Bornes SDP pour les codes de sous-espaces d'un espace vectoriel fini

Alberto Passuello, Christine Bachoc, Frank Vallentin*

Université de Bordeaux 1, TU Delft*

Journées C2, 8 octobre 2012

Codage de réseau

Un réseau est un graphe orienté.

Dans le codage de réseau (network coding), on s'interesse à optimiser la transmission des données dans un réseau, depuis les sources jusqu'aux récepteurs.
L'idée est de permettre aux noeuds de encoder les données reçues avant de le retransmettre (Ahlswede et al. - 2000).

Avantages principaux : meilleur taux de transmission, robustesse accrue.

Description du canal

Codage de réseau lineaire aléatoire :

- les noeuds transmettent des combinations lineaires aléatoires des données reçues.
- avantage de l'aléatoirité : les recepteurs n'ont pas besoin de connaître la topologie du réseau.

Description du canal

Codage de réseau lineaire aléatoire :

- les noeuds transmettent des combinations lineaires aléatoires des données reçues.
- avantage de l'aléatoirité : les recepteurs n'ont pas besoin de connaître la topologie du réseau.

La source injecte les paquets $p_1, \ldots, p_m \in \mathbb{F}_q^n$ dans le réseau.
Soit $\mathbf{p} = (p_1, \ldots, p_m)^T \in \mathbb{F}_q^{m \times n}$.
A cause du codage lineaire des noeuds, le recepteur recevra $A\mathbf{p}$ pour une matrice A.

L'espace vectoriel engendré par les paquets est fixé tout au long du réseau : la veritable information qui parcour le canal n'est pas la collection des $p_1, \ldots, p_m$, mais plutôt $\text{span}\{p_1, \ldots, p_m\}$.

Codes de sous-espaces (Koetter, Kschischang - 2006)

Les codes utilisés sont sous-ensembles de l'espace projectif

$$\mathcal{P}(\mathbb{F}_q^n) = \{ \text{ sous-espaces lineaires de } \mathbb{F}_q^n \ \}$$

ou de l'espace de Grassmann

$$\mathcal{G}_q(n,k) = \{ \text{ sous-espaces lineaires de } \mathbb{F}_q^n \text{ avec dimension } k \ \}.$$

Codes de sous-espaces (Koetter, Kschischang - 2006)

Les codes utilisés sont sous-ensembles de l'espace projectif

$$\mathcal{P}(\mathbb{F}_q^n) = \{ \text{ sous-espaces lineaires de } \mathbb{F}_q^n \ \}$$

ou de l'espace de Grassmann

$$\mathcal{G}_q(n,k) = \{ \text{ sous-espaces lineaires de } \mathbb{F}_q^n \text{ avec dimension } k \ \}.$$

Dans les deux espaces on a la distance

$$d(U,V) = \dim(U+V) - \dim(U \cap V) = \dim U + \dim V - 2\dim(U \cap V).$$

Definissons le coefficient binomiale q-aire par

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n-1)\dots(q^{n-k+1}-1)}{(q^k-1)\dots(q-1)} = |\mathcal{G}_q(n,k)| \ .$$

Bornes

On s'interesse à determiner le cardinal maximal des codes de sous-espaces :

- $A_q(n,d) := \max\{|\mathcal{C}| \text{ for } \mathcal{C} \subset \mathcal{P}(\mathbb{F}_q^n), d(\mathcal{C}) = d\}$
- $A_q(n,k,2\delta) := \max\{|\mathcal{C}| \text{ for } \mathcal{C} \subset \mathcal{G}_q(n,k), d(\mathcal{C}) = 2\delta\}$

où l'on peut se restreindre à $k \leq n/2$.

Dans cet exposé l'on s'interesse aux bornes superieures pour $A_q(n,d)$ et $A_q(n,k,2\delta)$.

Bornes pour $\mathcal{G}_q(n,k)$

Comme pour l'espace de Hamming, nous avons ici la borne sphere-packing et la borne de Singleton.
En outre :

Borne anticode :

$$A_q(n,k,2\delta) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_k(\delta-1)|} = \left(\frac{q^n-1}{q^k-1}\right)\cdots\left(\frac{q^{n-k+\delta}-1}{q^\delta-1}\right)$$

(Wang, Xing, Safavi-Naini - 2003)

Borne de Johnson :

$$A_q(n,k,2\delta) \leq \left\lfloor \frac{q^n-1}{q^k-1} A_q(n-1,k-1,2\delta) \right\rfloor$$

qui, en iterant, nous donne

$$A_q(n,k,2\delta) \leq \left\lfloor \frac{q^n-1}{q^k-1} \left\lfloor \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lfloor \frac{q^{n-k+\delta}-1}{q^\delta-1} \right\rfloor \cdots \right\rfloor \right\rfloor$$

(Xia, Fu - 2007)

La borne de programmation lineaire de Delsarte existe aussi, mais pour tous les paramètres testés, elle n'ameliore pas par rapport à la borne anticode.

Bornes pour $\mathcal{P}(\mathbb{F}_q^n)$

Un programme lineaire pour $\mathcal{P}(\mathbb{F}_q^n)$:

$$A_q(n, 2e+1) \leq \max \left\{ \begin{array}{lll} \sum_{k=0}^{n} D_k & : & D_k \leq A_q(n, k, 2e+2) \ \forall \ k \\ & & \sum_{i=0}^{n} c(i,k,e) D_i \leq \left[\begin{array}{c} n \\ k \end{array} \right] \ \forall \ k \end{array} \right\}$$

où $c(i, k, e) = |B(V, e) \cap \mathcal{G}_q(n, k)|$ pour V de dimension i.

Preuve : chaque code $\mathcal{C}$ donne une solution admissible de valeur $|\mathcal{C}|$ en definissant $D_k = |\mathcal{C} \cap \mathcal{G}_q(n, k)|$.

(Etzion, Vardy - 2008)

La methode SDP

Forme generale d'un programme semidefini positif :

$$\sup \left\{ \begin{array}{ll} \langle C, Y \rangle & \text{tel que : } \quad Y \succeq 0, \\ & \qquad \langle A_i, Y \rangle = b_i \text{ for } i = 1, \ldots, m \end{array} \right\}$$

pour A_i, C matrices symétriques.

- Generalisation de la programmation lineaire,
- bons algorithms pour resoudre SDP,
- beaucoup d'applications en combinatoire et théorie des codes.

D'après Lovász, on a un programme semidefini positif (SDP) pour borner le cardinal d'un code dans $X = \mathcal{P}(\mathbb{F}_q^n)$ avec distance minimale d :

$$A_q(n,d) \leq \sup \left\{ \begin{array}{lll} \sum_{X^2} F(x,y) & : & F \in \mathbb{R}^{X \times X}, F \succeq 0 \\ & & \sum_X F(x,x) = 1 \\ & & F(x,y) = 0 \text{ if } 0 < d(x,y) < d \end{array} \right\}$$

Preuve : pour chaque code $\mathcal{C} \subset X$ avec distance minimale d, la matrice

$$F(x,y) = \frac{1}{|\mathcal{C}|} \mathbf{1}(x \in \mathcal{C}) \mathbf{1}(y \in \mathcal{C})$$

donne une solution admissible, de valeur $\sum F(x,y) = |\mathcal{C}|$.

D'après Lovász, on a un programme semidefini positif (SDP) pour borner le cardinal d'un code dans $X = \mathcal{P}(\mathbb{F}_q^n)$ avec distance minimale d :

$$A_q(n,d) \leq \sup \left\{ \begin{array}{lll} \sum_{X^2} F(x,y) & : & F \in \mathbb{R}^{X \times X}, F \succeq 0 \\ & & \sum_X F(x,x) = 1 \\ & & F(x,y) = 0 \text{ if } 0 < d(x,y) < d \end{array} \right\}$$

Preuve : pour chaque code $\mathcal{C} \subset X$ avec distance minimale d, la matrice

$$F(x,y) = \frac{1}{|\mathcal{C}|} \mathbf{1}(x \in \mathcal{C}) \mathbf{1}(y \in \mathcal{C})$$

donne une solution admissible, de valeur $\sum F(x,y) = |\mathcal{C}|$.

Problème : les matrices F sont de taille trop grande.
Solution : utiliser l'action de $GL_n(q)$ sur X pour symetriser le programme.

Symétrisation

On peut se borner aux matrices F qui sont $GL_n(q)$-invariantes. L'algèbre de ces matrices peut être diagonalisé par blocs, et on obtient la parametrisation suivante : $F \succeq 0$ si et seulement si

$$F(x,y) = \sum_k \langle F_k, E_k(x,y) \rangle \text{ avec } F_k \succeq 0 \ \forall k = 0, \ldots, \lfloor n/2 \rfloor$$

où les F_k sont des blocs de taille $n - 2k + 1$.

Symétrisation

On peut se borner aux matrices F qui sont $GL_n(q)$-invariantes. L'algèbre de ces matrices peut être diagonalisé par blocs, et on obtient la parametrisation suivante : $F \succeq 0$ si et seulement si

$$F(x,y) = \sum_k \langle F_k, E_k(x,y) \rangle \text{ avec } F_k \succeq 0 \ \forall k = 0, \ldots, \lfloor n/2 \rfloor$$

où les F_k sont des blocs de taille $n - 2k + 1$.

Pour $k \leq s \leq t \leq n - k$, $\dim(x) = s$, $\dim(y) = t$

$$E_{kst}(x,y) = |X| \frac{\begin{bmatrix} t-k \\ s-k \end{bmatrix} \begin{bmatrix} n-2k \\ t-k \end{bmatrix}}{\begin{bmatrix} n \\ t \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix}} q^{k(t-k)} Q_k(n, s, t; s - \dim(x \cap y))$$

où les Q_k sont des polynômes de Hahn q-aires.

Resultats

	Etzion-Vardy LP	SDP
$A_2(7,3)$	832	776
$A_2(7,5)$	36	35
$A_2(8,3)$	9365	9268
$A_2(8,5)$	361	360
$A_2(9,3)$	114387	107419
$A_2(9,5)$	2531	2485
$A_2(10,3)$	2543747	2532929
$A_2(10,5)$	49451	49394
$A_2(10,7)$	1224	1223
$A_2(11,5)$	693240	660285
$A_2(11,7)$	9120	8990
$A_2(12,7)$	323475	323374
$A_2(12,9)$	4488	4487
$A_2(13,7)$	4781932	4691980
$A_2(13,9)$	34591	34306
$A_2(14,9)$	2334298	2334086
$A_2(14,11)$	17160	17159
$A_2(15,11)$	134687	134095