Correction du Problème II

Laurent Massoulié

March 29, 2007

1. On utilise la construction suivante des $k|C|$ arêtes issues des sommets $i \in C$. On se donne $k|C|$ variables aléatoires $U_1, \ldots, U_{k|C|}$, i.i.d. et uniformément distribuées sur $[0,1]$. La destination de la $n$ème arête est spécifiée par l'indice $J_n \in \{1, \ldots, M\}$ tel que $U_n \in [(J_n - 1)/M, J_n/M[$. Clairement cette construction produit des arêtes dont les destinations sont i.i.d. et uniformément distribuées sur V_2.

   On note D_n l'ensemble $\{J_1, \ldots, J_{n-1}\}$, et Z_n la v.a. qui vaut 1 si la destination J_n appartient à D_n, et vaut zéro sinon. Donc la taille de l'ensemble $\Gamma(C)$ s'écrit:

$$|\Gamma(C)| = k|C| - \sum_{n=1}^{k|C|} Z_n.$$

   Pour chaque sous-ensemble D de $\{1, \ldots, M\}$ de taille inférieure ou égale à $k|C|$, on se donne un sous-ensemble $F(D)$ tel que $D \subseteq F(D)$ et $|F(D)| = k|C|$. Pour tout $n = 1, \ldots, k|C|$, on définit la v.a. Z'_n par:

$$Z'_n = \begin{cases} 1 \text{ si } J_n \in F(D_n), \\ 0 \text{ sinon.} \end{cases}$$

   Clairement, $Z'_n \geq Z_n$. Par ailleurs, pour tous $z_1, \ldots, z_n \in \{0,1\}$, on vérifie aisément par récurrence sur n que:

$$\mathbf{P}(Z'_1 = z_1, \ldots, Z'_n = z_n) = \prod_{i=1}^{n} \left(\frac{k|C|}{M}\right)^{z_i} \left(1 - \frac{k|C|}{M}\right)^{1-z_i}.$$

   Ceci établit que $k|C| - \sum_{i=1}^{k|C|} Z'_n$ est une v.a. Binomiale, de paramètres $k|C|$ et $1 - k|C|/M$. Le résultat annoncé découle alors de l'inégalité

$$|\Gamma(C)| = k|C| - \sum_{n=1}^{k|C|} Z_n \geq k|C| - \sum_{n=1}^{k|C|} Z'_n.$$

2. D'après la définition d'un graphe $(\epsilon, (1-\delta)k)$-expansif, on a l'égalité

$$1 - \pi = \mathbf{P}(\exists C \subset V_1 : |C| \leq \epsilon N \text{ et } |\Gamma(C)| < k(1-\delta)|C|).$$

   En majorant la probabilité d'une union par la somme des probabilités, et en notant que la probabilité qu'un ensemble C soit tel que $|\Gamma(C)| < k(1-\delta)|C|$ ne dépend que de la taille $|C|$ de cet ensemble dans le modèle de graphe aléatoire considéré ici, on obtient:

$$1 - \pi \leq \sum_{a=1}^{\epsilon N} \binom{N}{a} \mathbf{P}(|\Gamma(C_a)| \leq k(1-\delta)a),$$

où $C_a = \{1, \dots, a\}$. D'après le résultat de la première question, la probabilité dans cette somme est majorée par

$$\mathbf{P}(\mathrm{Bin}(ka, ka/M) \geq k\delta a).$$

On peut remplacer le terme $k\delta a$ par $\lceil k\delta a \rceil$ dans cette expression puisqu'une variable binomiale est à valeurs entières. En représentant une telle v.a. binomiale comme la somme de v.a. Z'_n i.i.d, à valeurs dans $\{0,1\}$, et de moyenne ka/M, la probabilité ci-dessus s'écrit encore:

$$\mathbf{P}(\mathrm{Bin}(ka, ka/M) \geq k\delta a) = \mathbf{P}(\exists 1 < n(1) < \cdots < n(\lceil k\delta a \rceil) \leq ka : Z'_{n(i)} = 1, i = 1, \dots \lceil k\delta a \rceil).$$

En majorant à nouveau la probabilité de l'union par la somme des probabilités, on obtient la borne supérieure $\binom{ka}{\lceil k\delta a \rceil}(ka/M)^{\lceil k\delta a \rceil}$, ce qui implique le résultat recherché.

3. Il est facile d'établir que le terme binomial $\binom{u}{v}$ est majoré par $u^v/v!$. Une version raffinée de la formule de Stirling donne

$$v! = \left(\frac{v}{e}\right)^v \sqrt{2\pi v} e^{\alpha(v)}$$

où $\alpha(v) \in [1/(12v+1), 1/(12v)]$. La majoration de $\binom{u}{v}$ par $(ue/v)^v$ peut s'en déduire. On a donc, par des simplifications élémentaires, et en remplaçant M par αN:

$$\begin{aligned} &\tbinom{N}{a}\tbinom{ka}{\lceil k\delta a \rceil}\left(\tfrac{ka}{M}\right)^{\lceil k\delta a \rceil} \leq \\ &\leq \left(\tfrac{Ne}{a}\right)^a \left(\tfrac{kae}{ka\delta}\right)^{k\delta a+1} \left(\tfrac{ka}{M}\right)^{k\delta a} \\ &\leq \left[\left(\tfrac{a}{N}\right)^{k\delta - 1} B\right]^a \end{aligned}$$

où la constante B vaut

$$B = \left(\frac{k}{\alpha}\right)^{k\delta} \left(\frac{e}{\delta}\right)^{k\delta+1}.$$

Il reste à établir que, pour tout $\delta > 0$ tel que $k\delta > 1$, il existe un $\epsilon > 0$ tel que la somme

$$S := \sum_{a=1}^{\epsilon N} \left[\left(\frac{a}{N}\right)^{k\delta-1} B\right]^a$$

tend vers 0 lorsque N tend vers l'infini. On choisit $\epsilon > 0$ tel que $\epsilon^{k\delta-1}B < 1/2$. On sépare ensuite S en deux sommes S_1 et S_2 selon que $a \leq N_1$ ou $a > N_1$, pour un terme N_1 à déterminer.

On a:

$$S_1 \leq N_1 B \left(N_1/N\right)^{k\delta-1}$$

et

$$S_2 \leq \sum_{a=N_1+1}^{\epsilon N} \left[\epsilon^{k\delta-1}B\right]^a \leq 2^{-N_1}.$$

Il suffit maintenant de choisir N_1 tendant vers l'infini lorsque N tend vers l'infini, suffisamment lentement pour que la borne sur S_1 précédemment établie tende vers 0. Par exemple, $N_1 = \log(N)$ convient.

4. On note p la probabilité qu'un noeud arbitraire de V_1 soit connecté à un noeud de V_2 par plusieurs arêtes. La probabilité de ne pas avoir d'arêtes multiples vaut alors p^N. Un simple argument combinatoire permet d'établir que

$$p = \frac{M(M-1)\cdots(M-k+1)}{M^k} = \prod_{i=1}^{k-1}(1-\frac{i}{M}).$$

On a donc:

$$\begin{aligned}
\mathbf{P}(\text{pas d'arêtes multiples}) &= \left[\prod_{i=1}^{k-1}(1-\tfrac{i}{M})\right]^N \\
&= \left[1-\sum_{i=1}^{k-1}\tfrac{i}{\alpha N}+O(1/N^2)\right]^N \\
&= \exp\left(-\sum_{i=1}^{k-1} i/\alpha + O(1/N)\right) \\
&= \exp(-k(k-1)/(2\alpha)) + O(1/N).
\end{aligned}$$

En combinant ce résultat et le résultat précédent, il vient

$$\mathbf{P}(g_{N,M,k} \text{ sans arêtes multiples et } (\epsilon, k(1-\delta))\text{-expansif}) = \exp(-(k(k-1)/(2\alpha)) - o(1).$$

Ceci garantit, pour $k > 1$ et $\delta > 0$ tel que $\delta k > 1$, l'existence de graphes bi-partites qui sont $(\epsilon, (1-\delta)k)$-expansifs, dont tous les sommets de V_1 ont un degré k, et qui n'ont pas d'arêtes multiples.

5. Supposons qu'il existe deux mots codes x et y dont la distance de Hamming est inférieure strictement à ϵN. Alors, comme les mots codes constituent un espace vectoriel, le vecteur nul est à distance de Hamming strictement inférieure à ϵN du mot code $z := y - x$. On cherche à établir une contradiction.

   Soit C l'ensemble des indices $i \in V_1$ tels que $z_i = 1$. Par hypothèse, C est non vide, et de taille inférieure à ϵN. Comme le graphe est $(\epsilon, (1-\delta)k)$-expansif, nécessairement $|\Gamma(C)| \geq (1-\delta)k|C|$. Pour que z soit un mot code valide, il faut que chaque noeud de $\Gamma(C)$ soit incident à un nombre pair d'arêtes, donc au moins deux arêtes. Notant $d(v)$ le degré d'un noeud $v \in V_2$, on a:

$$\sum_{v\in\Gamma(C)} d(v) \geq 2|\Gamma(C)| \geq 2k(1-\delta)|C|$$

   d'après l'expansivité. Par ailleurs, $\sum_{v\in\Gamma(C)} = k|C|$. On arrive ainsi à la contradiction recherchée: $1 > 2(1-\delta)$ est impossible si $\delta < 1/2$.