On some iterative constructions of irreducible polynomials over finite fields

Simone Ugolini

University of Trento

The 13[th] International Conference on Finite Fields and their Applications
(Gaeta, 6 June 2017)

1. Iterative constructions of irreducible polynomials
2. The Q-transform and some variants
3. Transforms based on elliptic curve endomorphisms

Polynomial transforms

- Let $\mathbb{F}$ be a finite field.
- A polynomial transform T is a map

$$\begin{array}{rccc} T: & \mathbb{F}[x] & \to & \mathbb{F}[x] \\ & f & \mapsto & T(f) = f^T. \end{array}$$

- For any polynomial $f \in \mathbb{F}[x]$ we can consider its orbit

$$\{f_i\}_i := \{f_i : i \in \mathbb{N}\}$$

where $f_0 := f$ and

$$f_{i+1} := f_i^{\,T} \quad \text{for any } i \in \mathbb{N}.$$

Polynomial transforms and irreducibility

Some questions

- Can we find a transform T which preserves the irreducibility in the sequence $\{f_i\}_i$ once we know that f_0 is irreducible?
- Can we construct irreducible polynomials of large degree just by repeated applications of a transform T?

The Q-transform

Definition

If $f \in \mathbb{F}[x]$, then the Q-transform of f is

$$f^Q(x) := x^{\deg(f)} \cdot f\left(x + x^{-1}\right).$$

Remark

We notice that f^Q is a self-reciprocal polynomial of degree $2\deg(f)$.

The Q-transform

Theorem [Varshamov-Garakov (1969)]

If $f(x) = x^n + \cdots + a_1 x + a_0$ is irreducible in $\mathbb{F}_2[x]$, then f^Q is irreducible if and only if $a_1 = 1$.

Theorem [Meyn (1990)]

Let $\mathbb{F}$ be a finite field of characteristic two.
The Q-transform of a *self-reciprocal irreducible monic (srim)* polynomial $f(x) = x^n + \cdots + a_1 x + a_0$ with $\mathrm{Tr}(a_1) = 1$ is a *srim* $f^Q(x) = x^{2n} + \cdots + \tilde{a}_1 x + 1$ with $\mathrm{Tr}(\tilde{a}_1) = 1$.

Constructing irreducible polynomials via the Q-transform

A Q-transform based iterative construction [Meyn (1990)]

- Let $f_0(x) := x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ be an irreducible polynomial in $\mathbb{F}_2[x]$ with
$$a_{n-1} = a_1 = 1.$$
- The polynomials of the sequence $\{f_i\}_i$, where $f_{i+1} := f_i^Q$ for any $i \in \mathbb{N}$, are irreducible and $\deg(f_{i+1}) := 2\deg(f_i)$ for any i.

Question

What can we say if the condition $a_{n-1} = a_1 = 1$ does not hold?

Constructing irreducible polynomials via the Q-transform

A patched Q-transform based construction (Ugolini, 2013)

- If $f \in \mathbb{F}_2[x]$ is irreducible, then either f^Q is irreducible or it is the product of two equal-degree irreducible polynomials.
- If f_0 is irreducible in $\mathbb{F}_2[x]$, then we can set f_{i+1} equal to one of the at most two irreducible factors of f_i^Q for any $i \in \mathbb{N}$.
- After a finite number of steps we get an irreducible polynomial

$$f_j(x) = x^m + 1 \cdot x^{m-1} + \cdots + 1 \cdot x + 1$$

of positive degree m.

- Setting $f_{h+1} := f_h^Q$ for any $h \geq j$ we get an infinite sequence of increasing degree irreducible polynomials.

Constructing irreducible polynomials via the Q-transform

A patched Q-transform based construction: some remarks

- The number of factorizations required in the construction is bounded by $\ell + 3$, where ℓ is a non-negative integer such that 2^ℓ is the greatest power of 2 which divides the degree of f_0.
- The bound has been obtained relying upon the structure of the graphs associated with the map $\vartheta(x) = x + x^{-1}$ over finite fields of characteristic two (Ugolini, 2012).
- The map ϑ is involved in the definition of an endomorphism of the Koblitz curve having equation

$$y^2 + xy = x^3 + 1 \quad \text{over } \mathbb{F}_2.$$

Variants of the Q-transform

From Meyn's paper (1990)

When p is an odd prime the conditions under which an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ generates an infinite sequence of irreducible polynomials by iterated application of Q are much more complicated.

Variants of the Q-transform

Some variants

- Let $\mathbb{F}$ be a finite field of odd characteristic and f a polynomial in $\mathbb{F}[x]$.
- Cohen (1992) proposed an iterative construction of irreducible polynomials based on the transform

$$f^R(x) = (2x)^{\deg(f)} \cdot f\left(\frac{1}{2}(x + x^{-1})\right)$$

- Other quadratic transforms have been proposed (see for examples the papers by Kyuregyan (2003, 2006)).

Endomorphism based transforms

- The map $\vartheta(x) = x + x^{-1}$, upon which the Q-transform is based, is involved in the definition of an endomorphism of an elliptic curve over $\mathbb{F}_2$.
- Certain maps $\vartheta_k(x) = k \cdot (x + x^{-1})$ are also involved in the definition of endomorphisms of elliptic curves over fields of odd characteristic p, with some restrictions on p and the constant k.
- The maps ϑ_k can be used to define the Q_k-transforms

$$f^{Q_k}(x) = \left(\frac{x}{k}\right)^{\deg(f)} \cdot f(\vartheta_k(x))$$

  which can be used to produce infinite sequences of (finally) increasing degree (Ugolini (2015)).

Endomorphism based transforms

- The rational maps so far presented are quadratic and are involved in the definitions of endomorphisms of degree 2.
- Using such maps we can produce sequences of polynomials $\{f_i\}_i$ such that (finally)

$$\deg(f_{i+1}) = 2 \cdot \deg(f_i).$$

- More in general (see Ugolini (2017)) we can employ rational maps involved in the definition of endomorphisms of odd prime degree ℓ and produce sequences $\{f_i\}_i$ of irreducible polynomials such that (finally)

$$\deg(f_{i+1}) = \ell \cdot \deg(f_i).$$

Endomorphism based transforms

An endomorphism based iterative construction (1)

- Let $\mathbb{F}$ be a finite field of odd characteristic and E an elliptic curve over $\mathbb{F}$ (more restrictions apply).
- Let $\alpha(x,y) := (r(x), y \cdot s(x))$ be an endomorphism of E having odd prime degree ℓ, where $r(x) = \frac{a(x)}{b(x)}$ for certain polynomials $a(x)$ and $b(x)$ in $\mathbb{F}[x]$.
- For any polynomial $g \in \mathbb{F}[x]$ let

$$g^r(x) := (b(x))^{\deg(g)} \cdot g(r(x)).$$

- Let f_0 be an irreducible polynomial having positive degree d over $\mathbb{F}$.

Endomorphism based transforms

An endomorphism based iterative construction (2)

- Define f_{i+1} equal to one of the irreducible factors of f_i^r for any $i \in \mathbb{N}$.
- There exists a positive integer j such that f_{j+1} has degree $\tilde{d}\ell$, where $\tilde{d} \in \{d, 2d\}$.
- For any positive integer h we have that f_{j+h} is irreducible and has degree $\tilde{d}\ell^h$.

References I

S.D.Cohen
The explicit construction of irreducible polynomials over finite fields
Des. Codes Cryptogr., 2: 169–174, 1992.

M.K. Kyuregyan
Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristic
Finite Fields Appl., 9 (1): 39–58, 2003.

M.K. Kyuregyan
Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristic. II
Finite Fields Appl., 12 (3): 357–378, 2006.

References II

H.Meyn
On the construction of irreducible self-reciprocal polynomials over finite fields
AAECC, 1: 43–53, 1990.

S. Ugolini
Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two
Theory and Applications of Finite Fields, Contemp. Math., 579 (2012): 187–204, 2012.

S. Ugolini
Sequences of binary irreducible polynomials
Discrete Math., 313: 2656–2662, 2013.

References III

S. Ugolini
Sequences of irreducible polynomials over odd prime fields via elliptic curve endomorphisms
J. Number Theory, 152: 21–37, 2015.

S. Ugolini
On the construction of irreducible polynomials over finite fields via odd prime degree endomorphisms of elliptic curves
to appear in *Periodica Math. Hungarica*, 2017.

R.R. Varshamov, G. A. Garakov
On the theory of selfdual polynomials over a Galois field
Bull. Math. Soc. Sci. Math. R. S. Roumanie, 13: 403–415, 1969.