Network Coding
Lecture 1

Felice Manganiello
Clemson University

ICERM
Graduate Workshop on Linear Algebra over Finite Fields & Applications

- Facts about Finite Fields.
- From Channels to Networks
- One Source Networks
  - The Unicast Network
  - The Multicast Network

What is a field?

A field is a nonempty set $\mathbb{F}$ with two operations, addition $(+)$ and multiplication $(\cdot)$ such that for all $a, b, c \in \mathbb{F}$:

- ✓ $(\mathbb{F}, +)$ is an abelian group
  - $+$ is associative: $a + (b + c) = (a + b) + c$
  - there is an additive ~~unit~~ neutral element: $a + 0 = 0 + a = a$
  - there is an additive inverse element: $a + (-a) = (-a) + a = 0$
  - $+$ is commutative: $a + b = b + a$

What is a field?

A field is a nonempty set $\mathbb{F}$ with two operations, addition $(+)$ and multiplication $(\cdot)$ such that for all $a, b, c \in \mathbb{F}$:

- ✓ $(\mathbb{F}, +)$ is an abelian group
  - $+$ is associative: $a + (b + c) = (a + b) + c$
  - there is an additive unit element: $a + 0 = 0 + a = a$
  - there is an additive inverse element: $a + (-a) = (-a) + a = 0$
  - $+$ is commutative: $a + b = b + a$
- ✓ $\cdot$ is associative: $a(bc) = (ab)c$
- ✓ $\cdot$ is commutative: $ab = ba$
- ✓ there is a multiplicative ~~unit~~ neutral element: $a1 = 1a = a$
- ✓ there is a multiplicative inverse element: $aa^{-1} = a^{-1}a = 1$ if $a \neq 0$

What is a field?

A field is a nonempty set $\mathbb{F}$ with two operations, addition $(+)$ and multiplication $(\cdot)$ such that for all $a, b, c \in \mathbb{F}$:

- ✓ $(\mathbb{F}, +)$ is an abelian group
  - $+$ is associative: $a + (b + c) = (a + b) + c$
  - there is an additive unit element: $a + 0 = 0 + a = a$
  - there is an additive inverse element: $a + (-a) = (-a) + a = 0$
  - $+$ is commutative: $a + b = b + a$
- ✓ $\cdot$ is associative: $a(bc) = (ab)c$
- ✓ $\cdot$ is commutative: $ab = ba$
- ✓ there is a multiplicative unit element: $a1 = 1a = a$
- ✓ there is a multiplicative inverse element: $aa^{-1} = a^{-1}a = 1$ if $a \neq 0$
- ✓ Distributivity holds: $(a + b)c = ac + bc$

What is a field?

A field is a nonempty set $\mathbb{F}$ with two operations, addition ($+$) and multiplication ($\cdot$) such that for all $a, b, c \in \mathbb{F}$:

- $(\mathbb{F}, +)$ is an abelian group
  - $+$ is associative: $a + (b + c) = (a + b) + c$
  - there is an additive unit element: $a + 0 = 0 + a = a$
  - there is an additive inverse element: $a + (-a) = (-a) + a = 0$
  - $+$ is commutative: $a + b = b + a$
- $\cdot$ is associative: $a(bc) = (ab)c$
- $\cdot$ is commutative: $ab = ba$
- there is a multiplicative unit element: $a1 = 1a = a$
- there is a multiplicative inverse element: $aa^{-1} = a^{-1}a = 1$ if $a \neq 0$
- Distributivity holds: $(a + b)c = ac + bc$

Example of fields: $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{Z}_p$ p prime, $\mathbb{F}_q$

Finite Fields

Definition

A **finite field** is a field with a finite number of elements.

- The cardinality of a finite field is a power of a prime, meaning that if $\mathbb{F}_q$ is a finite field with q elements, then $q = p^t$ for some prime p.

Why?

- If p is a prime, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ and is called **prime field.**

Example: $\mathbb{F}_3$ = {0, 1, 2}

- If $q = p^t$ with p prime, then $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(\mu)$ where $\mu \in \mathbb{F}_p[x]$ is irreducible of degree t.

Example: $\mathbb{F}_9$ x^2+x-1 x^2+1 $\mathbb{F}_3[x]/(x^2+1) =$

Finite Fields

- Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ has q^m elements, where $m = [F : K]$. Moreover, for all $\mu \in \mathbb{K}[x]$ irreducible with degree m such that $\mathbb{F} \simeq \mathbb{K}[x]/(\mu)$.

- If $\mathbb{F}$ is a finite field with q elements, then $a^q = a$ for all $a \in \mathbb{F}$.

- If $\mathbb{F}$ is a finite field with q elements and $\mathbb{K}$ is a subfield of $\mathbb{F}$, then the polynomial $x^q - x \in \mathbb{K}[x]$ factors in $F[x]$ as

  $$x^q - x = \prod_{a \in \mathbb{F}} (x - a)$$

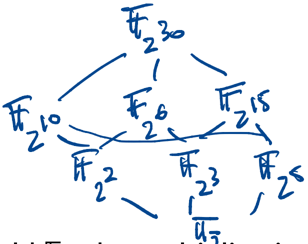
  and F is a splitting field of $x^q - x$ over $\mathbb{K}$.
  Example: $x^9 - x \in \mathbb{F}_3$

Finite Fields

- **Subfield Criterion.** Let $\mathbb{F}_q$ be the finite field with $q = p^t$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of t. Conversely, if m is a positive divisor of t, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Example: Diagram of $\mathbb{F}_{2^{30}}$

$30 = 2 \cdot 3 \cdot 5$

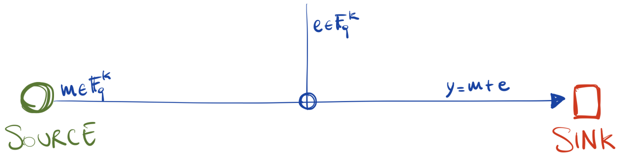


- For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic. A generator of $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$.

Example $\mathbb{F}_9^*$ $\quad \mathbb{F}_3[\alpha]/(\alpha^2+1) \qquad \langle \alpha + 1 \rangle = \mathbb{F}_9^*$

- Facts about Finite Fields.
- From Channels to Networks
- One Source Networks
  - The Unicast Network
  - The Multicast Network

Noisy-Channel Coding Theorem - Shannon 1948)



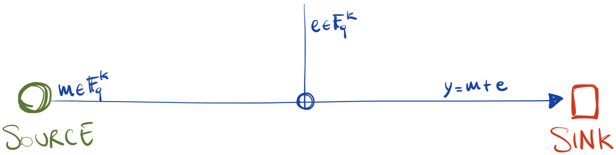
Over $\mathbb{F}_2$:

$m = 1$

$e = 1$

$y = 0$

Noisy-Channel Coding Theorem - Shannon 1948)



Over $\mathbb{F}_2$:

$m = 1$

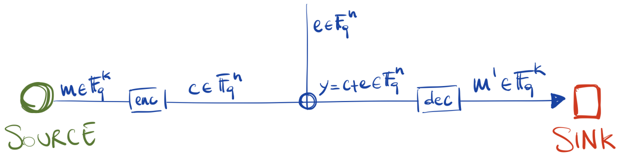
$e = 1$

$y = 0$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

“In communication theory, any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

Noisy-Channel Coding Theorem - Shannon 1948)

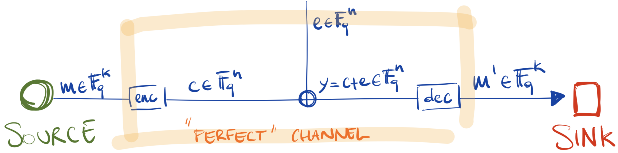


Over $\mathbb{F}_2$:
$m = 1$
$c = (111)$
$e = (010)$
$y = (101)$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

"In communication theory, any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

Noisy-Channel Coding Theorem - Shannon 1948)



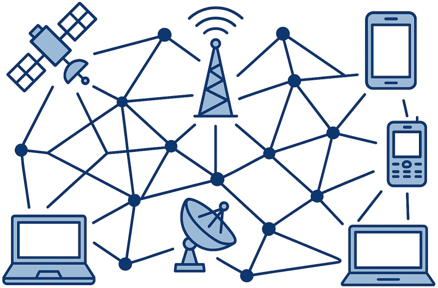
Over $\mathbb{F}_2$:
$m = 1$
$c = (111)$
$e = (010)$
$y = (101)$
$m' = 1$

Theorem (Noisy-Channel Coding Theorem - Shannon - 1948)

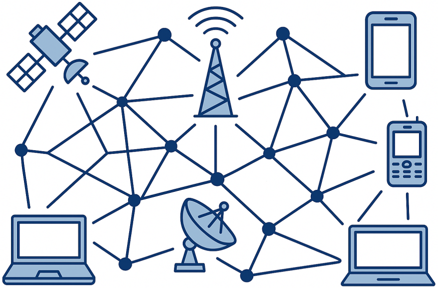
"In communication theory, any channel, however affected by noise, possesses a specific channel capacity - a rate of conveying information that can never be exceeded without error, but that can, in principle, always be attained with an arbitrarily small probability of error."

Turbo codes (LTE networks), Polar & LDPC codes (5G networks)

Example of (Communication) Networks



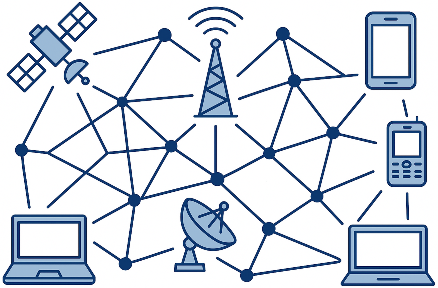
Example of (Communication) Networks



Question

Is routing the **best** communication strategy on a network?

Example of (Communication) Networks

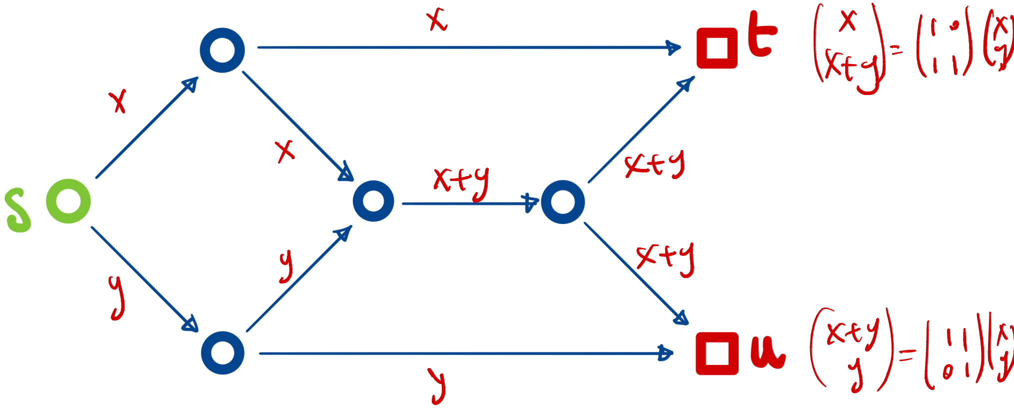


Question

Is routing the **best** communication strategy on a network?

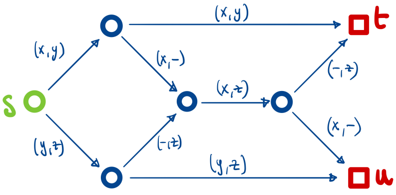
Notes adapted from [1, 2].

The Butterfly Network

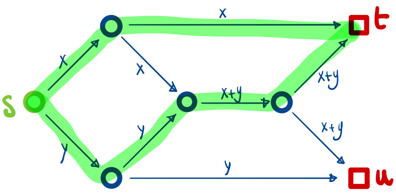


Made with Goodnotes

The Butterfly Network



(a) Rounting



(b) Network Coding

Rates (ρ):

Routing: $\frac{3}{2} = 1{,}5$

Network coding: $\frac{2}{1} = 2$

Can we do better?

Network representation

Disclaimer: We will consider the alphabet to be $\mathbb{F}_q$.

A **network** is a 4-tuple $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{T})$ where:

- ✓ $G = (\mathcal{V}, \mathcal{E})$ is a a finite directed acyclic multigraph with $\mathcal{V}$ is the set of vertices and $\mathcal{E}$ is the multiset of directed edges;
- ✓ $\mathcal{S} \subset \mathcal{V}$ is the set of sources;
- ✓ $\mathcal{T} \subset \mathcal{V}$ is the set of sinks (receivers, terminals);

Network representation

Disclaimer: We will consider the alphabet to be $\mathbb{F}_q$.

A **network** is a 4-tuple $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{T})$ where:

- ✓ $G = (\mathcal{V}, \mathcal{E})$ is a a finite directed acyclic multigraph with $\mathcal{V}$ is the set of vertices and $\mathcal{E}$ is the multiset of directed edges;
- ✓ $\mathcal{S} \subset \mathcal{V}$ is the set of sources;
- ✓ $\mathcal{T} \subset \mathcal{V}$ is the set of sinks (receivers, terminals);
- ✓ $\mathcal{S} \cap \mathcal{T} = \emptyset$;
- ✓ $I(s) = \emptyset$ for $s \in \mathcal{S}$;
- ✓ $O(t) = \emptyset$ for $t \in \mathcal{T}$;

Network representation

Disclaimer: We will consider the alphabet to be $\mathbb{F}_q$.

A **network** is a 4-tuple $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{T})$ where:

- ✓ $G = (\mathcal{V}, \mathcal{E})$ is a a finite directed acyclic multigraph with $\mathcal{V}$ is the set of vertices and $\mathcal{E}$ is the multiset of directed edges;
- ✓ $\mathcal{S} \subset \mathcal{V}$ is the set of sources;
- ✓ $\mathcal{T} \subset \mathcal{V}$ is the set of sinks (receivers, terminals);
- ✓ $\mathcal{S} \cap \mathcal{T} = \emptyset$;
- ✓ $I(s) = \emptyset$ for $s \in \mathcal{S}$;
- ✓ $O(t) = \emptyset$ for $t \in \mathcal{T}$;
- ✓ For every $v \in \mathcal{V} \setminus (\mathcal{S} \cup \mathcal{T})$ there esist a path from a source $s \in \mathcal{S}$ and a sink $t \in \mathcal{T}$ going through v.

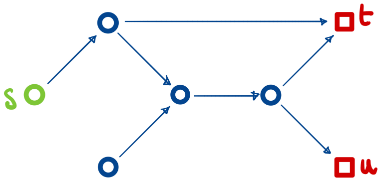
Network representation

Disclaimer: We will consider the alphabet to be $\mathbb{F}_q$.

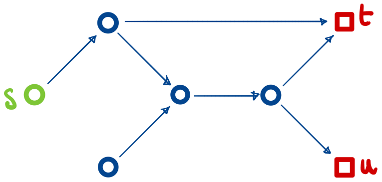
A **network** is a 4-tuple $\mathcal{N} = (\mathcal{V}, \mathcal{E}, \mathcal{S}, \mathcal{T})$ where:

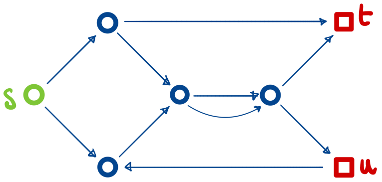
- ✓ $G = (\mathcal{V}, \mathcal{E})$ is a a finite directed acyclic multigraph with $\mathcal{V}$ is the set of vertices and $\mathcal{E}$ is the multiset of directed edges;
- ✓ $\mathcal{S} \subset \mathcal{V}$ is the set of sources;
- ✓ $\mathcal{T} \subset \mathcal{V}$ is the set of sinks (receivers, terminals);
- ✓ $\mathcal{S} \cap \mathcal{T} = \emptyset$;
- ✓ $I(s) = \emptyset$ for $s \in \mathcal{S}$;
- ✓ $O(t) = \emptyset$ for $t \in \mathcal{T}$;
- ✓ For every $v \in \mathcal{V} \setminus (\mathcal{S} \cup \mathcal{T})$ there esist a path from a source $s \in \mathcal{S}$ and a sink $t \in \mathcal{T}$ going through v.
- ✓ $(u, v) \in \mathcal{E}$ is a perfect unit capacity channel from u to v.

Examples of non networks



Examples of non networks





Examples of non networks