

Arithmétique et applications, graphes et combinatoire

Cours No. 3, Codes correcteurs 2 : codes BCH

Un code Hamming est linéaire, parfait et 1-correcteur. Si un vecteur reçu contient plusieurs erreurs, ce vecteur est corrigible mais pas au bon mot. Les codes BCH rectifient ce problème. Ces codes étaient inventés pas le mathématicien français Alexis Hocquenghem en 1959 et independamment par Raj Bose et D. K. Ray-Chaudhuri en 1960. Dans la construction d'un code BCH on peut contrôler le nombre d'erreurs corrigibles par le code. Les mots dans un tel code sont des polynômes plutôt que des vecteurs.

Construction d'un code BCH : Soit $f(x) = x^m - 1 \in \mathbb{F}_2[x]$ pour m un entier positif. Alors $R = \mathbb{F}_2[x]/(f(x))$ est un anneau dont les éléments sont représentés par des polynômes de degrés inférieur à m . On suppose que $g(x) \in \mathbb{F}_2[x]$ divise $f(x)$. Soit

$$C := \{u(x)g(x) \in \mathbb{F}_2[x] : \deg(u(x)g(x)) < m\}.$$

Alors C est un sous-espace de R de dimension $m - \deg g(x)$. Les polynômes de C sont les mots d'un $[m, m - \deg g(x)]$ -code linéaire dans R contenant $2^{m - \deg g(x)}$ mots (on se rappelle de la notation " $[n, k]$ -code linéaire" pour un sous-espace de dimension k de $(\mathbb{F}_2)^n$). Le polynôme $g(x)$ est le *polynôme générateur* du code. Dans ce code, la longueur d'un mot est m ce qui correspond aux termes de chaque polynôme. En effet, chaque mot $c(x) \in \mathbb{F}_2[x]$ avec m termes correspond à un vecteur unique dans $(\mathbb{F}_1[x])^m$ dont les composantes sont les coefficients de $c(x)$ en ordre croissant en puissances de x .

Remarques : 1. On peut définir C comme l'idéal de $R = \mathbb{F}_2[x]/(f(x))$ engendré par $g(x)$. En effet, les éléments de cet idéal sont représentés par des polynômes $u(x)g(x)$ avec $\deg(u(x)g(x)) < m$.

2. Il s'agit d'un code *cyclique* : si $a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} \leftrightarrow (a_0a_1a_2 \dots a_{m-1}) \in C$, il en est de même pour $x(a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1}) = a_{m-1} + a_0x + a_2x^2 + \dots + a_{m-2}x^{m-1} \leftrightarrow (a_{m-1}a_0a_1 \dots a_{m-2})$ (car $x^m = 1$ dans R).

Exemple : Soit $f(x) = x^7 - 1$ et $g(x) = x^3 + x + 1$ dans $\mathbb{F}_2[x]$. Une base pour le code C qui consistent des multiples de $g(x)$ dans $\mathbb{F}_2[x]$ de degré inférieur à 7 est donnée par

$$\{x^3 + x + 1, x^4 + x^2 + x, x^5 + x^3 + x^2, x^6 + x^4 + x^3\}.$$

Le code C est un $[7, 4]$ -code linéaire contenant $16 = 2^4$ mots qui correspondent à toutes les combinaisons linéaires des éléments de la base dans $\mathbb{F}_2[x]$. Dans ce

code, on suppose que le mot $x^5 + x^4 + x^3 + x$ sera transmis comme le vecteur $0 + 1x + 0x^2 + 1x^3 + 1x^4 + 1x^5 + 0x^6 = (0101110) \in \mathbb{F}_2^7$.

Rappel sur le polynôme minimal : Une *extension* d'un corps K est un corps L qui contient K comme sous-corps. Un élément de L qui est une racine d'un polynôme non nul sur K est dit *algébrique* sur K . Si tout élément de L est algébrique sur K on dit que l'extension est algébrique. Le *polynôme minimal* d'un élément algébrique d'une extension de K est le polynôme unitaire de degré minimal parmi les polynômes à coefficients dans le corps de base K qui annule l'élément. Il s'agit d'un polynôme irréductible. Dans la notation ci-dessus, une racine a de $f(x)$ détermine un polynôme minimal $m(x)$ dans $\mathbb{F}_2[x]$ qui divise $f(x)$.

Afin que le code construit ci-dessus soit un code *BCH* on doit choisir $g(x)$ comme suite. Soient a_1, \dots, a_s ($s < m$) racines de $f(x)$ avec polynômes minimaux $m_1(x), \dots, m_s(x) \in \mathbb{F}_2[x]$ respectivement, et soit $g(x)$ le plus petit commun multiple des $m_i(x)$. On remarque que $g(x)$ divise $f(x)$ et donc peut être utilisé comme un polynôme générateur d'un code. Ce choix de $g(x)$ nous permet de corriger les erreurs dans le code qui se déduit. On doit aussi choisir l'entier m et les racines d'une manière particulière.

Rappel sur les racines primitives : Un élément primitif d'un corps fini est un générateur de son groupe multiplicatif. Le polynôme minimal d'un élément primitif est un *polynôme primitif*. Plus précisément, si on considère le corps fini \mathbb{F}_{p^n} , un polynôme irréductible $f(x)$ avec coefficients dans $\mathbf{Z}/p\mathbf{Z}$ est un polynôme primitif si son degré est n et s'il présente une racine $\alpha \in \mathbb{F}_{p^n}$ telle que $\{0, 1, \alpha, \alpha^2, \dots, \alpha^{p^n-2}\} = \mathbb{F}_{p^n}$. Il existe toujours un polynôme primitif de degré n .

Une autre façon de dire la même chose : un polynôme $f(x)$ à coefficients dans \mathbb{F}_p (p premier) est primitif si $f(x)$ est irréductible et si \bar{x} est un générateur du groupe cyclique K^* où $K = \mathbb{F}_p[x]/(f(x))$. En effet \bar{x} est racine de $f(x)$ dans K : $f(\bar{x}) = \bar{0}$.

Un polynôme irréductible de degré n sur le corps \mathbb{F}_2 est primitif si l'ordre de \bar{x} (l'ordre de α est le plus petit entier m tel que $\alpha^m = 1$) est $2^n - 1$. Par exemple, le polynôme $x^2 + x + 1$ est primitif car il est irréductible et l'ordre de \bar{x} dans $\mathbb{F}_2[x]/(x^2 + x + 1)$ est $3 = 2^2 - 1$: $x^3 = x(x^2) = x(x + 1) = x^2 + x = x + x + 1 = 1 \pmod{x^2 + x + 1}$.

Choix des racines pour un code BCH : Soit $m = 2^n - 1$ pour un entier positif n et soit $f(x) = x^m - 1 \in \mathbb{F}_2[x]$. Soit $p(x)$ un polynôme primitif de degré n dans $\mathbb{F}_2[x]$. Alors $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(p(x))$ est un corps d'ordre 2^n dont les éléments non nuls sont engendrés

par l'élément $a = \bar{x}$ (projection de x dans \mathbb{F}_{2^n} ; il s'agit de la notation habituelle dans ce domaine). Pour un code BCH on choisit les racines a_1, \dots, a_s comme $a_i = a^i$ pour $i = 1, \dots, s$. Les polynômes minimaux $m_i(x)$ sont alors les polynômes minimaux de a^i pour chaque $i = 1, \dots, s$. On peut en déduire $g(x)$ à partir des polynômes $m_i(x)$ en construisant le produit qui contient un seul facteur pour chaque $m_i(x)$ distinct. On appelle le code qui en résulte un *code BCH de longueur n et de distance construite s sur \mathbb{F}_2* (ou plus généralement sur \mathbb{F}_p).

Calculs dans un code BCH : Puisqu'on travaille dans $\mathbb{F}_2[x]$ on remarque que

$$(x_1 + x_2 + \dots + x_r)^2 = x_1^2 + x_2^2 + \dots + x_r^2.$$

Donc pour un polynôme $h(x) = x^{i_1} + x^{i_2} + \dots + x^{i_r} \in \mathbb{F}_2[x]$, il s'ensuit que

$$h(a^2) = (a^2)^{i_1} + (a^2)^{i_2} + \dots + (a^2)^{i_r} = (a^{i_1} + a^{i_2} + \dots + a^{i_r})^2 = h(a)^2.$$

De la même façon $h(a^{2k}) = h(a^k)^2$ pour tout entier positif k , donc $h(a^{12}) = h(a^6)^2 = h(a^3)^4$.

Exemple : Soit $f(x) = x^7 - 1$ et soit $p(x)$ le polynôme primitif $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

Alors l'élément $a = \bar{x} \in \mathbb{F}_2[x]/(p(x))$ est d'ordre 7 :

puissance	élément du corps
a^1	a
a^2	a^2
a^3	$a + 1$
a^4	$a^2 + a$
a^5	$a^2 + a + 1$
a^6	$a^2 + 1$
a^7	1

Soit C le code BCH qui se déduit en considérant les quatre premières puissances de a . Il faut alors trouver leurs polynômes minimaux $m_1(x), \dots, m_4(x)$. Puisque $p(x)$ est primitif et $a = \bar{x}$ il s'ensuit que $p(a) = 0$. En plus $p(a^2) = p(a)^2 = 0$ et $p(a^4) = p(a)^4 = 0$, d'où $m_1(x) = m_2(x) = m_4(x) = p(x)$. Puisque a^3 est une racine de $f(x)$, son polynôme minimal est un facteur dans la décomposition de $x^7 - 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$ en facteurs irréductibles (en général cette factorisation se fait par ordinateur). On voit que $x^3 + x^2 + 1$ annule a^3 , donc $m_3(x) = x^3 + x^2 + 1$ (dans la pratique on peut en déduire ce polynôme du tableau ci-dessus). Alors $g(x) = m_1(x)m_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Le code BCH correspondant est un $[7, 1]$ -code BCH avec $\{g(x)\}$ comme base ; il contient deux mots.

⁴Exemple : Soit $f(x) = x^{15} - 1$ et soit $p(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Pour l'élément $a = \bar{x} \in \mathbb{F}_2[x]/(p(x))$ d'ordre 15 on a

puissance	élément du corps
a^1	a
a^2	a^2
a^3	a^3
a^4	$a + 1$
a^5	$a^2 + a$
a^6	$a^3 + a^2$
a^7	$a^3 + a + 1$
a^8	$a^2 + 1$
a^9	$a^3 + a$
a^{10}	$a^2 + a + 1$
a^{11}	$a^3 + a^2 + 1$
a^{12}	$a^3 + a^2 + a + 1$
a^{13}	$a^3 + a^2 + 1$
a^{14}	$a^3 + 1$
a^{15}	1

On considère les six premières puissances de a ($s = 6$). Puisque $p(a) = 0 \Rightarrow p(a^2) = p(a^4) = 0$ il s'ensuit que $m_1(x) = m_2(x) = m_4(x) = p(x)$. Puisque a^3 et a^5 sont racines de $f(x)$, alors $m_3(x)$ et $m_5(x)$ sont facteurs irréductibles de

$$x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

En substituant a^3 et a^5 dans les facteurs on trouve que $m_3(x) = x^4 + x^3 + x^2 + x + 1$ et $m_5(x) = x^2 + x + 1$. En plus $m_3(a^6) = m_3(a^3)^2 = 0$ et $m_6(x) = m_3(x)$, d'où

$$g(x) = m_1(x)m_3(x)m_5(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Le code qui en résulte est un $[15, 5]$ -code BCH avec base $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$ contenant $2^5 = 32$ mots.

On verra dans la suite que si $s = 2t$ alors le code BCH est t -correcteur, donc le code de l'exemple est 3-correcteur.

Décodage pour un code BCH

Lemme : Soit C un code BCH de longueur n et de distance construite s sur \mathbb{F}_2 . Soit $a = \bar{x}$ et supposons que $c(x) \in \mathbb{F}_2[x]$ est de degré $< 2^n - 1$. Alors $c(x) \in C$ si et seulement si $c(a^i) = 0$ pour tout $i = 1, \dots, s$.

Preuve : Soit $m_i(x) \in \mathbb{F}_2[x]$ le polynôme minimal de a^i pour $i = 1, \dots, s$ et soit $g(x) \in \mathbb{F}_2[x]$ le ppcm des $m_i(x)$. Si $c(x) \in C$, alors $c(x) = g(x)h(x)$ pour $h(x) \in \mathbb{F}_2[x]$. Il s'ensuit que $c(a^i) = g(a^i)h(a^i) = 0 \times h(a^i) = 0$ pour chaque i . Réciproquement, si $c(a^i) = 0$ pour chaque i , alors $m_i(x)$ divise $c(x)$, d'où $g(x)$ divise $c(x)$ et $c(x) \in C$. \square

Soit C un code BCH de longueur n et de distance construite $2t$ sur \mathbb{F}_2 . Soit $c(x) \in C$ un mot transmis et soit $r(x) \neq c(x)$ le polynôme reçu, qu'on suppose est de degré $< m = 2^n - 1$. Alors $r(x) = c(x) + e(x)$ pour un polynôme d'erreur $e(x) \in \mathbb{F}_2[x]$ non nul. Afin de corriger $r(x)$ il faut déterminer $e(x)$. Par le lemme ci-dessus, $r(a^i) = e(a^i)$ pour tout $i = 1, \dots, 2t$. On appelle les valeurs $r(a^i)$ les *syndromes* de $r(x)$. On va montrer que le code est t -correcteur.

Supposons que

$$e(x) = x^{m_1} + x^{m_2} + \dots + x^{m_p}$$

pour des entiers $m_1 < m_2 < \dots < m_p$ ($p \leq t, m_p < 2^n - 1$) qui représentent les positions d'erreur (on se rappelle que les coefficients des différentes puissances de x correspondent au mot du code en notation binaire). Afin de trouver les positions d'erreur, on calcule les premiers $2t$ syndromes de $r(x)$:

$$\begin{aligned} r_1 &= r(a) = e(a) = a^{m_1} + a^{m_2} + \dots + a^{m_p} \\ r_2 &= r(a^2) = e(a^2) = (a^2)^{m_1} + (a^2)^{m_2} + \dots + (a^2)^{m_p} \\ &\vdots \\ r_{2t} &= r(a^{2t}) = e(a^{2t}) = (a^{2t})^{m_1} + (a^{2t})^{m_2} + \dots + (a^{2t})^{m_p} \end{aligned}$$

On introduit le polynôme $E(z)$ appelé *polynôme localisateur d'erreurs* :

$$E(z) = (z - a^{m_1})(z - a^{m_2}) \dots (z - a^{m_p}) = z^p - \sigma_1 z^{p-1} + \dots + (-1)^p \sigma_p$$

où les coefficients σ_j sont les fonctions élémentaires symétriques en a^{m_1}, \dots, a^{m_p} . (Puisqu'on travaille sur \mathbb{F}_2 on peut écrire $-1 = +1$ ci-dessus.) Les racines du polynôme localisateur d'erreurs déterminent les positions des erreurs dans $r(x)$.

Alors

$$\begin{aligned} \sigma_1 &= \sum_{1 \leq i \leq p} a^{m_i} \\ \sigma_2 &= \sum_{1 \leq i, j \leq p} a^{m_i} a^{m_j} \\ &\vdots \\ \sigma_p &= a^{m_1} \dots a^{m_p} \end{aligned}$$

On évalue $E(a^{m_j})$ pour tout $1 \leq j \leq p$ et on multiplie chaque résultat par $(a^{m_j})^i$ pour $1 \leq i \leq p$. Puisque $E(a^{m_j}) = 0$ pour tout $1 \leq j \leq p$, on obtient le système suivant pour chaque $1 \leq i \leq p$:

$$\begin{aligned} 0 &= (a^{m_1})^i \{ (a^{m_1})^p + \sigma_1 (a^{m_1})^{(p-1)} + \dots + \sigma_p \} \\ 0 &= (a^{m_2})^i \{ (a^{m_2})^p + \sigma_1 (a^{m_2})^{(p-1)} + \dots + \sigma_p \} \\ &\vdots \\ 0 &= (a^{m_p})^i \{ (a^{m_p})^p + \sigma_1 (a^{m_p})^{(p-1)} + \dots + \sigma_p \} \end{aligned}$$

En prenant la somme on obtient

$$0 = r_{i+p} + \sigma_1 r_{i+p-1} + \sigma_2 r_{i+p-2} + \dots + \sigma_p r_i$$

Puisque cette équation est vérifiée pour tout $1 \leq i \leq p$, on obtient le système linéaire :

$$(1) \quad \begin{pmatrix} r_1 & \cdots & r_p \\ \vdots & \ddots & \vdots \\ r_p & \cdots & r_{2p-1} \end{pmatrix} \begin{pmatrix} \sigma_p \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} r_{p+1} \\ \vdots \\ r_{2p} \end{pmatrix}$$

Il s'agit d'un système de p équations linéaires dans les p inconnus $\sigma_1, \dots, \sigma_p$. Si la $p \times p$ - matrice des coefficients est non-singulière on peut résoudre le système pour trouver les solutions uniques $\sigma_1, \dots, \sigma_p$. Puis on peut calculer le polynôme localisateur d'erreurs $E(z)$ et déterminer a^{m_1}, \dots, a^{m_p} pour des méthodes ad hoc afin de trouver les positions des erreurs m_1, \dots, m_p .

Si $r(x)$ ne contient pas exactement t erreurs, alors le $t \times t$ - matrice en (1) sera singulière. Dans ce cas on réduit le nombre des erreurs supposées à $t - 1$ et on répète le processus un appliquant les premiers $2t - 2$ syndromes de $r(x)$. Si $r(x)$ ne contient pas exactement $t - 1$ erreurs la matrice sera singulière et on réduit encore le nombre d'erreurs supposées. On continue ainsi de suite. Si l'erreur en $r(x)$ n'est pas corrigible, la matrice des coefficients sera singulière pour tout nombre d'erreurs supposées entre 1 et t .

Exemple : On reprend l'exemple ci-dessus avec polynôme générateur

$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$. On suppose qu'on a transmis un mot dans \mathbb{F}_2^{15} et on reçoit le vecteur $r = (101111110010000) \in \mathbb{F}_2^{15}$. Ce vecteur correspond au polynôme $r(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{10} \in \mathbb{F}_2[x]$. On vérifie aisément que $g(x)$ ne divise pas $r(x)$ donc $r(x) \notin C$. Puisque C est 3-correcteur, on commence en calculant les 6 premiers syndromes de $r(x)$. Pour ça on applique le tableau des puissances de a . On laisse ces calculs comme une exercice :

$$r_1 = r(a) = \dots = a^3, \quad r_3 = r(a^3) = \dots = a^6, \quad r_5 = r(a^5) = \dots = a^{10}$$

Puisqu'on travaille sur \mathbb{F}_2 on peut trouver les syndromes qui restent :

$$r_2 = r(a^2) = (r(a))^2 = a^6, \quad r_4 = r(a^4) = (r(a))^4 = a^{12}, \quad r_6 = r(a^6) = (r(a^3))^2 = a^{12}$$

L'équation (1) devient:

$$\begin{pmatrix} a^3 & a^6 & a^6 \\ a^6 & a^6 & a^{12} \\ a^6 & a^{12} & a^{10} \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^{12} \\ a^{10} \\ a^{12} \end{pmatrix}$$

Le déterminant de la matrice des coefficients égale a^{12} ; elle est donc non-singulière.

On peut appliquer la règle de Cramer afin de déterminer $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{vmatrix} a^{12} & a^6 & a^6 \\ a^{10} & a^6 & a^{12} \\ a^{12} & a^{12} & a^{10} \end{vmatrix} = a^{14} \Rightarrow \sigma_3 = \frac{a^{14}}{a^{12}} = a^2$$

$$\begin{vmatrix} a^3 & a^{12} & a^6 \\ a^6 & a^{10} & a^{12} \\ a^6 & a^{12} & a^{10} \end{vmatrix} = a^{10} \Rightarrow \sigma_2 = \frac{a^{10}}{a^{12}} = a^{-2}$$

$$\begin{vmatrix} a^3 & a^6 & a^{12} \\ a^6 & a^6 & a^{10} \\ a^6 & a^{12} & a^{12} \end{vmatrix} = 1 \Rightarrow \sigma_1 = \frac{1}{a^{12}} = a^{-12}$$

Le polynôme localisateur d'erreurs est alors $E(z) = z^3 + a^3z^2 + a^{13}z + a^2$. On trouve ses racines en calculant ce polynôme en différentes puissances de a . Les racines sont $1, a^5, a^{12}$. Donc l'erreur en $r(x)$ est $e(x) = 1 + x^5 + x^{12}$. On corrige $r(x)$ afin de trouver le mot du code $c(x)$:

$$c(x) = r(x) + e(x) = x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12}$$

On peut vérifier directement que ce polynôme est un multiple de $g(x)$.

Supposons qu'on reçoit un autre vecteur $r = (100100010011010) \in \mathbb{F}_2^{15}$, ce qui correspond au polynôme $1 + x^3 + x^7 + x^{10} + x^{11} + x^{13} \in \mathbb{F}_2[x]$. Ce polynôme n'est pas un multiple de $g(x)$ donc $r(x) \notin C$. Dans ce cas, la matrice des coefficients

$$\begin{vmatrix} a^5 & a^{10} & a^2 \\ a^{10} & a^2 & a^5 \\ a^2 & a^5 & 1 \end{vmatrix}$$

est de déterminant 0. On suppose alors que r ne contient deux erreurs et on résout

$$\begin{pmatrix} a^5 & a^{10} \\ a^{10} & a^2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^2 \\ a^5 \end{pmatrix}$$

Dans ce cas le déterminant est non nul et on peut trouver l'erreur. On laisse les détails comme une exercice.

Théorème : Soit C un code BCH de longueur n et de distance construite $2t$ sur \mathbb{F}_2 . Alors C est t -correcteur.

Preuve : Soit $m = 2^n - 1$ et soit $a = \bar{x}$. On définit la matrice:

$$H = \begin{pmatrix} 1 & a & a^2 & \dots & a^{m-1} \\ 1 & a^2 & (a^2)^2 & \dots & (a^2)^{m-1} \\ 1 & a^3 & (a^3)^2 & \dots & (a^3)^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^{2t} & (a^{2t})^2 & \dots & (a^{2t})^{m-1} \end{pmatrix}$$

Pour un polynôme $r(x) = b_0 + b_1x + \dots + b_{m-1}x^{m-1} \in \mathbb{F}_2[x]$, si on écrit $b = (b_0, b_1, \dots, b_{m-1})$, alors $Hb^t = (r_1, r_2, \dots, r_{2t})^t$. Donc $r(x) \in C$ si et seulement si Hb^t est le vecteur nul.

On peut alors considérer H comme une matrice de contrôle pour C .

On montre que le nombre minimal de colonnes de H qui sont linéairement dépendantes est $2t + 1$. En effet, tout ensemble de $2t$ colonnes est indépendant : on choisit des entiers $0 \leq j_1 < j_2 < \dots < j_{2t} < m$; les colonnes de H correspondantes déterminent la $2t \times 2t$ -matrice

$$\begin{pmatrix} a^{j_1} & a^{j_2} & \dots & a^{j_{2t}} \\ (a^2)^{j_1} & (a^2)^{j_2} & \dots & (a^2)^{j_{2t}} \\ \vdots & \vdots & \ddots & \vdots \\ (a^{2t})^{j_1} & (a^{2t})^{j_2} & \dots & (a^{2t})^{j_{2t}} \end{pmatrix}$$

Le déterminant de cette matrice s'exprime :

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ a^{j_1} & a^{j_2} & \dots & a^{j_{2t}} \\ \vdots & \vdots & \ddots & \vdots \\ (a^{j_1})^{2t-1} & (a^{j_2})^{2t-1} & \dots & (a^{j_{2t}})^{2t-1} \end{vmatrix} \times a^{j_1} a^{j_2} \dots a^{j_{2t}}$$

Il s'agit d'une matrice de Vandermonde dont le déterminant est non-nul. Il s'ensuit que tout ensemble de $2t$ colonnes est indépendant. D'autre part, le nombre de lignes de H est $2t$ et par suite tout ensemble de $2t + 1$ colonnes est dépendant. Par un théorème du dernier chapitre, la distance minimale de C est $2t + 1$ et C est t -correcteur. \square

Référence : R. Klima, N. Sigmon et E. Stitzinger, Applications of Abstract Algebra⁹
with Maple, CRC Press 1999.