1 Brief review of Part I (Jul 2, 2008)

2 Construction of finite fields
   • Polynomials over finite fields
   • Explicit construction of the finite field $\mathbb{F}_q$, with $q = p^n$.
   • Examples

3 Classical coding theory
   • Decoding methods
   • The Coset-Leader Algorithm
   • Examples
1 Finite fields
   - Definitions
Finite fields

- Definitions
- Examples
Finite fields
  - Definitions
  - Examples
  - The structure of finite fields
Finite fields
  - Definitions
  - Examples
  - The structure of finite fields

Classical codes over finite fields
  - Linear codes: basic properties
1. Finite fields
   - Definitions
   - Examples
   - The structure of finite fields

2. Classical codes over finite fields
   - Linear codes: basic properties
   - Encoding methods
1 Finite fields
   - Definitions
   - Examples
   - The structure of finite fields

2 Classical codes over finite fields
   - Linear codes: basic properties
   - Encoding methods
   - Hamming distance as a metric
Polynomials over finite fields

Let $\mathbb{F}$ be a finite field. A *polynomial* over $\mathbb{F}$ is an expression of the form

$$f(x) = \sum_{i=1}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

where $n = \deg(f)$ is a nonnegative integer called the *degree* of $f(x)$, $a_i \in \mathbb{F}$ for all $0 \leq i \leq n$ and $x$ is a symbol not belonging to $\mathbb{F}$, called an *indeterminate* over $\mathbb{F}$.
Let $\mathbb{F}$ be a finite field. A *polynomial* over $\mathbb{F}$ is an expression of the form

$$f(x) = \sum_{i=1}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

where $n = \deg(f)$ is a nonnegative integer called the *degree* of $f(x)$, $a_i \in \mathbb{F}$ for all $0 \leq i \leq n$ and $x$ is a symbol not belonging to $\mathbb{F}$, called an *indeterminate* over $\mathbb{F}$.

We can define the *sum* and *product* of two polynomials using the usual rules of addition and multiplication over $\mathbb{F}$. 

*Example*: let $f(x) = x^2 + 2x + 1$ and $g(x) = 2x + 1$ be two polynomials over $\mathbb{F}_3$. Then $f(x) + g(x) = x^2 + x + 2$ and $f(x)g(x) = 2x^3 + 2x^2 + x + 1$. 

The polynomials over a finite field $\mathbb{F}$ form an *integral domain* and are denoted by $\mathbb{F}[x]$. 

Vlad Gheorghiu (CMU)
Finite fields: An introduction. Part II.
August 7, 2008 4 / 18
Let $\mathbb{F}$ be a finite field. A *polynomial* over $\mathbb{F}$ is an expression of the form

$$f(x) = \sum_{i=1}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

where $n = \deg(f)$ is a nonnegative integer called the *degree* of $f(x)$, $a_i \in \mathbb{F}$ for all $0 \leq i \leq n$ and $x$ is a symbol not belonging to $\mathbb{F}$, called an *indeterminate* over $\mathbb{F}$.

We can define the *sum* and *product* of two polynomials using the usual rules of addition and multiplication over $\mathbb{F}$.

**Example:** let $f(x) = x^2 + 2x + 1$ and $g(x) = 2x + 1$ be two polynomials over $\mathbb{F}_3$. Then

$$f(x) + g(x) = x^2 + x + 2$$

and

$$f(x)g(x) = 2x^3 + 2x^2 + x + 1.$$
Polynomials over finite fields

- Let $\mathbb{F}$ be a finite field. A *polynomial* over $\mathbb{F}$ is an expression of the form
  \[
  f(x) = \sum_{i=1}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n
  \]
  where $n = \deg(f)$ is a nonnegative integer called the *degree* of $f(x)$, $a_i \in \mathbb{F}$ for all $0 \leq i \leq n$ and $x$ is a symbol not belonging to $\mathbb{F}$, called an *indeterminate* over $\mathbb{F}$.

- We can define the *sum* and *product* of two polynomials using the usual rules of addition and multiplication over $\mathbb{F}$.

- Example: let $f(x) = x^2 + 2x + 1$ and $g(x) = 2x + 1$ be two polynomials over $\mathbb{F}_3$. Then
  \[
  f(x) + g(x) = x^2 + x + 2 \quad \text{and} \quad f(x)g(x) = 2x^3 + 2x^2 + x + 1.
  \]

- The polynomials over a finite field $\mathbb{F}$ form an *integral domain* and are denoted by $\mathbb{F}[x]$. 
Theorem 1: Division Algorithm

Let $g \neq 0$ be a polynomial in $\mathbb{F}[x]$. Then for any $f \in \mathbb{F}[x]$ there exist polynomials $q, r \in \mathbb{F}[x]$ such that

$$f = qg + r,$$

where $\text{deg}(r) < \text{deg}(g)$. 

Example: Consider $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{F}_5[x]$, $g(x) = 3x^2 + 1 \in \mathbb{F}_5[x]$. Then $q(x) = 4x^3 + 2x^2 + 2x + 1$ and $r(x) = 2x + 2$, with $\text{deg}(r) < \text{deg}(g)$. 

A polynomial with the leading term $a_n = 1$ is called a monic polynomial. A polynomial of degree zero is called a constant polynomial.
Theorem 1: Division Algorithm

Let $g \neq 0$ be a polynomial in $\mathbb{F}[x]$. Then for any $f \in \mathbb{F}[x]$ there exist polynomials $q, r \in \mathbb{F}[x]$ such that

$$f = qg + r,$$

where $\deg(r) < \deg(g)$.

**Example:** Consider $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{F}_5[x]$, $g(x) = 3x^2 + 1 \in \mathbb{F}_5[x]$. Then $q(x) = 4x^3 + 2x^2 + 2x + 1$ and $r(x) = 2x + 2$, with $\deg(r) < \deg(g)$. 
Theorem 1: Division Algorithm

Let \( g \neq 0 \) be a polynomial in \( \mathbb{F}[x] \). Then for any \( f \in \mathbb{F}[x] \) there exist polynomials \( q, r \in \mathbb{F}[x] \) such that

\[
f = qg + r, \text{ where } \deg(r) < \deg(g).
\]

- Example: Consider \( f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{F}_5[x], \)
  \( g(x) = 3x^2 + 1 \in \mathbb{F}_5[x] \). Then \( q(x) = 4x^3 + 2x^2 + 2x + 1 \) and
  \( r(x) = 2x + 2, \) with \( \deg(r) < \deg(g) \).

- A polynomial with the leading term \( a_n = 1 \) is called a monic polynomial. A polynomial of degree zero is called a constant polynomial.
Theorem 2: Greatest Common Divisor

Let \( f_1, f_2, \ldots, f_n \) be polynomials in \( \mathbb{F}[x] \) not all of which are 0. Then there exists a uniquely determined monic polynomial \( d \in \mathbb{F}[x] \) with the following properties: (i) \( d \) divides each \( f_j \), \( 1 \leq j \leq n \); (ii) any polynomial \( c \in \mathbb{F}[x] \) dividing each \( f_j \), \( 1 \leq j \leq n \), divides \( d \). Moreover, \( d \) can be expressed in the form

\[
d = b_1 f_1 + b_2 f_2 + \cdots + b_n f_n, \quad \text{with} \quad b_1, b_2, \ldots, b_n \in \mathbb{F}[x].
\]
Theorem 2: Greatest Common Divisor

Let \( f_1, f_2, \ldots, f_n \) be polynomials in \( \mathbb{F}[x] \) not all of which are 0. Then there exists a uniquely determined monic polynomial \( d \in \mathbb{F}[x] \) with the following properties: (i) \( d \) divides each \( f_j, 1 \leq j \leq n \); (ii) any polynomial \( c \in \mathbb{F}[x] \) dividing each \( f_j, 1 \leq j \leq n \), divides \( d \). Moreover, \( d \) can be expressed in the form

\[
d = b_1 f_1 + b_2 f_2 + \cdots + b_n f_n, \quad \text{with} \quad b_1, b_2, \ldots, b_n \in \mathbb{F}[x].
\]

A polynomial \( p \in \mathbb{F}[x] \) is said to be irreducible over \( \mathbb{F} \) (or prime in \( \mathbb{F}[x] \)) if \( p \) has positive degree and \( p = bc \) with \( b, c \in \mathbb{F}[x] \) implies that either \( b \) or \( c \) is a constant polynomial.
Theorem 2: Greatest Common Divisor

Let \( f_1, f_2, \ldots, f_n \) be polynomials in \( \mathbb{F}[x] \) not all of which are 0. Then there exists a uniquely determined monic polynomial \( d \in \mathbb{F}[x] \) with the following properties: (i) \( d \) divides each \( f_j \), \( 1 \leq j \leq n \); (ii) any polynomial \( c \in \mathbb{F}[x] \) dividing each \( f_j \), \( 1 \leq j \leq n \), divides \( d \). Moreover, \( d \) can be expressed in the form

\[
d = b_1 f_1 + b_2 f_2 + \cdots + b_n f_n, \quad \text{with } b_1, b_2, \ldots, b_n \in \mathbb{F}[x].
\]

- A polynomial \( p \in \mathbb{F}[x] \) is said to be \textit{irreducible over} \( \mathbb{F} \) (or \textit{prime in} \( \mathbb{F}[x] \)) if \( p \) has positive degree and \( p = bc \) with \( b, c \in \mathbb{F}[x] \) implies that either \( b \) or \( c \) is a constant polynomial.

- Example: \( x^2 - 2 \in \mathbb{Q}[x] \) is irreducible over the field \( \mathbb{Q} \) of rational numbers, but \( x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}) \) is reducible over the field \( \mathbb{R} \) of real numbers.
Theorem 3: Unique Factorization in $\mathbb{F}[x]$

Any polynomial $f \in \mathbb{F}[x]$ of positive degree can be written in the form

$$f = ap_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $a \in \mathbb{F}$, $p_1, p_2, \ldots, p_k$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$, and $e_1, e_2, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.
Theorem 3: Unique Factorization in $\mathbb{F}[x]$

Any polynomial $f \in \mathbb{F}[x]$ of positive degree can be written in the form

$$f = a p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $a \in \mathbb{F}$, $p_1, p_2, \ldots, p_k$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$, and $e_1, e_2, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

The above equation is called the canonical factorization of the polynomial $f$ in $\mathbb{F}[x]$. 

Theorem 3: Unique Factorization in $\mathbb{F}[x]$

Any polynomial $f \in \mathbb{F}[x]$ of positive degree can be written in the form

$$f = a p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $a \in \mathbb{F}$, $p_1, p_2, \ldots, p_k$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$, and $e_1, e_2, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

- The above equation is called the canonical factorization of the polynomial $f$ in $\mathbb{F}[x]$.
- Central question about polynomials in $\mathbb{F}[x]$: decide if it is reducible or not. Not a trivial problem.
An element \( b \in \mathbb{F} \) is called a \textit{root} (or a \textit{zero}) of the polynomial \( f \in \mathbb{F}[x] \) if \( f(b) = 0 \).
An element $b \in \mathbb{F}$ is called a \textit{root} (or a \textit{zero}) of the polynomial $f \in \mathbb{F}[x]$ if $f(b) = 0$.

\begin{itemize}
  \item \textbf{Theorem 4}
\end{itemize}

An element $b \in \mathbb{F}$ is a root of the polynomial $f \in \mathbb{F}[x]$ if and only if $x - b$ divides $f(x)$. 

\begin{itemize}
  \item \textbf{Theorem 5}
\end{itemize}

The polynomial $f \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible in $\mathbb{F}[x]$ if and only if $f$ has no root in $\mathbb{F}$. The converse holds for polynomials of degree 2 or 3, but not necessarily for polynomials of higher degree.
An element $b \in \mathbb{F}$ is called a root (or a zero) of the polynomial $f \in \mathbb{F}[x]$ if $f(b) = 0$.

**Theorem 4**

An element $b \in \mathbb{F}$ is a root of the polynomial $f \in \mathbb{F}[x]$ if and only if $x - b$ divides $f(x)$.

- If $f$ is an irreducible polynomial in $\mathbb{F}[x]$ of degree $\geq 2$, then Theorem 4 shows that $f$ has no root in $\mathbb{F}$. The converse holds for polynomials of degree 2 or 3, but not necessarily for polynomials of higher degree.
• An element $b \in \mathbb{F}$ is called a root (or a zero) of the polynomial $f \in \mathbb{F}[x]$ if $f(b) = 0$.

**Theorem 4**

An element $b \in \mathbb{F}$ is a root of the polynomial $f \in \mathbb{F}[x]$ if and only if $x - b$ divides $f(x)$.

• If $f$ is an irreducible polynomial in $\mathbb{F}[x]$ of degree $\geq 2$, then Theorem 4 shows that $f$ has no root in $\mathbb{F}$. The converse holds for polynomials of degree 2 or 3, but not necessarily for polynomials of higher degree.

**Theorem 5**

The polynomial $f \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible in $\mathbb{F}[x]$ if and only if $f$ has no root in $\mathbb{F}$. 
Explicit construction of the finite field $\mathbb{F}_q$

Theorem 6

For $f \in \mathbb{F}[x]$, the residue class ring $\mathbb{F}[x]/f$ is a field if and only if $f$ is irreducible over $\mathbb{F}$. 
Explicit construction of the finite field $\mathbb{F}_q$

Theorem 6

For $f \in \mathbb{F}[x]$, the residue class ring $\mathbb{F}[x]/f$ is a field if and only if $f$ is irreducible over $\mathbb{F}$.

In other words, to construct the finite field $\mathbb{F}_q$, with $q = p^n$, 

1. Select a monic irreducible polynomial $f(x)$ of degree $n$ in $\mathbb{F}_p[x]$ (it always exists).

2. The distinct residue classes comprising $\mathbb{F}_q[x]/f$ are described explicitly as $r + (f)$, where $r$ runs through all polynomials in $\mathbb{F}_p$ with $\deg(r) < \deg(f)$. Two residue classes $g + (f)$ and $h + (f)$ are identical precisely if $g \equiv h \mod f$, that is, $g - h$ is divisible by $f$. There are $p^n$ polynomials in $\mathbb{F}_p[x]$, of degree smaller than $n$.

3. Identify each element of $\mathbb{F}_q$ by an equivalence class. Construct the field table by computing sums and products of polynomials modulo $f$. 

Vlad Gheorghiu (CMU)  Finite fields: An introduction. Part II.  August 7, 2008  9 / 18
Explicit construction of the finite field $\mathbb{F}_q$

**Theorem 6**

For $f \in \mathbb{F}[x]$, the residue class ring $\mathbb{F}[x]/f$ is a field if and only if $f$ is irreducible over $\mathbb{F}$.

In other words, to construct the finite field $\mathbb{F}_q$, with $q = p^n$,

1. Select a monic irreducible polynomial $f(x)$ of degree $n$ in $\mathbb{F}_p[x]$ (it always exists).
Explicit construction of the finite field $\mathbb{F}_q$

**Theorem 6**

For $f \in \mathbb{F}[x]$, the residue class ring $\mathbb{F}[x]/f$ is a field if and only if $f$ is irreducible over $\mathbb{F}$.

In other words, to construct the finite field $\mathbb{F}_q$, with $q = p^n$,

1. Select a monic irreducible polynomial $f(x)$ of degree $n$ in $\mathbb{F}_p[x]$ (it always exists).

2. The distinct residue classes comprising $\mathbb{F}_q[x]/f$ are described explicitly as $r + (f)$, where $r$ runs through all polynomials in $\mathbb{F}_p$ with $\deg(r) < \deg(f)$. Two residue classes $g + (f)$ and $h + (f)$ are identical precisely if $g \equiv h \mod f$, that is, $g - h$ is divisible by $f$. There are $p^n$ polynomials in $\mathbb{F}_p[x]$, of degree smaller than $n$. 
Explicit construction of the finite field $\mathbb{F}_q$

**Theorem 6**

For $f \in \mathbb{F}[x]$, the residue class ring $\mathbb{F}[x]/f$ is a field if and only if $f$ is irreducible over $\mathbb{F}$.

In other words, to construct the finite field $\mathbb{F}_q$, with $q = p^n$,

1. Select a monic irreducible polynomial $f(x)$ of degree $n$ in $\mathbb{F}_p[x]$ (it always exists).

2. The distinct residue classes comprising $\mathbb{F}_q[x]/f$ are described explicitly as $r + (f)$, where $r$ runs through all polynomials in $\mathbb{F}_p$ with $\deg(r) < \deg(f)$. Two residue classes $g + (f)$ and $h + (f)$ are identical precisely if $g \equiv h \mod f$, that is, $g - h$ is divisible by $f$. There are $p^n$ polynomials in $\mathbb{F}_p[x]$, of degree smaller than $n$.

3. Identify each element of $\mathbb{F}_q$ by an equivalence class. Construct the field table by computing sums and product of polynomials modulo $f$. 
The finite field $\mathbb{F}_4$ (also called $GF(4)$).
Examples

The finite field $\mathbb{F}_4$ (also called $GF(4)$).

- Choose $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. 

The residue classes of $\mathbb{F}_2[x]/f$ are $\{[0], [1], [x], [x+1]\}$.

The addition and multiplication tables are:

+ | 0 | 1 | x | x+1 |
---|---|---|---|-----|
0 | 0 | 1 | x | x+1 |
1 | 1 | 0 | x+1 | x |
x | x | x+1 | 0 | 1 |
x+1 | x+1 | x | 1 | 0 |

and

$\ast$ | 0 | 1 | x | x+1 |
---|---|---|---|-----|
0 | 0 | 0 | 0 | 0 |
1 | 0 | 1 | x | x+1 |
x | 0 | x | x+1 | 0 |
x+1 | 0 | x+1 | 0 | 1 |
Examples

The finite field $\mathbb{F}_4$ (also called $GF(4)$).

- Choose $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.
- The residue classes of $\mathbb{F}_2[x]/f$ are $\{[0], [1], [x], [x + 1]\}$. 
Examples

The finite field $\mathbb{F}_4$ (also called $GF(4)$).

- Choose $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.
- The residue classes of $\mathbb{F}_2[x]/f$ are $\{[0], [1], [x], [x + 1]\}$. The addition and multiplication tables are:
The finite field $\mathbb{F}_4$ (also called $GF(4)$).

- Choose $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.
- The residue classes of $\mathbb{F}_2[x]/f$ are $\{[0], [1], [x], [x + 1]\}$. The addition and multiplication tables are:

<table>
<thead>
<tr>
<th></th>
<th>[0]</th>
<th>[1]</th>
<th>[x]</th>
<th>[x + 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[x]</td>
<td>[x + 1]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[0]</td>
<td>[x + 1]</td>
<td>[x]</td>
</tr>
<tr>
<td>[x]</td>
<td>[x]</td>
<td>[x + 1]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[x + 1]</td>
<td>[x + 1]</td>
<td>[x]</td>
<td>[1]</td>
<td>[0]</td>
</tr>
</tbody>
</table>

and
Examples

The finite field $\mathbb{F}_4$ (also called $GF(4)$).

- Choose $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.
- The residue classes of $\mathbb{F}_2[x]/f$ are \{[0], [1], [x], [x + 1]\}. The addition and multiplication tables are:

<table>
<thead>
<tr>
<th>+</th>
<th>[0]</th>
<th>[1]</th>
<th>[x]</th>
<th>[x + 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[x]</td>
<td>[x + 1]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[0]</td>
<td>[x + 1]</td>
<td>[x]</td>
</tr>
<tr>
<td>[x]</td>
<td>[x]</td>
<td>[x + 1]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
<tr>
<td>[x + 1]</td>
<td>[x + 1]</td>
<td>[x]</td>
<td>[1]</td>
<td>[0]</td>
</tr>
</tbody>
</table>

and

<table>
<thead>
<tr>
<th>*</th>
<th>[0]</th>
<th>[1]</th>
<th>[x]</th>
<th>[x + 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
<td>[0]</td>
</tr>
<tr>
<td>[1]</td>
<td>[0]</td>
<td>[1]</td>
<td>[x]</td>
<td>[x + 1]</td>
</tr>
<tr>
<td>[x]</td>
<td>[0]</td>
<td>[x]</td>
<td>[x + 1]</td>
<td>[1]</td>
</tr>
<tr>
<td>[x + 1]</td>
<td>[0]</td>
<td>[x + 1]</td>
<td>[1]</td>
<td>[x]</td>
</tr>
</tbody>
</table>
The finite field $\mathbb{F}_9$. 

Choose $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. The residue classes of $\mathbb{F}_3[x]/f$ are 

\{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]\}. 

Construct the addition and multiplication table. Too much LaTeX code to be put in a single slide...
The finite field $\mathbb{F}_9$.

- Choose $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. 
The finite field $\mathbb{F}_9$.

- Choose $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$.
- The residue classes of $\mathbb{F}_3[x]/f$ are $
\{[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]\}$.  

The finite field $\mathbb{F}_9$.

- Choose $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$.
- The residue classes of $\mathbb{F}_3[x]/f$ are 
  
  $\{[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2]\}$.
- Construct the addition and multiplication table. Too much LaTeX code to be put in a single slide...
Theorem 7

A code $C$ with minimum distance $d_C$ can correct up to $t$ errors if $d_C \geq 2t + 1$.

Proof.

A ball $B_t(x)$ of radius $t$ and center $x \in F_n_q$ consists of all vectors $y \in F_n_q$ such that $d(x, y) \leq t$. The nearest neighbor decoding rule ensures that each received word with $t$ or fewer errors must be in a ball of radius $t$ and center the transmitted code word. To correct $t$ errors, the balls with code words $x$ as centers must not overlap. If $u \in B_t(x)$ and $u \in B_t(y)$, $x, y \in C$, $x \neq y$, then $d(x, y) \leq d(x, u) + d(u, y) \leq 2t$, a contradiction to $d_C \geq 2t + 1$. 
Decoding methods

**Theorem 7**

A code $C$ with minimum distance $d_C$ can correct up to $t$ errors if $d_C \geq 2t + 1$. 

**Proof.** A ball $B_t(x)$ of radius $t$ and center $x \in F^n_q$ consists of all vectors $y \in F^n_q$ such that $d(x, y) \leq t$. The nearest neighbor decoding rule ensures that each received word with $t$ or fewer errors must be in a ball of radius $t$ and center the transmitted code word. To correct $t$ errors, the balls with code words $x$ as centers must not overlap. If $u \in B_t(x)$ and $u \in B_t(y)$, $x, y \in C$, $x \neq y$, then $d(x, y) \leq d(x, u) + d(u, y) \leq 2t$, a contradiction to $d_C \geq 2t + 1$. 

Vlad Gheorghiu (CMU)
Classical coding theory

Decoding methods

**Theorem 7**

A code $C$ with minimum distance $d_C$ can correct up to $t$ errors if $d_C \geq 2t + 1$.

**Proof.**

A ball $B_t(x)$ of radius $t$ and center $x \in \mathbb{F}_q^n$ consists of all vectors $y \in \mathbb{F}_q^n$ such that $d(x, y) \leq t$. The nearest neighbor decoding rule ensures that each received word with $t$ or fewer errors must be in a ball of radius $t$ and center the transmitted code word. To correct $t$ errors, the balls with code words $x$ as centers must not overlap. If $u \in B_t(x)$ and $u \in B_t(y)$, $x, y \in C$, $x \neq y$, then

$$d(x, y) \leq d(x, u) + d(u, y) \leq 2t,$$

a contradiction to $d_C \geq 2t + 1$. 
The following lemma is useful for determining the minimum distance of a code

Lemma 8
A linear code $C$ with parity-check matrix $H$ has minimum distance $D_C \geq s + 1$ if and only if any $s$ columns of $H$ are linearly independent.

Proof.
Assume there are $s$ linearly dependent columns of $H$, then $H^T c = 0$ and $\text{wt}(c) \leq s$ for suitable $c \in C, c \neq 0$, hence $d_C \leq s$. Similarly, if any $s$ columns of $H$ are linearly independent, then there is no $c \in C, c \neq 0$, of weight $\leq s$, hence $d_C \geq s + 1$. 

Vlad Gheorghiu (CMU)
Finite fields: An introduction. Part II.
August 7, 2008 13 / 18
The following lemma is useful for determining the minimum distance of a code

**Lemma 8**

A linear code $C$ with parity-check matrix $H$ has minimum distance $D_C \geq s + 1$ if and only if any $s$ columns of $H$ are linearly independent.
The following lemma is useful for determining the minimum distance of a code

**Lemma 8**

A linear code $C$ with parity-check matrix $H$ has minimum distance $D_C \geq s + 1$ if and only if any $s$ columns of $H$ are linearly independent.

**Proof.**

Assume there are $s$ linearly dependent columns of $H$, then $Hc^T = 0$ and $wt(c) \leq s$ for suitable $c \in C$, $c \neq 0$, hence $d_C \leq s$. Similarly, if any $s$ columns of $H$ are linearly independent, then there is no $c \in C$, $c \neq 0$, of weight $\leq s$, hence $d_C \geq s + 1$. 

The Cose Leader Algorithm

- Let $C$ be a $(n, k)$ linear code over $\mathbb{F}_q$. 
The Coset-Leader Algorithm

- Let $C$ be a $(n, k)$ linear code over $\mathbb{F}_q$.
- The vector space $\mathbb{F}_q^n / C$ consists of all cosets
  
  $$a + C = \{a + c : c \in C\}$$

  with $a \in \mathbb{F}_q^n$. 
The Coset-Leader Algorithm

- Let $C$ be a $(n, k)$ linear code over $\mathbb{F}_q$.
- The vector space $\mathbb{F}_q^n / C$ consists of all cosets

$$a + C = \{a + c : c \in C\}$$

with $a \in \mathbb{F}_q^n$.
- Each coset contains $q^k$ vectors and $\mathbb{F}_q^n$ can be regarded as being partitioned into cosets of $C$, namely
Let $C$ be a $(n, k)$ linear code over $\mathbb{F}_q$.

The vector space $\mathbb{F}_q^n / C$ consists of all cosets

$$a + C = \{a + c : c \in C\}$$

with $a \in \mathbb{F}_q^n$.

Each coset contains $q^k$ vectors and $\mathbb{F}_q^n$ can be regarded as being partitioned into cosets of $C$, namely

$$\mathbb{F}_q^n = (a^{(0)} + C) \cup (a^{(1)} + C) \cup \cdots (a^{(s)} + C),$$

where $a^{(0)} = 0$ and $s = q^{n-k} - 1$. 
Let $C$ be a $(n, k)$ linear code over $\mathbb{F}_q$.

The vector space $\mathbb{F}_q^n / C$ consists of all cosets

$$a + C = \{a + c : c \in C\}$$

with $a \in \mathbb{F}_q^n$.

Each coset contains $q^k$ vectors and $\mathbb{F}_q^n$ can be regarded as being partitioned into cosets of $C$, namely

$$\mathbb{F}_q^n = (a^{(0)} + C) \cup (a^{(1)} + C) \cup \cdots (a^{(s)} + C),$$

where $a^{(0)} = 0$ and $s = q^{n-k} - 1$.

A received vector $y$ must be in one of the cosets, say $a^{(i)} + C$. If the codeword $c$ was transmitted, then the error is given by $e = y - c = a^{(i)} + z \in a^{(i)} + C$ for suitable $z \in C$. 

All possible error vectors $e$ of a received vector $y$ are the vectors in the coset of $y$. 

**Definition**

Let $C \subseteq F^n_q$ be a linear $(n, k)$ code and let $F^n_q/C$ be the factor space. An element of minimum weight in a coset $a + C$ is called coset leader of $a + C$. If several vectors in $a + C$ have minimum weight, we choose one of them as coset leader.
• All possible error vectors $e$ of a received vector $y$ are the vectors in the coset of $y$.
• The most likely error vector is the vector $e$ with minimum weight in the coset of $y$. 

Definition
Let $C \subseteq F_{n,q}$ be a linear $(n,k)$ code and let $F_{n,q}/C$ be the factor space. An element of minimum weight in a coset $a+C$ is called coset leader of $a+C$. If several vectors in $a+C$ have minimum weight, we choose one of them as coset leader.
All possible error vectors $e$ of a received vector $y$ are the vectors in the coset of $y$.

The most likely error vector is the vector $e$ with minimum weight in the coset of $y$.

Thus we decode $y$ as $x = y - e$. 
• All possible error vectors $e$ of a received vector $y$ are the vectors in the coset of $y$.
• The most likely error vector is the vector $e$ with minimum weight in the coset of $y$.
• Thus we decode $y$ as $x = y - e$.

**Definition**

Let $C \subseteq \mathbb{F}_q^n$ be a linear $(n, k)$ code and let $\mathbb{F}_q^n/C$ be the factor space. An element of minimum weight in a coset $a + C$ is called *coset leader* of $a + C$. If several vectors in $a + C$ have minimum weight, we choose one of them as coset leader.
Definition

Let $H$ be the parity-check matrix of a linear $(n, k)$ code $C$. Then the vector $S(y) = H y^T$ of length $n - k$ is called the syndrome of $y$.
Definition

Let $H$ be the parity-check matrix of a linear $(n, k)$ code $C$. Then the vector $S(y) = H y^T$ of length $n - k$ is called the syndrome of $y$.

Theorem 9

For $y, z \in \mathbb{F}_q^n$ we have:

1) $S(y) = 0$ if and only if $y \in C$.
2) $S(y) = S(z)$ if and only if $y + C = z + C$.

Proof.

1) follows immediately from the definition of $C$ in terms of $H$.

For 2) note that $S(y) = S(z)$ if and only if $H y^T = H z^T$ if and only if $H (y - z)^T = 0$ if and only if $y - z \in C$ if and only if $y + C = z + C$. 

Vlad Gheorghiu (CMU)
Finite fields: An introduction. Part II.
August 7, 2008 16 / 18
**Definition**

Let $H$ be the parity-check matrix of a linear $(n, k)$ code $C$. Then the vector $S(y) = Hy^T$ of length $n - k$ is called the *syndrome* of $y$.

**Theorem 9**

For $y, z \in \mathbb{F}_q^n$ we have:

1. $S(y) = 0$ if and only if $y \in C$
Definition

Let $H$ be the parity-check matrix of a linear $(n, k)$ code $C$. Then the vector $S(y) = H y^T$ of length $n - k$ is called the *syndrome* of $y$.

Theorem 9

For $y, z \in \mathbb{F}_q^n$ we have:

1. $S(y) = 0$ if and only if $y \in C$
2. $S(y) = S(z)$ if and only if $y + C = z + C$
**Definition**

Let \( H \) be the parity-check matrix of a linear \((n, k)\) code \( C \). Then the vector \( S(y) = Hy^T \) of length \( n - k \) is called the *syndrome* of \( y \).

**Theorem 9**

For \( y, z \in \mathbb{F}_q^n \) we have:

1. \( S(y) = 0 \) if and only if \( y \in C \)
2. \( S(y) = S(z) \) if and only if \( y + C = z + C \)

**Proof.**

1) follows immediately from the definition of \( C \) in terms of \( H \).
Definition

Let $H$ be the parity-check matrix of a linear $(n, k)$ code $C$. Then the vector $S(y) = H y^T$ of length $n - k$ is called the syndrome of $y$.

Theorem 9

For $y, z \in \mathbb{F}_q^n$ we have:

1. $S(y) = 0$ if and only if $y \in C$
2. $S(y) = S(z)$ if and only if $y + C = z + C$

Proof.

1) follows immediately from the definition of $C$ in terms of $H$.

For 2) note that $S(y) = S(z)$ if and only if $H y^T = H z^T$ if and only if $H(y - z)^T = 0$ if and only if $y - z \in C$ if and only if $y + C = z + C$. 
If \( e = y - c \), \( c \in C \), \( y \in \mathbb{F}_q^n \), then

\[ S(y) = S(c + e) = S(c) + S(e) = S(e) \]

and \( y \) and \( e \) are in the same coset. The coset leader of that coset also has the same syndrome. We have the following decoding algorithm.

### The Coset-Leader Algorithm

1. Let \( C \subseteq \mathbb{F}_q^n \) be a linear \((n, k)\) code and let \( y \) be the received vector.
2. To correct errors in \( y \), calculate \( S(y) \) and find the coset leader, say \( e \), with syndrome equal to \( S(y) \).
3. Then decode \( y \) as \( x = y - e \). Here \( x \) is the code word with minimum distance to \( y \).
If $e = y - c$, $c \in C$, $y \in \mathbb{F}_q^n$, then

$$S(y) = S(c + e) = S(c) + S(e) = S(e)$$
If \( e = y - c, \; c \in C, \; y \in \mathbb{F}_q^n \), then

\[
S(y) = S(c + e) = S(c) + S(e) = S(e)
\]

and \( y \) and \( e \) are in the same coset. The coset leader of that coset also has the same syndrome. We have the following decoding algorithm.
If $e = y - c$, $c \in C$, $y \in \mathbb{F}_q^n$, then

$$S(y) = S(c + e) = S(c) + S(e) = S(e)$$

and $y$ and $e$ are in the same coset. The coset leader of that coset also has the same syndrome. We have the following decoding algorithm.

The Coset-Leader Algorithm

1. Let $C \subseteq \mathbb{F}_q^n$ be a linear $(n, k)$ code and let $y$ be the received vector.
If $\mathbf{e} = \mathbf{y} - \mathbf{c}$, $\mathbf{c} \in C$, $\mathbf{y} \in \mathbb{F}_q^n$, then

$$S(\mathbf{y}) = S(\mathbf{c} + \mathbf{e}) = S(\mathbf{c}) + S(\mathbf{e}) = S(\mathbf{e})$$

and $\mathbf{y}$ and $\mathbf{e}$ are in the same coset. The coset leader of that coset also has the same syndrome. We have the following decoding algorithm.

### The Coset-Leader Algorithm

1. Let $C \subseteq \mathbb{F}_q^n$ be a linear $(n, k)$ code and let $\mathbf{y}$ be the received vector.
2. To correct errors in $\mathbf{y}$, calculate $S(\mathbf{y})$ and find the coset leader, say $\mathbf{e}$, with syndrome equal to $S(\mathbf{y})$. Then decode $\mathbf{y}$ as $\mathbf{x} = \mathbf{y} - \mathbf{e}$. Here $\mathbf{x}$ is the code word with minimum distance to $\mathbf{y}$. 
If \( e = y - c, \ c \in C, \ y \in \mathbb{F}_q^n \), then

\[
S(y) = S(c + e) = S(c) + S(e) = S(e)
\]

and \( y \) and \( e \) are in the same coset. The coset leader of that coset also has the same syndrome. We have the following decoding algorithm.

**The Coset-Leader Algorithm**

1. Let \( C \subseteq \mathbb{F}_q^n \) be a linear \((n, k)\) code and let \( y \) be the received vector.
2. To correct errors in \( y \), calculate \( S(y) \) and find the coset leader, say \( e \), with syndrome equal to \( S(y) \).
3. Then decode \( y \) as \( x = y - e \). Here \( x \) is the code word with minimum distance to \( y \).
Coset-Leader example

Discuss it on the board.