Introduction to the Theory of Error-Correcting Codes

Antoine O. Berthet
antoine.berthet@centralesupelec.fr
☎ +33 (0)1 69 85 14 62

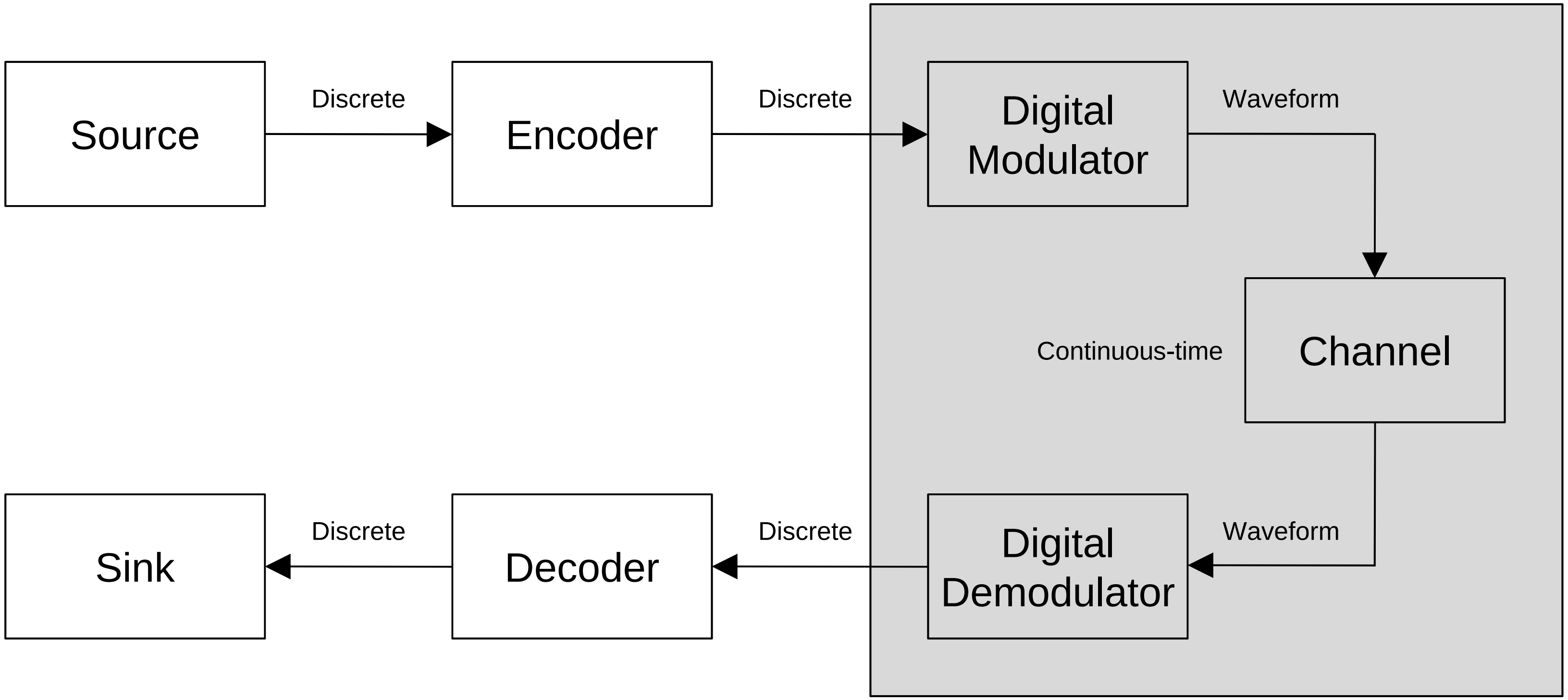
CentraleSupélec
Department of Telecommunications

References

- C.E. Shannon, *The Mathematical Theory of Communication*, Bell System Technical Journal, vol. 27, 1948.
- T. Cover, J.A. Thomas, *Elements of Information Theory*, Wiley, 1991.
- F.J. McWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North Holland Publishing, 1977.
- R.J. McEliece, *Finite fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987

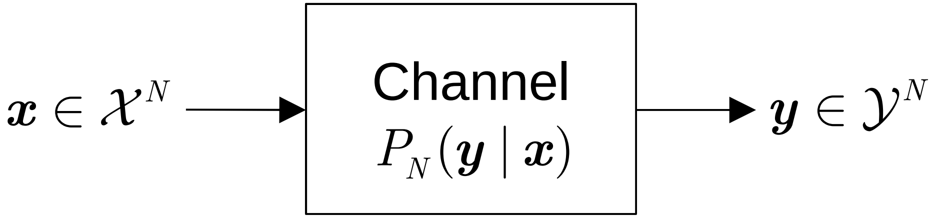
Basic concepts

Communication chain



Channels

- **Probabilistic model**. For each input sequence, we have a probability measure on the output sequence conditional on that input sequence (also referred to as channel transition probability or likelihood function)



$\boldsymbol{x} \in \mathcal{X}^N$

Channel

$P_N(\boldsymbol{y} \mid \boldsymbol{x})$

$\boldsymbol{y} \in \mathcal{Y}^N$

- **Discrete channel**. Input and output are each sequences of letters from *finite* alphabets
- **Discrete memoryless channel** (DMC). Output at a given time depends statistically only on the corresponding input

$$P_N(\boldsymbol{y} \mid \boldsymbol{x}) = \prod_{n=1}^{N} P(y_n \mid x_n)$$

Channel capacity

- **AMI**. The average mutual information (AMI) measures is a measure of the amount of information that a random variable contains on another random variable, and vice versa

$$I(X;Y) = \mathbb{E}_{P(x,y)}\left[\log_2 \frac{P(X,Y)}{Q(X)P(Y)}\right]$$

- It is therefore natural to consider the AMI between the random channel input and the random channel output (in bits/c.u.) as a measure of the “capacity” of the channel to convey information

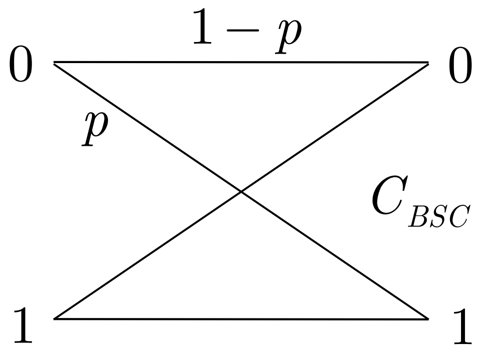
- **Capacity**. The information capacity of a DMC is defined as

$$\boxed{C \doteq \max_{\boldsymbol{Q}} I(X;Y)}$$

where the maximum is taken over all possible input distributions

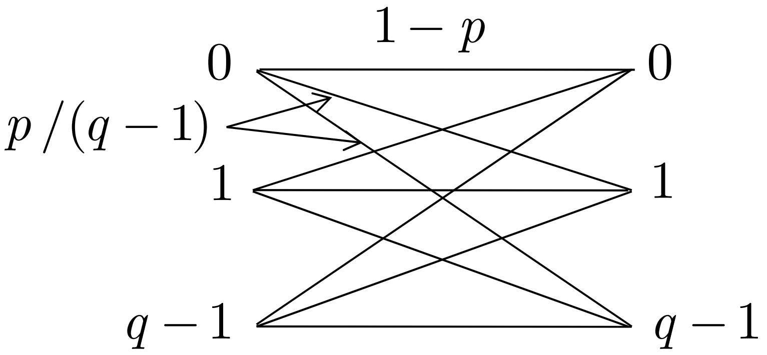
Channel capacity

- ✓ **Example**. Some reference discrete channels (BSC, BEC, QSC)



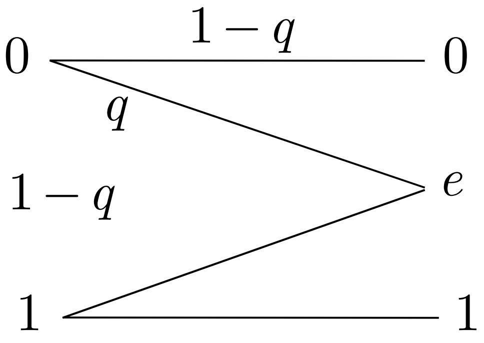
Binary symmetric channel

$$C_{BSC} = 1 - \mathcal{H}_2(p)$$



q-ary symmetric channel

$$C_{QSC} = \log_2 q - p\log_2(q-1) - \mathcal{H}_2(p)$$



$$C_{BEC} = 1 - q$$

Binary erasure channel

Codebook, code rate, coding and decoding

- **Definition**. An (N,M) block code $\mathcal{C}$ of size M, defined over a finite alphabet $\mathcal{X}$, is a set of M sequences of length N symbols of $\mathcal{X}$ referred to as *codewords.* The code rate is $R_c = \log M/N$

- **Definition**. The encoding is an injective (one-to-one) mapping from the index set to the codebook

$$f : m \in \{0,\ldots,M-1\} \to \boldsymbol{x}(m) \in \mathcal{C} \subset \mathcal{X}^N$$

- **Definition**. The decoding is a mapping from the observation space to the index set based on a deterministic decision rule (e.g., typical set decoding, MAP decoding, etc.)

$$g : \boldsymbol{y} \in \mathcal{Y}^N \to \hat{m} \in \{0,\ldots,M-1\}$$

Error probability

- ❑ **Definition**. Probability of error conditional on a particular index

$$P_e^{(N)}(m) = P(\hat{m} \neq m \mid m) = \sum\nolimits_{\boldsymbol{y} \in \mathcal{Y}^c(m)} P_N(\boldsymbol{y} \mid m)$$

with $\mathcal{Y}(m) \doteq \left\{ \boldsymbol{y} \,/\, \hat{m} = m \right\}$ and $\mathcal{Y}^c(m) \doteq \left\{ \boldsymbol{y} \,/\, \hat{m} \neq m \right\}$

- ❑ **Definition**. Maximum probability of error

$$\boxed{\lambda_e^{(N)} = \max_m P_e^{(N)}(m)}$$

- ❑ **Definition**. Arithmetic (or average) probability of error

$$\boxed{P_e^{(N)} = \sum\nolimits_m P(m) P_e^{(N)}(m) \leq \lambda_e^{(N)}}$$

The noisy channel coding theorem

- ❑ **Definition**. A rate R_c is said to be achievable if there exists a sequence of $\left(M=\left\lceil 2^{NR_c}\right\rceil, N\right)$ codes s.t. $\lim_{N\to\infty} P_e^{(N)}=0$

- ❑ **Theorem**. All rates below the channel capacity are achievable

  $\forall R_c \le C$, $\exists$ a sequence of $\left(M=\left\lceil 2^{NR_c}\right\rceil, N\right)$ codes s.t. $\lim_{N\to\infty} P_e^{(N)}=0$

  - ▪ **Proof**. Based on jointly typical sequences, typical set decoding, and the notion of random code ensemble

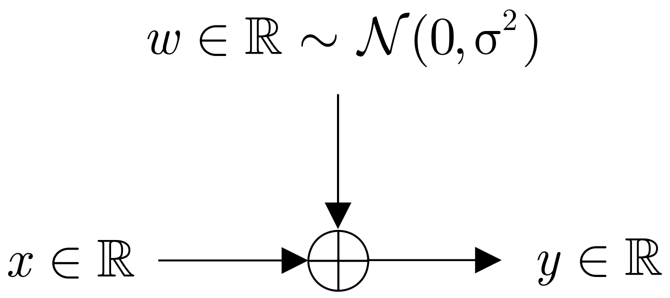
- ❑ **Weak converse**. Any sequence of $\left(M=\left\lceil 2^{NR_c}\right\rceil, N\right)$ code s.t. $\lim_{N\to\infty} P_e^{(N)}=0$ must have $R_c \le C$

  - ▪ **Proof**. Based on Fano’s inequality

(1) C.E. Shannon, 1949 ; (2) Cover and Thomas, chap. 3 and 8

Channels

- ❑ **Continuous-input continuous-output channel**, e.g., additive white Gaussian noise channel (AWGNC)



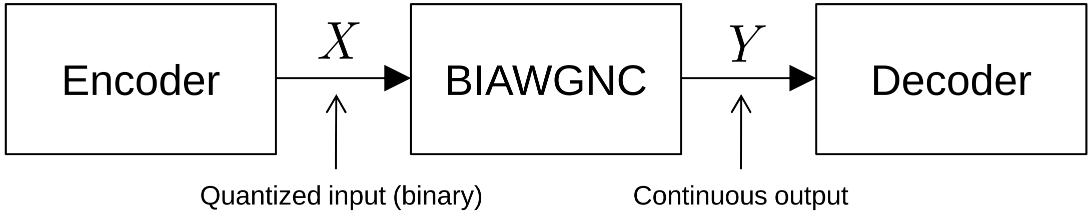
$$E_b = \frac{E_c}{R_c} = \frac{E_X}{R_c} \qquad \sigma^2 = \frac{N_0}{2E_X} = \frac{N_0}{2R_cE_b} = \frac{1}{2R_c\gamma_b}$$

$$C_{AWGN} = \frac{1}{2}\log_2\left(1 + 2R_c\gamma_b\right)$$

(1) Cover and Thomas, chap. 9 and 10

Hard versus soft decision decoding

❑ BIAWGNC. AWGNC with quantized input



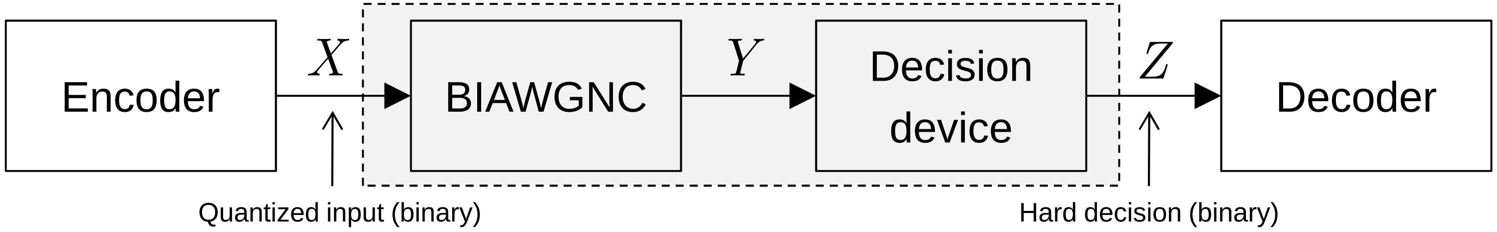
$$I(X;Y) \triangleq \mathbb{E}_{p(x,y)}\left[\log_2 \frac{p(X,Y)}{P(X)p(Y)}\right]$$

- Capacity (in bits/cu) achieved for uniform input distribution

$$C_{BIAWGNC} = 1 - \frac{1}{2}\sum_{x\in\{\pm 1\}} \mathbb{E}_{p(y|X=x)}\left[\log_2 \frac{p(Y)}{p(Y \mid X = x)}\right]$$

Hard versus soft decision decoding

❑ BIAWGNC followed by an (intermediate) decision device



- From data processing theorem

$$I(X;Y) \geq I(X;Z)$$

- Assume that the decision device takes a hard decision (ML)

$$Z \triangleq \begin{cases} +1 & p(y \mid +1) \geq p(y \mid -1) \\ -1 & p(y \mid -1) \geq p(y \mid +1) \end{cases}$$

Hard versus soft decision decoding

- The concatenation of the two modules can be modeled as a BSC with error probability

$$p = Q\left(\sqrt{2\gamma}\right) = Q\left(\sqrt{2R_c\gamma_b}\right)$$

- Capacity (in bits/cu) achieved for uniform input distribution

$$C_{BSC} = 1 - H_2(p) = f(\gamma_b, R_c)$$

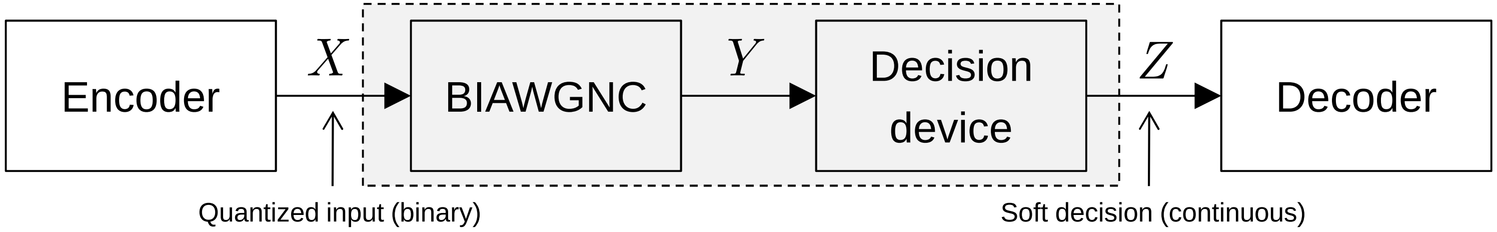
- Limit obtained by equality substituted for inequality (1)

$$R_c \overset{(1)}{\leq} C_{BSC} = f(\gamma_b, R_c) \rightarrow R_c = f(\gamma_b, R_c)$$

- **Note**. The reasoning could be further generalized to any other symmetrically quantized reduction of the BIAWGNC

Hard versus soft decision decoding

❑ BIAWGNC followed by an (intermediate) decision device



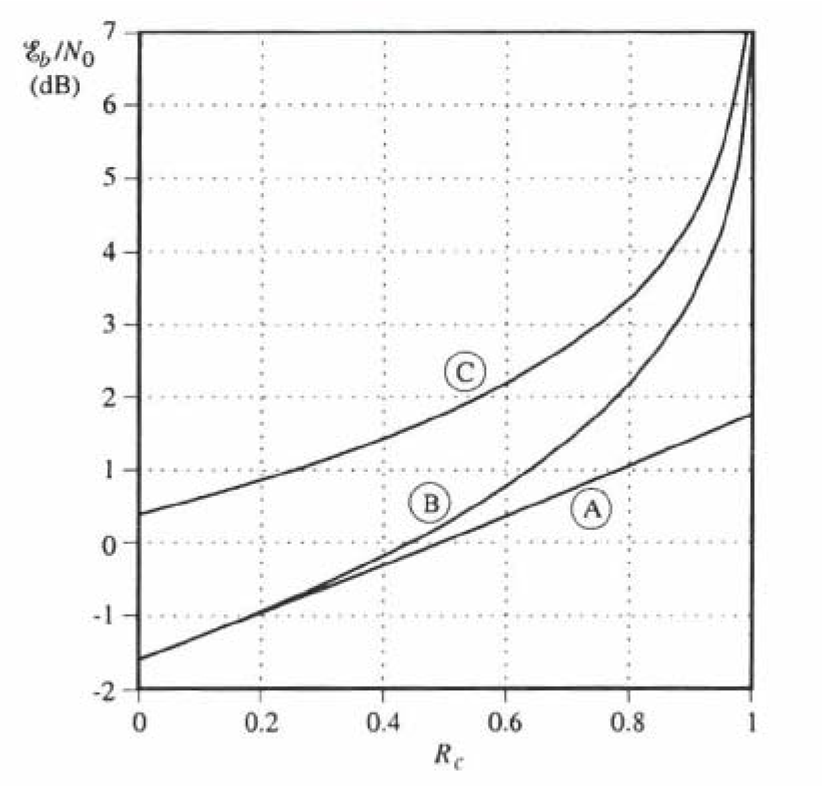
- Assume that the decision device takes a soft decision

$$Z \triangleq \ln \frac{p(y \mid +1)}{p(y \mid -1)} = 2\frac{y}{\sigma^2} = 4R_c\gamma_b y \Rightarrow I(X;Z) = I(X;Y)$$

- Limit obtained by equality substituted for inequality (1)

$$R_c \overset{(1)}{\leq} C_{BIAWGNC} = g(\gamma_b, R_c) \rightarrow R_c = g(\gamma_b, R_c)$$

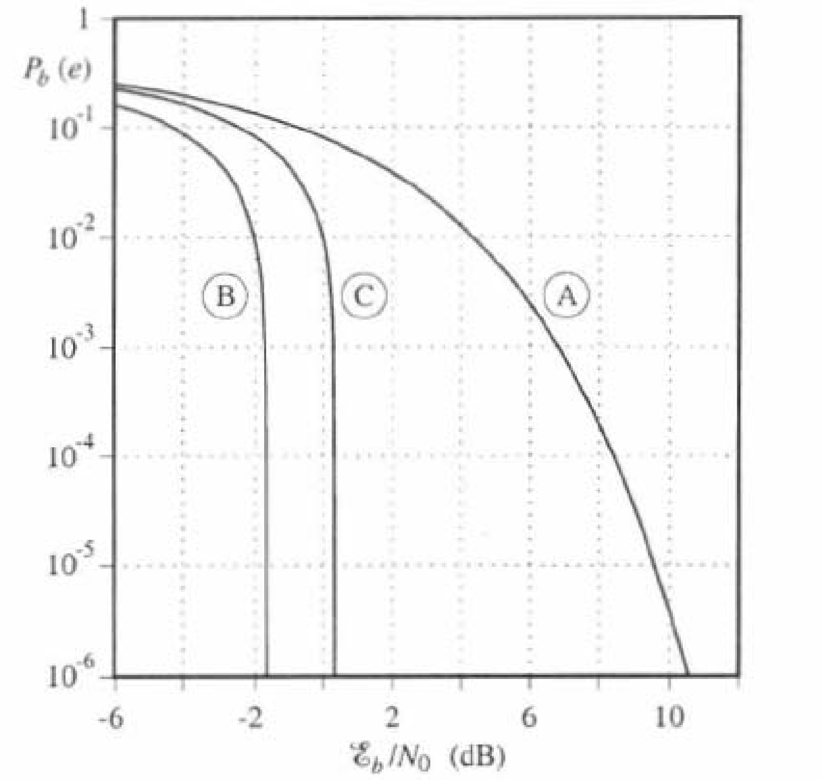
Hard versus soft decision decoding



A: unconstrained AWGNC
B: BIAWGNC (soft decisions)
C: BSC (hard decisions)

[1] From Biglieri et al., p. 146, Fig. 3.22.

Hard versus soft decision decoding



A: binary uncoded antipodal (BSPK)

B: capacity limit BIAWGNC (soft decisions)

C: capacity limit BSC (hard decisions)

(1) From Biglieri et al., p. 458, Fig. 10.3.

Problem statement

- ❑ **Most important parameters**. Rate, probability of (bit or block) error, delay, and complexity (encoding and decoding)
- ❑ **Objective**. Determine all achievable tuples

$$\left(R_c, P_e, N, \chi_E, \chi_D\right)$$

together with their associated coding/decoding schemes, a vast and very challenging problem whose complete characterization is still open research…

Problem. Transmit at the larger rate with low probability of error using simple encoding and decoding algorithms and short codes

Some remarks

- Delay is most often assimilated to the block length in FEC systems, but is more difficult to define if transmission occurs on channels with feedback, e.g., ARQ systems
- Complexity is a fuzzy notion. Computational complexity theory is a branch of the theory of computation in theoretical computer science that focuses on classifying problems according to their inherent difficulty (P, NP, and so on). Also evaluated in terms of hardware constraints

Minimum Hamming distance

- **Definition**. The Hamming distance between any two words $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathcal{X}^N$ is the number of their distinct components

$$d_H(\boldsymbol{x},\boldsymbol{y}) \geq 0 \qquad d_H(\boldsymbol{x},\boldsymbol{y}) = 0 \Rightarrow \boldsymbol{x} = \boldsymbol{y} \qquad d_H(\boldsymbol{x},\boldsymbol{y}) = d_H(\boldsymbol{y},\boldsymbol{x})$$

$$d_H(\boldsymbol{x},\boldsymbol{z}) \leq d_H(\boldsymbol{x},\boldsymbol{y}) + d_H(\boldsymbol{y},\boldsymbol{z})$$

- **Definition**. The Hamming space $\mathcal{X}^N$ endowed with the Hamming distance is known as the Hamming cube
- **Definition**. Hamming weight and support

$$w_H(\boldsymbol{x}) \doteq d_H(\boldsymbol{x},\boldsymbol{0}) = \left|Supp(\boldsymbol{x})\right| \text{ with } Supp(\boldsymbol{x}) \doteq \{i : x_i \neq 0\}$$

- **Definition**. The minimum Hamming distance of a block code is

$$d \doteq \min_{\boldsymbol{x}_i,\boldsymbol{x}_j \in \mathcal{C} \,/\, \boldsymbol{x}_i \neq \boldsymbol{x}_j} d_H(\boldsymbol{x}_i,\boldsymbol{x}_j) = \min_{\boldsymbol{x}_i,\boldsymbol{x}_j \in \mathcal{C} \,/\, \boldsymbol{x}_i \neq \boldsymbol{x}_j} w_H(\boldsymbol{x}_i - \boldsymbol{x}_j)$$

Decoding (or decision) rule

- **Type of decisions**
  1. No error have occurred, the decoder accepts the received word as it is
  2. Errors have occurred, the decoder corrects the received word into a codeword
  3. Errors have occurred, but no correction is possible. Retransmission might be the best strategy provided that there exists a feedback channel
- **Objective** is that the decoder take the course of action which leads to the greatest probability of correct decision

Nearest neighbor decoding

- **Principle**. **If** there is a *unique* codeword whose distance (in a sense to specify, Hamming distance for discrete channels) to the received word is minimum, **then** correct the received word into that codeword. **Else if** no such codeword exists, **then** report that errors have been detected, but no correction is possible

- **Discussion**. Nearest neighbor decoding (NND) strategy may on occasion lead to an incorrect decoding. Moreover, the decoding procedure may fail to decode some received words. Such a decoding is referred to as *incomplete*. By contrast, a *complete* decoding always outputs a codeword (correct or not). To transform an *incomplete* NND into a *complete* NND, we could imagine that in the event that a received word is not closest to a unique codeword, the decoder would correct it to any one of the codewords a minimum distance, selected at random

Link between NND and MLD

- **Maximum a posteriori (MAP) decoding rule**

$$\boxed{\hat{m}_{MAP} = \arg\max_{m} P(m \mid \boldsymbol{y})}$$

- By Bayes theorem, a posterior probability can be expanded as

$$P(m \mid \boldsymbol{y}) = \frac{P_N(\boldsymbol{y} \mid \boldsymbol{x}(m))P(m)}{\sum_m P_N(\boldsymbol{y} \mid \boldsymbol{x}(m))P(m)}$$

- **Maximum likelihood decoding (MLD) rule**. When messages are equally probable (unknown or non meaningful priors)

$$\boxed{\hat{m}_{MAP} = \arg\max_{m} P_N(\boldsymbol{y} \mid \boldsymbol{x}(m)) = \hat{m}_{ML}}$$

Link between NND and MLD

❑ System model

$$\boldsymbol{x} \in \mathcal{C} \subset \mathcal{X}^N \overset{\mathrm{QSC}(q,p)}{\to} \boldsymbol{y} \in \mathcal{Y}^N \overset{\mathrm{MLD}}{\to} \hat{\boldsymbol{x}}_{ML} = \arg\max_{\boldsymbol{x}\in\mathcal{C}} P_N(\boldsymbol{y}|\boldsymbol{x})$$

- The likelihood function is given by

$$P_N(\boldsymbol{y}|\boldsymbol{x}) = (1-p)^{N-d_H(\boldsymbol{x},\boldsymbol{y})}\left(\frac{p}{q-1}\right)^{d_H(\boldsymbol{x},\boldsymbol{y})} \propto \left(\frac{p}{(q-1)(1-p)}\right)^{d_H(\boldsymbol{x},\boldsymbol{y})}$$

$$\frac{p}{(q-1)(1-p)} < 1 \Rightarrow \max_{\boldsymbol{x}\in\mathcal{C}} P_N(\boldsymbol{y}|\boldsymbol{x}) = \max_{\boldsymbol{x}\in\mathcal{C}} \log P_N(\boldsymbol{y}|\boldsymbol{x}) = \min_{\boldsymbol{x}\in\mathcal{C}} d_H(\boldsymbol{x},\boldsymbol{y})$$

$$\boxed{\text{if } p < \frac{q-1}{q} \text{ then MLD coincides with NND}}$$

- Left as exercise. Also consider the two other cases

More about MLD

- ❑ **Maximum A Posteriori (MAP) decoding rule**. Minimizes the probability of decoding error for a given message ensemble, codebook (set of codewords) and channel

- ▪ **Bayes estimation/decision theory**. Expected cost to minimize

$$\begin{aligned}\chi &= \mathbb{E}_{m,\boldsymbol{y}}\left[c(m,\hat{m}(\boldsymbol{y}))\right] = \sum\nolimits_{m}\sum\nolimits_{\boldsymbol{y}} P(m,\boldsymbol{y})c(m,\hat{m}(\boldsymbol{y})) \\ &= \sum\nolimits_{\boldsymbol{y}} P(\boldsymbol{y})\underbrace{\sum\nolimits_{m} P(m \mid \boldsymbol{y})c(m,\hat{m}(\boldsymbol{y}))}_{\chi(\boldsymbol{y})}\end{aligned}$$

- • The cost function depends on the specific problem. We only consider non-negative cost functions

$$c(m,m') \geq 0,\ \forall m,m'$$

More about MLD

- In this case, minimizing the expected cost function

$$\chi = \sum_{\boldsymbol{y}} P(\boldsymbol{y}) \underbrace{\sum_{m} P(m \mid \boldsymbol{y}) c(m, \hat{m}(\boldsymbol{y}))}_{\chi(\boldsymbol{y})}$$

turns out to be equivalent to minimize the integrand

$$\chi(\boldsymbol{y}) = \sum_{m} P(m \mid \boldsymbol{y}) c(m, \hat{m}(\boldsymbol{y})) \ \forall \boldsymbol{y}$$

- Choose the following (non-negative) cost function

$$c(m, \hat{m}(\boldsymbol{y})) = \begin{cases} 1 \text{ if } \hat{m}(\boldsymbol{y}) \neq m \\ 0 \text{ if } \hat{m}(\boldsymbol{y}) = m \end{cases}$$

- Such a cost function is always meaning with discrete problems since an estimator will either right or wrong.

More about MLD

- With this cost function, the integrand is

$$\chi(\boldsymbol{y}) = \sum\nolimits_m P(m \mid \boldsymbol{y}) c(m, \hat{m}(\boldsymbol{y})) = 1 - P(\hat{m}(\boldsymbol{y}) \mid \boldsymbol{y})$$

- The integrand is minimized if we choose

$$\hat{m}(\boldsymbol{y}) = \arg\max_m P(m \mid \boldsymbol{y})$$

- Alternatively, the expected cost can be written as

$$\chi = \sum\nolimits_m P(m) \sum\nolimits_{\boldsymbol{y}} P_N(\boldsymbol{y} \mid m) c(m, \hat{m}(\boldsymbol{y}))$$

- Taking into account the definition of the cost function

$$\chi = \sum\nolimits_m P(m) \underbrace{\sum\nolimits_{\boldsymbol{y} \in \mathcal{Y}^c(m)} P_N(\boldsymbol{y} \mid m)}_{= P_e^{(N)}(m)} = P_e^{(N)}$$

Voronoï regions

- **Equivalent problem**. Partitioning the Hamming space in regions centered on each codeword

$$\mathcal{R}(\boldsymbol{x}_i) = \left\{ \boldsymbol{y} \in \mathcal{Y}^N : d_H(\boldsymbol{x}_i, \boldsymbol{y}) < d_H(\boldsymbol{x}_j, \boldsymbol{y}),\ \forall \boldsymbol{x}_j \in \mathcal{C},\ \boldsymbol{x}_j \neq \boldsymbol{x}_i \right\}$$

- **Algorithm** (equivalent to MLD)

Find i s.t. $\boldsymbol{y} \in \mathcal{R}(\boldsymbol{x}_i)$ and decode $\hat{\boldsymbol{x}} = \boldsymbol{x}_i$

- **Definition**. Up to the boundaries, such decoding regions correspond to Voronoï regions defined as

$$\mho(\boldsymbol{x}_i) = \left\{ \boldsymbol{y} \in \mathcal{Y}^N : d_H(\boldsymbol{x}_i, \boldsymbol{y}) \leq d_H(\boldsymbol{x}_j, \boldsymbol{y}),\ \forall \boldsymbol{x}_j \in \mathcal{C},\ \boldsymbol{x}_j \neq \boldsymbol{x}_i \right\} \supset \mathcal{R}(\boldsymbol{x}_i)$$

- Voronoï regions “cover” the Hamming space

Detection capability

- ❑ **Definition**. The maximum number of symbol errors below which an error processor is sure to detect an error

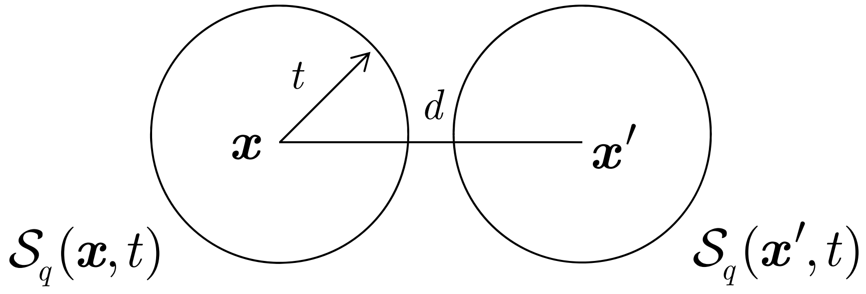
- ❑ **Proposition**. The detection capability of an (N,M,d) code is equal to $d-1$

- ▪ **Proof**. At least d symbols separate one codeword from another. Hence, $d-1$ errors or less can never transform a codeword into another, and error detection is certain

Correction capability

- **Definition**. The maximum number of symbol errors below which an error processor is sure to correct an error (under NND)
- **Proposition**. The correction capability of an $(N,M,d = 2t+1)$ code is equal to t

- **Proof**. Partition the Hamming space into spheres of radius t centered on codewords. No received word can be in two distinct spheres. Above this radius value, spheres may have non-zero intersection and the correction capability is exceeded


t
d
$\boldsymbol{x}$
$\boldsymbol{x}'$
$\mathcal{S}_q(\boldsymbol{x}, t)$
$\mathcal{S}_q(\boldsymbol{x}', t)$

Problem statement (cont.)

- **Conclusion**. Practical good codes require large minimum Hamming distances. The minimal Hamming distance is a critical parameter in the code design and must be optimized

- In essence, classical coding theory is focused on the two following problems

Find $d(N, M, q = |\mathcal{X}|) \doteq$ greatest d s.t. $\exists$ an $(N, M, d)_q$ code

- Or conversely,

Find $M(N, d, q = |\mathcal{X}|) \doteq$ greatest M s.t. $\exists$ an $(N, M, d)_q$ code

- These two problems are deeply rooted in combinatorial design theory (a branch of combinatorial theory)

Singleton bound and MDS codes

- **Proposition**. For any $(N,M,d)_q$ code

$$M \leq q^{N-d+1}$$

- **Proof**. Fix N and d. Consider the $M \times N$ matrix whose rows are the codewords. Delete $d-1$ columns (e.g., the first ones), i.e., project the matrix onto the last $N-d+1$ remaining columns. Since the code has minimal distance d , the rows are still distinct. So we still have M codewords but the block length has been reduced to $N-d+1$

- Any code whose code size meets this bound is said *maximum distance separable* (MDS)

[1] R.C. Singleton, IEEE IT, vol. 10, 1964

Hamming bound and prefect codes

- **Proposition**. For any $(N,M,d = 2t + 1)_q$ code

$$M \le \frac{q^N}{V_q(N,t)} \text{ where } V_q(N,t) \doteq \sum_{i=0}^{t} \binom{N}{i} (q-1)^i$$

- **Proof**. By previous theorem, the spheres of radius t centered around distinct codewords must be disjoint. Hence

$$\bigcup_{\boldsymbol{x}\in\mathcal{C}} \mathcal{S}_q(\boldsymbol{x},t) \subseteq \mathcal{X}^N \Leftrightarrow MV_q(N,t) \le q^N$$

- When the spheres of radius t centered on codewords are disjoint and exhaust the entire Hamming space, i.e., when the code size meets the Hamming bound, the code is said *perfect*

[1] R. W. Hamming, BSTJ, vol. 29. 1950

Gilbert-Varshamov (GV) bound

- **Proposition**. There exists an $(N,M,d)_q$ code such that

$$M \geq \frac{q^N}{V_q(N,d-1)} \text{ where } V_q(N,d-1) \doteq \sum_{i=0}^{d-1} \binom{N}{i} (q-1)^i$$

- **Proof**. Without loss of generality, we assume that the code is maximal in the sense that no codeword can be added to the code without decreasing the minimal distance. No word in $\mathcal{X}^N$ is at a distance greater or equal to d of a codeword. Otherwise, we could choose it to augment the code without decreasing the minimal distance. In that case, the spheres of radius $d-1$ centered around the codewords must cover the whole $\mathcal{X}^N$ and

$$\mathcal{X}^N \subseteq \bigcup_{\boldsymbol{x} \in \mathcal{C}} \mathcal{S}_q(\boldsymbol{x}, d-1) \Leftrightarrow q^N \leq M V_q(N, d-1)$$

[1] E. Gilbert, BSTJ, vol. 31, 1952

Elements of abstract algebra

Abelian group

- **Definition**. An abelian group is a set of elements together with an operation such that the following axioms are satisfied

$$\forall a, b \in \mathbb{G},\ a+b=b+a \in \mathbb{G}$$

$$\forall a, b, c \in \mathbb{G},\ (a+b)+c=a+(b+c)$$

$$\exists \text{ an identity element } 0 \text{ s.t. } a+0=0+a=a$$

$$\forall a \in \mathbb{G}, \exists \text{ an opposite element } -a \text{ s.t. } a+(-a)=0$$

- **Discussion**. We often distinguish a group being additive or multiplicative. However, the two are formally identical (from a graph-theoretical point of view). We are mainly interested in finite groups (finite cardinality or order)

Ring

- **Definition**. A ring is a set of elements together with two operations such that the following axioms are satisfied

$$(\mathbb{A},+) \text{ is an abelian group with identity element } 0$$

$$\forall a,b,\in \mathbb{A},\ a\times b\in \mathbb{A}$$

$$\forall a,b,c\in \mathbb{A},\ (a\times b)\times c = a\times (b\times c)$$

$$\forall a\in \mathbb{A}, \exists \text{ an identity element } 1 \text{ s.t. } a\times 1 = 1\times a = a$$

$$\forall a,b,c\in \mathbb{A},\ a\times (b+c) = a\times b + a\times c \text{ and } (a+b)\times c = a\times c + b\times c$$

$$\text{commutative ring : } \forall a,b\in \mathbb{A},\ a\times b = b\times a$$

$$\text{integral domain : } a\times b = b\times a = 0 \Rightarrow a = 0 \vee b = 0$$

✓ **Examples**. Integers $\mathbb{Z}$, integers modulo $n\in \mathbb{N}^*$ denoted $\mathbb{Z}_n$

Division algorithm and Euclidean algorithm

- **Division algorithm for integers**

$$\forall a \in \mathbb{Z}_{\geq 0}, b \in \mathbb{Z}_{>0}, \exists ! q \in \mathbb{Z} \text{ and } \exists ! r \in \mathbb{Z} \text{ s.t. } a = q \times b + r, 0 \leq r < b$$

- **Euclidean algorithm**. Can be used to find the greatest common divisor (gcd) between any two positive integers

$$r_0 = a, r_1 = b, \forall k \geq 2, r_{k-2} = q_k r_{k-1} + r_k, 0 \leq r_k < r_{k-1}$$

- The gcd is the last nonzero remainder in the sequence of remainders produced by repeated use of the division algorithm

Division algorithm and Euclidean algorithm

✓ **Application**. Find gcd(81,57)

k	do	r_k	q_k
0	$-$	81	$-$
1	$-$	57	$-$
2	$r_0 = q_2 r_1 + r_2,\ 0 < r_2 < r_1$	24	1
3	$r_1 = q_3 r_2 + r_3,\ 0 < r_3 < r_2$	9	2
4	$r_2 = q_4 r_3 + r_4,\ 0 < r_4 < r_3$	6	2
5	$r_3 = q_5 r_4 + r_5,\ 0 < r_5 < r_4$	3	1
6	$r_4 = q_6 r_5 + 0,\ r_6 = 0$	0	2

$$\boxed{\gcd(81,57) = 3}$$

Bézout's identity

❑ **Bézout's identity**.

$$\forall a, b \in \mathbb{Z}_{\geq 0}, \exists\, s, t \in \mathbb{Z} \text{ s.t. } s \times a + t \times b = \gcd(a, b)$$

- The two integers s and t are called Bézout's coefficients
- The identity can be generalized to more than two integers
- Bézout domain. Integral domain in which Bézout's identity holds

❑ **Extended Euclidean algorithm**

$$r_0 = a,\, r_1 = b,\, \forall k \geq 2,\, r_{k-2} = q_k r_{k-1} + r_k,\, r_k < r_{k-1}$$

$$s_0 = 1,\, s_1 = 0,\, \forall k \geq 2,\, s_k = s_{k-2} - q_k s_{k-1}$$

$$t_0 = 0,\, t_1 = 1, \forall k \geq 2,\, t_k = t_{k-2} - q_k t_{k-1}$$

Extended Euclidean algorithm

✓ **Application**. Find gcd(81,57) and the Bézout's coefficients

k	r_k	q_k	do	s_k	do	t_k
0	81	$-$	$-$	1	$-$	0
1	$-$	57	$-$	0	$-$	1
2	24	1	$s_2 = s_0 - q_2 s_1$	1	$t_2 = t_0 - q_2 t_1$	-1
3	9	2	$s_3 = s_1 - q_3 s_2$	-2	$t_3 = t_1 - q_3 t_2$	3
4	6	2	$s_4 = s_2 - q_4 s_3$	5	$t_4 = t_2 - q_4 t_3$	-7
5	3	1	$s_5 = s_3 - q_5 s_4$	-7	$t_5 = t_3 - q_5 t_4$	10
6	0	2	$-$	$-$	$-$	$-$

$$\boxed{-7 \times 81 + 10 \times 57 = \gcd(81,57) = 3}$$

Field

- □ **Definition**. A field is a set of elements together with two operations such that the following axioms are satisfied

$$(\mathbb{F}, +, \times) \text{ is an commutative ring with identity elements } 0 \text{ and } 1$$

$$\forall a \in \mathbb{F}^*, \exists \text{ an inverse element } a^{-1} \text{ s.t. } a \times a^{-1} = a^{-1} \times a = 1$$

- ✓ **Examples**. The set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$, and the set of complex numbers $\mathbb{C}$
- □ **Discussion**. In coding theory, we are mainly interested in finite fields or Galois fields [1,2] , so named in honor of Evariste Galois (1811-1832). Their role in the design of good algebraic codes is paramount. Finite fields are also important in other branches of mathematics, e.g., block designs, finite geometries, etc.

[1] McEliece, 1987 ; [2] Mac Williams, 1977

Finite field

- **Proposition**. $\mathbb{Z}_p$ is a finite field if and only if p is prime

- **Proof**. If p is not prime, then $p = a \times b$ with neither factors be the identity; in that case, the element b has no multiplicative inverse, since, by contradiction, if $b \times \mathrm{c} \equiv 1 \bmod(p)$ then

$$a \times b \times c \equiv a \bmod(p) \text{ and } a \times b \times c \equiv 0 \bmod(p) \Rightarrow a \equiv 0 \bmod(p)$$

- If p is prime, the existence of a multiplicative inverse for every nonzero element is guaranteed by Bézout's identity

$$0 < a < p \Rightarrow \gcd(a, p) = 1$$

$$\exists s, t \in \mathbb{Z} \text{ s.t. } s \times a + t \times p = 1 \Leftrightarrow s \times a \equiv 1 \bmod(p)$$

Using only prime fields $\mathbb{Z}_p$ and even $\mathbb{Z}_2$ much of the fundamental theory of error-correcting codes can be developed and very powerful codes designed

Finite field

- ❑ **Definition**. The characteristic of a field is the smallest positive integer m such that

$$\sum_{i=1}^{m} 1 = \underbrace{1+1+\cdots+1}_{m} = 0$$

- • If no such m exists, the characteristic of the field is 0
- ❑ **Proposition**. If the characteristic m of a field is not 0, then m must be prime
  - ▪ **Proof**. By contradiction, assuming that m is not prime
- ❑ **Proposition**. A finite field of characteristic p necessarily contains $\mathbb{Z}_p$ as a subfield (ground field)
  - ▪ **Proof**. Consider the subset of elements

$$1, 1+1, 1+1+1, \ldots, \sum_{i=1}^{p} 1 = 0 \bmod p$$

Ring of polynomials modulo a polynomial

- **Proposition**. The set $\mathbb{F}[x]$ of polynomials of an indeterminate x with coefficients from a field $\mathbb{F}$ is a ring with the standard addition and multiplication of polynomials

- **Division algorithm for polynomials**

$$\forall a(x), b(x) \in \mathbb{F}[x], \exists!\, q(x) \in \mathbb{F}[x] \text{ and } \exists!\, r(x) \in \mathbb{F}[x] \text{ s.t.}$$

$$a(x) = b(x) \times q(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r(x) < \deg b(x)$$

- **Definition**. Congruence modulo $f(x) \in \mathbb{F}[x]$

$$\forall g(x), h(x) \in \mathbb{F}[x],\ h(x) \equiv g(x) \bmod f(x) \Leftrightarrow f(x) \text{ divides } h(x) - g(x)$$

- Congruence modulo $f(x) \in \mathbb{F}[x]$ is an *equivalence relation* and as such partitions $\mathbb{F}[x]$ into equivalent classes. The equivalent class containing $g(x) \in \mathbb{F}[x]$ is $[g(x)] = \{h(x){:}h(x){\equiv}g(x) \bmod f(x)\}$

Ring of polynomials modulo a polynomial

- **Proposition**. The set of equivalent classes, denoted $\mathbb{F}[x]/f(x)$, is a *finite* ring with the polynomial addition and multiplication of equivalent classes

$$[g(x)]+[h(x)]=[g(x)+h(x)]$$

$$[g(x)]\times[h(x)]=[g(x)\times h(x)]$$

- The elements are all polynomials in $\mathbb{F}[x]$ of degree less than $f(x)$, i.e. all remainders after division by $f(x)$

- When the context is clear, we can omit square brackets for the equivalent class and designate it by its class representative

Bézout's identity for polynomials

- ❑ **Bézout's identity in $\mathbb{F}[x]$**. The gcd of two polynomials is the *monic* polynomial of largest degree which divides both of them. In this context, the Bézout's identity states that

$$\forall a(x), b(x) \in \mathbb{F}[x], \exists\, s(x), t(x) \in \mathbb{F}[x]$$

$$\text{s.t. } s(x) \times a(x) + t(x) \times b(x) = \gcd(a(x), b(x))$$

- ❑ **Euclidean and Extended algorithm for polynomials**. Can be used to find the remainder and the Bézout's coefficients

$$r_0(x) = a(x),\ r_1(x) = b(x),\ \forall k \geq 2,\ r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x)$$

$$\text{where } r_k(x) = 0 \ \text{ or } \deg r(x) < \deg r_{k-1}(x)$$

$$s_0 = 1,\ s_1 = 0,\ \forall k \geq 2,\ s_k(x) = s_{k-2}(x) - q_k(x) s_{k-1}(x)$$

$$t_0 = 0,\ t_1 = 1, \forall k \geq 2,\ t_k(x) = t_{k-2}(x) - q_k(x) t_{k-1}(x)$$

Extended Euclidean algorithm for polynomials

✓ **Application.** Find the gcd (monic by convention) of

$$a(x) = x^8 + 4x^7 + 4x^6 + 4x^5 + 4x^4 + 2x^3 + x + 2 \in \mathbb{Z}_5[x]$$

$$b(x) = x^6 + 3x^5 + 4x^4 + 2x^3 + 3x^2 + 2 \in \mathbb{Z}_5[x]$$

k	r_k	q_k
0	$a(x)$	$-$
1	$-$	$b(x)$
2	$2x^5 + x^4 + 2x^2 + 4x + 3$	$x^2 + x + 2$
3	$4x^4 + x^3 + x^2 + x + 2$	$3x$
4	$2x^2 + x + 4$	$3x + 2$
5	0	$2x^2 + 2x + 3$

$$\boxed{\begin{aligned} \gcd(a(x), b(x)) &= 3 \times r_4(x) \\ &= x^2 + 3x + 2 \end{aligned}}$$

Extended Euclidean algorithm for polynomials

- ✓ **Application**. Find the Bézout's coefficients of

$$a(x) = x^8 + 4x^7 + 4x^6 + 4x^5 + 4x^4 + 2x^3 + x + 2 \in \mathbb{Z}_5[x]$$

$$b(x) = x^6 + 3x^5 + 4x^4 + 2x^3 + 3x^2 + 2 \in \mathbb{Z}_5[x]$$

k	s_k	t_k
0	1	0
1	0	1
2	1	$4x^2 + 4x + 3$
3	$2x$	$3x^3 + 3x^2 + x + 1$
4	$4x^2 + x + 1$	$x^4 + 4x + 1$
5	$-$	$-$

$$\boxed{\begin{gathered} r_4(x) = s(x) \times a(x) + t(x) \times b(x) \\ \gcd(a(x), b(x)) = 3 \times r_4(x) \\ s'(x) = 3 \times s(x) = 2x^2 + 3x + 3 \\ t'(x) = 3 \times t(x) = 3x^4 + 3x + 3 \end{gathered}}$$

Finite field

- ❑ **Definition**. A polynomial is irreducible in $\mathbb{F}[x]$ or over the field $\mathbb{F}$ if it is not the product of two polynomials of $\mathbb{F}[x]$ of lower degree

- ✓ **Examples**. $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ but $x^2 + 1$ is not

- ❑ **Proposition**. If $f(x)$ is an irreducible polynomial of degree n over $\mathbb{Z}_p$ then $\mathbb{Z}_p[x]/f(x)$ is a field with p^n elements

- ▪ **Proof**. Based on Bézout's identity for polynomials

$$\forall g(x) \in \mathbb{Z}_p[x],\, g(x) \neq a(x)f(x) \text{ with } a(x) \in \mathbb{Z}_p[x],\, \gcd(f(x), g(x)) = 1$$

$$\Rightarrow \exists s(x), t(x) \in \mathbb{Z}_p[x] \text{ s.t. } s(x)g(x) + t(x)f(x) = 1$$

$$\Leftrightarrow [s(x)g(x)] = [s(x)][g(x)] = [1]$$

- Hence, every nonzero element in $\mathbb{Z}_p[x]/f(x)$ has an inverse

Finite field

- ✓ **Example**. Construct $\mathbb{F}_4$ as $\mathbb{Z}_2[x]/x^2 + x + 1$
- Contains the equivalence classes represented by the 4 possible remainders after dividing any polynomial in $\mathbb{Z}_2[x]$ by $x^2 + x + 1$
- The addition and multiplication tables in the field are given by

$+$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[0]$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[1]$	$[1]$	$[0]$	$[1+x]$	$[x]$
$[x]$	$[x]$	$[1+x]$	$[0]$	$[1]$
$[1+x]$	$[1+x]$	$[x]$	$[1]$	$[0]$

$\times$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[1+x]$
$[x]$	$[0]$	$[x]$	$[1+x]$	$[1]$
$[1+x]$	$[0]$	$[1+x]$	$[1]$	$[x]$

- When the context is clear, we can omit square brackets for the equivalent class and designate it by its class representative

Finite field

- ❑ **Elements as n-tuple**. Any representative of an equivalent class can be represented by an n-tuple with elements in $\mathbb{Z}_p$

$$\left[g(x) = \sum_{i=0}^{n-1} a_i x^i\right] \in \mathbb{Z}_p\,[x]/\,f(x) \leftrightarrow \boldsymbol{a} = \left(a_0, a_1, \ldots, a_{n-1}\right) \in \mathbb{Z}_p^n$$

- ✓ **Example**. In $\mathbb{F}_4$ as $\mathbb{Z}_2[x]/x^2 + x + 1$, this leads to the table

polynomial	2 - tuple
$[0]$	(00)
$[1]$	(10)
$[x]$	(01)
$[1+x]$	(11)

The field can be thought as a vector space of dimension n over $\mathbb{Z}_p$

Finite field

- This method of construction is referred to as *extension of a field* by *adjunction of a root* of an *irreducible* polynomial
- The root is $[x]$ since by definition

$$f([x]) = \left[f(x)\right] = [0]$$

- The n-tuples associated with the powers $[1]$,$[x]$,…,$[x^{n-1}]$ of the adjoined root $[x]$ form a natural (canonical) basis to generate the p^n elements of the field

A finite field of characteristic p is either $\mathbb{Z}_p$ or an extension of $\mathbb{Z}_p$

- The construction method works for infinite fields as well…

$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + \sqrt{2}b : a,b \in \mathbb{Q}\right\}$ by adjoining to $\mathbb{Q}$ a root of $x^2 - 2$

$\mathbb{C} = \left\{a + ib : a,b \in \mathbb{R}\right\}$ by adjoining to $\mathbb{R}$ a root of $x^2 + 1$

Finite field

❑ **Definition**. An element α in a finite field is said to *generate* the field, to be a generator, or a primitive element if

$$\left\{\alpha^i : 0 \leq i \leq n-1\right\} = \mathbb{F}^*$$

✓ **Example**. In $\mathbb{F}_4$ as $\mathbb{Z}_2[x]/x^2 + x + 1$, $\alpha = [x]$ is a generator

polynomial	2 - tuple	power of α
$[0]$	(00)	$\alpha^{-\infty}$
$[1]$	(10)	α^0
$[x]$	(01)	α^1
$[1+x]$	(11)	α^2

$$\boxed{\alpha^{p^n-1} = \alpha^3 = 1}$$

❑ **Proposition**. Every finite field contains a primitive element

Ideal

- ❑ **Definition**. Let $(\mathbb{A},+,\times)$ be a ring. An non-empty set $\mathbb{I}$ of $\mathbb{A}$ is an ideal of the ring if the following axioms are satisfied

$$(\mathbb{I},+) \text{ is an Abelian group with identity element } 0$$

$$\forall i \in \mathbb{I}, \forall a \in \mathbb{A}, i \times a = a \times i \in \mathbb{I}$$

- ❑ **Construction**. Take any non-zero element g of $\mathbb{A}$ and form

$$\mathbb{I} = \{g \times r = r \times g : r \in \mathbb{A}\} \text{ principal ideal generated by } g$$

- But… not all ideals of a ring can be constructed in this way

- ❑ **Definition**. A principal ring $\mathbb{A}$ is a ring where every ideal $\mathbb{I}$ is principal, i.e.,

$$\forall \mathbb{I}, \exists g \in \mathbb{I} \text{ s.t. } \mathbb{I} \text{ is the principal ideal generated by } g$$

Ideal

- ❑ **Proposition**. $\mathbb{F}[x]$ is a principal ideal ring
- ▪ **Proof**. Based on the division algorithm for polynomials
- ❑ **Proposition**. $\mathbb{F}[x]/f(x)$ is a principal ideal ring
- ▪ **Proof**. Based on the division algorithm for polynomials
- ✓ **Example**. Consider $\mathbb{Z}_2[x]/f(x)$ with $f(x) = x^6 + 1$ and the set

$$\mathbb{I} = \left\{0, 1 + x^2 + x^4, x + x^3 + x^5, 1 + x + x^2 + x^3 + x^4 + x^5\right\}$$

- It is easy to show that $\mathbb{I}$ is an ideal of $\mathbb{Z}_2[x]/f(x)$ and that it is the principal ideal generated by $g(x) = 1 + x^2 + x^4$

Ideals are central to the study of cyclic subspaces and play a fundamental role in the design of cyclic codes

Linear codes

Vector space

- ❑ **Definition**. A vector space over a field is a set of elements (vectors) together with two operations such that the following axioms are satisfied

$(\mathbb{V},+)$ is an abelian group with identity element $\boldsymbol{0}$

$$\forall\alpha\in\mathbb{F},\forall\boldsymbol{x}\in\mathbb{V},\ \alpha\cdot\boldsymbol{x}\in\mathbb{V}$$

For the neutral element $1\in\mathbb{F}, 1\cdot\boldsymbol{x}=\boldsymbol{x}$

$$\forall\alpha\in\mathbb{F},\forall\boldsymbol{x},\boldsymbol{y}\in\mathbb{V},\alpha\cdot(\boldsymbol{x}+\boldsymbol{y})=\alpha\cdot\boldsymbol{x}+\alpha\cdot\boldsymbol{y}$$

$$\forall\alpha,\beta\in\mathbb{F},\forall\boldsymbol{x}\in\mathbb{V},(\alpha+\beta)\cdot\boldsymbol{x}=\alpha\cdot\boldsymbol{x}+\beta\cdot\boldsymbol{x}$$

$$\forall\alpha,\beta\in\mathbb{F},\forall\boldsymbol{x}\in\mathbb{V},(\alpha\times\beta)\cdot\boldsymbol{x}=\alpha\times(\beta\cdot\boldsymbol{x})$$

- ✓ **Example.** $(\mathbb{F}_q^N,+,\cdot)$ is a vector space of dimension N

Linear block codes

- **Definition**. An $[N,K]_q$ *linear* block code $\mathcal{C}$ over $\mathbb{F}_q$ is a vector subspace of dimension K of the vector space $\mathbb{F}_q^N$

$$\forall \boldsymbol{x}_i, \boldsymbol{x}_j \in \mathcal{C},\ \forall \alpha, \beta \in \mathbb{F}_q,\ \alpha \boldsymbol{x}_i + \beta \boldsymbol{x}_j \in \mathcal{C}$$

- **Image representation**. K linearly independent vectors chosen as codewords are sufficient to generate the entire code (basis)

The code is the linear map generated by these vectors

- **Minimum Hamming distance**

$$d = \min_{\boldsymbol{x} \in \mathcal{C}^*} w_H(\boldsymbol{x})$$

- **Complexity**. Drastically reduced compared to a code with no internal structure, but still exponential in the code length…

Generator matrix

- **Definition**. The $K \times N$ matrix $\boldsymbol{G}$ whose rows are the K linearly independent codewords chosen as a basis is called generator matrix of the code

- **Encoding**. The encoding function is an injective linear mapping

$$f : \boldsymbol{u} \in \mathbb{F}_q^K \to \boldsymbol{x} = \boldsymbol{u}\boldsymbol{G} = \sum_{i=1}^{K} u_i \boldsymbol{g}_i \in \mathbb{F}_q^N$$

- **Definition**. Two generator matrices $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ generate the same linear block code **if** we can find an invertible $K \times K$ matrix $\boldsymbol{T}$ (i.e., having a nonzero determinant) such that

$$\boldsymbol{G}_1 = \boldsymbol{T}\boldsymbol{G}_2 \Leftrightarrow \boldsymbol{G}_2 = \boldsymbol{T}^{-1}\boldsymbol{G}_1$$

Then the information vectors $\boldsymbol{u}$ and $\boldsymbol{v} = \boldsymbol{u}\boldsymbol{T}$ generate the same codeword

Generator matrix

- ✓ **Example**. A simple [7,4,3] binary code defined by the following generator matrix

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

- Describe the code
- Find the minimum Hamming distance
- Detection and correction capability (under NND)

Systematic encoders

- ❑ **Definition**. Consider an $[N,K]_q$ code. The code possesses a *systematic* encoding if the K information symbols are part of the codewords, meaning that $\boldsymbol{G}$ has a reduced row-echelon (also referred to as canonical) form

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_K & \boldsymbol{P}_{K\times(N-K)} \end{bmatrix}$$

- ✓ **Example**. Show that the previous generator matrix can be put under the following row-reduced echelon form

$$\boldsymbol{G}_r = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Equivalent codes

- **Definition**. Two linear block codes are said to be *equivalent* if their generator matrices are linked by elementary operations on rows and column permutations, i.e., if we can find a $K \times K$ invertible matrix $\boldsymbol{T}$ and a $N \times N$ permutation matrix $\boldsymbol{P}$ such that

$$\boldsymbol{G}_1 = \boldsymbol{T}\boldsymbol{G}_2\boldsymbol{P} \Leftrightarrow \boldsymbol{G}_2 = \boldsymbol{T}^{-1}\boldsymbol{G}_1\boldsymbol{P}$$

- **Proposition**. Every linear block code is equivalent to a linear block code which has a systematic encoding

- **Proof**. Follows from the fact that the Gauss-Jordan elimination with full pivoting is a stable procedure

Duality

❑ **Definition**. Natural (symmetric) scalar product $\mathbb{F}_q^N$

$$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^N \mapsto \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{F}_q = \boldsymbol{x}\boldsymbol{y}^\top = \boldsymbol{y}\boldsymbol{x}^\top = \sum_{i=1}^N x_i y_i \in \mathbb{F}_q$$

- This is a bilinear form, i.e.,

$$f(\alpha\boldsymbol{x} + \beta\boldsymbol{y}, \boldsymbol{z}) = \alpha f(\boldsymbol{x}, \boldsymbol{z}) + \beta f(\boldsymbol{y}, \boldsymbol{z})$$

$$f(\boldsymbol{x}, \alpha\boldsymbol{y} + \beta\boldsymbol{z}) = \alpha f(\boldsymbol{x}, \boldsymbol{y}) + \beta f(\boldsymbol{x}, \boldsymbol{z})$$

- There are some isotropic vectors, i.e., such that

$$\langle \boldsymbol{x}, \boldsymbol{x} \rangle = 0 \text{ and } \boldsymbol{x} \neq \boldsymbol{0}$$

❑ **Definition** (orthogonality).

$$\boxed{\boldsymbol{x} \ \perp \ \boldsymbol{y} \Leftrightarrow \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0}$$

Dual code

- **Definition**. Consider an $[N,K]_q$ code $\mathcal{C}$. The dual code is the set of vectors defined as

$$\mathcal{C}^{\perp} = \left\{\boldsymbol{y} \in \mathbb{F}_q^N : \forall \boldsymbol{x} \in \mathcal{C}, \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0\right\}$$

- **Lemma**. The dual code of a code is the kernel of a linear transformation, i.e.,

$$\boxed{\boldsymbol{y} \in \mathcal{C}^{\perp} \Leftrightarrow \boldsymbol{y}\boldsymbol{G}^{\top} = \boldsymbol{0}_K}$$

- **Theorem**. Let $\mathcal{C}$ be an $[N,K]_q$ code. Then the dual $\mathcal{C}^{\perp}$ is an $[N,N\text{–}K]_q$ code

- **Proposition**. The dual of $\mathcal{C}^{\perp}$ is $\mathcal{C}$

Dual code

- Linearity of the dual induced by linearity of scalar product

$$\forall \boldsymbol{y},\boldsymbol{z} \in \mathcal{C}^{\perp}, \forall \alpha,\beta \in \mathbb{F}_q, \forall \boldsymbol{x} \in \mathcal{C}, \left\langle \alpha\boldsymbol{y}+\beta\boldsymbol{z},\boldsymbol{x}\right\rangle = 0 \Rightarrow \alpha\boldsymbol{y}+\beta\boldsymbol{z} \in \mathcal{C}^{\perp}$$

- **Proof** based on a constructive argument. Assume that the code has a *systematic encoding* and let introduce

$$\boldsymbol{H} = \begin{bmatrix}\boldsymbol{Q}_{(N-K)\times K} & \boldsymbol{I}_{N-K}\end{bmatrix} \text{s.t.} \, \boldsymbol{G}\boldsymbol{H}^{\top} = [\boldsymbol{0}]_{K\times(N-K)}$$

- Double inclusion. First we prove that $span(\mathbf{H}) \subseteq \mathcal{C}^{\perp}$

$$\forall \boldsymbol{y} \in span(\boldsymbol{H}),\, \forall \boldsymbol{x} \in \mathcal{C},\, \left\langle \boldsymbol{x},\boldsymbol{y}\right\rangle = \left\langle \boldsymbol{u}\boldsymbol{G},\boldsymbol{v}\boldsymbol{H}\right\rangle = 0 \Rightarrow \boldsymbol{y} \in \mathcal{C}^{\perp}$$

- Next, we prove that $\mathcal{C}^{\perp} \subseteq span(\mathbf{H})\ ^{\perp}$

$\forall \boldsymbol{x} \in \mathcal{C}^{\perp}$ introduce $\boldsymbol{y} \doteq \boldsymbol{x} - \sum_{i=1}^{N-K} x_{K+i}\boldsymbol{h}_i \Rightarrow (y_{K+1},\ldots,y_N) = \boldsymbol{0}_{N-K}$

Dual code

- Series of implications

$$\sum_{i=1}^{N-K} x_{K+i}\boldsymbol{h}_i \overset{(a)}{\in} \mathcal{C}^{\perp} \overset{(b)}{\Rightarrow} \boldsymbol{y} \in \mathcal{C}^{\perp} \overset{(c)}{\Rightarrow} \boldsymbol{y}\boldsymbol{G}^{\top} = \boldsymbol{0}_K \overset{(d)}{\Rightarrow} [y_1 \cdots y_K] = \mathbf{0}_K$$

(a) by first proven step

(b) due to the linearity of the dual code

(c) by previous lemma

(d) since $\boldsymbol{G}$ is under reduced canonical form

$$\forall \boldsymbol{x} \in \mathcal{C}^{\perp}, \boldsymbol{y} = \boldsymbol{0}_N \Rightarrow \boldsymbol{x} = \sum_{i=1}^{N-K} x_{K+i}\boldsymbol{h}_i \in span(\boldsymbol{H})$$

- **Another proof**. Consider the linear mapping

$$h : \boldsymbol{x} \in \mathbb{F}_q^N \to \boldsymbol{s} = \boldsymbol{x}\boldsymbol{G}^{\top} \in \mathbb{F}_q^K$$

Rank theorem : $\dim \mathbb{F}_q^N = \dim Ker\, h + \dim Im\, h$

Parity check matrix

- **Definition**. A generator matrix $\boldsymbol{H}$ of the dual code is called parity-check matrix of the direct code

- **Kernel representation**. Any linear block code is the kernel of a linear transformation, i.e.,

$$\boxed{\boldsymbol{x} \in \mathcal{C} \Leftrightarrow \boldsymbol{x}\boldsymbol{H}^\top = \boldsymbol{0}_{N-K}}$$

- The $N - K$ resulting equations are called parity-check equations

- The generator matrix $\boldsymbol{G}$ and the parity-check matrix $\boldsymbol{H}$ of a linear block code are linked by the relationship

$$\boxed{\boldsymbol{G}\boldsymbol{H}^\top = [\boldsymbol{0}]_{K\times(N-K)}}$$

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{I}_K & \boldsymbol{P} \end{bmatrix} \Leftrightarrow \boldsymbol{H} = \begin{bmatrix} -\boldsymbol{P}^\top & \boldsymbol{I}_{N-K} \end{bmatrix}$$

Weakly and strictly self dual code

- **Definition**. Let $\mathcal{C}$ be an $[N,K]_q$ code.

  if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ then the code is said weakly self dual

- **Proposition**. A linear code with generator matrix $\boldsymbol{G}$ is weakly self dual if and only if $\boldsymbol{G}\boldsymbol{G}^{\top} = [\mathbf{0}]_{K\times K}$

- **Definition**. Let $\mathcal{C}$ be an $[N,K]_q$ code.

  if $\mathcal{C} = \mathcal{C}^{\perp}$ then the code is said strictly self dual

- **Proposition**. A linear block code is strictly self dual if and only if it is weakly self dual and $K = N/2$

- **Remark**. The extended binary Golay code is strictly self dual

Syndrome

- **Definition**. The vector syndrome is defined as

$$\boxed{\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^{\top}}$$

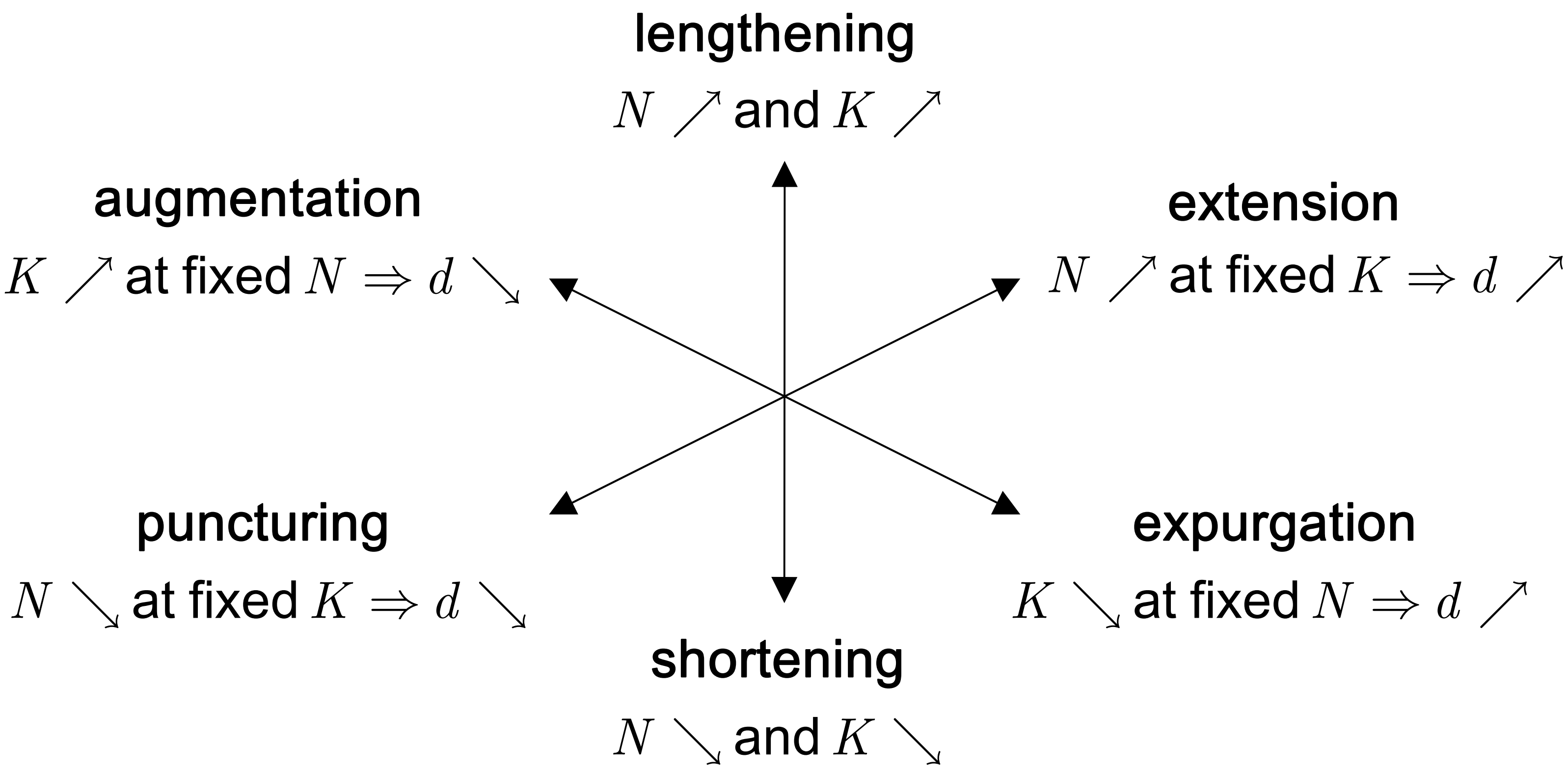
- **Algorithm** (error detection)

```
inputs : $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$, with $\boldsymbol{x}, \boldsymbol{e} \in \mathbb{F}_q^N$, and $\boldsymbol{H}$
compute $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^{\top}$
if $\boldsymbol{s} \neq \boldsymbol{0}_{N-K}$ then declare that an error occurred
```

- **Application**. ARQ coding. Efficient over very noisy channels where correction is not possible

- **Probability of error detection**. See below

Elementary transformations



lengthening

$N \nearrow$ and $K \nearrow$

augmentation

$K \nearrow$ at fixed $N \Rightarrow d \searrow$

extension

$N \nearrow$ at fixed $K \Rightarrow d \nearrow$

puncturing

$N \searrow$ at fixed $K \Rightarrow d \searrow$

expurgation

$K \searrow$ at fixed $N \Rightarrow d \nearrow$

shortening

$N \searrow$ and $K \searrow$

Parity-check matrix and minimum distance

- **Theorem**. Let $\boldsymbol{H}$ be the parity-check matrix of an $[N,K]_q$ code

$$d-1=\max\left\{m \text{ s.t. every submatrix } (N-K)\times m \text{ is of rank } m\right\}$$

- The minimum distance of an $[N,K]_q$ code with a parity-check matrix $\boldsymbol{H}$ is *at least* d if (and only if) any family of $d-1$ (or fewer) column vectors of $\boldsymbol{H}$ is linearly independent
- As a corollary, an $[N,K]_q$ code with parity-check matrix $\boldsymbol{H}$ has minimum distance d if (and only if) any family of $d-1$ (or fewer) column vectors of $\boldsymbol{H}$ is linearly independent and if at least one family of d column vectors of $\boldsymbol{H}$ is linearly dependent
- **Proof**. Direct consequence of the kernel representation of the code: A codeword of weight i exists if and only if i column vectors of $\boldsymbol{H}$ sum to the zero vector

Singleton bound

- **Proposition**. The parameters of an $[N,K,d]_q$ code satisfy the following inequality

$$d \leq N - K + 1$$

- **Proof**. The rank of matrix $\boldsymbol{H}$ being at most $N - K$, it must exist a family of $N - K + 1$ column vectors of $\boldsymbol{H}$ linearly dependent, which limits the minimal distance of the code to $N - K + 1$

- Any linear code whose minimum Hamming distance meets this bound is said *maximum distance separable* (MDS)

[1] R.C. Singleton, IEEE IT, vol. 10, 1964

GV bound

- **Proposition**. There exists a linear code over $\mathbb{F}_q$ of length N and minimal distance d with dimension *at least* equal to K (or equivalently *at most* $N - K$ parity symbols) provided that

$$V_q(N-1, d-2) < q^{N-K}$$

- **Note**. This weaker version also exists

$$V_q(N, d-1) \leq q^{N-K+1}$$

- **Proof**. (constructive) Recursively construct the parity-check matrix of dimension $(N - K) \times N$ such that every family of $d - 1$ column vectors chosen among $q^{N-K} - 1$ is linearly independent. By previous theorem, the minimal distance will be at least d

[1] E. Gilbert, BSTJ, vol. 31, 1952

GV bound

- **Recursion**. Assume that i columns have already been chosen such that every family of d – 1 columns is linearly independent
- How to choose the column $i + 1$ so as to preserve the property that every family of d – 1 column is linearly independent?
- Equivalent to evaluate the number of linear combinations of the new column with the d – 2 (or fewer) already chosen columns

$$\underbrace{\binom{i}{1}(q-1)}_{\text{with } 1 \text{ column}} + \underbrace{\binom{i}{2}(q-1)^2}_{\text{with } 2 \text{ columns}} + ... + \underbrace{\binom{i}{d-2}(q-1)^{d-2}}_{\text{with } d-2 \text{ columns}}$$

- As long as this number is less that q^{N-K} -1, we are sure that we can still choose the column $i + 1$ so that every family of d – 1 (or fewer) columns of the parity-check matrix is linearly independent
- We assume $i = N$ – 1 and search if we could add column N
- Possible if and only if the previous inequality is satisfied

Hamming codes

- **Definition**. A Hamming code of order m over $\mathbb{F}_q$ is linear code with the following parameters

$$\left[N = \frac{q^m - 1}{q - 1}, K = N - m,\ d = 3\right]$$

- **Construction**. The designed distance must be 3 with the maximum possible code length. The columns of the parity check matrix must be non-zero and no two columns must be scalar multiple of each other

- **Proposition**. Hamming codes are *perfect* codes

- **Remarks**. The dual of extended Hamming codes are the first-order Reed-Müller codes. The dual of Hamming codes are called simplex codes (shortened first-order Reed-Müller codes)

Decoding single-error correcting codes

- **Algorithm** (error correction)

```
inputs : $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$, with $\boldsymbol{x}, \boldsymbol{e} \in \mathbb{F}_q^N$, and $\boldsymbol{H}$
compute $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^\top$
if $\boldsymbol{s} = \boldsymbol{0}_{N-K}$ then decode $\hat{\boldsymbol{x}} = \boldsymbol{y}$
else compare $\boldsymbol{s}^\top$ with the column vectors of $\boldsymbol{H}$
   if $\exists j$ and $\alpha \in \mathbb{F}_q^*$ s.t. $\boldsymbol{s}^\top = \alpha\boldsymbol{h}^j$ then infer that $\boldsymbol{e}$ has $\alpha$ in position $j$
   and $0$'s elsewhere, and decode $\hat{\boldsymbol{x}} = \boldsymbol{y} - \boldsymbol{e}$
   else more than one error has occured
```

- **Note**. This is an incomplete decoding

Standard array decoding and syndrome decoding

❑ See exercise