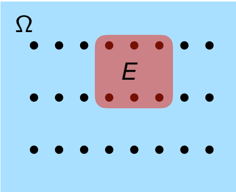
Discrete Probability (Reminder)

FINITE SAMPLE SPACE Ω, EQUALLY LIKELY OUTCOMES



SAMPLE SPACE

The **sample space** Ω is the set of all possible outcomes.

EVENT

An **event** E is a subset of Ω.

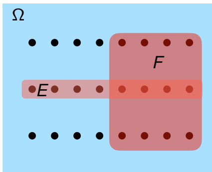
CONDITIONAL PROBABILITY

$p(E \mid F)$ is the probability of E occurring, given that F has occurred.

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)} = \frac{|E|}{|\Omega|} \text{ (here)}$$

INDEPENDENT EVENTS

E and F are independent $\Leftrightarrow$ $p(E \mid F) = p(E)$.



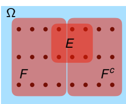
FINITE SAMPLE SPACE Ω, ARBITRARY DISTRIBUTION $p(\omega)$

PROBABILITY DISTRIBUTION

$p(\omega)$ gives for each $\omega \in \Omega$ a probability of occurring (such as $\sum_{\omega \in \Omega} p(\omega) = 1$).

PROBABILITY OF EVENTS

Then, the probability for events is given by $p(E) = \sum_{\omega \in E} p(\omega)$.



LAW OF TOTAL PROBABILITY (DIVIDE AND CONQUER)

$$p(E) = p(E \mid F) \cdot p(F) + p(E \mid \bar{F}) \cdot p(\bar{F})$$

This formula also holds for more cases.

BAYES' RULE

$$p(E \mid F) = \frac{p(F \mid E) \cdot p(E)}{p(F)}$$

RANDOM VARIABLES

A **random variable** X is a function $\Omega \to \mathbb{R}$.

PROBABILITY DISTRIBUTION

$p_X(x)$ gives for each value x its probability.

$p_X(x) = \sum_{\omega \in E} p(\omega)$

From a multi-variable distribution $p_{X,Y}(x, y)$, it is possible to extract a **marginal distribution** with respect to one variable (e.g. p_X or p_Y).

EXPECTED VALUE

$$\mathbb{E}[X] = \sum_{\omega} X(\omega)p(\omega) = \sum_x x \cdot p_X(x)$$

The expected value is **linear**.

Product: $\mathbb{E}[X \cdot Y] = \mathbb{E}[X] \cdot \mathbb{E}[Y]$ holds only for independent variables.

INDEPENDENCE

X, Y and Z are **mutually independent** $\Leftrightarrow p_{X,Y,Z}(x, y, z) = p_X(x)p_Y(y)p_Z(z)$

Also: definitions involving $p(E \mid F) = p(E)$… for instance $p_{Y|X}(y, x) = p_Y(y)$ for all x

CONDITIONAL DISTRIBUTION

$$p_{Y|X}(y \mid x) = \frac{p_{X,Y}(x, y)}{p_X(x)} \text{ (where } p_X(x) \neq 0)$$

Sources and Entropy

Entropy

HARTLEY'S MEASURE

To measure the quantity of transmitted information using n symbols from the alphabet $\mathscr{A}$, Hartley counts all different possibilities: $H_{\text{Hartley}} = n \cdot \log|\mathscr{A}|$.

SHANNON'S ENTROPY

The definition from Shannon takes into account the probabilities of each symbol s:

$$H_b(S) = -\sum_{s \in \mathscr{A}} p_S(s) \cdot \log_b p_S(s) \quad = \mathbb{E}[-\log p_S(s)]$$

Symbols with $p_S(s) = 0$ are ignored, using the convention $0 \cdot \log_b 0 = 0$.

It only depends on the distribution!

BASE

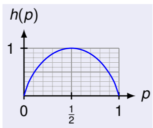
b is the **base**, with $b = 2$ by default (→ **bits**).

LINK WITH HARTLEY'S MEASURE

$H_{\text{Shannon}} = H_{\text{Hartley}}$
⇔ uniformly distributed alphabet.

BINARY ENTROPY FUNCTION

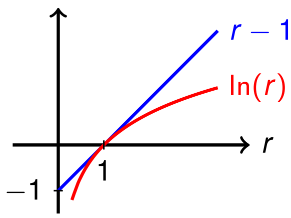
For two symbols of probability p and $1 - p$.



INFORMATION-THEORY (IT) INEQUALITY

$$\log_b r \leq (r - 1) \cdot \log_b(e) \quad \forall r > 0$$

with equality only if $r = 1$.



ENTROPY BOUNDS

For any discrete random variable $S \in \mathscr{A}$, the entropy is within:

$$0 \leq H_b(S) \leq \log_b|\mathscr{A}|$$

The case $0 = H_b(S)$ only happens when S is constant.

The case $H_b(S) = \log_b|\mathscr{A}|$ only happens when S is uniformly distributed.

ENTROPY OF MULTIPLE RANDOM VARIABLES

$$H(X, Y) = \mathbb{E}\Big[-\log p_{X,Y}(X, Y)\Big] = -\sum_{(x,y) \in \mathscr{X} \times \mathscr{Y}} p_{X,Y}(x, y) \cdot \log p_{X,Y}(x, y)$$

INEQUALITY

$H(S_1, \cdots, S_n) \leq H(S_1) + + \cdots + H(S_n)$, with equality for independent Ss.

Source Coding

DEFINITIONS

An encoder encodes a **source** (consisting of **symbols** s_i in an **input alphabet** $\mathscr{A}$)

to a **codebook** $\mathscr{C}$ (consisting of one or more symbols in the **output alphabet** $\mathscr{D}$)

using an **encoding map** $\mathscr{A}^k \to \mathscr{C}$ (injective).

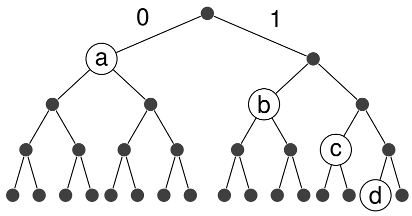
A code is **prefix-free** (= **instantaneous**) if no codeword starts with another codeword.

A code is **uniquely decodable** if every concatenation of codewords has a unique parsing.

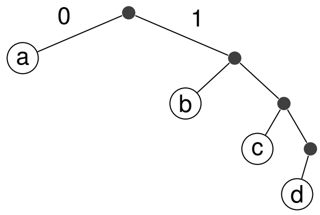
Prefix/suffix-free codes and are always uniquely decodable.

CODE TREES

CODE TREE



DECODING TREE



(Only branches that form a codeword)

KRAFT-MCMILLAN INEQUALITY

① NECESSARY CONDITION FOR THE CODE TO BE UNIQUELY DECODABLE

If a D-ary code $\mathscr{C}$ of lengths ℓ_i is uniquely decodable, then

$$\underbrace{D^{-\ell_1} + \cdots + D^{-\ell_M}}_{\text{Kraft's sum } \mathrm{K}(\mathscr{C})} \leq 1$$

② EXISTENCE OF A UNIQUELY DECODABLE CODE WITH THESE LENGTHS

If $K(\mathscr{C}) \leq 1$, then there exists a prefix-free code $\mathscr{C}$ with lengths ℓ_i.

AVERAGE CODEWORD LENGTH

For an encoding map Γ, the **average codeword length** in **code symbols** (e.g. bits for $D = 2$) is:

$$L(S, \Gamma) \stackrel{\text{def}}{=} \sum_{s \in \mathscr{A}} p_S(s) \cdot \ell\big(\Gamma(s)\big)$$

BOUNDS

$$H_D(S) \leq L(S, \Gamma)$$

The **entropy** of the source is the **ideal case.**

it is **reachable** only when all symbols s have probabilities of the form $p_S(s) = D^{-\ell(\Gamma(s))}$

(diadic / D-adic distribution).

SHANNON-FANO CODES

A **Shannon-Fano code** is a code where the **lengths** of the codewords are:

$$\ell_i = \lceil -\log p_i \rceil$$

Its average codeword length **fulfils**:

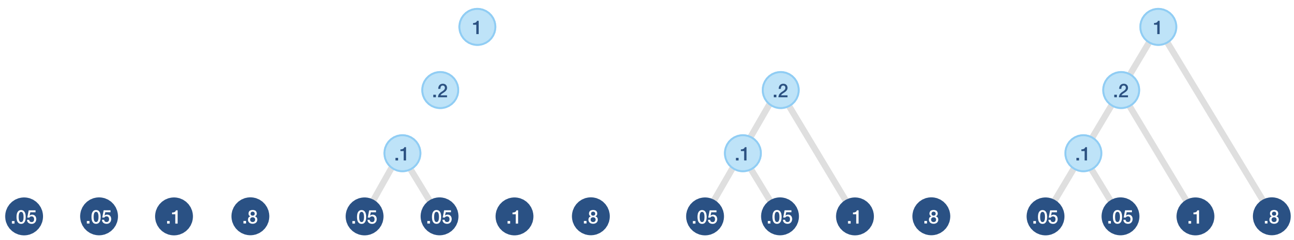
$$H_D(S) \leq L(S, \Gamma_{SF}) < H_D(S) + 1$$

The average codeword length is not too bad, but **not always optimal**!

An individual codeword can be much longer than needed.

HUFFMAN'S CONSTRUCTION

A **Huffman code** is constructed by starting from the terminal leaves, and connecting the two lowest probabilities. The new node has the sum of the probabilities of the children nodes.



This code is always prefix-free and **optimal** (L is as short as it can be).

PATH LENGTH LEMMA

If the q_i are the **probabilities** of the **intermediate nodes**,

$$L(S, \Gamma) = \sum_i q_i$$

✨ We can compute easily $L(S, \Gamma)$ using this property.

Conditional Entropy

Every probability distribution has an **entropy** associated to it.

Notation: probabilities

$p_X(\cdot) = p_X \to H(X)$

$p_{X|Y}(\cdot\,|\,y) = p_{X|Y=y} \to H(X\,|\,Y=y)$

CONDITIONAL ENTROPY OF X GIVEN $Y = y$

$$H(X\,|\,Y=y) \overset{\text{def}}{=} -\sum_{x\in\mathcal{X}} p_{X|Y}(x\,|\,y)\,\log p_{X|Y}(x\,|\,y)$$

CONDITIONAL ENTROPY OF X GIVEN Y

$$H(X\,|\,Y) = \sum_{y\in\mathcal{Y}} H(X\,|\,Y=y)\cdot p_Y(y)$$

for computations

$$= \mathbb{E}\big[-\log p_{X|Y}(X\,|\,Y)\big]$$

for relationships

$$= -\sum_{(x,\,y)\in\mathcal{X}\times\mathcal{Y}} p_{X|Y}(x\,|\,y)\cdot\log p_{X|Y}(x\,|\,y)$$

⚠️ **Conditioning reduces entropy**: $H(X\,|\,Y) \le H(X)$ (with equality for independent variables).

CHAIN RULE FOR ENTROPIES

✨ Gives entropy for multiple variables. Can be used to compute $H(X\,|\,Y)$.

$$H(S_1, S_2, \cdots S_n) = H(S_1) + H(S_2\,|\,S_1) + H(S_3\,|\,S_1, S_2) + \cdots + H(S_n\,|\,S_1, \cdots, S_{n-1})$$

(The order does not matter).

Individual variables have **more entropy**: $H(S_1, \cdots, S_n) \le H(S_1) + \cdots + H(S_n)$.

The chain rule can be used to deduce $H(X\,|\,Y)$ from $H(X, Y)$ and $H(Y)$.

Sources

DEFINITIONS

A **source** produces $1/n/\infty$ **symbols** ($\mathcal{S}$: infinite source).

ENTROPY OF A SYMBOL (D'UN SYMBOLE)

$$H(\mathcal{S}) = \lim_{n\to\infty} H(S_n)$$

ENTROPY RATE (ENTROPIE PAR SYMBOLE)

$$H^*(\mathcal{S}) = \lim_{n\to\infty} H(S_n \mid S_1, \cdots, S_{n-1})$$

SOURCE TYPES

- **Regular**: both $H(\mathcal{S})$ and $H^*(\mathcal{S})$ exist.
- **Stationary**: distribution unaffected by indice shifts.
  All stationary sources are **regular**.
  Also, $H(\mathcal{S}) \geq H^*(\mathcal{S})$ (equality if the symbols are independent).
- A stochastic process is **ergodic** if a typical realisation reveals its statistical properties.

EXAMPLES

- **Coin-flip** Probability of each result at $\frac{1}{2}$ (independent) ✅ R ✅ S ✅ E
- **Sunny-rainy** Probability of changing (first symbol uniformly distributed) ✅ R ✅ S ✅ E
- **Green-blue** Always the same (first symbol uniformly distributed) ✅ R ✅ S ❌ E
- **Weekly-coin-flip** Probability depending on the day: $p_{i+7k} = \frac{1}{i}\ \forall i \in [\![1,7]\!]$ ❌ R ❌ S ✅ E

SOURCE CODING THEOREM

Symbols emitted by the **stationary** source $\mathcal{S}$ can be encoded with $L(\mathscr{C}, \Gamma)$ **arbitrarily close** to $H_D^*(\mathcal{S})$ (which is the minimum).

For IID sources, $H_D(\mathcal{S}) = H_D^*(\mathcal{S})$.

CÉSARO MEANS THEOREM

✨ Used in the proof of the source coding theorem.

If a_n is a sequence with $a_n \xrightarrow{n\to\infty} \ell$, then the sequence $c_n = \dfrac{a_1 + \cdots + a_n}{n} \xrightarrow{n\to\infty} \ell$.

ELIAS CODE

✨ Prefix-free code to encode integers of any length.

ELIAS CODE 1

$c_1(n)$ = [0 × (l(n) – 1)] + [binary-encoded n]

ELIAS CODE 2

$c_2(n)$ = c_1(l(n)) + [binary-encoded n]

Length $= 2\lfloor \log_2(\lfloor \log_2 n \rfloor + 1) \rfloor + 1 + \lfloor \log_2 n \rfloor \approx \log_2 n + 1$

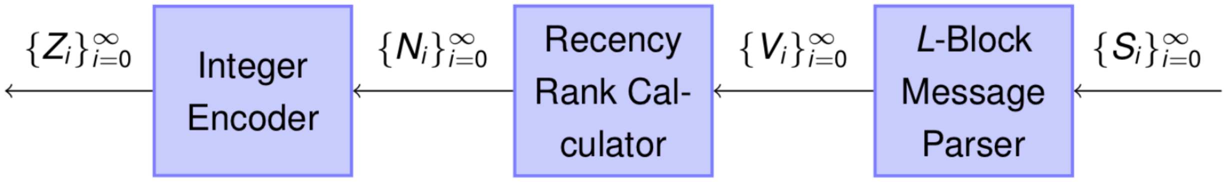
UNIVERSAL ENCODING SCHEME

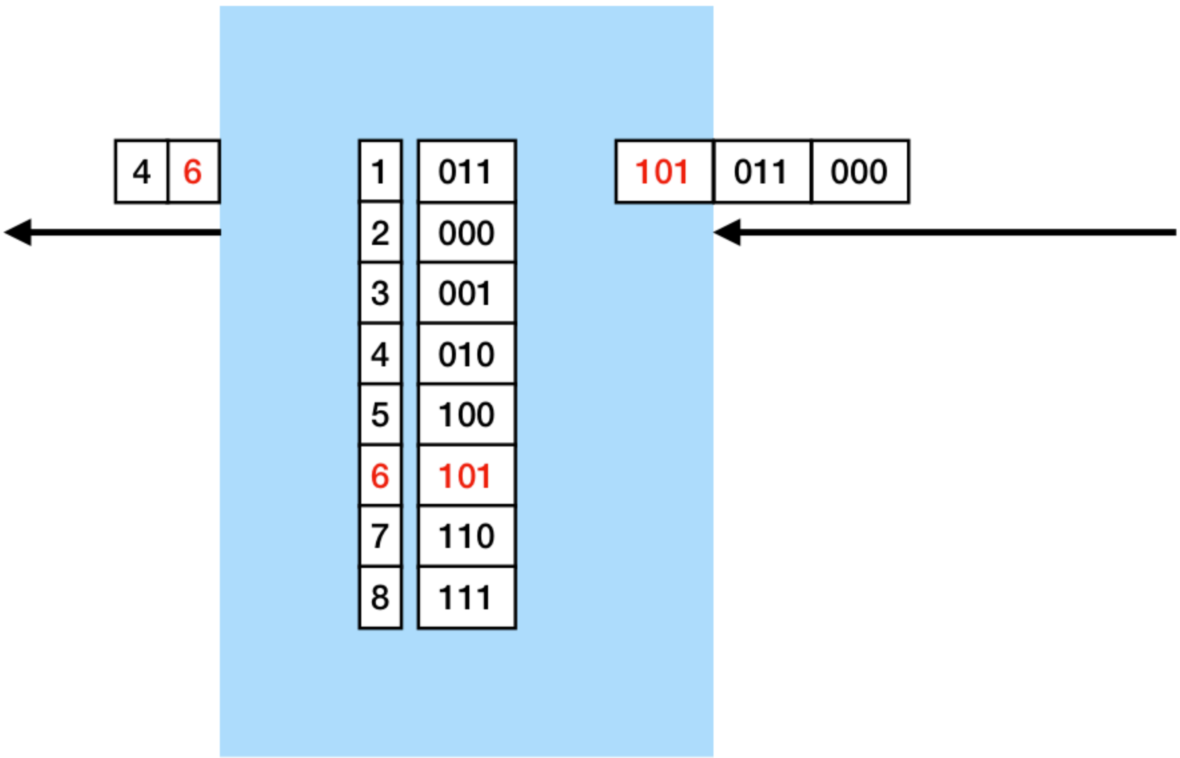
KAC'S LEMMA

If S_i is an ergodic process and V_i a group of L symbols, $\mathbb{E}[J \mid V_0 = v] = \frac{1}{p_V(v)}$.

In other words, an event with chance $\frac{1}{3}$ will occur approximately each 3 slots.

ELIAS-WILLEMS UNIVERSAL SOURCE CODING SCHEME





Cryptography

Introduction

Cryptography is used to send messages over an insecure channel to ensure their privacy and authenticity. The **plain text** is converted to a **cipher text** which is sent.

PRIMITIVE METHODS

MONOALPHABETIC CIPHER

Attribute to each symbol another symbol (e.g. **Caesar's cipher**: rotate each symbol).

POLYALPHABETIC CIPHER

Use multiple substitution tables (e.g. **Vigenère cipher**: alternate the amount of rotation).

ONE-TIME PAD

Bitwise XOR operation ($\oplus$) with the key.

PERFECTSECRECY

DEFINITION

A system is **perfectly secure** if the plaintext and the cryptogram are statistically independant.

It is secure to a cipher text-only attack.

Example: **One-time pad** (XOR operator with a key used only once)

PRECONDITION

$$\text{perfect secrecy (and decodability)} \Rightarrow H(K) \geq H(T)$$

MODERN CRYPTOGRAPHY

We assume that the security is based on the secret key, not on the method used.

It is based on computational security, not on perfect secrecy.

Key Exchange

DIFFIE-HELLMAN SYMMETRIC-KEY EXCHANGE

ONE-WAY FUNCTION

Function **quick** to do **in one direction**, but really **hard to reverse**.

DISCRETE LOGARITHM

Each prime number p has a **generator** g such that

$$\{g \bmod p,\ g^2 \bmod p,\ \ldots,\ g^{p-1} \bmod p\} = \{1,\ 2,\ \ldots,\ p-1\}.$$

$g^x = y$: easy to compute **(discrete exponentiation)**, but difficult to find x **(discrete logarithm)**.

DIFFIE-HELLMAN SYMMETRIC-KEY EXCHANGE

Shared: large prime p and a generator g of it

Alice's secret: x		Bob's secret: y
Alice sends g^x	→	Bob computes $(g^x)^y = g^{xy}$
Alice computes $(g^y)^x = g^{xy}$	←	Bob sends g^y

Both have the symmetric key g^{xy}

ELGAMAL ENCRYPTION SCHEME

TRAPDOOR ONE-WAY FUNCTION

A **trapdoor one-way function** is easy to reverse iff you have the **trapdoor information**.

E.g. Elgamal's trapdoor function: $t \mapsto g^{xy}t$ with known g^y, hard to reverse without x.

ELGAMAL ENCRYPTION SCHEME

Shared: large prime p and a generator g of it

Alice's secret: x		Bob's secret: y
Alice sends g^x	→	Bob computes $(g^x)^y = g^{xy}$
Alice computes $(g^y)^x = g^{xy}$	←	Bob sends g^y
Alice sends $g^{xy}t$ (t: message)	→	Bob computes t

Both have the symmetric key g^{xy}

Number Theory: Operations in $\mathbb{Z}$

EUCLIDIAN DIVISION

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exists unique q and r, $0 \leq r < d$ such that:

$$a = bq + r \quad \begin{cases} a & \text{: dividend} \\ b & \text{: divisor} \in \mathbb{N} \\ q = a \operatorname{div} b & \text{: dividend} \\ r = a \bmod b & \text{: remainder } (0 \leq r < |b|) \end{cases}$$

SIGN OF % IN PROGRAMMING LANGUAGES

In C/C++/Java: same sign as a. In Python: same sign as b, taking into account the shift.

a	b	a % b in `C/C++/Java`	a % b in `Python`	r
8	3	2	2	2
−8	3	−2	1	1
8	−3	2	−1	2
−8	−3	−2	−2	1

CONGRUENCE

$$\underbrace{a \equiv b \pmod m}_{\text{congruence modulus } m} \iff a \bmod m = b \bmod m \iff m \mid \underbrace{(a-b)}_{\Delta n}$$

SUM/PRODUCT OF CONGRUENCES

$$\begin{cases} a + b \equiv a' + b' \pmod m & + \text{ congruent} \\ a \cdot b \equiv a' \cdot b' \pmod m & \times \text{ congruent} \\ a^n \equiv (a')^n \pmod m & + \text{ same} \end{cases}$$

Numbers can be **replaced by a congruent**: $\begin{cases} a + b \bmod m = (a \bmod m) + (b \bmod m) \bmod m \\ a \cdot b \bmod m = (a \bmod m) \cdot (b \bmod m) \bmod m \end{cases}$

EQUIVALENCE RELATION

Congruence is an equivalence relation (reflexive, transitive, symmetric).

USEFUL RULES IN BASE 10

Divisible by two ⇔ last digit divisible by two.

Divisible by 9 ⇔ sum of digits divisible by 9.

MOD 97 – 10 PROCEDURE

✨ Allows to know whether two digits were swapped in a number.

GENERATE THE CHECK DIGITS

append $c = 98 - (100n \bmod 97)$

VERIFY

$N \bmod 97 = 1$

PRIME NUMBERS

PRIME NUMBER

A number $n > 1$ is **prime** ($\neq$ **composite**) if its only positive factors are 1 and n.

FUNDAMENTAL THEOREM OF ARITHMETIC

Every $n > 1$ can be written as a **unique** (except order) **product of primes**.

Prime factorisation can be a one-way function with large prime numbers.

GCD

$n = \gcd(a, b)$: greatest n such that $n \mid a$ and $n \mid b$ = min. powers of a and b primes.

RELATIVELY PRIME

a and b are **relatively prime/coprime** ⇔ $\gcd(a, b) = 1$. A prime p is coprime to every $a < p$.

DIVISION RESULTS

$ab \mid c \Rightarrow a \mid c$ and $b \mid c$

$a \mid c$ and $b \mid c \Rightarrow ab \mid c$ if a and b are relatively prime.

Modular arithmetic $\mathbb{Z}/m\mathbb{Z}$

CONGRUENCE CLASS $[a]_m$

$$[a]_m = \{i \in \mathbb{Z} \mid i \equiv a \pmod{m}\} \quad (m \text{ is the modulus})$$

Comparison: $[a]_m = [b]_m \Leftrightarrow a \equiv b \pmod{m}$.

$[r]_m$ is the (unique) **reduced form** if $r = r \bmod m$.

SET OF CONGRUENCE CLASSES

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, \ \ldots, \ [m-1]_m\}$$

OPERATIONS (DEFINITIONS)

ADDITION

$$[a]_m + [b]_m = [a+b]_m$$

MULTIPLICATION

$$[a]_m[b]_m = [a \cdot b]_m, \quad k[a]_m = \underbrace{[a]_m + \cdots + [a]_m}_{k \text{ times}}$$

EXPONENTIATION

$$([a]_m)^k = \underbrace{[a]_m \cdot \ldots \cdot [a]_m}_{k \text{ times}} \qquad ([a]_m)^0 = [1]_m \qquad ([a]_m)^{-k} = ([a]_m^{-1})^k$$

ABELIAN GROUPS AND COMMUTATIVE RINGS

Addition + has the following properties $\forall a, b, c \in \mathbb{Z}$:

- **Associativity** $([a]_m + [b]_m) + [c]_m = [a]_m + ([b]_m + [c]_m)$
- **Commutativity** $[a]_m + [b]_m = [b]_m + [a]_m$
- **Additive identity** $\exists [0]_m : [a]_m + [0]_m = [a]_m$
- **Additive inverse** $\exists -[a]_m : [a]_m + (-[a]_m) = [0]_m$

Abelian group

Multiplication ·/× has the following properties:

- **Associativity** $([a]_m \cdot [b]_m) \cdot [c]_m = [a]_m \cdot ([b]_m \cdot [c]_m)$
- **Commutativity** $[a]_m \cdot [b]_m = [b]_m \cdot [a]_m$
- **Multiplicative identity** $\exists [1]_m : [a]_m \cdot [1]_m = [a]_m$

The operations are distributive:

- **Distributivity** $[a]_m([b]_m + [c]_m) = [a]_m[b]_m + [a]_m[c]_m$

Commutative ring

MULTIPLICATIVE INVERSES

An element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ has a **inverse** $[a]_m^{-1}$ if $[a]_m \cdot [a]_m^{-1} = [1]_m$.

When it exists, it is **unique.**

EXISTENCE

$$[a]_m \text{ has an inverse } \Leftrightarrow \gcd(a,\ m) = 1$$

When m **is a prime number**, the inverses **always exist** for all $[a]_m \neq [0]_m$.

SOLVING EQUATIONS WITH INVERSE

$$[a]_m \text{ has an inverse} \Leftrightarrow x[a]_m = [b]_m \text{ has a unique solution for one/every } [b]_m$$

If $[a]_m$ has **no inverse**, there are **no solutions** for some $[b]_m$ and **multiple solutions** for other.

EUCLIDIAN ALGORITHM

USEFUL FACTS ABOUT gcd

- The sign does not matter. $\gcd(a, b) = \gcd(\pm a,\ \pm b)$
- Remove multiple of the other numbers. $\gcd(a, b) = \gcd(a - qb,\ b) \quad \forall q \in \mathbb{Z}$

EUCLIDIAN ALGORITHM

To find $\gcd(a,\ b)$, apply $\gcd(a,\ b) = \gcd(b,\ r) = \cdots$ until $\gcd(x,\ 0) = x$ is found.

BÉZOUT'S IDENTITY

$$\forall (a,\ b) \in \mathbb{Z}^2,\ \exists (u,\ v) \in \mathbb{Z}^2 \text{ such that } \gcd(a, b) = au + bv$$

EXTENDED EUCLIDIAN ALGORITHM

✨ To find $(u,\ v)$.

① Euclid

② $(u,\ v)$

$\gcd(a, b)$	$a = bq + r$	q	$u = \tilde{v}$	$v = \tilde{u} - q\tilde{v}$
$\gcd(122,\ 22)$	$122 = 22 \cdot 5 + 12$	**5**	2	−1 − 10
$\gcd(22,\ 12)$	$22 = 12 \cdot 1 + 10$	**1**	−1	1 − (−1)
$\gcd(12,\ 10)$	$12 = 10 \cdot 1 + 2$	**1**	1	0 − 1
$\gcd(10,\ 2)$	$10 = 2 \cdot 5 + 0$	**5**	0	1
$\gcd(2,\ 0) = 2$	–	–	1	0

FIND MULTIPLICATIVE INVERSES

Apply the extended Euclidian algorithm.

Commutative Groups

DEFINITION

A **commutative group** (*Abelian group*) $(G, \star)$ is the set G and the binary operation $\star : G^2 \to G$ where the **group operation** $\star$ has the following properties $\forall a, b, c \in G$:

- **Closure** $a \star b \in G$
- **Associativity** $(a \star b) \star c = a \star (b \star c)$
- **Commutativity** $a \star b = b \star a$
- **Identity element** $\exists \mathbf{1} \in G$ such that $\forall a \in G, a \star e = \mathbf{1}$
- **Inverse element** $\forall a \in G, \exists a^{-1} \in G$ such that $a \star a^{-1} = \mathbf{1}$.

SET OF ELEMENTS WITH MULTIPLICATIVE INVERSE

$$\mathbb{Z}/m\mathbb{Z}^* = \left\{ a \in \mathbb{Z}/m\mathbb{Z} \;\middle|\; a \text{ has a multiplicative inverse} \right\}$$

COMMUTATIVE GROUP

$\mathbb{Z}/m\mathbb{Z}$ is not a commutative group (because $[0]_m$ has no inverse), but $\mathbb{Z}/m\mathbb{Z}^*$ is.

EULER'S TOTIENT FUNCTION

$$\phi(n) = \#\text{ of numbers in } \{1, \ldots, n\} \text{ that are relatively prime to } n.$$

If p, q are prime, $\begin{cases} \phi(p) = p - 1 \\ \phi(p^k) = p^k - p^{k-1} \end{cases}$ Gives the size of the comm. group: $\phi(n) = \left|\mathbb{Z}/n\mathbb{Z}^*\right|$

CARTESIAN PRODUCTS

If $(G_1, \star_1)$ and $(G_2, \star_2)$ are commutative groups, then the **product group** $(G, \star)$ is a commutative group as well.

(with $G = G_1 \times G_2$ and the **product operation** $\star$ is $(a, \alpha) \star (b, \beta) = (a \star_1 b, \alpha \star_2 \beta)$).

ISOMORPHISMS

An **isomorphism** from $(G, \star)$ to $(H, \oplus)$ (sets + binary operations) is a **bijection** ψ such that:

$$\forall a, b \in G, \quad \psi(a \star b) = \psi(a) \oplus \psi(b)$$

$(G, \star)$ and $(H, \oplus)$ are isomorphic if there exists an **isomorphism** between them.

COMMUTATIVE GROUPS

If $(G, \star)$ is a commutative group isomorphic to $(H, \oplus)$, then $(H, \oplus)$ is a commutative group.

SHARED IDENTITY ELEMENT

If e is the identity element of $(G, \star)$, then $\psi(e)$ is the identity element of $(H, \oplus)$.

INVERSE OF EACH OTHER

If a and b are the inverse of each other in $(G, \star)$, then $\psi(a)$ and $\psi(b)$ are as well in $(H, \oplus)$.

ORDERS

Let $(G, \star)$ be a finite commutative group with identity element e.

The **order** k is the smallest $k \in \mathbb{N}^*$ such that $\underbrace{a \star \cdots \star a}_{k \text{ terms}} = e$.

ORDER AND ISOMORPHISMS

The order of a and $\psi(a)$ is the same.

Two commutative groups are **isomophic** ⇔ they have the **same set of orders**.

✨ Allows to know **whether two commutative groups are isomorphic**.

ORDER'S IFF

$$a^n = e \quad \Leftrightarrow \quad n = q \cdot k, \text{ where } k \text{ is the order. } (q \in \mathbb{N}^*)$$

✨ Allows to **solve equations** similar to $a^n = e$.

LAGRANGE THEOREM: THE ORDER DIVIDES THE NUMBER OF ELEMENTS

Let $(G, \star)$ be a finite commutative group of n elements. Then $\forall a \in G$, k_a divides n.

EULER THEOREM: EXP. WITH TOTIENT

$$\forall a \in \mathbb{Z}/m\mathbb{Z}^*, \quad a^{\varphi(m)} = [1]_m$$

FERMAT'S THEOREM: EXP. WITH PRIME

$$\forall a \in \mathbb{Z}/p\mathbb{Z} \ (p \text{ prime}), \ a^p = a$$

CHINESE REMAINDERS THEOREM

✨ Allows to know **whether** $\mathbb{Z}/m_1m_2\mathbb{Z}$ **and** $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ **are isomorphic**.

$$n \text{ and } m \text{ relatively prime} \Leftrightarrow \begin{array}{c} \psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} \mapsto ([a]_m, [a]_n) \end{array} \text{ is an isomorphism (w.r. to } + \text{ and } \cdot)$$

INVERSE MAP

$$1 = \underbrace{m \cdot u}_{b} + \underbrace{n \cdot v}_{a} \quad \rightsquigarrow \quad \begin{array}{c} \psi^{-1} : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z} \\ ([x]_m, [y]_n) \mapsto [ax + by]_{mn} \end{array}$$

SOLVING EQUATIONS

✨ We can often try to reduce a problem to a product group: $x^3 = [7]_{12} \Leftrightarrow ([x_1]_3, [x_2]_4)^3 = ([1]_3, [3]_4)$.

COROLLARY: EULER (TOTIENT OF PRODUCT)

$$\gcd(n, m) = 1 \ \Rightarrow \ \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

FERMAT + CRT (NEUTRALIZING EXPONENTS)

For p and q **distinct primes**, and k a **multiple** of $(p-1)$ and $(q-1)$.

$$\left([a]_{pq}\right)^{qk+1} = [a]_{pq} \quad \forall q \in \mathbb{Z}$$

RSA Cryptosystem

WORKING WITH RSA

VALUES

- **Public key**: $K = pq$ (with p and q large primes)
- **Private key**: $k = \text{lcm}(p-1, q-1)$ (or any multiple of $p-1$ and $q-1$).
- **Encryption exponent**: e known by everyone, relatively prime with k (e.g. 655357, prime)
- **Decryption exponent**: $d = [e]_k^{-1}$

ENCRYPTION

$$[C]_K = ([P]_K)^e$$

DECRYPTION

$$[P]_K = ([C]_K)^d$$

Complexity: $2 \log_2 K$ multiplications.

Cryptography Applications & Standards

- **Hash function** Many-to-one function (to the same number of bits), hard to reverse.
  SHA1, SHA2, SHA3…
- **Digital signature** Share $f^{-1}\big(h(t)\big)$, ($h(t)$: hash of the content, f: trapdoor one-way function).
  DSA, ECDSA…
- **Trusted agency** Sign [key + owner] with a trusted key.
- **Symmetric-key cryptography:** *DES (insecure), AES…*
- **Public-key cryptography**: *RSA…*

📝 RSA is more capable but uses more time/memory than some usage-specific standards.

Cyclic Groups

Let $(G, \star)$ be a finite commutative group.

$H \subset G = \{e, g, g^2, \cdots, g^{n-1}\}$ is a **cyclic group** of **order** n (g is one of its **generators**).

A cyclic group is always **finite** and **commutative**, even if $(G, \star)$ is not.

ORDER OF AN ELEMENT

The **order** of $b = g^i, i \in [\![1, n]\!]$ is the smallest k such that $b^k = e$.

$$k = \frac{\text{lcm}(i, n)}{i} = \frac{n}{\text{gcd}(i, n)}$$

GENERATORS

Each element of order n is a **generator** of H. There are $\phi(n)$ generators.

DISCRETE LOGARITHM

In $(H, \star)$, if g is a generator, then $g^i = h$ is a bijection (of inverse $\log_g h$).

Usual rules of exp/log are still valid in the discrete case ($a^i \star a^j$, $(a^i)^j$, $\log_g a + \log_g b$, $\log_g a^k$).

Error Detection & Error Correction Codes

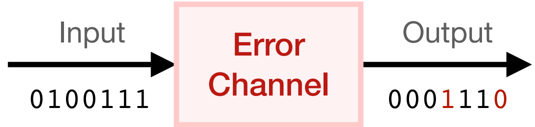
Channel Coding

ERASURE CHANNEL

Some input symbols are “erased” and replaced by the $?$ symbol.

ERASURE WEIGHT p
= Number of erasures

ERROR CHANNEL



Sone inputs get flipped into a different symbol.

ERROR WEIGHT p
= Number of errors

TERMINOLOGY

- **Code $\mathscr{C}$**: set of codewords ($\mathscr{C} \subseteq \mathscr{A}^n$, where $\mathscr{A}$ is the **alphabet**, we want it to be **large**)
- n: **block length** (we only consider block codes, with the same block length; we want it **small**).
- $k = \log_{|\mathscr{A}|} |\mathscr{C}|$: number of **information symbols** carried a codeword (for linear codes: **dim.**).
- **Rate** of the code: $\frac{k}{n}$ bits/symbol (for a (n, k) code) (we want it **large**).

HAMMING DISTANCE

$$d(x, y) = \text{number of positions where } x \text{ and } y \text{ differ}$$

DISTANCE AXIOMS

It can be called a distance because $\forall x, y, z$, we have:

- Positive $d(x, y) \geq 0,$
- Symmetric $d(x, y) = d(y, x),$
- Zero iff equality $d(x, y) = 0 \Leftrightarrow x = y,$
- Triangle inequality $d(x, z) \leq d(x, y) + d(y, z).$

MINIMUM DISTANCE OF A CODE

$$d_{\min}(\mathscr{C}) = \min_{x \neq x'} d(x, x')$$

Must be **large** to correct more errors.

SINGLETON BOUND

$$d_{\min} \leq n - k + 1 \text{ for any block code}$$

With equality, the code is a **MDS code** (maximum distance separable).

MINIMUM DISTANCE DECODER

$$\hat{c} = \arg\min_{x \in \mathscr{C}} d(x, y)$$

There can be multiple minimum distance decoders sometimes.

ON ERASURE CHANNELS

The MD decoder is guaranteed correct if

$$p < d_{\min}(\mathscr{C})$$

ON ERROR CHANNELS

The MD decoder is guaranteed to correct if

$$p < \frac{1}{2} d_{\min}(\mathscr{C}) \quad \text{(detection: } p < d_{\min}\text{)}$$

Finite Fields

FIELDS

DEFINITION

$(K, +, \cdot)$ is a **field** when:

- K is a **set**,
- $(K, +)$ is a **commutative group** with identity element "0" and inverse $-x$,
- $(K \backslash \{0\}, \cdot)$ is a **commutative group** with identity element "1" and inverse x^{-1}.
- $+$ and $\cdot$ are **distributive**: $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{K}$.

E.g. $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$.

PROPERTIES

- $0 \cdot x = 0 \quad \forall x \in \mathbb{K}$
- $x \cdot y = 0 \ \Rightarrow \ x = 0$ or $y = 0 \quad \forall x, y \in K$

FINITE FIELDS

A **finite field** is a field where K is a finite set.

$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a finite field **iff p is prime.** So if p is prime, $\mathbb{F}_p$, is isomorphic to it.

CHARACTERISTIC

The additive order of 1 (least amount of adds to have 0) is the **characteristic** of a finite field.
It is always a **prime number**.

The **cardinality** of the field is an integer **power** of its characteristic.

ISOMORPHISM

An **isomorphism** between two fields $\mathbb{F} = (\mathscr{F}, +, \cdot)$ and $\mathbb{K} = (\mathscr{K}, \oplus, \odot)$
is a **bijection** $\psi : \mathscr{F} \to \mathscr{K}$ such that $\forall a, b \in \mathscr{F}$, $\begin{cases} \varphi(a+b) = \varphi(a) \oplus \varphi(b) \\ \varphi(a \cdot b) = \varphi(a) \odot \varphi(b) \end{cases}$.

$\mathbb{F}$ and $\mathbb{K}$ are **isomorphic** if there is an isomorphism between them.

All finite fields of the **same cardinality** are isomorphic.

FIELDS $\mathbb{F}_n$

If p is a prime number, a field of cardinality p^m exists for all integers m.

It is denoted $\mathbb{F}_{p^m}$ or $GF(p^m)$. Is characteristic is p.

Vector Spaces

VECTOR SPACES OVER FINITE FIELDS

The non-empty set V is a **vector space** over the finite field $\mathbb{F}$ if:

- **Vector addition** It has a binary operation "$+$" such that $(V, +)$ is a commutative group.
- **Scalar multiplication** It has a mixed operation "$\cdot$" which is **associative**, has an **identity** $1 \cdot \overrightarrow{v}$ and is **distributive** with $+$.

For instance: $\mathbb{F}^n$ with component-wise addition and scalar multiplication.

SUBSPACES

$S \subseteq V$ is a **subspace** of the vector space V if it is closed $+$ and $\cdot$.

BASIS AND RANK

LINEAR INDEPENDENCE

$\{\overrightarrow{v_1}, \cdots, \overrightarrow{v_n}\}$ is **linearly independent** iff $\sum_{i=1}^{n} \lambda_i \cdot \overrightarrow{v_i} = \overrightarrow{0} \Rightarrow \lambda_i = 0 \ \ \forall i.$

SPAN

$\text{span}\{\overrightarrow{v_1}, \cdots, \overrightarrow{v_i}\} = \left\{\lambda_1 \overrightarrow{v_1} + \cdots + \lambda_n \overrightarrow{v_n} \,\middle|\, \lambda_i \in \mathbb{F}\right\}$

BASIS & DIMENSION

A **basis** B of V is a list of vectors that span V and are linearly independent.

If its is finite, V is called **finite-dimensional** and its cardinality $|B|$ is called $\dim V$ (always same).
$\Rightarrow$ The cardinality of V is $(\text{car}\,\mathbb{F})^{\dim V}$.

A list of $m < n$ elements can be completed into a basis, and a list of $m > n$ elements can be reduced to a basis.

B is a basis of $V \Leftrightarrow$ every element of V can be written uniquely as a linear combination of B.

RANK OF A MATRIX

$\text{rank}(M)$ = number of linearly independent columns = number of linearly independents columns

RANK THEOREM

The solutions of a linear homogeneous equations is a subspace.

The **rank theorem** says for any equation with n variables:

$$\boxed{n = \dim\,[\text{Sol}] + \text{rank}\,[\text{Coeffs}]}$$

Linear Codes

DEFINITIONS

LINEAR CODE

A code $\mathscr{C} \subseteq \mathbb{F}^n$ is **linear** if it is a subspace. Its **dimension** is the dimension of the subspace.

We have to check that it contains the **all-zero sequence**, that the **scaling is closed**, and the **addition is closed** (or find a basis of the right size that spans $\mathscr{C}$).

NUMBER OF BASES

If there are q^k codewords,

$$(q^k - 1) \cdots (q^k - q^{k-1})$$

NUMBER OF CODEWORDS

$$\operatorname{card} \mathscr{C} = [\operatorname{card} \mathbb{F}]^k$$

BINARY LINEAR MDS CODES

Only three binary linear codes satisfy the Singleton bound with equality:

- **Parity-check code** Codewords with an even number of 1s
- **Repetition code** Only two codewords, only 0 and only 1
- $\mathbb{F}_2^n$

HAMMING WEIGHT

HAMMING WEIGHT

The **Hamming weight** $w(\overrightarrow{x})$ of $\overrightarrow{x} \in \mathbb{F}^n$ is the number of non-zero positions $= d(\overrightarrow{x}, \overrightarrow{0})$.

MINIMUM DISTANCE OF A LINEAR CODE

$$d_{\min}(\mathscr{C}) = \min_{\overrightarrow{x} \in \mathscr{C}*} w(\overrightarrow{x})$$

PARITY-CHECK MATRIX

The **parity-check matrix** H contains the coefficient of a system of equation that describes the system.

SYNDROME

$$\vec{s} = \overrightarrow{y} H^T \quad (\vec{s} = \overrightarrow{0} \Leftrightarrow \overrightarrow{y} \in \mathscr{C})$$

COMPUTE $d_{\min}$

$d_{\min}$ is the minimum number of **linearly dependent columns** of H.

GENERATOR MATRIX

Contains the vectors of a basis.

$$G = \begin{pmatrix} \boxed{\quad \vec{c_1} \quad} \\ \vdots \\ \boxed{\quad \vec{c_k} \quad} \end{pmatrix}$$

An encoding map is given by: $\vec{c} = \vec{u}G$ ($\vec{u}$: information vector).

SYSTEMATIC FORM

Use Gaussian elimination to find:

$$G = \left(\begin{array}{c:c} I_k & P \end{array} \right) \qquad \Rightarrow H = \left(\begin{array}{c:c} -P^T & I_{n-k} \end{array} \right)$$

Sometimes, it's not possible to find it, but we can invert columns to do it in a similar code.

DECODING

COSETS

Let $(\mathscr{G}, \star)$ be a group and $(\mathscr{H}, \star)$ a subgroup.

$[a]$ is the **coset of** $\mathscr{H}$ with respect to a. We write:

$$[a] \overset{\text{not}}{=} a \star \mathscr{H} \overset{\text{def}}{=} \{y \in \mathscr{H} : \exists x \in \mathscr{H}, y = x \star a\}$$

All cosets $[a]$ have **cardinality** $\text{card}\, \mathscr{H}$.

The relation $a \sim b$ ($\exists x \in \mathscr{H}, b = x \star a$) is an **equivalence relation** that forms a partition of $\mathscr{G}$.

STANDARD ARRAY

The **standard array** of the linear code $\mathscr{C} \subset \mathbb{F}^n$ contains all the elements of $\mathbb{F}^n$.

The code is on the first line, and the first column contains the "individual errors" (that must have the smallest weight possible in order to reach maximum decoding accuracy).

$$\begin{array}{c} \mathscr{C} \\ [t_1] \\ [t_2] \\ \vdots \end{array} \begin{bmatrix} \mathbf{0} & c_1 & c_2 & \cdots \\ t_1 & c_1 + t_1 & c_2 + t_1 & \\ t_2 & c_1 + t_2 & c_2 + t_2 & \\ \vdots & & & \end{bmatrix} = \begin{bmatrix} 000 & 111 \\ 100 & 011 \\ 010 & 101 \\ 001 & 110 \end{bmatrix}$$

Each elements of a line has the **same syndrome**. Thus, it is necessary to store only the first column and its syndromes.

COSET DECODING

We compute the syndrome of what we received, and we subtract the corresponding error.

Specific Codes

POLYNOMIAL OVER FIELDS

POLYNOMIAL OVER FIELDS

Let $\overrightarrow{u} \in \mathbb{F}^k = (u_1, \cdots, u_k)$. We associate it to the polynomial:

$$P_{\overrightarrow{u}}(x) = u_1 + u_2 x + \cdots + u_k x^{k-1}$$

Its **degree** is the highest i such that x^i has a non-zero coefficient

(the zero polynomial has degree $-\infty$).

LAGRANGE'S INTERPOLATION POLYNOMIALS

✨ From a series of points (x_i, y_i), get the lowest degree polynomial f such that $f(x_i) = y_i \ \forall i$.

With distinct x_i,

$$p_{x_i}(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \quad \Rightarrow P(x) = \sum_i y_i \cdot p_{x_i}(x)$$

The top part sets the value of the polynomial to 0 at the other points.

The lower part sets the value of the polynomial to 1 at x_i.

FUNDAMENTAL THEOREM OF ALGEBRA

A non-zero polynomial of degree n has at most n distinct roots.

REED-SOLOMON CODES

Choose $\mathbb{F}$ (finite) and $1 \leq k \leq n \leq \operatorname{card} \mathbb{F}$, and n distinct elements a_i.

The encoding map is:

$$\begin{aligned} \mathbb{F}^k &\to \mathbb{F}^n \\ \overrightarrow{u} &\mapsto \overrightarrow{c} = \left(P_{\overrightarrow{u}}(a_1), \ \cdots, \ P_{\overrightarrow{u}}(a_n)\right) \end{aligned}$$

This code is **linear** and **MDS**.