POST-QUANTUM CRYPTOGRAPHY - CODES
STARTING EXERCISES

1. Basic Exercises on Codes

In what follows, $|\cdot|$ will denote the Hamming weight, namely

$$\forall \mathbf{x} \in \mathbb{F}_q^k, \quad |\mathbf{x}| \stackrel{\text{def}}{=} \sharp \{i \in [\![1,n]\!],\ x_i \neq 0\}.$$

Exercise 1. Give the dimension of the following linear codes:

1. $\{(f(x_1),\ldots,f(x_n)) : f \in \mathbb{F}_q[X] \text{ and } \deg(f) < k\}$ where the x_i's are distinct elements of $\mathbb{F}_q$,
2. $\{(\mathbf{u},\mathbf{u}+\mathbf{v}) : \mathbf{u} \in U \text{ and } \mathbf{v} \in V\}$ where U (*resp.* V) is an $[n,k_U]_q$-code (*resp.* $[n,k_V]_q$-code).

Exercise 2. *Let* $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ *be a generator matrix of some code* $\mathcal{C}$. *Let* $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *of rank* $n-k$ *such that* $\mathbf{G}\mathbf{H}^\intercal = \mathbf{0}$. *Show that* $\mathbf{H}$ *is a parity-check matrix of* $\mathcal{C}$.

Exercise 3. Give the minimum distance of the following codes:

1. $\{(f(x_1),\ldots,f(x_n)) : f \in \mathbb{F}_q[X] \text{ and } \deg(f) < k\}$ where the x_i's are distinct elements of $\mathbb{F}_q$.
2. $\{(\mathbf{u},\mathbf{u}+\mathbf{v}) : \mathbf{u} \in U \text{ and } \mathbf{v} \in V\}$ where U (*resp.* V) is a code of length n over $\mathbb{F}_q$ and minimum distance d_U (*resp.* d_V).
3. The Hamming code of length 2^r-1, namely the code which admits a parity check matrix $\mathbf{H} \in \mathbb{F}_q^{r\times(2^r-1)} \stackrel{\text{def}}{=} (\mathbf{x}^\intercal)_{\mathbf{x}\in\mathbb{F}_2^r\setminus\{\mathbf{0}\}}$.

   Hint: *A code has minimum distance* d *if and only if for some parity-check matrix* $\mathbf{H}$ *every* $(d-1)$*-tuple of columns are linearly independent and there is at least one linearly linked* d*–tuple of columns.*

Exercise 4. *Let* $\mathbf{H}$ *be a parity-check matrix of a code* $\mathcal{C}$ *of minimum distance* d. *Show that the* $\mathbf{H}\mathbf{e}^\intercal$*'s are distinct when* $|\mathbf{e}| \leq \frac{d-1}{2}$.

Exercise 5. *Let* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *be a code of minimum distance* d *and* $t > n - \frac{d}{2}$. *Show that there exists at most one codeword* $\mathbf{c} \in \mathcal{C}$ *of weight* t.

Exercise 6. *Let us introduce the following problems*

> **Problem 1** (Noisy Codeword Decoding)**.** *Given* $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ *of rank* k, $t \in [\![0,n]\!]$, $\mathbf{y} \in \mathbb{F}_q^n$ *where* $\mathbf{y} = \mathbf{c}+\mathbf{e}$ *with* $\mathbf{c} = \mathbf{m}\mathbf{G}$ *for some* $\mathbf{m} \in \mathbb{F}_q^k$ *and* $|\mathbf{e}| = t$, *find* $\mathbf{e}$.
>
> **Problem 2** (Syndrome Decoding)**.** *Given* $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *of rank* $n-k$, $t \in [\![0,n]\!]$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ *where* $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$ *with* $|\mathbf{e}| = t$, *find* $\mathbf{e}$.

Show that any solver of Problem 2 (resp. *1) can be turned in polynomial time into an algorithm solving Problem 1* (resp. *2).*

Exercise 7. *Recall that*

$$\mathsf{GRS}_k(\mathbf{x},\mathbf{z}) \stackrel{def}{=} \{(z_1 f(x_1),\dots,z_n f(x_n)) \ : \ f \in \mathbb{F}_q[X] \text{ and } \deg(f) < k\}.$$

where $\mathbf{z} \in (\mathbb{F}_q^\star)^n$ *and* $\mathbf{x}$ *be an* n*-tuple of pairwise distinct elements of* $\mathbb{F}_q$ *(in particular* $n \leq q$*) and* $k \leq n$*.*

Show that $\mathsf{GRS}_k(\mathbf{x},\mathbf{z})^* = \mathsf{GRS}_{n-k}(\mathbf{x},\mathbf{z}')$ *where* $z_i' = \frac{1}{z_i \prod_{j\neq i}(x_i - x_j)}$*. Deduce that* $\mathsf{GRS}_k(\mathbf{x},\mathbf{z})$ *has a parity-check matrix of the following form:*

$$\mathbf{H} \stackrel{def}{=} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ x_1^{n-k-1} & x_2^{n-k-1} & \cdots & x_n^{n-k-1} \end{pmatrix} \begin{pmatrix} z_1' & & & 0 \\ & z_2' & & \\ & & \ddots & \\ 0 & & & z_n' \end{pmatrix}$$

Exercise 8. *Describe how the public-key encryption scheme of McEliece works with generator matrices.*

Exercise 9. *Let us define the problem* DDP *as*

Problem 3 (Decision Decoding Problem - $\mathsf{DDP}(n,q,R,\tau)$)**.** *Let* $k \stackrel{def}{=} \lfloor Rn \rfloor$ *and* $t \stackrel{def}{=} \lfloor \tau n \rfloor$*.*

- *Distributions:*
  - $\mathscr{D}_0$ *:* $(\mathbf{H},\mathbf{s})$ *be uniformly distributed over* $\mathbb{F}_q^{(n-k)\times n} \times \mathbb{F}_q^{n-k}$*.*
  - $\mathscr{D}_1$ *:* $(\mathbf{H},\mathbf{x}\mathbf{H}^\mathsf{T})$ *where* $\mathbf{H}$ *(resp.* $\mathbf{x}$*) being uniformly distributed over* $\mathbb{F}_q^{(n-k)\times n}$ *(resp. words of Hamming weight* t*).*
- *Input:* $(\mathbf{H},\mathbf{s})$ *distributed according to* $\mathscr{D}_b$ *where* $b \in \{0,1\}$ *is uniform,*
- *Decision:* $b' \in \{0,1\}$*.*

Let us introduce the following definitions,

Definition 1. *The* $\mathsf{DDP}(n,q,R,\tau)$*-advantage of an algorithm* $\mathscr{A}$ *is defined as:*

$$Adv^{\mathsf{DDP}(n,q,R,\tau)}(\mathscr{A}) \stackrel{def}{=} \frac{1}{2}\left(\mathbb{P}\left(\mathscr{A}(\mathbf{H},\mathbf{s}) = 1 \mid b = 1\right) - \mathbb{P}\left(\mathscr{A}(\mathbf{H},\mathbf{s}) = 1 \mid b = 0\right)\right)$$

where the probabilities are computed over the internal randomness of $\mathscr{A}$*, a uniform* $b \in \{0,1\}$ *and inputs according to* $\mathscr{D}_b$ *which is defined in* $\mathsf{DDP}(n,q,R,\tau)$ *(Problem 3). We define the* $\mathsf{DDP}(n,q,R,\tau)$*-computational success in time* T *as:*

$$Succ^{\mathsf{DDP}(n,q,R,\tau)}(t) \stackrel{def}{=} \max_{\mathscr{A}:|\mathscr{A}|\leq T}\left(Adv^{\mathsf{DDP}(n,q,R,\tau)}(\mathscr{A})\right).$$

where $|\mathscr{A}|$ *denotes the running time of* $\mathscr{A}$*.*

Prove that when $(\mathbf{H},\mathbf{s})$ *is distributed according to* $\mathscr{D}_b$ *(for a fixed* $b \in \{0,1\}$*) we have:*

$$\mathbb{P}\left(\mathscr{A}(\mathbf{H},\mathbf{s}) = b\right) = \frac{1}{2} + Adv^{\mathsf{DDP}}(\mathscr{A}).$$

2. About Random Codes

Recall for this section the definition of the *statistical distance*, sometimes called the *total variational distance*. It is a distance for probability distributions, which in the case where X and Y are two random variables taking their values in a same finite space $\mathscr{E}$ is defined as

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

Furthermore, $\mathscr{S}_t$ will denote the set of words of Hamming weight t in $\mathbb{F}_q^n$, namely

$$\mathscr{S}_t \stackrel{\text{def}}{=} \left\{ \mathbf{x} \in \mathbb{F}_q^n \ : \ |\mathbf{x}| = t \right\}.$$

Exercise 10 (Important)**.** *Let us introduce the following* average *decoding problems*

Problem 4 (Decoding Problem - $\mathsf{DP}(n,q,R,\tau)$)**.** *Let $k \stackrel{def}{=} \lfloor Rn \rfloor$ and $t \stackrel{def}{=} \lfloor \tau n \rfloor$.*
- Input : $(\mathbf{H}, \mathbf{s} \stackrel{def}{=} \mathbf{x}\mathbf{H}^{\intercal})$ *where* $\mathbf{H}$ *(resp.* $\mathbf{x}$*) is uniformly distributed over* $\mathbb{F}_q^{(n-k)\times n}$ *(resp. words of Hamming weight t in $\mathbb{F}_q^n$).*
- Output : *an error $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t such that $\mathbf{e}\mathbf{H}^{\intercal} = \mathbf{s}$.*

Problem 5. $\mathsf{DP}'(n,q,R,\tau)$. *Let $k \stackrel{def}{=} \lfloor Rn \rfloor$ and $t \stackrel{def}{=} \lfloor \tau n \rfloor$.*
- Input : $(\mathbf{G}, \mathbf{y} \stackrel{def}{=} \mathbf{s}\mathbf{G} + \mathbf{e})$ *where $\mathbf{G}, \mathbf{s}$ and $\mathbf{e}$ are uniformly distributed over $\mathbb{F}_q^{k\times n}$, $\mathbb{F}_q^k$ and words of Hamming weight t in $\mathbb{F}_q^n$.*
- Output : *an error $\mathbf{e}' \in \mathbb{F}_q^n$ of Hamming weight t such that $\mathbf{y} - \mathbf{e}' = \mathbf{m}\mathbf{G}$ for some $\mathbf{m} \in \mathbb{F}_q^k$.*

Show that for any algorithm $\mathscr{A}$ solving $\mathsf{DP}'(n,q,R,\tau)$ with probability ε and time T, there exists an algorithm $\mathscr{B}$ which solves $\mathsf{DP}(n,q,R,\tau)$ in time $O\left(n^3\, T\right)$ with probability $\geq \varepsilon - O\left(q^{-\min(k,n-k)}\right)$. Show that we can exchange DP' by DP in the previous question.

Hint: *the following lemma may be useful*

Lemma 1. *Let $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ (resp. $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$) be a uniformly random matrix and $\mathbf{G}_k \in \mathbb{F}_q^{k\times n}$ (resp. $\mathbf{H}_{n-k} \in \mathbb{F}_q^{(n-k)\times n}$) be a uniformly random matrix of rank k (resp. $n-k$). We have:*

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

Exercise 11. *Show that for any non-zero $\mathbf{y} \in \mathbb{F}_q^n$, $\mathbf{G}$ being distributed uniformly at random among $\mathbb{F}_q^{k\times n}$,*

$$\mathbb{P}_{\mathbf{G}}(\mathbf{y} \in \mathcal{C}^*) = \frac{1}{q^k}$$

where $\mathcal{C}^*$ is defined as $\left\{\mathbf{c}^* \in \mathbb{F}_q^n \ : \ \mathbf{G}\mathbf{c}^{*\intercal} = \mathbf{0}\right\}$.

Exercise 12. *Let $\mathbf{G}$ and $\mathbf{H}$ being uniformly distributed at random among $\mathbb{F}_q^{k\times n}$ and $\mathbb{F}_q^{(n-k)\times n}$. Show that,*

$$\mathbb{E}_{\mathbf{G}}\left(\sharp\left\{\mathbf{c} \in \mathcal{C} : |\mathbf{c}| = t\right\}\right) = \frac{q^k - 1}{q^n}\binom{n}{t}(q-1)^t \quad \textit{and} \quad \mathbb{E}_{\mathbf{H}}\left(\sharp\left\{\mathbf{c} \in \mathcal{C} : |\mathbf{c}| \textit{ is even}\right\}\right) = \frac{1}{2}\,\frac{q^n + (2-q)^n}{q^{n-k}}.$$

Hint: For the first part of the exercise first show that $\mathbf{m}\mathbf{G}$ is uniformly distributed over $\mathbb{F}_q^n$ when $\mathbf{m} \in \mathbb{F}_q^k \backslash \{\mathbf{0}\}$.

Exercise 13. *Let $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ being uniformly distributed and $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $\mathbf{e} \in \mathscr{S}_t$ being some random variables. Show that*

$$\mathbb{E}_{\mathbf{H}}\left(\Delta\left(\mathbf{e}\mathbf{H}^{\intercal}, \mathbf{s}\right)\right) = \frac{1}{q^{(n-k)\times n}} \sum_{\mathbf{H}_0 \in \mathbb{F}_q^{(n-k)\times n}} \Delta\left(\mathbf{e}\mathbf{H}_0^{\intercal}, \mathbf{s}\right)$$

Exercise 14. *Let us admit the following lemma (a variation of the left-over hash lemma)*

Lemma 2. *Let $\mathscr{H} = (h_i)_{i \in I}$ be a finite family of applications from E in F. Let ε be the "collision bias"*

$$\mathbb{P}_{h,e,e'}(h(e) = h(e')) = \frac{1}{\sharp F}(1+\varepsilon)$$

where h is uniformly drawn in $\mathscr{H}$, e and e' be uniformly distributed over E. Let $\mathscr{U}$ be the uniform distribution over F and $\mathscr{D}(h)$ be the distribution $h(e)$ when e is chosen uniformly at random in E. We have,

$$\mathbb{E}_h\left(\Delta(\mathscr{D}(h), \mathscr{U})\right) \leq \frac{1}{2}\sqrt{\varepsilon}.$$

*Let $\mathbf{e}$ (*resp. $\mathbf{e}^{\mathrm{Ber}}$*) be uniformly distributed at random in the words of Hamming weight t (*resp. *the e_i^{Ber} are independent Bernoulli random variables of parameter $\tau \stackrel{def}{=} t/n$) in $\mathbb{F}_2^n$. Show that*

$$\mathbb{E}_{\mathbf{H}}\left(\Delta\left(\mathbf{e}\mathbf{H}^{\intercal}, \mathbf{s}\right)\right) \leq \frac{1}{2}\sqrt{\frac{2^{n-k}-1}{\binom{n}{t}}}.$$

$$\mathbb{E}_{\mathbf{H}}\left(\Delta\left(\mathbf{e}^{\mathrm{Ber}}\mathbf{H}^{\intercal}, \mathbf{s}\right)\right) \leq \frac{1}{2}\sqrt{2^k\left(1+(1-2\tau)^2\right)^n}.$$

What can you deduce when comparing both results with $\mathbf{e}$ or $\mathbf{e}^{\mathrm{Ber}}$? What is the "better" choice of error $\mathbf{x}$ to ensure that $\mathbf{x}\mathbf{H}^{\intercal}$ is uniformly distributed?

Exercise 15. *Let $\mathcal{C}$ be a fixed $[n,k]_q$-code of parity-check matrix $\mathbf{H}$ and $\mathbf{y}, \mathbf{s}, \mathbf{e} \in \mathbb{F}_q^n \times \mathbb{F}_q^{n-k} \times \mathscr{S}_t$ be uniformly distributed. Our aim in this exercise is to show that $\Delta(\mathbf{c}+\mathbf{e}, \mathbf{y}) = \Delta(\mathbf{e}\mathbf{H}^{\intercal}, \mathbf{s})$.*

1. *Given $\mathbf{s} \in \mathbb{F}_q^{n-k}$, let $\mathbf{y}(\mathbf{s}) \in \mathbb{F}_q^n$ be such that $\mathbf{y}(\mathbf{s})\mathbf{H}^{\intercal} = \mathbf{s}$. Show that*

$$\sum_{\mathbf{y} \in \mathbb{F}_q^n} \left| \mathbb{P}_{\mathbf{e},\mathbf{c}}(\mathbf{c}+\mathbf{e} = \mathbf{y}) - \frac{1}{q^n} \right| = \sum_{\mathbf{s} \in \mathbb{F}_q^{n-k}} \sum_{\mathbf{c}' \in \mathcal{C}} \left| \mathbb{P}_{\mathbf{e},\mathbf{c}}(\mathbf{c}+\mathbf{e} = \mathbf{y}(\mathbf{s}) + \mathbf{c}') - \frac{1}{q^n} \right|.$$

2. *Deduce that $\Delta(\mathbf{c}+\mathbf{e}, \mathbf{y}) = \Delta(\mathbf{e}\mathbf{H}^{\intercal}, \mathbf{s})$.*

3. Information Set Decoding Algorithms

Exercise 16. *Let $\tau \in [0, 1/2]$. Show how from an algorithm solving $\mathsf{DP}(n, 2, R, \tau)$ (Problem 4) we can deduce an algorithm solving $\mathsf{DP}(n, 2, R, 1-\tau)$ in the same running-time (and reciprocally).*

Let $\mathscr{I} \subseteq [\![1,n]\!]$ and $\mathbf{c} \in \mathbb{F}_q^n$. We will denote $\mathbf{c}_{\mathscr{I}}$ the vector whose coordinates are those of $\mathbf{c} = (c_i)_{1 \leq i \leq n}$ which are indexed by $\mathscr{I}$, *i.e.* $\mathbf{c}_{\mathscr{I}} = (c_i)_{i \in \mathscr{I}}$. Given $\mathbf{H} \in \mathbb{F}_q^{r \times n}$ we will denote by $\mathbf{H}_{\mathscr{I}}$ the matrix whose *columns* are those of $\mathbf{H}$ which are indexed by $\mathscr{I}$.

Exercise 17. *Let $\mathcal{C}$ be an $[n,k]$-code and $\mathscr{I} \subseteq [\![1,n]\!]$ be of size k. Recall that $\mathscr{I}$ is an information set of $\mathcal{C}$ if*

$$\forall \mathbf{x} \in \mathbb{F}_q^k : \quad \exists ! \mathbf{c} \in \mathcal{C} \text{ such that } \mathbf{c}_{\mathscr{I}} = \mathbf{x}.$$

Show that,

$$\begin{aligned} \mathscr{I} \text{ is an information set for } \mathcal{C} &\iff \forall \mathbf{G} \text{ generator matrix of } \mathcal{C},\ \mathbf{G}_{\mathscr{I}} \text{ is invertible} \\ &\iff \forall \mathbf{H} \text{ parity-check matrix of } \mathcal{C},\ \mathbf{H}_{\overline{\mathscr{I}}} \text{ is invertible} \end{aligned}$$

Let $\mathscr{I}$ be an information set of $\mathcal{C}$. Given $\mathbf{x} \in \mathbb{F}_q^k$, how to compute the unique codeword $\mathbf{c} \in \mathcal{C}$ such that $\mathbf{c}_{\mathscr{I}} = \mathbf{x}$? Is it easy?

Exercise 18. *Recall that Prange's algorithm works as follows*

The distribution $\mathscr{D}_t$.

– *If $t < \frac{q-1}{q}(n-k)$, $\mathscr{D}_t$ only outputs $\mathbf{0} \in \mathbb{F}_q^k$,*

– *if* $t \in [\![\frac{q-1}{q}(n-k), k+\frac{q-1}{q}(n-k)]\!]$, $\mathscr{D}_t$ *outputs uniform vectors of weight* $t-\frac{q-1}{q}(n-k)$,
– *if* $t > k + \frac{q-1}{q}(n-k)$, $\mathscr{D}_t$ *outputs uniform vectors of weight* k.

The algorithm.

1. Picking the information set. *Let* $\mathscr{I} \subseteq [\![1,n]\!]$ *be a random set of size* k. *If* $\mathbf{H}_{\overline{\mathscr{I}}} \in \mathbb{F}_q^{(n-k)\times(n-k)}$ *is not of full-rank, pick another set* $\mathscr{I}$.
2. Linear algebra. *Perform a Gaussian elimination to compute a non-singular matrix* $\mathbf{S} \in \mathbb{F}_q^{(n-k)\times(n-k)}$ *such that* $\mathbf{S}\mathbf{H}_{\overline{\mathscr{I}}} = \mathbf{1}_{n-k}$.
3. Test Step. *Pick* $\mathbf{x} \in \mathbb{F}_q^k$ *according to the distribution* $\mathscr{D}_t$ *and let* $\mathbf{e} \in \mathbb{F}_q^n$ *be such that*
$$\mathbf{e}_{\overline{\mathscr{I}}} = \left(\mathbf{s} - \mathbf{x}\mathbf{H}_{\mathscr{I}}^{\intercal}\right)\mathbf{S}^{\intercal} \quad ; \quad \mathbf{e}_{\mathscr{I}} = \mathbf{x}.$$
If $|\mathbf{e}| \neq t$ *go back to Step* 1*, otherwise it is a solution.*

Describe Prange's algorithm with the generator matrix formalism in the same fashion as above (with also three steps and the distribution $\mathscr{D}_t$*).*

Exercise 19. *Let* $\mathcal{C}$ *be an* $[n,k]$*-code and* $\mathscr{J} \subseteq [\![1,n]\!]$ *be of size* $k+\ell$. *Recall that* $\mathscr{J}$ *is an augmented information set of* $\mathcal{C}$ *if it contains an information set.*

Show that,

$$\mathscr{J} \text{ is an augmented information set for } \mathcal{C} \iff \mathscr{D} \stackrel{def}{=} \left\{\mathbf{c}_{\mathscr{J}} \in \mathbb{F}_q^{k+\ell} \;:\; \mathbf{c} \in \mathcal{C}\right\} \text{ is a code of dimension } k.$$

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *be a parity-check matrix of* $\mathcal{C}$. *Suppose that* $\mathscr{J}$ *is an augmented information set of* $\mathcal{C}$. *Give a parity-check matrix of* $\mathscr{D}$ *(this code is known that punctured code of* $\mathcal{C}$ *at positions* $\overline{\mathscr{J}}$*).*

Exercise 20. *Recall that Dumer's algorithm is as follows*

The algorithm.

1. Splitting in two parts. *First we randomly select a set* $\mathscr{S} \subseteq [\![1,n]\!]$ *of* $n/2$ *positions.*
2. Building lists step. *We build,*
$$\mathscr{L}_1 \stackrel{def}{=} \left\{\mathbf{H}_{\mathscr{S}}\mathbf{e}_1^{\intercal} : |\mathbf{e}_1| = \frac{t}{2}\right\} \quad ; \quad \mathscr{L}_2 \stackrel{def}{=} \left\{-\mathbf{H}_{\overline{\mathscr{S}}}\mathbf{e}_2^{\intercal} + \mathbf{s}^{\intercal} : |\mathbf{e}_2| = \frac{t}{2}\right\}.$$
3. Collisions step. *We merge the above lists (with an efficient technique like hashing or sorting)*
$$\mathscr{L}_1 \bowtie \mathscr{L}_2 \stackrel{def}{=} \left\{(\mathbf{e}_1,\mathbf{e}_2) \in \mathscr{L}_1 \times \mathscr{L}_2, \quad \mathbf{H}_{\mathscr{S}}\mathbf{e}_1^{\intercal} = -\mathbf{H}_{\overline{\mathscr{S}}}\mathbf{e}_2^{\intercal} + \mathbf{s}^{\intercal}\right\}.$$
and output this new list. If it is empty we go back to Step 1 *and pick another set of* $n/2$ *positions.*

and we have the following proposition

Proposition 1. *The complexity* $C_{\text{Dumer}}(n,q,R,\tau)$ *of Dumer's algorithm to solve* $\mathsf{DP}(n,q,R,\tau)$ *is up to a polynomial factor (in* n*) given by*
$$\sqrt{\binom{n}{t}(q-1)^t} + \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$
Furthermore, Dumer's algorithm finds $\max\left(1, \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}\right)$ *solutions (up to a polynomial factor in* n*) where* $k \stackrel{def}{=} Rn$ *and* $t \stackrel{def}{=} \tau n$.

We have made the choice in the above Dumer's algorithm to build lists of maximum size, namely $\binom{n/2}{t/2}(q-1)^{t/2}$. *Let* $(\mathbf{H},\mathbf{s}) \in \mathbb{F}_q^{(n-k)\times n} \times \mathbb{F}_q^{n-k}$ *be an instance of a decoding problem that we would like to solve at distance* t. *We suppose that* $(\mathbf{H},\mathbf{s})$ *are uniformly distributed, in particular we do not suppose that there is always a solution. Show that a slight variation of Dumer's algorithm enables to compute* $\frac{L^2}{q^{n-k}}$ *solutions (there is no maximum in this formula, why?) in time* $L + \frac{L^2}{q^{n-k}}$ *(up to polynomial factors). Furthermore* L *has necessarily to verify* $L \leq \binom{n/2}{t/2}(q-1)^{t/2}$, *why? What is the condition over* t *and* L *for this algorithm to output solutions in amortized time one?*