SCIENCE CHINA
Information Sciences

• **Supplementary File** •

More permutation polynomials with differential uniformity six

Ziran TU[1], Xiangyong ZENG[2*] & Zhiyong ZHANG[3]

[1]*School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang* 471003*, China;*
[2]*Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan,* 430062*, China;*
[1]*School of Information Engineering, Henan University of Science and Technology, Luoyang* 471003*, China*

Appendix A

Lemma 1. ([1]) For a positive integer n, the quadratic equation $x^2+ax+b=0$ over $\mathbb{F}_{2^n}$ has two roots in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right)=0$.

To obtain a lower bound on the nonlinearity, the following two lemmas about function fields are needed. The readers can find more details in [2].

Lemma 2. (Riemann's Inequality) Suppose that K/F be a function field and $K=F(x,y)$. Then we have the following estimate for the genus g of K/F:

$$g \leqslant ([K:F(x)]-1)\cdot([K:F(y)]-1),$$

where $[K:F(x)]$ and $[K:F(y)]$ are degrees of the field extension of $K/F(x)$ and $K/F(y)$, respectively.

Lemma 3. (Hasse-Weil Bound) Let $\mathtt{C}$ be a projective curve with genus g over a finite field $\mathbb{F}_q$, then the number of rational points on the curve, denoted by $\sharp\mathtt{C}(\mathbb{F}_q)$ satisfies

$$|\sharp\mathtt{C}(F_q)-(q+1)| \leqslant g\cdot 2q^{\frac{1}{2}}.$$

Proof of Theorem 3: From the definition of nonlinearity, it suffices to prove that

$$|W_f(\alpha,\beta)| \leqslant 3\cdot 2^{\frac{n}{2}+1}+2$$

for any $\alpha\in\mathbb{F}_{2^n}^*$ and $\beta\in\mathbb{F}_{2^n}$.

The Walsh transform of the function f equals

$$\begin{aligned} W_f(\alpha,\beta) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\alpha f(x)+\beta x)} \\ &= \sum_{\mathrm{Tr}_1^n(\delta x)=0} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} + \sum_{\mathrm{Tr}_1^n(\delta x)=1} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{\delta x}+\beta x\right)}. \end{aligned}$$

We need to give estimate on the two sums respectively. The main idea is to transform computing exponential sums into determining the number of rational points on certain projective curves. For the convenience of subsequent discussions, we denote the two sums by $s_1=\sum\limits_{\mathrm{Tr}_1^n(\delta x)=0}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)}$ and $s_2=\sum\limits_{\mathrm{Tr}_1^n(\delta x)=1}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{\delta x}+\beta x\right)}$, respectively.

It can be verified that

$$\begin{aligned} s_1 &= \sum_{\mathrm{Tr}_1^n(\delta x)=0,\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=0} 1 - \sum_{\mathrm{Tr}_1^n(\delta x)=0,\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=1} 1 \\ &= 2\cdot \sum_{\mathrm{Tr}_1^n(\delta x)=0,\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=0} 1 - \sum_{\mathrm{Tr}_1^n(\delta x)=0} 1 \end{aligned}$$

* Corresponding author (email: xiangyongzeng@aliyun.com)

$$= 2 \cdot \sharp A - 2^{n-1}, \tag{A1}$$

where the set A is defined by

$$A = \left\{ x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(\delta x) = 0, \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x} + \beta x\right) = 0 \right\}.$$

Note that for $i, j \in \mathbb{F}_2$,

$$\sum_{x \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\delta x)=i, \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=j} \sum_{u_1,u_2 \in \mathbb{F}_2} (-1)^{u_1 \mathrm{Tr}_1^n(\delta x) + u_2 \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} = \begin{cases} 4 \cdot \sharp A & if\ i = j = 0; \\ 0 & otherwise. \end{cases}$$

Consequently, by (A1) we have

$$\begin{aligned}
& 2^n + 2s_1 \\
= \ & 4 \cdot \sharp A \\
= \ & \sum_{x \in \mathbb{F}_{2^n}} \sum_{u_1,u_2 \in \mathbb{F}_2} (-1)^{u_1 \mathrm{Tr}_1^n(\delta x) + u_2 \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} \\
= \ & \sum_{u_1,u_2 \in \mathbb{F}_2} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{u_1 \mathrm{Tr}_1^n(\delta x) + u_2 \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} \\
= \ & 2^n + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\delta x)} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\delta x) + \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} \\
= \ & 2^n + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\delta x) + \mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)}
\end{aligned}$$

and then

$$2s_1 = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+(\beta+\delta)x\right)}. \tag{A2}$$

The first exponential sum

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)} &= \sum_{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=0} 1 - \sum_{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)=1} 1 \\
&= 2 \cdot \sharp B - 2^n.
\end{aligned}$$

where $B = \left\{ x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(\frac{\alpha}{x^2+x} + \beta x) = 0 \right\}$. To count the cardinal number $\sharp B$, we now define two affine curves $\mathtt{C}_0$ and $\mathtt{C}_0'$ over $\mathbb{F}_{2^n}$

$$\begin{aligned}
\mathtt{C}_0 \ &: \ y^2 + y = \frac{\alpha}{x^2+x} + \beta x \\
\mathtt{C}_0' \ &: \ (y^2+y)(x^2+x) = \alpha + \beta x(x^2+x).
\end{aligned}$$

Denote by $\sharp\mathtt{C}_0$ and $\sharp\mathtt{C}_0'$ the numbers of rational points on $\mathtt{C}_0$ and $\mathtt{C}_0'$, respectively. Note that every point (x_0, y_0) on $\mathtt{C}_0$ satisfies $y_0^2 + y_0 = \frac{\alpha}{x_0^2+x_0} + \beta x_0$ and then $\mathrm{Tr}_1^n(\frac{\alpha}{x_0^2+x_0} + \beta x_0) = \mathrm{Tr}_1^n(y_0^2 + y_0) = 0$, i.e., $x_0 \in B$. Further, for each $x_1 \in B$, by Lemma 1 there are two elements $y_1 \in \mathbb{F}_{2^n}$ such that $y_1^2 + y_1 = \frac{\alpha}{x_1^2+x_1} + \beta x_1$. This is to say,

$$\sharp\mathtt{C}_0 = 2 \cdot \sharp B.$$

It is also true that

$$\sharp\mathtt{C}_0 = \begin{cases} \sharp\mathtt{C}_0' + 2, \ \mathrm{Tr}_1^n(\beta) = 1, \\ \sharp\mathtt{C}_0' + 4, \ \mathrm{Tr}_1^n(\beta) = 0. \end{cases}$$

Indeed, each point (x, y) with $x \notin \mathbb{F}_2$ is on $\mathtt{C}_0$ if and only if it is on $\mathtt{C}_0'$. Further, for $x = 0$, the points $(x, 0), (x, 1)$ are on $\mathtt{C}_0$ but not on $\mathtt{C}_0'$, and for $x = 1$, from the definition of curve $\mathtt{C}_0$, $(x, y) \in \mathtt{C}_0$ means $y^2 + y = \beta$, if and only if $\mathrm{Tr}_1^n(\beta) = 0$ there are two points $(1, y_0), (1, y_0 + 1)$ belonging to $\mathtt{C}_0$, but not belonging to $\mathtt{C}_0'$. We consider the function field $\mathbb{F}_{2^n}(x, y)/\mathbb{F}_{2^n}$ which comes from curve $\mathtt{C}_0'$. The associated homogeneous equation of the curve $\mathtt{C}_0'$ is

$$(y^2 + yz)(x^2 + xz) = \alpha z^4 + \beta xz(x^2 + xz).$$

Let N_0 be the number of rational points on the projective curve. Note that $(0 : 1 : 0)$ and $(1 : 0 : 0)$ are two infinite points on the curve. Consequently, we have

$$N_0 - 2 = \sharp\mathtt{C}_0' = \begin{cases} \sharp\mathtt{C}_0 - 2, \ \mathrm{Tr}_1^n(\beta) = 1, \\ \sharp\mathtt{C}_0 - 4, \ \mathrm{Tr}_1^n(\beta) = 0. \end{cases}$$

By checking the defining equation of $\mathtt{C}_0'$, if we regard it as a polynomial with coefficients in the rational function field $\mathbb{F}_{2^n}(y)$, the algebraic degree of x is not more than 3 and then the degree of the field extension $[\mathbb{F}_{2^n}(x, y) : \mathbb{F}_{2^n}(y)] \leqslant 3$. Meanwhile, if we regard it as a polynomial with coefficients in $\mathbb{F}_{2^n}(x)$, the algebraic degree of y is not more than 2 and

then $[\mathbb{F}_{2^n}(x,y):\mathbb{F}_{2^n}(x)]\leqslant 2$. Then from Riemann's inequality in Lemma 2, the genus of the function field $\mathbb{F}_{2^n}(x,y)/\mathbb{F}_{2^n}$, which is denoted by $g(\mathtt{C}_0')$ for convenience, satisfying $g(\mathtt{C}_0')\leqslant 2$. By Hasse-Weil bound in Lemma 3, we have

$$|N_0-2^n-1|\leqslant 2\cdot 2^{\frac{n}{2}+1}$$

and then

$$|\sharp\mathtt{C}_0-2^n|\leqslant\begin{cases}2\cdot 2^{\frac{n}{2}+1}+1,\ \mathrm{Tr}_1^n(\beta)=1,\\ 2\cdot 2^{\frac{n}{2}+1}+3,\ \mathrm{Tr}_1^n(\beta)=0.\end{cases}$$

Thus, by the above analysis, we have

$$\left|\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+\beta x\right)}\right|\leqslant\begin{cases}2\cdot 2^{\frac{n}{2}+1}+1,\ \mathrm{Tr}_1^n(\beta)=1,\\ 2\cdot 2^{\frac{n}{2}+1}+3,\ \mathrm{Tr}_1^n(\beta)=0.\end{cases}$$

In the same way, we can give an estimate on the second sum in (A2)

$$\left|\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x^2+x}+(\beta+\delta)x\right)}\right|\leqslant\begin{cases}2\cdot 2^{\frac{n}{2}+1}+1,\ \mathrm{Tr}_1^n(\beta+\delta)=1,\ \text{i.e., } \mathrm{Tr}_1^n(\beta)=0,\\ 2\cdot 2^{\frac{n}{2}+1}+3,\ \mathrm{Tr}_1^n(\beta+\delta)=0,\ \text{i.e., } \mathrm{Tr}_1^n(\beta)=1.\end{cases}$$

Consequently, by (A2) we have

$$|s_1|\leqslant 2^{\frac{n}{2}+2}+2.$$

For the exponential sum s_2, we similarly have

$$\begin{aligned}s_2&=\sum_{\mathrm{Tr}_1^n(\delta x)=1}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{\delta x}+\beta x\right)}\\&=\sum_{\mathrm{Tr}_1^n(x)=1}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)}\\&=2\cdot\sharp D-2^{n-1}\end{aligned}\tag{A3}$$

where $D=\left\{x\in\mathbb{F}_{2^n}:\mathrm{Tr}_1^n(x)=1,\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)=0\right\}$. Then

$$\begin{aligned}&2^n+2s_2\\=\;&4\cdot\sharp D\\=\;&\sum_{u_1,u_2\in\mathbb{F}_2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{u_1\left(\mathrm{Tr}_1^n(x)+1\right)+u_2\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)}\\=\;&2^n+\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)}-\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+(1+\beta\delta^{-1})x\right)}.\end{aligned}$$

This shows that

$$2s_2=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)}-\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+(1+\beta\delta^{-1})x\right)},$$

where the two sums are respectively the well-known Kloosterman sums

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+\beta\delta^{-1}x\right)}=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{1}{x}+\alpha\beta\delta^{-1}x\right)}=K(\alpha\beta\delta^{-1})$$

and

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n\left(\frac{\alpha}{x}+(1+\beta\delta^{-1})x\right)}=K\left((1+\beta\delta^{-1})\alpha\right).$$

From the bound that $|K(a)|\leqslant 2^{\frac{n}{2}+1}$, we have

$$|s_2|\leqslant 2^{\frac{n}{2}+1}.$$

The bounds on s_1 and s_2 built as above give $|W_f(\alpha,\beta)|\leqslant|s_1|+|s_2|\leqslant 2^{\frac{n}{2}+2}+2^{\frac{n}{2}+1}+2$ and then

$$\begin{aligned}NL(f)&=2^{n-1}-\frac{1}{2}\max_{\alpha\in\mathbb{F}_{2^n}^*,\beta\in\mathbb{F}_{2^n}}|W_f(\alpha,\beta)|\\&\geqslant 2^{n-1}-3\cdot 2^{\frac{n}{2}}-1.\end{aligned}$$

The proof is finished.

References

1 Lidl R, Niederreiter H. Finite Fields, Encyclopedia of Mathematics and its Applications. Vol. 20, second edition, Cambridge University Press, 1997

2 Stichenoth H. Algebraic Function Fields and Codes. Graduate Texts in Mathematics 254, Berlin, Germany: Springer-Verlag, 1993