LECTURE 2
RANDOM CODES

Summer School: *Introduction to Quantum-Safe Cryptography*

Thomas Debris-Alazard

July 02, 2024

Inria, École Polytechnique

Goal:

Building cryptographic primitives whose security relies on

hardness of the average decoding problem

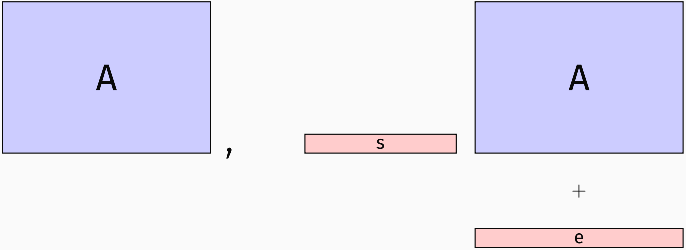
How does this problem behave as function of its parameters?

e.g. what is the number of solutions?

- A Quick Recap of Lecture 1
- Model of Random Codes
- Weight Distribution of Random Codes
- Minimum Distance of Random Codes

A QUICK RECAP

Shannon (1948/1949) introduced the following problem (decoding),



Aim:

Recover s

There are cryptosystems whose security relies on this problem: code-based cryptography (McEliece 78, Alekhnovich 03, etc. . .)

$\mathcal{C}$ be an $[n,k]_q$-code, *i.e.*, subspace of $\mathbb{F}_q^n$ with dimension k

n length ; k dimension

$$\mathcal{C} \stackrel{\text{def}}{=} \left\{ \mathbf{m}\mathbf{G} : \ \mathbf{m} \in \mathbb{F}_q^k \right\}$$

$\mathbf{G} \in \mathbb{F}_q^{k \times n}$ rank k : generator matrix

$$\mathcal{C} \stackrel{\text{def}}{=} \left\{ \mathbf{c} \in \mathbb{F}_q^n : \ \mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0} \right\}$$

$\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ rank $n-k$: parity-check matrix

DP(n, q, R, τ), $k \stackrel{\text{def}}{=} Rn$ and $t \stackrel{\text{def}}{=} \tau n$

Sample: $\boxed{\mathbf{H}} \longleftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k)\times n}\right)$, $\boxed{\mathbf{x}} \longleftarrow \mathrm{Unif}\left(\mathbf{z} \ : \ |\mathbf{z}| = t\right)$

Input: $\boxed{\mathbf{H}}$, $\boxed{\mathbf{s}} = \boxed{\mathbf{H}}\,\boxed{\mathbf{x}}$

Recover: $\boxed{\mathbf{e}}$ s.t $\boxed{\mathbf{H}}\,\boxed{\mathbf{e}} = \boxed{\mathbf{s}}$ and $\boxed{\mathbf{e}} \in \left\{\mathbf{z} \ : \ |\mathbf{z}| = t\right\}$

Average Decoding Problem (DP)

- *Sample*: $\mathbf{H} \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k)\times n}\right)$, $\mathbf{x} \leftarrow \mathrm{Unif}\left(\left\{\mathbf{z} \in \mathbb{F}_q^n : \ |\mathbf{z}| = t\right\}\right)$,
- **Input:** $(\mathbf{H}, \mathbf{H}\mathbf{x}^{\mathsf{T}})$,
- **Output:** $\mathbf{e} \in \mathbb{F}_q^n$ such that $\begin{cases} \mathbf{H}\mathbf{e}^{\mathsf{T}} = \mathbf{H}\mathbf{x}^{\mathsf{T}} \\ |\mathbf{e}| = t \end{cases}$

A trivial algorithm:

$$\text{pick } \mathbf{e} \in \left\{\mathbf{z} \in \mathbb{F}_q^n : \ |\mathbf{z}| = t\right\} \ \text{ and test if } \ \mathbf{H}\mathbf{e}^{\mathsf{T}} = \mathbf{H}\mathbf{x}^{\mathsf{T}}$$

Average Decoding Problem (DP)

- *Sample*: $\mathbf{H} \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k)\times n}\right)$, $\mathbf{x} \leftarrow \mathrm{Unif}\left(\left\{\mathbf{z} \in \mathbb{F}_q^n : \ |\mathbf{z}| = t\right\}\right)$,
- **Input:** $(\mathbf{H}, \mathbf{H}\mathbf{x}^{\intercal})$,
- **Output:** $\mathbf{e} \in \mathbb{F}_q^n$ such that $\begin{cases} \mathbf{H}\mathbf{e}^{\intercal} = \mathbf{H}\mathbf{x}^{\intercal} \\ |\mathbf{e}| = t \end{cases}$

A trivial algorithm:

$$\text{pick } \mathbf{e} \in \left\{\mathbf{z} \in \mathbb{F}_q^n : \ |\mathbf{z}| = t\right\} \quad \text{and test if} \quad \mathbf{H}\mathbf{e}^{\intercal} = \mathbf{H}\mathbf{x}^{\intercal}$$

- If one solution, probability of success: $\frac{1}{\sharp\left\{\mathbf{z}\in\mathbb{F}_q^n :\ |\mathbf{z}|=t\right\}}$
- **If N solutions**, probability of success: $\frac{N}{\sharp\left\{\mathbf{z}\in\mathbb{F}_q^n :\ |\mathbf{z}|=t\right\}}$

What is the value of N?

To compute N: use the theory of random codes!

Random Code:

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^n : \ \mathbf{H}\mathbf{c}^{\mathsf{T}} = \mathbf{0} \right\} \quad \text{such that} \quad \mathbf{H} \longleftarrow \mathbf{Unif}\left(\mathbb{F}_q^{(n-k)\times n} \right)$$

defines what is called a random code!

MODEL OF RANDOM CODES

And generator matrices?

Random Code(s):

- $\mathcal{C} = \left\{ \mathbf{m}\mathbf{G}_u : \mathbf{m} \in \mathbb{F}_q^k \right\}$ where $\mathbf{G}_u \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{k \times n}\right)$

or,

- $\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^n : \mathbf{H}_u \mathbf{c}^{\mathsf{T}} = \mathbf{0} \right\}$ where $\mathbf{H}_u \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k) \times n}\right)$

Are these models equivalent? Do they define a random $[n, k]_q$-code?

Random Code(s):

- $\mathcal{C} = \left\{ \mathbf{m}\mathbf{G}_u \ : \ \mathbf{m} \in \mathbb{F}_q^k \right\}$ where $\mathbf{G}_u \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{k \times n}\right)$

  $\longrightarrow$ $\dim \mathcal{C} \leq k$ as $\mathrm{rank}(\mathbf{G}_u) \leq k$

- $\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^n \ : \ \mathbf{H}_u \mathbf{c}^{\mathsf{T}} = \mathbf{0} \right\}$ where $\mathbf{H}_u \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k) \times n}\right)$

  $\longrightarrow$ $\dim \mathcal{C} \geq k$ as $\mathrm{rank}(\mathbf{H}_u) \leq n - k$

Both models do not seem to be equivalent. . . (Spoiler: they “are”!)

Statistical Distance:

Let X and Y be random variables,

$$\Delta(X, Y) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{a \in \mathcal{E}} |\mathbb{P}(X = a) - \mathbb{P}(Y = a)|$$

A Crucial Property: Data Processing Inequality

$$\Delta(f(X), f(Y)) \leq \Delta(X, Y)$$

Consequence: $\forall \mathcal{A}$ algorithm

$$\left|\mathbb{P}_X\left(\mathcal{A}(X) = \text{“success”}\right) - \mathbb{P}_Y\left(\mathcal{A}(Y) = \text{“success”}\right)\right| \leq \Delta(X, Y).$$

G_u or H_u-models $\iff$ draw uniformly an $[n,k]$-code:

$\mathsf{G}_k \in \mathbb{F}_q^{k\times n}$ $\left(\mathsf{H}_{n-k} \in \mathbb{F}_q^{(n-k)\times n}\right)$ be uniform of rank k (*resp.* $n-k$):

$$\Delta\left(\mathsf{G}_u, \mathsf{G}_k\right) = O\left(q^{-(n-k)}\right) \quad \left(\textit{resp. } \Delta\left(\mathsf{H}_u, \mathsf{H}_{n-k}\right) = O\left(q^{-k}\right)\right)$$

Computation are the same in G_u and H_u-models:

Let $\mathcal{E}$ be a set of codes (defined as an event). We have,

$$\left|\mathbb{P}_{\mathsf{G}_u}(\mathcal{E}) - \mathbb{P}_{\mathsf{H}_u}(\mathcal{E})\right| = O\left(q^{-\min(k,n-k)}\right).$$

$\mathbf{G}_u$ or $\mathbf{H}_u$-models $\iff$ draw uniformly an $[n,k]$-code:

$\mathbf{G}_k \in \mathbb{F}_q^{k\times n}$ $\left(\mathbf{H}_{n-k} \in \mathbb{F}_q^{(n-k)\times n}\right)$ be uniform of rank k (*resp.* $n-k$):

$$\Delta\left(\mathbf{G}_u, \mathbf{G}_k\right) = O\left(q^{-(n-k)}\right) \quad \left(\textit{resp. } \Delta\left(\mathbf{H}_u, \mathbf{H}_{n-k}\right) = O\left(q^{-k}\right)\right)$$

Computation are the same in $\mathbf{G}_u$ and $\mathbf{H}_u$-models:

Let $\mathcal{E}$ be a set of codes (defined as an event). We have,

$$\left|\mathbb{P}_{\mathbf{G}_u}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_u}(\mathcal{E})\right| = O\left(q^{-\min(k,n-k)}\right).$$

Proof:

$$\left|\mathbb{P}_{\mathbf{G}_u}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_u}(\mathcal{E})\right| \leq \left|\mathbb{P}_{\mathbf{G}_u}(\mathcal{E}) - \mathbb{P}_{\mathbf{G}_k}(\mathcal{E})\right| + \left|\mathbb{P}_{\mathbf{H}_{n-k}}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_u}(\mathcal{E}) + \left|\mathbb{P}_{\mathbf{G}_k}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_{n-k}}(\mathcal{E})\right|\right.$$

- $\left|\mathbb{P}_{\mathbf{G}_u}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_u}(\mathcal{E})\right|$ and $\left|\mathbb{P}_{\mathbf{H}_{n-k}}(\mathcal{E}) - \mathbb{P}_{\mathbf{H}_u}(\mathcal{E})\right|$ are $O(q^{-\min(k,n-k)})$ because of the statistical distance
- $\mathbb{P}_{\mathbf{G}_k}(\mathcal{E}) = \mathbb{P}_{\mathbf{H}_{n-k}}(\mathcal{E})$ because codes defined by $\mathbf{G}_k$ and $\mathbf{H}_{n-k}$ have the same distribution: uniform over $[n,k]_q$-codes.

$\mathrm{DP}'(n,q,R,\tau)$. **Let** $k \stackrel{\text{def}}{=} \lfloor Rn \rfloor$ **and** $t \stackrel{\text{def}}{=} \lfloor \tau n \rfloor$

- **Input:** $(\mathbf{G}_u, \mathbf{y} \stackrel{\text{def}}{=} \mathbf{s}\mathbf{G}_u + \mathbf{x})$ where $\mathbf{G}_u$, $\mathbf{s}$ and $\mathbf{x}$ are uniformly distributed over $\mathbb{F}_q^{k\times n}$, $\mathbb{F}_q^k$ and words of Hamming weight t.
- **Output:** an error $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t such that $\mathbf{y} - \mathbf{e} = \mathbf{m}\mathbf{G}_u$ for some $\mathbf{m} \in \mathbb{F}_q^k$.

Exercise Session 1: any algorithm solving $\mathrm{DP}'(n,q,R,\tau)$ with probability ε can be turned

into an algorithm solving $\mathrm{DP}(n,q,R,\tau)$ with probability $\geq \varepsilon - O(q^{-\min(k,n-k)})$

$\Big($and reciprocally$\Big)$

$\longrightarrow$ *Used arguments were the same: statistical distance, closeness with matrices of fixed rank*

WEIGHT DISTRIBUTION

Our Goal:

Given $\mathbf{H}\mathbf{x}^\top$, we want to estimate:

$$N = \sharp \left\{ \mathbf{e} \in \mathbb{F}_q^n : \begin{array}{c} \mathbf{H}\mathbf{e}^\top = \mathbf{H}\mathbf{x}^\top \\ \text{and} \\ |\mathbf{e}| = t \end{array} \right\}$$

Fundamental Equality:

Given, $\mathbf{s}$ and $\mathbf{y} \neq \mathbf{0}$ (fixed), $\mathbf{H}_u \leftarrow \mathrm{Unif}\left(\mathbb{F}_q^{(n-k)\times n}\right)$, then:

$$\mathbb{P}_{\mathbf{H}_u}\left(\mathbf{H}_u \mathbf{y}^\intercal = \mathbf{s}^\top\right) = \frac{1}{q^{n-k}}$$

Fundamental Equality:

Given, $\mathbf{s}$ and $\mathbf{y} \neq \mathbf{0}$ (fixed), $\mathbf{H}_u \leftarrow \text{Unif}\left(\mathbb{F}_q^{(n-k)\times n}\right)$, then:

$$\mathbb{P}_{\mathbf{H}_u}\left(\mathbf{H}_u\mathbf{y}^\intercal = \mathbf{s}^\top\right) = \frac{1}{q^{n-k}}$$

Proof:

$\mathbf{y} \neq 0$: there exists $j_0 \in [1,n]$ such that $y_{j_0} \neq 0$. As $\mathbb{F}_q$ is a field, we write $\mathbf{H}_u\mathbf{y}^\top = \mathbf{s}^\top$ as

$$\forall i \in [1,n-k], \quad h_{i,j_0} = \frac{1}{y_{j_0}}\left(s_i - \sum_{j\neq j_0} y_j h_{i,j}\right)$$

Above $n-k$ equations are true with probability $1/q$ as the $h_{j,i}$ are uniform and independent.

Lattice analogue: $\frac{1}{q^{n-k}} = \frac{q^k}{q^n} = \frac{\sharp\mathcal{C}}{\sharp\mathbb{F}_q^n}$ *plays the role of* $\frac{1}{|\Lambda|}$

EXPECTED NUMBER OF SOLUTIONS IN DP

Given $\left(\mathbf{H}_u, \mathbf{H}_u\mathbf{x}^\top \text{ where } |\mathbf{x}| = t\right)$, we are ready to compute:

$$N\left(\mathbf{H}_u, \mathbf{H}_u\mathbf{x}^\top, t\right) = \sharp\left\{\mathbf{e} \in \mathbb{F}_q^n \;:\; |\mathbf{e}| = t \text{ and } \mathbf{H}_u\mathbf{e}^\intercal = \mathbf{H}_u\mathbf{x}^\top\right\}.$$

Proposition:

We have,

$$\forall t > 0,\;\; \mathbb{E}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{H}_u\mathbf{x}^\top, t\right)\right) = 1 + \frac{\sharp\left\{\mathbf{e}\in\mathbb{F}_q^n : |\mathbf{e}|=t\right\} - 1}{q^{n-k}} = 1 + \frac{\binom{n}{t}(q-1)^t - 1}{q^{n-k}}$$

Proof.

$$N\left(\mathbf{H}_u, \mathbf{H}_u\mathbf{x}^\top, t\right) = \sum_{\substack{\mathbf{e}:\; |\mathbf{e}|=t \\ \mathbf{e}\neq\mathbf{x}}} 1_{\{\mathbf{H}_u(\mathbf{e}-\mathbf{x})^\top = \mathbf{0}\}} + 1$$

We conclude by linearity of the expectation and the probability given in the previous slide. □

Proposition:

Given any fixed $\mathbf{s} \in \mathbb{F}_q^{n-k}$, we have

$$\forall t > 0,\;\; \mathbb{E}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{s}, t\right)\right) = \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

$\longrightarrow$ When $\mathbf{s} = \mathbf{0}$: average number of codewords of weight t

$$\sharp \left\{ \mathbf{e} \in \mathbb{F}_q^n : \ |\mathbf{e}| = t \right\} = \binom{n}{t}(q-1)^t$$

$$\binom{n}{t}(q-1)^t = \Theta\left(\frac{1}{n}\right) \ q^{n \cdot h_q\left(\frac{t}{n}\right)}$$

$$h_q(x) \stackrel{\text{def}}{=} -x \log_q\left(\frac{x}{q-1}\right) - (1-x)\log_q(1-x) \quad (q\text{-ary entropy})$$

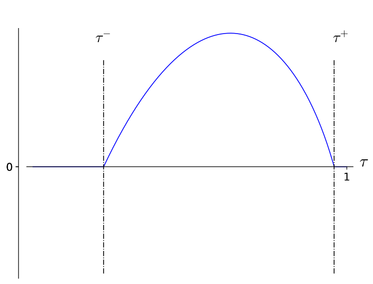
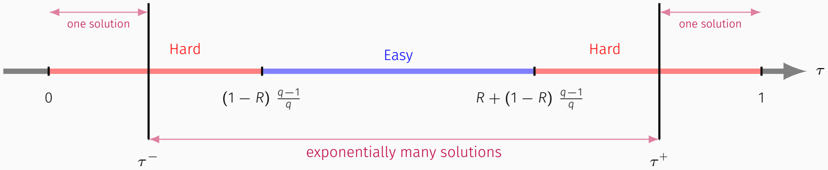


Figure 1: $\lim_{n \to +\infty} \frac{1}{n} \log_q \mathbb{E}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{H}_u \mathbf{x}^\top, t\right)\right)$ where $|\mathbf{x}| = t$, $q = 3$, $k/n = 1/4$ as function of $\tau = t/n$.

HARDNESS OF DP?



In what follows: we will focus on

$$N\left(\mathbf{H}_u, \mathbf{s}, t\right) = \sharp \left\{ \mathbf{e} \in \mathbb{F}_q^n : \ |\mathbf{e}| = t \text{ and } \mathbf{H}_u \mathbf{e}^\top = \mathbf{s}^\top \right\}$$

- $\mathbf{s}$ is fixed an independent of $\mathbf{H}_u$
- $N\left(\mathbf{H}_u, \mathbf{s}, t\right)$ is a random variable (according to $\mathbf{H}_u$) be defined as

$$N\left(\mathbf{H}_u, \mathbf{s}, t\right) = \sum_{\mathbf{e}:\ |\mathbf{e}|=t} 1_{\left\{\mathbf{H}_u \mathbf{e}^\top = \mathbf{s}^\top\right\}}$$

$\longrightarrow$ The number of solutions of DP as distance t behaves as $1 + N\left(\mathbf{H}_u, \mathbf{s}, t\right)$

For now, only $\mathbb{E}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{s}, t\right)\right) = \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$ is known

where $N(\mathbf{H}_u, \mathbf{H}_u, t) = \sharp\left\{\mathbf{e} \in \mathbb{F}_q^n \ : \ |\mathbf{e}| = t \text{ and } \mathbf{H}_u \mathbf{e}^{\mathsf{T}} = \mathbf{s}^{\top}\right\}$.

Be more precise?

First Moment Technique:

For any $a > 0$,

$$\mathbb{P}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{s}, t\right) > a\right) \leq \frac{1}{a} \cdot \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

Proof.

By Markov inequality: $\mathbb{P}_{\mathbf{H}_u}\left(N\left(\mathbf{H}_u, \mathbf{s}, t\right) > a\right) \leq \frac{1}{a} \cdot \mathbb{E}_{\mathbf{H}_u}\left(N(\mathbf{H}_u, t)\right) = \frac{1}{a} \cdot \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$ $\square$

Issue:

$$\mathbb{P}_{\mathbf{H}_u}\left(N(\mathbf{H}_u, \mathbf{s}, t) > a\right) \leq \frac{1}{a} \cdot \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

$\longrightarrow$ We can only deduce that $N(\mathbf{H}_u, \mathbf{s}, t) > a$ is unlikely **if** $a \gg \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$

Could we know $N(\mathbf{H}_u, \mathbf{s}, t)$ ***with accuracy?***

$\longrightarrow$ Yes! We used Markov inequality which is a very crude concentration inequality...

Proposition (admitted):

Let $\mathbf{s} \in \mathbb{F}_q^{n-k}$. For any $a > 0$, we have,

$$\mathbb{P}_{\mathbf{H}_u}\left(\left| N_t(\mathbf{H}_u, \mathbf{s}, t) - \frac{\binom{n}{t}(q-1)^t}{q^{n-k}} \right| \geq a \right) \leq \frac{q-1}{a^2} \cdot \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

$$\textit{Suppose that } \frac{\binom{n}{t}(q-1)^t}{q^{n-k}} = 2^{\Omega(n)}$$

$\longrightarrow$ We can choose $a = \left(\frac{\binom{n}{t}(q-1)^t}{q^{n-k}} \right)^{3/4} = 2^{-\Omega(n)} \cdot \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$ and then

we deduce that $N_t(\mathbf{H}_u, \mathbf{s}, t) = \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}(1 + o(1))$ with probability exponentially close to one

MINIMUM DISTANCE

Given $\mathbf{H}$ be a parity-check matrix. The number of codewords of weight t is given by

$$\sharp \left\{ \mathbf{x} \in \mathbb{F}_q^n : \ |\mathbf{x}| = t \ \text{ and } \ \mathbf{H}\mathbf{x}^\top = \mathbf{0} \right\}$$

By choosing $\mathbf{H}$ uniformly at random:

$$\mathbb{E}_{\mathbf{H}_u} \left(\sharp \left\{ \mathbf{x} \in \mathbb{F}_q^n : \ |\mathbf{x}| = t \ \text{ and } \ \mathbf{H}_u \mathbf{x}^\top = \mathbf{0} \right\} \right) = \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

$\longrightarrow$ We expect that the the minimum distance of a random code is given by

the minimum t such that

$$\frac{\binom{n}{t}(q-1)^t}{q^{n-k}} \geq 1$$

Gilbert-Varshamov Radius:

Given q, n, k: Gilbert-Varshamov radius t_{GV} is the smallest t such that:

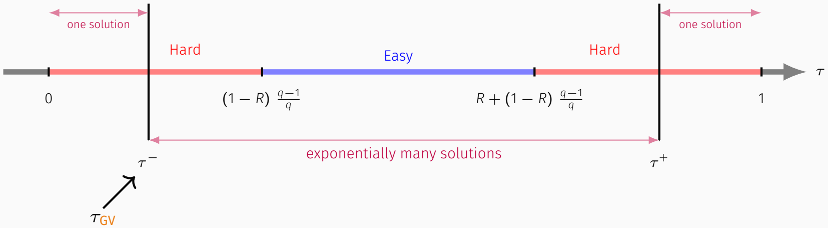
$$\binom{n}{t}(q-1)^t \geq q^{n-k} \iff q^k \cdot \binom{n}{t}(q-1)^t \geq q^n$$

Asymptotic Behaviour:

Given q, n, k where $k/n = R$,

$$\frac{t_{\mathrm{GV}}}{n} \underset{n \to +\infty}{=} \underbrace{h_q^{-1}(1-R)}_{\stackrel{\text{def}}{=} \tau_{\mathrm{GV}}}(1+o(1))$$

The Gilbert-Varshamov radius gives the boundary where DP *admits one solution (with exponentially close to one probability) and exponentially many solutions*



The Gilbert-Varshamov radius gives the minimum distance of a random code

Proposition

Let $\varepsilon > 0$. Given $\mathcal{C}$ with parity-check matrix $\mathbf{H}$. Suppose that $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ is uniformly chosen. Then,

$$\mathbb{P}_{\mathbf{H}}\left((1-\varepsilon)\cdot\tau_{\mathrm{GV}} \leq \frac{d_{\min}(\mathcal{C})}{n} \leq (1+\varepsilon)\cdot\tau_{\mathrm{GV}}\right) \geq 1 - q^{-\alpha n} \quad \text{where} \quad \alpha > 0.$$

Hamming Ball of center $\mathbf{x} \in \mathbb{F}_q^n$ and radius r: $\mathcal{B}_{\mathrm{H}}(\mathbf{c}, r) \stackrel{\text{def}}{=} \left\{\mathbf{y} \in \mathbb{F}_q^n : |\mathbf{y}-\mathbf{x}| \leq r\right\}$

Proposition:

For any $[n,k]_q$-code $\mathcal{C}$ with minimum distance d,

$$\forall \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \quad \mathbf{c} \neq \mathbf{c}' \implies \mathcal{B}_{\mathrm{H}}\left(\mathbf{c}, \left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor\right) \bigcap \mathcal{B}_{\mathrm{H}}\left(\mathbf{c}', \left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor\right) = \emptyset$$

$\longrightarrow$ The $\mathbf{c}+\mathbf{e}$ are distinct when $|\mathbf{e}| < d_{\min}(\mathcal{C})/2$ and $\mathbf{c} \in \mathcal{C}$

Be Careful:

Do not conclude that the “unique decoding regime” is given for errors of Hamming weight $< d_{\min}(\mathcal{C})/2$

$\longrightarrow$ For random codes the situation is extremely different!

For a random code: $d_{\min}(\mathcal{C}) = t_{\mathsf{GV}}$ with probability exponentially close to 1

$\mathcal{C}$ be a random code:

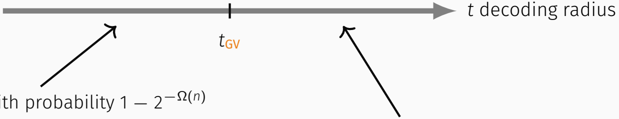
$$\forall \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \quad \mathbf{c} \neq \mathbf{c}': \quad \mathcal{B}_{\mathrm{H}}\left(\mathbf{c}, t_{\mathsf{GV}}\right) \bigcap \mathcal{B}_{\mathrm{H}}\left(\mathbf{c}', t_{\mathsf{GV}}\right) \approx \emptyset$$

$\longrightarrow$ **Not $\frac{t_{\mathsf{GV}}}{2}$!**

- We have defined the model of random codes (via generator or parity-check point of view)
- We have computed the average number (over codes) of solutions of $\mathrm{DP}(q, n, k, t)$ given by

$$1 + \frac{\binom{n}{t}(q-1)^t - 1}{q^{n-k}}$$

- An important quantity: Gilbert-Varshamov radius t_{GV} as function of q, n, k
  - $t_{\mathrm{GV}}/n = h_q^{-1}(1 - R)$ where $R = k/n$ and h_q the q-ary entropy
  - The minimum distance of a random code is given by $\approx t_{\mathrm{GV}}$ with probability exponentially close to one
  - Regarding the number of solutions of DP:



one solution with probability $1 - 2^{-\Omega(n)}$

exponentially many solutions

there are $\frac{\binom{n}{t}(q-1)^t}{q^{n-k}}(1 + o(1))$ solutions with probability $1 - 2^{-\Omega(n)}$