Ovales et codages

Coll. Math. Discrètes : Codes et Hypergraphes, Bruxelles 1978
Cahiers C.E.R.O., Vol.20, 3-4, 1978

OVALES ET CODAGES

J. van LINT
Technische Hogeschool Eindhoven

1. *Introduction*

Nous nous proposons ici d'exposer certaines connexions entre les "designs" projectifs et les codes linéaires. Comme introduction nous rappelons quelques faits bien connus. Soit $n \equiv 2 \pmod 4$ et A la matrice d'incidence d'un plan projectif d'ordre n (désigné par PG(2, n)). Les lignes de A correspondent aux droites du plan. Les lignes de A engendrent un code binaire de longueur $n^2 + n + 1$. Il est facile de vérifier (voir [3]) que C a la dimension $1/2\,(n^2 + n + 2)$, et que le code étendu C est auto-dual. En outre le poids minimal de C est n + 1 et de manière surprenante les seuls mots de poids minimal sont les lignes de A, c'est-à-dire le plan projectif peut être reconstruit à partir de C. Dans la suite nous identifions souvent un ensemble S avec le vecteur (0, 1), s décrivant la fonction caractéristique de S.

Les mots de poids n + 2 de C ont aussi une interprétation géométrique. Nous introduisons d'abord l'objet géométrique correspondant. Un *ovale* est un ensemble O de n + 1 points de PG(2, n) tel que trois quelconques d'entre eux ne sont pas alignés. Une droite qui coupe O en un point est une *tangente* de l'ovale. Si n est pair O a n + 1 tangentes qui sont concourantes en un point appelé le noyau de O. Si on ajoute ce point à O on obtient un ensemble S qui a aussi la propriété que chaque ligne coupe S en au plus 2 points. On appelle S un hyperovale. La seconde propriété surprenante du code C est le fait que les mots de poids n + 2 sont les hyperovales de PG(2, n). Toutes ces propositions peuvent être démontrées par des arguments de comptage. On obtient des résultats comparables si $n \equiv 0 \pmod 4$ et des généralisations sont connues pour les plans d'ordre impair, utilisant des alphabets autres que GF(2) (voir [1] , [5]).

Les connexions entre les plans projectifs et les codes qu'ils engendrent ont été utilisées dans le but de démontrer que certains plans n'existent pas. Par exemple, F.J. MacWillimans, N.J.A. Sloane et J.G. Thompson (voir [3], [4]) ont démontré que le code engendré par PG(2, 10), si ce plan existe, n'a aucun mot de poids 15. Un résultat comparable pour deux autres poids serait suffisant pour établir la nonexistence de PG(2, 10).

Les arguments que nous avons présentés ci-dessus constituent une motivation pour les généralisations que nous voulons considérer dans les parties suivantes. Les résultats seront publiés en détail dans un travail commun avec E.F. Assmus (voir [2]).

2. *Ovales dans designs projectifs*

Dans la suite D est un design projectif avec $\lambda > 1$, c'est-à-dire un design symétrique $2 - (v, k, \lambda)$ avec $2 < k < v - 1$, $\lambda > 1$. *L'ordre* de D est $k - \lambda$. Comme ci-dessus A désigne la matrice d'incidence de D et les lignes de A correspondent aux blocs de D. Un *arc* S est un ensemble de points de D tel que trois quelconques d'entre eux ne sont pas dans un même bloc de D. Un bloc qui coupe S en un point est appelé *tangente* de S.

Théorème 1. Pour un arc S dans un (v, k, λ)-design projectif D on a

i) $|S| < \frac{k+\lambda-1}{\lambda}$ si $k - \lambda$ est impair

$k - \lambda$ est pair, $\lambda \nmid k$,

ii) $|S| < \frac{k+\lambda}{\lambda}$ si $k - \lambda$ est pair, $\lambda | k$.

Preuve. D'abord supposons que S ait une tangente B_0 et soit $p = S \cap B_0$. Pour chaque point $q \in S \setminus \{p\}$ il y a λ blocs B avec $S \cap B = \{p, q\}$. Alors il y a au moins $\lambda(|S| - 1)$ blocs distincts contenant p. Parce qu'il y a k blocs contenant p on obtient l'inégalité i). Si S n'a pas de tangentes on trouve de la même façon $|S| = (k + \lambda)/\lambda$. En ce cas soit $p \notin S$ et supposons qu'il y ait x blocs contenant p qui coupent S. Alors, $2x = \lambda |S| = k + \lambda$, c'est-à-dire $k + \lambda$ et $k - \lambda$ sont pairs.

Définition. Si S est un arc dans un (v, k, λ)-design projectif avec égalité en i) ou ii) du Théorème 1 on appelle S un *ovale* de D. L'ensemble des ovales de D est désigné par Ovale (D).

Si S est un ovale et que $p \notin S$ on appelle P un *point extérieur* s'il y a une tangente de S qui contient p; sinon p est *point intérieur*. *Sécantes* et *blocs extérieurs* sont définis comme d'habitude.

En [2] des arguments de comptage élémentaires sont utilisés pour déterminer les nombres donnés ci-dessous, où S est un ovale dans un (v, k, λ)-design projectif.

	S	points extérieurs	points intérieurs	tangents	sécantes	blocs extérieurs
$k-\lambda$ pair, λ/k	$(k+\lambda)/\lambda$	0	$k(k-2)/\lambda$	0	$k(k+\lambda)/2\lambda$	$(k-2)(k-\lambda)/2\lambda$
$k-\lambda$ impair, $\lambda/(k-1)$	$(k+\lambda-1)/\lambda$	$(k+\lambda-1)(k-1)/2\lambda$	$(k-\lambda-1)(k-1)/2\lambda$	$(k+\lambda-1)/\lambda$	$(k+\lambda-1)(k-1)/2\lambda$	$(k-\lambda-1)(k-1)/2\lambda$

Dans le cas restant, c'est-à-dire $k - \lambda$ pair et $\lambda | (k - 1)$ les nombres de blocs sont les mêmes mais évidemment il n'y a pas de points intérieurs.

Remarques : Les nombres dans la table ci-dessus nous montrent que dans le cas d'ordre pair et $\lambda | k$ on obtient un design $2 - \left(\frac{(k-2)(k-\lambda)}{2\lambda}, \frac{k-\lambda}{2}, \lambda\right)$ qui a comme points les blocs

extérieurs d'un ovale O et comme blocs les points de D\O. Il est possible que ce design ait des blocs répétés.

En [2] plusieurs théorèmes concernant des designs avec ovales sont démontrés. Certains d'entre eux sont des généralisations de théorèmes classiques. On remarque une propriété intéressante observée par B. Andriamanalamanana. A nouveau la démonstration se fait par comptage.

Théorème 2. Si S est un ovale dans un (v, k, λ)-design projectif d'ordre pair avec $\lambda \mid (k - 1)$ il y a un ensemble de λ points (le noyau) contenu dans chacune des $|S|$ tangentes.

Nous donnons un exemple d'un design avec beaucoup d'ovales. Considérons le biplan unique d'ordre 3, c'est-à-dire un $2 - (11, 5, 2)$ design. En ce cas un ovale est un ensemble de trois points qui ne sont pas contenus dans un bloc. C'est évident que deux points quelconques déterminent trois ovales. Alors les ovales forment un $2 - (11, 3, 3)$ design.

3. *Connexions avec les codes*

Soit D un (v, k, λ)-design projectif d'ordre pair avec $\lambda \mid k$. Comme dans l'introduction nous considérons le code binaire C engendré par les lignes de A, la matrice d'incidence de D. D'après la définition d'un ovale O dans D, O est un ensemble de $(k + \lambda)/\lambda$ points tel que chaque bloc de D coupe O en deux ou aucun point(s). O est donc un mot de poids $(k + \lambda)/\lambda$ de $C^{\perp}$. Considérons encore un mot $\underline{s}$ de $C^{\perp}$ comme un ensemble de points de D. Alors, chaque bloc de D coupe $\underline{s}$ en un nombre pair de points. Pour un point fixe p de $\underline{s}$ nous comptons les drapeaux (q, B) avec $q \in \underline{s}$, $q \neq p$, $q \in B$ de deux manières différentes. Nous trouvons

$$\lambda(w(s) - 1) \geqslant |\{B \mid p \in B\}| = k ,$$

c'est-à-dire $w(\underline{s}) \geqslant (k + \lambda)/\lambda$. L'égalité n'est possible que si $\underline{s}$ est un ovale.
En résumé :

Théorème 3. Si C est le code binaire engendré par les blocs d'un (v, k, λ)-design projectif D d'ordre pair avec $\lambda \mid k$ et si D possède un ovale, les ovales de D sont les mots de poids minimal de $C^{\perp}$.

Ce théorème montre que le code $C^{\perp}$ a un poids minimal plus grand que l'estimation a priori si D n'a pas d'ovales. Des théorèmes comparables existent pour le cas d'ordre impair (voir [2], [6]).

Comme exemple intéressant de la collaboration des méthodes du codage et la théorie des designs nous démontrons un théorème qui donne une caractérisation du biplan d'ordre 2.

Théorème 4. Soit D un (v, k, λ)-design projectif avec $k \equiv 0 \pmod 4$, $\lambda \equiv 2 \pmod 4$, $\lambda \mid k$. Si Ovale (D) est un 2-design alors D est le biplan d'ordre 2.

Preuve. On remarque que les paramètres V, K, Λ, R du design Ovale (D) satisfont $V = v$, $K = (k + \lambda)/\lambda$, $R = (k - 1)\Lambda$. Soit A la matrice d'incidence de D et C le code engendré par les lignes de A. Evidemment $C \subset C^{\perp}$, c'est-à-dire dim $C \leqslant 1/2(v - 1)$; (ici on utilise le fait que v est impair). Soient $e_1, e_2, \ldots e_v$ les facteurs invariants de A. Avec la notation $d_i : e_1 e_1 \ldots e_i$ on a $d_v = \det(A) = k(k - \lambda)^{v-1/2}$. Pour calculer det (A) on ajoute à la dernière ligne la somme des autres lignes et on développe suivant la dernière ligne. On voit que le pgcd des mineurs d'ordre $v - 1$ de A est un diviseur de $(k - \lambda)^{v-1/2}$ et donc $d_{v-1} \mid (k - \lambda)^{v-1/2}$. Par suite au moins $\frac{v-1}{2}$ des facteurs invariants sont impairs, c'est-à-dire le rang (mod 2) de A est $\geqslant 1/2(v - 1)$. Il résulte que dim $C = 1/2(v - 1)$. Ceci montre que $C^{\perp}$ est engendré par les lignes de A et le vecteur $\underline{1} = (1, 1, \ldots, 1)$.

Soit $\underline{s}$ un vecteur de poids d de C (interprété comme sous-ensemble des points de D). Soit p un point fixe de $\underline{s}$. Pour chaque $q \in \underline{s}$, $q \neq p$, il y a Λ ovales contenant p et q. D'après le théorème 3 on sait que les ovales sont les mots de poids minimal de $C^{\perp}$. Par suite $\underline{s}$ coupe chaque ovale en un nombre pair de points. Comme dans la preuve du théorème 3 on obtient $(d - 1) \geqslant R$, c'est-à-dire $d \geqslant k$. Donc C a un poids minimal k. Par conséquent chaque ovale est de la forme $\underline{1} + \underline{c}$, avec $\underline{c} \in C$, et ceci montre que deux ovales se coupent . Si $\underline{1} + \underline{c}$ et $\underline{1} + \underline{c}'$ sont deux ovales qui se coupent en a points nous trouvons, puisque leur somme est un mot de C ,

$$2\left(\frac{k + \lambda}{\lambda} - a\right) \geqslant k ,$$

et donc $\lambda = 2$, $a = 1$. On trouve que Ovale (D) est un plan projectif d'ordre $\frac{1}{2}k$ et alors k doit être 4. □

Comme dernier exemple nous signalons les efforts récents fournis en vue de trouver un plan projectif d'ordre 10. Dans l'introduction nous avons vu qu'un plan d'ordre 10 engendre un code binaire C pour lequel $\bar{C}$ est un (112,56)-code auto-dual. Eh bien, soit B la matrice d'incidence d'un biplan,d'ordre 9, c'est-à-dire un 2- (56, 11, 2)-design. Alors $(I_{56}\ B)$ est matrice génératrice d'un (112, 56)-code auto-dual. De nouveau, des arguments simples de comptage montrent qu'il existe trois types de mots de poids 12 dans ce code. Ils correspondent aux blocs du biplan, les sommes de tous les blocs contenant un point fixe du biplan, et aux ovales du biplan. Pendant quelque temps on espérait trouver un biplan d'ordre 9 avec assez d'ovales pour produire le plan d'ordre 10. Maintenant on connait quatre biplans d'ordre 9 et aucun n'a donné le résultat escompté. Il ne vaut pas la peine je crois de continuer cette approche.

REFERENCES

[1] ASSMUS, E.F., Jr et SACHAR, H.E., Ovals from the point of view of coding theory, dans *Higher Combinatorics* (M. Aigner, ed.), Reidel, Dordrecht, 1977, pp. 213-216.

[2] ASSMUS, E.F., van LINT, J.H., Ovals in projective designs, *J. Combinatorial Theory (A)*, à paraître.

[3] CAMERON, P.J. et van LINT, J.H., Graph Theory, Coding Theory and Block Designs, *London Math. Soc. Lecture Note Series 19*, Cambridge Univ. Press, 1975.

[4] MACWILLIAMS, F.J., SLOANE, N.J.A. et THOMPSON, J.G., On the existence of a projective plane of order 10, *J. Combinatorial Theory 14* (1973), 66-78.

[5] SACHAR, H., The F_p span of the incidence matrix of a finite projective plan, *Math. Z.*, à paraître.

[6] SALWACH, C.J., *Biplanes and projective planes*, Ph. D. Dissertation, Lehigh University, Bethlehem, Pa. 1976.