# Codes correcteurs d'erreurs avec les polynômes tordus

Felix Ulmer
IRMAR, Université de Rennes 1

Avec un automorphisme $\theta$ non trivial de $\mathbb{F}_q$ on définit via la règle $Xa = \theta(a)X$ (avec $a \in \mathbb{F}_q$) une structure d'anneau non commutatif sur

$$\mathbb{F}_q[X,\theta] = \left\{a_n X^{n-1} + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ et } n \in \mathbb{N}\right\}$$

qui est étendue à tout $\mathbb{F}_q[X,\theta]$ par associativité et distributivité. Ces anneaux de "polynômes tordus" sont euclidiens à droite et à gauche. Lorsque $f \in \mathbb{F}_q[X,\theta]$ de degré $n$ engendre un idéal, ses facteurs à droite engendrent des idéaux à gauche du quotient $\mathbb{F}_q[X,\theta]/(f)$. L'idéal à gauche $(g)/(f)$ est alors un sous-espace vectoriel de $(\mathbb{F}_q)^n$ et donc un code linéaire défini sur $\mathbb{F}_q$. Comme dans $\mathbb{F}_q[X,\theta]$ la factorisation n'est pas unique on obtient un grand nombre de code linéaire de cette manière, qui en plus sont munis d'une structure d'idéal. Pour $f = X^n - 1$ on obtient ainsi des codes $\theta$-cycliques $\mathcal{C}_\theta$ qui sont caractérisés par la propriété suivante

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}_\theta \quad \Rightarrow \quad (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in \mathcal{C}_\theta.$$

De nouveaux codes ont ainsi été obtenus, dont la distance minimale améliore celle des meilleurs codes connus. Dans une collaboration avec Delphine Boucher nous montrons que le dual d'un code $\theta$-cyclique est encore $\theta$-cyclique et un nouveau code autodual $[38, 19, 11]$ sur $\mathbb{F}_4$ a été obtenu, dont la distance minimale améliore celle des meilleurs codes autoduaux connus. Il est également possible de généraliser la notion de code BCH aux polynômes tordus.