PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

MICHEL ANDRÉ

Théorie noethérienne des codes linéaires

Publications des séminaires de mathématiques et informatique de Rennes, 1980, fascicule S3
« Colloque d'algèbre », , p. 83-111

<http://www.numdam.org/item?id=PSMIR_1980___S3_83_0>

THEORIE NOETHERIENNE DES CODES LINEAIRES

Michel ANDRE - EPFL

Un code linéaire sur un anneau commutatif et noethérien A consiste en un monomorphisme fendu de A-modules aboutissant à un A-module libre (de rang fini) dont une base est fixée. L'anneau A est un corps dans la théorie classique. Un code linéaire possède une distance de Hamming qui est le minimum des poids des éléments non nuls de l'image du monomorphisme, le poids d'un élément étant le nombre de composantes non nulles. Un homomorphisme d'anneaux de A dans B et un code sur A produisent par produit tensoriel un code sur B . Par un raisonnement axiomatique simple, il est démontré que toutes les distances de Hamming peuvent être calculées en utilisant des corps seulement. En d'autres termes, en utilisant les anneaux noethériens au lieu des corps seulement, on n'obtient pas des codes avec de meilleures performances, on obtient seulement des codes avec d'autres alphabets. En fait, la distance de Hamming d'un code linéaire sur une A-algèbre B est égale au minimum des entiers obtenus de la manière suivante. On considère un idéal premier P de l'anneau A, associé au A-module B et on considère la distance de Hamming du code linéaire défini sur la A-algèbre k(P) , l'anneau k(P) étant le corps des fractions de l'anneau intègre A/P. Un exemple est étudié de manière complète : l'anneau est local et le code est cyclique (avec une restriction). Alors le code sur le corps résiduel possède non seulement une distance de Hamming, mais encore une distance de Cohen et le code sur l'anneau local a une distance de Hamming égale à l'un ou l'autre de ces deux nombres.

ALGEBRE COMMUTATIVE

Tous les anneaux considérés sont commutatifs et unitaires. Tous les modules considérés sont unitaires.

Définition 1. Une quasi-distance sur l'anneau A (notée d_A ou simplement d) associe à chaque A-module M un nombre entier d(M) , strictement positif, en satisfaisant aux deux conditions suivantes.

Axiome I. A chaque suite exacte courte de A-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

correspond une inégalité double

$$d(M') \geqslant d(M) \geqslant \min [d(M'), d(M'')].$$

Axiome II. A chaque A-module M correspond une égalité

$$d(M) = \min [d(M') \mid M' \varepsilon \overline{M}]$$

$\overline{M}$ désignant l'ensemble des sous-modules de M de type fini.

Remarque 2. Deux modules isomorphes donnent lieu au même entier. L'axiome I permet de démontrer une inégalité

$$d(M) \leqslant \min[d(M') \mid M' \varepsilon \overline{M}] \ .$$

L'axiome II affirme en plus qu'il existe un sous-module M' de type fini avec l'égalité

$$d(M) = d(M').$$

L'entier $d(M)$ est toujours majoré par l'entier $d(0)$, appelé la norme de la quasi-distance. C'est utile d'avoir la convention suivante concernant l'ensemble vide

$$\min [d(M) \mid M \varepsilon \Phi] = d(0).$$

Définition 3. Une quasi-distance satisfaisant à la condition supplémentaire suivante est une distance.

Axiome III. A chaque produit direct de A-modules

$$M = \Pi[M_i \mid i \varepsilon I].$$

correspond une égalité

$$d(M) = \min[d(M_i) \mid i \varepsilon I].$$

Cet axiome est intéressant seulement pour I infini. Il affirme simplement qu'il existe un facteur M_i avec $d(M_i)$ et $d(M)$ égaux. Dénotons par Ass M (ou plus précisément par $\mathrm{Ass}_A M$) l'ensemble des idéaux premiers associés au A-module M. Un premier P est associé au module M, si et seulement s'il existe un monomorphisme de A-modules de A/P dans M. Si l'anneau A est noethérien, l'ensemble Ass M n'est pas vide, si M n'est pas nul et cet ensemble est fini, si le module est de type fini (voir [1] Chapitre IV, Paragraphe 1, Proposition 2, Corollaire 1 et Théorème 2, Corollaire 1).

Remarque 4. Il est bien connu (voir [1] Chapitre IV, Paragraphe 1, Proposition 3) qu'à une suite exacte courte de A-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

correspond une inclusion double

$$\mathrm{Ass}\ M' \subseteq \mathrm{Ass}\ M \subseteq \mathrm{Ass}\ M' \cup \mathrm{Ass}\ M''$$

De plus le foncteur Ass préserve les unions.
Si le A-module M est présenté comme une réunion de certains de ses sous-modules

$$M = \cup [M_j \mid j \in J]$$

alors l'égalité suivante a lieu

$$\mathrm{Ass}\ M = \cup [\mathrm{Ass}\ M_j \mid j \in J] \ .$$

Exemple 5. Un entier n est fixé. Pour chaque idéal premier P de l'anneau A est donné un entier $f(P)$ compris entre 1 et n. On considère alors l'entier

$$d(M) = \min [f(P) \mid P \in \mathrm{Ass}_A M]$$

pour chaque A-module M (en particulier l'entier n pour le module nul). Par exemple $d(A/P)$ et $f(P)$ sont égaux. On a là une quasi-distance sur A. En effet, l'inclusion double (respectivement l'égalité)

de la remarque précédente donne immédiatement l'axiome I (respectivement l'axiome II).

Remarque 6. Soit S un ensemble multiplicativement clos dans A et soit M un A-module. Supposons S disjoint de l'annulateur dans A de tout élément non nul de M. Cette condition est satisfaite en particulier si, de manière simultanée, l'anneau A est noethérien et l'ensemble S a une intersection vide avec tous les idéaux premiers associés à M (voir [1] Chapitre IV, Paragraphe 1, Proposition 2). Il est alors élémentaire de vérifier que les A-modules M et $S^{-1}M$ ont les mêmes sous-modules de type fini, à isomorphismes près. En conséquence $d(M)$ et $d(S^{-1}M)$ sont égaux. En particulier, remplacer un anneau intègre par son corps des fractions ne modifie pas la valeur d'une quasi-distance.

Théorème 7. Soit d une quasi-distance sur un anneau noethérien A. Alors l'égalité

$$d(M) = \min [d(A/P) \mid P \in \mathrm{Ass}_A M]$$

est satisfaite pour tout A-module M.

Démonstration. D'après l'axiome II et d'après l'égalité de la remarque 4, il suffit de démontrer le cas d'un A-module M de type fini. On va procéder par induction sur le nombre k des idéaux premiers associés à M.

Commençons l'induction par le cas où k est égal à 1 : autrement dit M possède un unique idéal premier associé P. On localise par rapport à l'ensemble multiplicativement clos S égal à $A-P$. On obtient un anneau local noethérien A_P d'idéal maximal PA_P et un A_P-module M_P de type fini avec un unique idéal premier associé PA_P (voir [1] Chapitre IV, Paragraphe 1, Proposition 5, Corollaire 1). Mais alors il existe une suite de décomposition (formée de A_P-modules) .

$$0 = N_0 \subset N_1 \subset \ldots \subset N_{h-1} \subset N_h = M_P$$

avec le A_P-module N_i/N_{i-1} toujours isomorphe à A_P/PA_P, c'est-à-dire à $(A/P)_P$ (voir [1] Chapitre IV, Paragraphe 1, Théorèmes 1 et 2). L'axiome I donne alors des inégalités

$$d(N_{i-1}) \geq d(N_i) \geq \min[d(N_{i-1}), d(N_1)]$$

qui donnent immédiatement l'égalité

$$d(M_p) = d(A_p/PA_p) .$$

Mais alors la remarque 6 donne deux égalités

$$d(M) = d(M_p) \text{ et } d(A/P) = d(A_p/PA_p)$$

qui donnent finalement l'égalité souhaitée

$$d(M) = d(A/P)$$

du cas particulier où k est égal à 1.

Passons au pas général de l'induction. Soit Q un idéal premier associé à M jouissant de la propriété

$$d(A/P) \geq d(A/Q) \quad \text{si} \quad P \in \mathrm{Ass}_A M .$$

Alors il existe une suite exacte courte de A-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

donnant lieu à deux égalités

$$\mathrm{Ass}\ M' = \{Q\} \text{ et } \mathrm{Ass}\ M'' = \mathrm{Ass}\ M - \{Q\} .$$

D'après l'axiome I et d'après l'hypothèse d'induction, les inégalités suivantes sont satisfaites

$$\begin{aligned}
&\min[d(A/P) \mid P \in \mathrm{Ass}\ M] = d(A/Q) = \\
&d(M') \geq d(M) \geq \min[d(M'), d(M'')] \geq \\
&\min[d(A/Q), \min[d(A/P) \mid P \in \mathrm{Ass}\ M'']] = \\
&\min[d(A/P) \mid P \in \mathrm{Ass}\ M] .
\end{aligned}$$

On a donc bien l'égalité du théorème. La démonstration par induction

est ainsi terminée.

Exemple 8. Il est utile de prendre note du cas particulier suivant, qui se démontre d'ailleurs directement. Soit B une A-algèbre intègre et soit P l'annulateur dans A de l'élément 1 de B . Alors les entiers d(A/P) et d(B) sont égaux.
Le théorème précédent s'applique à la théorie des codes, comme nous le verrons plus loin. Pour le moment, contentons-nous de redémontrer un résultat connu, utile pour la suite (voir [1] Chapitre IV, Paragraphe 2, Théorème 2).

Proposition 9. Pour deux A-modules M et F l'égalité suivante est satisfaite

$$\mathrm{Ass}_A(M \otimes_A F) = \{P \in \mathrm{Ass}_A M \mid F \neq PF\}$$

si l'anneau A est noethérien et si le module F est plat.

Démonstration. Le module plat F est fixé et un idéal premier Q est fixé. Pour tout A-module M, on pose alors la définition suivante

$$d(M) = 1 \quad \text{si} \quad Q \in \mathrm{Ass}_A (M \otimes_A F)$$
$$d(M) = 2 \quad \text{si} \quad Q \notin \mathrm{Ass}_A (M \otimes_A F) .$$

Considérons une suite exacte courte de A-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Par platitude, on obtient une seconde suite exacte courte de A-modules

$$0 \longrightarrow M' \otimes_A F \longrightarrow M \otimes_A F \longrightarrow M'' \otimes_A F \longrightarrow 0$$

et par suite une inclusion double (voir la remarque 4)

$$\mathrm{Ass}(M' \otimes F) \subseteq \mathrm{Ass}(M \otimes F) \subseteq \mathrm{Ass}(M' \otimes F) \cup \mathrm{Ass}(M'' \otimes F) .$$

Il est alors facile de montrer que l'axiome I est vérifié par d. Considérons un monomorphisme (d'inclusion d'un sous-module de type fini)

$$M' \longrightarrow M \quad \text{avec} \quad M' \quad \text{dans} \quad \overline{M} .$$

Par platitude, on obtient un second monomorphisme (à identifier avec une inclusion)

$$M' \otimes_A F \longrightarrow M \otimes_A F .$$

En fait, on a une égalité

$$M \otimes F = \bigcup [M' \otimes F \mid M' \in \overline{M}]$$

puisque tout élément de $M \otimes F$ peut se décrire en utilisant un nombre fini d'éléments de M. On a alors une égalité (voir la remarque 4)

$$Ass(M \otimes F) = \bigcup [Ass(M' \otimes F) \mid M' \in \overline{M}] .$$

Il est alors facile de montrer que l'axiome II est vérifié par d. On a donc une quasi-distance d sur A et on peut appliquer le théorème 7. La conclusion en est celle-ci : l'idéal premier Q est associé au A-module $M \otimes_A F$ si et seulement s'il existe un idéal premier P associé au A-module M avec Q associé au A-module

$$A/P \otimes_A F = F/PF .$$

On a alors la conclusion de la proposition, car si le A-module F/PF n'est pas nul, il a P comme unique associé, Pour le voir, on utilise la platitude de F. Un élément a de A n'appartenant pas à P donne un premier monomorphisme

$$a : A/P \longrightarrow A/P \quad \text{(multiplication par a)}$$

donc un second monomorphisme par platitude

$$a : F/PF \longrightarrow F/PF \quad \text{(multiplication par a)} .$$

Mais alors l'annulateur dans A d'un élément non nul de F/PF est forcément égal à P. S'il n'est pas nul, le A-module F/PF a donc P comme unique associé. La proposition est ainsi démontrée.

Revenons à la théorie générale des quasi-distances. En particulier sur les anneaux noethériens, on peut donner à l'axiome II une forme plus forte que voici .

Lemme 10 . Soit d une quasi-distance sur un anneau noethérien A. Si le A-module M est présenté comme une réunion de certains de ses sous-modules

$$M = \bigcup [M_j | j \in J]$$

alors l'égalité suivante a lieu

$$d(M) = \min [d(M_j) | j \in J] .$$

Démonstration. C'est un corollaire du théorème 7, grâce à l'égalité de la remarque 4. Les égalités

$$\begin{aligned} & d(M) = \min [d(A/P) | P \in \operatorname{Ass} M] = \\ & \min [d(A/P) | P \in \bigcup [\operatorname{Ass} M_j | j \in J]] = \\ & \min [\min [d(A/P) | P \in \operatorname{Ass} M_j] | j \in J] = \\ & \min [d(M_j) | j \in J] \end{aligned}$$

constituent la démonstration du lemme.

Remarque 11. Considérons une quasi-distance (respectivement une distance) d_A sur un anneau noethérien A et aussi une A-algèbre B, pas forcément noethérienne. Alors d_A donne une quasi-distance (respectivement une distance) d_B sur l'anneau B , par la définition suivante pour tout B-module M

$$d_B(M) = d_A(M)$$

avec la structure naturelle de A-module que possède M . L'axiome I (respectivement III) sur A donne l'axiome I (respectivement III) sur B . Le lemme précédent donne l'axiome II sur B , les sous-modules M_j étant les sous-modules de type fini du B-module M, considérés comme A-modules.

Proposition 12. Soit d une quasi-distance sur un anneau noethérien A. Alors il s'agit d'une distance si et seulement si l'inégalité suivante

$$d(A/P) \leqslant d(A/Q)$$

a lieu chaque fois que l'idéal premier P contient l'idéal premier Q.

Démonstration. Etablissons la nécessité de la condition. D'après l'exemple 8 pour les A-algèbres $(A/Q)_P$ et $(A/P)_P$, on a deux égalités utiles

$$d(A/Q) = d((A/Q)_P), d(A/P) = d((A/P)_P).$$

Il suffit donc de considérer un anneau local A avec une distance d, un idéal premier P maximal et un idéal premier Q nul. On veut démontrer l'inégalité

$$d(A/P) \leqslant d(A) .$$

Le A-module A/P^i a un unique idéal premier associé, à savoir P. On a donc l'égalité du théorème 7

$$d(A/P^i) = d(A/P)$$

égalité qui se démontre d'ailleurs directement à partir de l'axiome I. Considérons maintenant l'inclusion de Krull (voir [1] Chapitre III, Paragraphe 3, Proposition 5, Corollaire 1)

$$A \longrightarrow \Pi[A/P^i \mid i \leqslant 1] .$$

Les axiomes I et III donnent alors les inégalités suivantes

$$d(A) \geqslant d(\Pi[A/P^i \mid i \geqslant 1]) =$$
$$\min[d(A/P^i) \mid i \geqslant 1] = d(A/P)$$

ce qui donne l'inégalité souhaitée.

Etablissons la suffisance de la condition. Pour tout ensemble E d'idéaux de A, considérons le sous-ensemble E^* des éléments de E maximaux pour l'inclusion. Comme A est noethérien, tout idéal appartenant à E est contenu dans un idéal au moins appartenant à E^*. Vu l'hypothèse, l'égalité du théorème 7 s'écrit de la manière suivante

$$d(M) = \min[d(A/P) | P \in \mathrm{Ass}^* M] .$$

Il nous faut considérer un produit direct de A-modules

$$M = \Pi[M_i | i \in I] .$$

On a une inclusion de nature élémentaire

$$\cup[\mathrm{Ass}\ M_i | i \in I] \subseteq \mathrm{Ass}\ M .$$

Les éléments maximaux sont les mêmes à gauche et à droite (voir ci-dessous). On a alors les égalités concluantes suivantes

$$\begin{aligned}
&\min[d(M_i) | i \in I] = \\
&\min[\min[d(A/P) | P \in \mathrm{Ass}\ M_i] | i \in I] = \\
&\min[d(A/P) | P \in \cup[\mathrm{Ass}\ M_i | i \in I]] = \\
&\min[d(A/P) | P \in \cup^*[\mathrm{Ass}\ M_i | i \in I]] = \\
&\min[d(A/P) | P \in \mathrm{Ass}^* M] = d(M) .
\end{aligned}$$

Démontrons pour terminer l'égalité mentionnée ci-dessus à propos des éléments maximaux. Il s'agit essentiellement de démontrer qu'un élément maximal P de $\mathrm{Ass}\ M$ est associé à un des modules M_i. Comme P est associé à M, il existe un monomorphisme de A/P dans M. En utilisant la projection correspondant à un indice i bien choisi, on obtient un homomorphisme non nul η de A/P dans M_i. Soit Q un idéal premier associé à l'image de η. D'une part Q contient P et d'autre part Q est associé non seulement à M_i mais encore à M. Il ne peut donc s'agir que de P lui-même. Autrement dit P est bien associé à un des modules M_i au moins. La proposition 12 est démontrée.

Remarque 13. Pour une distance d sur un anneau noethérien A, l'égalité suivante

$$d(M) = \min[d(A/P) \mid P \in Ass^*_A M]$$

est toujours satisfaite. On désigne par Ass^* le sous-ensemble de Ass formé des éléments de Ass maximaux pour l'inclusion (à ne pas confondre avec le sous-ensemble des idéaux maximaux appartenant à Ass).

Il est utile de disposer du résultat suivant, comme le démontre l'exemple ci-dessous.

Lemme 14. Pour deux A-modules M et F l'égalité suivante est satisfaite

$$d(M \otimes_A F) = d(M)$$

si l'anneau A est noethérien et si le module F est fidèlement plat.

Démonstration. Puisque le module A/P n'est pas nul, le module

$$F/PF = A/P \otimes F$$

n'est pas nul. D'après la proposition 9, les A-modules M et $M \otimes F$ ont les mêmes associés, donc la même valeur pour la quasi-distance d d'après le théorème 7.

Exemple 15. Considérons un anneau local et noethérien A ainsi que son complété-séparé $\hat{A}$ (pour la topologie due à l'idéal maximal). Le lemme précédent dans le cas particulier

$$M = A \quad \text{et} \quad F = \hat{A}$$

démontre que les entiers $d(A)$ et $d(\hat{A})$ sont égaux (pour la fidèle platitude du A-module $\hat{A}$ voir [1] Chapitre III, Paragraphe 3, Proposition 9).

CODES LINEAIRES

Considérons le A-module libre A^n de rang n , accompagné de sa base canonique. Par définition, un code linéaire de longueur n et d'alphabet A est un sous-module direct L de A^n . Autrement dit, on a non seulement un monomorphisme d'inclusion j mais encore un épimorphisme q de A-modules avec une bonne propriété.

$$j:L \longrightarrow A^n \ , \ q:A^n \longrightarrow L \ , \ q \circ j = Id \ .$$

L'homomorphisme q (ou plus exactement Id-q) joue le rôle d'une matrice de contrôle (check matrix) dans le cas classique où l'anneau A est un corps (voir [2] Chapitre I, Paragraphe 1). Le A-module L est projectif, sans être libre en général, si l'anneau A n'est pas local. Généralisons un peu.

Définition 16. Considérons un A-module M et le A-module M^n .

$$M^n = A^n \otimes_A M$$

sans oublier qu'il s'agit d'un produit direct

$$M^n = M_1 \times \ldots \times M_n \quad \text{avec} \quad M_i = M \ .$$

Soit $\Pi_i : M^n \longrightarrow M$ la i-ème projection due au module $M_i = M$. Alors un code linéaire de longueur n sur M est un sous-module direct L de M^n . On dira simplement qu'il s'agit d'un code. Un élément s de M^n a un poids

$$w(s) = \text{card } \{1 \leqslant i \leqslant n \mid \Pi_i(s) \neq 0\} \ .$$

C'est la définition classique. Alors la distance de Hamming du code est égale par définition à l'entier strictement positif.

$$d = \min [w(s) \mid s \in L, \ s \neq 0] \ .$$

Ce nombre est compris entre 1 et n . Il est bien connu qu'un code ayant la distance de Hamming d est un code corrigeant $[(d-1)|2]$ erreurs de transmission (voir [2] Chapitre I, Paragraphe 3). Si le code est tri-

vial, c'est-à-dire si le module L est nul, la distance de Hamming est dite valoir n .

Exemple 17. Voici l'exemple générique qui va nous intéresser par la suite. Considérons un code de longueur n sur l'anneau A , autrement dit un sous-module direct L du module A^n . Un sous-module direct donne un sous-module direct par produit tensoriel :

$$L(M) = L \otimes_A M \subseteq M^n = A^n \otimes_A M .$$

Ainsi un code de longueur n sur l'anneau quelconque A produit de manière naturelle un code de longueur n sur un A-module quelconque M . Le code sur M peut être trivial, autrement dit le module $L(M)$ peut être nul, sans que le module M soit nul. Cela ne se produit pas si le module non nul L est libre, par exemple si A est supposé local. La distance de Hamming du code sur M est dénotée par $d(M)$. La famille de tous les entiers $d(M)$ est appelée la distance générique du code sur A .

Proposition 18. La distance générique d'un code sur un anneau satisfait aux trois axiomes de la définition d'une distance sur un anneau.

Démonstration. A une suite exacte courte de A-modules correspond un diagramme commutatif dont les lignes sont des suites exactes courtes (soit de manière élémentaire ou soit par la projectivité du A-module L donné)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L(M') & \longrightarrow & L(M) & \longrightarrow & L(M'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'^n & \longrightarrow & M^n & \longrightarrow & M''^n & \longrightarrow & 0 \\
 & & \downarrow \Pi'_i & & \downarrow \Pi_i & & \downarrow \Pi''_i & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 .
\end{array}$$

Soit s' un élément de $L(M')$ de poids $d(M')$. Utilisons l'image s de s' dans $L(M)$. On obtient alors la première inégalité de l'axiome I

$$d(M') = w(s') = w(s) \geq d(M) .$$

Soit s un élément de $L(M)$ de poids $d(M)$. Si l'image s'' de s

dans $L(M'')$ n'est pas nulle, on obtient la seconde inégalité de l'axiome I comme suit

$$d(M) = w(s) \geqslant w(s'') \geqslant d(M'') .$$

Sinon, l'élément s est l'image d'un élément s' de $L(M')$ et on obtient la seconde inégalité de l'axiome I comme suit

$$d(M) = w(s) = w(s') \geqslant d(M') .$$

Passons à l'axiome II et considérons un élément s de $L(M)$ de poids $d(M)$

$$s = \Sigma_{i \leqslant h \leqslant k} \quad l_h \otimes m_h \in L \otimes M .$$

Soit M' le sous-module de M que les k éléments m_h engendrent. Alors l'élément s' de $L(M')$

$$s' = \Sigma_{i \leqslant h \leqslant k} \quad l_h \otimes m_h \in L \otimes M'$$

donne l'inégalité essentielle de l'axiome II

$$d(M) = w(s) = w(s') \geqslant d(M') .$$

Passons à l'axiome III et considérons un produit direct quelconque

$$M = \Pi[M_i \mid i \in I] .$$

On a un isomorphisme canonique (dû au rang fini n)

$$\begin{aligned} M^n = A^n \otimes M &= A^n \otimes \Pi\, M_i \\ &\cong \Pi(A^n \otimes M_i) = \Pi\, M_i^n . \end{aligned}$$

Comme le A-module L a une présentation finie, on a un autre isomorphisme canonique (restriction du précédent)

$$\begin{aligned} L(M) = L \otimes M &= L \otimes \Pi\, M_i \\ &\cong \Pi(L \otimes M_i) = \Pi\, L(M_i) . \end{aligned}$$

Utilisons ces isomorphismes de manière libre. Soit s un élément de $L(M)$ de poids $d(M)$. La i-ème composante de s, c'est-à-dire celle dans $L(M_i)$ est dénotée par s_i. Pour un bon choix de l' indice i, l'élément s_i n'est pas nul. On obtient alors l'inégalité essentielle de l'axiome III

$$d(M) = w(s) \geqslant w(s_i) > d(M_i) .$$

La proposition est démontrée.

Corollaire 19. La distance générique d'un code sur un anneau noethérien A satisfait à l'égalité suivante

$$d(M) = \min[d(A/P) \mid P \in Ass_A M]$$

pour tout A-module M et à l'inégalité suivante

$$d(A/P) \leqslant d(A/Q) \quad \text{si} \quad P \supseteq Q$$

pour toute inclusion d'idéaux premiers de A.

Démonstration. Il s'agit d'utiliser le théorème 7 et la proposition 12.

En particulier, passer aux corps des fractions ne modifie pas les distances de Hamming (voir l'exemple 8) et passer aux complétés-séparés ne modifie pas les distances de Hamming (voir l'exemple 15). En bref, tous les résultats sur les distances sont utilisables. Par exemple, la distance de Hamming d'un code sur un anneau noethérien A est égale au minimum des distances de Hamming des codes sur les anneaux A_P, l'idéal premier P parcourant l'ensemble des idéaux maximaux de A.

Exemple 20. Soit $A[x]$ l'anneau des polynômes à une variable et à coefficients dans A. Considérons un polynôme unitaire $l(x)$ dans $A[x]$, divisant le polynôme $x^n - 1$ et possédant le degré $\lambda < n$. Soit k l'entier $n - \lambda$. Pour tout $s(x)$ de $A[x]$ de degré égal à $n - 1$ au plus, il existe une unique décomposition

$$s(x) = l(x)a(x) + b(x)$$

avec $a(x)$ dans $A[x]$ de degré égal à $k-1$ au plus et avec $b(x)$ dans $A[x]$ de degré égal à $\lambda - 1$ au plus. Considéré comme A-module, l'anneau

$$A[x] / (x^n-1)$$

peut être identifié au A-module A^n . La base canonique est alors la suivante

$$1, x, \ldots, x^{n-2}, x^{n-1} .$$

Soit maintenant L l'idéal principal engendré par $l(x)$. Ce sous-module est un A-module libre dont voici une base

$$l(x), xl(x), \ldots, x^{k-2}l(x), x^{k-1}l(x) .$$

De plus, il s'agit d'un sous-module direct, comme le démontre l'homomorphisme dû à la décomposition

$$q(s(x)) = s(x) - b(x) .$$

Un tel code est dit principal. Bien entendu, un code principal est un code cyclique. Rappelons qu'un code est dit cyclique, s'il satisfait à la condition suivante (voir [2] Chapitre 7, Paragraphe 2) : un élément de L

$$a_1 a_2 \cdots a_{n-1} a_n$$

donne toujours un élément de L

$$a_2 a_3 \cdots a_n a_1 .$$

Il est équivalent de dire que L est non seulement un sous-module direct du A-module

$$A[x] / (x^n-1) \cong A^n$$

mais encore un idéal de cet anneau (idéal pas forcément direct, comme

le montre le code binaire principal dû au polynôme $x+1$) .

Un code cyclique n'est pas toujours principal. En effet, il se peut fort bien qu'un code L sur un anneau A soit cyclique, sans que le A-module L soit libre, ce qui empêche le code d'être principal. Par exemple, considérons un code cyclique L sur un anneau A possédant un idempotent e autre que 0 et 1 . Alors eL est encore un code cyclique sur le même anneau. Mais le A-module eL n'est pas libre, s'il n'est pas nul. Il reste donc à imposer la condition nécessaire d'un A-module libre L pour obtenir la réciproque du résultat de l'exemple 20.

Proposition 21. Un code cyclique dû à un A-module libre L est toujours un code principal.

Démonstration. Soit k le rang (non nul) du A-module libre L et soit λ la différence de n et de k , l'entier n étant la longueur du code. Considérons le sous-module libre de rang λ

$$M \subseteq A[x] /(x^n-1) \cong A^n$$

formé des polynômes de degrés au plus $\lambda-1$. Les homomorphismes d'injection de L et de M dans A donnent lieu à un homomorphisme de A-modules (tous les deux de rang n)

$$\eta : L \oplus M \longrightarrow A^n \quad \text{(somme directe)} .$$

On peut aussi écrire $\eta(A)$ pour être plus précis. La décomposition unique décrite dans l'exemple 20 démontre que η est un isomorphisme si le code est principal. On obtient la réciproque comme suit.

Supposons avoir un isomorphisme η. L'élément x^λ de A^n appartient à l'image de η . Il existe donc $l(x)$ de L et $a(x)$ de M donnant lieu à une égalité utile

$$x^\lambda = l(x)+a(x) .$$

On a donc obtenu un élément intéressant dans L

$$l(x) = x^{\lambda}+a_1x^{\lambda-1}+\ldots+a_{\lambda} \ .$$

Pour tout $s(x)$ de degré quelconque, on peut effectuer une division et écrire

$$s(x) = l(x)b(x)+c(x), \ c(x)\varepsilon M \ .$$

Si $s(x)$ appartient à L, alors $c(x)$ appartient à L aussi, puisque L est un idéal (le code est cyclique). Comme η est un monomorphisme, l'intersection de L et de M est nulle. Par suite $c(x)$ est forcément nul. Autrement dit, l'élément $l(x)$ engendre l'idéal L. Il reste à contrôler que $l(x)$ divise x^n-1. On a une égalité (à nouveau par division)

$$x^n-1 = l(x)b(x)+c(x)$$

qui prend la forme suivante modulo x^n-1

$$0 = l(x)b(x)+c(x) \ .$$

Comme ci-dessus $c(x)$ doit être nul, d'où la divisibilité de x^n-1 par $l(x)$.

La proposition est vraie lorsque l'anneau A est un corps. En effet, tous les idéaux de $A[x]$ sont alors principaux. Par suite, l'idéal L est forcément principal. On peut toujours l'engendrer par un polynôme unitaire, puisque A est un corps. Passons maintenant au cas général. Soit P un idéal maximal quelconque de A et considérons non seulement le code correspondant sur A/P, mais encore l'homomorphisme (du début de la démonstration)

$$\eta(A/P) = \eta(A) \otimes_A (A/P) \ .$$

Le code est cyclique sur A, il est donc cyclique sur A/P. Il vient d'être dit qu'il est alors principal sur A/P, puisque A/P est un corps. Autrement dit $\eta(A/P)$ est un isomorphisme et cela pour chaque idéal maximal P. Par suite $\eta(A)$ lui-même est un isomorphisme. Il est alors connu par la première partie de la démonstration que le code sur

A est forcément principal. La proposition est ainsi démontrée.

Sur un anneau local, les codes cycliques et les codes principaux sont les mêmes. C'est clair puisque, dans ce cas, tout module projectif est libre. Une classe d'exemples sera étudiée un peu plus loin. Il est utile de prendre note auparavant de ce qui se passe pour les anneaux finis.

Proposition 22. Tout code linéaire sur un anneau fini peut être remplacé par un code linéaire sur un produit direct de corps finis, avec les mêmes propriétés essentielles pour les deux codes.

Démonstration. Soit A un anneau fini. Il a un nombre fini d'idéaux maximaux P_i et il se décompose en un produit direct d'anneaux locaux finis A_i (voir [1] Chapitre IV, Paragraphe 2, Proposition 9, Corollaire 1). L'anneau local A_i a le corps fini A/P_i comme corps résiduel. En utilisant le gradué associé de l'anneau local A_i, il est élémentaire de vérifier qu'il existe un entier h_i donnant l'égalité suivante

$$\text{card } A_i = (\text{card } A/P_i)^{hi} .$$

Le corps fini A/P_i peut être plongé dans un corps fini K_i ayant précisément ce nombre comme nombre d'éléments (voir [2] Chapitre IV, Paragraphe 3). Enfin on considère le produit direct des corps K_i ; cet anneau est dénoté par A^* et appelé le simplifié de A. De manière canonique A^* possède une structure d'algèbre sur A

$$A = \Pi A_i \longrightarrow \Pi A/P_i \longrightarrow \Pi K_i = A^* .$$

Les A-modules A et A^* ont le même nombre d'éléments et ont les mêmes idéaux premiers associés, à savoir tous les P_i.

Soit maintenant un code L sur A. Il en découle un code L^* sur A^* (dit code simplifié). Ces deux codes ont les mêmes propriétés essentielles. Bien évidemment, ils ont la même longueur. Il vient d'être vu que les deux alphabets ont le même nombre d'éléments. Si le code donné est cyclique (respectivement principal), alors le code simplifié est cyclique (respectivement principal) puisqu'un idéal donne un idéal (puisque

respectivement un polynôme unitaire donne un polynôme unitaire) en passant de l'anneau donné à l'anneau simplifié. Vu la remarque faite ci-dessus à propos des idéaux associés, on a la même distance de Hamming pour les deux codes (d'après le corollaire 19). Enfin L et L^* ont le même nombre d'éléments pour la raison suivante. Le A-module L n'est pas libre en général, mais le A_i-module $L(A_i)$ est libre (de rang s_i disons) puisque l'anneau A_i est local. On peut alors écrire les égalités suivantes

$$\begin{aligned} &\text{card } L(A) = \prod \text{card } L(A_i) = \\ &\prod (\text{card } A_i)^{s_i} = \prod (\text{card } K_i)^{s_i} \\ &\prod \text{card } L(K_i) = \text{card } L(A^*) \ . \end{aligned}$$

Voilà donc achevée la liste des propriétés que l'on peut dire essentielles et qui sont préservées en passant au simplifié d'un code.

Exemple local

Considérons un anneau local et noethérien A et son corps résiduel K. Rappelons que sur A il est équivalent de parler de codes cycliques ou de codes principaux. Un code défini sur A donne naturellement un code défini sur K, appelé le code résiduel. D'après le corollaire 19, la distance de Hamming n'augmente pas par passage au code résiduel. Le code résiduel d'un code cyclique est lui aussi cyclique. Reformulons le lemme de Hensel dans le cas qui nous intéresse (voir [1] Chapitre III, Paragraphe 4, Théorème 1). Si s est un élément de $A[x]$, alors $\bar{s}$ désigne son image dans $K[x]$.

Lemme 23. Soit $f(x)$ un polynôme unitaire dans $K[x]$, divisant (x^n-1) avec

$$f(x) \text{ et } g(x) = (x^n-1)/f(x)$$

relativement premiers. Alors il y a au plus un code cyclique sur A ayant le code cyclique dû à $f(x)$ comme code résiduel. De plus, il y en a exactement un, si l'anneau A est complet.

Démonstration. Si l'anneau A est complet (ou simplement hensélien), il existe une paire unique

$$l(x) \ , \ m(x)$$

de polynômes unitaires dans $A[x]$ avec les propriétés suivantes

$$l(x)m(x) = x^n-1, \ \bar{l}(x) = f(x), \ \bar{m}(x) = g(x) \ .$$

Puisque $l(x)$ détermine $m(x)$, le lemme est démontré dans le cas où A est complet. Dans le cas général, on utilise $\hat{A}$ qui contient A . Si la paire $(l(x),m(x))$ existe dans $A[x]$, elle existe dans $\hat{A}[x]$ avec les mêmes propriétés. Conséquemment l'unicité sur $\hat{A}$ implique l'unicité sur A .

Proposition 24. La distance de Hamming d'un code cyclique sur un anneau local et noethérien est égale à la distance de Hamming du code résiduel, si le corps résiduel a la caractéristique nulle.

Démonstration. A cause de la caractéristique nulle, l'unicité du lemme précédent est présente sans restriction. A cause de la caractéristique nulle, l'anneau A contient le corps Q des entiers rationnels. De plus, l'extension K/Q est séparable. D'après I. Cohen, l'homorphisme identité de K (le corps résiduel) se relève en un homomorphisme d'anneaux de K dans $\hat{A}$, le complété de A (voir [3]Théorème 28.J). L'image du code cyclique défini sur K et l'image du code cyclique sur A sont, l'une et l'autre, deux codes cycliques définis sur $\hat{A}$ et possédant le même code cyclique résiduel. D'après le lemme 23, elles coïncident. D'après le corollaire 19 (dans le cas simple d'un corps) les entiers $d(K)$ et $d(\hat{A})$ coïncident. D'après l'exemple 15, les entiers $d(A)$ et $d(\hat{A})$ coïncident. Par suite, les distances de Hamming $d(A)$ et $d(K)$ sont égales, ce qu'il fallait démontrer. Remarquons aussi que $d(K)$ est la distance de Hamming pour tout corps contenant les coefficients de $l(x)$, si $l(x)$ est le polynôme unitaire décrivant le code cyclique sur A .

Passons maintenant au cas de caractéristique positive, ce qui est un peu

plus compliqué.

Définition 25. Un code cyclique sur un corps est dit hensélien si le polynôme unitaire $f(x)$ qui l'engendre jouit de la propriété suivante :

$$f(x) \quad \text{et} \quad g(x) = (x^n-1)/f(x)$$

sont relativement premiers. En caractéristique nulle, un code cyclique est toujours hensélien. En caractéristique positive p, un code cyclique est hensélien, si par exemple p ne divise pas n.

Soit $GF(p^m)$ le corps fini à p^m éléments. Puis soit $C(p^m)$ l'unique anneau complet de valuation discrète avec $GF(p^m)$ comme corps résiduel et avec $p.1$ comme paramètre local. La construction en est rappelée ci-dessous. En premier lieu, l'anneau $C(p)$ est celui des entiers p-adiques. Puis on choisit un élément primitif ϑ de $GF(p^m)$ (voir [2] Chapitre IV, Paragraphe 2, Théorème 4) et on considère son polynôme minimal

$$z(t) \in GF(p)[t] .$$

Cela étant, on choisit un polynôme unitaire

$$s(t) \in C(p)[t]$$

au-dessus de $z(t)$. Alors on a la définition

$$C(p^m) = C(p)[t]/(s(t)) .$$

La démonstration de l'unicité a quelque chose à voir avec le lemme de Hensel. Oublions-la, puisqu'elle n'est d'aucune utilité pour nous.

Définition 26. Considérons un code hensélien, sur un corps K de caractéristique p, engendré par un polynôme $f(x)$. Soit $GF(p^m)$ le plus petit corps contenant les coefficients de $f(x)$. Il existe, car ces coefficients sont algébriques sur $GF(p)$, puisque $f(x)$ divise x^n-1. On a donc alors un code hensélien sur $GF(p^m)$. D'après le lemme 23, il existe un unique code cyclique sur $C(p^m)$ ayant le code précédent,

comme code résiduel. La distance de Hamming du code cyclique sur $C(p^m)$ est appelée la distance de Cohen du code hensélien.

La proposition 28 démontre que la distance de Cohen est un nombre bien défini, sans avoir besoin de démontrer l'unicité de $C(p^m)$. La distance de Cohen est au moins égale à la distance de Hamming d'après le corollaire 19. Une méthode pour calculer les distances de Cohen est indiquée plus loin (remarque 30).

Remarque 27. Utilisons la définition et la notation introduites ci-dessus et considérons un $C(p^m)$-module M . L'anneau $C(p^m)$ a les deux idéaux premiers (0) et (p) . Le second est associé à M si et seulement s'il existe un monomorphisme de $C(p^m)$-modules

$$C(p^m)/p\,C(p^m) \longrightarrow M \quad .$$

Le module-source ci-dessus est isomorphe au module $GF(p^m)$ qui est simple. Un monomorphisme du type ci-dessus n'est donc rien d'autre qu'un homomorphisme non nul. Il en existe un si et seulement si M possède un élément non nul d'ordre p . Supposons donné en outre un code cyclique sur $C(p^m)$ à code résiduel hensélien, autrement dit supposons donné en outre un code hensélien que l'on relève en un code cyclique sur $C(p^m)$ (selon le lemme 23). Alors la distance de Hamming $d(M)$ est égale à la distance de Hamming du code résiduel si M contient un élément non nul d'ordre p et à la distance de Cohen du code résiduel si M ne contient pas d'élément non nul d'ordre p .

Proposition 28. La distance de Hamming d'un code cyclique sur un anneau local et noethérien à code résiduel supposé hensélien (de caractéristique positive p) est égale à la distance de Hamming du code résiduel si l'anneau possède un élément non nul d'ordre p et à la distance de Cohen du code résiduel si l'anneau ne possède pas d'élément non nul d'ordre p .

Démonstration. Puisque $\hat{A}$ est complet, il existe un unique homomorphisme d'anneaux de $C(p)$ dans $\hat{A}$. Pour le prolonger, revenons à la définition 25 de l'anneau $C(p^m)$. Le polynôme $s(t)$ donne un polynôme à coefficients dans $\hat{A}$. Par le lemme de Hensel (voir [1] Chapitre III, Para-

graphe 4, Théorème 1), il possède une unique racine α au-dessus de la racine primitive θ. Alors l'homomorphisme de $C(p)$-algèbres, de source $C(p)[t]$ et de but $\hat{A}$, envoyant t sur α, donne un homomorphisme d'anneaux de $C(p^m)$ dans $\hat{A}$. Maintenant nous disposons d'un diagramme commutatif d'homomorphismes d'anneaux

$$\begin{array}{ccc} C(p^m) & \longrightarrow & \hat{A} \\ \downarrow & & \downarrow \\ GF(p^m) & \longrightarrow & K \ . \end{array}$$

Il y a un code cyclique sur chacun des quatres anneaux. Le code sur A donne les codes sur $\hat{A}$ et sur K. Par restriction, le code sur K donne le code sur $GF(p^m)$ (définition 26) et par relèvement, le code sur $GF(p^m)$ donne le code sur $C(p^m)$ (définition 26). Les quatre codes en question sont tous images les uns des autres (pour le passage de $C(p^m)$ à $\hat{A}$, on utilise la propriété d'unicité du lemme 23).

Appliquons maintenant la remarque 27 pour calculer la distance de Hamming sur $\hat{A}$. Cela donne le résultat pour la distance de Hamming sur A grâce aux deux remarques suivantes. L'homomorphisme

$$p : A \longrightarrow A \quad \text{(multiplication par } p \text{)}$$

est un monomorphisme si et seulement si l'homomorphisme

$$p : \hat{A} \longrightarrow \hat{A} \quad \text{(multiplication par } p \text{)}$$

est un monomorphisme, puisque le A-module $\hat{A}$ est fidèlement plat. En outre, les distances de Hamming $d(A)$ et $d(\hat{A})$ sont égales, aussi par fidèle platitude (exemple 15).

Remarque 29. Avec les hypothèses de la proposition 28, considérons un A-module M quelconque. Alors à nouveau la distance de Hamming $d(M)$ est égale, soit à la distance de Hamming du code résiduel, soit à la distance de Cohen du code résiduel.

D'après le corollaire 19 et la proposition 28, le premier cas a lieu ci-dessus si et seulement si le A-module M possède un idéal premier

associé P avec l'anneau intègre A/P de caractéristique p, autrement dit si et seulement si $p.1$ appartient à un idéal premier associé du A-module M. La réunion de ces idéaux associés est formée des éléments de A qui annulent l'un ou l'autre des éléments non nuls de M (voir [1] Chapitre IV, Paragraphe 1, Proposition 2, Corollaire 2). En résumé, l'entier $d(M)$ est égal à la distance de Hamming du code résiduel si M possède un élément non nul d'ordre p et à la distance de Cohen du code résiduel si M ne possède pas un tel élément.

La distance de Cohen peut être calculée de la manière suivante : on utilise la proposition 26 pour un bon anneau intègre local de caractéristique nulle et on calcule la distance de Hamming d'un code sur le corps des fractions. Tout cela est précisé dans la remarque suivante.

Remarque 30. La caractéristique résiduelle est égale à p et la longueur des codes vaut n

$$n = tm \ , \ t = p^h \ , \ p \nmid m \ .$$

Considérons un corps K de caractéristique p et un code cyclique sur K dû à un polynôme unitaire $f(x)$ de degré λ. Supposons ce code hensélien. Autrement dit les racines de $f(x)$ ont toutes la même multiplicité p^h et alors le degré λ est un entier de la forme $p^h e$. Cela étant, choisissons un générateur μ du groupe cyclique de toutes les racines de x^n-1 en caractéristique nulle et un générateur ν du groupe cyclique de toutes les racines de x^n-1 en caractéristique p. Soient maintenant (dans un ordre quelconque et avec des répétitions peut-être)

$$\alpha_i \ , \ 1 \leqslant i \leqslant \lambda \ ,$$

les λ entiers pris modulo n, tels que les λ éléments ν^{α_i} soient exactement les racines de $f(x)$, avec la multiplicité correcte p^h. Ensuite, considérons le polynôme unitaire de degré λ

$$l(x) = \Pi(x-\mu^{\alpha_i}) \in Q(\mu)[x] \ .$$

Alors la distance de Hamming du code cyclique sur $Q(\mu)$ dû au polynôme

$l(x)$ est égale à la distance de Cohen du code hensélien sur K dû au polynôme $f(x)$.

En effet, considérons le sous-anneau de $Q(\mu)$ engendré par l'élément μ et localisons-le en un idéal premier maximal contenant l'élément $p.1$. L'anneau local et noethérien obtenu de cette manière est noté A et les coefficients de $l(x)$ s'y trouvent. Le polynôme $l(x)$ se trouve au-dessus du polynôme $f(x)$ si le générateur μ se trouve au-dessus du générateur ν . On peut alors appliquer la proposition 28. La distance de Hamming du code sur $Q(\mu)$, autrement dit la distance de Hamming du code sur A , est égale à la distance de Cohen du code sur le corps résiduel, autrement dit à la distance de Cohen du code donné sur K . Si le générateur μ ne se trouve pas au-dessus du générateur ν , il se peut que le polynôme $l(x)$ ne soit pas au-dessus du polynôme $f(x)$. Mais la conclusion ci-dessus est encore valable, grâce à la remarque générale suivante, qui permet une réduction au cas particulier traité ci-dessus. La remarque générale s'applique ici à l'anneau $Z[\mu]$ ou au corps $Q(\mu)$ indifféremment. Un code est défini sur un anneau B . Alors un automorphisme de B transforme ce code en un autre code en général, mais ne modifie pas la distance de Hamming, bien évidemment.

Les distances de Hamming et de Cohen peuvent être différentes On va le voir dans l'exemple des codes cycliques binaires de longueur un nombre premier.

Exemple 31. Considérons un polynôme

$$f(x) \in GF(2)[x]$$

de degré λ et divisant x^n+1 , l'entier n étant premier impair. Dans le cas trivial

$$(x+1)\, f(x) = x^n+1$$

la distance de Hamming est égale à n , puisqu'elle est calculée à l'aide de l'unique élément

$$x^{n-1}+x^{n-2}+\dots+x+1$$

et la distance de Cohen est égale à n aussi, puisqu'elle est comprise entre la distance de Hamming qui vaut n et la longueur du code qui vaut n aussi. Dans le cas trivial

$$f(x) = x+1$$

les distances de Hamming et de Cohen valent 2 par un argument élémentaire. Considérons maintenant le cas général

$$x+1 \neq f(x) \neq x^{n-1}+\dots+1 .$$

Alors les distances de Hamming et de Cohen sont différentes (par exemple dans le cas

$$f(x) = x^3+x+1 \quad \text{et} \quad n = 7$$

elles valent 3 et 4 respectivement). En voici la raison. D'une part la distance de Hamming est égale au plus au degré λ de $f(x)$. Sinon cette distance vaut $\lambda+1$ et le mot $f(x)$ doit avoir le poids $\lambda+1$. Comme cela se passe dans $GF(2)$, on a alors

$$f(x) = x^{\lambda}+x^{\lambda-1}+\dots+x+1 .$$

Comme ce polynôme divise par ailleurs x^n+1 avec n premier, il est facile de constater que λ vaut soit 1 , soit $n-1$. Il s'agit alors des deux cas triviaux que l'on a déjà traités. D'autre part, la distance de Cohen est égale exactement à $\lambda+1$. Pour le voir, il suffit de considérer l'anneau

$$A = \dot{Z}[\mu] \subseteq Q(\mu) , \quad \mu^n = 1, \mu \neq 1$$

et de démontrer qu'un polynôme $l(x)$ de $A[x]$ divisant x^n-1 , de degré λ , donne toujours un code principal dont la distance de Hamming vaut $\lambda+1$. Considérons l'idéal de A

$$I = (n.1, \mu-1) .$$

Il est maximal, avec $GF(n)$ comme corps résiduel. Comme la distance de Hamming décroit pour un idéal premier croissant d'après le corollaire 19, il suffit de démontrer ce qui suit. La distance de Hamming d'un code cyclique sur $GF(n)$, de longueur n, dû à un polynôme $\varphi(x)$ de degré λ, est toujours égale à $\lambda+1$. Bien entendu, on a

$$\varphi(x) = (x-1)^{\lambda} .$$

Il reste donc à démontrer le résultat simple suivant sur $GF(n)$, ou sur un corps de caractéristique n.

Remarque 32. Un polynôme à coefficients dans un corps de caractéristique p, de degré égal au plus à $p-1$ et possédant une racine non nulle de multiplicité égale au moins à λ, a au moins $\lambda+1$ de ses coefficients non nuls. On peut toujours supposer qu'il s'agit de la racine 1. Considérons un polynôme

$$f(x) = a_{p-1}x^{p-1}+\dots+a_0 .$$

La condition sur la racine 1 se traduit en λ égalités concernant les dérivées successives

$$a_{p-1}\binom{p-1}{i}+\dots+a_0\binom{0}{i} = 0$$

pour i compris entre 0 et $\lambda-1$. Il est équivalent de considérer le système suivant d'équations linéaires homogènes

$$a_{p-1}(p-1)^i+\dots+a_0(0)^i = 0$$

pour i compris entre 0 et $\lambda-1$. On voit donc apparaître la matrice suivante

$$H = (j^i) , \quad 0 \leqslant j \leqslant p-1 , \quad 0 \leqslant i \leqslant \lambda-1 .$$

Tous les mineurs $\lambda\times\lambda$ de cette matrice ont des déterminants non nuls (ce sont des déterminants de Vandermonde). Cela démontre le résultat sur les coefficients.

[1] N. Bourbaki. Algèbre commutative - Chapitres III et IV. Hermann 1967.

[2] F. Mac Williams - N. Sloane. The theory of error - correcting codes. North Holland 1978.

[3] H. Matsumura. Commutative algebra. Benjamin 1970.

[4] P. Shankar. On BCH codes over arbitrary integer rings. IEEE Trans. Inform. IT 25 (1979) 480-483.