Chapter 2: Error Detection and Correction Codes

Lectures 7-8

Hamming weight $w(\mathbf{x}) = |\{i : x_i \neq 0\}|$

minimum weight $w(C) = \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$

weight number $A_i(C) = |\{\mathbf{x} \in C : w(\mathbf{x}) = i\}|$

Example

	codewords	weights	weight numbers
C	0 0 0 0 0	0	$A_0 = 1$
	0 0 1 0 1	2	$A_1 = 0$
	1 1 0 0 1	3	$A_2 = 1$
	0 1 1 1 0	3	$A_3 = 2$
			$A_4 = 0$
			$A_5 = 0$

minimum weight $w = w(C) = 2$

Hamming weight $w(\mathbf{x}) = |\{i : x_i \neq 0\}|$

minimum weight $w(C) = \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$

weight number $A_i(C) = |\{\mathbf{x} \in C : w(\mathbf{x}) = i\}|$

Example

The 8-bit ASCII has minimum weight $d = 2$.

The Hamming codes have minimum weight $d = 3$ (we prove this later).

Hamming distance $d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$

minimum distance $d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

Example

codewords	distances
0 0 0 0 0	$d(00000, 00101) = 2$
0 0 1 0 1	$d(00000, 11001) = 3$
1 1 0 0 1	$d(00000, 01110) = 3$
0 1 1 1 0	$d(00101, 11001) = 3$
	$d(00101, 01110) = 3$
	$d(11001, 01110) = 4$

$$C \left\{ \begin{array}{c} 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 1 \\ 1\ 1\ 0\ 0\ 1 \\ 0\ 1\ 1\ 1\ 0 \end{array} \right.$$

minimum distance $d = d(C) = 2$

Hamming weight $w(\mathbf{x}) = |\{i : x_i \neq 0\}|$

Hamming distance $d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$

minimum weight $w(C) = \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$

minimum distance $d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

Lemma

$d(\cdot, \cdot)$ is a metric on $\mathbb{Z}_2^n$:

- $d(\mathbf{x}, \mathbf{y}) \geq 0$
- $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$
- $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$
- $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$

Lemma

- $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$
- $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ if $\mathbf{x}, \mathbf{y}$ are over an Abelian group

Hamming weight $w(\mathbf{x}) = |\{i : x_i \neq 0\}|$

Hamming distance $d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$

minimum weight $w(C) = \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$

minimum distance $d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$

Lemma

- $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$
- $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ if $\mathbf{x}, \mathbf{y}$ are over an Abelian group

Exercise

Show that if $\mathbf{0} \in C$, then $d(C) \leq w(C)$.

Note

If $\mathbf{x} \rightsquigarrow \mathbf{y}$, then $d(\mathbf{x}, \mathbf{y})$ is the number of errors in $\mathbf{y}$.

$$C = \{\text{Hello}, \text{Help!}\}$$

$$d(\text{Hello}, \text{Hell!}) = 1$$
$$d(\text{Help!}, \text{Hell!}) = 1$$

Decoding strategies

- minimum distance decoding
- standard strategy
- pure error detection
- many others...

Minimum distance decoding strategy

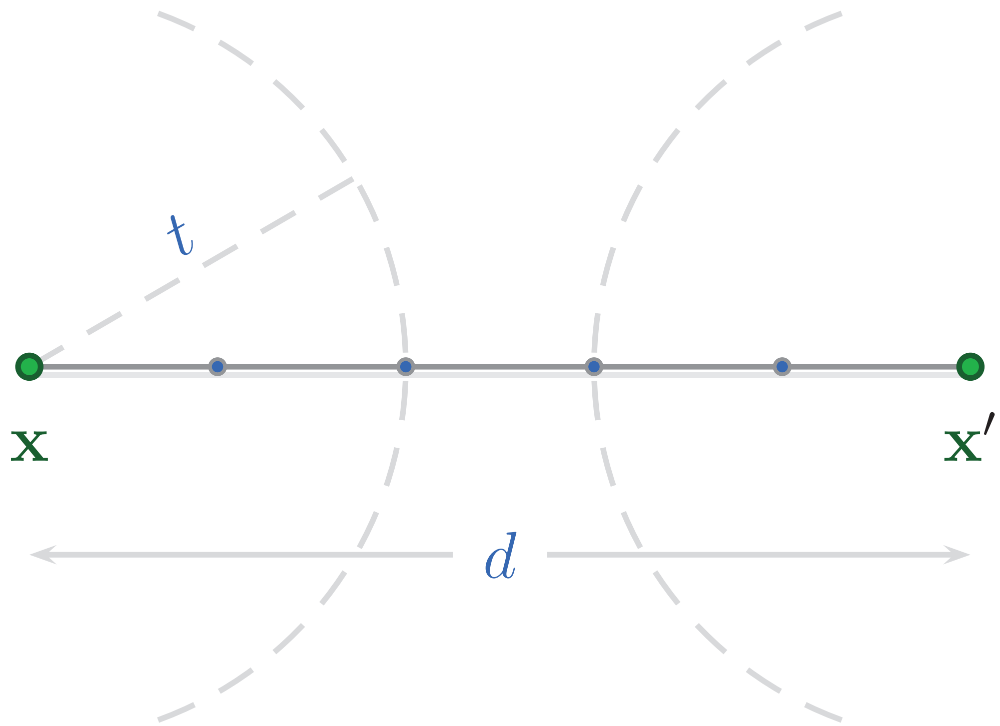
Given a received word $\mathbf{y}$, decode to closest codeword $\mathbf{x}$.

$$C = \{\text{Hello}, \text{Help!}\}$$

$$d(\text{Hello}, \text{Halp!}) = 3$$
$$d(\text{Help!}, \text{Halp!}) = 1$$

Minimum distance decoding strategy

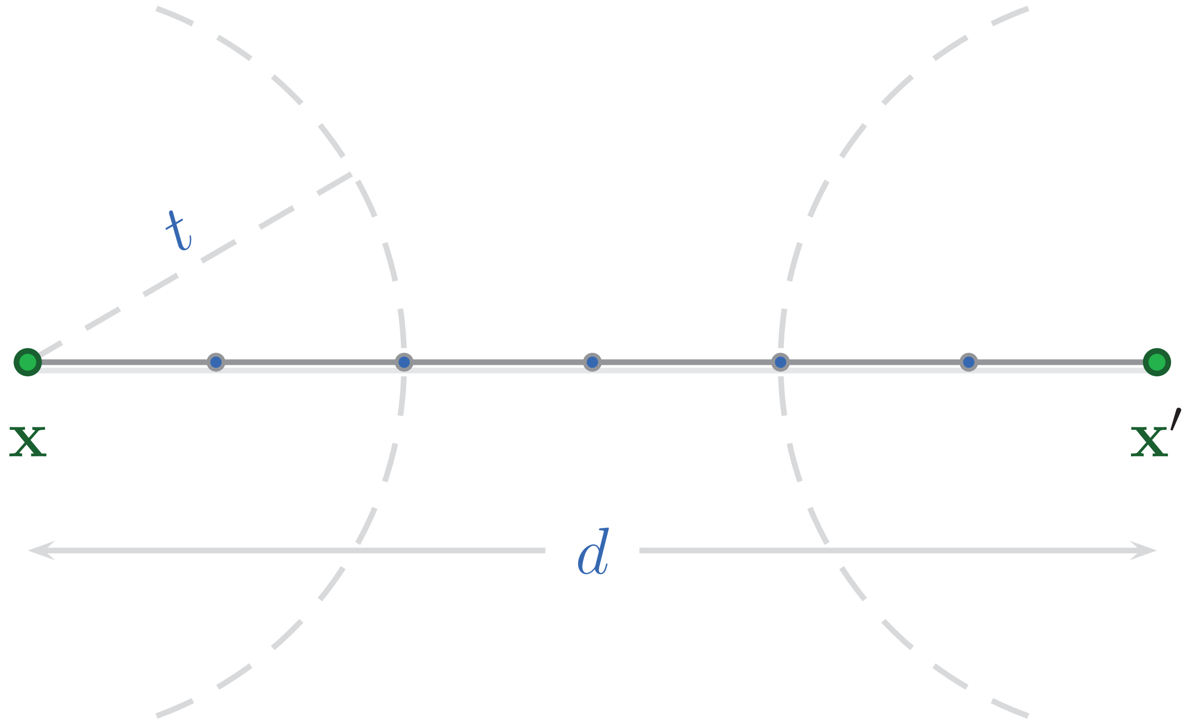
Given a received word $\mathbf{y}$, decode to closest codeword $\mathbf{x}$.



If $d = 2t + 1$, then C is a t-error correcting code.

Minimum distance decoding strategy

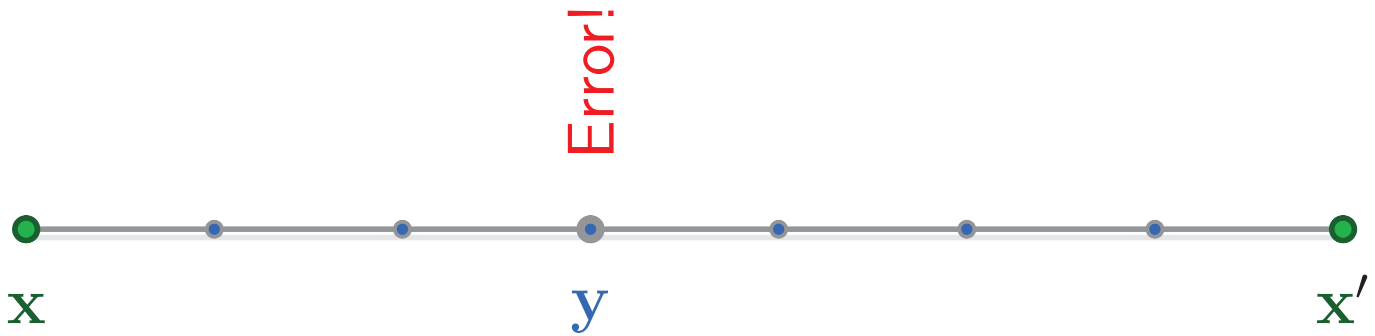
Given a received word $\mathbf{y}$, decode to closest codeword $\mathbf{x}$.



If $d = 2t + 2$, then C is a t-error correcting and $t + 1$-error detecting code.

Standard strategy

If received word $\mathbf{y}$ is distance at most t from a codeword $\mathbf{x}$, then decode $\mathbf{y}$ to $\mathbf{x}$; otherwise, flag an error.



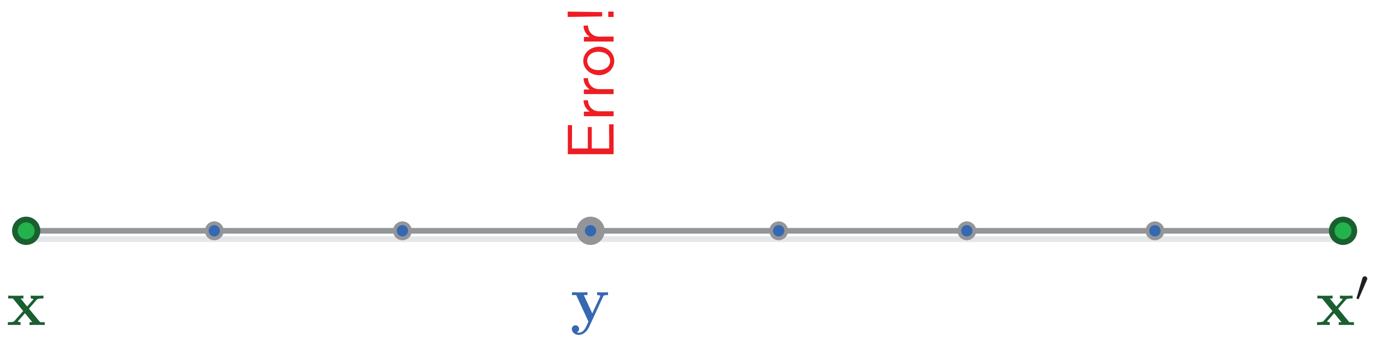
$$d = 5$$
$$t = 2$$

Exercise

If such a codeword $\mathbf{x}$ exists, then it is unique. Why?

Pure error detection

If received word $\mathbf{y}$ is not a codeword $\mathbf{x}$, then flag an error.



Theorem

If $e + f = d - 1$ and $f \geq e$,
then there is a strategy which is e-error correcting and f-error detecting.

Theorem

If $d = 2t + 1$, then C is t-error correcting.
If $d = 2t + 2$, then C is t-error correcting and $t + 1$-error detecting.

Example

The 8-bit ASCII has minimum weight $d = 2$ and is thus 1-error detecting.

Hamming codes have minimum weight $d = 3$ and are 1-error correcting.

Let $\mathbf{c} \in \mathbb{Z}_2^n$ be an n-bit word.

The sphere of radius r around $\mathbf{c}$:

$$S_r(\mathbf{c}) = \{\mathbf{x} \in \mathbb{Z}_2^n \ : \ d(\mathbf{x}, \mathbf{c}) \leq r\}$$

The volume of this sphere is its size $|S_r(\mathbf{c})|$.

Example

For $\mathbf{c} = 1100$,

$S_1(\mathbf{c})$	$S_2(\mathbf{c})$	
1100	1100	1111
1101	1101	1001
1110	1110	0101
1000	1000	1010
0100	0100	0110
		0000

$|S_1(\mathbf{c})| = 5$

$|S_2(\mathbf{c})| = 11$

Let $\mathbf{c} \in \mathbb{Z}_2^n$ be an n-bit word.

The sphere of radius r around $\mathbf{c}$:

$$S_r(\mathbf{c}) = \{\mathbf{x} \in \mathbb{Z}_2^n \ : \ d(\mathbf{x}, \mathbf{c}) \leq r\}$$

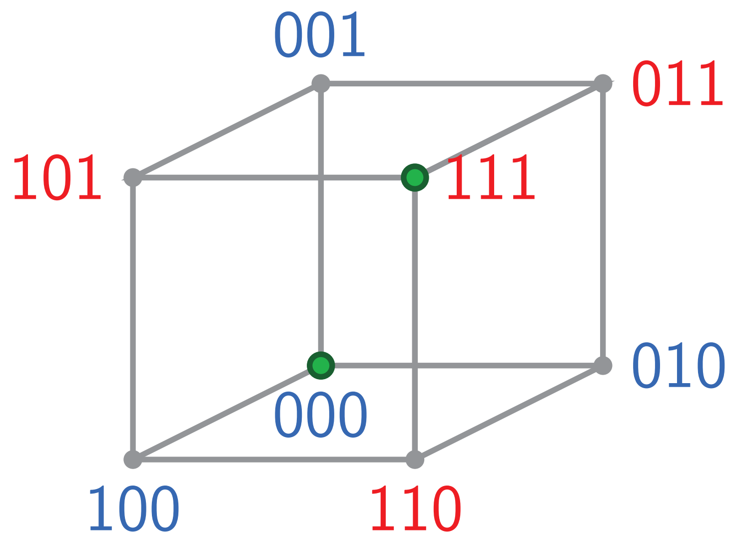
The volume of this sphere is its size $|S_r(\mathbf{c})|$.

Theorem

$$|S_r(\mathbf{c})| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$$

Example

Consider the code $C = \{000, 111\}$.

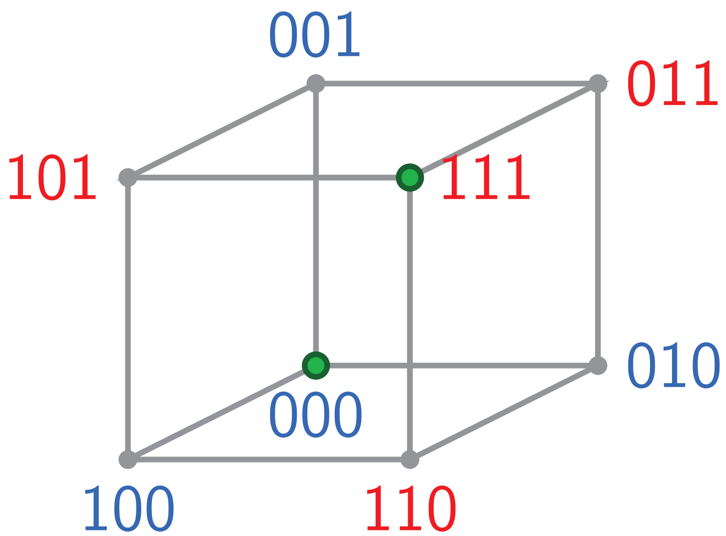


$$S_1(000) = \{000, 001, 010, 100\}$$
$$S_1(111) = \{111, 110, 101, 011\}$$

Note that these spheres do not overlap.
They therefore form a sphere packing.

Example

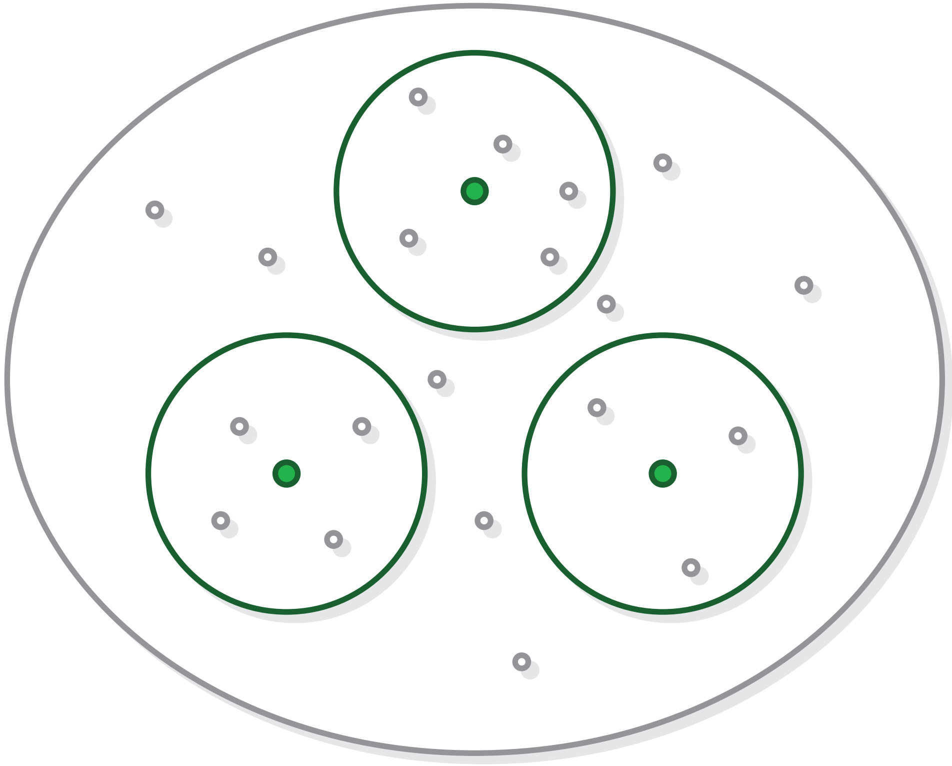
Consider the code $C = \{000, 111\}$.

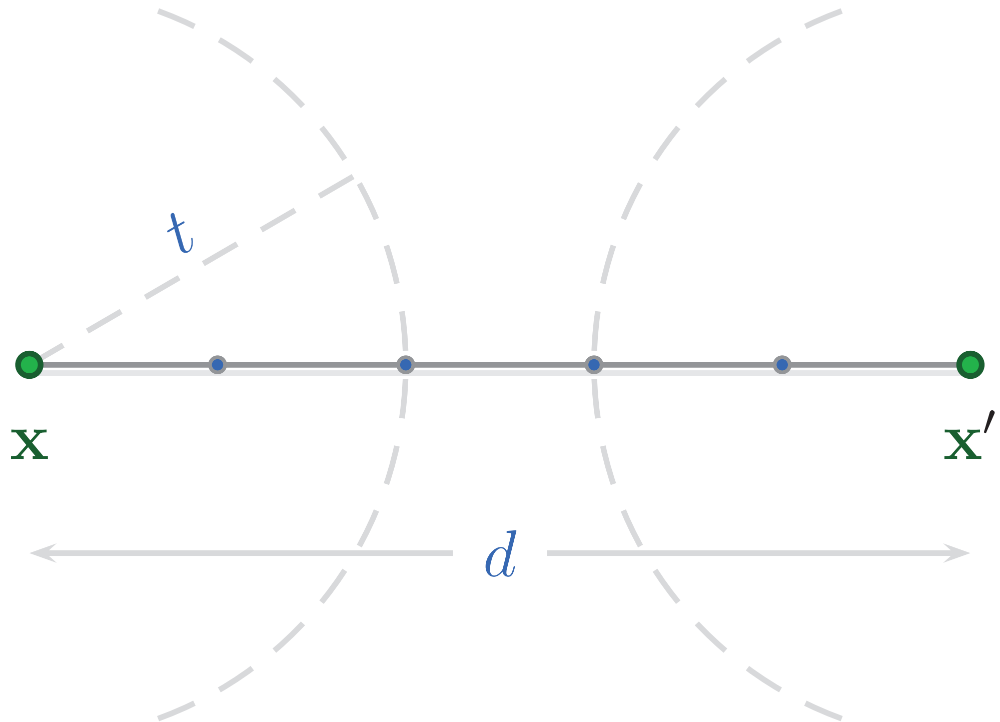


$$S_2(000) = \{000,001,010,100,101,110,011\}$$
$$S_2(111) = \{111,110,101,001,010,100,011\}$$

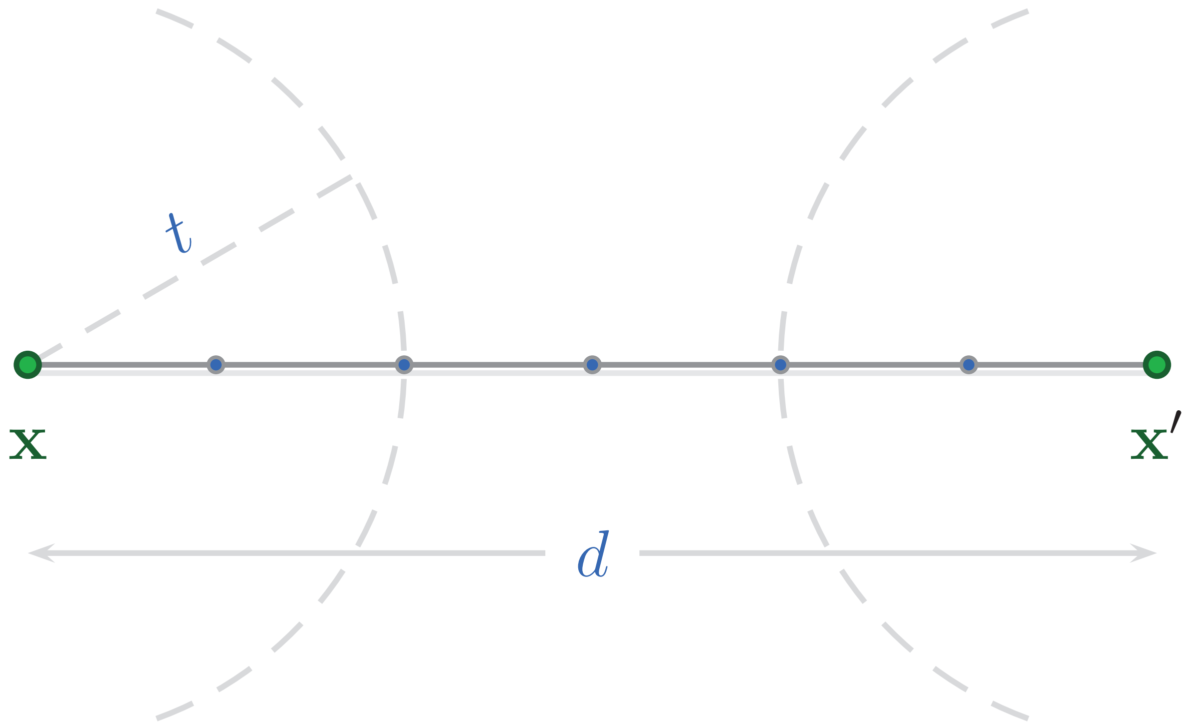
Note that these spheres do overlap.
They therefore do not form a sphere packing.

If the spheres of radius r around each codeword $\mathbf{x}$ do not overlap, then they form a sphere packing.



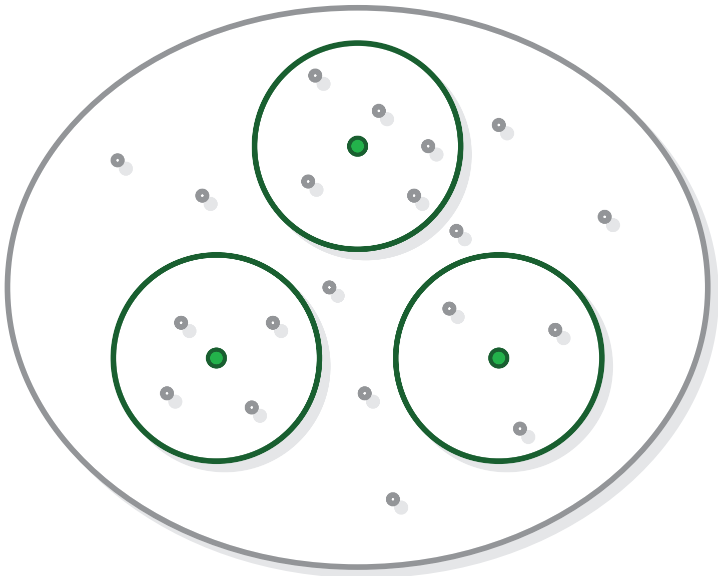


If $d = 2t + 1$, then C is a t-error correcting code.



If $d = 2t + 2$, then C is a t-error correcting and $t + 1$-error detecting code.

If the spheres of radius r around each codeword $\mathbf{x}$ do not overlap, then they form a sphere packing.



Sphere-Packing Condition Theorem (binary case)

A t-error correcting binary code C of length n has minimum distance $d = 2t + 1$ or $2t + 2$, and

$$|C| \sum_{i=0}^{t} \binom{n}{i} \leq 2^n \, .$$

Hamming weight	$w(\mathbf{x}) = \lvert\{i : x_i \neq 0\}\rvert$
minimum weight	$w(C) = \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$
weight number	$A_i(C) = \lvert\{\mathbf{x} \in C : w(\mathbf{x}) = i\}\rvert$

Example

	codewords	weights
C	0 0 0 0 0	0
	0 0 1 0 1	2
	1 1 0 0 1	3
	$\boxed{0\ 1\ 1\ 1\ 0}$	3