TD4

Exercices $\star$: à préparer avant le TD, seront corrigés au début de la séance.

Exercice 1 : $\star$
1) Soit $G = X \sqcup Y$ un graphe fini biparti possédant $\delta|X||Y|$ arêtes. Démontrer l'existence d'une partie X' de X de cardinal $\geq \delta|X|$ telle que deux éléments quelconques de X' sont reliés par un chemin de longueur 2 dans G. Démontrer que la borne $\delta|X|$ ne peut être remplacée par $\delta|X|+1$, même pour $|X|$ et $|Y|$ suffisamment grands.
2) On suppose que $|X| = |Y| = N$ et que $\delta \leq \frac{1}{2}$. Démontrer l'existence de parties X' et Y' de X et Y, possédant chacune au moins $\frac{1}{2}\log(\frac{1}{\delta})^{-1}\log(N) - 1$ éléments telles que tout élément de X' est connecté à chaque élément de Y' par une arête de G.

Exercice 2 (Le *Nullstellensatz* combinatoire, et applications)
1) Soit $P \in k[X_1, \ldots, X_n]$ un polynôme de degré $d = d_1 + \cdots + d_n$ à coefficients dans un corps k, et soient $S_1, \ldots, S_n$ des parties de k telles que $|S_i| > d_i$. Démontrer que si P s'annule sur $S_1 \times \cdots \times S_n$, alors le coefficient de $X_1^{d_1} \ldots X_n^{d_n}$ dans P est nul. On pourra procéder par récurrence sur n.
2) Soit p un nombre premier et A, B des parties de $\mathbb{Z}/p\mathbb{Z}$. Démontrer l'inégalité

$$|A+B| \geq \min(|A|+|B|-1, p),$$

en appliquant la question 1 au polynôme $P(X_1, X_2) = \prod_{c \in A+B}(X_1 + X_2 - c)$.
3) Soit p un nombre premier et A, B des parties de $\mathbb{Z}/p\mathbb{Z}$. Démontrer l'inégalité

$$|\{a+b \mid a \in A, b \in B, a \neq b\}| \geq \min(|A|+|B|-3, p).$$

Exercice 3
Soit A un ensemble fini et soit k un corps. Le *rang* $r(f)$ d'une application $f : A^n \to k$ est le plus petit entier r tel que f s'écrit comme la somme de r fonctions de la forme $(x_1, \ldots, x_n) \mapsto g(x_i)h((x_j)_{j \neq i})$, pour un certain i entre 1 et n.
1) Soit $f : A^n \to k$ une fonction telle que $f(a_1, \ldots, a_n) = 0$ lorsque les a_i ne sont pas tous égaux. Démontrer que le rang de f est égal au nombre de $a \in A$ tels que $f(a, \ldots, a) \neq 0$. On pourra procéder par récurrence sur n.
2) On suppose que $k = \mathbb{Z}/p\mathbb{Z}$. Soit a, b, c des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ tels que $a+b+c = 0$, et soit A une partie de $(\mathbb{Z}/p\mathbb{Z})^d$ telle que

$$\forall (x,y,z) \in A^3,\ (ax+by+cz=0) \implies (x=y=z).$$

Démontrer que la fonction $f : (x,y,z) \in A^3 \mapsto 1_{ax+by+cz=0}$ est de rang au plus

$$3|\{r \in [|0, p-1|]^d \mid \sum_{i=1}^{d} r_i \leq \frac{d}{3}(p-1)\}|.$$

3) En déduire l'existence d'une constante $c_p < p$ ne dépendant que de p, telle que $|A| \leq 3c_p^d$.
4) Essayer de traiter similairement le cas du système d'équations $x - 2y + z = 0, y - 2z + w = 0$ en quatre variables, qui détecte les progressions arithmétiques de longueur 4. Pourquoi n'obtient on rien ?

Exercice 4 (Le *lemme de Schwartz-Zippel*, et applications)
Soit k un corps. Si $P \in k[X_1, \dots, X_n]$ est un polynôme à coefficients dans k, et si x est un élément de k^n, on appelle *multiplicité de P en x* et on note $\mu(P, x)$ le plus grand entier μ tel que le polynôme $P(x_1 + X_1, \dots, x_x + X_n)$ n'admet de monôme non nul $cX_1^{r_1} \dots X_n^{r_n}$ avec $r_1 + \dots + r_n < \mu$.
1) Soient $S_1, \dots, S_n$ des parties finies de k, chacune possédant au moins s éléments, et soit $P \in k[X_1, \dots, X_n]$ est un polynôme non nul de degré au plus d. Démontrer l'inégalité de Schwartz-Zippel

$$\sum_{x \in \prod_{i=1}^n S_i} \mu(P, x) \leq \frac{d}{s} \prod_{i=1}^n |S_i|.$$

On suppose dorénavant que k est fini, de cardinal q. On se donne une fonction $f : k^n \to \mathbb{R}_+$.
2) Démontrer que l'on peut trouver une suite $(P_m)_{m \geq 1}$ d'éléments de $k[X_1, \dots, X_n]$ tels que $\mu(P_m, x) \geq mf(x)$ pour chaque $x \in k^n$ et tels que P_m soit non nul, de degré d_m satisfaisant à l'inégalité

$$d_m \leq \left(\left(\sum_{x \in k^n} f(x)^n \right)^{\frac{1}{n}} + o(1) \right) m,$$

lorsque m tend vers l'infini.
3) Soit $H(P_m)$ la partie homogène de plus haut degré de P_m. Démontrer que pour chaque $b \in k^n$ non nul, on a

$$m \max_{a \in k^n} \sum_{t \in k} f(a + tb) \leq d_m + (q - 1)\mu(H(P_m), b).$$

4) En déduire à l'aide de la question 1) l'inégalité

$$\sum_{b \in k^n \setminus \{0\}} \max_{a \in k^n} \sum_{t \in k} f(a + tb) \leq 2(q^n - 1) \left(\sum_{x \in k^n} f(x)^n \right)^{\frac{1}{n}}$$

5) Soit A une partie de k^n telle que pour tout $b \in k^n$ non nul, il existe $a \in k^n$ tel que $a + kb \subseteq A$. Démontrer que l'on a $|A| \geq 2^{-n} q^n$. Cette dernière inégalité est due à Dvir-Kopparty-Saraf-Sudan, améliorant le résultat de Dvir vu en cours, à savoir $|A| \geq n!^{-1} q^n$.

Exercice 5
Soit $\mathcal{L}$ un ensemble de droites affines dans $\mathbb{R}^3$. Un *noeud* de $\mathcal{L}$ est un point de $\mathbb{R}^3$ par lequel passe trois droites non coplanaires appartenant à $\mathcal{L}$. On note $N(\mathcal{L})$ l'ensemble des noeuds de $\mathcal{L}$.
1) Soit $P \in \mathbb{R}[X_1, X_2, X_3]$ un polynôme non nul s'annulant sur $N(\mathcal{L})$, de degré d minimal. Démontrer que l'on a $d \leq 3|N(\mathcal{L})|^{\frac{1}{3}}$.
2) Démontrer qu'il existe une droite $L \in \mathcal{L}$ telle que la restriction $P_{|L}$ ne soit pas identiquement nulle. Démontrer qu'alors L contient au plus $3|N(\mathcal{L})|^{\frac{1}{3}}$ noeuds de $\mathcal{L}$.
3) En déduire l'inégalité de Guth-Katz : $|N(\mathcal{L})| \leq 10|\mathcal{L}|^{\frac{3}{2}}$.
4) Démontrer que l'exposant $\frac{3}{2}$ dans la question précédente est optimal.
5) Généraliser le résultat de la question 3 à une famille de droites affines dans $\mathbb{R}^n$.