Dillon's observation and APN functions $f : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$

Hiroaki Taniguchi*

*Department of Education, Yamato University

Abstract

Let $\mathbb{F}_2$ be the binary field and $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ an APN function with $n > 2$. In p 381 of [1], we encounter the following statement: "J. Dillon (private communication) observed that the property of Proposition 161 implies that, for every nonzero $c \in \mathbb{F}_{2^n}$, the equation $F(x)+F(y)+F(z)+F(x+y+z) = c$ must have a solution". This statement means that every APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ must satisfy the condition $\{f(x+y+z)+f(x)+f(y)+f(z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^n$. After the above observation, we will call the Dillon's observation is satisfied for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if we have $\{f(x+y+z)+f(x)+f(y)+f(z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$.

In this talk, we firstly note the following simple expression for the Dillon's observation.

Corollary 1. For an APN function $f : {\mathbb{F}_2}^n \to {\mathbb{F}_2}^m$, the Dillon's observation is satisfied if and only if $\pi \circ f$ are not APN functions for any $\mathbb{F}_2$-linear surjection $\pi : {\mathbb{F}_2}^m \to {\mathbb{F}_2}^{m-1}$.

Next we give examples of APN functions $f : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ $(n \geq 6)$ which satisfy the Dillon's observation $\{f(x+y+z)+f(x)+f(y)+f(z) \mid x, y, z \in \mathbb{F}_2^{n-1}\} = \mathbb{F}_2^n$. These examples are obtained as $f|_{T_0} : T_0 \to K$ with $K := \mathbb{F}_{2^n}$ and $T_0 := \{x \in K \mid Tr(x) = 0\}$ where $Tr : K \to \mathbb{F}_2$ is the absolute trace of K, and $f : K \to K$ are quadratic APN functions and monomial APN functions.

References

[1] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge Univ. Press, Cambridge (2020).