Partie I : Codes correcteurs

1.1 Montrons que $\delta_{H,n}$ est une distance. Pour $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ dans $\mathscr{A}^n$, on note $A_{x,y} = \{i \in [\![1, n]\!] \ , \ x_i \neq y_i\}$ de telle sorte que $\delta_{H,n}(x, y) = \mathsf{Card} A_{x,y}$.

— Pour tout x, y dans $\mathscr{A}^n$, $\delta_{H,n}(x, y) \geq 0$ par définition. De plus comme $A_{x,y} = A_{y,x}$, $\delta_{H,n}(x, y) = \delta_{H,n}(y, x)$.

— Soit $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ dans $\mathscr{A}^n$,

$$\delta_{H,n}(x, y) = 0 \iff (\forall i \in [\![1, n]\!], x_i = y_i) \iff x = y$$

— Soit $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ et $z = (z_1, \dots, z_n)$ dans $\mathscr{A}^n$, On remarque que si $i \in \overline{A_{x,y}} \cap \overline{A_{y,z}}$ alors $i \in \overline{A_{x,z}}$ où, pour toute partie X de $[\![1, n]\!]$, $\overline{X}$ désigne son complémentaire dans $[\![1, n]\!]$. En effet, $x_i = y_i$ et $y_i = z_i$ implique $x_i = z_i$. De ce fait,

$$\mathsf{Card}(\overline{A_{x,y} \cup A_{y,z}}) = \mathsf{Card}(\overline{A_{x,y}} \cap \overline{A_{y,z}}) \leq \mathsf{Card}\overline{A_{x,z}}$$

On en déduit que

$$\delta_{H,n}(x, z) = \mathsf{Card} A_{x,z} \leq \mathsf{Card}(A_{x,y} \cup A_{y,z}) \leq \mathsf{Card} A_{x,y} + \mathsf{Card} A_{y,z} = \delta_{H,n}(x, y) + \delta_{H,n}(y, z).$$

On a bien montré que $\boxed{\delta_{H,n} \text{ est une distance sur } \mathscr{A}^n}$.

1.2. Soit C un code. C'est un ensemble ayant au moins deux éléments. On en déduit que $\{(x, y) \in C \times C \ , \ x \neq y\}$ est un ensemble non vide. De ce fait, l'ensemble $\{\delta_H(x, y) \ ; \ (x, y) \in C \times C \ , \ x \neq y\}$ est une partie non vide de $\mathbb{N}^*$. Elle admet un plus petit élément.

1.3. On suppose que $d_C \geq 2e + 1$. Supposons par l'absurde qu'il existe $y \in \mathscr{A}^n$ et x, x' dans C tels que $\delta_H(y, x) \leq e$ et $\delta_H(y, x') \leq e$. D'après l'inégalité triangulaire, on obtient

$$\delta_H(x, x') \leq \delta_H(x, y) + \delta_H(y, x') \leq 2e.$$

Par définition de d_C, $d_C \leq \delta_H(x, x') \leq 2e$. Ce qui contredit l'hypothèse.

1.4. a) Soit $x \in \mathscr{A}^n$ et $r \in \mathbb{N}$. La distance δ_H prenant ses valeurs dans $\mathbb{N}$, $B(x, r) = \bigcup_{i=0}^{r} S(x, i)$. Ces sphères étant deux à deux disjointes,

$$\mathsf{Card}(B(x, r)) = \sum_{i=0}^{r} \mathsf{Card}(S(x, i))$$

b) Soit $x = (x_1, \dots, x_n) \in \mathscr{A}^n$ et $i \in [\![0, n]\!]$. Pour se donner un élément $y \in S(x, i)$, il suffit de choisir les i indices k parmi $[\![1, n]\!]$; tels que $x_k \neq y_k$ (il y a $\binom{n}{i}$ possibilités) puis de choisir,

pour chacun de ces indices, un élément $y_k \in \mathscr{A} \setminus \{x_k\}$. On en déduit [1] que

$$\mathsf{Card}(S(x,i)) = \binom{n}{i}(\mathsf{Card}\mathscr{A} - 1)^i.$$

Finalement en utilisant la question précédente, on obtient bien que

$$\mathsf{Card}(B(x,r)) = \sum_{i=0}^{r} \binom{n}{i}(\mathsf{Card}\mathscr{A} - 1)^i.$$

1.5. Soit P l'ensemble des rayons $r \in \mathbb{N}$ tel que l'ensemble des boules de rayons r centrées aux mots du codes recouvrent $\mathscr{A}^n$:

$$P = \{r \in \mathbb{N} \ ; \ \mathscr{A}^n \subset \bigcup_{x \in C} B(x,r)\}$$

C'est un ensemble non vide car C n'étant pas vide, $n \in P$. En effet soit $x_0 \in C$, $\mathscr{A}^n \subset B(x,n)$ puisque pour tout $y \in \mathscr{A}^n$,

$$\delta_H(x,y) = \mathsf{Card}(A_{x,y}) \leq n$$

L'ensemble P étant une partie non vide de $\mathbb{N}$, elle admet un plus petit élément.

1.6. a) Par définition de la capacité de décodage e, pour tout x, x' dans C, les boules $B(x,e)$ et $B(x',e)$ sont disjointes. On en déduit que

$$\mathsf{Card}\left(\bigcup_{x \in C} B(x,e)\right) = \sum_{x \in C} \mathsf{Card}(B(x,e)) = \sum_{x \in C}\left(\sum_{i=0}^{e} \binom{n}{i}(\mathsf{Card}(\mathscr{A}) - 1)^i\right).$$

En utilisant alors $\bigcup_{x \in C} B(x,e) \subset \mathscr{A}^n$, on obtient donc

$$\mathsf{Card}(C) \times \left(\sum_{i=0}^{e} \binom{n}{i}(\mathsf{Card}(\mathscr{A}) - 1)^i\right) \leq \mathsf{Card}\,(\mathscr{A}^n) = (\mathsf{Card}(A))^n$$

b) Par définition de $\rho(C)$, $\mathscr{A}^n \subset \left(\bigcup_{x \in C} B(x, \rho(C))\right)$. On en déduit

$$(\mathsf{Card}(A))^n = \mathsf{Card}\,(\mathscr{A}^n) \leq \mathsf{Card}\left(\bigcup_{x \in C} B(x,\rho(C))\right) \leq \sum_{x \in C} \mathsf{Card}(B(x,\rho(C)))$$

---

1. Plus formellement, on pouvait aussi numéroter les éléments de $\mathscr{A}$ de 1 à n. Cela revient à construire une bijection $\theta : [\![0, n-1]\!] \to \mathscr{A}$. On peut alors définir une bijection de $\varphi_i : K_i \times [\![1, n-1]\!]^i \to S(x,i)$ où $K_i = \{I \subset [\![1,n]\!] \ ; \ \mathsf{Card}I = i\}$ est l'ensemble des parties de $[\![1,n]\!]$ ayant i éléments. On pose

$$\begin{array}{rccc} \varphi_i : & K_i \times [\![1,n-1]\!]^i & \to & S(x,i) \\ & (I, (\alpha_1, \ldots, \alpha_i)) & \mapsto & (y_1, \ldots, y_n) \end{array}$$

où, en posant $I = (k_1, \ldots, k_i)$, pour tout $k \in [\![1,n]\!]$,

$$y_k = \begin{cases} x_k & \text{si } k \notin I \\ \theta(\theta^{-1}(x_{k_r}) + \alpha_r) & \text{si } k = k_r \end{cases}$$

L'addition $\theta^{-1}(x_{k_r}) + \alpha_r$ étant prise modulo n.

En utilisant encore que toutes les boules ont le même nombre d'éléments comme calculé à la question 1.4.b, on obtient finalement

$$(\mathsf{Card}(A))^n \leq \sum_{x\in C} \mathsf{Card}(B(x,\rho(C))) = \mathsf{Card}(C) \times \left(\sum_{i=0}^{\rho(C)} \binom{n}{i} (\mathsf{Card}(\mathscr{A})-1)^i \right)$$

Partie II : Décodage d'une famille de codes

Remarquons pour la suite que si C est un code linéaire, par définition $\dim(C) \geq 1$ et donc $C \neq \{0\}$.

2.1. L'application w_H n'est pas norme. Elle n'est pas homogène.
Soit $x \in C \setminus \{0\}$, $w_H(x) = \delta_H(x,0) \neq 0$ et

$$w_H(2x) = \delta_H(2x,0) = \delta_H(x,0) = w_H(x) \neq 2w_H(x).$$

2.2. Soit $x, y \in K^n$, on remarque que $A_{x,y} = A_{x-y,0}$ car en notant $x = (x_1,\dots,x_n)$ et $y = (y_1,\dots,y_n)$, pour tout $i \in [\![1,n]\!]$,

$$i \in A_{x,y} \iff x_i \neq y_i \iff x_i - y_i \neq 0 \iff i \in A_{x-y,0}$$

On en déduit que $\delta_H(x,y) = w_H(x-y)$. En notant que l'application $(x,y) \to x-y$ est une surjection de $\{(x,y) \in C\times C \ ; \ x \neq y\}$ dans $C \setminus \{0\}$, on obtient que

$$\{\delta_H(x,y) \ ; \ (x,y) \in C\times C \ , \ x \neq y\} = \{w_H(x) \ ; \ x \in C \setminus \{0\}\}$$

et donc

$$d_C = \min\{\delta_H(x,y) \ ; \ (x,y) \in C\times C \ , \ x \neq y\} = \min\{w_H(x) \ ; \ x \in C \setminus \{0\}\}$$

2.3. Soit C un code $[n,k]$. On sait que $F = \{(x_1,\dots,x_n) \in \mathbb{K}^n \ ; \ \forall i \leq n-d+1, x_i = 0\}$ est un sous-espace vectoriel de dimension $d-1$.
Soit $x \in C \setminus \{0\}$, on sait que $w_H(x) \geq d$. En particulier, $x \notin F$ car les éléments de F ont, au plus, $n-(n-d+1) = d-1$ composantes non nulles. On en déduit que $C \cap F = \{0\}$ et donc, d'après la formule de Grassmann, $\dim(C \cup F) = \dim C + \dim F$ ce qui implique que

$$k + (d-1) = \dim C + \dim F \leq n$$

Finalement, $\boxed{k+d \leq n+1}$.

2.4. Soit $\alpha = (\alpha_1,\dots,\alpha_n)$ des éléments deux à deux distincts. Soit k compris entre 1 et n, la restriction de ev_α à L_k (encore notée ev_α) est injective.
En effet, soit $f \in L_k$ tel que $\mathrm{ev}_\alpha(f) = 0$, la fonction polynomiale (encore notée f) associée à f s'annule en $\alpha_1,\dots,\alpha_n$. Comme $n \geq k > \deg f$, on a que f est nul.
On en déduit que $\dim \mathrm{ev}_\alpha(L_k) = \dim L_k = k$. $\boxed{\text{C'est-à-dire que } \mathrm{RS}_{\alpha,k} \text{ est un code } [n,k]}$.

2.5. a) Soit f un polynôme non nul de degré au plus $k-1$ ($f \in L_k \setminus \{0\}$). Il existe au plus $k-1$ éléments x de $\mathbb{K}$ tels que $f(x) = 0$ et donc $\mathrm{ev}_\alpha(f)$ a au plus $k-1$ composantes nulles.

b) Soit $x \in \mathrm{RS}_{\alpha,k} \setminus \{0\}$. Il existe $f \in L_k \setminus \{0\}$ tel que $x = \mathrm{ev}_\alpha(f)$. On déduit que la question précédente que $w_H(x) \geq n - (k-1) = n - k + 1$.

Inversement, soit $f = \prod_{i=1}^{k-1}(X - \alpha_i)$ qui appartient à L_k,

$$x = \mathrm{ev}_\alpha(L_k) = (0, \ldots, 0, f(x_k), \ldots, f(x_n))$$

En particulier, $w_H(x) = n - (k-1) = n - k + 1$. Cela implique que la distance minimale de $\mathrm{RS}_{\alpha,k}$ est $n + 1 - k$.

On en déduit que la borne du singleton de la question 3 est atteinte.

2.6. Soit $f \in \mathbb{K}[X]$ tel que $\deg(f) < k$. Soit $y \in \mathbb{K}^n$ tel que $\delta_H(\mathrm{ev}_\alpha(f), y) \leq e$. Cela signifie que $A_{\mathrm{ev}_\alpha(f),y}$ est de cardinal au plus e. Soit I un partie de cardinal e de $[\![1, n]\!]$ telle que $A_{\mathrm{ev}_\alpha(f),y} \subset I$. On pose alors $E = \prod_{i \in I}(X - \alpha_i)$ et $F = f \times E$.

Par construction

— Soit i un entier compris entre 1 et n. Si $i \in I$, $F(\alpha_i) = E(\alpha_i) = 0$ donc $F(\alpha_i) - y_i E(\alpha_i) = 0$. Par contre, si $i \notin I$ alors $i \notin A_{\mathrm{ev}_\alpha(f),y}$ d'où $f(\alpha_i) = y_i$ et donc, en multipliant par $E(\alpha_i)$, $F(\alpha_i) - y_i E(\alpha_i) = 0$.

— Par hypothèses, $\deg f < k$ d'où $\deg F = e + \deg f < e + k$.

— Par construction, E est unitaire et de degré e

Pour finir, on a bien $f = F/E$.

2.7. Soit (E_1, F_1) et (E_2, F_2) deux polynômes satisfaisant les conditions 1.a, 1.b et 1.c. On veut montrer que dans $\mathbb{K}(X)$, $\dfrac{F_1(X)}{E_1(X)} = \dfrac{F_2(X)}{E_2(x)}$ ce qui signifie que le polynôme $F_1E_2 - E_1F_2$ est le polynôme nul.

Remarquons que, par hypothèse, $\deg F_1 \leq e + k - 1$ et donc

$$\deg(F_1E_2) = \deg F_1 + \deg E_2 \leq 2e + k - 1 < (n - k + 1) + k - 1 < n.$$

De plus, pour tout $i \in [\![1, n]\!]$,

$$F_1(\alpha_i)E_2(\alpha_i) - F_2(\alpha_i)E_1(\alpha_i) = y_iE_1(\alpha_i)E_2(\alpha_i) - y_iE_1(\alpha_i)E_2(\alpha_i) = 0.$$

Les éléments $\alpha_1, \ldots, \alpha_n$ étant deux à deux disjoints, on a bien $F_1E_2 - E_1F_2 = 0$.

2.8. — On suppose qu'il existe $f \in L_k$ tel que $\delta_H(\mathrm{ev}_\alpha(f), y) \leq e$. D'après la question 6. il existe un polynôme E et un polynôme $F = f \times E$ vérifiant les conditions 1.a, 1.b et 1.c
De ce fait, on suppose que l'étape 1 renvoie un couple de polynôme E_1, F_1. D'après 7. on a alors, dans $\mathbb{K}(X)$ que

$$\frac{F_1}{E_1} = \frac{F}{E} = f$$

Cela implique que E_1 divise F_1 et que $F_1/E_1 = f$. C'est ce que l'on veut.

— Réciproquement, s'il n'existe pas $f \in L_k$ tel que $\delta_H(\mathrm{ev}_\alpha(f), y) \leq e$, l'algorithme renvoie « échec ». En effet, même s'il arrive a l'étape 3, il renverra nécessairement « échec » par hypothèses.

2.9. On pose $p = e+k-1$. On considère le système dont les inconnues sont $a_0, a_1, \ldots, a_p$ les coefficients de F et $b_0, \ldots, b_{e-1}$ les coefficients de E (on ne considère par b_e car E est supposé unitaire). Il y a donc $e + k + e = 2e + k \leq n$ coefficients. Les n équations sont données par les n équations de la condition 1.a

2.10. a) Soit (Q_1, Q_2, R_1, R_2) quatre polynômes tels que $A = BQ_1 + R_1 = BQ_2 - R_2$ avec $\deg(R_1) < m$ et $\deg(R_2) < m$. On a donc $B(Q_1 - Q_2) = R_2 - R_1$ ce qui implique que $B|(R_2 - R_1)$. Cependant, $\deg B = m > \deg(R_2 - R_1)$ donc $R_2 - R_1 = 0$. Du fait que $\mathbb{K}[X]$ est intègre on obtient alors que $Q_1 - Q_2 = 0$. Finalement $\boxed{(Q_1, R_1) = (Q_2, R_2)}$.

b) La cas où $n < m$ est évident. Dans ce cas, on a $A = 0 \times B + A$ avec $\deg(A) = n < m = \deg(B)$.

Traitons le cas où $n \geq m$. Modifions un peu l'algorithme en calculant Q au fur et à mesure. Rajoutons dans la ligne 2, l'instruction $Q \leftarrow 0$ et dans la ligne 4, $Q \leftarrow Q + q_i X^i$, ce qui permet de renvoyer à la fin le polynôme Q voulu : $Q = \sum_{i=0}^{n-m} q_i X^i$.

On utilise alors l'invariant de boucle $A = BQ + R$. De ce fait, au début de la boucle des instructions 3 et 4, on a $A = BQ + R$ car $Q = 0$ et $R = A$.

Soit $i \in [\![0, n-m]\!]$. Supposons que l'invariant est vérifié avant d'exécuter l'instruction pour i. On pose alors Q_0 et R_0 les valeurs des variables Q et R avant l'exécution de la ligne et Q_1, R_1 les valeurs de ces mêmes variables après l'exécution. On a donc $Q_1 = q_i X^i + Q_0$ et $R_1 = R_0 - q_i X^i$ par construction. De ce fait, $A = Q_1 B + R_1$.

On en déduit qu'à la fin de l'exécution de la boucle, on a bien $A = BQ + R$.

Montrons de plus, que si avant l'exécution de la ligne 4 pour $i \in [\![0, n-m]\!]$, $\deg R \leq m + i$ alors, après l'instruction $\deg R < m+i$. En effet, dans le cas, où $\deg R \neq m+i$ on ne change par R et si $\deg R = m+i$, on « tue » le coefficient de degré $m+i$ de R car $q_i X^i B$ a le même coefficient dominant par construction. Comme au début de la boucle, $\deg R = \deg A = m \leq m + (n-m)$, a la fin de l'exécution, $\deg R < m$.

Cela prouve que $\boxed{\text{l'algorithme renvoie bien } Q, R \text{ tels que } A = BQ + R \text{ et } \deg R < m.}$

c) Examinons le coût de cet algorithme. On passe $n-m+1$ fois dans la ligne 4. A chaque passage dans cette ligne,

- On calcule q_i qui nécessite 1 opération
- On calcule $q_i X^i B$ qui nécessite $m + 1$ opérations car B est de degré m et la multiplication par X^i ne coûte rien.
- On calcule $R - q_i X^i B$ qui nécessite $m + 1$ opérations car B est de degré m.

Cela nécessite donc $2m + 3$ opérations par passages dans la boucle, mais on sait (d'après la question précédente) que par construction le coefficient dominant de $q_i X^i B$ sera celui de R et qu'il sera « tué » dans la soustraction. On peut donc éviter de faire ce calcul ce qui ne demande plus que $2m + 1$ opérations.

On obtient finalement un coût total au plus égal à $(n-m+1) \times (2m+1) + 1$ le $+1$ final venant du calcul u à la ligne 2.

2.11. Analysons l'algorithme 2.

- On reçoit un mot $(y_1, \ldots, y_n) \in \mathbb{K}^n$.
- On cherche des polynômes E et F vérifiant les conditions 1a, 1b et 1c. On a vu à la question 9 que cela revient à résoudre un système linéaire de taille au plus n ce qui peut se faire en $O(n^3)$ par le pivot de Gauss d'après l'énoncé.

— S'il n'existe pas de tels polynômes (si le système ci-dessus n'a pas de solutions), l'algorithme renvoie « echec ».
— S'il existe de tels polynômes, on teste si E divise F. Pour cela on réalise la division euclidienne de F par E. Comme $\deg E \leq n$ et que $\deg F \leq n$, cela nécessite $O(n^2)$ opérations d'après la question 10c. Il suffit alors de tester si R est le polynôme nul

On peut donc exécuter l'algorithme 2 en $O(n^3)$ opérations.

Partie III : Décodage via l'interpolation et l'algorithme d'Euclide étendu

3.1. a) Montrons par récurrence finie que pour tout i compris entre 0 et l,

$$U_i \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix}$$

— Initialisation : pour $i = 0$, $U_0 = \begin{pmatrix} S_0 & T_0 \\ S_1 & T_1 \end{pmatrix}$ et donc

$$U_0 \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} S_0A + T_0B \\ S_1A + T_1B \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$$

— Hérédité : soit i compris entre 0 et $l-1$. On suppose que $U_i \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix}$.

On a alors

$$U_{i+1} \begin{pmatrix} A \\ B \end{pmatrix} = W_{i+1}U_i \begin{pmatrix} A \\ B \end{pmatrix} = W_{i+1} \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = \begin{pmatrix} R_{i+1} \\ R_i - Q_{i+1}R_{i+1} \end{pmatrix}$$

Maintenant, par définition, (Q_{i+1}, R_{i+2}) sont les polynômes renvoyés par l'algorithme 3. Ce sont donc les quotient et reste de la division euclidienne de R_i par R_{i+1}. De ce fait, $R_i = Q_{i+1}R_{i+1} + R_{i+2}$ et donc $R_i - Q_{i+1}R_{i+1} = R_{i+2}$.

Cela prouve bien que $U_{i+1} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} R_{i+1} \\ R_{i+2} \end{pmatrix}$.

b) En utilisant encore que pour i compris entre 0 et $l-1$, $U_{i+1} = W_{i+1}U_i$ et $S_{i+1} = S_{i-1} - Q_iS_i$, $T_{i+1} = T_{i-1} - Q_iT_i$, une récurrence similaire à la précédente montre que pour tout $i \in [\![0, l]\!]$, $U_i = \begin{pmatrix} S_i & T_i \\ S_{i+1} & T_{i+1} \end{pmatrix}$.

On en déduit donc que pour tout i compris entre 0 et l,

$$\begin{pmatrix} S_i & T_i \\ S_{i+1} & T_{i+1} \end{pmatrix} \times \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix}$$

Cela implique que $\boxed{\text{pour tout } i \text{ compris entre } 0 \text{ et } l+1,\ S_iA + T_iB = R_i}$

c) Pour tout i compris entre 0 et l,

$$S_iT_{i+1} - S_{i+1}T_i = \det(U_i) = \det(W_i)\det(W_{i-1})\cdots\det(W_1)\det(U_0) = (-1)^i(S_0T_1 - S_1T_0) = (-1)^i$$

car pour tout k compris entre 1 et i, $\det(W_k) = -1$ et $S_0T_1 - S_1T_0 = 1$.

d) Pour tout i compris entre 1 et l, par construction (algorithme 3), $R_{i-1} = Q_i R_i + R_{i+1}$. On en déduit que les pgcd de R_{i-1} et R_i sont aussi des pgcd de R_i et R_{i+1}. En effet
   — Soit D un pgcd de R_i et R_{i+1}, alors D divise aussi R_{i-1} car $R_{i-1} = Q_i R_i + R_{i+1}$. De plus, si E divise R_i et R_{i-1}, il divise aussi R_{i+1} car $R_{i+1} = R_{i-1} - Q_i R_i$ donc, E divise D. On en déduit que D est bien un pgcd de R_{i-1} et R_i.
   — Réciproquement, soit D un pgcd de R_{i-1} et R_i, alors D divise aussi R_{i+1} car $R_{i+1} = -Q_i R_i + R_{i-1}$. De plus, si E divise R_i et R_{i+1}, il divise aussi R_{i-1} car $R_{i-1} = Q_i R_i + R_{i+1}$ donc, E divise D. On en déduit que D est bien un pgcd de R_i et R_{i+1}.

   De proche en proche, en divisant à chaque fois par le coefficient dominant,

$$\text{pgcd}(A, B) = \text{pgcd}(R_0, R_1) = \cdots = \text{pgcd}(R_i, R_{i+1}) = \cdots = \text{pgcd}(R_l, R_{l+1})$$

   Or, par définition, $R_{l+1} = 0$ donc $\text{pgcd}(A, B) = \text{pgcd}(R_l, 0) = R_l/\text{cd}(R_l)$. La dernière égalité venant du fait que si P est un polynôme non nul, P est un pgcd de P et de 0 de manière immédiate.

3.2. Commençons par remarquer que $Q_1 \neq 0$ car $\deg A \geq \deg B$ et que pour tout i compris entre 2 et l, $\deg Q_i > 0$. Supposons par l'absurde qu'il existe $i \geq 2$ tel que $\deg Q_i \leq 0$, on a que la division euclidienne de R_{i-1} par R_i s'écrit $R_{i-1} = Q_i R_i + R_{i+1}$. De ce fait, $\deg(R_{i-1}) \leq \max(\deg(R_{i+1}), \deg(Q_i R_i)) \leq \deg R_i$ ce qui est absurde car, par construction, $\deg(R_i) < \deg(R_{i-1})$ par définition de la division euclidienne.

Montrons alors par récurrence finie que pour tout $i \in [\![2, l+1]\!]$,

$$\deg S_i = \sum_{2 \leq j < i} \deg Q_j = \deg R_1 - \deg R_{i-1} \text{ et } \deg S_i > \deg S_{i-1}.$$

— Initialisation : Pour $i = 2$, on a $S_2 = 1 - 0Q_1 = 1$. On a bien

$$\deg S_2 = 0 = \sum_{j \in \emptyset} \deg Q_j = \deg R_1 - \deg R_1$$

De plus, $\deg S_2 = 0 > \deg S_1$ car $S_1 = 0$.

— Hérédité : Soit $i \in [\![2, l]\!]$, on suppose que

$$\deg S_i = \sum_{2 \leq j < i} \deg Q_j = \deg R_1 - \deg R_{i-1} \text{ et } \deg S_i > \deg S_{i-1}.$$

Comme $S_{i+1} = S_{i-1} - Q_i S_i$ et que $\deg S_{i-1} < \deg S_i \leq \deg(Q_i S_i)$ car $Q_i \neq 0$,

$$\deg S_{i+1} = \deg(Q_i S_i) = \deg S_i + \deg Q_i = \sum_{2 \leq j < i+1} \deg Q_j = \deg R_1 - \deg R_{i-1} + \deg Q_i$$

De plus, par définition, $R_{i-1} = Q_i R_i + R_{i+1}$. Là encore, $\deg R_{i+1} < \deg R_i \leq \deg(Q_i R_i)$ car $Q_i \neq 0$ donc $\deg R_{i-1} = \deg Q_i + \deg R_i$. Cela donne $\deg S_{i+1} = \deg R_1 - \deg R_i$. Pour finir, $\deg S_{i+1} = \deg S_i + \deg Q_i > \deg S_i$.

On procède de même pour la famille de polynômes (T_i). On vérifie d'abord que $T_1 = 1$ et donc $\deg T_1 = 0$ puis que $\deg T_2 = \deg(-Q_1 T_1) = \deg Q_1 = \deg R_0 - \deg R_1$. La suite est une récurrence similaire.

3.3. Commencer par remarquer que si $\deg A = n < m = \deg B$, la première exécution de l'instruction 3 renvoie $Q_1 = 0$, $R_2 = A$ (la division euclidienne dans ce cas est en $O(1)$) puis $S_2 = S_0 = 1$, $T_2 = T_0 = 1$, comme $Q_1 = 0$ cela se fait aussi en temps constant. Finalement, on se ramène à étudier le cas où $n \geq m$.

Dans ce cas, les calculs effectués à la question précédente, montre que la suite $(\deg R_i)_{1\leq i\leq l+1}$ est strictement décroissante. Tous les termes sont donc majorés par $\deg R_1 = m$ et $l \leq m$.

— Étudions la première ligne de l'instruction 3. On réalise les divisions euclidiennes de R_0 par R_1, de R_1 par $R_2, \ldots$ de R_{l-1} par R_l. D'après la question 2.10, le cout total est donc majoré par

$$\begin{aligned}\sum_{i=1}^{l}(2\deg R_l + 1)(\deg R_{l-1} - \deg R_l + 1) + 1 &\leq (2m+1)\sum_{i=1}^{l}(\deg R_{l-1} - \deg R_l + 1) + l \\ &\leq (2m+1)(l + \deg R_0 - \deg R_l) + l \\ &\leq (2m+1)(m+n) + m \leq 7mn\end{aligned}$$

— Étudions la deuxième ligne de l'instruction 3. L'opération $S_{i+1} \leftarrow S_{i-1} - Q_iS_i$ se décompose en la multiplication qui se réalise en $O(\deg Q_i \deg S_i)$ et l'addition dont le coût est majoré par $\min(\deg S_{i-1}, \deg(Q_iS_i)) + 1$.

Pour l'addition, on majore son coût par $\deg S_{i-1} + 1 \leq \deg R_1 + 1 \leq m + 1$ d'après la question 2. Le coût total de ces additions est donc $O(m^2) = O(mn)$.

Pour la multiplication, on a vu que $\deg Q_i = \deg R_{i-1} - \deg R_i$. Là encore, on peut majorer $\deg S_i$ par $m + 1$ et obtenir, par un téléscopage similaire à ci-dessus que le coût total des multiplications est $O(m \deg R_0) = O(mn)$.

— Étudions la troisième ligne de l'instruction 3. La méthode est similaire à celle ci-dessus pour la deuxième ligne. Il faut juste se méfier que l'on ne peut majorer $\deg T_i$ que par $\deg R_0 = n$.

Pour les additions, on obtient cette fois $O(mn)$ car on passe au plus m fois dans la boucle.

Pour les multiplications, on sépare la première ($i = 1$) des autres. Pour la première, $\deg Q_1 \leq n$ et $\deg T_1 = 0$, le calcul est donc en $O(n)$. Pour les suivantes, $\deg Q_i = \deg R_{i-1} - \deg R_i$. Un téléscopage comme ci-dessus permet de majorer le coût des multiplications par $O\left(\sum_{i=2}^{l} \deg T_i \deg Q_i\right)$ or

$$\sum_{i=2}^{l} \deg T_i \deg Q_i \leq n \sum_{i=2}^{l} \deg R_{i-1} - \deg R_i \leq n \deg R_1 = nm$$

L'algorithme 4 a bien un coût total en $O(nm)$.

3.4. On applique l'algorithme 4 aux polynômes M et P. On en déduit les suites (R_i) et (T_i). On a vu que la suite $(\deg R_i)_{0\leq i\leq l+1}$ est strictement décroissante avec $\deg R_{l+1} = -\infty$ et $\deg(R_0) = n$. Pour $k \in [\![0, n]\!]$, il existe donc un entier $i \in [\![1, l+1]\!]$ tel que

$$\deg R_i < k \leq \deg R_{i-1}$$

Pour cet entier, on a d'après 3.1 $S_iM + T_iP = R_i$ ce qui implique que R_i est congru à T_iP modulo M. De plus, $\deg R_i < k$ et, d'après la question 3.2

$$\deg T_i = \deg R_0 - \deg R_{i-1} = n - \deg R_{i-1} \leq n - k$$

3.5. a) On considère l'application $\Phi : \mathbb{K}_{n-1}[X] \to \mathbb{K}^n$ définie par $\Phi : P \mapsto (P(u_1), \dots, P(u_{n-1})$. C'est une application linéaire. Déterminons son noyau. Soit $P \in \mathsf{Ker}(\Phi)$. Pour tout $i \in [\![0, n-1]\!]$, $P(u_i) = 0$ et donc $(X - u_i)$ divise P. Comme les polynômes $(X - u_i)$ sont deux à deux premiers entre eux (puisque les u_i sont deux à deux distincts), $\prod_{i=0}^{n-1}(X - u_i)$ divise P. Or $\deg \prod_{i=0}^{n-1}(X - u_i) = n > \deg P$ donc $P = 0$.

On en déduit que Φ est injective. Comme $\dim \mathbb{K}_{n-1}[X] = n = \dim \mathbb{K}^n$, l'application Φ est bijective. Cela signifie que pour tout $(v_0, \dots, v_{n-1}) \in \mathbb{K}^n$, il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que $\Phi(P) = (v_0, \dots, v_{n-1})$ c'est-à-dire, $\forall i \in [\![0, n-1]\!], P(u_i) = v_i$.

b) En utilisant les notations de l'algorithme, à la fin de la boucle 2, $A = \prod_{k=0}^{n-1}(X - u_k)$ et donc, pour tout $i \in [\![0, n-1]\!]$, $A_i = \prod_{k \neq i}(X - u_k)$. Le polynôme renvoyé est donc

$$P = \sum_{i=0}^{n-1} v_i A_i / \alpha_i = \sum_{i=0}^{n-1} v_i \frac{\prod_{k \neq i}(X - u_k)}{\prod_{k \neq i}(\alpha_i - u_k)}$$

Il est clair que ce polynôme est le polynôme cherché car il est bien de degré inférieur ou égal à $n-1$, de plus, pour tout $i \in [\![0, n-1]\!]$ et tout $j \in [\![0, n-1]\!]$,

$$A_i(u_j) = \begin{cases} 0 & \text{si } i \neq j \\ \alpha_i & \text{si } i = j \end{cases}$$

De ce fait,

$$P(u_j) = \sum_{i=0}^{n-1} v_i \frac{A_i(u_j)}{\alpha_i} = v_j.$$

c) — La ligne 2 de l'algorithme consiste en n multiplications de polynômes. Le polynôme $X - u_i$ est de degré 1 et A est de degré au plus n. Chaque multiplication a un coût en $O(n)$ et donc le coût total est en $O(n^2)$.

— Étudions l'instruction 4. Le calcul du quotient de A (qui est de degré n) par $X - u_i$ qui est de degré 1 nécessite d'après la question 2.10 au plus $3n + 1$ opérations. Le calcul de α_i se fait en $O(n)$ opérations car $\deg(A_i) = n - 1 \leq n$. Pour finir $P \leftarrow P + v_i A_i / \alpha_i$ nécessite 1 opération pour calculer $\frac{v_i}{\alpha_i}$, n opérations pour calculer $v_i A_i / \alpha_i$ et finalement n opérations au plus pour la somme car $\deg(v_i A_i / \alpha_i) = n - 1$.

Finalement, l'instruction 4. se réalise en $O(n)$ opérations. Comme la boucle de la ligne 3. fait passer n fois dans cette ligne, on a un coût total en $O(n^2)$.

L'algorithme 5. se réalise en $O(n^2)$ opérations.

3.6. On pose $M = \prod_{i=0}^{n-1}(X - u_i)$ et P le polynôme interpolateur de degré au plus $n-1$ tel que pour tout $i \in [\![0, n-1]\!]$, $P(u_i) = v_i$.

Comme $\deg P < n = \deg M$, d'après la question 3.4, pour tout $k \in [\![0, n]\!]$, il existe un couple (R, T) tels que R soit congru à TP modulo M, $\deg R < k$ et $\deg T \leq n - k$ où $T \neq 0$.

Alors si on note $U \in \mathbb{K}[X]$ tel que $R = TP + UM$, pour tout $i \in [\![0, n-1]\!]$,

$$R(u_i) = T(u_i)P(u_i) + U(u_i)M(u_i) = T(u_i)v_i$$

car $M(u_i) = 0$.

3.7. En reprenant les calculs de la question 2.11, on voit que l'on a montré que la ligne 1. nécessitait $O(n^3)$ opérations et les les lignes 2 et 3 se réalisaient en $O(n^2)$.

La question 3.6 montre que l'on peut réaliser le calcul de la ligne 1. de l'algorithme 2 en $O(n^2)$ opérations. En effet il suffit de faire ce qui suit :

— On calcul $M = \prod_{i=0}^{n-1}(X - u_i)$ et P le polynôme interpolateur de degré au plus $n-1$ tel que pour tout $i \in [\![0, n-1]\!]$, $P(u_i) = v_i$. Le calcul de M se fait en $O(n^2)$ opérations et le calcul de P en $O(n^2)$ opérations d'après la question 3.5

— Pour $k = e$ fixé entre 0 et n, on détermine R et T comme dans la question 3.4 où v_i vaut y_i. On utilise pour cela l'algorithme 4. qui se réalise en $O(n^2)$ opérations d'après la question 3.3

— Le polynôme T n'est pas nul. Le polynôme F de l'algorithme 2. est $R/\mathrm{cd}(T)$, le polynôme E est $T/\mathrm{cd}(T)$ pour que E soit unitaire.

Finalement l'algorithme 2. peut se réaliser en $O(n^2)$ opérations.

Partie IV : Borne de la programmation linéaire

4.1. a) Soit $z \in \mathbb{R}$ tel que $|z| < \dfrac{1}{q-1}$. Commençons par faire le calcul, nous le justifierons après

$$\begin{aligned}
\sum_{k=0}^{\infty} K_k(x) z^k &= \sum_{k=0}^{\infty}\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j}z^k \\
&= \sum_{j=0}^{\infty}(-1)^j\binom{x}{j}\sum_{k=j}^{\infty}\binom{n-x}{k-j}(q-1)^{k-j}z^k \\
&= \sum_{j=0}^{\infty}\binom{x}{j}(-z)^j\sum_{k=0}^{\infty}\binom{n-x}{k}((q-1)z)^k \\
&= (1-z)^x(1+(q-1)z)^{n-x}
\end{aligned}$$

Il faut justifier que les séries considérées convergent et que l'on peut intervertir les deux sommes entre la première et la deuxième ligne. Pour cela il suffit de considérer la famille $(u_{j,k})_{(j,k)\in\mathbb{N}^2}$ définie par

$$u_{k,j} = \begin{cases} (-1)^j\binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j}z^k & \text{si } j \le k \\ 0 & \text{sinon} \end{cases}$$

On veut montrer que c'est une famille sommable. Pour cela on remarque que comme $|z| < \dfrac{1}{q-1} \le 1$, les deux séries $\sum_{j\ge 0}\binom{x}{j}(-z)^j$ et $\sum_{k\ge 0}\binom{n-x}{k}((q-1)z)^k$ sont absolument convergentes. Le calcul ci-dessus, en ajoutant des valeurs absolues, montre que pour tout $j \ge 0$, $\sum_{k\ge 0}|u_{j,k}|$ converge et que $\sum_{j\ge 0}\sum_{k=0}^{\infty}|u_{j,k}|$ converge. La famille $(u_{j,k})_{(j,k)\in\mathbb{N}^2}$ est bien sommable. Cela justifie le calcul précédent.

Note : On pouvait aussi reconnaitre un produit de Cauchy de deux séries entières.

b) Soit z tel que $|z| < \dfrac{1}{q-1}$,

$$\begin{aligned}
(1-z)^x(1+(q-1)z)^{n-x} &= (1-z)^n\left(\frac{1+(q-1)z}{1-z}\right)^{n-x} \\
&= (1-z)^n\left(1+\frac{qz}{1-z}\right)^{n-x} \\
&= (1-z)^n\sum_{i=0}^{\infty}\binom{n-x}{i}(qz)^i(1-z)^{-i} \\
&= \sum_{i=0}^{\infty}\binom{n-x}{i}q^iz^i(1-z)^{n-i} \\
&= \sum_{i=0}^{\infty}\sum_{j=0}^{n-i}\binom{n-x}{i}q^iz^i\binom{n-i}{j}(-1)^jz^j \\
&= \sum_{k=0}^{\infty}c_kz^k
\end{aligned}$$

où on pose $k = i + j$ et donc

$$c_k = \sum_{j=0}^{k}\binom{n-x}{k-j}q^{k-j}\binom{n-k+j}{j}(-1)^j$$

On obtient la formule voulue par unicité du développement en série entière.

c) Soit $m \in \mathbb{N}$, par définition, $\binom{n-x}{m}$ est un polynôme de degré m en x.

Soit $k \in \mathbb{N}$, pour tout $j \in [\![0,k]\!]$, $x \mapsto (-1)^jq^{k-j}\binom{n-k+j}{j}\binom{n-x}{k-j}$ est donc un polynôme de degré $k-j$. On en déduit que K_k est un polynôme de degré k.
Son coefficient dominant est obtenu en regardant le coefficient dominant du terme $j = 0$ de la somme. Ce terme $j = 0$ vaut

$$q^k\binom{n-x}{k} = \frac{q^k}{k!}(n-x)(n-x-1)\cdots(n-x-k+1) = \frac{q^k}{k!}((-1)^kx^k+\cdots)$$

Finalement le coefficient dominant de K_k est bien $\dfrac{(-q)^k}{k!}$.
En écrivant l'expression obtenue en a) pour $x = 0$, on a :

$$\sum_{k=0}^{\infty}K_k(0)z^k = (1+(q-1)z)^n = \sum_{k=0}^{n}\binom{n}{k}(q-1)^kz^k.$$

Par unicité du développement en série entière, $K_k(0) = \binom{n}{k}(q-1)^k$. En particulier, il est nul si $n > k$.

d) Soit $n \in N$. Soit y, z tels que $|y| \leq \frac{1}{q-1}$ et $|z| \leq \frac{1}{q-1}$. On a vu à la question a) que les séries $\sum_{k\geq 0} K_k(x)y^k$ et $\sum_{l\geq 0} K_l(x)z^l$ étaient absolument convergentes. On en déduit que, en posant

$$\alpha_{k,l} = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_k(i) K_l(i)$$

on a

$$\begin{aligned}
\sum_{k=0}^{\infty}\sum_{l=0}^{\infty} \alpha_{k,l} y^k z^l &= \sum_{i=0}^{n} \binom{n}{i} (q-1)^i (1-y)^i (1+(q-1)y)^{n-i} (1-z)^i (1+(q-1)z)^{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i} [(q-1)(1-y)(1-z)]^i [(1+(q-1)y)(1+(q-1)z)]^{n-i} \\
&= (1+(q-1)^2 yz + (q-1) + (q-1)yz)^n \\
&= q^n (1+(q-1)yz)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} q^n (q-1)^k z^k y^k
\end{aligned}$$

En travaillant à z fixé, par unicité du développement en série entière (de la variable y) on obtient que pour tout $k \in \mathbb{N}$,

$$\sum_{l=0}^{\infty} \alpha_{k,l} z^l = \binom{n}{k} q^n (q-1)^k z^k$$

On en déduit, par unicité du développement en série entière que

$$\forall (k,l) \in \mathbb{N}^2, \alpha_{k,l} = \begin{cases} \binom{n}{k} q^n (q-1)^k & \text{si } l = k \\ 0 & \text{sinon.} \end{cases}$$

e) On procède comme à la question précédente (les justifications des calculs sont les mêmes). Posons pour simplifier

$$\beta_{i,k} = (q-1)^i \binom{n}{i} K_k(i)$$

On a alors pour y et z tels que $|y| \leq \frac{1}{q-1}$ et $|z| \leq \frac{1}{q-1}$

$$\begin{aligned}
\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} \beta_{i,k} z^i y^k &= \sum_{i=0}^{\infty} (q-1)^i \binom{n}{i} z^i (1+(q-1)y)^{n-i} (1-y)^i \\
&= (1+(q-1)y + (q-1)z(1-y))^n \\
&= (1+(q-1)y + (q-1)z - (q-1)yz)^n
\end{aligned}$$

Le résultat obtenu est symétrique en y et z, on en déduit que

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} \beta_{i,k} z^i y^k = \sum_{i=0}^{\infty}\sum_{k=0}^{\infty} \beta_{i,k} y^i z^k$$

ce qui implique (comme ci-dessus en utilisant deux fois l'unicité de la décomposition en série entière) que, pour tout $(i,k) \in \mathbb{N}^2$, $\beta_{i,k} = \beta_{k,i}$

f) Soit k, l dans $\mathbb{N}$, en utilisant les deux questions précédentes,

$$\delta_{k,l}\binom{n}{k}(q-1)^k q^n = \sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_l(i) = \binom{n}{k}(q-1)^k \sum_{i=0}^{n} K_i(k)K_l(i)$$

Donc

$$\delta_{k,l} q^n = \sum_{i=0}^{n} K_i(k)K_l(i)$$

g) Soit $m \in \mathbb{N}$. On utilise b)

$$\begin{aligned}
\sum_{k=0}^{m}\binom{n-k}{n-m}K_k(x) &= \sum_{k=0}^{m}\binom{n-k}{n-m}\sum_{j=0}^{k}(-1)^j q^{k-j}\binom{n-x}{k-j}\binom{n-k+j}{j} \\
&= \sum_{j=0}^{m}\sum_{k=j}^{m}\binom{n-k}{n-m}(-1)^j q^{k-j}\binom{n-x}{k-j}\binom{n-k+j}{j} \\
&= \sum_{j=0}^{m}\sum_{k=0}^{m-j}\binom{n-k-j}{n-m}(-1)^j q^k\binom{n-x}{k}\binom{n-k}{j} \\
&= \sum_{k=0}^{m} q^k\binom{n-x}{k}\gamma_k
\end{aligned}$$

où

$$\gamma_k = \sum_{j=0}^{m-k}(-1)^j\binom{n-k-j}{n-m}\binom{n-k}{j}$$

or

$$\binom{n-k-j}{n-m}\binom{n-k}{j} = \binom{n-k}{n-m}\binom{m-k}{j}$$

donc

$$\gamma_k = \binom{n-k}{n-m}\sum_{j=0}^{m-k}(-1)^j\binom{m-k}{j} = \binom{n-k}{n-m}(1-1)^{m-k} = \delta_{m,k}$$

Dans la somme il ne reste que le terme pour $k = m$ et donc

$$\sum_{k=0}^{m}\binom{n-k}{n-m}K_k(x) = q^m\binom{n-x}{m}$$

h) On a vu que la famille (K_k) était une famille échelonnée en degré, c'est donc une base de $\mathbb{R}[X]$. De ce fait, si f est un polynôme de degré r, il existe $(f_0, \ldots, f_r)$ tels que $f = \sum_{k=0}^{r} f_k K_k$.

Pour déterminer les f_k il suffit d'utiliser les relations d'orthogonalité prouvée à la question d). On pose pour A, B deux polynômes

$$(A, B) = \sum_{i=0}^{n}\binom{n}{i}(q-1)^i A(i)B(j)$$

qui est une forme bilinéaire. Dès lors pour tout $s \in [\![0, r]\!]$,

$$(f, K_s) = \sum_{k=0}^{r} f_k (K_k, K_s) = f_s \binom{n}{s} (q-1)^s q^n$$

D'autre part,

$$(f, K_s) = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) K_s(i) = \sum_{i=0}^{n} \binom{n}{s} (q-1)^s f(i) K_i(s)$$

On en déduit que

$$f_s = q^{-n} \sum_{i=0}^{n} f(i) K_i(s)$$

4.2. On rappelle que pour $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ dans $\mathscr{A}^n$, on note $A_{x,y} = \{i \in [\![1, n]\!] \ , \ x_i \neq y_i\}$. Pour $u \in \mathscr{A}^n$, on notera pour simplifier

$$A_u = A_{u,0} = \{i \in [\![1, n]\!] \ , \ x_i \neq 0\}.$$

On pose alors pour tout $k \in [\![0, n]\!]$ et $j \in [\![0, k]\!]$

$$H_k = \{v \in (\mathbb{Z}/q\mathbb{Z})^n \ ; \ w_H(v) = k\} = \{v \in (\mathbb{Z}/q\mathbb{Z})^n \ ; \ \mathsf{Card}(A_v) = k\}$$

et

$$H_k(j) = \{v \in H_k \ ; \ \mathsf{Card}(A_u \cap A_v) = j\}$$

On voit pour commencer que les $H_k(j)$ quand j varie de 0 à k forment une partition de H_k et donc

$$\sum_{v \in H_k} \zeta^{u.v} = \sum_{j=0}^{k} \sum_{v \in H_k(j)} \zeta^{u.v}$$

Fixons alors j, se donner un élément $v \in H_k(j)$ revient à se donner :

(A) L'ensemble $\{p_1, \ldots, p_j\} = A_u \cap A_v$. Pour cela il faut choisir j nombres parmi les i éléments de A_u. Il y a $\binom{i}{j}$ possibilités.

(B) Choisir les éléments $v_{p_1}, \ldots, v_{p_j}$.

(C) Choisir les $k - j$ éléments de $\overline{A_u}$ qui sont dans A_v. Il y a $\binom{n-i}{k-j}$ possibilités.

(D) Choisir ses éléments. On sait juste qu'ils ne sont pas nul et donc il y a $(q-1)^{k-j}$ possibilités.

On suppose que l'on a fixé les choix pour (A), (C) et (D) et que l'on fait la somme que l'on obtient sur ces éléments de $H_k(j)$. On regarde donc

$$\sum_{(v_{p_1}, \ldots, v_{p_j}) \in (\mathbb{Z}/q\mathbb{Z} \setminus \{0\})^j} \zeta^{u_{p_1}.v_{p_1} + \cdots + u_{p_j}.v_{p_j}} = \sum_{(v_{p_1}, \ldots, v_{p_j}) \in (\mathbb{Z}/q\mathbb{Z} \setminus \{0\})^j} \zeta^{u_{p_1}.v_{p_1}} \times \cdots \times \zeta^{u_{p_j}.v_{p_j}}$$

Or, pour toute valeur $\alpha \in (\mathbb{Z}/q\mathbb{Z} \setminus \{0\})$,

$$\sum_{\beta \in (\mathbb{Z}/q\mathbb{Z} \setminus \{0\})} \zeta^{\alpha.\beta} = \sum_{\beta \in (\mathbb{Z}/q\mathbb{Z} \setminus \{0\})} (\zeta^{\alpha})^{\beta} = -1$$

car ζ^α étant une racine q-ième de l'unité différente de 1 (puisque ζ est supposée primitive), $\sum_{\beta=0}^{q-1} (\zeta^\alpha)^\beta = 0$. On obtient finalement que la valeur éttudiée ci-dessus, ne dépend pas des valeurs de $u_{p_1}, \dots, u_{p_k}$ et que l'on a à chaque fois

$$\sum_{(v_{p_1},\dots,v_{p_j})\in(\mathbb{Z}/q\mathbb{Z}\setminus\{0\})^j} \zeta^{u_{p_1}.v_{p_1}+\dots+u_{p_j}.v_{p_j}} = (-1)^j.$$

Finalement, en utilisant le dénombrement ci-dessus,

$$\sum_{v\in H_k} \zeta^{u.v} = \sum_{j=0}^{k} \sum_{v\in H_k(j)} \zeta^{u.v} = \sum_{j=0}^{k} (-1)^j \binom{i}{j}\binom{n-i}{k-j}(q-1)^{k-j} = K_k(i)$$

4.3. On fait le calcul

$$\begin{aligned}
|M| \sum_{i=0}^{n} A_i(C)K_k(i) &= \sum_{i=0}^{n} \sum_{\substack{(x,y)\in C^2 \\ \delta(x,y)=i}} K_k(i) \\
&= \sum_{i=0}^{n} \sum_{\substack{(x,y)\in C^2 \\ \delta(x,y)=i}} \sum_{v\in H_k} \zeta^{(x-y).v} \\
&= \sum_{(x,y)\in C^2} \sum_{v\in H_k} \zeta^{(x-y).v} \\
&= \sum_{v\in H_k} \sum_{(x,y)\in C^2} \zeta^{-x.v}\zeta^{-y.v} \\
&= \sum_{v\in H_k} \left(\sum_{x\in C} \zeta^{-x.v}\right)\overline{\left(\sum_{x\in C} \zeta^{y.v}\right)} \\
&= \sum_{v\in H_k} \left|\sum_{x\in C} \zeta^{-x.v}\right|^2 \geq 0
\end{aligned}$$

4.4. Soit C un code de taille maximale parmi tous les codes de longueur n et de distance d. On regarde la distribution des fréquences de C. Notons $M = A_q(n,d)$ sa taille.

- Il est clair que $A_0(C) = 1$ car $\{(u,v) \in C\times C \ ; \ d(u,v) = 0\}$ est la diagonale $\{(u,u) \ ; \ u \in C\}$ qui est de cardinal M.
- Comme C est de distance minimale d, si $i < d$, $\{(u,v) \in C\times C \ ; \ d(u,v) = 0\} = \emptyset$ et donc $A_i(C) = 0$.
- De manière évidente, $A_i(C) \geq 0$ pour $i \in [\![0,n]\!]$
- On vient de montrer que pour tout $k \in [\![0,n]\!]$, $\sum_{i=0}^{n} A_i(C)K_k(i) \geq 0$.

Remarquons de plus, que les ensembles $D_i = \{(u,v) \in C\times C \ ; \ d(u,v) = i\}$ quand i varie de 0 à n forment une partition de C^2 donc

$$\sum_{i=0}^{n} A_i(C) = \frac{1}{M}\sum_{i=0}^{n} \mathsf{Card}(D_i) = \frac{1}{M}\mathsf{Card}(C^2) = M.$$

On en déduit la formule voulue.

4.5. Considérons encore un code de taille maximale parmi tous les codes de longueur n et de distance d. On regarde la distribution des fréquences de C. Notons $M = A_q(n,d)$ sa taille. On a vu que pour tout $k \in [[0,n]]$ $\sum_{i=0}^{n} A_i(C)K_k(i) \geq 0$. En utilisant que $A_0(C) = 1$ et que $A_i(C) = 0$ pour $i \in [[1, d-1]]$, on obtient que $K_k(0) \geq -\sum_{i=d}^{n} A_i(C)K_k(i)$. De ce fait,

$$\begin{aligned} f(0) &= 1 + \sum_{k=1}^{n} f_k K_k(0) \\ &\geq 1 - \sum_{k=1}^{n} f_k \sum_{i=d}^{n} A_i(C)K_k(i) \\ &\geq 1 - \sum_{i=d}^{n} A_i(C) \sum_{k=1}^{n} f_k K_k(i) \\ &\geq 1 - \sum_{i=d}^{n} A_i(C)(f(i)-1) \\ &\geq 1 - \sum_{i=d}^{n} A_i(C)f(i) + \sum_{i=d}^{n} A_i(C) \\ &\geq 1 + \sum_{i=d}^{n} A_i(C) = M \end{aligned}$$

On a bien obtenu que $A_q(n,d) \leq f(0)$.

1) Soit d compris entre 1 et n. On considère le polynôme

$$f(x) = q^{n-d+1} \frac{\prod_{j=d}^{n}(j-x)}{\prod_{j=d}^{n} j}$$

Vérifions qu'il vérifie les conditions de la question précédente.

— Par construction, pour $j \geq d$, $f(j) = 0$.

— On sait que f se décompose sous la forme $f(x) = \sum_{k=0}^{n} f_k K_k(x)$ où, d'après la question 4.1.h,

$$\begin{aligned}
f_k &= \frac{1}{q^n}\sum_{i=0}^{n} f(i)K_i(k) \\
&= q^{1-d}\sum_{i=0}^{d-1} \frac{\prod_{j=d}^{n}(j-i)}{\prod_{j=d}^{n} j} K_i(k) \\
&= q^{1-d}\sum_{i=0}^{d-1} \frac{\frac{(n-i)!}{(d-i-1)!}}{\frac{n!}{(d-1)!}} K_i(k) \\
&= q^{1-d}\sum_{i=0}^{d-1} \frac{\binom{n-i}{n-d+1}}{\binom{n}{d-1}} K_i(k) \\
&= \frac{q^{1-d}}{\binom{n}{d-1}}\sum_{i=0}^{d-1} \binom{n-i}{n-d+1} K_i(k) \\
&= \frac{\binom{n-k}{d-1}}{\binom{n}{d-1}}
\end{aligned}$$

La dernière égalité venant de la question 4.1.g

En particulier, pour tout tout $k \in [\![0, n]\!]$, $f_k \geq 0$ et $f_0 = 1$.

On peut appliquer le résultat de la question précédente et on obtient que

$$A_q(n, q) \leq f(0) = q^{n-d+1}$$