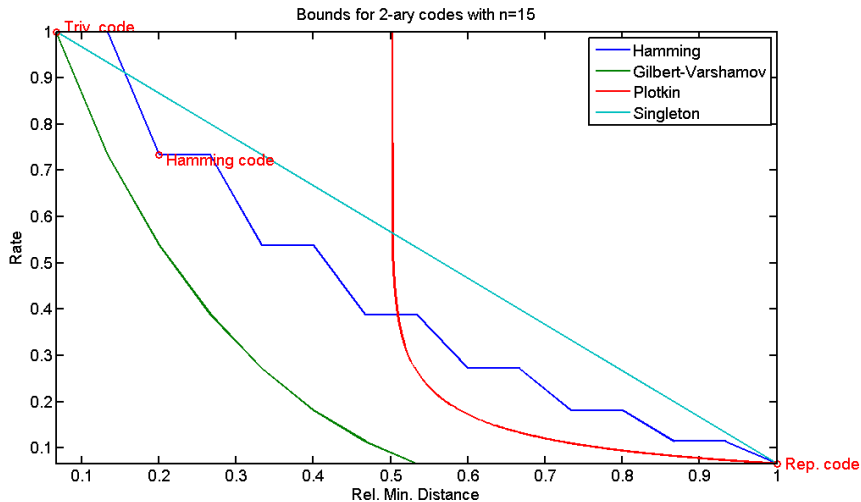
where

$$d(x, \mathcal{C}) = \min_{y \in \mathcal{C}} d(x, y)$$

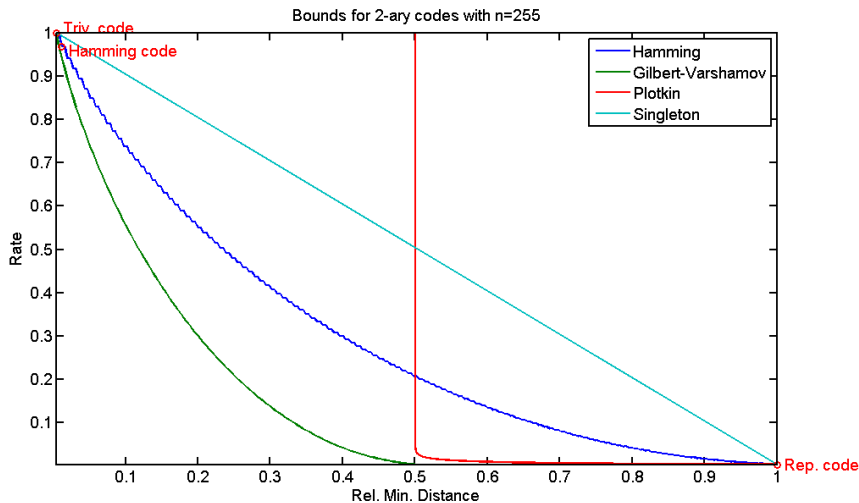
Plot of the Bounds (I)



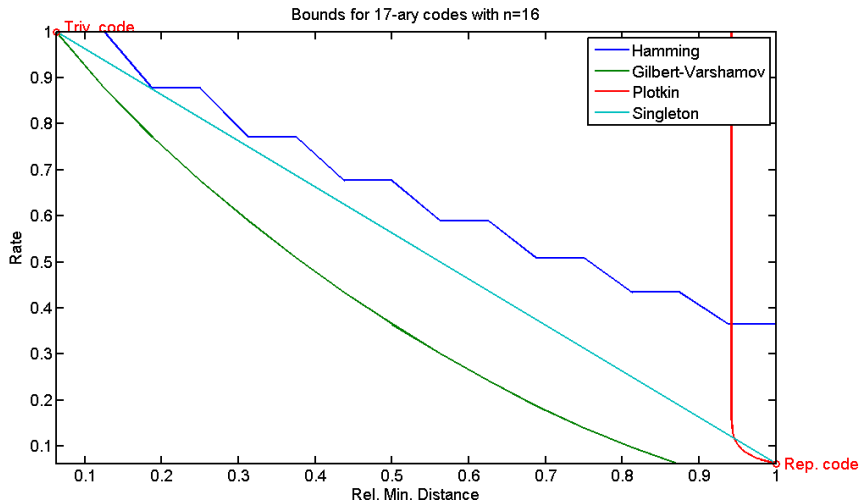
Plot of the Bounds (II)



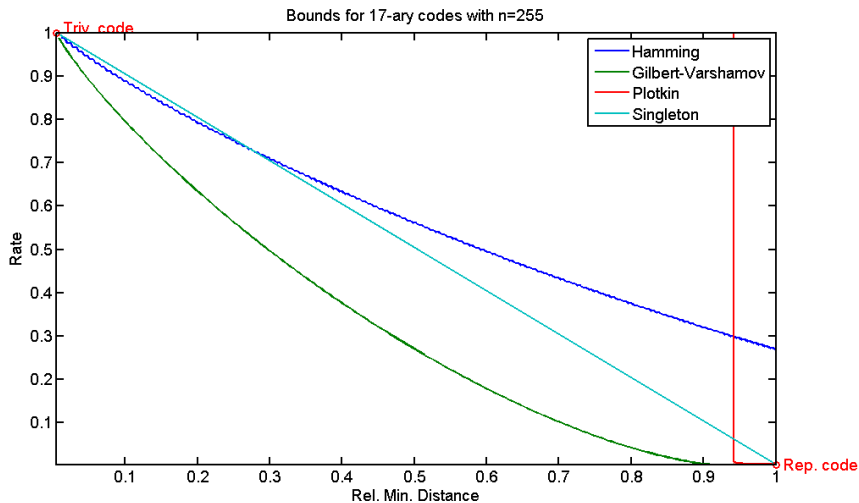
Plot of the Bounds (III)



Plot of the Bounds (IV)



Plot of the Bounds (V)



Outline

- 1 Block Codes and Bounds
- 2 Background on Finite Fields**

Prime Fields

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only n is prime. We denote it as $GF(n)$ or \mathbb{F}_n . It is usually known as a **prime field**.

If n is a composite integer then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors. On the other hand, Bezout's inequality guarantees the existence on inverses modulo n when n is prime.

Prime Fields

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only n is prime. We denote it as $GF(n)$ or \mathbb{F}_n . It is usually known as a **prime field**.

If n is a composite integer then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors. On the other hand, Bezout's inequality guarantees the existence on inverses modulo n when n is prime.

The **characteristic** of a finite field \mathbb{K} , $\text{char}(\mathbb{K})$, is the minimum positive integer p such that $p1_{\mathbb{K}} = 0_{\mathbb{K}}$. It is always a prime number. (Otherwise, \mathbb{K} would have zero divisors.)

Subfields (I)

\mathbb{F}_p is always a subfield of any finite field \mathbb{K} with $\text{char}(\mathbb{K}) = p$.
Therefore, \mathbb{K} is a \mathbb{F}_p -vector space, and has cardinality $q = p^e$
for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

Subfields (I)

\mathbb{F}_p is always a subfield of any finite field \mathbb{K} with $\text{char}(\mathbb{K}) = p$. Therefore, \mathbb{K} is a \mathbb{F}_p -vector space, and has cardinality $q = p^e$ for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

Similarly, if \mathbb{K} is a finite field and \mathbb{K}' is a subfield, then \mathbb{K} is a \mathbb{K}' -vector space. Therefore, if \mathbb{K} has $q = p^e$ elements then \mathbb{K}' has $q' = p^d$ elements for some $d \mid e$.

Subfields (I)

\mathbb{F}_p is always a subfield of any finite field \mathbb{K} with $\text{char}(\mathbb{K}) = p$. Therefore, \mathbb{K} is a \mathbb{F}_p -vector space, and has cardinality $q = p^e$ for some $e \geq 1$.

Then any finite field is a finite **extension** of a prime field.

Similarly, if \mathbb{K} is a finite field and \mathbb{K}' is a subfield, then \mathbb{K} is a \mathbb{K}' -vector space. Therefore, if \mathbb{K} has $q = p^e$ elements then \mathbb{K}' has $q' = p^d$ elements for some $d \mid e$.

E.g., a field with 2^{15} elements can only have proper subfields of cardinalities 2 , 2^3 and 2^5 .

Primitive Elements

Theorem

For any finite field \mathbb{K} , the multiplicative group \mathbb{K}^\times is cyclic.

Primitive Elements

Theorem

For any finite field \mathbb{K} , the multiplicative group \mathbb{K}^\times is cyclic.

Assume \mathbb{K} has p^e elements. Since \mathbb{K}^\times is an abelian finite group, it is the direct product of r cycles of lengths l_1, l_2, \dots, l_r fulfilling $l_1 \mid l_2 \mid \dots \mid l_r$.

But the order of the group is $p^e - 1 = l_1 l_2 \dots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.

Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Primitive Elements

Theorem

For any finite field \mathbb{K} , the multiplicative group \mathbb{K}^\times is cyclic.

Assume \mathbb{K} has p^e elements. Since \mathbb{K}^\times is an abelian finite group, it is the direct product of r cycles of lengths l_1, l_2, \dots, l_r fulfilling $l_1 \mid l_2 \mid \dots \mid l_r$.

But the order of the group is $p^e - 1 = l_1 l_2 \dots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.

Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Every generator α of \mathbb{K}^\times is called a **primitive** element.

Primitive Elements

Theorem

For any finite field \mathbb{K} , the multiplicative group \mathbb{K}^\times is cyclic.

Assume \mathbb{K} has p^e elements. Since \mathbb{K}^\times is an abelian finite group, it is the direct product of r cycles of lengths l_1, l_2, \dots, l_r fulfilling $l_1 \mid l_2 \mid \dots \mid l_r$.

But the order of the group is $p^e - 1 = l_1 l_2 \dots l_r$, and all $x \in \mathbb{K}^\times$ fulfils $x^{l_r} = 1$.

Therefore, the polynomial $X^{l_r} - 1 \in \mathbb{K}[X]$ has at least $p^e - 1$ roots, which is only possible if $l_r \geq p^e - 1$, and then $r = 1$.

Every generator α of \mathbb{K}^\times is called a **primitive** element.

In particular, we can write $\mathbb{K} = \{0, 1 = \alpha^0, \alpha^1, \dots, \alpha^{p^e-2}\}$

Fröbenius Automorphism (I)

Given a finite field \mathbb{K} of characteristic p , the map $\phi_p : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_p(x) = x^p$ is a field automorphism.

Fröbenius Automorphism (I)

Given a finite field \mathbb{K} of characteristic p , the map $\phi_p : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_p(x) = x^p$ is a field automorphism.

$\phi_p(0) = 0$ and ϕ_p is a bijection in \mathbb{K}^\times , as $\gcd(p, p^e - 1) = 1$

$$\phi_p(xy) = (xy)^p = x^p y^p = \phi_p(x)\phi_p(y)$$

$$\phi_p(x+y) = (x+y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} = x^p + y^p = \phi_p(x) + \phi_p(y)$$

since for any prime p , and $0 < i < p$, $\binom{p}{i} \equiv 0 \pmod{p}$.

Fröbenius Automorphism (I)

Given a finite field \mathbb{K} of characteristic p , the map $\phi_p : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_p(x) = x^p$ is a field automorphism.

$\phi_p(0) = 0$ and ϕ_p is a bijection in \mathbb{K}^\times , as $\gcd(p, p^e - 1) = 1$

$$\phi_p(xy) = (xy)^p = x^p y^p = \phi_p(x)\phi_p(y)$$

$$\phi_p(x+y) = (x+y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} = x^p + y^p = \phi_p(x) + \phi_p(y)$$

since for any prime p , and $0 < i < p$, $\binom{p}{i} \equiv 0 \pmod{p}$.

Moreover, for any polynomial $g \in \mathbb{F}_q[X]$ and $x \in \mathbb{K}$,

$\phi_p(g(x)) = g(\phi_p(x))$ (since elements in \mathbb{F}_p are fixed by ϕ_p).

Thus, if α is a root of g , so do $\alpha^p, \alpha^{p^2}, \dots$. We call all of them **conjugate** roots.

Fröbenius Automorphism (II)

We can do the same thing with respect to a subfield \mathbb{K}' with cardinality $q = p^d$ of a finite field \mathbb{K} of characteristic p .

$\phi_q : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_q(x) = x^q$ is a field automorphism, which fixes the elements in \mathbb{K}' . ($\phi_q = \phi_p \circ \dots \circ \phi_p$)

Fröbenius Automorphism (II)

We can do the same thing with respect to a subfield \mathbb{K}' with cardinality $q = p^d$ of a finite field \mathbb{K} of characteristic p .

$\phi_q : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_q(x) = x^q$ is a field automorphism, which fixes the elements in \mathbb{K}' . ($\phi_q = \phi_p \circ \dots \circ \phi_p$)

Moreover, for any polynomial $g \in \mathbb{K}'[X]$ and $x \in \mathbb{K}$,
 $\phi_q(g(x)) = g(\phi_q(x))$

Thus, if α is a root of g , so do $\alpha^q, \alpha^{q^2}, \dots$

Fröbenius Automorphism (II)

We can do the same thing with respect to a subfield \mathbb{K}' with cardinality $q = p^d$ of a finite field \mathbb{K} of characteristic p .

$\phi_q : \mathbb{K} \rightarrow \mathbb{K}$ defined as $\phi_q(x) = x^q$ is a field automorphism, which fixes the elements in \mathbb{K}' . ($\phi_q = \phi_p \circ \dots \circ \phi_p$)

Moreover, for any polynomial $g \in \mathbb{K}'[X]$ and $x \in \mathbb{K}$,
 $\phi_q(g(x)) = g(\phi_q(x))$

Thus, if α is a root of g , so do $\alpha^q, \alpha^{q^2}, \dots$

Theorem (Galois)

For any finite field \mathbb{K} and subfield \mathbb{K}' , the automorphisms of \mathbb{K} that fix \mathbb{K}' are exactly the powers of ϕ_q , where $q = |\mathbb{K}'|$.

Subfields (II)

Given a finite field \mathbb{K} with p^e elements, all $x \in \mathbb{K}$ satisfies $x^{p^e} = x$, that is, the elements of \mathbb{K} are the roots of $X^{p^e} - X$, and then

$$X^{p^e} - X = \prod_{x \in \mathbb{K}} (X - x) = X \prod_{i=0}^{p^e-2} (X - \alpha^i)$$

where α is a primitive element of \mathbb{K} .

Subfields (II)

Given a finite field \mathbb{K} with p^e elements, all $x \in \mathbb{K}$ satisfies $x^{p^e} = x$, that is, the elements of \mathbb{K} are the roots of $X^{p^e} - X$, and then

$$X^{p^e} - X = \prod_{x \in \mathbb{K}} (X - x) = X \prod_{i=0}^{p^e-2} (X - \alpha^i)$$

where α is a primitive element of \mathbb{K} .

Now, if \mathbb{K}' is a subfield with p^d elements, all $x \in \mathbb{K}'$ also satisfies $x^{p^d} = x$. Then, \mathbb{K}' is the set of roots of $X^{p^d} - X$.

Lemma

$$X^{p^d} - X \mid X^{p^e} - X \quad \Leftrightarrow \quad p^d - 1 \mid p^e - 1 \quad \Leftrightarrow \quad d \mid e$$

Minimal Polynomials

Given a finite field \mathbb{K} with p^e elements, for any nonzero $x \in \mathbb{K}$ we define its **minimal polynomial**, $m_x \in \mathbb{F}_p[X]$ as the monic polynomial of minimal degree such that $m_x(x) = 0$. (It is the monic generator of the ideal of the polynomials vanishing at x .)

Minimal Polynomials

Given a finite field \mathbb{K} with p^e elements, for any nonzero $x \in \mathbb{K}$ we define its **minimal polynomial**, $m_x \in \mathbb{F}_p[X]$ as the monic polynomial of minimal degree such that $m_x(x) = 0$. (It is the monic generator of the ideal of the polynomials vanishing at x .)

m_x is irreducible in $\mathbb{F}_p[X]$ and its roots are the conjugates of x , i.e. $x, x^p, x^{p^2}, \dots, x^{p^{d-1}}$, where d is the degree of m_x .

Minimal Polynomials

Given a finite field \mathbb{K} with p^e elements, for any nonzero $x \in \mathbb{K}$ we define its **minimal polynomial**, $m_x \in \mathbb{F}_p[X]$ as the monic polynomial of minimal degree such that $m_x(x) = 0$. (It is the monic generator of the ideal of the polynomials vanishing at x .)

m_x is irreducible in $\mathbb{F}_p[X]$ and its roots are the conjugates of x , i.e. $x, x^p, x^{p^2}, \dots, x^{p^{d-1}}$, where d is the degree of m_x .

Then, $x^{p^d} = x$ and $x^{p^e} = x$, which is only possible if $d \mid e$. Moreover, x lies in the subfield of q^d elements.

Minimal Polynomials

Given a finite field \mathbb{K} with p^e elements, for any nonzero $x \in \mathbb{K}$ we define its **minimal polynomial**, $m_x \in \mathbb{F}_p[X]$ as the monic polynomial of minimal degree such that $m_x(x) = 0$. (It is the monic generator of the ideal of the polynomials vanishing at x .)

m_x is irreducible in $\mathbb{F}_p[X]$ and its roots are the conjugates of x , i.e. $x, x^p, x^{p^2}, \dots, x^{p^{d-1}}$, where d is the degree of m_x .

Then, $x^{p^d} = x$ and $x^{p^e} = x$, which is only possible if $d \mid e$. Moreover, x lies in the subfield of q^d elements.

Summarizing,

$$m_x = \prod_{i=0}^{d-1} (X - x^{p^i}) \quad \text{for some } d \mid e$$

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Corollary

The irreducible factors of $X^{p^e} - X$ in $\mathbb{F}_p[X]$ are exactly the irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing e

Irreducible Polynomials

Lemma

A polynomial $g \in \mathbb{F}_p[X]$ of degree $e > 0$ is irreducible if and only if $g \mid X^{p^e} - X$, but $g \nmid X^{p^d} - X$ for all nontrivial $d \mid e$.

Corollary

The irreducible factors of $X^{p^e} - X$ in $\mathbb{F}_p[X]$ are exactly the irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing e

Let $n_e(p)$ be the no. of irred. polynomials of degree e in $\mathbb{F}_p[X]$.

Corollary

$$\sum_{d|e} dn_d(p) = p^e \quad \text{and} \quad 0 \leq \frac{p^e - 2p^{\lfloor e/2 \rfloor}}{e} < n_e(p) \leq \frac{p^e - p}{e}$$

Construction of Finite Fields

The quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$ is a field if and only if g is an irreducible polynomial in $\mathbb{F}_p[X]$. If g has degree e , then the field has p^e elements.

Construction of Finite Fields

The quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$ is a field if and only if g is an irreducible polynomial in $\mathbb{F}_p[X]$. If g has degree e , then the field has p^e elements.

Theorem

For every prime p and for every $e \geq 1$ there exists a unique (up to isomorphism) finite field with p^e elements.

The finite field with p^e elements, denoted as $GF(p^e)$ or \mathbb{F}_{p^e} , can always be constructed as the quotient ring $\mathbb{F}_p[X]/g\mathbb{F}_p[X]$, for any irreducible polynomial $g \in \mathbb{F}_p[X]$ of degree e .

Example: \mathbb{F}_{2^8}

$$\mathbb{F}_2 = \{0, 1\}$$

$g = X^8 + X^4 + X^3 + X^2 + 1$ is irreducible in $\mathbb{F}_2[X]$

$$\mathbb{F}_{2^8} = \mathbb{F}_2[X]/g\mathbb{F}_2[X]$$

Addition:

$$(X^7 + X^4 + X) + (X^6 + X^5 + X^4 + 1) = X^7 + X^6 + X^5 + X + 1$$

$$10010010 + 01110001 = 11100011$$

Multiplication: $(X^7 + X^4 + X) * (X^6 + X^5 + X^4 + 1) =$
 $X^7 + X + 1 + (X^5 + X^4 + X^3 + X^2 + 1)g$

$$10010010 * 01110001 = 10000011$$

Example: \mathbb{F}_{2^8}

Primitive element: $\alpha = X$ or 00000010

$$|\mathbb{F}_{2^8}^\times| = 2^8 - 1 = 255 = 3 * 5 * 17$$

$$\alpha^{255/17} = X^5 + X^2 + X \quad \text{or } 00100110$$

$$\alpha^{255/5} = X^3 + X \quad \text{or } 00001010$$

$$\alpha^{255/3} = X^7 + X^6 + X^4 + X^2 + X \quad \text{or } 11010110$$

$$\alpha^{255} = 1 \quad \text{or } 00000001$$

Codes and Cryptography

Jorge L. Villar

MAMME, Fall 2015

END OF PART V