Coding Theory
Lecture 8: Bounds on the parameters of the code
• It is easy to construct optimal codes with minimum distance $d = 1 - 4$. Their dual codes have minimum distance $d \approx n/2$. However, all these codes are not asymptotically optimal (either rate or minimum distance tends to 0 when length tends to infinity).

• In order to say about efficiency of a certain class of codes we need to know upper and lower bounds on achievable code parameters.
Singleton bound

**Theorem**

Let $\mathcal{C}$ be an $(n, M, d)$-code over a finite field $\mathbb{F}_q$. Then $M \leq q^{n-d+1}$.

**Proof.**

Assume by contrary that $M > q^{n-d+1}$. Then there are two codewords $u \in \mathcal{C}$ and $v \in \mathcal{C}$ that coincide in their $n-d+1$ coordinates. Thus, the Hamming distance between those two codewords is at most $d-1$. This is a contradiction, since we assumed that the minimum Hamming distance of $\mathcal{C}$ is $d$. \hfill $\blacksquare$
Singleton bound for linear codes

Singleton bound for a linear \([n, k, d]\) code over \(\mathbb{F}_q\) can be restated as follows:

\[ q^k \leq q^{n-d+1}, \]

or

\[ k + d - 1 \leq n. \]

**Definition**
A code that achieves the Singleton bound, is called **maximum distance separable** (MDS).

Examples of MDS codes

- A linear \([n, n, 1]\) code over \(\mathbb{F}_q\).
- The \([n, n - 1, 2]\) single parity-check code over \(\mathbb{F}_q\).
- The \([n, 1, n]\) repetition code over \(\mathbb{F}_q\).
- Reed-Solomon code.
Definition
A sphere of radius $t > 0$ around a vector $\mathbf{v} \in \mathbb{F}_q^n$ is defined as

$$S_{t,n}(\mathbf{v}) = \{ \mathbf{x} \in \mathbb{F}_q^n : d(\mathbf{x}, \mathbf{v}) \leq t \}.$$

That sphere contains all vectors in $\mathbb{F}_q^n$, which are located at the Hamming distance at most $t$ from $\mathbf{v}$. For any $\mathbf{v} \in \mathbb{F}_q^n$, the size of a sphere of radius $t > 0$ is given by the following expression:

$$S_{t,n} = S_{t,n}(\mathbf{v}) = \sum_{i=0}^{t} \binom{n}{i} (q - 1)^i.$$
Let $C$ be an $(n, M, d)$ code over $\mathbb{F}_q^n$. Consider a collection of spheres of radius $t = \lfloor (d - 1)/2 \rfloor$ around the codewords of $C$. These spheres have to be disjoint. Otherwise, assume that the spheres around codewords $c_i \in C$ and $c_j \in C$, $c_i \neq c_j$, have a nonempty intersection. Take a vector $x$ in this intersection. We obtain that $d(x, c_i) \leq \lfloor (d - 1)/2 \rfloor$ and $d(x, c_j) \leq \lfloor (d - 1)/2 \rfloor$. The triangle inequality yields that $d(c_i, c_j) \leq d - 1$, in contradiction to the fact that $d$ is the minimum distance of $C$. 
Sphere-packing/Hamming bound

\[ t = \left\lfloor \frac{d-1}{2} \right\rfloor \]

\[ c_1, c_2, c_3 \]

\[ \geq d \]

\[ F^n \]
Since all spheres have to be disjoint, and all together are contained in $\mathbb{F}_q^n$, we obtain the following inequality, which is known as the Hamming bound or sphere-packing bound.

\[
MS\left\lfloor \frac{d-1}{2} \right\rfloor, n \leq q^n
\]

or, equivalently,

\[
M \sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i}(q - 1)^i \leq q^n
\]
If $C$ is a linear $[n, k, d]$ code, then the Hamming bounds becomes:

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

The code that attains this bound with equality is called \textit{perfect}.
Example

Let $C$ be a binary $[n, 1, n]$ repetition code, and $n$ be an odd integer.

$$S_{(n-1)/2,n} = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i}$$

Taking into account that $\binom{n}{i} = \binom{n}{n-i}$ and $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ we obtain that

$$S_{(n-1)/2,n} = \sum_{i=\frac{n-1}{2}+1}^{n} \binom{n}{i} = \frac{1}{2} \sum_{i=0}^{n} \binom{n}{i} = 2^{n-1}$$

or

$$2S_{(n-1)/2,n} = 2^n$$
Example

Let $C$ be a binary $[n, n - m, 3]$ Hamming code, where $m > 1$ and $n = 2^m - 1$.

$$S_{1,n} = 1 + n = 2^m.$$  

We obtain that

$$2^{n-m}S_{1,n} = 2^n,$$

and therefore the code $C$ is perfect.
Example

Other perfect codes include:

- The $q$-ary Hamming code.
- The $[23, 12, 7]$ Golay code over $\mathbb{F}_2$.
Theorem

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

$$S_{d-2,n-1} < q^{n-k}. \quad (1)$$

Then there exists a \textit{linear} $[n, k, \geq d]$ code over $\mathbb{F}_q$. 
Proof.
We construct an \((n - k) \times n\) \(H\), such that any \(d - 1\) columns are linearly independent. We start with \((n - k) \times (n - k)\) \(I_{n-k}\). Assume that \(l - 1\) columns \((h_1, h_2, \ldots, h_{l-1})\) are selected. A vector in \(\mathbb{F}_q^{n-k}\) can not be selected as an \(l\)-th column iff it can be expressed as a linear combination of any \(d - 2\) existing columns from \((h_1, h_2, \ldots, h_{l-1})\). The number of such linear combinations is:

\[
\sum_{i=0}^{d-2} \binom{l - 1}{i} (q - 1)^i
\]

which is equal to \(S_{d-2, l-1}\). \(\square\)
In order to be able to select an \( l \)-th column, it is sufficient to require that \( S_{d-2,l-1} < q^{n-k} \) (i.e. there exists a suitable vector).

From (1), we have that \( S_{d-2,n-1} < q^{n-k} \). However, in that case, for any \( l \leq n \) we have \( S_{d-2,l-1} \leq S_{d-2,n-1} < q^{n-k} \), which means that we are able to add a column to \( H \).

The first two bounds are upper bounds on the parameters of the code (every code satisfies them). The third bound is a lower bound (i.e., there exists a code that satisfies that bound).
Grismer bound

Theorem

\[ N(k, d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil, \]

where \( N(k, d) \) denotes minimal possible length of a binary linear code of dimension \( k \) and minimum distance \( d \).

Proof is based on the following lemma.

Lemma

\[ N(k, d) \geq d + N(k - 1, \left\lceil \frac{d}{2} \right\rceil) \]
Proof.
Let \( n = N(k, d) \), we represent a generator matrix \( G \) in the form

\[
G = \begin{pmatrix}
0^{N(k,d)-d} & 1^d \\
G_1 & G_2
\end{pmatrix}
\]

Let minimal weight of a codeword of \( G_1 \) satisfies \( d_1 < d/2 \) and its continuation has weight \( d - d_1 > d/2 \). By summing up this codeword with the first row of \( G \) we obtain that the right part of the codeword has weight \( < d/2 \), that is the initial code has minimum distance \( < d \). This is contradiction and means that the code determined by \( G_1 \) has minimum distance \( \geq d/2 \), that is, at least \( \lceil d/2 \rceil \). Applying Lemma \( (k - 1) \) times we come to the statement of the theorem.
Simplex codes (dual with respect to Hamming codes) and Reed-Miller codes of the first order (dual with respect to extended Hamming codes) satisfy the Grismer bound.
Asymptotic versions of the bounds

Next, we turn to the asymptotic versions of these three bounds. We consider a regime where $n \to \infty$. We use the following notations:

- The rate of the code: $R = \log_q M / n$
- The relative minimum distance of the code: $\delta = d / n$

The asymptotic versions of the bounds are presented below.
Asymptotic versions of the bounds

Singleton bound:

$$R \leq 1 - \delta.$$  

Sphere-packing (Hamming) bound:

$$R \leq 1 - h_q(\delta/2),$$

where

$$h_q(x) = -x \log_q x - (1-x) \log_q (1-x) + x \log_q (q-1)$$

is the $q$-ary entropy function, $\delta = d/n$. 

Irina Bocharova, Tartu, 2022, Page 20 of 36
Gilbert-Varshamov bound:
For the sufficiently long length $n$ and arbitrary small $\epsilon > 0$, there exits a $[n, k]$-code with relative minimum distance $\delta$ and rate $R = k/n$ that satisfies

$$R \geq R_{VG}(\delta) - \epsilon,$$

where $R_{VG} = 1 - h_q(\delta)$. 
Stirling’s approximation: 

\[ \sqrt{2\pi} n^n e^{-n} \exp\left\{\frac{1}{12n+1}\right\} < n! < \sqrt{2\pi} n^n e^{-n} \exp\left\{\frac{1}{12n}\right\}. \]

\[
\frac{n!}{d!(n-d)!} = \frac{n^d}{d^d (n-d)^{n-d}} \frac{n^{n-d}}{e^{-d} e^{-(n-d)}} \psi(n) = \\
= \delta^{-n\delta} (1 - \delta)^{-n(1-\delta)} \psi(n) = \\
= 2^{\{n(h(\delta)+o(n))\}},
\]

where \( \delta = \frac{d}{n}, \quad h(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta), \)

\[ o(n) = \log_2 \frac{\psi(n)}{n} \rightarrow 0, \quad n \rightarrow \infty. \]
Consider \[ \binom{n}{t}; \quad \sum_{i=0}^{t} \binom{n}{i}; \]

By using Stirling’s approximation

\[ \binom{n}{t} = K_s(n)2^{nh(\rho)}; \quad \sum_{i=0}^{t} \binom{n}{i} = K_b(n)2^{nh(\rho)}; \quad \rho = \frac{t}{n} \]

where \(K_s(n)\) and \(K_b(n) < nK_s(n)\) are polynomial terms which do not influence the exponential growth rate when \(n\) tends to infinity. We assume that \(t\) grows linearly with \(n\), that is, \(\rho = \frac{t}{n}\) is a constant.
Hamming bound (rate in symbols)

\[ \log_q (M) \leq \log_q \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i} \]

By using the maximal term

\[ R \leq 1 - \frac{1}{n} \log_q \binom{n}{t} - \frac{t}{n} \log_q (q-1) \]

By using Stirling’s approximation

\[ R \leq 1 - \frac{1}{n} \left( n \log_q n - t \log_q t - (n - t) \log_q (n - t) \right) - \frac{t}{n} \log_q (q-1) \]

\[ = 1 - h_q(\delta/2), \]

\[ t/n = \delta/2. \]

For binary codes we have

\[ R \leq 1 - h(\delta/2). \]
Hamming bound (rate in bits)

\[ M \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q - 1)^i}; \]

\[ q^k \leq \frac{q^n}{\binom{n}{t} (q - 1)^t} = \frac{q^n}{2^{n(h(\frac{t}{n}) + o(n))} 2^{n \frac{t}{n} \log_2(q-1)}}, \]

\[ k \log_2 q \leq n \log_2 q - n h \left( \frac{d}{2n} \right) - n \frac{d}{2n} \log_2(q - 1) + o(n) \]

\[ R_b \leq \log_2 q - h \left( \frac{\delta}{2} \right) - \frac{\delta}{2} \log_2(q - 1) \]

\[ R_b = \frac{\log_2 M}{n}. \text{ For linear codes } R_b = \frac{k \log_2 q}{n}. \]

For \( q = 2 \): \( R_b \leq 1 - h \left( \frac{\delta}{2} \right). \)
\[
\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i \leq q^{n-k}
\]

\[
\log_q \left( \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i \right) \leq n - k
\]

\[
-\delta \log_q \delta - (1-\delta) \log_q (1-\delta) + \delta \log_q (q-1) \leq 1 - R
\]

\[
R_{VG} = 1 - h_q(\delta)
\]
Consider a random code. We construct $H$ of size $(n - k) \times n$ by choosing its entries randomly from the set $\{0, 1\}$ with probability $1/2$. An arbitrary sequence will be a codeword (syndrome will be zero) with probability $2^{-(n-k)}$. The probability that its weight will be less than $d$ is

$$P_d \leq 2^{-(n-k)} \sum_{i=0}^{d-1} \binom{n}{i} \approx 2^{-n(1-R-h(\delta)+o(n))}$$

Then, for any rate

$$R < 1 - h(\delta) \Rightarrow P_d \to 0 \text{ if } n \to \infty$$

Almost all random codes (with $n \to \infty$) satisfy the GV bound.
Capacity of the BSC is $C = 1 - h(p)$. A code with minimum distance $d = n\delta$ corrects $\approx d/2 = n\delta/2$ errors. In order to correct all errors in the BSC it is required a code with relative distance $\delta/2 = p + \epsilon$.

Bounds:

$$R \leq 1 - h(\delta/2) \quad \text{(Hamming)}$$
$$R \geq 1 - h(\delta) \quad \text{(Gilbert-Varshamov)}$$

- If to construct codes satisfying the Hamming bound, they would provide an arbitrary small error for any rate $R < C$.
- If to construct codes satisfying the Gilbert-Varshamov bound and use them for correcting error of multiplicity $d/2$ then it is impossible to achieve capacity with an arbitrary small error, $R < 1 - h(2p) < C$. 

Irina Bocharova, Tartu, 2022, Page 29 of 36
There is a gap between the lower and upper bound. Comparison shows that the Hamming and the GV bounds differ at point $R = 0$. Which of two bounds is tighter? The $[n, 1, n]$ code exists but asymptotically the $[n, 2, d < n]$ also has $R = 0$. The answer to the question about achievable minimum distance at point $R = 0$ is given by the Plotkin bound.
Lemma

Sum over all codewords of the \([n, k]\) linear code in any position is equal either to 0 or \(2^{k-1}\). In other words, each position in the code is either always equal to 0 or takes on value 0 and 1 in half of codewords.

Proof.

If in \(G\) the first column is zero then the symbol is 0 in all codewords. Otherwise, one of rows of \(G\) starts with 1. Without loss of generality assume that it is the last row. By using Gaussian elimination we can set to zero other elements of the first column.

Linear combinations of the first \(k-1\) rows of \(G\) give \(2^{k-1}\) codewords which start with 0. By summing up the last row of \(G\) with these codewords, we obtain \(2^{k-1}\) codewords which start with 1.

\[
G = \begin{pmatrix}
0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\sim
\begin{pmatrix}
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\]
Lemma
For any linear code

\[ \frac{n2^{k-1}}{2^k - 1} \geq d. \quad (2) \]

Proof.
In the numerator we have an upper bound on the total number of 1s in all codewords. In the denominator we have the total number of nonzero codewords. Since the average weight cannot be less than the minimal weight, we obtain the statement of the lemma.

\[ \frac{d}{n} \leq \frac{1}{2} + \frac{1}{2^{k+1} - 2} \approx \frac{1}{2}; \]

\[ k \leq \log_2 \frac{2d}{2d - n} \text{ for } n < 2d \quad (3) \]
Let $K(n, d)$ denote the maximal $k$ for given $n$ and $d$. For $n > d$

$$K(n, d) \leq K(n - 1, d) + 1$$

**Proof.**

If exists $[n, k]$ code with minimum distance $d$ then we can find $[n - 1, k - 1]$ code with minimum distance $d$. Indeed, from $G$ in systematic form for $[n, k, d]$ code by removing the first row and first column of $G$, we obtain $[n - 1, k - 1, \geq d]$ code.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$[6, 3, 3] \Rightarrow [5, 2, 3]$
Plotkin bound

Theorem
For $[n, k]$ code of large enough $n$ with relative distance $\delta = d/n$

$$R \leq R_P(\delta) = 1 - 2\delta.$$ 

Proof.
From $K(n, d) \leq K(n - 1, d) + 1$ after $n - 2d + 1$ steps

$$K(n, d) \leq K(2d - 1, d) + n - 2d + 1 \leq \log_2(2d) + n - 2d + 1$$

By dividing both parts of inequality by $n$, if $n \to \infty$, we obtain the statement of the theorem.
Gilbert-Varshamov bound
Hamming bound
Singleton bound
Plotkin bound
Conclusions

• There exists a hypothesis that the GV bound is tight for binary codes

• Common mistake: asymptotic bounds cannot be used for the analysis of finite length codes. It is necessary to use non-asymptotic form of bounds.

• In Internet there exist tables (for example, http://www.codetables.de) which contain improved bounds for specific codes

• “White spots” exist already for \( n = 32 \). Does [32,14,9] code exist is open problem