1 The proof of Theorem 1

Proof. According to Lemma 1, $f(x) = x^{r+s}g(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if both $\gcd(r+s, q-1) = 1$ and $x^{r+s}g(x)^{q-1}$ permutes μ_{q+1}. Thus, we only need to prove the permutation property of the polynomial $x^{r+s}g(x)^{q-1}$ over μ_{q+1}.

By substituting $g(x) = g_1(x)g_2(x)$ into $x^{r+s}g(x)^{q-1}$, we can obtain

$$x^{r+s}g(x)^{q-1} = x^{r+s}\frac{g(x)^q}{g(x)} = x^{r+s}\frac{(g_1(x)g_2(x))^q}{g_1(x)g_2(x)}. \tag{1}$$

Since $x^q = x^{-1}$ over μ_{q+1} and $a_i^q = a_{s-i}$, it follows that

$$x^s g_2(x)^q = x^s(\sum_{i=0}^{s} a_i x^i)^q = \sum_{i=0}^{s} a_i^q x^{s+qi} = \sum_{i=0}^{s} a_{s-i}x^{s-i} = g_2(x). \tag{2}$$

According to the equation (1) and the equation (2), we can get

$$x^{r+s}g(x)^{q-1} = x^{r+s}\frac{g_1(x)^q g_2(x)^q}{g_1(x)g_2(x)} = x^r\frac{g_1(x)^q g_2(x)}{g_1(x)g_2(x)}.$$

Note that $g_2(x)$ has no root in μ_{q+1}. Then,

$$x^{r+s}g(x)^{q-1} = x^r\frac{g_1(x)^q}{g_1(x)} = x^r g_1(x)^{q-1}.$$

Since $x^r g_1(x)^{q-1}$ permutes μ_{q+1}, it follows that $x^{r+s}g(x)^{q-1}$ permutes μ_{q+1}. The proof is complete. □

2 The proof of Theorem 2

Proof. According to Lemma 1, $f(x) = x^{r-s}g(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if both $\gcd(r-s, q-1) = 1$ and $x^{r-s}g(x)^{q-1}$ permutes μ_{q+1}. Similar to the proof of Theorem 1, we only need to prove the permutation property of the polynomial $x^{r-s}g(x)^{q-1}$ over μ_{q+1}.

According to the proof of Theorem 1, the equation $x^s g_2(x)^q = g_2(x)$ holds. Since $g(x) = g_1(x)g_2(x)$ and $g_2(x)$ has no root in μ_{q+1}, it follows that

$$\begin{aligned} x^{r-s}g(x)^{q-1} &= x^{r-s}\frac{g(x)^q}{g(x)} = x^{r-s}\frac{g_1(x)^q g_2(x)}{g_1(x)g_2(x)^q} \\ &= x^r\frac{g_1(x)^q g_2(x)}{g_1(x)g_2(x)} = x^r g_1(x)^{q-1}. \end{aligned}$$

Since $x^r g_1(x)^{q-1}$ permutes μ_{q+1}, it follows that $x^{r-s}g(x)^{q-1}$ permutes μ_{q+1}. The proof is complete. □

3 The proof of Theorem 3

Proof. Denote $x^{2^k+1} + x + 1$ and $x^{2s} + x^s + 1$ by $g_1(x)$ and $g_2(x)$, respectively. Then the polynomial $h_1(x) = g_1(x)g_2(x)$.

Firstly, we will prove that $g_2(x)$ has no root in μ_{2^m+1}. Assume that there exists $\alpha \in \mu_{2^m+1}$ such that $\alpha^2 + \alpha + 1 = 0$. Then it is obvious that $\alpha \neq 0$ and $\alpha \neq 1$. By substituting $\alpha^2 = \alpha + 1$ into the equation $\alpha^2 + \alpha + 1 = 0$, we can get $\alpha(\alpha+1) + 1 = \alpha^3 + 1 = 0$. Since m is even, it follows that $\gcd(3, 2^m + 1) = 1$. Then, the equation $\alpha^3 + 1 = 0$ only has one solution $\alpha = 1$ in μ_{2^m+1}, which is contradict to $\alpha \neq 1$. Thus, the equation $x^2 + x + 1 = 0$ has no solution in μ_{2^m+1}. For all $x \in \mu_{2^m+1}, x^s \in \mu_{2^m+1}$, thus $g_2(x) = x^{2s} + x^s + 1 = 0$ has no solution in μ_{2^m+1}.

Now we will prove that $x^{2^k+1}g_1(x)^{2^m-1}$ permutes μ_{2^m+1}. Since $\gcd(2^k-1, 2^m+1) = 1$, it follows that $x^{2^k+1}g_1(x)^{2^m-1} = \frac{x^{2^k+1}+x^{2^k}+1}{x^{2^k+1}+x+1}$ permutes μ_{2^m+1} by Lemma 2.

Since $g_2(x)$ has no root in μ_{2^m+1} and $x^{2^k+1}g_1(x)^{2^m-1}$ permutes μ_{2^m+1}, the polynomial $f_1(x) = x^{2^k+2s+1}h_1(x^{2^m-1})$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\gcd(2^k + 2s + 1, 2^m - 1) = 1$ according to Theorem 1. The proof is complete. □

4 The proof of Theorem 4

Proof. Denote $x^{2^k} + x + 1$ and $x^{2s} + x^s + 1$ by $g_1(x)$ and $g_2(x)$, respectively. Then the polynomial $h_2(x) = g_1(x)g_2(x)$.

According to the proof of Theorem 3, the equation $g_2(x) = x^{2s} + x^s + 1 = 0$ has no solution in μ_{2^m+1}. Since $\gcd(2^k + 1, 2^m + 1) = 1$, it follows that $x^{2^k+1}g_1(x)^{2^m-1} = \frac{x^{2^k+1}+x^{2^k}+x}{x^{2^k}+x+1}$ permutes μ_{2^m+1} by Lemma 3.

Therefore, the polynomial $f_2(x) = x^{2^k+2s+1}h_2(x^{2^m-1})$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\gcd(2^k + 2s + 1, 2^m - 1) = 1$ by Theorem 1. The proof is complete. □

5 The proof of Theorem 5

Proof. Denote $x^2 + x + 1$ by $g_2(x)$. According to the proof of Theorem 3, the equation $g_2(x) = x^2 + x + 1 = 0$ has no solution in μ_{2^m+1}. Now consider two cases.

Case 1: k is even.

Denote $x^{2^k+1} + x + 1$ by $g_1(x)$. Then $h_3(x) = g_1(x)/g_2(x)$ because k is even. Since $\gcd(2^k - 1, 2^m + 1) = 1$, it follows that $x^{2^k+s(2^m+1)+1}g_1(x)^{2^m-1} = x^{2^k+1}g_1(x)^{2^m-1} = \frac{x^{2^k+1}+x^{2^k}+1}{x^{2^k+1}+x+1}$ permutes μ_{2^m+1} by Lemma 2.

Case 2: k is odd.

Denote $x^{2^k} + x + 1$ by $g_1(x)$. Then $h_3(x) = g_1(x)/g_2(x)$ because k is odd. Since $\gcd(2^k + 1, 2^m + 1) = 1$, it follows that $x^{2^k+s(2^m+1)+1}g_1(x)^{2^m-1} = x^{2^k+1}g_1(x)^{2^m-1} = \frac{x^{2^k+1}+x^{2^k}+x}{x^{2^k}+x+1}$ permutes μ_{2^m+1} by Lemma 3.

Therefore, the polynomial $f_3(x) = x^{2^k+s(2^m+1)-1}h_3(x^{2^m-1})$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\gcd(2^k + s(2^m + 1) - 1, 2^m - 1) = 1$ by Theorem 2.The proof is complete. □

6 The proof of Lemma 5

Proof. According to Definition 1, $v_1(x)$ is the compositional inverse of $u_1(x)$ if $u_1(v_1(x)) = v_1(u_1(x)) = x$ in μ_{2^m+1}. It is easy to conclude that $u_1(v_1(x)) = v_1(u_1(x))$ since $t \equiv -2 \pmod{2^m+1}$. Note that $x^{2^m+1} = x$ in μ_{2^m+1}. Thus,

$$\begin{aligned} u_1(v_1(x)) &= \frac{x^{t2^k+t} + x^{t2^k} + 1}{x^{t2^k+t} + x^t + 1} = \frac{x^{2^m} + x + 1}{x^{2^m} + x^{2^m-1} + 1} \\ &= \frac{x(x^{2^m-1} + 1 + x^{2^m})}{x^{2^m} + x^{2^m-1} + 1} = x. \end{aligned}$$

The proof is complete. □

7 The proof of Lemma 6

Proof. According to Definition 1, $v_2(x)$ is the compositional inverse of $u_2(x)$ if $u_2(v_2(x)) = v_2(u_2(x)) = x$ in μ_{2^m+1}. It is easy to conclude

that $u_2(v_2(x)) = v_2(u_2(x))$ since $t \equiv 2 \pmod{2^m+1}$. Note that $x^{2^m+1} = x$ in μ_{2^m+1}. Thus,

$$u_2(v_2(x)) = \frac{x^{t2^k+t} + x^{t2^k} + x^t}{x^{t2^k} + x^t + 1} = \frac{x^3 + x + x^2}{x + x^2 + 1} = \frac{x(x^2+1+x)}{x+x^2+1} = x.$$

The proof is complete. □

■ 8 The proof of Theorem 6

Proof. In the cycilc subgroup μ_{2^m+1}, the polynomial

$$x^{2^k+2s+1} h_1(x)^{2^m-1}$$

can be written as

$$\frac{(x^{2^k+1} + x^{2^k} + 1)(x^{2s} + x^s + 1)}{(x^{2^k+1} + x + 1)(x^{2s} + x^s + 1)} = \frac{x^{2^k+1} + x^{2^k} + 1}{x^{2^k+1} + x + 1}.$$

Then $f_1^{-1}(x)$ can be concluded by Lemma 4 and Lemma 5. The proof is complete. □

■ 9 The proof of Theorem 7

Proof. Similar to the proof of theorem 6, the polynomial

$$x^{2^k+2s+1} h_2(x)^{2^m-1}$$

can be written as

$$\frac{x^{2^k+1} + x^{2^k} + x}{x^{2^k} + x + 1}$$

over μ_{2^m+1}. Then $f_2^{-1}(x)$ can be concluded by Lemma 4 and Lemma 6. The proof is complete. □

■ 10 The proof of Theorem 8

Proof. Note that $k = 2m-1$ is odd. Similar to the proof of theorem 6, the polynomail

$$x^{2^k+s(2^m+1)-1} h_3(x)^{2^m-1}$$

can be written as

$$\frac{x^{2^k+1} + x^{2^k} + x}{x^{2^k} + x + 1}$$

over μ_{2^m+1}. Then $f_3^{-1}(x)$ can be concluded by Lemma 4 and Lemma 6. The proof is complete. □

■ 11 The proof of Theorem 9

Proof. For any positive integer n and any $\alpha, \beta \in \mathbb{F}_{2^{2m}}^*$, the polynomial $\alpha F_1(\beta x^n)$ is a monomial or a trinomial over $\mathbb{F}_{2^{2m}}$. However, there exist some k, s such that $f_1(x)$ has more terms than $\alpha F_1(\beta x^n)$. For example, let $k = 3, s = 2$, then $f_1(x) = x^{13\cdot 2^m} + x^{11\cdot 2^m+2} + x^{9\cdot 2^m+4} + x^{5\cdot 2^m+8} + x^{4\cdot 2^m+9} + x^{3\cdot 2^m+10} + x^{2\cdot 2^m+11} + x^{2^m+12} + x^{13}$ has nine terms since $m > 2$.

According to Definition 2, there exist some k, s such that $f_1(x)$ is multiplicatively inequivalent to $F_1(x)$. Similarly, it is easy to prove that there exist some k, s such that $f_1(x)$ is multiplicatively inequivalent to $F_2(x)$. The proof is complete. □

■ 12 The proof of Theorem 10

Proof. Let $k = 3, s = 2$, then $f_2(x) = x^{12\cdot 2^m+1} + x^{10\cdot 2^m+3} + x^{8\cdot 2^m+5} + x^{5\cdot 2^m+8} + x^{4\cdot 2^m+9} + x^{3\cdot 2^m+10} + x^{2\cdot 2^m+11} + x^{2^m+12} + x^{13}$ has nine terms since $m > 2$. According to the proof of Theorem 9, it is obvious that there exist some k, s such that $f_2(x)$ is multiplicatively inequivalent to $F_1(x)$ and $F_2(x)$. The proof is complete. □

■ 13 The proof of Theorem 11

Proof. Let $k = 3, s = 0$, then $f_3(x) = x^{6\cdot 2^m+1} + x^{5\cdot 2^m+2} + x^{3\cdot 2^m+4} + x^{2\cdot 2^m+5} + x^7$ has five terms since $m > 2$. According to the proof of Theorem 9, it is obvious that there exist some k, s such that $f_3(x)$ is multiplicatively inequivalent to $F_1(x)$ and $F_2(x)$. The proof is complete. □

■ 14 The proof of Theorem 12

Proof. Let w be an integer with $1 \le w \le 2^m$, then $w = \sum_{i=j+1}^{m-1} w_i 2^i + 2^j$, where $w_i \in \{0, 1\}$ and j is the minimum i such that $w_i \neq 0$. Thus, $w(2^m - 1) = \sum_{i=j+1}^{m-1} w_i 2^{i+m} + 2^j(2^m - 1 - \sum_{i=j+1}^{m-1} w_i 2^{i-j})$. Now consider the Hamming weight of $w(2^m - 1)$. It is obvious that $wt_2(\sum_{i=j+1}^{m-1} w_i 2^{i+m}) = wt_2(w) - 1$ and $wt_2(2^m - 1 - \sum_{i=j+1}^{m-1} w_i 2^{i-j}) = m - (wt_2(w) - 1)$. Since $2^{j+m+1} > 2^{j+m}$, it follows that $wt_2(w(2^m - 1)) = wt_2(w) - 1 + m - (wt_2(w) - 1) = m$. Thus, $wt_2(w(2^m - 1) + 1) \le m + 1$. Therefore, the algebraic degree of $F_1(x)$ and $F_2(x)$ is less than or equal to $m + 1$.

Let $k = 1$ and $s = 2^{2m-1} - 3$, then there exists a term $x^{2^{2m}-3}$ in $f_1(x)$. Since $wt_2(2^{2m} - 3) = 2m - 1$, the algebraic degree of $f_1(x)$ is $2m - 1$. Note that $2m - 1 > m + 1$. Thus, $f_1(x)$ has different algebraic degree from $F_1(x)$ and $F_2(x)$. The proof is complete. □

■ 15 The proof of Theorem 13

Proof. According to the proof of Theorem 12, the algebraic degree of $F_1(x)$ and $F_2(x)$ is less than or equal to $m + 1$. Let $k = 1$ and $s = 2^{2m-1} - 3$, then there exists a term $x^{2^{2m}-3}$ in $f_2(x)$. Since $wt_2(2^{2m} - 3) = 2m - 1$, the algebraic degree of $f_2(x)$ is $2m - 1$. Note that $2m - 1 > m + 1$. Thus, $f_2(x)$ has different algebraic degree from $F_1(x)$ and $F_2(x)$. The proof is complete. □

■ 16 The proof of Theorem 14

Proof. According to the proof of Theorem 12, the algebraic degree of $F_1(x)$ and $F_2(x)$ is less than or equal to $m+1$. Let $k = 2m-1$ and $s = 0$, then there exists a term $x^{2^{2m-1}-1}$ in $f_3(x)$. Since $wt_2(2^{2m-1} - 1) = 2m-1$, the algebraic degree of $f_3(x)$ is $2m-1$. Note that $2m-1 > m+1$, thus, $f_3(x)$ has different algebraic degree from $F_1(x)$ and $F_2(x)$. The proof is complete. □