COLLOQUE NATIONAL SUR LE TRAITEMENT DU SIGNAL
ET SES APPLICATIONS

NICE du 26 au 30 AVRIL 1977

SUR LE DECODAGE GEOMETRIQUE DES CODES CORRECTEURS

ON THE GEOMETRICAL DECODING OF ERROR CORRECTING CODES

Gérard COHEN et Philippe GODLEWSKI

ECOLE NATIONALE SUPERIEURE DES TELECOMMUNICATIONS, 46 Rue Barrault, 75013 PARIS -

RESUME

Le problème du décodage des codes en blocs correcteurs d'erreurs multiples est complexe. Il peut être simplifié par une approche de type géométrique, si les supports des mots du code dual possèdent certaines propriétés combinatoires de régularité. On utilise alors des méthodes de décodage à décision majoritaire en une ou plusieurs étapes. Dans un premier temps, nous décrivons les structures qui permettent la construction de tels codes : configurations tactiques ("designs"), géométries finies, matroïdes. Des exemples de construction sont également donnés. Nous présentons ensuite, dans le cas des codes géométriques, deux méthodes simplificatrices du décodage. L'une, dite "réduction séquentielle", permet de diminuer le nombre des relations de parité à calculer, au prix d'un accroissement du temps de décodage. Elle fait appel à des multiplications polynomiales, qui sont facilitées par l'emploi d'idempotents. L'autre pré-traite les bits d'information en les multipliant par une matrice quasi-circulante. A la réception, on épargne une étape dans l'obtention de presque toute l'information. Cette "réduction partielle" peut s'appliquer quand les bits sont d'importance inégale.

SUMMARY

The problem of decoding multiple error block correcting codes is complex. It may be simplified by a geometrical viewpoint, when the supports of words of the dual code possess some combinatorial properties of regularity. One or multi-step orthogonalization can then be used. We first describe structures allowing the construction of such codes : designs, finite geometries, matroïds,... Some examples are given. We then present, in the case of finite geometry codes, two methods to simplify the decoding. One, named "sequential reduction", reduces the number of parity-check relations to compute, at the cost of a slight increase in decoding time. It requires polynomial multiplications, made easier using idempotents. The other method "pre-processes" the bits, multiplying them by a quasi-circulant matrix. At the receiver, one step less is necessary to recover almost all the informations. This "partial reduction" can be applied when bits have inequal importance.

SUR LE DECODAGE GEOMETRIQUE DES CODES CORRECTEURS

INTRODUCTION

Parmi les méthodes connues de décodage des codes en blocs correcteurs d'erreurs, celles employant des décisions majoritaires sont intéressantes par la simplicité de leur principe et de leur mise en oeuvre. L'exemple (antédiluvien ?) du code (n.1), obtenu en répétant n fois le message (ou symbole) à transmettre, illustre bien cette simplicité. On effectue au décodage un vote majoritaire : on choisit le symbole qui apparait le plus grand nombre de fois dans le mot reçu.

Une part du succès qu'ont eu ces techniques de décodage majoritaire est peut-être due au faible investissement théorique qui est nécessaire à leur appréhension. Par exemple la notion de corps extension n'est pas indispensable pour comprendre leurs mécanismes. Il n'en est pas de même des algorithmes de décodage du type algébrique (BCH, Goppa).

Si les techniques de décodage majoritaire sont simples, la construction des codes correspondants pose des problèmes difficiles. Elle a donné lieu à de multiples travaux, principalement sur l'aspect géométrique de ces codes (géométries projectives, eudidiennes, sur un corps fini, géométries euclidiennes généralisées,etc.) [1-4] .

Dans un premier temps nous passons en revue différentes méthodes de construction qui font principalement appel aux aspects combinatoires de la théorie des codes correcteurs. Puis nous exposons des techniques de décodage qui s'adaptent à certaines classes de codes.

RAPPELS SUR LES CODES LINEAIRES EN BLOCS

On considère l'ensemble $\mathcal{R}$ de tous les n-uplets d'éléments du corps fini à q éléments $\mathbb{F}_q$.

$$u = (u_o, u_1, \ldots u_{n-1}) \qquad u_i \in \mathbb{F}_q$$

$\mathcal{R} = (\mathbb{F}_q)^n$ est un espace vectoriel (e.v.) de dimension n sur $\mathbb{F}_q$.

Un (n,k) code linéaire en blocs C est un sous e.v. de dimension k de $\mathcal{R}$. Les éléments de C sont appelés mots de code.

On munit $\mathcal{R}$ du produit scalaire habituel

$$< u,u' > = \sum_{i=o}^{n-1} u_i\, u'_i$$

On définit alors le code dual $C^\perp$ de C comme l'ensemble des vecteurs de $\mathcal{R}$ orthogonaux à tous les vecteurs de C. L'ensemble $C^\perp$ est un e.v. de dimension (n-k). Les éléments de $C^\perp$ sont appelés règles de parité. Pour qu'un mot c de $\mathcal{R}$ appartienne à C il est nécessaire et suffisant que

$$\forall c' \in C^\perp \ , \quad < c,c' > = o \qquad (1)$$

Une matrice de vérification de parité de C est un tableau H dont les lignes sont des mots générant $C^\perp$. La matrice H est donc de rang (n-k). L'expression (1) devient

$$c \in C \iff c.H^T = \bar{o} \qquad (2)$$

où $\bar{o}$ est le vecteur ligne nul de dimension r si la matrice H est de dimension (r x n), $r \geqslant n-k$. Notons que la matrice H caractérise le code mais qu'elle n'est pas unique.

CORRECTION DES ERREURS, DECODAGE PAR DECISIONS MAJORITAIRES.

Soit c un mot du code C. Les symboles c_i , $\{i=o,1,\ldots,n-1\}$, sont transmis sur un canal et affectés de l'erreur additive e_i ($e_i \in \mathbb{F}_q$). A la réception on dispose du n-uplet $u = c+e$, le problème du décodage consiste à rechercher dans $\mathcal{R}$ le mot $\hat{c}$ de C le plus proche, pour une certaine métrique, du mot reçu u. Si le canal possède certaines propriétés (canal sans mémoire, symétrique, ...), la métrique utilisée est celle de Hamming. Le poids de Hamming p(u), d'un mot u de $\mathcal{R}$ est le nombre des composantes non nulles de u ; $d(u,v) = p(u-v)$ est alors la distance entre deux mots u et v de $\mathcal{R}$.

On définit la distance minimale d'un code linéaire :

$$d = \min_{\substack{(x,y)\in C^2 \\ x\neq y}} d(x,y) = \min_{x \in C\setminus\{o\}} p(x)$$

et sa capacité de correction $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Le décodage consiste à rechercher dans $\mathcal{R}$ le mot $\hat{c}$ de C qui est à une distance inférieure ou égale à t du mot reçu v. Le problème a une solution si $p(e) \leqslant t$. Elle est unique d'après les propriétés de distance minimale du code C . Il n'existe pas d'algorithmes généraux de complexité acceptable permettant de résoudre ce problème pour tout code. Pour certaines classes de codes auxquelles nous nous intéressons maintenant on peut utiliser des procédures de décodage par décision majoritaire. Nous allons illustrer par deux exemples leur principe.

1) Code cyclique (7.3) sur $\mathbb{F}_2$: ce code qui est l'ensemble des mots pairs du code de Hamming (7,4) a comme distance minimale d = 4. Il corrige donc une erreur. Il admet la matrice de vérification de parité :

$$H = \begin{bmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \\ 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 1&0&1&0&0&0&1 \end{bmatrix} \begin{matrix} = x \\ \\ \\ \\ = y \\ \\ = z \end{matrix} \qquad (3)$$

qui est de rang 4 sur $\mathbb{F}_2$. Soit u = c+e le mot reçu, on forme $u.H^T$; d'après (2)

$$u.H^T = (c+e)\ H^T = e\ H^T.$$

Considérons la sous-matrice H' de H formée des 1^{ere}, $5^{ème}$ et $7^{ème}$ colonnes de H

$$eH'^T = u.H^T \iff \begin{cases} e_o = e_1 + e_3 + u_o + u_1 + u_3 \\ e_o = e_4 + e_5 + u_o + u_4 + u_5 \\ e_o = e_2 + e_6 + u_o + u_2 + u_6 \end{cases}$$

u_i est un symbole reçu, e_i est inconnu. On suppose que la contrainte $p(e) \leqslant t = 1$ est vérifiée. En l'absence d'erreur $uH^T = o$ et $\hat{c} = u$. Si $p(e) = 1$, il existe une seule erreur e_i non nulle, e_o est donc égal à au moins deux des trois expressions :

$$\begin{cases} X = u_o + u_1 + u_3 = < u,x > \\ Y = u_o + u_4 + u_5 = < u,y > \\ Z = u_o + u_2 + u_6 = < u,z > \end{cases}$$

et on note :

$$e_o = Maj(< u,x >, < u,y >, < u,z >)$$

où $Maj(X_1,X_2,\ldots,X_J) = \lambda$, si il y a une absolue d'éléments X_i dont la valeur est λ. S'il n'existe pas de telle majorité $Maj(X_1,\ldots) = O$.

On peut ainsi estimer l'erreur qui affecte le premier symbole. Le code étant cyclique et donc invariant par permutation circulaire on pourra d'une manière similaire déterminer $e_1,e_2,\ldots.e_6$, c'est-à-dire le vecteur erreur e.

2) Code cyclique (7.4) sur $\mathbb{F}_2$. (code de Hamming de longueur 7)

Ce code peut corriger une erreur (d=3). La matrice de vérification de parité :

$$H = \begin{bmatrix} 1&0&1&1&1&0&0 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \\ 1&0&0&1&0&1&1 \\ 1&1&0&0&1&0&1 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \end{bmatrix} \qquad (4)$$

est de rang 3 sur $\mathbb{F}_2$. Considérons la sous matrice

$$H' = \begin{bmatrix} 1&1&0&0&1&0&1 \\ 1&1&1&0&0&1&0 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

Soit u = c+e, le vecteur reçu. Comme précédemment on peut écrire : $e.H'^T = uH'^T$. La capacité de correction du code est 1. Supposons donc p(e) = 1. Dans un premier temps nous tentons de déterminer $\hat{e}_o + \hat{e}_1$.

$$\begin{cases} e_o + e_1 = e_4 + e_6 + < a,u > \\ e_o + e_1 = e_2 + e_5 + < b,u > \end{cases}$$

Si l'erreur, supposée unique, affecte l'une des positions 4,6,2 ou 5 : elle n'affecte aucun des deux premiers symboles : $e_o+e_1 = o$. Les deux estimations de e_o+e_1 sont alors différentes. Dans les autres cas les deux estimations sont égales et fournissent la valeur de e_o+e_1. On peut donc écrire :

$$\hat{e}_o + \hat{e}_1 = Maj(O, < a,v > , < b,v >).$$

On peut de même déterminer $\hat{e}_6+\hat{e}_o$. La deuxième étape du décodage consiste à déterminer $\hat{e}_o$ à partir de $\hat{e}_o + \hat{e}_6$ et $\hat{e}_o + \hat{e}_1$. Si l'erreur est unique on peut écrire :

$$e_o = Maj(\hat{e}_6 + \hat{e}_o,\ \hat{e}_o + \hat{e}_1,\ O).$$

En effectuant le même traitement sur $e_1,\ldots,e_6$, on détermine $\hat{e}$ et donc $\hat{c} = u + \hat{e}$

Ainsi, quand il existe une matrice H ou une sous matrice H' de H possédant certaines propriétés combinatoires, on peut utiliser des techniques de décodage majoritaire. Nous allons maintenant étudier des tableaux H qui correspondent à des structures d'incidence présentant une certaine régularité.

STRUCTURE D'INCIDENCE

Une structure d'incidence ([5]) est un triplet S = (P,B,I), où P,B,I sont des ensembles $P \cup B = \emptyset$ et $I \subset B \times P$. Les éléments de P sont appelés points, ceux de B, blocs.

Si $P = \{p_j,\ 1 \leqslant j \leqslant v\}$, $|P| = v$, $B = \{b_i,\ 1 \leqslant i \leqslant b\}$ $|B| = b$, la matrice (b×v) d'incidence de cette structure sera définie ici par son terme générique : $h_{ij} = 1$ si le i-ème bloc b_i et le j-ième point p_j sont incidents, i.e. $(b_i,p_j) \in I$, $h_{ij} = 0$ sinon.

On note [X] le nombre de blocs (respectivement points) incidents à un ensemble de points (resp.blocs)X et on définit :

$$v_o = v \quad , \quad v_n = \binom{b}{m}^{-1} \sum_{\substack{Y \subset B \\ |Y| = m}} [Y] \quad , \quad m = 1,2,\ldots b \quad ,$$

$b_0 = b$, $b_n = \binom{v}{n}^{-1} \sum_{\substack{y \subset P \\ |y| = n}} [y]$, $n = 1,2,\ldots v$;

l'entier v_n (resp.b_n) est le nombre moyen de points (blocs) incidents à m blocs(npoints).

Un cas particulier intéressant est le suivant : Pour tout X de B et tout x de P, $[X]= v_1$ $[x] = b_1$: Tous les blocs "comportent" le même nombre de points et tous les points, le même nombre de blocs. La structure d'incidence est alors une configuration tactique. Notant b_1 et v_1 par r et k on a :
$bk = vr$, $v_m \binom{b}{m} = v\binom{r}{m}$, $b_n \binom{v}{n} = b\binom{k}{n}$.

On suppose de plus que pour tout couple (x,y) d'éléments de P, $[x,y] = b_2 = \lambda$. On a alors une (b, v, r, k, λ) -configuration, avec
$r(k-1) = \lambda(v-1)$.
Les blocs seront généralement considérés comme des ensembles de points : $B \subset \mathcal{P}(P)$.

Exemples de configurations

- Le tableau (.4), ensemble des mots non nuls d'un code binaire (7,3) est une (7,7,4,4,2) configuration.
- Plans inversifs. Si deux blocs quelconques ne sont jamais incidents sur le même triplet (x,y,z) la configuration est appelée plan circulaire fini, et les blocs, cercles. Si de plus [x,y,z] = 1 on a un 3-design. Il existe des 3-designs de paramètres : $v = \mu^2 + 1$, $k = \lambda = \mu + 1$, $b = \mu(\mu^2 + 1)$, $r = \mu(\mu + 1)$ pour $\mu = 2^{2m+1}$, $m > 0$ ([5]). On les appelle plans inversifs d'ordre μ. Delsarte ([6]) les a utilisés pour construire des codes binaires de longueur $\mu^2 + 1$, de rendement 1/2, de distance minimale $\mu + 1$, decodable majoritairement en une étape ; P. Camion ([7]) a mis en évidence leur structure quadratique et les généralise au cas m-aire. Pour $\mu = 3$, on obtient un code (10,5) de distance minimale 4, à partir de la matrice d'incidence d'un plan circulaire (15, 10, 6, 4, 2) :

$$\begin{bmatrix} 1&0&0&0&1&1&0&1&0&0 \\ 0&1&0&0&1&1&1&0&0&0 \\ 0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&1&0&0&1&1&1&0 \\ 0&0&0&0&0&1&0&1&1&1 \\ 1&1&0&0&0&0&1&1&0&0 \\ 0&1&1&0&0&1&0&0&1&0 \\ 0&0&1&1&1&0&0&1&0&0 \\ 0&0&0&1&0&1&1&0&0&1 \\ 1&1&0&1&0&0&0&0&1&0 \\ 0&1&1&0&0&0&0&1&0&1 \\ 1&0&1&1&0&1&0&0&0&0 \\ 0&1&0&1&1&0&0&0&0&1 \\ 1&0&1&0&0&0&1&0&0&1 \\ 1&0&0&0&1&0&0&0&1&1 \end{bmatrix} = H$$

La matrice H est de rang 5 sur $\mathbb{F}_2$. On vérifie que :

b = 15 , 15 lignes ,
v = 10 , 10 colonnes ,
r = 6 , 6 "1" par colonne (6 cercles par point) ,
k = 4 , 4 "1" par ligne (4 points par cercle) ,
λ = 2 , 2 lignes coïncident au plus en 2 "1" (2 cercles ont 2 points en commun).

Cet exemple illustre la technique de construction qui sera utilisée dans la suite : le code est défini par sa matrice H de vérification de parité qui est la matrice d'incidence d'une structure. On peut dire que les points de la structure servent à indicer les n composantes d'un vecteur mot de code, on a donc n = v.

Un problème souvent difficile est la détermination du rang (n-k) de H, considérée comme matrice à éléments dans le corps fini $\mathbb{F}_q$ ($\mathbb{F}_q$ est l'alphabet dans lequel les composantes des mots du code prennent leur valeur). Ce rang doit être faible pour donner des codes ayant un rendement k/n intéressant. Le problème a été résolu dans certains cas lorsque l'ensemble des blocs définissant les règles de parité appartiennent à des structures plus vastes (géométries projectives, euclidiennes etc...).

GEOMETRIES

Ce sont les structures d'incidence les plus utilisées pour construire des codes correcteurs. Les blocs sont appelés plans et partitionnés en 0-plans (points), 1-plans (droite) , i-plans ($2 \leq i < m-1$), (m-1)-plans (hyperplans)et un unique m-plan contenant tous les points ; m est l'ordre de la géométrie. Le nombre de points d'un i-plan est seulement fonction de son rang i. Le nombre de j-plans contenant un i-plan donné et contenus dans un k-plan donné est fonction de i, j, k seuls. Il n'existe qu'un seul i-plan contenant un (i-1)-plan donné et "passant" par un point fixé non contenu dans le (i-1)-plan. Ces propriétés combinatoires sont utiles au décodage. Dans le cas des géométries euclidiennes (: affines) ou projectives le rang est simplement la dimension au sens linéaire (nombre maximal d'éléments "indépendants").

Citons une structure plus générale, celle de matroïde, définie comme un ensemble de points P et une collection $\mathcal{J} \subset \mathcal{P}(P)$ d'ensembles indépendants caractérisés par les deux propriétés :

P1) Tout sous-ensemble d'un ensemble indépendant est indépendant

P2) Soit A une partie de P. Deux sous-ensembles indépendants quelconques de A, maximaux pour l'inclusion ont le même cardinal r(A) (rang de A).

Les plans sont alors des parties "fermées" de P. Leur rang est bien défini d'après P2 mais leur cardinal ne dépend pas que de ce rang.

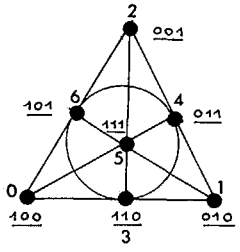
D'une manière générale, un code géométrique q-aire sur une géométrie $\mathcal{G}$ est défini par la matrice H de vérification de parité qui est la matrice d'incidence de l'ensemble des r-plans de $\mathcal{G}$.

Exemples de géométries finies : géométries euclidiennes, projectives.

Comme dans le cas du corps des réels $\mathbb{R}$ on peut construire à partir des corps finis $\mathbb{F}_{q'}$ des géométries projectives ou affines (appelées ici euclidiennes).

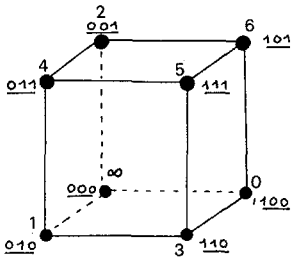
- La géométrie euclidienne de dimension m sur $\mathbb{F}_{q'}$, EG(m,q') correspond à l'ensemble des m-uplets de $\mathbb{F}_{q'}$; EG(m,q') contient donc $(q')^m$ points.
- La géométrie projective de dimension m sur $\mathbb{F}_{q'}$, PG(m,q') correspond à l'ensemble des (m+1)-uplets de $\mathbb{F}_{q'}$ quotienté par la relation de colinéarité : $(a_o, a_1, \ldots a_m) \sim (b_o, b_1, \ldots b_m)$, a_i et $b_i \in \mathbb{F}_{q'}$ s'il existe un élément non nul λ de $\mathbb{F}_{q'}$ tel que $a_i = \lambda\, b_i$ $(0 \leqslant i \leqslant m)$. La géométrie PG(m,q') contient donc $((q')^{m+1} - 1) / (q'-1)$ points.

Nous avons représenté sur les figures 1, 2 et 3 les géométries PG(2,2), EG(3,2) et PG(3,2).



PG(2,2) : 2-plan projectif binaire.

Fig. 1.



EG(3,2) : 3-plan euclidien binaire (toutes les droites ne sont pas représentées).

Fig. 2.

Exemples de codes définis par une géométrie

- Le code cyclique binaire (7,3) : la matrice H écrite en (3) est la matrice d'incidence des droites (1-plans) de la géométrie PG(2,2) (fig.2).
- Plus généralement le code cyclique $(2^m - 1, 2^m - m - 1)$, ensemble des mots pairs du code de Hamming de longueur $2^m - 1$, a pour matrice de vérification de parité la matrice d'incidence des hyperplans de la géométrie PG(m-1, 2) la figure 3 représente PG(3,2).
- Le code de Hamming binaire de longueur 7 : la matrice H, écrite en (4) est la matrice d'incidence des 2-plans de la géométrie EG(3,2) ne passant pas par l'origine.

Principe du décodage des codes géométriques.

Il se fait en plusieurs étapes qui seront explicites sur des exemples : On décode d'abord les (r-1)-plans à l'aide des r-plans les contenants, puis les (r-2)-plans par les (r-1)-plans etc..., de proche en proche jusqu'aux 0-plans (points). Ainsi pour le code cyclique(7,4) évoqué plus haut, les deux plans (1 1 0 0 1 0 1) et (1 1 1 0 0 1 0) passant par les 4 points 0, 1, 4, 6 et 0, 1, 2, 5 respectivement, se coupent en D, droite joignant les points 0 et 1. Ils permettent de la "décoder" (: d'estimer $e_o + e_1$). On décode similairement D' passant par 0 et 6, puis le point 0, au moyen de D et D'.

L'utilisation de structures géométriques permet donc d'obtenir des règles de parité dont les supports ont des propriétés qui facilitent le décodage. Considérons ainsi les trois 2-plans de PG(3,2) contenant la droite D_o passant par les points 0, 1, 4. Ces trois plans (cf.figure 3) partitionnent l'ensemble des points de PG(3,2)-D_o, leur matrice d'incidence H' comporte soit des colonnes de 1 (points de D_o), soit des colonnes de poids 1.

$$H' = \begin{bmatrix} 1&1&1&0&1&1&0&0&1&0&1&0&0&0&0 \\ 1&1&0&0&1&0&1&0&0&0&0&1&1&1&0 \\ 1&1&0&1&1&0&0&1&0&1&0&0&0&0&1 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

On dit que les trois règles de parité (a,b,c) sont orthogonales sur les positions 0, 1, 4.

Soit t_M la capacité de correction par décodage majoritaire d'un code défini à partir de la matrice d'incidence des r-plans d'une géométrie. L'entier t_M dépend généralement de la possibilité de décoder les (r-1)-plans, c'est-à-dire du nombre

J de r-plans contenant un (r-1)-plan fixé. Il y a donc J règles de parité orthogonales sur les positions correspondantes aux points du (r-1)-plan. En effectuant un décodage majoritaire on peut ainsi corriger les erreurs de poids $\lfloor (J-1)/2 \rfloor = t_M$.

Pour une géométrie euclidienne EG(m,q) où PG(m,q')

$$J = (q'^{m-r+1} - 1) / (q' - 1) \quad ,$$

J est bien sûr inférieur ou égal à la distance minimale d du code.

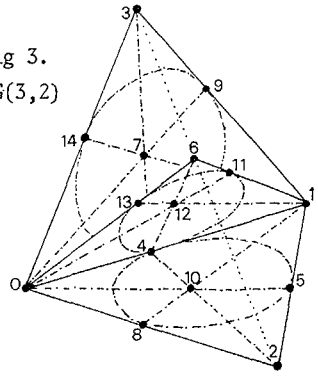


Fig 3.
PG(3,2)

0 : 1000
1 : 0100
2 : 0010
3 : 0001
4 : 1100
5 : 0110
6 : 0011
7 : 1101
...

CODES EUCLIDIENS

Il est toujours possible d'ordonner les points d'une géométrie projective (resp.euclidienne) de telle façon que les codes correspondants soient cycliques (resp. soient des codes cycliques étendus)

En fait, les codes euclidiens tels que nous les définissons ci-dessous sont cycliques, si on "enlève" le point origine de la géométrie euclidienne qui correspond à un symbole de vérification de parité. Cette remarque nous permet d'identifier les plans de EG(m,q') ne contenant pas l'origine, avec des polynômes à coefficients sur $\mathbb{F}_q$ modulo $x^n - 1$:

$$(i,j,k,\ldots) \rightarrow x^i + x^j + x^k + \ldots$$

Dans ce qui suit, les codes sont binaires (q=2) et $q' = 2^s$.

Définition : Le code euclidien binaire d'ordre (r,s) et de longueur $n = 2^m - 1$ est le plus grand code linéaire dont le dual contienne les polynômes correspondants aux (r+1)-plans de $EG(m,2^s)$ ne passant pas par l'origine.

Pour s=1 on retrouve les codes de Reed et Muller d'ordre r, RM_r, de paramètres $n = 2^m - 1$, $k = \sum_{i=0}^{n} \binom{m}{i}$, $d = d_{Mr} = 2t + 1$.

Chen ([8]) montre qu'avec un décodage majoritaire en $L = 1 + \mathrm{Log}_2(\frac{m}{m-r})$ étapes on peut corriger $\lfloor \frac{d_{Mr} - 1}{2} \rfloor$ erreurs où $d_{Mr} = (2^{(m-r)s} - 1)/(2^s - 1) - 1$; alors que l'algorithme ordinaire nécessite (r+ 1) étapes. Ainsi pour $r \leqslant m/2$, L = 2. Pour décoder on considère des r-plans orthogonaux, non sur un (r-1)-plan (procédé ordinaire) mais sur une position.

Exemple : m = 5, r = 2, : n = 31, k = 16, d = 8, t = 3. ([10])

Les 6 plans 3-plans

$$f_1 = (1,5,8,29,10,14,22,25) \quad ,$$
$$f_2 = (1,5,8,29,9,24,28,30) \quad ,$$
$$f_3 = (1,5,8,29,11,18,23,27) \quad ,$$
$$f_4 = (1,5,8,29,15,16,17,26) \quad ,$$
$$f_5 = (1,5,8,29,4,7,13,21) \quad ,$$
$$f_6 = (1,5,8,29,0,6,12,19)$$

sont un ensemble E_3 de règles de parité orthogonales sur le 2-plan (1,5,8,29).

Les 6 2-plans $f'_1 = (1,5,8,29)$, $f'_2 = (1,2,7,10)$, $f'_3 = (1,21,23,28)$, $f'_4 = (1,3,24,26)$, $f'_5 = (1,4,14,20)$, $f'_6 = (1,11,15,25)$ sont orthogonaux sur la première position.

Nous évoquons maintenant la méthode dite de réduction séquentielle ([9]) qui permet de simplifier la deuxième étape.

Elle réduit la complexité du décodeur (économie de portes majoritaires par exemple) par l'emploi de circuits séquentiels linéaires qui effectuent des multiplications polynomiales. Elle consiste principalement à exprimer tous les r-plans $f_i(x)$ en fonction d'un r-plan déterminé $f_1(x)$, $f_i(x) = a_i(x)\, f_1(x)$. On suppose ainsi qu'il existe un r-plan générateur. Pour les codes de Reed et Muller on conjecture ([9]) que tout code d'ordre (m-r), dual du code d'ordre (r-1), admet un r-plan générateur. Pour m < 2047 cette conjoncture est vérifiée et on peut utiliser la méthode de réduction séquentielle.

Dans l'exemple précédent $f'_1(x)$ est un 2-plan générant un code RM_{m-2}(i.e.code (31,25), ensemble des mots pairs d'un code de Hamming).

On a $f'_1(x) = a_i(x)\, f'_1(x)\, [x^{31} - 1]$, avec
$a_1(x) = 1$, $a_2(x) = x^2$, $a_3(x) = x^{23}$,
$a_4(x) = x^{26}$, $a_5(x) = x^2+x^4+x^5+x^{12}$
$a_6(x) = x^{13}+x^{15}+x^{20}+x^{23}$, { [10] }.

Notons que l'utilisation de polynômes idempotents peut simplifier la recherche des $a_i(x)$ ([10]) . Une formule explicite permettant de calculer ces idempotents est donnée dans [11].

Nous présentons pour finir deux méthodes basées sur une prémultiplication matricielle des bits d'information (codage non systématique), et diminuant de un le nombre d'étapes nécessaires au décodage.
La première consiste à ne considérer qu'un sous-code cyclique du code utilisé et implique donc une perte en débit d'information.
La seconde conserve le rendement originel mais fait jouer un rôle inégal aux différents symboles d'information.

Soit un code euclidien d'ordre (r,s) de polynôme générateur g(x). Notons $f'_1(x)$ un des plans obtenus après $L-1 = \mathrm{Log}_2\left[\frac{m}{m-r}\right]$ étapes (si $r \leqslant m/2$, $L-1 = 1$ et $f'_1(x)$ est un r-plan). Soit f(x) le polynôme réciproque de $f'_1(x)$, alors :

Méthode 1 :

Le code cyclique de longueur $n = 2^{ms} - 1$, noté (fg), de polynôme générateur f(x)g(x), corrige $L = (d_{Mr} - 1)$ erreurs par un décodage en L - 1 étapes.
Remarquons d'abord que
dim(fg) = dim(g) - dim(f/pgcd(fg)).
Cette méthode fait perdre donc au maximum n - dim(f) bits d'information, en général pgcd(f,g) = 1 et cette borne est atteinte.
Exemple : Nous considérons toujours le code RM_2 de longueur 31. f'_1 engendre un code (31,25) : pgcd(f,g) = 1, dim(g) = 16 dim(fg) = 10. On obtient un code (31,10) corrigeant 3 erreurs par décodage majoritaire en une étape.

Méthode 2 :

Elle consiste à prémultiplier les k bits d'information par la matrice Q^{-1} de dimension (k×k) ;
Q est une matrice "quasi circulante" ayant pour i-ème ligne $x^{i-1}f(x)$ si $i \leqslant k-\deg(f)$, x^{i-1} sinon.
Les k symboles obtenus sont ensuite codés d'une manière systématique (grâce à un circuit divisant par g(x), par exemple). Au décodage on obtient dim(fg) bits d'information en L-1 étapes, les dim(g) - dim(fg) derniers nécessitant L étapes.
En reprenant l'exemple précédent :
10 bits sont décodables en une étape
6 bits sont décodables en deux étapes.
Ce décodage différentiel peut s'appliquer quand les bits sont d'importance inégale.

CONCLUSION

Après une longue période consacrée à la génération algébrique de codes et à l'étude de leur comportement asymptotique vis-à-vis des bornes, la théorie du codage s'oriente actuellement vers des aspects combinatoires et géométriques qui la rendent directement applicable. Notamment la notion de structure d'incidence fournit un cadre conceptuel simple pour une vaste classe de codes. Elle a l'avantage de faire apparaître naturellement la technique de décodage. Pour les codes géométriques la mise en oeuvre est encore facilitée par les réductions "séquentielle" ou "partielle" décrites ici.

REFERENCES

[1] L.D. Rudolph, A class of majority logic decodable codes, IEEE-IT, Vol.IT-13 n°2, Avril 1967, pp. 305-307.
[2] P. Delsarte et J.M. Goethals, Codes correcteurs d'erreurs et décodage par décision majoritaire, Revue MBLE, Vol 13, n°1, 1970, pp.23-35.
[3] P. Delsarte, A geometrical approach to a class of cyclic codes, J.of Combinatorial Theory 6,1969, pp.340-359.
[4] C. Hartmann, J. Ducey et L. Rudolph, On the structure of generalized finite-geometry codes, IEEE IT, Vol IT-20, n°2, Mars 1974, pp 240-252.
[5] P. Dembowski, Finite geometries, Springer-Verlay Berlin, New-York 1968.
[6] P. Delsarte, Majority logic decodable codes derived from finite inversive planes, Inf. Control 18,1971, pp.319-325.
[7] P. Camion, Codes quadratiques abéliens et plans inversifs Miqueliens.
[8] C.L. Chen, Note on majority logic decoding of finite geometry codes, IEEE IT, Vol IT-18, Juillet 1972, pp.539-541.
[9] L.D. Rudolph et C.P. Hartmann, Decoding by sequential code reduction, IEEE IT, Vol IT-19, n°4, Juillet 1973, pp.549-555.

[10] F.D. Schmandt, On the pratical application of sequential code reduction, IEEE IT, Vol IT-22, n°4, Juillet 1976, pp.482-483.

[11] G. Cohen, P. Godlewski et S. Perrine, Sur les idempotents des codes, Comptes rendus de l'Académie des Sciences, Note du 3 Janvier 1977.