The Differential Spectrum of A Ternary Power Mapping

Yongbo Xia*, Xianglai Zhang and Chunlei Li†

Abstract

Let GF($p^n$) denote the finite field with $p^n$ elements and GF($p^n$)$^*$ = GF($p^n$) \ {0}, where $p$ is a prime. Let $f(x)$ be a mapping from GF($p^n$) to GF($p^n$). Let $N_f(a, b)$ denote the number of solutions $x \in$ GF($p^n$) of $f(x + a) - f(x) = b$, where $a, b \in \mathbb{F}_{p^n}$. Then

$$\Delta_f = \max \{N_f(a, b) \mid a \in \text{GF}(p^n)^*, b \in \text{GF}(p^n)\}$$

is called the differential uniformity of $f(x)$.

When $f(x)$ is a power function, i.e., $f(x) = x^d$ for some positive integer $d$, we have $N_f(a, b) = N_f(1, \frac{b}{a})$ for all $a \neq 0$. Denote by $\omega_i$ the number of output differences $b$ that occur $i$ times, i.e., $\omega_i = |\{b \in \text{GF}(p^n) \mid N_f(1, b) = i\}|$. Then, the differential spectrum of $f(x)$ is defined as the set

$$S = \{\omega_0, \omega_1, \cdots, \omega_k\},$$

where $k = \Delta_f$.

Recently, the differential spectra of several families of power functions over finite fields were computed. Here we consider the ternary power mapping $f(x) = x^d$ over GF($3^n$), where $d = 3^n - 3$. When $n > 1$ is odd, this power mapping was proved to be differentially 2-uniform by Helleseth, Rong and Sandberg in 1999. For even $n$, they showed the differential uniformity $\Delta_f$ of $f(x)$ satisfies $1 \leq \Delta_f \leq 5$ (IEEE Trans. Inf. Theory, vol. 45, no. 2, 1999).

Following their work, for $d = 3^n - 3$, we further investigate the differential uniformity of $x^d$. We show that for even $n > 2$ the power mapping $x^d$ is differentially 4-uniform if $n \equiv 2 \pmod{4}$ and is differentially 5-uniform if $n \equiv 0 \pmod{4}$. When $n = 2$, $x^d$ is differentially 1-uniform. Furthermore, in each case, including case where $n > 1$ is odd, the corresponding differential spectrum of $x^d$ is determined.

The problem of determining the differential spectrum of the power mapping $x^{3^n-3}$ is reduced to that of counting the number of $u \in \text{GF}(3^n) \setminus \text{GF}(3)$ such that the quartic polynomial $g_u(x) = x^4 + x^2 - ux + 1$ has $i$ roots in $\text{GF}(3^n)$, where $i = 0, 1, \cdots, 4$. The key point of our study is that we successfully find the necessary and sufficient condition for $g_u(x)$ having two or four roots in $\text{GF}(3^n)$. Then, we establish an approach to count the corresponding number of $u$, which turns out to be closely related to the cyclotomic numbers over $\text{GF}(3^n)$. In this way, we eventually obtain the differential spectrum of $x^{3^n-3}$. However, our method relies heavily on the characteristic $p = 3$, and it cannot be applied to the general case where $d = p^n - 3$ with $p > 3$ being an odd prime. In order to deal with the general case, we need new technique and this is a future work.

---

*Y. Xia and Y. Zhang are with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China (e-mail: xia@mail.scuec.edu.cn).
†C. Li is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: chunlei.li@uib.no).