Fonctions puissances parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_p$

Elodie Leducq

Jedlicka, Hernando et McGuire ont démontré que les fonctions de Gold et de Kasami sont les seules fonctions puissances qui sont presque parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_2$. Pour p premier impair, on démontre que les seules fonctions puissances $x \mapsto x^m$ avec $m \equiv 1 \mod p$ qui sont parfaitement non linéaires sur une infinité d'extensions de $\mathbb{F}_p$ sont celles telles que $m = 1 + p^l$, $l \geq 1$. Comme Jedlicka, Hernando et McGuire, on prouve en utilisant le théorème de Bézout que $\frac{(x+1)^{m+1} - x^m - (y+1)^m + y^m}{x-y}$ a un facteur absoluement irréductible.