Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

Definition. Let $(R, +, \times)$ be a ring. A polynomial with coefficients in R is an expression of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

where $a_0, \ldots, a_m \in R$.

- a_i are called the coefficient of degree i of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree i
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

Notation. The set of all polynomials with coefficients in R is written $R[X]$.

- $2 + 5X$: polynomial in $\mathbb{Z}[X]$ of degree 1
- $5X + 2$: same polynomial, order of the terms does not matter
- $0X^2 + 5X + 2$: same polynomial, terms with 0 coefficient don't matter.

Implementation: a polynomial $A \in R[X]$ is just implemented as an array `A` where `A[i]` is the coefficient of degree i.

Polynomial addition

$$(\sum a_iX^i) + (\sum b_iX^i) = \sum (a_i + b_i)X^i$$

Polynomial multiplication

$$(\sum a_iX^i) \times (\sum b_iX^i) = \sum c_iX^i$$

$$c_i = \sum a_jb_{i-j}$$

Definition. Let R be a ring and $r \in R$. Let $A \in R[X]$ be $a_0 + a_1X + \cdots + a_mX^m$. The evaluation of A at r is

$$\underbrace{a_0}_{\in R} + \overset{\in R}{\underbrace{a_1}_{\in R}\underbrace{r}_{\in R}} + \overset{\in R}{a_2 r^2} + \cdots + \overset{\in R}{a_m r^m}$$

$r^2 = r \times r$

$r^3 = r \times r \times r$

Basically what you are used to when applying a function to an argument

$f : \mathbb{R} \longrightarrow \mathbb{R}$

$f(x) = \cos(2x) \qquad f(5) \in \mathbb{R}$

Definition. Let R be a ring and $r \in R$. Let $A \in R[X]$ be $a_0 + a_1 X + \cdots + a_m X^m$. The evaluation of A at r is

$$a_0 + a_1 r + a_1 r^2 + \cdots + a_m r^m$$

Basically what you are used to when applying a function to an argument

$A = X^2 + X + 1$ polynomial in $(\mathbb{Z}/2\mathbb{Z})[X]$ $\quad r = 1 \quad \rightsquigarrow A(r) = 1$

$1^2 + 1 + \underline{1}$

Definition. Let R be a ring and $r \in R$. Let $A \in R[X]$ be $a_0 + a_1X + \cdots + a_mX^m$. The evaluation of A at r is

$$a_0 + a_1r + a_1r^2 + \cdots + a_mr^m$$

Basically what you are used to when applying a function to an argument

$$A = X^2 + X + 1 \text{ polynomial in } (\mathbb{Z}/2\mathbb{Z})[X] \qquad r = 1 \qquad \rightsquigarrow A(r) = 1$$

We say that r is a root of A if $A(r) = 0$. neutral element for $+$ in R.

Definition. Let R be a ring and $r \in R$. Let $A \in R[X]$ be $a_0 + a_1 X + \cdots + a_m X^m$. The evaluation of A at r is

$$a_0 + a_1 r + a_1 r^2 + \cdots + a_m r^m$$

Basically what you are used to when applying a function to an argument

$$A = X^2 + X + 1 \text{ polynomial in } (\mathbb{Z}/2\mathbb{Z})[X] \qquad r = 1 \qquad \rightsquigarrow A(r) = 1$$

We say that r is a root of A if $A(r) = 0$.

Theorem. Let $\mathbb{K}$ be a field. Then r is a root of A if, and only if, $X - r$ divides A.

$$P(r) = 0 \Rightarrow P = (X - r) \cdot Q$$

For every $n \geq 2$, we know at least one ring: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Recall: For prime n, this is a field

$(\mathbb{R}, +, \times)$ $(\mathbb{Q}, +, \times)$

n prime

$a \in \{1, \ldots, n-1\}$

$u \cdot a + v \cdot n = 1$

$\Rightarrow u \cdot a = 1 \mod n$

For every $n \geq 2$, we know at least one ring: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

2, 3, 5, 7, 11, ...

Recall: For prime n, this is a field

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

$2^2 = 4$

$3^2 = 9$

$\mathbb{Z} \rightsquigarrow p = 3 \rightsquigarrow$ eq. rel $\rightsquigarrow \mathbb{Z}/_p\mathbb{Z}$

For every $n \geq 2$, we know at least one ring: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Recall: For prime n, this is a field

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Particularly interesting for us: $\mathrm{GF}(2^k)$, elements =

For every $n \geq 2$, we know at least one ring: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Recall: For prime n, this is a field

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Particularly interesting for us: $\mathrm{GF}(2^k)$, elements = binary strings of length k

Rough idea of the construction:

- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

$(\mathbb{Z}/p\mathbb{Z})[X]$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Rough idea of the construction:

- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Rough idea of the construction:

- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

Example with $p = 2, k = 2$: $p^k = 4$

- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Prime polynomial of degree 2: $N = X^2 + X + 1$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Rough idea of the construction:

- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

$$\begin{array}{r|l} X^2+X & X^2+X+1 \\ \hline -(X^2+X+1) & 1 \\ \hline \boxed{1} & \end{array}$$

Example with $p = 2, k = 2$:

- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Prime polynomial of degree 2: $N = X^2 + X + 1$

$$\begin{aligned} 0 &\equiv X^2 + X + 1 \\ 1 &\equiv X^2 + X \\ X &\equiv X^2 + 1 \\ X^2 &\equiv 1 + X \end{aligned}$$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Rough idea of the construction:
- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

X^5 | $X^2 + X + 1$

$X^4 + X^3$ | $X^3 + X^2 + 1$

X^2

$X + 1$

Example with $p = 2, k = 2$:
- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Prime polynomial of degree 2: $N = X^2 + X + 1$

$$
\begin{aligned}
0 &\equiv X^2 + X + 1 \\
1 &\equiv X^2 + X \\
X &\equiv X^2 + 1 \\
X^2 &\equiv 1 + X \\
X^5 &\equiv ? \quad 1 + X
\end{aligned}
$$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k. If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

Rough idea of the construction:

- We know how to construct fields of prime size
- Find prime polynomial N of degree k
- Define $A \equiv_N B$ if A, B have same remainder modulo N
- This defines a new ring $(\mathbb{Z}/p\mathbb{Z})[X]/\equiv$
- This happens to have size p^k and to be a field

Example with $p = 2, k = 2$:

- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Prime polynomial of degree 2: $N = X^2 + X + 1$
- Every polynomial is equivalent to a polynomial of degree ≤ 1

$$\begin{aligned} 0 &\equiv X^2 + X + 1 \\ 1 &\equiv X^2 + X \\ X &\equiv X^2 + 1 \\ X^2 &\equiv 1 + X \end{aligned}$$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

+	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

$$X(1+X) \equiv X+(X^2) \equiv X+(1+X) \equiv 1$$

Example with $p = 2, k = 2$:
- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Prime polynomial of degree 2: $N = X^2 + X + 1$
- Every polynomial is equivalent to a polynomial of degree ≤ 1

$$\begin{aligned} 0 &\equiv X^2 + X + 1 \\ 1 &\equiv X^2 + X \\ X &\equiv X^2 + 1 \\ X^2 &\equiv 1 + X \end{aligned}$$

Theorem. For every prime p and $k \geq 1$, there exists a unique field of size p^k.
If $\mathbb{K}$ is a finite field, then $|\mathbb{K}| = p^k$ for a prime p and $k \geq 1$.

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

$\times$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	1	$1+X$
$1+X$	0	$1+X$	$1+X$	1

Example with $p = 2, k = 2$:

- Starting point: $\mathbb{Z}/2\mathbb{Z}$
- Polynomial of degree 2: $N = X^2 + 1 = (1+X)(1+X)$
- Every polynomial is equivalent to a polynomial of degree ≤ 1

$$
\begin{aligned}
X &\equiv X^2 + X + 1 \\
1 + X &\equiv X^2 + X \\
0 &\equiv X^2 + 1 \\
X + X^2 &\equiv 1 + X
\end{aligned}
$$

This construction is not limited to finite fields!

- Start with $\mathbb{R}$
- Take $N = X^2 + 1$
- This is a prime polynomial

This construction is not limited to finite fields!

- Start with $\mathbb{R}$
- Take $N = X^2 + 1$
- This is a prime polynomial
- $\mathbb{R}[X]/(X^2 + 1)$ is a field

This construction is not limited to finite fields!

- Start with $\mathbb{R}$
- Take $N = X^2 + 1$
- This is a prime polynomial
- $\mathbb{R}[X]/(X^2 + 1)$ is a field
- Equivalence classes:
  - one for each $a \in \mathbb{R}$
  - one equivalence class of each $aX + b$
  - $X^2 \equiv \cancel{?}\ -1$

$$\begin{array}{r|l} X^2 & X^2+1 \\ \hline -(X^2+1) & 1 \\ \hline -1 & \end{array}$$

This construction is not limited to finite fields!

- Start with $\mathbb{R}$
- Take $N = X^2 + 1$
- This is a prime polynomial
- $\mathbb{R}[X]/(X^2 + 1)$ is a field
- Equivalence classes:
  - one for each $a \in \mathbb{R}$
  - one equivalence class of each $aX + b$
  - $X^2 \equiv ?$

Addition and multiplication in $\mathbb{R}[X]/(X^2 + 1)$:

$$(aX+b)+(cX+d) \equiv (a+c)X+(b+d)$$

$$(aX+b)\times(cX+d) \equiv acX^2+(b+d)X+bd$$

$$\equiv (b+d)X + (bd - ac)$$

This construction is not limited to finite fields!

- Start with $\mathbb{R}$
- Take $N = X^2 + 1$
- This is a prime polynomial
- $\mathbb{R}[X]/(X^2 + 1)$ is a field
- Equivalence classes:
  - one for each $a \in \mathbb{R}$
  - one equivalence class of each $aX + b$
  - $X^2 \equiv ?$

Addition and multiplication in $\mathbb{R}[X]/(X^2 + 1)$:

$$(aX+b)+(cX+d) \equiv (a+c)X+(b+d)$$

$$(aX+b)\times(cX+d) \equiv acX^2+(b+d)X+bd$$

- You might know this as $\mathbb{C}$, the complex numbers $X \rightsquigarrow i$
- Despite this abstract nonsense, incredibly useful in practice (quantum mechanics, electrical engineering, computer graphics)

Theorem. Let $(\mathbb{K}, +, \times)$ be a finite field. Then $(\mathbb{K} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

Theorem. Let $(\mathbb{K}, +, \times)$ be a finite field. Then $(\mathbb{K} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

This means: there exists a bijective function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{K} \setminus \{0\}$ that "transforms" $+$ into $\times$

Theorem. Let $(\mathbb{K}, +, \times)$ be a finite field. Then $(\mathbb{K} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

This means: there exists a bijective function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{K} \setminus \{0\}$ that "transforms" $+$ into $\times$

Proof.* Idea: count the numbers of elements of order d, for each divisor d of n. Call this number $\psi(n)$.

- $\psi(d) \leq \varphi(d)$
- so $\sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d)$
- Every element has an order, so $\sum_{d|n} \psi(d) = n$
- (one of Euler's identities:) $\sum_{d|n} \varphi(d) = n$
- So we must have $\varphi(d) = \psi(d)$ for all d

In particular, some element $\alpha \in \mathbb{K} \setminus \{0\}$ has order $n = |\mathbb{K}| - 1$: $\alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n = 1$ are all different.
Define $f : m \mapsto a^m$. $\square$

Theorem. Let $(\mathbb{K}, +, \times)$ be a finite field. Then $(\mathbb{K} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

This means: there exists a bijective function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{K} \setminus \{0\}$ that "transforms" $+$ into $\times$

Proof.* Idea: count the numbers of elements of order d, for each divisor d of n. Call this number $\psi(n)$.

- $\psi(d) \leq \varphi(d)$
- so $\sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d)$
- Every element has an order, so $\sum_{d|n} \psi(d) = n$
- (one of Euler's identities:) $\sum_{d|n} \varphi(d) = n$
- So we must have $\varphi(d) = \psi(d)$ for all d

In particular, some element $\alpha \in \mathbb{K} \setminus \{0\}$ has order $n = |\mathbb{K}| - 1$: $\alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n = 1$ are all different.
Define $f : m \mapsto a^m$. $\square$

$1, 1+1, 1+1+1, \ldots$

In particular some element $\alpha \in \mathbb{K} \setminus \{0\}$ enumerates the whole $\mathbb{K} \setminus \{0\}$ with its powers:

Definition. An element α in $\mathbb{K}$ is primitive if $\{\alpha, \alpha^2, \ldots, \alpha^m\} = \mathbb{K} \setminus \{0\}$ for some m.

Theorem. Let $(\mathbb{K}, +, \times)$ be a finite field. Then $(\mathbb{K} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

- 1: not primitive, since $\{1, 1^2, 1^3, \dots\} = \{1\}$
- α primitive: $\alpha, \alpha^2 = 1 + \alpha, \alpha^3 = 1$ and $\{1, \alpha, 1+\alpha\} = \mathbb{K} \setminus \{0\}$
- $1 + \alpha$? $\alpha + \alpha^2 = \cancel{\alpha} + \cancel{\alpha} + 1$

In particular some element $\alpha \in \mathbb{K} \setminus \{0\}$ enumerates the whole $\mathbb{K} \setminus \{0\}$ with its powers:

Definition. An element α in $\mathbb{K}$ is primitive if $\{\alpha, \alpha^2, \dots, \alpha^m\} = \mathbb{K} \setminus \{0\}$ for some m.

Error-correcting codes

Goal: make a message robust against a certain number of transmission errors

Goal: make a message robust against a certain number of transmission errors

- Ethernet cables/WiFi not 100% reliable
- Even without communication: bits can spontaneously flip inside CPU/memory
- Many examples of this happening because of **cosmic rays**

Goal: make a message robust against a certain number of transmission errors

- Ethernet cables/WiFi not 100% reliable
- Even without communication: bits can spontaneously flip inside CPU/memory
- Many examples of this happening because of **cosmic rays**

BBC

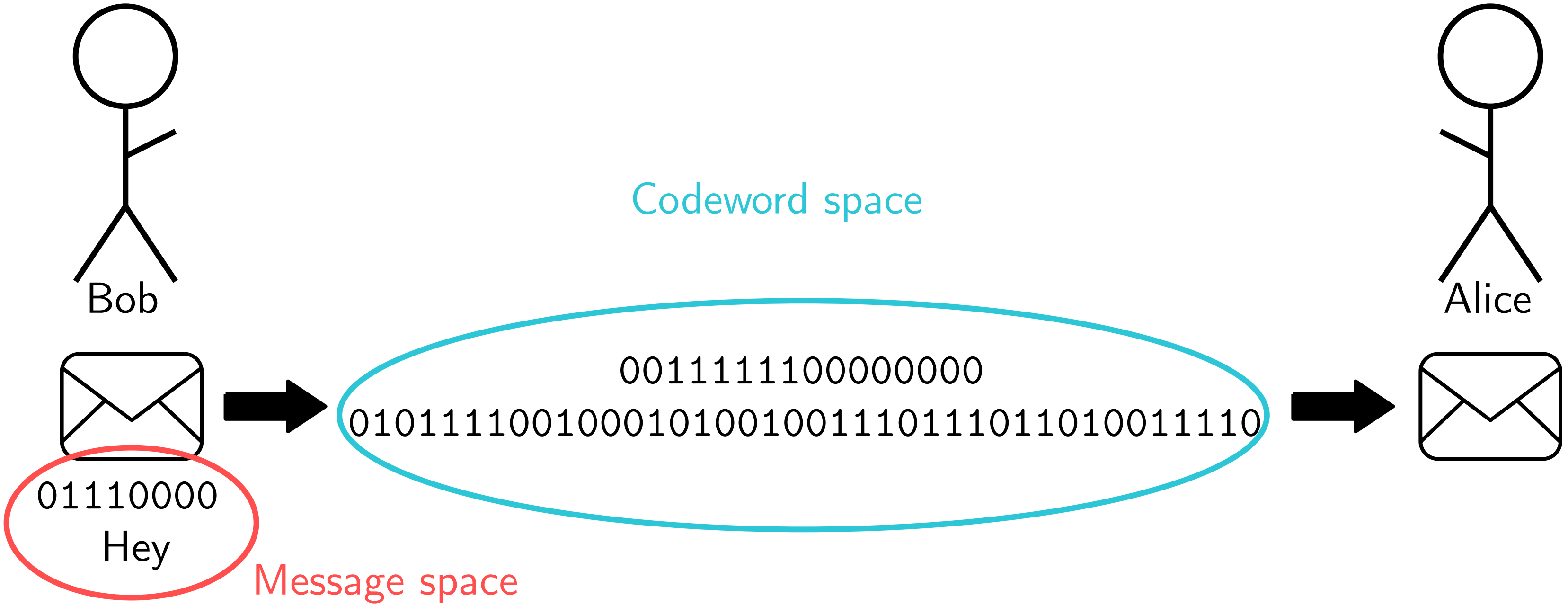
Radiation from space that led to more than 6,000 Airbus aircraft needing emergency computer updates could become a growing problem as ever more microchips run our lives.

"We need medical equipment," the pilot of a JetBlue passenger jet announced over the radio to air traffic control. His plane, an Airbus A320 commercial airliner had suddenly and unexpectedly dropped altitude during a flight from Cancun, in Mexico, to Newark, in New Jersey, US, on 30 October 2025. Three people appeared to have suffered "a laceration in the head", the pilot said. At least 15 people were later taken to hospital when the flight landed after being diverted to Florida.

A month later, this incident would lead to the mass grounding of more than 6,000 aircraft – one of the largest ever aviation industry recalls. It triggered widespread disruption and cancellations over the final weekend of November 2025, one of the busiest of the year for air travel following Thanksgiving in the US.

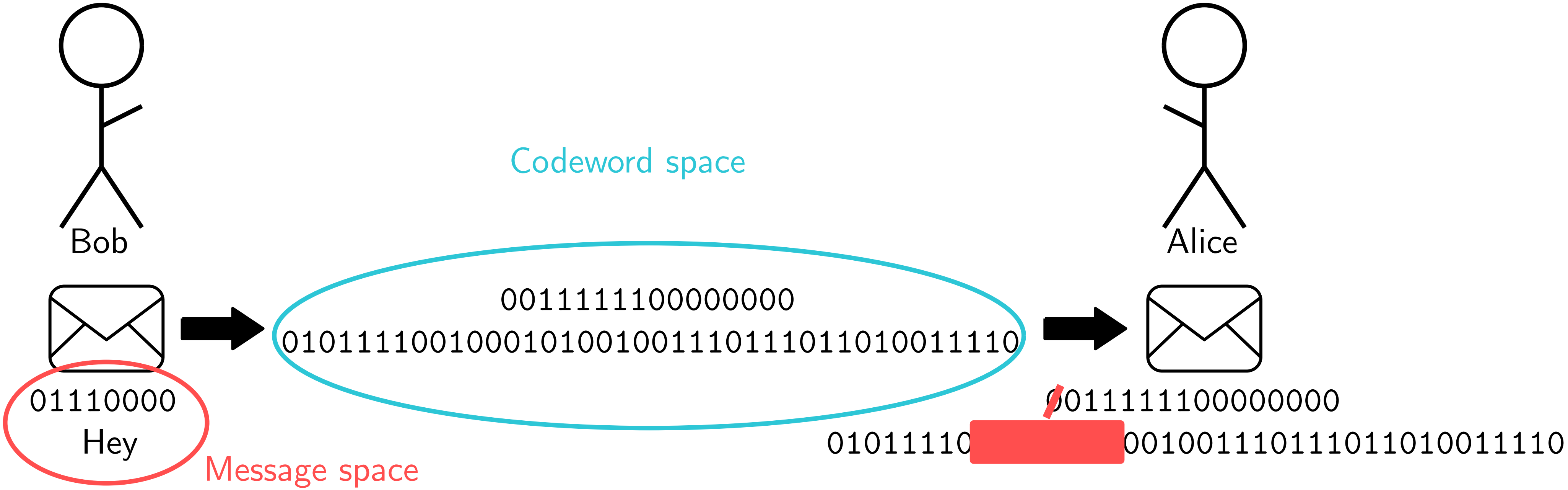
Goal: make a message robust against a certain number of transmission errors

- Ethernet cables/WiFi not 100% reliable
- Even without communication: bits can spontaneously flip inside CPU/memory
- Many examples of this happening because of **cosmic rays**



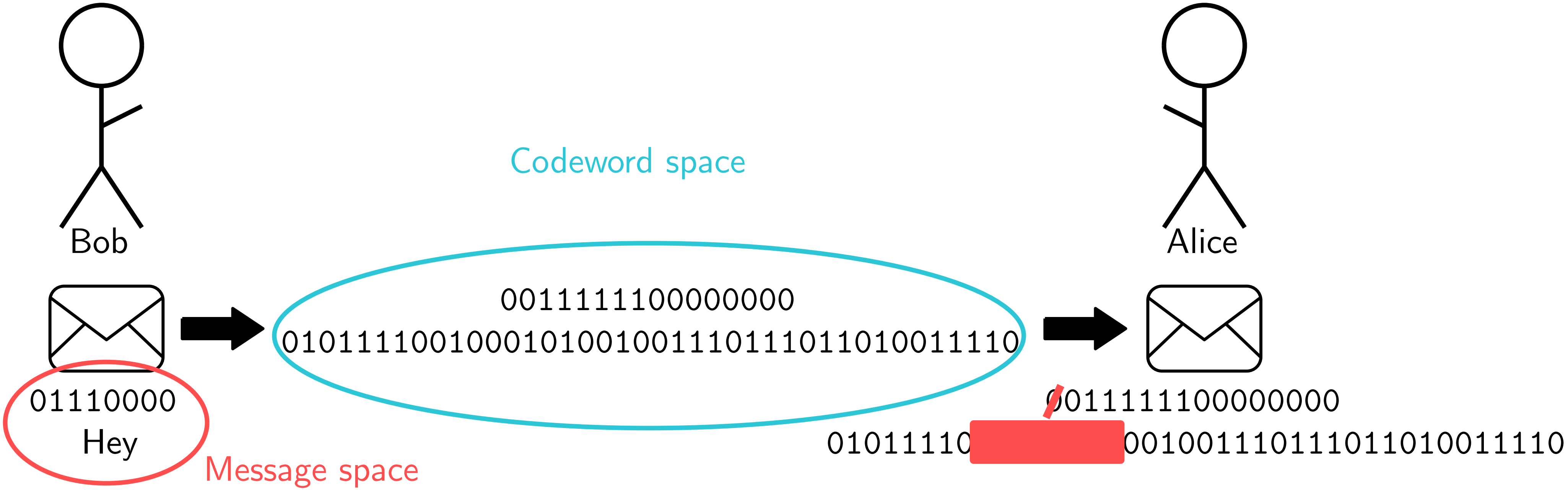
Goal: make a message robust against a certain number of transmission errors

- Ethernet cables/WiFi not 100% reliable
- Even without communication: bits can spontaneously flip inside CPU/memory
- Many examples of this happening because of **cosmic rays**



Goal: make a message robust against a certain number of transmission errors

- Ethernet cables/WiFi not 100% reliable
- Even without communication: bits can spontaneously flip inside CPU/memory
- Many examples of this happening because of **cosmic rays**



Introduction of an error-correcting code that makes input longer but more resistant

- Error detection: just want to know *whether* an error occurred
- Error correction: also want to be able to fix the errors that occurred

- Message of arbitrary length k
- Want to detect $t = 1$ error

- Message of arbitrary length k
- Want to detect $t = 1$ error

Parity bit:

Message	**Codeword**
00011110101010	000111101010101
$m_1 \dots m_k$	11 $\sum_{i=1}^{k} m_i \bmod 2$

- Say we receive $c_1 \dots c_{k+1}$.
- Compute $\sum_{i=1}^{k} c_i \bmod 2$ and compare with c_{k+1}
- If different: there has been an error
- Otherwise: either 0 or > 1 error

- Message of arbitrary length k
- Want to detect $t = 1$ error

Parity bit:

Message	**Codeword**
00011110101010	000111101010101
$m_1 \dots m_k$	$\sum_{i=1}^{k} m_i \bmod 2$

- Say we receive $c_1 \dots c_{k+1}$.
- Compute $\sum_{i=1}^{k} c_i \bmod 2$ and compare with c_{k+1}
- If different: there has been an error
- Otherwise: either 0 or > 1 error

If we see an error, we can't fix it

- Message of arbitrary length k
- Want to detect $t = 1$ error

Parity bit:

Message	**Codeword**
00011110101010	000111101010101
$m_1 \dots m_k$	$\sum_{i=1}^{k} m_i \bmod 2$

- Say we receive $c_1 \dots c_{k+1}$.
- Compute $\sum_{i=1}^{k} c_i \bmod 2$ and compare with c_{k+1}
- If different: there has been an error
- Otherwise: either 0 or > 1 error

If we see an error, we can't fix it

Luhn's code:

Message	**Codeword**
4546 1796 5432 123	

- Message of arbitrary length k
- Want to detect $t = 1$ error

Parity bit:

Message	**Codeword**
00011110101010	000111101010101
$m_1 \dots m_k$	$\sum_{i=1}^{k} m_i \bmod 2$

- Say we receive $c_1 \dots c_{k+1}$.
- Compute $\sum_{i=1}^{k} c_i \bmod 2$ and compare with c_{k+1}
- If different: there has been an error
- Otherwise: either 0 or > 1 error

If we see an error, we can't fix it

Luhn's code:

Message	**Codeword**
4546 1796 5432 123	4546 1796 5432 1236

- Message of arbitrary length k
- Want to detect $t = 1$ error

Parity bit:

Message	**Codeword**
00011110101010	000111101010101
$m_1 \dots m_k$	$\sum_{i=1}^{k} m_i \bmod 2$

- Say we receive $c_1 \dots c_{k+1}$.
- Compute $\sum_{i=1}^{k} c_i \bmod 2$ and compare with c_{k+1}
- If different: there has been an error
- Otherwise: either 0 or > 1 error

If we see an error, we can't fix it

Luhn's code:

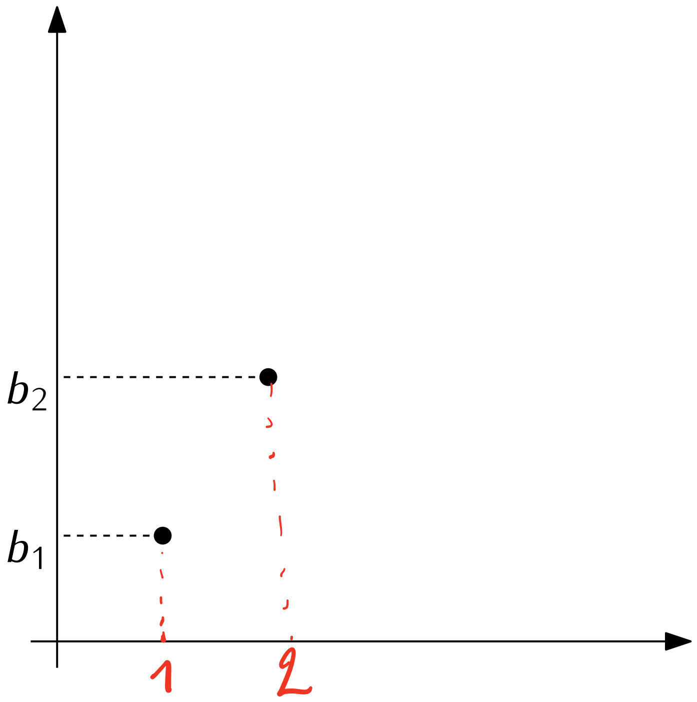
Message	**Codeword**
4546 1796 5432 123	4546 1796 5432 1236
$m_1 \dots m_k$	$10 - \sum_{i=1}^{k}(1.5 + (-0.5)^{i+1})m_i \bmod 10$

Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Genius idea:

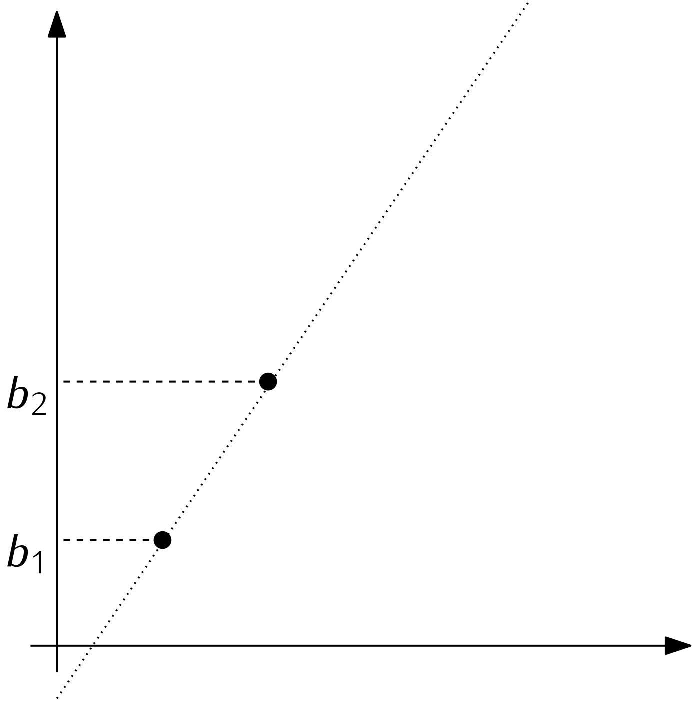
- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$



Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Genius idea:

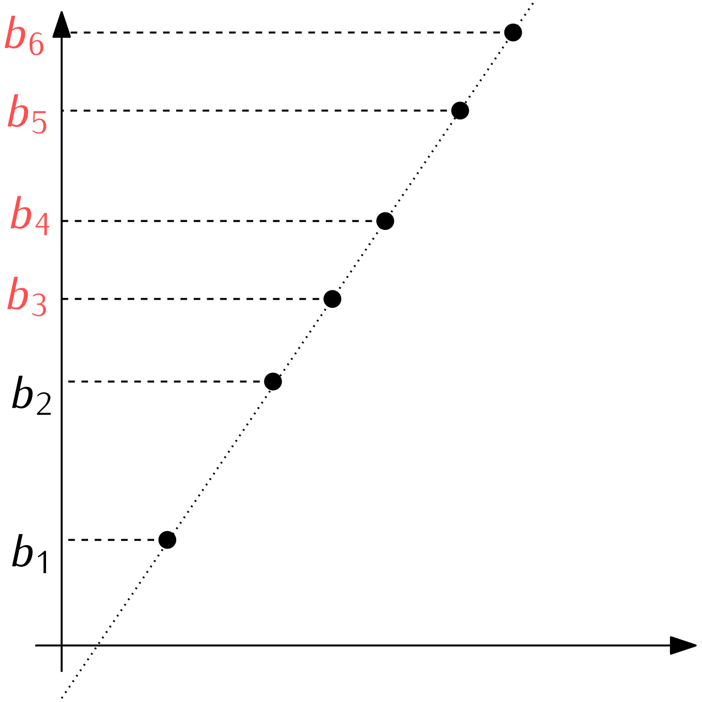
- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$



Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Genius idea:

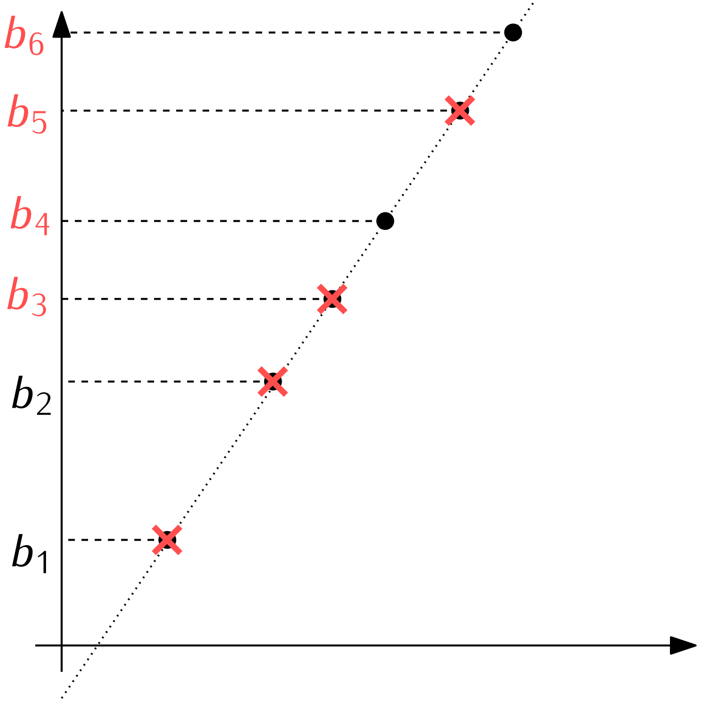
- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$
- add 4 points on line passing through b_0 and b_1



Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Genius idea:

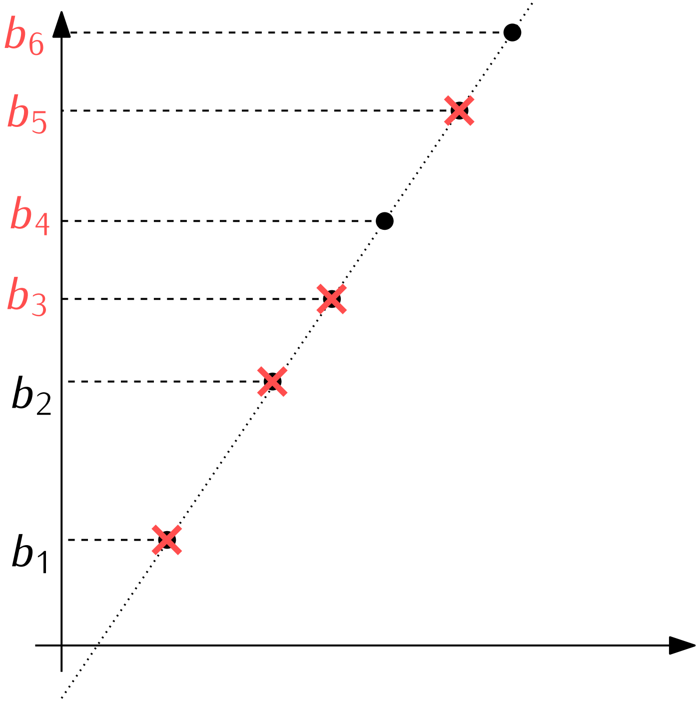
- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$
- add 4 points on line passing through b_0 and b_1
- any removal of ≤ 4 points still allows us to recover the line and therefore original message



Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

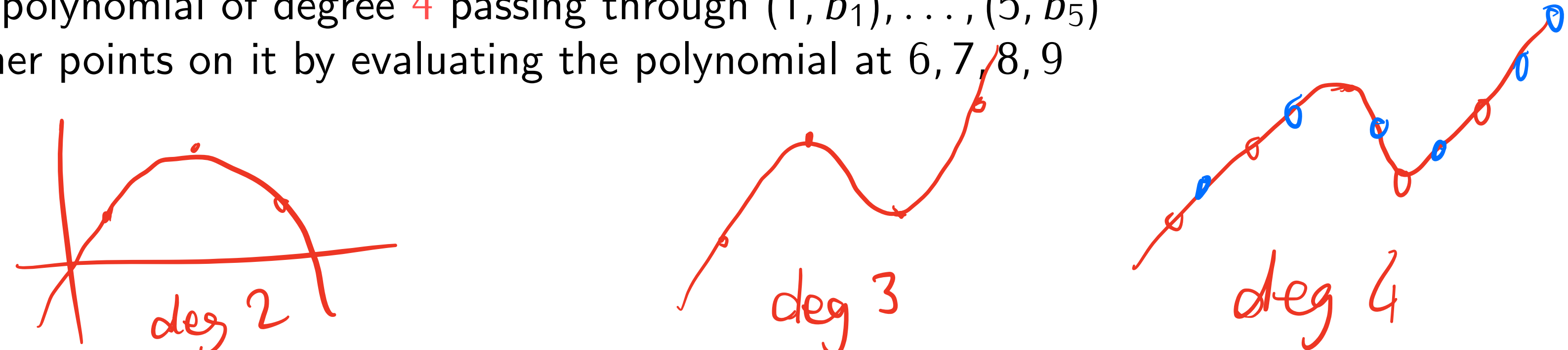
Genius idea:

- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$
- add 4 points on line passing through b_0 and b_1
- any removal of ≤ 4 points still allows us to recover the line and therefore original message



Want to send $b_1 \ldots b_5$ of length $k = 5$?

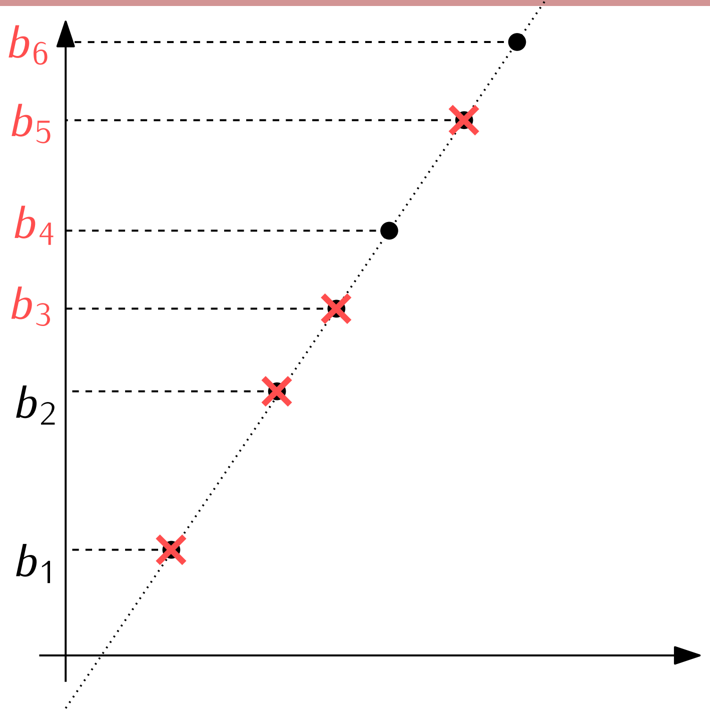
- Compute polynomial of degree 4 passing through $(1, b_1), \ldots, (5, b_5)$
- Add 4 other points on it by evaluating the polynomial at $6, 7, 8, 9$



Message to send: $b_1 b_2$ of length $k = 2$
Want to make it resistant to $t = 4$ errors

Genius idea:

- see message as points $(1, b_1), (2, b_2)$ in $\mathbb{R}^2$
- add 4 points on line passing through b_0 and b_1
- any removal of ≤ 4 points still allows us to recover the line and therefore original message



Want to send $b_1 \ldots b_5$ of length $k = 5$?

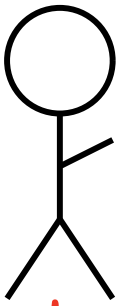
- Compute polynomial of degree 4 passing through $(1, b_1), \ldots, (5, b_5)$
- Add 4 other points on it by evaluating the polynomial at $6, 7, 8, 9$

In tutorials this week: implementation of a variant of this code in Python

- Units of data: bits or packets of bits (8 bits = 1 byte)
- Number of possible values for a byte? 2^8
- There is a field $\mathbb{K}$ of that size
- k bytes $\leftrightarrow$ coefficients of a polynomial of degree $\leq k-1$ with coefficients in $\mathbb{K}$

- Units of data: bits or packets of bits (8 bits = 1 byte)
- Number of possible values for a byte?
- There is a field $\mathbb{K}$ of that size
- k bytes $\leftrightarrow$ coefficients of a polynomial of degree $\leq k-1$ with coefficients in $\mathbb{K}$

$k=3$



I<3~~|~~DAS

I<3

10010010 $\in \mathbb{K}$ → 10010010
00111100 $\in \mathbb{K}$ → $+00111100X$
11001100 $\in \mathbb{K}$ → $+11001100X^2$

DAS

00100010 → 00100010
10000010 → $+10000010X$
11001010 → $+11001010X^2$

`StringToPolynomials`

$$P_0 = 10010010 + 00111100X + 11001100X^2 \qquad P_1 = 00100010 + 10000010X + 11001010X^2$$

Encoding method:

- Want to make each block robust against t wrong coefficients

$$P_0 = 10010010 + 00111100X + 11001100X^2 \qquad P_1 = 00100010 + 10000010X + 11001010X^2$$

Encoding method:

- Want to make each block robust against t wrong coefficients
- Let α be a primitive element of $\mathbb{K}$ (has order $= 255$ in the group $(\mathbb{K} \setminus \{0\}, \times)$)

$P_0 = 10010010 + 00111100X + 11001100X^2$ $P_1 = 00100010 + 10000010X + 11001010X^2$

Encoding method:

- Want to make each block robust against t wrong coefficients
- Let α be a primitive element of $\mathbb{K}$ (has order $= 255$ in the group $(\mathbb{K} \setminus \{0\}, \times)$)
- $G = (X - \alpha)(X - \alpha^2) \ldots (X - \alpha^{2t})$

$$P_0 = 10010010 + 00111100X + 11001100X^2 \qquad P_1 = 00100010 + 10000010X + 11001010X^2$$

Encoding method:

- Want to make each block robust against t wrong coefficients
- Let α be a primitive element of $\mathbb{K}$ (has order $= 255$ in the group $(\mathbb{K} \setminus \{0\}, \times)$)
- $G = (X - \alpha)(X - \alpha^2) \dots (X - \alpha^{2t})$
- Compute P_0G and P_1G, of degree $k - 1 + 2t$

$$P_0 = 10010010 + 00111100X + 11001100X^2 \qquad P_1 = 00100010 + 10000010X + 11001010X^2$$

Encoding method:

- Want to make each block robust against t wrong coefficients
- Let α be a primitive element of $\mathbb{K}$ (has order $= 255$ in the group $(\mathbb{K} \setminus \{0\}, \times)$)
- $G = (X - \alpha)(X - \alpha^2) \dots (X - \alpha^{2t})$
- Compute $P_0 G$ and $P_1 G$, of degree $k - 1 + 2t$

For $t = 1$: $(X-\alpha)\cdot(X-\alpha^2)$

- $G = 00010000 + 01100000X + 10000000X^2$
- $D_0 := P_0 G = 01001110 + 01101010X + 00100010X^2 + 01101001X^3 + 11001100X^4$
- $D_1 := P_1 G = 01011000 + 11101101X + 10111110X^2 + 01101101X^3 + 11001010X^4$

6 bytes in, 10 bytes out. Erasing any byte will be recoverable.

$$P_0 = 10010010 + 00111100X + 11001100X^2 \qquad P_1 = 00100010 + 10000010X + 11001010X^2$$

Encoding method:

- Want to make each block robust against t wrong coefficients
- Let α be a primitive element of $\mathbb{K}$ (has order $= 255$ in the group $(\mathbb{K} \setminus \{0\}, \times)$)
- $G = (X - \alpha)(X - \alpha^2) \dots (X - \alpha^{2t})$
- Compute $P_0 G$ and $P_1 G$, of degree $k - 1 + 2t$

For $t = 1$:

- $G = 00010000 + 01100000X + 10000000X^2$
- $D_0 := P_0 G = 01001110 + 01101010X + 00100010X^2 + 01101001X^3 + 11001100X^4$
- $D_1 := P_1 G = 01011000 + 11101101X + 10111110X^2 + 01101101X^3 + 11001010X^4$

6 bytes in, 10 bytes out. Erasing any byte will be recoverable.

Decoding method: divide the received polynomial by G

Problem to solve: given a polynomial $F \in \mathbb{K}[X]$, how to know whether it has been correctly transmitted?

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = \mathtt{10} + \mathtt{60}X + \mathtt{80}X^2$	known
Error:	$E = F - D = \mathtt{16}X^2$	unknown

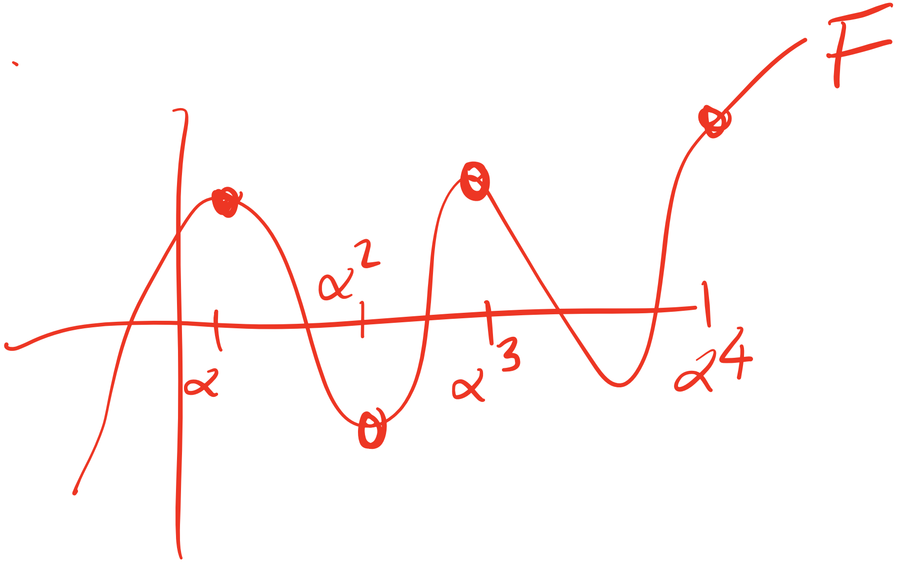
Problem to solve: given a polynomial $F \in \mathbb{K}[X]$, how to know whether it has been correctly transmitted?

$$
\begin{aligned}
E(\alpha^i) &= (F - D)(\alpha^i) \\
&= F(\alpha^i) - \cancel{G(\alpha^i)P(\alpha^i)}\ 0 \\
&= F(\alpha^i)
\end{aligned}
$$

Sent:	$D = 4\mathtt{E} + 6\mathtt{A}X + 22X^2 + 69X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = 4\mathtt{E} + 6\mathtt{A}X + 34X^2 + 69X^3 + \mathtt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

$G = (X-\alpha)(X-\alpha^2)\cdots$

$G(\alpha) = \underbrace{(\alpha-\alpha)}_{0}(\alpha-\alpha^2)\cdots$



Problem to solve: given a polynomial $F \in \mathbb{K}[X]$, how to know whether it has been correctly transmitted?

$$\begin{aligned} E(\alpha^i) &= (F - D)(\alpha^i) \\ &= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\ &= F(\alpha^i) \end{aligned}$$

It should be 0 if no errors!

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = \mathtt{10} + \mathtt{60}X + \mathtt{80}X^2$	known
Error:	$E = F - D = \mathtt{16}X^2$	unknown

Theorem. If $F(\alpha^i) \neq 00000000$ for some $i \in \{1, \ldots, 2t\}$, then we know there has been an error.

Problem to solve: given a polynomial $F \in \mathbb{K}[X]$, how to know whether it has been correctly transmitted?

$$\begin{aligned} E(\alpha^i) &= (F - D)(\alpha^i) \\ &= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\ &= F(\alpha^i) \end{aligned}$$

It should be 0 if no errors!

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = \mathtt{10} + \mathtt{60}X + \mathtt{80}X^2$	known
Error:	$E = F - D = \mathtt{16}X^2$	unknown

Theorem. If $F(\alpha^i) \neq 00000000$ for some $i \in \{1, \ldots, 2t\}$, then we know there has been an error.

- Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?
- Error correction: If we detect an error, can we still recover D?

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = n \overbrace{\begin{pmatrix} \\ \\ \\ \end{pmatrix}}^{1}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix}$$

$$\begin{array}{c} \begin{array}{cccc} c_1 & c_2 & & c_n \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \end{array} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = x_1 \cdot \overset{c_1}{\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}} + \cdots + x_n \overset{c_n}{\begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

- Solving $Ax = b$ means: is there a way to express b as a (weighted) sum of the columns of A

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

- Solving $Ax = b$ means: is there a way to express b as a (weighted) sum of the columns of A
- What can we say if A has an inverse?

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- Solving $Ax = b$ means: is there a way to express b as a (weighted) sum of the columns of A
- What can we say if A has an inverse?
- What can we say if we know $x_4 = \dots = x_n = 0$?

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ \vdots & & \\ a_{n1} & a_{n2} & a_{n3} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = b$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

- Solving $Ax = b$ means: is there a way to express b as a (weighted) sum of the columns of A
- What can we say if A has an inverse?
- What can we say if we know $x_4 = \dots = x_n = 0$?

Theorem. Let $\alpha_1, \dots, \alpha_n$ be pairwise distinct elements of a field which are all different from 0.
Then $\begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \alpha_1^2 & \dots & \alpha_n^2 \\ \vdots & & \vdots \\ \alpha_1^n & \dots & \alpha_n^n \end{pmatrix}$ has an inverse.

$$E(\alpha^i) = (F - D)(\alpha^i)$$
$$= F(\alpha^i) - G(\alpha^i)P(\alpha^i)$$
$$= F(\alpha^i)$$

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + 22X^2 + 69X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + 34X^2 + 69X^3 + \mathtt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

$$
\begin{aligned}
E(\alpha^i) &= (F - D)(\alpha^i) \\
&= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\
&= F(\alpha^i)
\end{aligned}
$$

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = \mathtt{10} + \mathtt{60}X + \mathtt{80}X^2$	known
Error:	$E = F - D = \mathtt{16}X^2$	unknown

$$E(\alpha^i) = (F - D)(\alpha^i)$$
$$= F(\alpha^i) - G(\alpha^i)P(\alpha^i)$$
$$= F(\alpha^i)$$

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- So $E(\alpha) = e_0 + e_1\alpha + e_2\alpha^2 + \ldots e_{k+2t-1}\alpha^{k+2t-1}$ $= F(\alpha)$

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + 22X^2 + 69X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + 34X^2 + 69X^3 + \mathtt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

$$E(\alpha^i) = (F-D)(\alpha^i) = F(\alpha^i) - G(\alpha^i)P(\alpha^i) = F(\alpha^i)$$

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- In general: $E(\alpha^i) = e_0 + e_1 \alpha^i + e_2 \alpha^{2i} + \cdots + e_{k+2t-1} \alpha^{(k+2t-1)i}$

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = \mathtt{10} + \mathtt{60}X + \mathtt{80}X^2$	known
Error:	$E = F - D = \mathtt{16}X^2$	unknown

$$\begin{aligned} E(\alpha^i) &= (F - D)(\alpha^i) \\ &= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\ &= F(\alpha^i) \end{aligned}$$

Sent:	$D = \mathtt{4E} + \mathtt{6A}X + \mathtt{22}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = \mathtt{4E} + \mathtt{6A}X + \mathtt{34}X^2 + \mathtt{69}X^3 + \mathtt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- In general: $E(\alpha^i) = e_0 + e_1 \alpha^i + e_2 \alpha^{2i} + \cdots + e_{k+2t-1} \alpha^{(k+2t-1)i}$
- So $\begin{pmatrix} 00000000 \\ \vdots \\ 00000000 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \ldots & \alpha^{(k+2t-1)2t} \end{pmatrix} \begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}$

$$\| \\ \begin{pmatrix} E(\alpha) \\ E(\alpha^2) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}$$

$$\begin{aligned} E(\alpha^i) &= (F - D)(\alpha^i) \\ &= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\ &= F(\alpha^i) \end{aligned}$$

Sent:	$D = \texttt{4E} + \texttt{6A}X + \texttt{22}X^2 + \texttt{69}X^3 + \texttt{CC}X^4$	unknown
Received:	$F = \texttt{4E} + \texttt{6A}X + \texttt{34}X^2 + \texttt{69}X^3 + \texttt{CC}X^4$	known
Generator:	$G = \texttt{10} + \texttt{60}X + \texttt{80}X^2$	known
Error:	$E = F - D = \texttt{16}X^2$	unknown

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \dots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- In general: $E(\alpha^i) = e_0 + e_1 \alpha^i + e_2 \alpha^{2i} + \cdots + e_{k+2t-1} \alpha^{(k+2t-1)i}$
- So $\underbrace{\begin{pmatrix} 00000000 \\ \vdots \\ 00000000 \end{pmatrix}}_{= b}$ can be written as $\underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{= A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{= x}$

$$
\begin{aligned}
E(\alpha^i) &= (F - D)(\alpha^i) \\
&= F(\alpha^i) - G(\alpha^i)P(\alpha^i) \\
&= F(\alpha^i)
\end{aligned}
$$

Sent:	$D = 4\mathtt{E} + 6\mathtt{A}X + 22X^2 + 69X^3 + \mathtt{CC}X^4$	unknown
Received:	$F = 4\mathtt{E} + 6\mathtt{A}X + 34X^2 + 69X^3 + \mathtt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \ldots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- In general: $E(\alpha^i) = e_0 + e_1 \alpha^i + e_2 \alpha^{2i} + \cdots + e_{k+2t-1} \alpha^{(k+2t-1)i}$
- So $\underbrace{\begin{pmatrix} 00000000 \\ \vdots \\ 00000000 \end{pmatrix}}_{=\, b}$ can be written as $\underbrace{2t\left\{\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \ldots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \ldots & \alpha^{(k+2t-1)2t} \end{pmatrix}\right.}_{k+2t;\ =\, A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{=\, x}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$E(\alpha^i) = (F - D)(\alpha^i) = F(\alpha^i) - G(\alpha^i)P(\alpha^i) = F(\alpha^i)$$

Sent:	$D = \texttt{4E} + \texttt{6A}X + 22X^2 + 69X^3 + \texttt{CC}X^4$	unknown
Received:	$F = \texttt{4E} + \texttt{6A}X + 34X^2 + 69X^3 + \texttt{CC}X^4$	known
Generator:	$G = 10 + 60X + 80X^2$	known
Error:	$E = F - D = 16X^2$	unknown

Error detection: What can we say if $F(\alpha^i) = 00000000$ for all $i \in \{1, \dots, 2t\}$?

- Write $E = e_0 + e_1 X + \cdots + e_{k+2t-1} X^{k+2t-1}$
- In general: $E(\alpha^i) = e_0 + e_1 \alpha^i + e_2 \alpha^{2i} + \cdots + e_{k+2t-1} \alpha^{(k+2t-1)i}$
- So $\underbrace{\begin{pmatrix} 00000000 \\ \vdots \\ 00000000 \end{pmatrix}}_{b}$ can be written as $\underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

But there could be many solutions... (there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- So $\begin{pmatrix} 00000000 \\ b \\ 00000000 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & A & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix} \begin{pmatrix} e_0 \\ x \\ e_{k+2t-1} \end{pmatrix}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

What if we can assume there were at most $2t$ errors?

- So $\begin{pmatrix} 00000000 \\ b \\ 00000000 \end{pmatrix}$ can be written as $2t \left\{ \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & A & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix} \right. \begin{pmatrix} e_0 \\ x \\ e_{k+2t-1} \end{pmatrix}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

What if we can assume there were at most $2t$ errors?

- Only $\leq 2t$ components $x_{j_1}, \dots, x_{j_{2t}}$ of **x** are not zero.
- The system of equations $\underbrace{A_J}_{2t \times 2t} \cdot \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_{2t}} \end{pmatrix} = \mathbf{b}$ has a solution $\begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_{2t}} \end{pmatrix}$

- So $\begin{pmatrix} 00000000 \\ b \\ 00000000 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & A & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix} \begin{pmatrix} e_0 \\ x \\ e_{k+2t-1} \end{pmatrix}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

What if we can assume there were at most $2t$ errors?

- Only $\leq 2t$ components $x_{j_1}, \dots, x_{j_{2t}}$ of $\mathbf{x}$ are not zero.
- The system of equations $A_J \cdot \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_{2t}} \end{pmatrix} = \mathbf{b}$ has a solution $\begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_{2t}} \end{pmatrix}$
- Even a unique solution since all $1, \alpha, \alpha^2, \dots, \alpha^{k+2t-1}$ are different!

- So $\begin{pmatrix} 00000000 \\ b \\ 00000000 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & A & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix} \begin{pmatrix} e_0 \\ x \\ e_{k+2t-1} \end{pmatrix}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

What if we can assume there were at most $2t$ errors?

- Only $\leq 2t$ components $x_{j_1}, \dots, x_{j_{2t}}$ of $\mathbf{x}$ are not zero.
- The system of equations $A_J \cdot \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_{2t}} \end{pmatrix} = \mathbf{b}$ has a solution $\begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_{2t}} \end{pmatrix}$
- Even a unique solution since all $1, \alpha, \alpha^2, \dots, \alpha^{k+2t-1}$ are different!
- We know a trivial solution: $\mathbf{x} = \mathbf{0}$

  These solutions must be equal: all coefficients of E are 0!

$Bx = 0 \Rightarrow x = 0.$

- So $\begin{pmatrix} 00000000 \\ \vdots \\ b \\ \vdots \\ 00000000 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & A & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix} \begin{pmatrix} e_0 \\ x \\ \vdots \\ e_{k+2t-1} \end{pmatrix}$

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

What if we can assume there were at most $2t$ errors?

- Only $\leq 2t$ components $x_{j_1}, \dots, x_{j_{2t}}$ of $\mathbf{x}$ are not zero.
- The system of equations $A_J \cdot \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_{2t}} \end{pmatrix} = \mathbf{b}$ has a solution $\begin{pmatrix} e_{j_1} \\ \vdots \\ e_{j_{2t}} \end{pmatrix}$
- Even a unique solution since all $1, \alpha, \alpha^2, \dots, \alpha^{k+2t-1}$ are different!
- We know a trivial solution: $\mathbf{x} = \mathbf{0}$

  These solutions must be equal: all coefficients of E are 0!

Theorem. Let F be the polynomial we received, and E be the error polynomial. Then either:

- $F(\alpha^i) \neq 00000000$ for some $i \in \{1, \dots, 2t\}$, and there was at least one transmission error
- $F(\alpha^i) = 00000000$ for all $i \in \{1, \dots, 2t\}$ and there was either 0 or $> 2t$ errors

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- Assume there were $\leq t$ errors at positions $J = \{j_1, \dots, j_t\}$
  \+ **x** solution to $Ax = b$ that has at most t non-zero components $J' = \{j'_1, \dots, j'_t\}$

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- Assume there were $\leq t$ errors at positions $J = \{j_1, \dots, j_t\}$
  \+ x solution to $Ax = b$ that has at most t non-zero components $J' = \{j_1', \dots, j_t'\}$
- $|J \cup J'|$? $\leq 2t$

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- Assume there were $\leq t$ errors at positions $J = \{j_1, \dots, j_t\}$
  $+$ **x** solution to $Ax = b$ that has at most t non-zero components $J' = \{j'_1, \dots, j'_t\}$
- $|J \cup J'|$?
- $A_{J \cup J'}$ has two solutions: solution given by $e_{j_1}, \dots, e_{j_t}$ and the solution given by **x**
- Same argument as before: $A_{J \cup J'}$ has only one solution, so $J \subseteq J'$
  $\rightsquigarrow e_{j_1}, \dots, e_{j_t}$ are the components of **x**

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- Assume there were $\leq t$ errors at positions $J = \{j_1, \dots, j_t\}$
  $+$ x solution to $Ax = b$ that has at most t non-zero components $J' = \{j'_1, \dots, j'_t\}$
- $|J \cup J'|$?
- $A_{J \cup J'}$ has two solutions: solution given by $e_{j_1}, \dots, e_{j_t}$ and the solution given by x
- Same argument as before: $A_{J \cup J'}$ has only one solution, so $J \subseteq J'$
  $\rightsquigarrow e_{j_1}, \dots, e_{j_t}$ are the components of x

Theorem. Suppose that $Ax =$ b has a solution x with at most t non-zero coefficients.
If there are at most t errors, then the non-zero coefficients of x list all the errors.

Can we *fix* it?

Theorem. The coefficients of E are a solution to the system of equations $Ax = b$.

$$\underbrace{\begin{pmatrix} E(\alpha) \\ \vdots \\ E(\alpha^{2t}) \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(k+2t-1)2} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha^{2t} & \alpha^{4t} & \dots & \alpha^{(k+2t-1)2t} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e_0 \\ \vdots \\ e_{k+2t-1} \end{pmatrix}}_{x}$$

But there could be many solutions...
(there are in fact $\geq 256^k = 2^{8k}$ solutions in column vectors of length $k + 2t$)

- Assume there were $\leq t$ errors at positions $J = \{j_1, \dots, j_t\}$
  \+ $\mathbf{x}$ solution to $Ax = b$ that has at most t non-zero components $J' = \{j'_1, \dots, j'_t\}$
- $|J \cup J'|$?
- $A_{J \cup J'}$ has two solutions: solution given by $e_{j_1}, \dots, e_{j_t}$ and the solution given by $\mathbf{x}$
- Same argument as before: $A_{J \cup J'}$ has only one solution, so $J \subseteq J'$
  $\rightsquigarrow e_{j_1}, \dots, e_{j_t}$ are the components of $\mathbf{x}$

Theorem. Suppose that $Ax = \mathbf{b}$ has a solution $\mathbf{x}$ with at most t non-zero coefficients.
If there are at most t errors, then the non-zero coefficients of $\mathbf{x}$ list all the errors.

(Note: there are much more efficient ways to correct errors, but too clever for this course)

Bytes = 8-bit strings = elements of GF(256), the field of size 256

Encoding: Multiply message P by the generator polynomial $G = (X - \alpha) \dots (X - \alpha^{2t})$

Decoding of correct message: Division by that same polynomial

Detecting errors:

1. Evaluate the received polynomial F: $F(\alpha), F(\alpha^2), \dots, F(\alpha^{2t})$
2. If all results are 0: no errors (or maybe $> 2t$ errors)
3. If some is not 0: can be sure there was an error

Bytes = 8-bit strings = elements of GF(256), the field of size 256

Encoding: Multiply message P by the generator polynomial $G = (X - \alpha) \dots (X - \alpha^{2t})$

Decoding of correct message: Division by that same polynomial

Detecting errors:

1. Evaluate the received polynomial F: $F(\alpha), F(\alpha^2), \dots, F(\alpha^{2t})$
2. If all results are 0: no errors (or maybe $> 2t$ errors)
3. If some is not 0: can be sure there was an error

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

×	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$k = 2, t = 1$

$G = X^2 + X + 1$

I received $F = X^3 + (1+\alpha)X + \alpha$

Was there a communication error?

- $F(\alpha) = \alpha^3 + (1+\alpha)\alpha + \alpha = 1 + \alpha + \alpha^2 + \alpha = 1$
- $F(\alpha^2) = \alpha^6 + (1+\alpha)\alpha^2 + \alpha = 1 + \alpha$?

Bytes = 8-bit strings = elements of GF(256), the field of size 256

Encoding: Multiply message P by the generator polynomial $G = (X - \alpha) \dots (X - \alpha^{2t})$

Decoding of correct message: Division by that same polynomial

Detecting errors:

1. Evaluate the received polynomial F: $F(\alpha), F(\alpha^2), \dots, F(\alpha^{2t})$
2. If all results are 0: no errors (or maybe $> 2t$ errors)
3. If some is not 0: can be sure there was an error

Fixing errors: for each $J = \{j_1, \dots, j_{2t}\} \subseteq \{1, \dots, k + 2t - 1\}$ of size $2t$:

1. Compute matrix $A_J = \begin{pmatrix} \alpha^{j_1} & \dots & \alpha^{j_{2t}} \\ \vdots & & \vdots \\ \alpha^{2tj_1} & \dots & \alpha^{2t_{2t}} \end{pmatrix}$
2. Solve $A_J x = \begin{pmatrix} F(\alpha) \\ \vdots \\ F(\alpha^{2t}) \end{pmatrix}$
3. If x has at most t entries that are not 0: $E = \sum_{n=1}^{2t} e_{j_n} X^{j_n}$
4. The corrected polynomial is $F - E$

$$\begin{array}{c|cccc|} & 0 & 1 & \alpha & 1+\alpha \\ \hline 0 & 0 & 1 & \alpha & 1+\alpha \\ 1 & 1 & 0 & 1+\alpha & \alpha \\ \alpha & \alpha & 1+\alpha & 0 & 1 \\ 1+\alpha & 1+\alpha & \alpha & 1 & 0 \\ \hline \end{array} \qquad \begin{array}{c|cccc|} & 0 & 1 & \alpha & 1+\alpha \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & \alpha & 1+\alpha \\ \alpha & 0 & \alpha & 1+\alpha & 1 \\ 1+\alpha & 0 & 1+\alpha & 1 & \alpha \\ \hline \end{array}$$

Fixing errors: for each $J = \{j_1, \dots, j_{2t}\} \subseteq \{1, \dots, k+2t-1\}$ of size $2t$:

1. Compute matrix $A_J = \begin{pmatrix} \alpha^{j_1} & \dots & \alpha^{j_{2t}} \\ \vdots & & \vdots \\ \alpha^{2tj_1} & \dots & \alpha^{2t_{2t}} \end{pmatrix}$
2. Solve $A_J x = \begin{pmatrix} F(\alpha) \\ \vdots \\ F(\alpha^{2t}) \end{pmatrix}$
3. If x has at most t entries that are not 0: $E = \sum_{n=1}^{2t} e_{j_n} X^{j_n}$
4. The corrected polynomial is $F - E$

$k = 2, t = 1$
$G = X^2 + X + 1$
I received $F = X^3 + (1+\alpha)X + \alpha$ and know that the coefficient of X or X^2 is wrong.
What was the communication error?

$$\begin{pmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1+\alpha \end{pmatrix}$$

Already implemented for you:

- `FiniteField.py`: implementation of field with 256 elements
- `Gauss.py`: solving systems of linear equations $Ax = b$ with arbitrary coefficients (when A is invertible)

Your task:

- `Polynomial.py`: implement addition, multiplication, division with remainder, evaluation function
- `ReedSolomon.py`: implement encoding/decoding, error detection, error correction