Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 5.12 (bis)

Par interpolation polynomiale de Lagrange, pour tout sous-ensemble S de $(\mathbb{Z}/p\mathbb{Z})^*$, il est toujours possible de construire un polynôme f qui satisfait les conditions de l'exercice 5.12 avec $\deg(f) = s - 1$. L'exercice suivant montre que si l'ensemble S est choisi aléatoirement, alors ce résultat ne peut pas être amélioré (avec forte probabilité).

Soient p un nombre premier impair et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Soient s et k deux entiers avec $0 < k < s$. Étant donné un polynôme $f(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ de degré $s - k$ et un ensemble à s éléments $S \subset (\mathbb{Z}/p\mathbb{Z})^*$, nous dirons que le polynôme f *interpole* l'ensemble S si $f(g^x) \equiv x \bmod p$ pour tout $x \in (\mathbb{Z}/(p-1)\mathbb{Z})$ tel que $g^x \in S$. L'ensemble *interpolé par un polynôme* f est l'ensemble maximal pour l'inclusion que f interpole. Nous notons $P_k(p, s)$ la probabilité qu'un ensemble aléatoire à s éléments $S \subset (\mathbb{Z}/p\mathbb{Z})^*$ soit interpolé par un polynôme $f(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ de degré strictement inférieur à $s - k$ Le but de l'exercice suivant est de montrer que cette probabilité décroit exponentiellement avec k.

Exercice 5.12 (bis) INTERPOLATION POLYNOMIALE DE LOGARITHME DISCRET

Soient p un nombre premier impair et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Soient s et k deux entiers avec $0 < k < s$.

1. Soient $S_1, \ldots, S_N$ les différents ensembles de cardinaux respectifs $s_1, \ldots, s_N$ interpolés par des polynômes de degré $n < s - k$. Montrer que

$$\sum_{i=1}^{N} \binom{s_i}{n+1} \leq \binom{p-1}{n+1}.$$

2. Posons $n = s - k - 1$. Montrer que

$$P_k(p, s) = \binom{p-1}{n+1}^{-1} \binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \binom{s_i}{n+1} \binom{s_i - n + 1}{k}.$$

3. Montrer que

$$\binom{u}{v}^{-1} \binom{w}{v} \leq \left(\frac{w}{u}\right)^v,$$

pour des entiers $u, v, w \geq 1$ avec $w \leq u$. En déduire, en utilisant l'exercice précédent, que

$$P_k(p, s) \leq \left(\frac{2s}{p-2}\right)^{k/2}.$$

Solution :

1. Considérons les N ensembles $S_i \subseteq \{1,\dots,p-1\}$ pour $i \in \{1,\dots,N\}$ interpolés par des polynômes f_i de degré $n \leq s-k-1$. Si les ensembles S_i pour $i \in \{1,\dots,N\}$ sont distincts, par maximalité des S_i, les polynômes f_i sont également deux à deux distincts.

   Pour $i,j \in \{1,\dots,N\}$ avec $i \neq j$, le polynôme (non nul) $f_i - f_j$ de degré au plus n s'annule sur l'ensemble $S_i \cap S_j$ et nous avons
   $$\#S_i \cap S_j \leq n.$$

   Par conséquent, chaque sous-ensemble de $(\mathbb{Z}/p\mathbb{Z})^*$ à $(n+1)$ éléments est contenu dans au plus un ensemble S_i avec $i \in \{1,\dots,N\}$ et nous obtenons
   $$\sum_{i=1}^{N} \binom{s_i}{n+1} = \sum_{i=1}^{N} \sum_{T \subset S_i, \#T=n+1} 1 \leq \sum_{T \subset \{1,\dots,p-1\}, \#T=n+1} 1 = \binom{p-1}{n+1}.$$

2. Nous avons $s = n+1+k$. Chaque ensemble à s éléments S est union d'un ensemble T de $(n+1)$ éléments et de k éléments en dehors de T. Pour chaque ensemble à $(n+1)$ éléments T, il y a exactement $\binom{p-n-2}{k}$ tels ensembles S.

   Pour tout sous-ensemble T de $\{1,\dots,p-1\}$ à $(n+1)$ éléments, nous notons f_T l'unique polynôme de degré au plus n tel que f_T interpole T et R_T l'ensemble (maximal) effectivement interpolé par f_T. Chaque ensemble S est interpolé par f_T seulement si $S \subset R_T$. Nous avons donc
   $$\begin{aligned} P_k(p,s) &= \sum_{\#T=n+1} \binom{p-1}{n+1}^{-1} \sum_{T \subset S \subset R_T, \#S=s} \binom{p-n-2}{k}^{-1} \\ &= \binom{p-1}{n+1}^{-1} \binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \sum_{T \subset S_i, \#T=n+1} \sum_{T \subset S \subset S_i, \#S=s} 1 \\ &= \binom{p-1}{n+1}^{-1} \binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \binom{s_i}{n+1} \binom{s_i-n+1}{k} \end{aligned}$$

3. Nous avons
   $$\binom{u}{v}^{-1} \binom{w}{v} = \frac{v!(u-v)!}{u!} \frac{w!}{(w-v)!v!} = \frac{w(w-1)\dots(w-v+1)}{u(u-1)\dots(u-v+1)} \leq \left(\frac{w}{u}\right)^v.$$

   Nous avons donc
   $$\binom{p-n-2}{k}^{-1} \binom{s_i-n+1}{k} \leq \left(\frac{s_i-n-1}{p-n-2}\right)^k \leq \left(\frac{s_i-1}{p-2}\right)^k.$$

   D'après l'exercice précédent, nous avons
   $$s_i \leq (2n(p-2))^{1/2} \text{ pour tout } i \in \{1,\dots,N\}$$
   et donc
   $$\binom{p-n-2}{k}^{-1} \binom{s_i-n+1}{k} \leq \left(\frac{2n}{p-2}\right)^{k/2} \leq \left(\frac{2s}{p-2}\right)^{k/2}$$
   et en combinant les questions 1 et 2, nous obtenons le résultat. □