

Empilements de Sphères et Optimisation Combinatoire

Christine Bachoc

Université Bordeaux I, IMB

Séminaire Tripode 16/01/2009

Plan de l'exposé

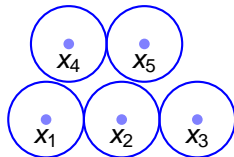
- ▶ Empilements de sphères
- ▶ Graphes et optimisation combinatoire
- ▶ Généralisations du ϑ de Lovász aux espaces compacts
- ▶ Applications: bornes pour la densité des empilements
- ▶ Hiérarchies de ϑ ; espace euclidien

En collaboration avec: Gabriele Nebe (Aachen univ.), Fernando Mario de Oliveira Filho et Frank Vallentin (CWI Amsterdam).

Empilements de sphères

- ▶ (X, d) un espace métrique, équipé d'une mesure régulière positive μ .
- ▶ Un **empilement de sphères** \mathcal{E} est une réunion de boules $B(x_i, r)$ d'intérieurs disjoints et de même rayon.

$$\mathcal{E} = \cup_i B(x_i, r)$$



- ▶ La donnée d'un empilement \mathcal{E} est équivalente à celle de l'ensemble des centres $\mathcal{C} = \{x_i, i \in I\}$ avec la contrainte $d(x_i, x_j) \geq 2r$, aussi appelé un **code de distance minimale $2r$** .

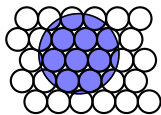
Densité

- ▶ La **densité** $\delta(\mathcal{E})$ d'un empilement de sphères mesure la proportion d'espace occupée par \mathcal{E} .
- ▶ Cas facile: X est de mesure finie et le volume des boules ne dépend que de leur rayon.

$$\delta(\mathcal{E}) = \frac{\text{vol}(\mathcal{E})}{\text{vol}(X)} = \frac{\text{vol}(B(1))}{\text{vol}(X)} \text{card}(\mathcal{E}).$$

- ▶ Autre: $X = \mathbb{R}^n$.

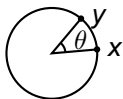
$$\delta(\mathcal{E}) = \limsup_{R \rightarrow +\infty} \frac{\text{vol}(\mathcal{E} \cap B(R))}{\text{vol}(B(R))}.$$



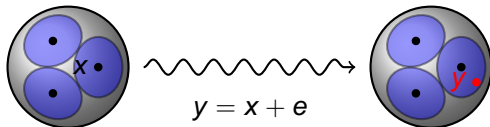
ne dépend pas du centre de $B(R)$, ni du rayon r .

Exemple: la sphère unité

- ▶ $X = S^{n-1}$, distance angulaire $\theta(x, y)$.

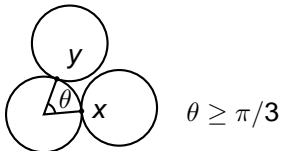


- ▶ Si \mathcal{E} est un “empilement de sphères” de rayon $\theta/2$, l'ensemble des centres est un **code sphérique de distance minimale θ** .
- ▶ Applications en théorie de l'information.



Le problème du “kissing number”

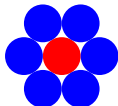
- ▶ Problème: dans l'espace euclidien \mathbb{R}^n , combien de sphères de rayon 1 peuvent simultanément toucher une même sphère de rayon 1 ?
- ▶ Ce nombre est appelé le **kissing number** de la dimension n et est noté τ_n .
- ▶ Dans une telle configuration, les points de contacts ont une distance angulaire au moins égale à $\pi/3$. Ils forment donc un code sphérique de distance minimale $\pi/3$.



Les petites dimensions

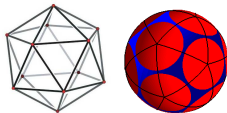
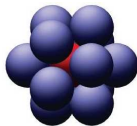
- ▶ Dimension 2

- ▶ $\tau_2 = 6$
- ▶ La configuration est unique à isométrie près.



- ▶ Dimension 3

- ▶ L'icosaèdre régulier fournit une solution avec 12 points.
- ▶ L'angle minimal est $\simeq 63.4^\circ$.



Historique

- ▶ 1694:
La question de savoir si une treizième sphère peut être insérée est un sujet de dispute entre Isaac Newton et David Gregory.



- ▶ 1953: Schütte et Van der Waerden démontrent que $\tau_3 = 12$.
- ▶ 1956: Leech donne une preuve plus élégante.

Les autres valeurs connues de τ_n sont:

- ▶ 1979: $\tau_8 = 240$ (E_8) et $\tau_{24} = 196560$ (vecteurs min. du réseau de Leech) Levenshtein; indép. Odlysko et Sloane
- ▶ 2003: $\tau_4 = 24$ (D_4), démontré par Oleg Musin

Pour les autres valeurs de $n \leq 24$, bornes d'Odlysko-Sloane (1979) améliorée par B. et Vallentin en 2006.

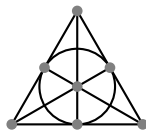
L'espace de Hamming

- ▶ $X = \mathbb{F}_2^n$
- ▶ **Distance de Hamming** $d_H(x, y)$

$$d_H(x, y) = \text{card}\{i : x_i \neq y_i\}$$

- ▶ Un code de distance minimale 3 permet de corriger une erreur.
- ▶ Exemple: le code de Hamming dans \mathbb{F}_2^7 contient 16 mots et transmet 4 bits d'information.

- ▶ 0000000
- ▶ 1111111
- ▶ 7 droites du plan projectif
- ▶ leurs complémentaires



Autres espaces

- ▶ A^n , A alphabet, pour la distance de Hamming ou des variantes.
- ▶ $J(k, n)$ espace de Johnson: ensemble des mots binaires de longueur n et de poids k .
- ▶ $PG(q, n)$ ensemble des sous-espaces vectoriels de \mathbb{F}_q^n , avec

$$\dim(A, B) = \dim(A) + \dim(B) - 2 \dim(A \cap B)$$

Applications au codage de réseau.

- ▶ $\mathcal{G}_{m,n}(\mathcal{K})$, $\mathcal{K} = \mathbb{R}, \mathbb{C}$ espaces grassmanniens. La position relative de deux sous-espaces de dimension m est mesurée par leurs angles principaux $(\theta_1, \dots, \theta_m)$. Applications aux systèmes de communication multi-antennes.
- ▶ Les espaces de Stiefel, les espaces de matrices unitaires, etc..

Graphes

- ▶ $G = (V, E)$ un graphe fini.
- ▶ Stable S : sous-ensemble de V tel que $S^2 \cap E = \emptyset$
- ▶ Nombre de stabilité de G : $\alpha(G) = \max_{S \text{ stable}} \text{card}(S)$
- ▶ 1978, L. Lovász, *On the Shannon capacity of a graph* introduit le nombre theta $\vartheta(G)$ et démontre le Sandwich Theorem:

Théorème

$$\alpha(G) \leq \vartheta(G) \leq \chi(\overline{G})$$


($\chi(G)$ =nbre chromatique=nbre min de classes d'une partition de V en stables).

- ▶ $\vartheta(G)$ est la valeur optimale d'un programme semi-défini positif.
- ▶ Il démontre que la capacité du pentagone vaut $\sqrt{5}$.

La capacité du pentagone

- ▶ Shannon définit un canal “zéro erreurs” associé à un graphe G . Celui-ci transmet des mots de G^n mais confond les paires de mots qui sont des arêtes du graphe produit.
- ▶ Graphe produit G^2 :
 $(x, y) - (x', y')$ si $((x = x' \text{ ou } x - x')$ et $(y = y' \text{ ou } y - y')$).
- ▶ Nombre de mots distincts transmis : $\alpha(G^n)$.
- ▶ Capacité :

$$c(G) = \limsup_{n \rightarrow +\infty} (\alpha(G^n))^{1/n}$$

- ▶ $G =$ le pentagone. $\alpha(G) = 2$  donc $c(G) \geq 2$.
- ▶ $\alpha(G^2) = 5$ ($S = \{00, 12, 24, 31, 43\}$). Donc $c(G) \geq \sqrt{5}$. Égalité conjecturée par Shannon.
- ▶ $\alpha(G^n) \leq \vartheta(G^n) \leq \vartheta(G)^n$ et $\vartheta(G) = \sqrt{5}$!

ϑ de Lovász

- ▶ $G = (V, E)$ et $V = \{1, \dots, n\}$

$$\vartheta(G) = \max \left\{ \sum_{i,j} B_{i,j} : \begin{array}{l} B = (B_{i,j})_{1 \leq i,j \leq n}, B \succeq 0 \\ \sum_i B_{i,i} = 1, \\ B_{i,j} = 0 \quad (i,j) \in E \end{array} \right\}$$

- ▶ Preuve de $\alpha(G) \leq \vartheta(G)$:

- ▶ Si S est un stable, la matrice B définie par

$$B_{i,j} = \frac{\mathbf{1}_S(i) \mathbf{1}_S(j)}{\text{card}(S)}$$

vérifie les contraintes ci-dessus.

- ▶ De plus $\sum_{i,j} B_{i,j} = \text{card}(S)$.
- ▶ Donc $\text{card}(S) \leq \vartheta(G)$.

Programmes SDP

► Programme initial:

$$m = \min \left\{ \begin{array}{l} b_1 x_1 + \cdots + b_m x_m : \\ -A_0 + x_1 A_1 + \cdots + x_m A_m \succeq 0 \end{array} \right\}$$

où A_i sont des matrices symétriques $r \times r$.

► Programme dual:

$$m^* = \max \left\{ \begin{array}{l} \text{Trace}(A_0 Z) : \\ Z \succeq 0, \quad \text{Trace}(A_i Z) = b_i, \quad i = 1, \dots, m \end{array} \right\}$$

- Les programmes linéaire (LP) correspondent au cas de matrices A_i diagonales.
- En général, $m \geq m^*$. Sous certaines conditions, $m = m^*$.
- Dans ce cas, les méthodes dites des points intérieurs donnent des algorithmes permettant d'approximer m avec une précision arbitraire, en complexité polynomiale.

ϑ de Lovász

Programmes initiaux et duaux pour $\vartheta(G)$:



$$\vartheta'(G) = \max \left\{ \sum_{i,j} B_{i,j} : \begin{array}{l} B \succeq 0, \quad \mathbf{B} \geq 0 \\ \sum_i B_{i,i} = 1, \\ B_{i,j} = 0 \quad (i,j) \in E \end{array} \right\}$$



$$\vartheta'(G) = \min \left\{ t : \begin{array}{l} B \succeq 0 \\ B_{i,i} \leq t - 1, \\ B_{i,j} \leq -1 \quad (i,j) \notin E \end{array} \right\}$$

Graphes et codes

- ▶ X fini. Les codes de distance minimale au moins d sont les stables d'un graphe et réciproquement:
 - ▶ $G = (V, E)$ avec $V = X$ et $E = \{(x, y) : d(x, y) < d\}$.
 - ▶ À $G = (V, E)$ on associe la distance du plus court chemin entre deux sommets. Stable de G = code de dist. min. au moins d .
- ▶ $X = \mathbb{F}_2^n$: le nombre de sommets est **exponentiel en n** . donc aussi la complexité du calcul de ϑ !
- ▶ La **méthode de programmation linéaire de Delsarte** (1973) permet de borner le cardinal d'un code de distance minimale donnée en temps polynomial.
- ▶ Mc Eliece, Rodemich, Rumsey et indépendamment Schrijver ont montré que la borne de Delsarte est exactement ϑ' . L'action du **groupe des symétries** de l'espace de Hamming est l'ingrédient qui améliore la complexité.

Généralisations du ϑ de Lovász

- ▶ But: traiter les espaces (X, d) infinis.
- ▶ **Grphe métrique:** $D \subset \mathcal{D} := \{d(x, y), x \neq y\}$. Le graphe métrique $G = G(V, D)$ est le graphe de sommets $V = X$ et d'arêtes

$$E = \{(x, y) \in V^2 : d(x, y) \in D\}.$$

- ▶ Exemple typique: $V = S^{n-1}$ et $D =]0, \delta[$ ou $D = \{\delta\}$.
- ▶ Hypothèse supplémentaire: **(X, d) est compact.**

Généralisations du ϑ de Lovász

- ▶ On remplace les matrices $B = (B_{i,j})$ indexées par $V = \{1, \dots, n\}$, par les **fonctions continues symétriques** $K : V^2 \rightarrow \mathbb{R}$.
- ▶ $K \in \mathcal{C}(V^2)$ est **semi-définie positive** ($K \succeq 0$) si, pour tout n , $(x_1, \dots, x_n) \in V^n$, et $(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$, $\sum_{i,j} \alpha_i \alpha_j K(x_i, x_j) \geq 0$.



$$\vartheta_2 = \sup \left\{ \int \int_{V^2} K(x, y) d\mu(x) d\mu(y) : K \in \mathcal{C}(V^2), K \succeq 0, K \geq 0 \right. \\ \left. \int_V K(x, x) d\mu(x) = 1 \right. \\ \left. K(x, y) = 0 \quad d(x, y) \in D \right\}$$



$$\vartheta_1 = \inf \left\{ t : K \in \mathcal{C}(V^2), K \succeq 0 \right. \\ \left. K(x, x) \leq t - 1, \right. \\ \left. K(x, y) \leq -1 \quad d(x, y) \notin D \right\}$$

Bornes pour les stables mesurables

- ▶ $\mathcal{C}(V)^* = \mathcal{M}(V)$ l'espace des mesures de Borel régulières sur V .
- ▶ En général $\vartheta_1^* \neq \vartheta_2$.
- ▶ On dit que D est **isolé de 0** si $0 \notin \overline{D}$, ou encore $D \subset [\epsilon, +\infty[$ pour un $\epsilon > 0$.
- ▶ $D^c := \{d(x, y) : x \neq y, d(x, y) \notin D\}$.
- ▶ Exemple: $V = S^{n-1}$, $D =]0, \delta[$: D^c est isolé de 0; $D = \{\delta\}$ est isolé de 0.

Théorème

Soit C un stable mesurable de $G(V, D)$.

- ▶ Si D^c est isolé de 0,

$$\text{card}(C) \leq \vartheta_1(V, D) = \vartheta_1^*(V, D)$$

- ▶ Si D est isolé de 0,

$$\mu(C) \leq \vartheta_2(V, D) = \vartheta_2^*(V, D)$$

Symétrisation

- ▶ Un **groupe compact** Γ agit sur V continument, laissant d et μ invariants.
- ▶ Les programmes ϑ_i sont Γ -invariants. Si K est une solution réalisable, \bar{K} aussi, avec

$$\bar{K}(x, y) = \frac{1}{\text{vol}(\Gamma)} \int_{\Gamma} K(\gamma(x), \gamma(y)) d\gamma$$

et on peut remplacer le programme par **son symétrisé**.

- ▶ Bochner a caractérisé les **noyaux continus positifs Γ -invariants**: si la décomposition de $\mathcal{C}(V)$ en sous-espaces Γ -irréductibles est

$$\mathcal{C}(V) \simeq \bigoplus_{k \geq 0} R_k^{m_k}$$

alors on peut associer à chaque $R_k^{m_k}$ une matrice $Z_k(x, y)$ de taille m_k , telle que

$$K \succeq 0 \text{ ssi } K(x, y) = \sum_{k \geq 0} \langle F_k, Z_k(x, y) \rangle \text{ avec } F_k \succeq 0.$$

La sphère S^{n-1}

- ▶ $\Gamma = O(\mathbb{R}^n)$ est **2-points homogène** sur S^{n-1} .

$$\mathcal{C}(S^{n-1}) \simeq_{O(\mathbb{R}^n)} \bigoplus_{k \geq 0} \text{Harm}_k$$

- ▶ $m_k = 1$ and $Z_k(x, y) = P_k^n(x \cdot y)$ où $P_k^n(u)$ sont les polynômes de Gegenbauer de paramètre $n/2 - 1$.

$$P_k^n \in \mathbb{R}[u], \deg(P_k^n) = k, P_k^n(1) = 1$$

$$\int_{-1}^1 P_k^n(u) P_l^n(u) (1 - u^2)^{n/2-1} du = 0, k \neq l$$

- ▶ $K \succeq 0$ ssi $K(x, y) = \sum_{k \geq 0} f_k P_k^n(x \cdot y)$ avec $f_k \geq 0$ pour tout $k \geq 0$.

La sphère S^{n-1}

Cas $D =]0, \delta[$ avec $\delta = \arccos(t)$. Un stable est un code sphérique C avec $x \cdot y \leq t$. On obtient:

$$\text{card}(C) \leq \vartheta_1 = \inf \left\{ 1 + \sum_{k \geq 0} f_k : \begin{array}{l} f_k \geq 0 \\ \sum_{k \geq 0} f_k P_k^n(u) \leq -1 \quad -1 \leq u \leq t \end{array} \right\}$$

- ▶ On retrouve la borne de programmation linéaire de Delsarte (Delsarte, Goethals, Seidel 1977).
- ▶ **Kissing number**: borne exacte pour $n = 8, 24$, et bornes de Odlysko-Sloane.
- ▶ On ne sait pas résoudre analytiquement ϑ_1 mais donner d'excellentes solutions réalisables (Levenshtein) et une asymptotique (Kabatskii-Levenshtein).

Autres espaces

- ▶ Tous les espaces compacts 2-points homogènes conduisent à un LP faisant intervenir une famille de polynômes orthogonaux à une variable (70-80, Delsarte, Seidel, Kabatianskii, Levenshtein,..).
- ▶ Les espaces symétriques: LP, polynômes orthogonaux multivariés ($\mathcal{G}_{m,n}$ (B. 2006), $U_n(\mathbb{C})$ (Creignou, Diet 2008), codes de permutations (Tarnanen), codes ordonnés (Barg),..).
- ▶ D'autres cas conduisent à des SDP. Exemple: une calotte sphérique (B. Vallentin 2007).

La sphère S^{n-1}

[B. F.M. de Oliveira Filho, G. Nebe, F. Vallentin (2007)].

Cas $D = \{\delta\}$, $\delta = \arccos t$. On note $G(S^{n-1}, D) = G(n, t)$. Le programme ϑ_2 se résout en toute généralité.

Théorème

- ▶ Soit $m(t)$ le minimum de $P_k^n(t)$ pour $k = 0, 1, 2, \dots$.

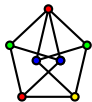
$$\vartheta_2 = \omega_n \frac{m(t)}{m(t) - 1}.$$

- ▶ Soit $\chi_m(G(n, t))$ le **nombre chromatique mesurable** de $G(n, t)$.

$$\chi_m(G(n, t)) \geq \frac{\omega_n}{\vartheta_2} = \frac{m(t) - 1}{m(t)}.$$

$\chi_m(\mathbb{R}^n)$

- ▶ $\chi(\mathbb{R}^n) = \chi(\mathbf{G}(\mathbb{R}^n, \{1\}))$.
- ▶ $4 \leq \chi(\mathbb{R}^2) \leq 7$



- ▶ $\chi_m(\mathbb{R}^n) \geq 5$ (Falconer 1981).
- ▶ $\chi_m(\mathbb{R}^n) \geq \chi_m(\mathbf{G}(n, t))$ pour tout t . Avec $t \rightarrow 1$,

Théorème

$$\chi_m(\mathbb{R}^n) \geq 1 + \frac{(j_{\alpha+1})^\alpha}{2^\alpha \Gamma(\alpha+1) |J_\alpha(j_{\alpha+1})|} \approx_{+\infty} (1.165)^n$$

avec $\alpha = (n-3)/2$, $J_\alpha(u)$ est la fonction de Bessel première espèce et j_α son premier zéro positif.

Hiérarchies de ϑ

- ▶ A. Schrijver 2005: améliore les bornes LP pour les codes binaires en utilisant un programme SDP.
- ▶ Plus généralement des hiérarchies de SDP ont été développées afin d'approcher le nombre de stabilité d'un graphe fini:

$$\alpha(\mathbf{G}) \leq \dots \leq \vartheta^{(r)} \leq \dots \leq \vartheta^{(1)} = \vartheta$$

(Lovász-Schrijver, Lasserre, M. Laurent, etc..)

- ▶ Idée: étendre cette approche aux graphes infinis (travail commun avec F. Vallentin).

Hiérarchies de ϑ

- ▶ Idée de la première étape: soit S un stable.

$$K(i, j, k) := \frac{\mathbf{1}_S(i) \mathbf{1}_S(j) \mathbf{1}_S(k)}{\text{card}(S)}$$

Construire un programme SDP avec ses propriétés semi-définies comme:

K est symétrique

$$(i, j) \rightarrow K(i, j, k) \succeq 0 \text{ and } \succeq 0$$

$$(i, j) \rightarrow K(i, j, j) - K(i, j, k) \succeq 0 \text{ and } \succeq 0$$

$$\sum_{i,j} K(i, j, j) = \text{card}(S)$$

$$K(i, j, k) = 0 \text{ if } (i, j) \in E$$

.....

- ▶ Écrire le programme dual, puis généraliser aux espaces compacts et leurs fonctions continues, puis symétriser...

Meilleures bornes pour τ_n

n	constructions (borne inf)	meilleure borne précédente	borne LP	borne SDP (B. Vallentin 2006)
3	12	12 (Schütte, v.d. Waerden)	13	12
4	24	24 (Musin)	25	24
5	40	46 (Odlyzko, Sloane)	46	45
6	72	82 (O., S.)	82	78
7	126	140 (O., S.)	140	135
8	240	240 (O., S., Levenshtein)	240	240
9	306	379 (Rzhevskii, Vsemirnov)	380	365
10	500	594 (Pfender)	595	557
11	582	915	915	877
12	840	1416	1416	1365
13	1130	2233	2233	2087
14	1582	3492	3492	3215
15	2564		5431	4908
16	4320		8313	7469
17	5346		12218	11382
18	7398		17877	17061
19	10688		25900	25654
20	17400		37974	37850
21	27720		56851	56024
22	49896		86537	84802
23	93150		128095	127191

L'espace euclidien

- ▶ H, Cohn et N. Elkies 2003: borne LP pour la densité des empilements de sphères de \mathbb{R}^n , améliorant les borne précédentes pour $4 \leq n \leq 24$.
- ▶ F.M. de Oliveira Filho et F. Vallentin 2008: borne pour $\chi_m(\mathbb{R}^n)$, améliorant les bornes précédentes pour $n \geq 3$ (même formule avec $n \rightarrow n + 1$..).
- ▶ Les deux approches sont similaires: exploitent la structure de groupe topologique (transformée de Fourier et formule de Poisson) et l'action du groupe orthogonal pour formuler des analogues de ϑ_i .
- ▶ Cas des empilements: difficile de construire de bonnes solutions; cas des nombres chromatiques: se résoud analytiquement.