# Opérations modulo un ensemble triangulaire en un temps quasi linéaire.

Soient $\mathbb{F}$ un corps parfait, et $\mathbf{Y} = Y_1, \ldots, Y_n$ des indeterminées sur $\mathbb{F}$. Un ensemble triangulaire (unitaire) $\mathbf{T} = (T_1, \ldots, T_n)$ est une famille de polynômes de $\mathbb{F}[\mathbf{Y}]$ telle que pour tout $i$, $T_i \in \mathbb{F}[Y_1, \ldots, Y_i]$ est unitaire et réduit modulo $\langle T_1, \ldots, T_{i-1}\rangle$. Le *degré* de $\mathbf{T}$ est le produit $\deg(T_1, Y_1) \cdots \deg(T_n, Y_n)$. Ces objets permettent de résoudre de nombreux problèmes pour les systèmes d'équaions polynomiales.

Cet exposé, s'intéresse à la complexité de diverses opérations modulo un ensemble triangulaire : la multiplication, l'inversion (quand celà est possible), calculer la norme de $A \in \mathbb{F}[\mathbf{Y}]/\langle T\rangle$, le problème de composition modulaire (calculer $F(G_1(\mathbf{Y}), \cdots, G_m(Y)) \mod \langle T\rangle$) et le problème transposé de projection des puissances, et enfin le problème de changement d'ordre.

Nous décrirons pour ces problèmes des algorithmes ayant une complexité binaire quasi-linéaire en la taille du problème, ce qui améliore les algorithmes existants quand le nombre de variable $s$ n'est pas borné par une constante.

Enfin, si le temps le permet, nous illustrerons une application de ces algorithmes dans le cas du problème de comptage de points des courbes elliptiques.