# Autour du critère de Xing pour les codes séparants

Hugues RANDRIAM

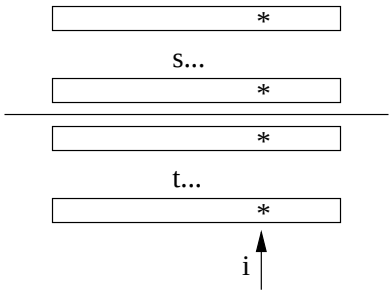
Lundi 29 septembre 2003

## 1 Codes séparants

Soit $Q$ un ensemble (alphabet) fini de cardinal $q$. On rappelle qu'un code $C$ de longueur $n$ sur $Q$ est une partie non-vide $C \subset Q^n$. Le rendement $q$-aire de $C$ est le réel $\rho(C) = \frac{1}{n} \log_q \#C$. Si $C_1, C_2, \ldots$ forment une suite de codes de longueurs $n_1, n_2, \cdots \to \infty$, le rendement asymptotique de cette suite est la limite supérieure des $\rho(C_k)$.

Un code $C$ est dit $(s,t)$-séparant si pour toute donnée de $s+t$ mots de code distincts $x^{(1)}, \ldots, x^{(s+t)} \in C$ il existe un indice $i$ telle que l'ensemble des $i$-èmes coordonnées des $s$ premiers d'entre eux soit disjoint de l'ensemble des $i$-èmes coordonnées des $t$ derniers :

$$\exists i \;\; \forall \sigma \in \{1, \ldots, s\} \;\; \forall \tau \in \{1, \ldots, t\} \;\; x_i^{(\sigma)} \neq x_i^{(s+\tau)} \tag{1}$$



Dans le cas où $s = 1$, on parlera de code $t$-séparant (au lieu de $(1,t)$-séparant). Dans la littérature anglophone on trouve le terme *$t$-frameproof code*.

Le problème considéré ici est d'estimer le rendement asymptotique maximal $R_q(s,t)$ d'une famille de codes $(s,t)$-séparants. On notera aussi $R_q(t) = R_q(s,t)$. Il n'est pas difficile de voir qu'on a

$$R_q(s,t) \leq \min\{R_q(s), R_q(t)\} \tag{2}$$

et

$$R_q(t) \leq \frac{1}{t}. \tag{3}$$

Lorsque $Q = \mathbb{F}_q$ est un corps fini, la condition (1) définissant les codes $(s,t)$-séparants peut se réécrire

$$\exists i \prod_{1 \leq \sigma \leq s; 1 \leq \tau \leq t} (x_i^{(\sigma)} - x_i^{(s+\tau)}) \neq 0. \tag{4}$$

Supposons maintenant le code $C$ linéaire (i.e. $C$ est un sous-$\mathbb{F}_q$-espace vectoriel de $\mathbb{F}_q^n$). Alors les différences $y^{(\sigma,\tau)} = x^{(\sigma)} - x^{(s+\tau)}$ sont encore des mots de code, et l'on voit qu'*une condition suffisante sur un code linéaire pour être $(s,t)$-séparant est que le mot produit (coordonnée par coordonnée) de $st$ mots de code non nuls ne soit jamais le mot nul :*

$$\prod_{\sigma,\tau} y^{(\sigma,\tau)} \not\equiv 0. \tag{5}$$

Remarquons que cette condition est remplie dès lors que chaque mot de code non nul a strictement moins $n/st$ zéros : le produit de $st$ mots aura en effet strictement moins de $n$ zéros. Si l'on considère donc un code linéaire $C$ de longueur $n$, de dimension $k$, et de distance minimale $d$, le rendement de $C$ est $\rho = k/n$, et une condition suffisante sur la distance normalisée $\delta = d/n$ pour que (5) soit vérifiée est que

$$\delta \gtrapprox 1 - \frac{1}{st}. \tag{6}$$

Un réel $\delta$ étant fixé, la géométrie algébrique (Tsfasman-Vladut-Zink, Garcia-Stichtenoth...) fournit une famille de codes linéaires dur $\mathbb{F}_q$ de distance normalisée $\delta$ et de rendement asymptotique $\rho$ dès lors que

$$\rho + \delta = 1 - \frac{1}{A(q)} \tag{7}$$

où $A(q)$ est une constante déterminant asymptotiquement le nombre maximal de points d'une courbe sur $\mathbb{F}_q$ en fonction de son genre (lorsque $q$ est un carré, on a $A(q) = \sqrt{q} - 1$). De ceci et de (6) on conclut :

**Proposition 1** *On a*

$$R_q(s,t) \geq \frac{1}{st} - \frac{1}{A(q)}. \tag{8}$$

# 2 La construction de Xing

La minoration obtenue au paragraphe précédent reposait sur la condition (6). La construction de [Xing02] se propose d'utiliser la condition plus faible (5), qui se traduit agréablement dans le langage de la géométrie algébrique. En effet, rappelons qu'un code algébro-géométrique est construit, à partir de la donnée d'une courbe $X$, d'un diviseur $D$, et d'un diviseur effectif $G$ de degré $n$, en évaluant les sections de $\mathcal{L}(D)$ en les points de $G$. Si les $y^{(\sigma,\tau)}$ intervenant dans la condition (5) sont des sections de $\mathcal{L}(D)$, leur produit est une section de $\mathcal{L}(stD)$. Ainsi le critère (5) peut se reformuler ainsi :

**Proposition 2** *Le code construit en évaluant les sections de $\mathcal{L}(D)$ en les points de $G$ est $(s,t)$-séparant si et seulement si*

$$\mathcal{L}(stD - G) = 0. \tag{9}$$

Afin de pouvoir appliquer ce critère pour montrer l'existence de codes $(s,t)$-séparants disposant de bons paramètres, il faut pouvoir estimer le degré maximal $m$ d'un diviseur $D$ vérifiant cette proposition. Pour ce faire on procède par comptage :

- on estime le nombre de classes d'équivalence de diviseurs de degré $stm - n$ admettant un représentant de la forme $stD - G$ pour $D$ de degré $m$ ;
- on compte le nombre de diviseurs effectifs de degré $stm - n$ ;

et dès lors que ceux-ci sont moins nombreux que ceux-là, on est assuré de l'existence d'un $D$ convenable.

Numériquement, on arrive ainsi au résultat suivant, qui améliore la proposition 1 :

**Proposition 3** *On a*

$$R_q(s,t) \geq \frac{1}{st} - \frac{1}{A(q)} + \frac{1 - 2\log_q st}{stA(q)}. \tag{10}$$

# 3 Quelques remarques

Une première remarque est que la borne inférieure sur $R_q(s,t)$ à laquelle on parvient n'est proche (à $q$ tendant vers l'infini) de la borne supérieure que lorsque l'on a $s = 1$. Il serait intéressant de savoir rapprocher ces bornes pour $s \geq 2$. Dans ce cas général, il ne semble pas déraisonnable d'espérer un rendement optimal de l'ordre de

$$\frac{1}{s+t-1}. \tag{11}$$

Une deuxième remarque est qu'il est possible d'améliorer un peu l'argument de comptage dès lors qu'on sait estimer le rang du groupe de $st$-torsion du groupe de Picard de la courbe considérée. Par exemple, en caractéristique $p$, le rang du groupe des points de $p$-torsion d'une variété abélienne de dimension $g$ étant au plus $g$ (et non $2g$), on trouve

$$R_q(p) \geq \frac{1}{p} - \frac{1}{A(q)} + \frac{1 - \log_q p}{pA(q)} \tag{12}$$

(le facteur 2 devant le log disparaît). Dans cette direction, il serait intéressant par exemple de montrer que ce groupe de torsion est «petit», voire nul, pour une infinité de courbes approchant la constante optimale $A(q)$.

# Références

[Xing02] Chaoping Xing. *Asymptotic bounds on frameproof codes.* IEEE Transactions on Information Theory **48** (2002) 2991–2995.