

Several classes of negabent functions over finite fields

Gaofei WU¹, Nian LI^{2,3}, Yuqing ZHANG^{1,4*} & Xuefeng LIU¹

¹State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China;

²Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, China;

³Department of Informatics, University of Bergen, Bergen N-5020, Norway;

⁴National Computer Network Intrusion Protection Center, UCAS, Beijing 100043, China

Appendix A

Proof of Lemma 2: Suppose that $A = 0$, then we have $\text{Tr}_1^k(cx^{-1}) = 0$ when $\text{Tr}_1^k(bx) = 0$. We also know $\text{Tr}_1^k(bx)$ is linear, that is, $\#\text{Support}(\text{Tr}_1^k(bx) + 1) = 2^{k-1}$. Thus, we have $\#\text{Support}(\text{Tr}_1^k(cx^{-1}) + 1) \geq 2^{k-1}$. Since $\text{Tr}_1^k(cx^{-1})$ is a balanced function, we obtain $\text{Tr}_1^k(cx^{-1}) = 1$ if $\text{Tr}_1^k(bx) = 1$. From the above discussion, we have $\text{Tr}_1^k(cx^{-1}) = \text{Tr}_1^k(bx)$, i.e., $\sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(bx+cx^{-1})} = q > 2\sqrt{q}$ due to $k > 2$, a contradiction with Lemma 1. \square

Proof of Lemma 4: According to Lemma 3, $f(x)$ is a permutation polynomial over \mathbb{F}_{2^n} if and only if $\gcd(\frac{x^{3k}-1}{x^k-1}, x^n-1) = 1$. Note that $\gcd(\frac{x^{3k}-1}{x^k-1}, x^k-1) = \gcd(3, x^k-1) = 1$. This implies that $\gcd(x^{3k}-1, x^n-1) = \gcd(\frac{x^{3k}-1}{x^k-1}, x^n-1) \cdot \gcd(x^k-1, x^n-1)$ which leads to $\gcd(\frac{x^{3k}-1}{x^k-1}, x^n-1) = \frac{x^{\gcd(n,3k)}-1}{x^{\gcd(n,k)}-1}$. Thus, $f(x)$ is a permutation polynomial over \mathbb{F}_{2^n} if and only if $\gcd(n, 3k) = \gcd(n, k)$.

If $g(x)$ is the compositional inverse of $f(x)$, then we have $g(x)$ is a 2-polynomial over \mathbb{F}_2 due to Lemma 3. Moreover, we have $g(1) = 1$ since $f(1) = 1$, i.e., $g(x)$ has odd number of terms. This leads to $\text{Tr}_1^n(g(x)) = \text{Tr}_1^n(x)$ since $g(x)$ is a 2-polynomial over \mathbb{F}_2 . \square

Proof of Lemma 5: Note that $f(x)$ is a 2^k -polynomial over \mathbb{F}_{2^k} . Thus the first assert follows directly from Lemma 3. Further, by Lemma 3 we have that $g(x)$ is also a 2^k -polynomial over \mathbb{F}_{2^k} if $g(x)$ is the compositional inverse of $f(x)$. Suppose that $g(x) = \sum_{i=0}^{r-1} c_i x^{2^{ki}}$, where $c_i \in \mathbb{F}_{2^k}$. Then, we have $\text{Tr}_1^n(g(x)) = \text{Tr}_1^k(\text{Tr}_k^{r^k}(g(x))) = \text{Tr}_1^k(\text{Tr}_k^{r^k}(\sum_{i=0}^{r-1} c_i x^{2^{ki}})) = \text{Tr}_1^k(\sum_{i=0}^{r-1} c_i \text{Tr}_k^{r^k}(x^{2^{ki}})) = \text{Tr}_1^k(g(1)\text{Tr}_k^{r^k}(x))$. Then the result follows from the fact that $g(1) = 1$ since $f(1) = 1$. \square

Appendix B

Proof of Theorem 2: According to Theorem 1, to complete this proof, it is sufficient to prove that $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced for all nonzero $a \in \mathbb{F}_{2^n}$ if and only if λ, u, v satisfy one of the conditions given in Theorem 2. A direct calculation gives

$$\begin{aligned} f(x) + f(x+a) + \text{Tr}_1^n(ax) &= \text{Tr}_1^k(\lambda(a^{2^k}x + ax^{2^k})) + \text{Tr}_1^n(ua)\text{Tr}_1^n(vx) + \text{Tr}_1^n(va)\text{Tr}_1^n(ux) + \text{Tr}_1^n(ax) \\ &\quad + \text{Tr}_1^k(\lambda a^{2^k+1}) + \text{Tr}_1^n(ua)\text{Tr}_1^n(va) \\ &= \text{Tr}_1^n((\lambda a^{2^k} + a)x) + \text{Tr}_1^n(v\text{Tr}_1^n(ua)x) + \text{Tr}_1^n(u\text{Tr}_1^n(va)x) \\ &\quad + \text{Tr}_1^k(\lambda a^{2^k+1}) + \text{Tr}_1^n(ua)\text{Tr}_1^n(va). \end{aligned}$$

This implies that $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced if and only if $\lambda a^{2^k} + a + v\text{Tr}_1^n(ua) + u\text{Tr}_1^n(va) \neq 0$. Notice that $\lambda a^{2^k} + a$ is a 2^k -polynomial and $\gcd(\lambda a^k + 1, a^{2^k} + 1) = \gcd(\lambda a^k + 1, (a^k + 1)^2) = \gcd(\lambda + 1, a^k + 1) = 1$ only if $\lambda \neq 1$. This together with Lemma 3 shows that $\lambda a^{2^k} + a$ is permutation polynomial over \mathbb{F}_{2^n} if $\lambda \neq 1$. Moreover, for any $\lambda \neq 1$ and $b \in \mathbb{F}_{2^n}$, if $\lambda a^{2^k} + a = b$, then one gets $\lambda a + a^{2^k} = b^{2^k}$ since $n = 2k$ and $\lambda \in \mathbb{F}_{2^k}$. These two identities lead to

$$a = \frac{b + \lambda b^{2^k}}{\lambda^2 + 1}, \tag{B1}$$

* Corresponding author (email: zhangyq@ucas.ac.cn)

which is the unique solution to $\lambda a^{2^k} + a = b$.

For simplicity, define $h(a) = \lambda a^{2^k} + a + v\text{Tr}_1^n(ua) + u\text{Tr}_1^n(va)$. Then by (B1), for $\lambda \neq 1$ we have

- 1) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 0)$: For this case, $h(a) = 0$ has the only solution $a = 0$.
- 2) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 1)$: By (B1), $a = \frac{u+\lambda u^{2^k}}{\lambda^2+1}$ is the unique solution to $\lambda a^{2^k} + a + u = 0$. Note that $\text{Tr}_1^n(ua) = \text{Tr}_1^n(u \cdot \frac{\lambda u^{2^k}+u}{1+\lambda^2}) = \text{Tr}_1^n(\frac{\lambda u^{2^k+1}}{1+\lambda^2}) + \text{Tr}_1^n(\frac{u^2}{1+\lambda^2}) = \text{Tr}_1^n(\frac{u}{1+\lambda})$ since $n = 2k$ and $\frac{\lambda u^{2^k+1}}{1+\lambda^2} \in \mathbb{F}_{2^k}$. Thus, in this case $h(a) = 0$ has the only solution $a = \frac{u+\lambda u^{2^k}}{\lambda^2+1}$ if and only if $\text{Tr}_1^n(\frac{u}{1+\lambda}) = 0$ and $\text{Tr}_1^n(va) = \text{Tr}_1^n(v \cdot \frac{\lambda u^{2^k}+u}{1+\lambda^2}) = 1$.
- 3) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (1, 0)$: Similar as above, for this case $h(a) = 0$ has the only solution $a = \frac{v+\lambda v^{2^k}}{\lambda^2+1}$ if and only if $\text{Tr}_1^n(\frac{v}{1+\lambda}) = 0$ and $\text{Tr}_1^n(ua) = \text{Tr}_1^n(u \cdot \frac{\lambda v^{2^k}+v}{1+\lambda^2}) = 1$.
- 4) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (1, 1)$: In this case, $a = \frac{u+v+\lambda(u+v)^{2^k}}{\lambda^2+1}$ is the unique solution to $\lambda a^{2^k} + a + u + v = 0$ due to (B1). By the same techniques used in Cases 2) and 3) one can conclude that $h(a) = 0$ has the only solution if and only if $\text{Tr}_1^n(\frac{u}{1+\lambda} + \frac{(\lambda v^{2^k}+v)u}{1+\lambda^2}) = 1$ and $\text{Tr}_1^n(\frac{v}{1+\lambda} + \frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}) = 1$.

Notice that $\text{Tr}_1^n(\frac{(\lambda v^{2^k}+v)u}{1+\lambda^2}) = \text{Tr}_1^n(\frac{(\lambda v u^{2^k})^{2^k}}{(1+\lambda^2)^{2^k}}) + \text{Tr}_1^n(\frac{vu}{1+\lambda^2}) = \text{Tr}_1^n(\frac{\lambda v u^{2^k}}{1+\lambda^2}) + \text{Tr}_1^n(\frac{vu}{1+\lambda^2}) = \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2})$ due to $n = 2k$ and $\lambda \in \mathbb{F}_{2^k}$. Thus, Case 2) shows that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \notin \{(0, 1, 0), (0, 1, 1)\}$, Case 3) shows that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \notin \{(0, 1, 0), (1, 1, 0)\}$, and Case 4) shows that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \notin \{(0, 1, 0), (1, 0, 1)\}$. Therefore, if $\lambda \neq 1$, one has that $h(a) = \lambda a^{2^k} + a + v\text{Tr}_1^n(ua) + u\text{Tr}_1^n(va) \neq 0$ for any nonzero $a \in \mathbb{F}_{2^n}$ if and only if the first condition in Theorem 2 is satisfied.

Now we consider the case of $\lambda = 1$. First we discuss the number of solutions of $h(a) = \lambda a^{2^k} + a + v\text{Tr}_1^n(ua) + u\text{Tr}_1^n(va)$ under the condition $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 0)$. In this case, $h(a) = 0$ is equivalent to $a \in \mathbb{F}_{2^k}$. Let $N(u, v)$ denote the number of nonzero $a \in \mathbb{F}_{2^k}$ such that $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 0)$, where $(u, v) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$. Then, according to the balanced property of the trace function and the fact that $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (\text{Tr}_1^k(a(u+u^{2^k})), \text{Tr}_1^k(a(v+v^{2^k})))$, it can be readily verified that $N(u, v) = 2^k - 1$ if $u, v \in \mathbb{F}_{2^k}$, $N(u, v) = 2^{k-1} - 1$ if exactly one of u, v belongs to \mathbb{F}_{2^k} , $N(u, v) = 2^{k-1} - 1$ if $u, v \notin \mathbb{F}_{2^k}$ with $u + v \in \mathbb{F}_{2^k}$ and $N(u, v) = 2^{k-2} - 1$ if $u, v, u + v \notin \mathbb{F}_{2^k}$ respectively. This implies that $h(a) = 0$ under the condition $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 0)$ has at least one nonzero solution for any given $u, v \in \mathbb{F}_{2^n}$ if $k > 2$, i.e., $f(x)$ cannot be negabent if $\lambda = 1$ and $k > 2$. The conditions on $u, v \in \mathbb{F}_{2^n}$ such that $f(x)$ is negabent for $k = 1, 2$ can be easily verified based on a simple discussion. This completes the proof. \square

Proof of Corollary 1:

We only give the proof for $\lambda \neq 1$ since the proof for $\lambda = 1$ is trivial due to Theorem 2. For $\lambda \neq 1$, we first determine the number of ordered pairs (u, v) such that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \in \{(0, 0, 0), (0, 0, 1)\}$. Note that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \in \{(0, 0, 0), (0, 0, 1)\}$ is equivalent to $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2})) = (0, 0)$. Clearly, the number of $u \in \mathbb{F}_{2^n}^*$ satisfying $\text{Tr}_1^n(\frac{u}{1+\lambda}) = 0$ is $2^{n-1} - 1$, and for each such u , there are $2^{n-1} - 2$ v 's in $\mathbb{F}_{2^n}^* \setminus \{u\}$ such that $\text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}) = 0$ (notice that $\lambda x^{2^k} + x$ is a permutation polynomial over \mathbb{F}_{2^n} due to $\lambda \neq 1$, then $\lambda u^{2^k} + u \neq 0$ if $u \neq 0$). Thus, in this case we get $(2^{n-1} - 1)(2^{n-1} - 2)$ ordered pairs (u, v) such that $f(x)$ is negabent.

Next we count the number of the pairs (u, v) such that $(\text{Tr}_1^n(\frac{u}{1+\lambda}), \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}), \text{Tr}_1^n(\frac{v}{1+\lambda})) \in \{(1, 0, 0), (1, 1, 1)\}$, which is equivalent to counting the number of the pairs (u, v) satisfying $\text{Tr}_1^n(\frac{u}{1+\lambda}) = 1$ and $\text{Tr}_1^n(\frac{(\lambda u^{2^k}+u)v}{1+\lambda^2}) + \text{Tr}_1^n(\frac{v}{1+\lambda}) = \text{Tr}_1^n(\frac{(\lambda u^{2^k}+u+1+\lambda)v}{1+\lambda^2}) = 0$. Similar as above, for this case the number of $u \in \mathbb{F}_{2^n}^*$ satisfying $\text{Tr}_1^n(\frac{u}{1+\lambda}) = 1$ is 2^{n-1} , and for each such u (notice that $u \neq 1$ since $\text{Tr}_1^n(\frac{1}{1+\lambda}) = 0$), there are $2^{n-1} - 2$ v 's in $\mathbb{F}_{2^n}^* \setminus \{u\}$ such that $\text{Tr}_1^n(\frac{(\lambda u^{2^k}+u+1+\lambda)v}{1+\lambda^2}) = 0$ (notice that $\lambda x^{2^k} + x + 1 + \lambda$ is a permutation polynomial over \mathbb{F}_{2^n} due to $\lambda \neq 1$, thus $\lambda u^{2^k} + u + 1 + \lambda \neq 0$ since $u \neq 1$), i.e., we have $2^{n-1}(2^{n-1} - 2)$ ordered pairs (u, v) such that $f(x)$ is negabent. \square

Proof of Theorem 3:

According to Theorem 1, it is sufficient to prove that

$$f(x) + f(x+a) + \text{Tr}_1^n(ax) = \text{Tr}_1^n\left(\left(\text{Tr}_1^n(va)u + \text{Tr}_1^n(ua)v + a\right)x\right) + \text{Tr}_1^n(ua)\text{Tr}_1^n(va)$$

is balanced for all nonzero $a \in \mathbb{F}_{2^n}$, which is equivalent to show that $\text{Tr}_1^n(va)u + \text{Tr}_1^n(ua)v + a \neq 0$ for all nonzero a . Let $h(a) = \text{Tr}_1^n(va)u + \text{Tr}_1^n(ua)v + a$, we have

- 1) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 0)$: For this case, $h(a) = 0$ has the only solution $a = 0$.
- 2) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (0, 1)$: In this case, $h(a) = 0$ has the only solution $a = u$ if and only if $\text{Tr}_1^n(u) = 0$ and $\text{Tr}_1^n(uv) = 1$.
- 3) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (1, 0)$: Similar as above, for this case $h(a) = 0$ has the only solution $a = v$ if and only if $\text{Tr}_1^n(uv) = 1$ and $\text{Tr}_1^n(v) = 0$.

- 4) $(\text{Tr}_1^n(ua), \text{Tr}_1^n(va)) = (1, 1)$: In this case, $a = u + v$ is the only solution to $\text{Tr}_1^n(va)u + \text{Tr}_1^n(ua)v + a = 0$ if and only if $\text{Tr}_1^n(u(u+v)) = 1$ and $\text{Tr}_1^n(v(u+v)) = 1$.

Based on Cases 1)-4), it can be seen that $\text{Tr}_1^n(va)u + \text{Tr}_1^n(ua)v + a \neq 0$ for all nonzero a if and only if one of the two conditions in Theorem 3 is satisfied. \square

Proof of Theorem 4:

According to Theorem 1, we only need to show that $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced for all nonzero $a \in \mathbb{F}_{2^n}$ if $\text{Tr}_1^n(v) = 0$. A direct calculation gives

$$\begin{aligned} f(x) + f(x+a) + \text{Tr}_1^n(ax) &= \text{Tr}_1^n(a^{2^k}x + ax^{2^k}) + \text{Tr}_1^n(a)\text{Tr}_1^n(vx) + \text{Tr}_1^n(va)\text{Tr}_1^n(x) + \text{Tr}_1^n(ax) \\ &\quad + \text{Tr}_1^n(a^{2^k+1}) + \text{Tr}_1^n(a)\text{Tr}_1^n(va) \\ &= \text{Tr}_1^n((a^{2^k} + a^{2^{-k}} + a)x) + \text{Tr}_1^n((v\text{Tr}_1^n(a))x) + \text{Tr}_1^n(\text{Tr}_1^n(va)x) \\ &\quad + \text{Tr}_1^n(a^{2^k+1}) + \text{Tr}_1^n(a)\text{Tr}_1^n(va). \end{aligned}$$

This shows that $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced if and only if $a^{2^k} + a^{2^{-k}} + a + v\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0$, i.e., $a + a^{2^k} + a^{2^{2k}} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0$. Notice that $a + a^{2^k} + a^{2^{2k}}$ is a permutation of \mathbb{F}_{2^n} due to Lemma 4. Let $g(a) = a + a^{2^k} + a^{2^{2k}} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va)$ and $h(a)$ be the compositional inverse of $a + a^{2^k} + a^{2^{2k}}$, then we have

- 1) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (0, 0)$: For this case, $g(a) = 0$ has the only solution $a = 0$.
- 2) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (0, 1)$: In this case, $g(a) = 0$ means that $a + a^{2^k} + a^{2^{2k}} = 1$, i.e., $a = h(1) = 1$. However, $\text{Tr}_1^n(va) = \text{Tr}_1^n(v) = 0$, which shows that $g(a) = 0$ has no solution in this case.
- 3) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (1, 0)$: In this case, $g(a) = 0$ is reduced to $a + a^{2^k} + a^{2^{2k}} = v^{2^k}$, i.e., $a = h(v^{2^k})$. However, by Lemma 4, $\text{Tr}_1^n(a) = \text{Tr}_1^n(h(v^{2^k})) = \text{Tr}_1^n(v^{2^k}) = \text{Tr}_1^n(v) = 0$. This shows that $g(a) = 0$ has no solution in this case.
- 4) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (1, 1)$: Similar as above, $g(a) = 0$ implies that $a + a^{2^k} + a^{2^{2k}} = 1 + v^{2^k}$, i.e., $a = h(1 + v^{2^k})$. Note that $\text{Tr}_1^n(1) = 0$ since n is even. From Lemma 4, $\text{Tr}_1^n(a) = \text{Tr}_1^n(h(1 + v^{2^k})) = \text{Tr}_1^n(1 + v^{2^k}) = \text{Tr}_1^n(v) = 0$, which shows that $g(a) = 0$ has no solution in this case.

From the above Cases 1)-4), we can see that $a + a^{2^k} + a^{2^{2k}} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0$ for all $a \in \mathbb{F}_{2^n}^*$ if $\text{Tr}_1^n(v) = 0$. \square

Proof of Theorem 5:

According to Theorem 1, it is enough to prove that $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced for all nonzero $a \in \mathbb{F}_{2^n}$ for the $v \in \mathbb{F}_{2^n}$ satisfying $\text{Tr}_1^n(v) = 0$. Note that

$$\begin{aligned} f(x) + f(x+a) + \text{Tr}_1^n(ax) &= \text{Tr}_1^n(\lambda(a^{2^k}x + ax^{2^k})) + \text{Tr}_1^n(a)\text{Tr}_1^n(vx) + \text{Tr}_1^n(va)\text{Tr}_1^n(x) + \text{Tr}_1^n(ax) \\ &\quad + \text{Tr}_1^n(\lambda a^{2^k+1}) + \text{Tr}_1^n(a)\text{Tr}_1^n(va) \\ &= \text{Tr}_1^n((\lambda a^{2^k} + (\lambda a)^{2^{-k}} + a)x) + \text{Tr}_1^n(v\text{Tr}_1^n(a)x) + \text{Tr}_1^n(\text{Tr}_1^n(va)x) \\ &\quad + \text{Tr}_1^n(\lambda a^{2^k+1}) + \text{Tr}_1^n(a)\text{Tr}_1^n(va). \end{aligned}$$

Thus, $f(x) + f(x+a) + \text{Tr}_1^n(ax)$ is balanced if and only if

$$\lambda a^{2^k} + (\lambda a)^{2^{-k}} + a + v\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0. \quad (\text{B2})$$

Raising both sides of (B2) to the 2^k -th power, we get $\lambda a^{2^{2k}} + \lambda a + a^{2^k} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0$ due to $\lambda \in \mathbb{F}_{2^k}$. Let $g(a) = \lambda a + a^{2^k} + \lambda a^{2^{2k}} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va)$. According to Lemma 5, $\lambda a + a^{2^k} + \lambda a^{2^{2k}}$ is a permutation of \mathbb{F}_{2^n} since $\gcd(\lambda + x + \lambda x^2, x^3 - 1) = 1$. Let $h(a)$ be the compositional inverse of $\lambda a + a^{2^k} + \lambda a^{2^{2k}}$. Similar as in the proof of Theorem 4, we have

- 1) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (0, 0)$: For this case, $g(a) = 0$ has the only solution $a = 0$.
- 2) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (0, 1)$: In this case, $g(a) = 0$ means that $\lambda a + a^{2^k} + \lambda a^{2^{2k}} = 1$, i.e., $a = h(1) = 1$ since $\lambda \cdot 1 + 1^{2^k} + \lambda \cdot 1^{2^{2k}} = 1$. However, $\text{Tr}_1^n(va) = \text{Tr}_1^n(v) = 0$, which shows that $g(a) = 0$ has no solution in this case.
- 3) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (1, 0)$: In this case, $g(a) = 0$ means that $\lambda a + a^{2^k} + \lambda a^{2^{2k}} = v^{2^k}$, i.e., $a = h(v^{2^k})$. From Lemma 5, $\text{Tr}_1^n(a) = \text{Tr}_1^n(h(v^{2^k})) = \text{Tr}_1^n(v^{2^k}) = \text{Tr}_1^n(v) = 0$, which shows that $g(a) = 0$ has no solution in this case.
- 4) $(\text{Tr}_1^n(a), \text{Tr}_1^n(va)) = (1, 1)$: Similar as above, $g(a) = 0$ implies that $\lambda a + a^{2^k} + \lambda a^{2^{2k}} = 1 + v^{2^k}$, i.e., $a = h(1 + v^{2^k})$. Note that $\text{Tr}_1^n(1) = 0$ due to n is even. Again by Lemma 5, $\text{Tr}_1^n(a) = \text{Tr}_1^n(h(1 + v^{2^k})) = \text{Tr}_1^n(1 + v^{2^k}) = \text{Tr}_1^n(v) = 0$. This implies that $g(a) = 0$ has no solution in this case.

From the above Cases 1)-4), we can see that if $\text{Tr}_1^n(v) = 0$, then $\lambda a + a^{2^k} + \lambda a^{2^{2k}} + v^{2^k}\text{Tr}_1^n(a) + \text{Tr}_1^n(va) \neq 0$ for all nonzero $a \in \mathbb{F}_{2^n}$. \square

Proof of Corollary 3:

According to Theorem 5, it is sufficient to show that $\gcd(\lambda + x + \lambda x^2, x^3 - 1) = 1$ if $\lambda \neq 1$. Then the result follows from the fact that $\gcd(\lambda + x + \lambda x^2, x^3 - 1) = \gcd(\lambda + x + \lambda x^2, x^2 + x + 1) = \gcd(\lambda(x^2 + x + 1) + (\lambda + 1)x, x^2 + x + 1) = \gcd((\lambda + 1)x, x^2 + x + 1)$. \square

Proof of Corollary 4:

The result follows from that if $r = 4$, then $\gcd(\lambda + x + \lambda x^2, x^4 - 1) = \gcd(\lambda + x + \lambda x^2, x - 1) = 1$ for any $\lambda \in \mathbb{F}_{2^k}^*$. \square
Proof of Corollary 5:

According to Theorem 5, we need to determine the condition on λ such that $\gcd(\lambda + x + \lambda x^2, x^5 - 1) = 1$. Notice that $\gcd(\lambda + x + \lambda x^2, x^5 - 1) = \gcd(\lambda + x + \lambda x^2, x^4 + x^3 + x^2 + x + 1)$. By a simple calculation, we have $x^4 + x^3 + x^2 + x + 1 = (1 + \mu x + x^2)(\mu^2 + \mu + (\mu + 1)x + x^2) + (\mu^2 + \mu + 1)(\mu x + 1)$, where $\mu = \lambda^{-1}$. This leads to $\gcd(\lambda + x + \lambda x^2, x^4 + x^3 + x^2 + x + 1) = \gcd(1 + \mu x + x^2, x^4 + x^3 + x^2 + x + 1) = \gcd(1 + \mu x + x^2, (\mu^2 + \mu + 1)(\mu x + 1)) = 1$ if and only of $\mu^2 + \mu + 1 \neq 0$. \square

Appendix C

Proof of Theorem 6:

Since k is odd, then $f(x) = x^2 + x + 1$ is irreducible over \mathbb{F}_{2^k} as it is irreducible over \mathbb{F}_2 . Let ω be a root of $f(x)$. Then $\mathbb{F}_{2^n} = \mathbb{F}_{2^k}[\omega]$, i.e., each $x \in \mathbb{F}_{2^n}$ can be uniquely represented as $x_0 + x_1\omega$, where $x_i \in \mathbb{F}_{2^k}$. Then

$$x^d = (x_0 + x_1\omega)^d = x_0^d + x_1^d + x_1x_0^3 + x_0x_1^3 + (x_0^2x_1^2 + x_0x_1^3 + x_1^4)\omega \quad (C1)$$

and

$$(x + a)^d = (x_0 + a_0)^d + (x_1 + a_1)^d + (x_1 + a_1)(x_0 + a_0)^3 + (x_0 + a_0)(x_1 + a_1)^3 + ((x_0 + a_0)^2(x_1 + a_1)^2 + (x_0 + a_0)(x_1 + a_1)^3 + (x_1 + a_1)^4)\omega, \quad (C2)$$

where $a = a_0 + a_1\omega$.

Note that $\text{Tr}_k^{2k}(1) = 0$ and $\text{Tr}_k^{2k}(\omega) = \omega + \omega^{2^k} = 1$ since k is odd and ω is a root of $x^2 + x + 1$. Let $\lambda = \lambda_0 + \lambda_1\omega$. Then from (C1), (C2) and $\text{Tr}_k^{2k}(ax) = a_0x_1 + a_1x_0 + a_1x_1$, we have

$$\begin{aligned} & \text{Tr}_k^{2k}(\lambda x^d + \lambda(x + a)^d + ax) \\ &= \lambda_1x_0^2a_1^2 + \lambda_0x_0a_1^3 + \lambda_0x_0^2a_1^2 + \lambda_1a_1x_0^3 + \lambda_0a_0x_1^3 + a_1x_0 + \lambda_1x_1x_0a_0^2 + \lambda_1x_1x_0^2a_0 + \lambda_1a_1x_0a_0^2 \\ &+ \lambda_1a_1x_0^2a_0 + x_1a_1 + \lambda_0a_0x_1^2a_1 + \lambda_0x_0x_1^2a_1 + \lambda_0x_0x_1a_1^2 + \lambda_0a_0x_1a_1^2 + \lambda_0a_0a_1^3 + \lambda_0a_1^4 \\ &+ \lambda_1a_0^4 + \lambda_1x_1a_0^3 + \lambda_1a_1a_0^3 + \lambda_1a_0^2x_1^2 + \lambda_1a_0^2a_1^2 + \lambda_0a_0^2x_1^2 + \lambda_0a_0^2a_1^2 + a_0x_1 = G(x_0, x_1). \end{aligned} \quad (C3)$$

Suppose that $\lambda_1 \neq 0$. We will show that for each $\lambda = \lambda_0 + \lambda_1\omega$ with $\lambda_1 \neq 0$, there exists at least one nonzero $a = a_0 + a_1\omega \in \mathbb{F}_{2^n}$ such that $\text{Tr}_1^n(\lambda x^d + \lambda(x + a)^d + ax) = \text{Tr}_1^k(G(x_0, x_1))$ is not balanced. We consider this in three cases.

Case (i) $\lambda_1 \neq 0, \lambda_0^2 + \lambda_1^2 + \lambda_0\lambda_1 + 1 \neq 0$.

In this case, let $a_1 = 0$ and $a_0 \neq 0$. Then

$$\begin{aligned} & \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} \\ &= \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_1x_1x_0^2a_0 + \lambda_1x_1x_0a_0^2 + \lambda_1a_0^2x_1^2 + \lambda_0a_0x_1^3 + \lambda_0a_0^2x_1^2 + \lambda_1a_0^4 + \lambda_1x_1a_0^3 + a_0x_1)} \\ &= \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_1a_0^2x_1^2 + \lambda_0a_0x_1^3 + \lambda_0a_0^2x_1^2 + \lambda_1a_0^4 + \lambda_1x_1a_0^3 + a_0x_1)} \sum_{x_0 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k((\lambda_1x_1a_0 + \lambda_1^2x_1^2a_0^4)x_0^2)} \\ &= 2^k \sum_{x_1=0 \text{ or } x_1=(\lambda_1a_0^3)^{-1}} (-1)^{\text{Tr}_1^k(\lambda_1a_0^2x_1^2 + \lambda_0a_0x_1^3 + \lambda_0a_0^2x_1^2 + \lambda_1a_0^4 + \lambda_1x_1a_0^3 + a_0x_1)} \\ &= 2^k((-1)^{\text{Tr}_1^k(\lambda_1a_0^4)} + (-1)^{\text{Tr}_1^k(\lambda_1a_0^2t^2 + \lambda_0a_0t^3 + \lambda_0a_0^2t^2 + \lambda_1a_0^4 + \lambda_1ta_0^3 + a_0t)}), \end{aligned} \quad (C4)$$

where $t = (\lambda_1a_0^3)^{-1}$. By (C4), if there exists $a_0 \in \mathbb{F}_q^*$ such that $\text{Tr}_1^k(\lambda_1a_0^2t^2 + \lambda_0a_0t^3 + \lambda_0a_0^2t^2 + \lambda_1ta_0^3 + a_0t) = 0$, then $\sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} = (-1)^{\text{Tr}_1^k(\lambda_1a_0^4)} \cdot 2^{k+1} \neq 0$, i.e., $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced for such $a_0 \in \mathbb{F}_q^*$. Since $t = (\lambda_1a_0^3)^{-1}$, we have $\text{Tr}_1^k(\lambda_1a_0^2t^2 + \lambda_0a_0t^3 + \lambda_0a_0^2t^2 + \lambda_1ta_0^3 + a_0t) = \text{Tr}_1^k(\frac{\lambda_1^2 + \lambda_0^2 + 1 + \lambda_0\lambda_1}{\lambda_1^4}(a_0^8)^{-1} + 1)$, which implies that there exists $a_0 \neq 0$ such that $\text{Tr}_1^k(\frac{\lambda_1^2 + \lambda_0^2 + 1 + \lambda_0\lambda_1}{\lambda_1^4}(a_0^8)^{-1}) + 1 = 0$ if $\lambda \in \mathbb{F}_{2^n}$ satisfying $\lambda_0^2 + \lambda_1^2 + \lambda_0\lambda_1 + 1 \neq 0$ and $\lambda_1 \neq 0$.

Case (ii) $\lambda_1 \neq 0, \lambda_0^2 + \lambda_1^2 + \lambda_0\lambda_1 + 1 = 0$ and $\lambda_0 \neq 0$.

In this case, let $a_0 = 0$ and $a_1 \neq 0$. Then

$$\begin{aligned} & \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} \\ &= \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_0x_0x_1^2a_1 + (\lambda_0a_1^2x_0 + a_1)x_1 + \lambda_1a_1x_0^3 + (\lambda_1a_1^2 + \lambda_0a_1^2)x_0^2 + (\lambda_0a_1^3 + a_1)x_0 + \lambda_0a_1^4)} \\ &= \sum_{x_0 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_1a_1x_0^3 + (\lambda_1a_1^2 + \lambda_0a_1^2)x_0^2 + (\lambda_0a_1^3 + a_1)x_0 + \lambda_0a_1^4)} \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k((\lambda_0x_0a_1 + \lambda_0^2a_1^4x_0^2 + a_1^2)x_1^2)} \\ &= 2^k \sum_{x_0=y_1 \text{ or } x_0=y_2} (-1)^{\text{Tr}_1^k(\lambda_1a_1x_0^3 + (\lambda_1a_1^2 + \lambda_0a_1^2)x_0^2 + (\lambda_0a_1^3 + a_1)x_0 + \lambda_0a_1^4)}, \end{aligned} \quad (C5)$$

where y_1 and y_2 are the two roots of $\lambda_0x_0a_1 + \lambda_0^2a_1^4x_0^2 + a_1^2 = 0$ (x_0 as the indeterminate variable) under the condition $\text{Tr}_1^k(a_1) = 0$. Thus, $y_1 + y_2 = \frac{1}{\lambda_0a_1^3}$ and $y_1y_2 = \frac{1}{\lambda_0^2a_1^2}$. By (C5), if there exists $a_1 \in \mathbb{F}_q^*$ such that $\text{Tr}_1^k(a_1) = 0$ and

$\text{Tr}_1^k(\lambda_1 a_1(y_1^3 + y_2^3) + (\lambda_1 a_1^2 + \lambda_0 a_1^2)(y_1 + y_2)^2 + (\lambda_0 a_1^3 + a_1)(y_1 + y_2)) = 0$, then $\sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} = \pm 2^{k+1} \neq 0$, i.e., $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced for such $a_1 \in \mathbb{F}_q^*$. By $y_1^3 + y_2^3 = (y_1 + y_2)^3 + y_1 y_2 (y_1 + y_2) = \frac{1}{\lambda_0^3} (\frac{1}{a_1^3} + \frac{1}{a_1^3})$, one obtains that

$$\begin{aligned} & \text{Tr}_1^k(\lambda_1 a_1(y_1^3 + y_2^3) + (\lambda_1 a_1^2 + \lambda_0 a_1^2)(y_1 + y_2)^2 + (\lambda_0 a_1^3 + a_1)(y_1 + y_2)) \\ &= \text{Tr}_1^k\left(\left(\frac{\lambda_1^2}{\lambda_0^6} + \frac{\lambda_0^2 + \lambda_1^2 + \lambda_0 \lambda_1 + 1}{\lambda_0^4}\right) \frac{1}{a_1^8} + 1\right) = \text{Tr}_1^k\left(\frac{\lambda_1^2}{\lambda_0^6} \cdot \frac{1}{a_1^8} + 1\right). \end{aligned}$$

According to Lemma 2, for odd $k > 2$, there exists $a_1 \in \mathbb{F}_q^*$ such that $\text{Tr}_1^k(\frac{\lambda_1^2}{\lambda_0^6} \cdot \frac{1}{a_1^8} + 1) = \text{Tr}_1^k((\frac{\lambda_1^2}{\lambda_0^6})^{-8} \cdot \frac{1}{a_1}) + 1 = 0$ and $\text{Tr}_1^k(a_1) = 0$. Thus, for any $\lambda \in \mathbb{F}_q$ such that $\lambda_0^2 + \lambda_1^2 + \lambda_0 \lambda_1 + 1 = 0$ and $\lambda_0 \lambda_1 \neq 0$, there exists $a_1 \neq 0$ such that $\text{Tr}_1^k(a_1) = 0$ and $\text{Tr}_1^k(\lambda_1 a_1(y_1^3 + y_2^3) + (\lambda_1 a_1^2 + \lambda_0 a_1^2)(y_1 + y_2)^2 + (\lambda_0 a_1^3 + a_1)(y_1 + y_2)) = 0$. That is, $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced for such $a_1 \in \mathbb{F}_q^*$.

Case (iii) $\lambda_1 \neq 0, \lambda_0^2 + \lambda_1^2 + \lambda_0 \lambda_1 + 1 = 0$ and $\lambda_0 = 0$.

For this case, $\lambda_1 = 1$ and $\lambda_0 = 0$. Let $a_0 = a_1 \neq 0$. Then

$$\begin{aligned} & \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} \\ &= \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(a_0^2 x_1^2 + (x_0^2 a_0 + x_0 a_0^2 + a_0^3) x_1 + x_0^3 a_0 + (a_0^3 + a_0) x_0 + a_0^4)} \\ &= \sum_{x_0 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(x_0^3 a_0 + (a_0^3 + a_0) x_0 + a_0^4)} \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k((a_0 + x_0^2 a_0 + x_0 a_0^2 + a_0^3) x_1)} \\ &= 2^k \sum_{x_0=y_1 \text{ or } x_0=y_2} (-1)^{\text{Tr}_1^k(x_0^3 a_0 + (a_0^3 + a_0) x_0 + a_0^4)}, \end{aligned} \tag{C6}$$

where y_1 and y_2 are the two roots of $a_0 + x_0^2 a_0 + x_0 a_0^2 + a_0^3 = 0$ (x_0 as the indeterminate variable) under the condition $\text{Tr}_1^k(a_0^{-1}) = 1$. Thus, $y_1 + y_2 = a_0$ and $y_1 y_2 = 1 + a_0^2$. By (C6), if there exists $a_0 \in \mathbb{F}_q^*$ such that $\text{Tr}_1^k(a_0^{-1}) = 1$ and $\text{Tr}_1^k((y_1^3 + y_2^3) a_0 + (a_0^3 + a_0)(y_1 + y_2)) = 0$, then $\sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} = \pm 2^{k+1} \neq 0$. That is, $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced for such $a_0 \in \mathbb{F}_q^*$. Note that $y_1^3 + y_2^3 = (y_1 + y_2)^3 + y_1 y_2 (y_1 + y_2) = a_0^3 + (1 + a_0^2) a_0 = a_0$, then $\text{Tr}_1^k((y_1^3 + y_2^3) a_0 + (a_0^3 + a_0)(y_1 + y_2)) = \text{Tr}_1^k(a_0^3 + (a_0^3 + a_0) a_0) = \text{Tr}_1^k(a_0) = 0$. Again by Lemma 2, for odd $k > 2$, there exists $a_0 \in \mathbb{F}_q^*$ such that $\text{Tr}_1^k(a_0) = 0$ and $\text{Tr}_1^k(a_0^{-1}) = 1$. Thus, for $\lambda = \lambda_0 + \lambda_1 \omega = \omega$, there exists $a_0 \neq 0$ such that $\text{Tr}_1^k(a_0^{-1}) = 1$ and $\text{Tr}_1^k((y_1^3 + y_2^3) a_0 + (a_0^3 + a_0)(y_1 + y_2)) = 0$, which implies that $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced.

From the above Cases (i)-(iii), for each $\lambda = \lambda_0 + \lambda_1 \omega$ with $\lambda_1 \neq 0$, there exists at least one nonzero $a = a_0 + a_1 \omega \in \mathbb{F}_q$ such that $\text{Tr}_1^k(\lambda x^d + \lambda(x+a)^d + ax) = \text{Tr}_1^k(G(x_0, x_1))$ is not balanced.

In the following we assume that $\lambda_1 = 0$ and $\lambda = \lambda_0 + \lambda_1 \omega = \lambda_0 \neq 0$. Let $a_1 = 0$. Then

$$\begin{aligned} \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} &= \sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_0 a_0 x_1^3 + \lambda_0 a_0^2 x_1^2 + a_0 x_1)} \\ &= 2^k \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_0 a_0 x_1^3 + \lambda_0 a_0^2 x_1^2 + a_0 x_1)} \\ &= 2^k \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(\lambda_0 a_0 x_1^3 + (\lambda_0^{2^{k-1}} a_0 + a_0) x_1)}. \end{aligned} \tag{C7}$$

Since k is odd, then $\gcd(3, 2^k - 1) = 1$. Let $\lambda_0 = r^3, a_0 = t^3$, then from (C7), one gets

$$\sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} = 2^k \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(x_1^3 + (r^{3 \cdot 2^{k-1}} + 1) r^{-1} t^2 x_1)}.$$

Thus, if $\lambda_0 = r^3 \neq 1$, then $r^{3 \cdot 2^{k-1}} + 1 \neq 0$. We claim that for any $r \in \mathbb{F}_q^*$ and $r \neq 1$, there must exist some $a_0 \in \mathbb{F}_q^*$ such that $\sum_{x_0, x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(G(x_0, x_1))} = 2^k \sum_{x_1 \in \mathbb{F}_q} (-1)^{\text{Tr}_1^k(x_1^3 + (r^{3 \cdot 2^{k-1}} + 1) r^{-1} t^2 x_1)} \neq 0$, i.e., $\text{Tr}_1^k(G(x_0, x_1))$ is not balanced. Otherwise, the Walsh-Hadamard transform of $\text{Tr}_1^k(x^3)$ at any point $t \in \mathbb{F}_q$ is zero, which contradicts with Parseval's theorem¹⁾.

Therefore, if $\text{Tr}_1^n(\lambda x^d)$ is negabent on \mathbb{F}_q , then λ has to be in \mathbb{F}_2 . Zhou and Qu [8, Theorem 6] proved that if $\lambda \in \mathbb{F}_2$, then $\text{Tr}_1^n(\lambda x^d)$ is indeed negabent on \mathbb{F}_q . \square

1) Parseval's theorem shows that for any Boolean function $f(x)$ from \mathbb{F}_q to \mathbb{F}_2 , its Walsh-Hadamard transform $W_f(u)$ satisfies $\sum_{u \in \mathbb{F}_q} (W_f(u))^2 = 2^{2k}$.