On the Arithmetic of Sequences of Permutation Polynomials

Alev Topuzoğlu
(joint work with Tekgül Kalaycı and Henning Stichtenoth)
Sabancı University, İstanbul

Carleton Finite Fields eSeminar, 15 July 2020

Outline:

- A class of permutation polynomials
- Factorization, degrees of irreducible factors
- Sequences of permutation polynomials
- Number theoretic properties

We study a class of permutation polynomials F_n of $\mathbb{F}_q$, which are defined recursively as

$$F_0(x) = a_0 x + a_1 \in \mathbb{F}_q[x], a_0 \neq 0 \text{ and}$$
$$F_n(x) = F_{n-1}(x)^{q-2} + a_{n+1},\ n \geq 1,\ a_{n+1} \in \mathbb{F}_q.$$

Recall that the set of permutation polynomials over $\mathbb{F}_q$ of degree $< q$ forms a group $\mathbf{G}_P$ under composition modulo $x^q - x$. The group $\mathbf{G}_P$ is generated by the linear polynomials $ax + b$ for $a, b \in \mathbb{F}_q$, $a \neq 0$ and x^{q-2}, (L. Carlitz, 1953).

In other words, any permutation σ of $\mathbb{F}_q$, can be represented by

$F_n(x) = F_{n-1}(x)^{q-2} + a_{n+1},\ n \geq 1,\ a_{n+1} \in \mathbb{F}_q$ for some $n \geq 0$, with $F_0(x) = a_0 x + a_1 \in \mathbb{F}_q[x], a_0 \neq 0,$

i.e., there is a polynomial

$$F_n(x) = (\ldots((a_0 x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1},$$

satisfying $\sigma(c) = F_n(c)$ for all $c \in \mathbb{F}_q$, where $n \geq 0$, $a_1, a_{n+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^*$ for $i = 0, 2, \ldots, n$.

$$F_n(x) = (\ldots((a_0 x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1}$$

The polynomial $F_n(x)$ can be approximated by rational fractions in the folowing sense. The rational fraction

$$R_n(x) = \frac{\alpha_{n+1} x + \beta_{n+1}}{\alpha_n x + \beta_n},$$

with

$$\alpha_{n+2} = a_{n+2}\alpha_{n+1} + \alpha_n, \ \beta_{n+2} = a_{n+2}\beta_{n+1} + \beta_n$$

for $n \geq 0$ with $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$,

satisfies

$$F_n(c) = R_n(c), \text{ for all } c \in \mathbb{F}_q \setminus S_n,$$

where the cardinality of S_n is at most n.

Question. Consider

$$F_n(x) = (\dots((ax + a_1)^{q-2} + a_2)^{q-2} \dots + a_n)^{q-2} + a_{n+1} \in \mathbb{F}_q[x]$$

of degree $(q-2)^n$. What can one say about the irreducible factors?

Example:

Let $F_2(x) = (x^{27} + 3)^{27} - 2 \in \mathbb{F}_{29}[x]$.

$F_2(x) = (x+12)\,(x^{\mathbf{2}}+17x-1)\,(x^{\mathbf{6}}+2x^3-1)\,(x^{\mathbf{18}}+x^9-1)\,(x^{\mathbf{54}}+2x^{27}+18)$
$(x^{\mathbf{162}} + 18x^{135} + 19x^{108} + 9x^{54} + 15x^{27} + 16)\ \ (x^{\mathbf{486}} + 25x^{459} + 14x^{432} +$
$21x^{405} + 26x^{378} + 27x^{351} + 16x^{324} + 16x^{297} + 8x^{270} + 14x + 243 +$
$20x^{216} + 5x^{189} + 17x^{162} + 21x^{135} + 3x^{108} + 24x^{81} + 24x^{54} + 21x^{27} + 10)$

Let $n \geq 1$ and $a_1, \ldots, a_n \in \mathbb{F}_q$. Suppose that the integers $d_1, \ldots, d_n$ satisfy

$$d_i \geq 2 \quad \text{and} \quad \gcd(d_i, q) = \gcd(d_i, q-1) = 1 \ \text{ for } \ 1 \leq i \leq n.$$

Put

$$F_0(x) = x \quad \text{and} \quad F_i(x) = F_{i-1}(x)^{d_i} + a_i$$

Aim: Determine the degrees of the irreducible factors.

Let $Q(x)$ be an irreducible factor of $F_n(x)$ of deg $Q(x) > 1$.

Put $K = \mathbb{F}_q$, choose a root $\lambda \in \bar{K}$ of the polynomial $Q(x) \Longrightarrow$ deg $Q(x) = [K(\lambda) : K]$.

Define

$$\lambda_i = F_i(\lambda) = F_{i-1}(\lambda)^{d_i} + a_i \ \text{ for } \ i = 0, \ldots, n.$$

Hence

$$\lambda_0 = F_0(\lambda) = \lambda,$$
$$\lambda_i = \lambda_{i-1}^{d_i} + a_i, \ 1 \leq i \leq n-1,$$
$$\lambda_n = F_n(\lambda) = 0.$$

Consider

$$\mathbb{F}_q = \mathbb{F}_q(\lambda_n) = K(\lambda_n) \subseteq K(\lambda_{n-1}) \subseteq \ldots \subseteq K(\lambda_1) \subseteq K(\lambda_0) = K(\lambda).$$

$$
\begin{array}{c}
K(\lambda) = K(\lambda_0) \\
| \\
\vdots \\
| \\
K(\lambda_{i-1}) \\
| \qquad \lambda_{i-1}^{d_i} = \lambda_i - a_i \\
K(\lambda_i) \\
| \\
\vdots \\
| \\
K(\lambda_{n-1}) \\
| \\
\mathbb{F}_q = K = K(\lambda_n)
\end{array}
$$

Let $d = \operatorname{lcm}(d_1, \ldots, d_n)$, and $L = K(\omega)$, where $\omega \in \bar{K}$ is a primitive d-th root of unity.

Put $M = L \cap K(\lambda)$ and let $L(\lambda) = L \cdot K(\lambda)$.

$$
\begin{tikzcd}
 & L(\lambda) = L(\lambda_0) & \\
K(\lambda) \arrow[ur, dash] \arrow[dddddd, dash] & \vdots \arrow[u, dash] & \\
 & L(\lambda_{i-1}) \arrow[u, dash] & \lambda_{i-1}^{d_i} = \lambda_i - a_i \\
 & L(\lambda_i) \arrow[u, dash] & \\
 & \vdots \arrow[u, dash] & \\
 & L(\lambda_{n-1}) \arrow[u, dash] & \\
 & L = K(\omega) = L(\lambda_n) \arrow[u, dash] & \\
M = K(\lambda) \cap L \arrow[ur, dash] & & {[K(\lambda) : M] = [L(\lambda) : L]} \\
K = \mathbb{F}_q \arrow[u, dash] \arrow[uur, dash] & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & L(\lambda) = L(\lambda_0) \arrow[dl, dash] \arrow[d, dash] \\
K(\lambda) \arrow[dddddd, dash] & \vdots \arrow[d, dash] \\
 & L(\lambda_{i-1}) \arrow[d, dash] & \lambda_{i-1}^{d_i} = \lambda_i - a_i \\
 & L(\lambda_i) \arrow[d, dash] \\
 & \vdots \arrow[d, dash] \\
 & L(\lambda_{n-1}) \arrow[d, dash] \\
 & L = K(\omega) = L(\lambda_n) \arrow[dl, dash] \arrow[ddl, dash, "\operatorname{ord}_d(q)"] \\
M = K(\lambda) \cap L \arrow[d, dash] & & [L(\lambda) : L] | d_1 \cdot d_2 \cdot \ldots \cdot d_n \\
K = \mathbb{F}_q
\end{tikzcd}
$$

Theorem: Let

$$F_0(x) = x \quad \text{and} \quad F_i(x) = F_{i-1}(x)^{d_i} + a_i,$$

with $a_i \in \mathbb{F}_q$, $d_i \geq 2$, and

$$\gcd(d_i, q) = \gcd(d_i, q-1) = 1 \quad \textit{for} \quad 1 \leq i \leq n.$$

Put $d = \mathrm{lcm}(d_1, \dots, d_n)$. Suppose that $Q(x) \in \mathbb{F}_q[x]$ is an irreducible factor of $F_n(x)$. Then,

$$\deg Q(x) \mid d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot d_n \cdot \mathrm{ord}_d(q).$$

$$
\begin{tikzcd}
 & L(\lambda) = L(\lambda_0) \arrow[dl, dash] \arrow[d, dash] & \\
K(\lambda) \arrow[dddddd, dash] & \vdots \arrow[d, dash] & \\
 & L(\lambda_{i-1}) \arrow[d, dash] & \lambda_{i-1}^{d_i} = \lambda_i - a_i \\
 & L(\lambda_i) \arrow[d, dash] & \\
 & \vdots \arrow[d, dash] & \\
 & L(\lambda_{n-2}) \arrow[d, dash] & \\
 & L = L(\lambda_n) = L(\lambda_{n-1}) \arrow[dl, dash] \arrow[ddl, dash, "\mathrm{ord}_d(q)"] & \\
M = K(\lambda) \cap L \arrow[d, dash] & & \\
K = \mathbb{F}_q & &
\end{tikzcd}
$$

Theorem: Let

$$F_0(x) = x \quad \text{and} \quad F_i(x) = F_{i-1}(x)^{d_i} + a_i,$$

with $a_i \in \mathbb{F}_q$, $d_i \geq 2$, and

$$\gcd(d_i, q) = \gcd(d_i, q-1) = 1 \quad \textit{for} \quad 1 \leq i \leq n.$$

Put $d = \mathrm{lcm}(d_1, \ldots, d_n)$. Suppose that $Q(x) \in \mathbb{F}_q[x]$ is an irreducible factor of $F_n(x)$. Then,

$$\deg Q(x) \mid d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot \mathrm{ord}_d(q).$$

$$\deg Q(x) \mid d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot \mathrm{ord}_d(q).$$

Example:

Let $F_2(x) = (x^{27} + 3)^{27} - 2 \in \mathbb{F}_{29}[x]$.

$d = d_1 = d_2 = 27, \; ord_{27}(29) = 18$.

Degrees of the irreducible factors are: $1, 2, 6, 18, 54, 162, 486 = 18 \cdot 27$.

Theorem: Let

$$F_0(x) = x \ \text{ and } \ F_i(x) = F_{i-1}(x)^{d_i} + a_i,$$

with $a_i \in \mathbb{F}_q$, $d_i \geq 2$, and

$$\gcd(d_i, q) = \gcd(d_i, q-1) = 1 \ \ \textit{for} \ \ 1 \leq i \leq n.$$

Put $d = \mathrm{lcm}(d_1, \ldots, d_n)$. Suppose that $Q(x) \in \mathbb{F}_q[x]$ is an irreducible factor of $F_n(x)$. Then,

(i) $\deg Q(x) \mid d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot \mathrm{ord}_d(q)$.

(ii) Suppose $\deg Q(x) > 1$. Then there exists some $j \in \{1, 2, \ldots, n\}$ and a prime number $\ell \mid d_j$ such that $\mathrm{ord}_\ell(q) \mid \deg Q(x)$.

Example:
Let $F_2(x) = (x^{27} + 3)^{27} - 2 \in \mathbb{F}_{29}[x]$.
$d = d_1 = d_2 = 3^3$, $ord_3(29) = 2$.
Degrees of the irreducible factors are: $1, 2, 6, 18, 54, 162, 486$.

Let $A = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $D = (d_1, \ldots, d_n) \in \mathbb{Z}^n$, where

$$d_i \geq 2 \quad \text{and} \quad \gcd(d_i, q) = \gcd(d_i, q-1) = 1, \; 1 \leq i \leq n.$$

$$F_n^{(A,D)} := F_n(x) = (\ldots(x^{d_1} + a_1)^{d_2} \ldots + a_n)^{d_n} + a_n.$$

We introduce the sets

$$\Delta_n^{(A,D)} := \{\deg Q(x) \mid Q(x) \text{ is an irreducible factor of } F_n^{(A,D)}(x)\},$$

$$\bar{\Delta}_n^{(D)} := \bigcup_{A \in \mathbb{F}_q^n} \Delta_n^{(A,D)}.$$

$$\Delta_n^{(D)} := \{k > 1 \mid k \text{ divides } d_1 d_2 \cdots d_{n-1} \cdot \mathrm{ord}_d(q), \text{and } k \text{ is divisible by } \mathrm{ord}_\ell(q) \text{ for some prime divisor } \ell \text{ of } d\} \cup \{1\},$$

$$\Longrightarrow \bar{\Delta}_n^{(D)} \subseteq \Delta_n^{(D)}.$$

Question: How are these sets related?

$$\Delta_n^{(A,D)} = \{\deg Q(x) \mid Q(x) \text{ is an irreducible factor of } F_n^{(A,D)}(x)\},$$

$$\bar{\Delta}_n^{(D)} = \bigcup_{A \in \mathbb{F}_q^n} \Delta_n^{(A,D)}.$$

$$\Delta_n^{(D)} = \{k > 1 \mid k \text{ divides } d_1 d_2 \cdots d_{n-1} \cdot \mathrm{ord}_d(q), \text{and } k \text{ is divisible by } \mathrm{ord}_\ell(q) \text{ for some prime divisor } \ell \text{ of } d\} \cup \{1\},$$

Theorem: Let m be any divisor of d_1. Then $\mathrm{ord}_m(q) \in \bar{\Delta}_n^{(D)}$. Moreover, $\mathrm{ord}_m(q) \in \Delta_n^{(A,D)}$ for any $A \in \mathbb{F}_q^n$, satisfying $F_n^{(A,D)}(0) \neq 0$.

$$\Delta_n^{(A,D)} = \{\deg Q(x) \mid Q(x) \text{ is an irreducible factor of } F_n^{(A,D)}(x)\}.$$

Theorem: Let $A \in \mathbb{F}_q^n$ be arbitrary. Suppose $F_n^{(A,D)}$ has an irreducible factor $Q(x)$ of degree $r > 1$. Then $F_n^{(A,D)}$ has an irreducible factor $R(x)$ also with $\deg R(x) = t$, where

$$t = \frac{\mathrm{lcm}(r, \mathrm{ord}_m(q))}{f},$$

m is a divisor of d_1 and f is a divisor of $\gcd(r, \mathrm{ord}_m(q))$.
In other words, if $r \in \Delta_n^{(A,D)}$, then $t \in \Delta_n^{(A,D)}$.

Problem: If $\bar{\Delta}_n^{(D)} \subsetneq \Delta_n^{(D)}$, determine $\Delta_n^{(D)} \setminus \bar{\Delta}_n^{(D)}$, i.e., eliminate the degrees in $\Delta_n^{(D)}$, which are not in $\bar{\Delta}_n^{(D)}$ (and hence find $\bar{\Delta}_n^{(D)}$).

Theorem: Suppose that $d = \mathrm{lcm}(d_1, \ldots, d_n) = \ell \cdot e$, where ℓ is a prime number and $\ell \nmid e \cdot \mathrm{ord}_e(q)$. Let m be an integer with $\mathrm{ord}_\ell(q) \nmid m$. Then $m \cdot \ell \notin \Delta_n^{(A,D)}$ for any $A \in \mathbb{F}_q^n$.

Example:

Let $q = 683, D = (45, 15)$. Then,

$$\Delta_2^{(D)} = \{1, 2, 4, 6, 10, 12, 18, 20, 30, 60, 90, 180, \}.$$

The degrees $10, 30, 90$, can be eliminated to yield

$$S := \{1, 2, 4, 6, 12, 18, 20, 36, 60, 108\}.$$

Indeed, $\bar{\Delta}_2^{(D)} = S$.

Example:

Let $q = 59, D = (357, 357)$. Then

$$\Delta_2^{(D)} = \{1, 2, 4, 6, 8, 12, 14, 18, 24, 28, 34, 36, 42, 56, 68, 72, 84, 102,$$

$$126, 136, 168, 204, 238, 252, 306, 408, 476, 504, 612, 714, 952, 1224,$$

$$1428, 2142, 2856, 4284, 8568\}.$$

Example:

Let $q = 59, D = (357, 357)$. Then

$$\Delta_2^{(D)} = \{1, 2, 4, 6, 8, 12, 14, 18, 24, 28, 34, 36, 42, 56, 68, 72, 84, 102, 126, 136, 168, 204, 238, 252, 306, 408, 476, 504, 612, 714, 952, 1224, 1428, 2142, 2856, 4284, 8568\}.$$

$\Longrightarrow$

$$\bar{\Delta}_2^{(D)} = \{1, 2, 6, 8, 18, 24, 42, 72, 126, 136, 168, 408, 504, 1224, 2856, 8568\}.$$

If $A = (1, 45)$, then $\Delta_2^{(A,D)} = \bar{\Delta}_2^{(D)}$, while $\deg(F_2^{(A,D)}) = 127449$, and $w(F_2^{(A,D)}) = 13507$.

Example:

Let $q = 317$, $D = (3, 5, 13)$. Then,

$$\Delta_n^{(D)} = \{1, 2, 4, 6, 10, 12, 20, 30, 60\}.$$

Let $A = (19, 128, 254)$. One can eliminate $6, 10, 30$ to find

$$\Delta_3^{(A,D)} = \{1, 2, 4, 12, 20, 60\}.$$

The polynomial $F_n^{(A,D)}$ is of degree 195 and weight 196.

Let $A = \{a_i\}_{i\geq 1}$ be a sequence over $\mathbb{F}_q^*$ and $D = \{d_i\}_{i\geq 1}$ be a sequence in $\mathbb{Z}$, satisfying

$$d_i \geq 2 \quad \text{and} \quad \gcd(d_i, q) = \gcd(d_i, q-1) = 1.$$

Consider the sequence $\mathcal{F} = \mathcal{F}^{(A,D)} = \{F_i^{(A,D)}(x)\}_{i\geq 0}$, of permutation polynomials associated to the sequences A and D, which we define recursively by

$$F_0(x) = x + a_1 \quad \text{and} \quad F_i(x) = F_{i-1}(x)^{d_i} + a_{i+1} \;\; \text{for} \quad i \geq 1.$$

Questions:

- Find upper/lower bounds for the largest degree $\mathcal{D}(F_n)$ of irreducible factors of the n'th term of the sequence $\mathcal{F}$,
- Find upper/lower bounds for the number $\nu(F_n)$ of irreducible factors of the n'th term of the sequence $\mathcal{F}$.

  Let $F_n = \prod_{Q \in irr(F_n)} Q^{e_{n,Q}}$, where $irr(F_n)$ denotes the set of all irreducible factors of F_n.
- Find upper/lower bounds for the multiplicities $e_{n,Q}$, when $Q(x)$ ranges over $irr(F_n)$.
- Find upper/lower bounds for $\Sigma_{Q \in irr(F_n)} e_{n,Q}$.
- Given q, D, N. Can one construct a sequence $\mathcal{F}$ over $\mathbb{F}_q$ of N terms, such that $F_1, F_2, \ldots, F_N$ are pairwise relatively prime?

Theorem: Let $\mathcal{D}(F_n)$ be the largest degree of irreducible factors of the nth term F_n of the sequence $\mathcal{F}$. Then,

$$\mathrm{ord}_{d_n}(q) \leq \mathcal{D}(F_n) \leq d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot \mathrm{ord}_{d_n}(q).$$

A polynomial is m-smooth if the degrees of its irreducible factors are all at most m.

Recall that

$$\mathcal{D}(F_n) \leq d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} \cdot \mathrm{ord}_{d_n}(q).$$

Corollary: Let $m = d_1 \cdot d_2 \cdots d_{n-1} \cdot \mathrm{ord}_{d_n}(q)$, then $F_n^{(A,D)}$ is m-smooth for any A.

Examples:

- Let $q = 2^7, n = 4, d_1 = d_2 = d_3 = 3,\ d_4 = 129$. Then $\mathrm{ord}_{d_4}(q) = 2$, $\deg(F_4(x)) = 3483$ and $m = 54$.
- Let $q = 289, D = (5, 5, 5, 145)$. Then $\mathrm{ord}_{d_4}(q) = 2$, $\deg(F_4(x)) = 18125$ and $m = 250$.

$\rho(m) :=$ number of irreducible factors of $(T^m - 1)$ over $\mathbb{F}_q$.

Theorem: Let $\nu(F_n)$ be the number of irreducible factors of the polynomial F_n. Then,

(i) $\nu(F_n) \geq \rho(d_n)$ for all $n \geq 1$. If $F_n(-a_1) \neq 0$ then $\nu(F_n) \geq \rho(d_1)$.

(ii) For any $q > 2$ and any fixed $n \geq 1$, there is a sequence $A = \{a_i\}_{i \geq 1}$ in $\mathbb{F}_q^*$ such that

$$\nu(F_n^{(A,D)}) \geq \rho(d_1) + \sum_{i=2}^{n} (\rho(d_i) - 1) \geq n + 1.$$

Method:

Let $0 \leq i < j \leq n$. We define auxiliary polynomials $H_{i,j} \in \mathbb{F}_q[T]$ as follows.

$$H_{j-1,j}(T) = T + a_{j+1},$$

$$H_{i,j}(T) = (\ldots((T + a_{i+2})^{d_{i+2}} + a_{i+3})^{d_{i+3}} + \ldots + a_j)^{d_j} + a_{j+1} \text{ for } i \leq j-2,$$

$$\Longrightarrow$$

$$F_j = H_{i,j}(F_i^{d_{i+1}}) \text{ for } 0 \leq i < j \leq n.$$

$$H_{i,k}(T) = H_{j,k}(H_{i,j}(T)^{d_{j+1}}) \text{ for } 0 \leq i < j < k \leq n.$$

$$H_{i,j}(T) = H_{i,j-1}(T)^{d_j} + a_{j+1} \text{ for } 0 \leq i \leq j-1 < n.$$

Lemma: The following hold for $0 \leq i < j \leq n$.

(i) $\gcd(F_i, F_j) = 1$ if and only if $H_{i,j}(0) \neq 0$.

(ii) If $\gcd(F_i, F_j) \neq 1$, then $F_i^{d_{i+1}} \mid F_j$.

Theorem: Let $J \subseteq \{0, 1, ..., N\}$ and $|J| > q$. Then there exist $i, j \in J$ with $i < j$ such that $\gcd(F_i, F_j) \neq 1$ (and hence $F_i^{d_{i+1}} \mid F_j$).

Theorem: For all n with $1 \leq n \leq q-1$ and for all n-tuples $(a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, there exists an element $a_{n+1} \in \mathbb{F}_q^*$ such that $\gcd(F_i, F_n) = 1$ for all $i = 0, ..., n-1$.

Corollary: For all n with $1 \leq n \leq q-1$ and for all n-tuples $(a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, one can choose an element $a_{n+1} \in \mathbb{F}_q^*$ such that all polynomials $F_0^{(A,D)}, ..., F_n^{(A,D)}$ are squarefree, where $A = \{a_n\}_{n \geq 1}$.

Theorem: Let $Q \in \mathbb{F}_q[x]$ be an irreducible factor of F_n, and $e_{n,Q}$ be the multiplicity of Q in F_n. Put $I_{n,Q} = \{i : \ Q \mid F_i, \ 0 \leq i < n\}$. Then, either

$$e_{n,Q} = 1 \quad \textit{or} \quad e_{n,Q} = \prod_{i \in I_{n,Q}} d_{i+1}.$$

Theorem: Let $d_i = d$ for all $i \geq 1$, and

$$e_n = \max\{e_{n,Q} : Q \in \mathrm{irr}(F_n)\}.$$

Then $e_n \leq d^{\frac{n}{2}}$, if n is even, and $e_n \leq d^{\frac{n-1}{2}}$, if n is odd.

Let $G = \{G_n(x)\}_{n \geq 1}$ be a sequence in $\mathbb{F}_q[x]$. An irreducible polynomial $Q(x)$ is called a primitive irreducible divisor of $G_n,\ n \geq 2$, if $Q \mid G_n$ and $\gcd(Q, G_i) = 1$, for any $1 \leq i < n$.

Theorem: Every term F_n of the sequence $\mathcal{F}$ has a primitive irreducible divisor.

Open Problems:

- Suppose $\deg F_n = d_1 \cdots d_n < q$, and σ is the permutation induced by F_n. Is there a relation between the factorization pattern of F_n and properties of σ?
- Find conditions on A, such that $\Delta_n^{(A,D)} = \bar{\Delta}_n^{(D)}$.
- Construct sequences of length N, $N \geq 1$, such that all the irreducible factors of $F_i^{(A,D)}, \ldots, F_{i+N}^{(A,D)}$, $i \geq 1$, are of the same degree or of distinct degrees (except for the factor of degree 1).

For details of proofs and references see *"Permutation polynomials and factorization" by T. Kalaycı, H. Stichtenoth and A. Topuzoğlu*, which appeared in Cryptography and Communications; https://doi.org/10.1007/s12095-020-00446-y