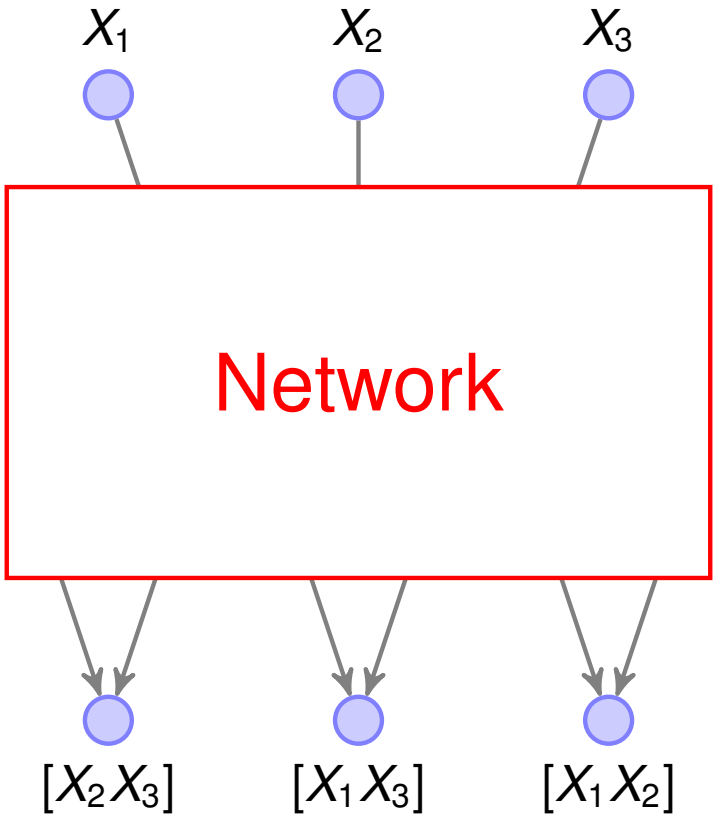
Une introduction au codage de réseau aléatoire
La région Γ_n^* des vecteurs d'entropie

Christine Bachoc

Université Bordeaux I, IMB

École de printemps Codage et Cryptographie
17 - 21 Mars 2014, Université Joseph Fourier, Grenoble

Réseaux multi-sources multi-destinataires



$\mathcal{R}$

C'est la région $\mathcal{R}$ des taux de transmission ω réalisables:

- $G = (V, E)$ acyclique; capacité c_e de chaque arête.
- s sources, t destinataires.
- On demande que t_i reçoive l'information transmise par un certain sous-ensemble σ_i de sources.
- $\mathbf{X} = (X_1, \ldots, X_s)$, X_i variable aléatoire associée à la source s_i, de loi uniforme sur A^{ω_i}, indépendantes.

$\omega = (\omega_1, \ldots, \omega_s)$ est un taux de transmission réalisable s'il existe des fonctions d'encodage $f_e(X)$ pour chaque arête, définies localement, et de décodage D_i aux destinataires, telles que,

$$\text{Prob}\left(D_i\left(f_e(\mathbf{X})\right)_{e\in \text{In}(t_i)}\right) = \left(X_i\right)_{i\in\sigma_i}\Big) \mapsto 1 \quad (|A| \to +\infty)$$

et chaque arête est utilisée au plus c_e fois.

$\mathcal{R}$

Si $\omega = (\omega_1, \ldots, \omega_s)$ est un taux de transmission réalisable, il existe des v.a.

$$Y_s,\ s \in S \quad U_e,\ e \in E$$

vérifiant:

$$H(Y_s) \geq \omega_s \ (s \in S)$$
$$H(Y_S) = \sum_{s \in S} H(Y_s)$$
$$H(U_{\mathrm{Out}(v)} | U_{\mathrm{In}(v)}) = 0 \ (v \in V)$$
$$H(U_e) \leq c_e$$
$$H(Y_{\beta(t)} | U_{\mathrm{In}(t)}) = 0 \ (t \in T).$$

Toutes ces conditions sont linéaires en les entropies des v.a. jointes.

Problème: décrire le lieu des vecteurs d'entropie associés à n v.a. $X_1, \ldots, X_n$:

$$\mathbf{h} = (h_\alpha)_{\alpha \subset [n]}, \quad h_\alpha = H(X_\alpha).$$

Plan

1. Entropie d'une variable aléatoire
2. Vecteur d'entropie associé à n v.a. et région Γ_n^*
3. Inégalités informationnelles, inégalités de base, inégalités de Shannon. Le cône Γ_n.
4. Vecteurs d'entropie et groupes finis.
5. Petites dimensions: $n = 2, 3, 4$.

Entropie d'une variable aléatoire

- Quantité d'information contenue dans un évènement A:

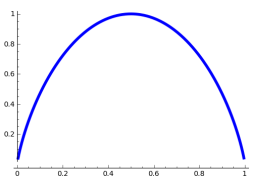
$$-\log(P(A))$$

- Entropie d'une v.a. discrète X = quantité d'information contenue dans X

$$H(X) = -\sum_x P(X = x) \log P(X = x)$$

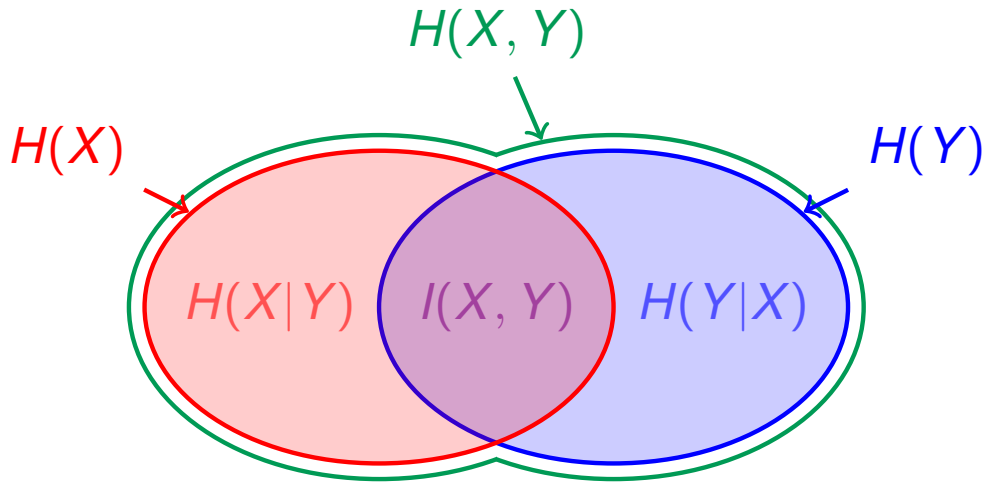
- Exemple: X variable binaire, $P(X = 0) = p$, $P(X = 1) = 1 - p$,

$$H(X) = h(p) := -p \log(p) - (1 - p) \log(1 - p)$$



- Exemple: loi de X uniforme sur m éléments, $H(X) = \log(m)$.

Quantités informationnelles associées à deux v.a.



- Entropie conditionnelle

$$H(X|Y) = H(X,Y) - H(Y) \geq 0$$

- Information mutuelle

$$I(X,Y) = H(X) + H(Y) - H(X,Y) \geq 0$$

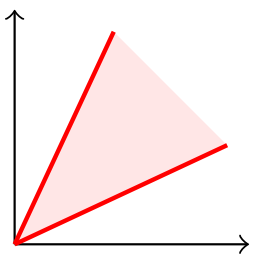
Γ_n^*

- $\mathbf{X} = (X_1, \ldots, X_n)$ v.a. discrètes. Pour $\alpha \subset [n]$, $X_\alpha := (X_i)_{i \in \alpha}$.
- Le vecteur d'entropie associé à $\mathbf{X}$:

$$\mathbf{h} = \mathbf{h}(\mathbf{X}) = (h_\alpha)_{\alpha \neq \emptyset} \in \mathbb{R}^{2^n - 1}$$
$$h_\alpha = H(X_\alpha) \quad \alpha \subset [n], \quad (h_\emptyset = 0).$$

- Soit Γ_n^* l'ensemble de tous les vecteurs $\mathbf{h}$. C'est la région d'entropie.
- Problème: décrire Γ_n^*. Il n'est pas fermé.

Son adhérence $\overline{\Gamma}_n^*$ est un cône convexe.



$\overline{\Gamma}_n^*$ est un cône convexe

- Si $\mathbf{h}, \mathbf{h}' \in \Gamma_n^*$, alors $\mathbf{h} + \mathbf{h}' \in \Gamma_n^*$: si $\mathbf{h}$ correspond à $(X_1, \ldots, X_n)$ et $\mathbf{h}'$ à $(X_1', \ldots, X_n')$, alors $\mathbf{h} + \mathbf{h}'$ est le vecteur d'entropie de $(Y_1, \ldots, Y_n)$ pour $Y_i = (X_i, X_i')$ (copies indépendantes).
- En particulier, si $\mathbf{h} \in \Gamma_n^*$ et $k \in \mathbb{Z}_{\geq 0}$, $k\mathbf{h} \in \Gamma_n^*$.
- Si $\mathbf{h} \in \Gamma_n^*$ et $\ell \in \mathbb{Z}_{\geq 0}$, alors $\mathbf{h}/\ell \in \overline{\Gamma}_n^*$: soit $m \geq 0$ et

U une variable binaire telle que $P(U = 1) = 1/(\ell m)$

$$Y_i = \begin{cases} 0 & \text{si } U = 0 \\ X_i^m & \text{si } U = 1. \end{cases}$$

Alors:

$$H(Y_\alpha|U) \leq H(Y_\alpha) \leq H(Y_\alpha, U) = H(U) + H(Y_\alpha|U)$$

soit

$$\frac{1}{\ell} H(X_\alpha) \leq H(Y_\alpha) \leq h(1/(\ell m)) + \frac{1}{\ell} H(X_\alpha).$$

Le cône Γ_n

- C'est le cône défini par les inégalités de base.
- Exemple: $n = 2$. On a vu:

$$H(X_1, X_2) \geq H(X_1) \geq 0, \quad H(X_1) + H(X_2) - H(X_1, X_2) \geq 0.$$

Donc

$$\begin{aligned}\Gamma_2^* \subset \Gamma_2 := \{(h_1, h_2, h_{12}) \in \mathbb{R}^3 \ : h_1 \geq 0,\ h_2 \geq 0,\\ h_{12} \geq h_1,\ h_{12} \geq h_2\\ h_1 + h_2 - h_{12} \geq 0.\}\end{aligned}$$

- En général, les inégalités de base sont ($H(X_\emptyset) = 0$):

$$\begin{aligned}&H(X_\alpha) \geq H(X_\beta) \geq 0 \text{ si } \beta \subset \alpha\\ &H(X_\alpha) + H(X_\beta) - H(X_{\alpha\cup\beta}) - H(X_{\alpha\cap\beta}) \geq 0.\end{aligned}$$

- Toute inégalité linéaire sur les $H(X_\alpha)$ qui se déduit des inégalités de base s'appelle une inégalité de Shannon. Ce sont donc les combinaisons linéaires à coefs positifs des inégalités de base.
- On définit le cône des inégalités de Shannon:

$$\begin{aligned}\Gamma_n := \{\mathbf{h} = (h_\alpha) \in \mathbb{R}^{2^n-1} \ : & \ h_\alpha \geq 0 \\ & \ h_\alpha - h_\beta \geq 0 \quad (\beta \subset \alpha) \\ & \ h_\alpha + h_\beta - h_{\alpha\cup\beta} - h_{\alpha\cap\beta} \geq 0.\}\end{aligned}$$

- On a vu que:

$$\Gamma_n^* \subset \overline{\Gamma}_n^* \subset \Gamma_n$$

- Un grand nombre de résultats en théorie de l'information peuvent se démontrer par programmation linéaire sur Γ_n.

Exemple: le partage de secrets

On veut partager un secret S en trois morceaux X, Y, Z de sorte que:

1. Aucun des morceaux X, Y ou Z ne fournisse d'information sur S
2. On peut retrouver S à partir de deux parmi les trois.

On veut savoir comment réaliser un tel schéma de façon la plus économique, c'est-à-dire en minimisant les 'tailles' de X, Y, Z relativement à S.

Traduction des contraintes en termes de quantités informationnelles:

1. $I(S, X) = I(S, Y) = I(S, Z) = 0$
2. $H(S|X, Y) = H(S|Y, Z) = H(S|X, Z) = 0$.

On cherche à minimiser

$$(H(X) + H(Y) + H(Z))/H(S).$$

On va chercher s'il y a une limite informationnelle.

Exemple: le partage de secrets

Rappel:

$$I(S,X) = H(S) + H(X) - H(S,X), \quad H(S|X,Y) = H(S,X,Y) - H(X,Y).$$

On résoud le programme linéaire:

$$\begin{aligned} \min\{h_1 + h_2 + h_3 \ : \ & \mathbf{h} \in \Gamma_4 \\ & h_4 = 1 \\ & h_1 + h_4 - h_{14} = 0, \ h_2 + h_4 - h_{24} = 0, \ h_3 + h_4 - h_{34} = 0, \\ & h_{124} - h_{12} = 0, \ h_{234} - h_{23} = 0, \ h_{134} - h_{13} = 0\} \end{aligned}$$

On trouve $\min = 3$ (software ITIP *Information Theoretic Inequality Prover*, Yeung and Yan). Ensuite on se demande si cette valeur est atteinte sur Γ_4^*.

C'est le cas avec: S, N indépendantes uniformément distribuées sur $\{0,1,2\}$ et

$$X = N, \quad Y = S + N \bmod 3, \quad Z = S + 2N \bmod 3.$$

Groupes finis

On va voir une construction qui permet essentiellement de réaliser tout vecteur d'entropie à l'aide de groupes finis et de leurs sous-groupes.

Construction:

- G un groupe et $G_1, \ldots, G_n$ des sous-groupes de G.
- $G/G_i = \{gG_i \ : \ g \in G\}$ les classes à gauche de G modulo G_i.
- G est muni de la loi uniforme. On considère les v.a. X_i:

$$X_i : G \to G/G_i$$
$$g \mapsto gG_i$$

- On note $G_\alpha := \cap_{i \in \alpha} G_i$. Alors

$$H(X_\alpha) = \log \frac{|G|}{|G_\alpha|}.$$

$$H(X_\alpha) = \log \frac{|G|}{|G_\alpha|}.$$

Loi de X_α: soit $g_i G_i \in G/G_i$.

$$\begin{aligned} P(X_\alpha = (g_i G_i)_{i\in\alpha}) &= P(X_i = g_i G_i,\ i \in \alpha) \\ &= P(gG_i = g_i G_i,\ i \in \alpha) \\ &= P(g \in g_i G_i,\ i \in \alpha) \\ &= \frac{|\cap_{i\in\alpha}\, g_i G_i|}{|G|}. \end{aligned}$$

Mais soit $\cap_{i\in\alpha} g_i G_i = \emptyset$, soit $\cap_{i\in\alpha} g_i G_i$ contient un élément $g \in G$, auquel cas $gG_i = g_i G_i$ et

$$|\cap_{i\in\alpha}\, g_i G_i| = |\cap_{i\in\alpha}\, gG_i| = |g\big(\cap_{i\in\alpha}\, G_i\big)| = |gG_\alpha| = |G_\alpha|.$$

On a montré:

$$P(X_\alpha = (g_i G_i)_{i\in\alpha}) = \begin{cases} 0 & \text{si } \cap_{i\in\alpha} g_i G_i = \emptyset \\ \frac{|G_\alpha|}{|G|} & \text{sinon.} \end{cases}$$

Donc la loi de X_α est uniforme sur son support, donc

$$H(X_\alpha) = \log \frac{|G|}{|G_\alpha|}.$$

Résumé: à tout groupe G et tout sous-groupes $(G_1, \ldots, G_n)$ on a associé le vecteur d'entropie $\mathbf{h} = (h_\alpha)_{\alpha\subset[n]} \in \Gamma_n^*$:

$$h_\alpha = \log \frac{|G|}{|G_\alpha|}, \quad G_\alpha = \cap_{i\in\alpha} G_i.$$

On note Υ_n l'ensemble de tous les vecteurs d'entropie obtenus par cette construction. On a donc:

$$\Upsilon_n \subset \Gamma_n^* \subset \overline{\Gamma}_n^* \subset \Gamma_n.$$

Réciproque: Pour tout $h \in \Gamma_n^*$, il existe $(f_k)_{k\geq 0}$, $f_k \in \Upsilon_n$ tels que

$$\lim_{k\to+\infty} \frac{f_k}{k} = h.$$

- Soit $h \in \Gamma_n^*$ associé à $\mathbf{X} = (X_1, \ldots, X_n)$, où X_i prend ses valeurs dans A_i. On note $A_\alpha = \prod_{i\in\alpha} A_i$.
- On suppose que k est tel que $kP(\mathbf{X} = \mathbf{a}) \in \mathbb{Z}_{\geq 0}$ pour tout $\mathbf{a} \in A_{[n]}$.
- Soit $T \in \mathbb{R}^{n\times k}$ le tableau:

$$T = \begin{array}{cccccccc} \mathbf{a}_1 & \ldots & \mathbf{a}_1 & \ldots & \mathbf{a'}_1 & \ldots & \mathbf{a'}_1 \\ \mathbf{a}_2 & \ldots & \mathbf{a}_2 & \ldots & \mathbf{a'}_2 & \ldots & \mathbf{a'}_2 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \mathbf{a}_n & \ldots & \mathbf{a}_n & \ldots & \mathbf{a'}_n & \ldots & \mathbf{a'}_n \\ \underbrace{\qquad\qquad}_{kP(\mathbf{X}=\mathbf{a})} & & & & \underbrace{\qquad\qquad}_{kP(\mathbf{X}=\mathbf{a'})} & & \end{array}$$

- Soit T_α le tableau extrait formée des lignes de T d'indice $i \in \alpha$. Soit

$$G = \mathfrak{S}_k, \text{ permutant les colonnes de } T, \quad G_i = \mathrm{Stab}(T_i)\ (i \in [n]).$$

- On a $G_\alpha = \mathrm{Stab}(T_\alpha)$ est le produit direct de $\mathfrak{S}_{kP(X_\alpha = a_\alpha)}$. Donc

$$\begin{aligned}\frac{1}{k}\log\frac{|G|}{|G_\alpha|} &= \frac{1}{k}\log\frac{k!}{\prod_{a_\alpha \in A_\alpha}(kP(X_\alpha = a_\alpha))!}\\ &\simeq_{k\to+\infty} -\sum_{a_\alpha \in A_\alpha} P(X_\alpha = a_\alpha)\log P(X_\alpha = a_\alpha)\\ &\simeq_{k\to+\infty} H(X_\alpha).\end{aligned}$$

On a montré que, pour $f_k = \left(\log\frac{|G|}{|G_\alpha|}\right)_{\alpha\subset[n]}$,

$$\lim_{k\to+\infty}\frac{f_k}{k} = h.$$

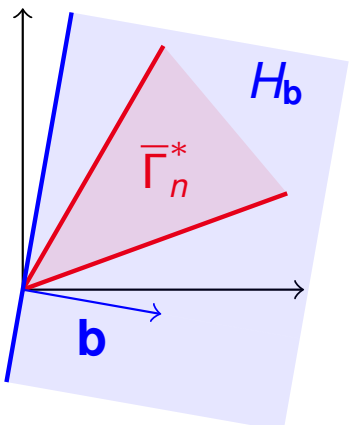
Groupes finis et inégalités informationnelles

Une inégalité informationnelle est une relation

$$\sum_{\alpha \subset [n]} b_\alpha h_\alpha \geq 0$$

vérifiée par tout $\mathbf{h} \in \Gamma_n^*$. On peut l'écrire aussi $\mathbf{b} \cdot \mathbf{h} \geq 0$.

Interprétation géométrique: le cône $\overline{\Gamma}_n^*$ est contenu dans le demi-plan $H_{\mathbf{b}} = \{\mathbf{h} \ : \ \mathbf{b} \cdot \mathbf{h} \geq 0\}$.



D'après ce qui précède,

$$\Gamma_n^* \subset H_{\mathbf{b}} \iff \Upsilon_n \subset H_{\mathbf{b}}.$$

Autrement dit, pour montrer une inégalité du type:

$$\sum_{\alpha \subset [n]} b_\alpha H(X_\alpha) \geq 0,$$

il suffit de montrer que, pour tout groupe fini G et tout sous-groupes $G_1, \ldots, G_n$ de G,

$$\sum_{\alpha \subset [n]} b_\alpha \log \frac{|G|}{|G_\alpha|} \geq 0.$$

Exemple: les inégalités de base

Rappel: ce sont celles qui définissent Γ_n:

$$H(X_\alpha) \geq H(X_\beta) \geq 0 \text{ si } \beta \subset \alpha$$
$$H(X_\alpha) + H(X_\beta) - H(X_{\alpha\cup\beta}) - H(X_{\alpha\cap\beta}) \geq 0.$$

Pour les éléments de Υ_n, elle deviennent:

$$\frac{|G_\alpha|}{|G_\beta|} \leq 1 \text{ si } \beta \subset \alpha \quad \text{et} \quad \frac{|G_\alpha||G_\beta|}{|G_{\alpha\cup\beta}||G_{\alpha\cap\beta}|} \leq 1.$$

La première est immédiate. La deuxième se déduit facilement du résultat bien connu: si H et K sont deux sous-groupes d'un même groupe Γ et si $HK := \{hk : h \in H, k \in K\}$, alors

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

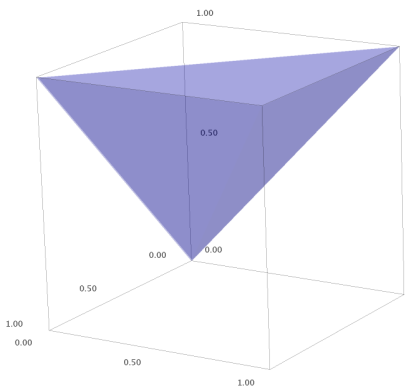
(indication: $H = G_\alpha$, $K = G_\beta$, $H \cap K = G_{\alpha\cup\beta}$, et prendre $\Gamma = G_{\alpha\cap\beta}$).

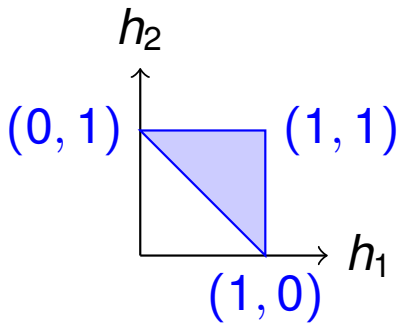
$$\overline{\Gamma}_2^* = \Gamma_2, \overline{\Gamma}_3^* = \Gamma_3,$$

Stratégie pour montrer que $\overline{\Gamma}_n^* = \Gamma_n$: on cherche les sommets du polytope $\Gamma_n \cap \{h_{[n]} = 1\}$ puis on cherche à les réaliser à l'aide de groupes, à un facteur multiplicatif près.

Exemple: $n = 2$:

$$\Gamma_2 = \{(h_1, h_2, h_{12}) \in \mathbb{R}^3 \ : h_1 \geq 0,\ h_2 \geq 0, h_{12} \geq h_1,\ h_{12} \geq h_2,$$
$$h_1 + h_2 - h_{12} \geq 0.\}$$





Notons qu'il suffit de considérer un sommet dans chaque orbite sous l'action du groupe $\mathfrak{S}_n$.

n=2:

sommet	G	G_1	G_2	G_{12}
$(1,0)$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\{0\}$	$\{0\}$
$(1,1)$	$\mathbb{Z}_2$	$\{0\}$	$\{0\}$	$\{0\}$

n=3:

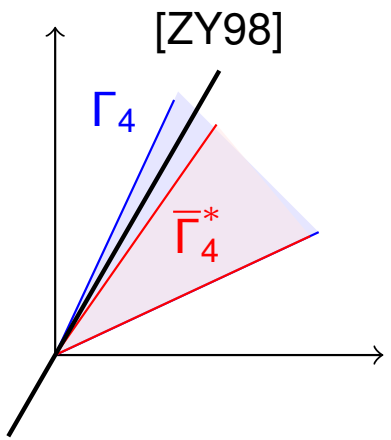
$$\Gamma_3 = \{\ (h_1, h_2, h_3, h_{23}, h_{13}, h_{12}, h_{123}) \in \mathbb{R}^7\ :\ h_{123} \geq h_{12} \geq h_1 \geq 0$$
$$h_1 + h_2 - h_{12} \geq 0$$
$$h_{12} + h_3 - h_{123} \geq 0$$
$$h_{12} + h_{13} - h_{123} - h_1 \geq 0$$
$$\text{et permutations..}\ \}$$

sommet	G	G_1	G_2	G_3
10001011	$\mathbb{Z}_2$	$\{0\}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
0111111	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\{0\}$	$\{0\}$
1111111	$\mathbb{Z}_2$	$\{0\}$	$\{0\}$	$\{0\}$
$\frac{1}{2}\frac{1}{2}\frac{1}{2}1111$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle(1,0)\rangle$	$\langle(0,1)\rangle$	$\langle(1,1)\rangle$

La dimension 4: $\overline{\Gamma}_4^* \neq \Gamma_4$

- Zhang et Yeung (1998): une inégalité entropique 'non Shannon' (ie non impliquée par les inégalités de base):

$$2I(X_3, X_4) \leq I(X_1, X_2) + I(X_1, (X_3, X_4)) + 3I(X_3, X_4|X_1) + I(X_3, X_4|X_2).$$



La dimension 4

- En termes de groupes ($|G_\alpha = \cap_{i\in\alpha} G_i$):

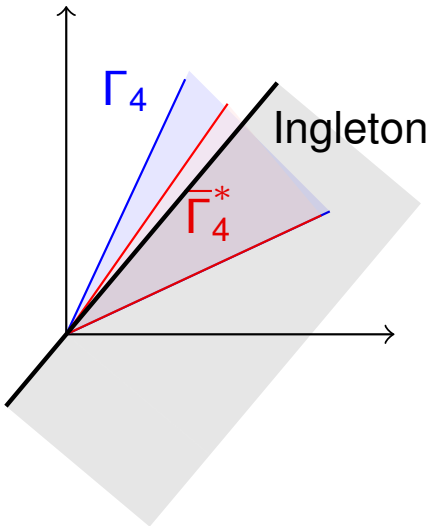
$$|G_{13}|^3|G_{14}|^3|G_{34}|^3|G_{23}||G_{24}| \leq |G_1||G_{12}||G_3|^2|G_4|^2|G_{134}|^4|G_{234}|.$$

- Autres inégalités 'non Shannon': Makarychev et al. (2002), Zhang (2003), Matús (2007), Dougherty et al. (2006).
- Matús (2007) montre que $\overline{\Gamma}_4^*$ n'est pas polyhedral ie ne peut être caractérisé pas un nombre fini d'inégalités.

L'inégalité d'Ingleton

L'inégalité d'Ingleton, vérifiée par le rang d'un matroïde représentable, définit avec Γ_4 un sous-ensemble de $\overline{\Gamma}_4^*$:

$$h_{12} + h_{13} + h_{14} + h_{23} + h_{24} \geq h_{123} + h_{124} + h_{34} + h_1 + h_2.$$



R. W. Yeung, *Information Theory and Network Coding*, Springer, 2008

R. W. Yeung, *Facets of entropy*, 2012 (ISIT plenary talk 2009)

Algebra, Codes and Networks

June 16–20, 2014

Bordeaux Institute of Mathematics

Plenary speakers

Andrew Barron,	Yale
Ronald Cramer,	U. Leiden and CWI
Alexandros Dimakis,	U. Texas at Austin
Michael Gastpar,	EPFL
Swastik Kopparty,	Rutgers
Damien Stehlé,	ENS Lyon
Vinod Vaikuntanathan,	MIT
Mary Wootters,	U. Michigan
Sergey Yekhanin,	Microsoft

The centre of excellence CPU - IdEx Bordeaux together with the COST programme of the European Science Foundation, and the Institut de Mathématiques de Bordeaux, are pleased to announce the conference ACN 2014 from June 16 to June 20 in Bordeaux.

Coding theory has emerged from the need to ensure reliable communication and has since morphed into a multi-purpose tool whose methods borrow from computer science, information theory and mathematics. Coding techniques are very much present in the development of a number of recent applications, such as : network coding, cloud computing and distributed storage, multi-antenna systems of communication, or quantum computing.

This conference will address theory and applications of coding theory, featuring interactions with algebra, theoretical computer science and discrete mathematics. The event has been initiated by COST Action IC1104 and will be particularly welcoming to contributions relevant to its themes.

Scientific committee : Christine Bachoc, Alexander Barg, Marcus Greferath, Frank Kschischang, Madhu Sudan, Gilles Zémor.

`http://acn2014.u-bordeaux.fr/`