Simone Ugolini

On an iterated construction of irreducible polynomials over finite fields of even characteristic by Kyuregyan

Czechoslovak Mathematical Journal, Vol. 66 (2016), No. 1, 243–250

Persistent URL: http://dml.cz/dmlcz/144889

Czechoslovak Mathematical Journal, 66 (141) (2016), 243–250

ON AN ITERATED CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS OF EVEN CHARACTERISTIC BY KYUREGYAN

Simone Ugolini, Trento

(Received April 26, 2015)

Abstract. We deal with the construction of sequences of irreducible polynomials with coefficients in finite fields of even characteristic. We rely upon a transformation used by Kyuregyan in 2002, which generalizes the Q-transform employed previously by Varshamov and Garakov (1969) as well as by Meyn (1990) for the synthesis of irreducible polynomials. While in the iterative procedure described by Kyuregyan the coefficients of the initial polynomial of the sequence have to satisfy certain hypotheses, in the present paper these conditions are removed. We construct infinite sequences of irreducible polynomials of non-decreasing degree starting from any irreducible polynomial.

Keywords: finite field; irreducible polynomial; iterative construction

MSC 2010: 11R09, 11T55, 12E05

1. Introduction

In the last decades many investigators dealt with the iterative construction of sequences of irreducible polynomials of non-decreasing degree with coefficients over finite fields. A survey of works related to such a topic can be found in [6], Section 3.2.

One of the possible iterative constructions relies on the so-called Q-transform, which takes any polynomial f of positive degree n to $f^Q(x) = x^n f(x+x^{-1})$. Among others, the construction of irreducible polynomials via the Q-transform was studied by Varshamov and Garakov [10] and later by Meyn [5].

Adopting the notation of [5], the reciprocal f^* of a polynomial f of degree n is the polynomial $f^*(x) = x^n f(1/x)$. If $f = f^*$, then f is self-reciprocal. In general, the Q-transform f^Q of any polynomial f is self-reciprocal.

If α is an element of the field $\mathbb{F}_{2^n}$ with 2^n elements for some positive integer n, then the absolute trace of α is

$$\mathrm{Tr}_n(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}.$$

We remind the reader that $\mathrm{Tr}_n(\alpha) \in \{0, 1\}$.

The following result plays a crucial role for the synthesis of sequences of irreducible polynomials over finite fields of even characteristic.

Theorem 1.1 ([5], Theorem 9)**.** *The Q-transform of a self-reciprocal irreducible monic polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_1 x + 1 \in \mathbb{F}_{2^k}[x]$ with $\mathrm{Tr}_k(a_1) = 1$ is a self-reciprocal irreducible monic polynomial of the same kind, i.e., $f^Q(x) = x^{2n} + \widetilde{a}_1 x^{2n-1} + \ldots + \widetilde{a}_1 x + 1$ satisfies $\mathrm{Tr}_k(\widetilde{a}_1) = 1$.*

Relying upon Theorem 1.1 Meyn shows, after [5], Example 3, page 50, how to construct iteratively a sequence $\{f_i\}_{i \geqslant 0}$ of irreducible polynomials in $\mathbb{F}_2[x]$, starting from any monic irreducible polynomial $f_0 = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}_2[x]$ such that $a_{n-1} = a_1 = 1$. The polynomials of the sequence are inductively defined as $f_i := f_{i-1}^Q$ for any positive integer i. Moreover, according to Theorem 1.1, the degree of f_i is twice the degree of f_{i-1} for any positive integer i.

In the same paper, Meyn noticed that the Q-transform was not suitable for the iterative construction of irreducible polynomials over finite fields of odd characteristic. Indeed, he was not able to find easy conditions upon which starting from an irreducible polynomial a sequence of irreducible polynomials could be generated.

For that reason Cohen [1] defined the so-called R-transform, which is obtained by a slight modification of the Q-transform, and proved that a sequence of irreducible polynomials could be produced by means of repeated applications of such a transform starting from any irreducible polynomial satisfying certain conditions on the coefficients.

Later, in [7] we analysed how the R-transform behaves when any additional condition on the initial irreducible polynomial is removed.

In [8] we concentrated on the construction of sequences of irreducible polynomials with coefficients in $\mathbb{F}_2$ removing any assumption on the coefficients of the initial polynomial of the sequence. The drawback of relaxing the hypotheses on the initial polynomial is that we could face a finite number of factorizations of a polynomial in two equal-degree polynomials in $\mathbb{F}_2[x]$. The number of factorizations depends on the greatest power of 2 which divides the degree of the initial polynomial of the sequence, as explained in [8], Section 3.2.

In [4] Kyuregyan introduced a more general construction of sequences of irreducible polynomials having coefficients in finite fields of even characteristic. Such a construction is based on the transformations which take a polynomial f of degree n to the polynomial $x^n f(x+\delta^2 x^{-1})$ for some nonzero element δ in the field of the coefficients of f. For the sake of clarity we introduce a notation for this family of transformations.

Definition 1.2. If f is a polynomial of a positive degree n in $\mathbb{F}_{2^s}[x]$ for some positive integer s, and $\alpha \in \mathbb{F}_{2^s}^*$, then the (Q,α)-transform of f is

$$f^{(Q,\alpha)}(x) = x^n f(x+\alpha x^{-1}).$$

Remark 1.3. For $\alpha = 1$ the (Q,α)-transform coincides with the Q-transform.

The forthcoming theorem proved by Kyuregyan [4] furnishes an iterative procedure for constructing sequences of irreducible polynomials with coefficients in finite fields of even characteristic. The procedure is based on the (Q,α)-transforms and requires that some hypotheses on the initial polynomial of the sequence be satisfied. We state [4], Theorem 3, using the notation introduced in the present paper. Actually, we adapt the statement of the theorem as presented in [3].

Theorem 1.4 ([3], Proposition 3)**.** *Let $\delta \in \mathbb{F}_{2^s}^*$ and let $F_1(x) = \sum_{u=0}^{n} c_u x^u$ be an irreducible polynomial over $\mathbb{F}_{2^s}$ whose coefficients satisfy the conditions*

$$\mathrm{Tr}_s\left(\frac{c_1\delta}{c_0}\right) = 1 \quad \textit{and} \quad \mathrm{Tr}_s\left(\frac{c_{n-1}}{\delta}\right) = 1.$$

Then all members of the sequence $(F_k(x))_{k\geqslant 1}$ defined by

$$F_{k+1}(x) = F_k^{(Q,\delta^2)}(x), \quad k \geqslant 1$$

are irreducible polynomials over $\mathbb{F}_{2^s}$.

In the present paper we aim at constructing sequences of irreducible polynomials $\{f_k\}_{k\geqslant 0}$, where the initial polynomial f_0 of the sequence is monic and irreducible, but the other hypotheses of [3], Proposition 3, are removed. To do that, we rely on the dynamics of the maps

$$\theta_\alpha\colon\ x \mapsto \begin{cases} \infty & \text{if } x \in \{0,\infty\}, \\ x+\alpha x^{-1} & \text{otherwise} \end{cases}$$

over $\mathbf{P}^1(\mathbb{F}_{2^s}) = \mathbb{F}_{2^s} \cup \{\infty\}$ for any positive integer s and any choice of $\alpha \in \mathbb{F}_{2^s}^*$.

Actually, the dynamics of the maps θ_α is strictly related to the dynamics of the map θ_1, studied by us in [9]. Consider in fact the bijective map defined over $\mathbf{P}^1(\mathbb{F}_{2^s}) = \mathbb{F}_{2^s} \cup \{\infty\}$ for any positive integer s and for any $\gamma \in \mathbb{F}_{2^s}^*$, as follows:

$$\psi_\gamma \colon x \mapsto \begin{cases} \infty & \text{if } x = \infty, \\ \gamma x & \text{otherwise.} \end{cases}$$

If $\gamma = \sqrt{\alpha}$, namely γ is the square root of α for a generic element $\alpha \in \mathbb{F}_{2^s}^*$, then

$$\theta_\alpha = \psi_\gamma \circ \theta_1 \circ \psi_{\gamma^{-1}}. \tag{1.1}$$

We can construct a graph $\mathrm{Gr}_s(\alpha)$ related to the dynamics of the map θ_α over $\mathbf{P}^1(\mathbb{F}_{2^s})$ as in [9]. The vertices of the graph are labelled by the elements of $\mathbf{P}^1(\mathbb{F}_{2^s})$ and an arrow joins a vertex β_1 to a vertex β_2 if $\beta_2 = \theta_\alpha(\beta_1)$.

We notice that the graph $\mathrm{Gr}_s(1)$ is isomorphic to $\mathrm{Gr}_s(\alpha)$. Indeed, if δ_1 and δ_2 are two adjacent vertices in $\mathrm{Gr}_s(1)$, namely $\delta_2 = \theta_1(\delta_1)$, then

$$\theta_\alpha(\psi_\gamma(\delta_1)) = \psi_\gamma(\theta_1(\delta_1)) = \psi_\gamma(\delta_2)$$

according to (1.1), namely $\psi_\gamma(\delta_1)$ and $\psi_\gamma(\delta_2)$ are adjacent in $\mathrm{Gr}_s(\alpha)$.

As in [9] we say that an element $\beta \in \mathbf{P}^1(\mathbb{F}_{2^s})$ is θ_α-periodic if $\theta_\alpha^i(\beta) = \beta$ for some positive integer i. If β is θ_α-periodic, then the vertex β in $\mathrm{Gr}_s(\alpha)$ belongs to a cycle whose length is equal to the smallest of the positive integers i such that $\theta_\alpha^i(\beta) = \beta$.

If for some $\beta \in \mathbf{P}^1(\mathbb{F}_{2^s})$ there is no positive integer i such that $\theta_\alpha^i(\beta) = \beta$, then we say that β is non-θ_α-periodic. Nevertheless, since $\mathbf{P}^1(\mathbb{F}_{2^s})$ is finite, there exist two positive integers d and e such that

$$\theta_\alpha^d(\beta) = \theta_\alpha^{d+e}(\beta).$$

For this reason, any non-θ_α-periodic element in $\mathbf{P}^1(\mathbb{F}_{2^s})$ is preperiodic, namely some iterate $\theta_\alpha^i(\beta)$ is θ_α-periodic. In particular, if β is a non-θ_α-periodic element of $\mathbf{P}^1(\mathbb{F}_{2^s})$ and t is the smallest of the positive integers i such that $\theta_\alpha^i(\beta)$ is θ_α-periodic, then the vertex β belongs to the level t of a reversed binary tree rooted at $\theta_\alpha^t(\beta)$ in $\mathrm{Gr}_s(\alpha)$.

The paper is organized as follows: in Section 2 we briefly describe some properties of the graphs $\mathrm{Gr}_s(\alpha)$ and in Section 3 we study the sequences of irreducible polynomials generated by the iterations of the (Q, α)-transforms.

We note that, while the current setting is more general than [8], in the proofs of the current paper we can still employ the same arguments as in [8].

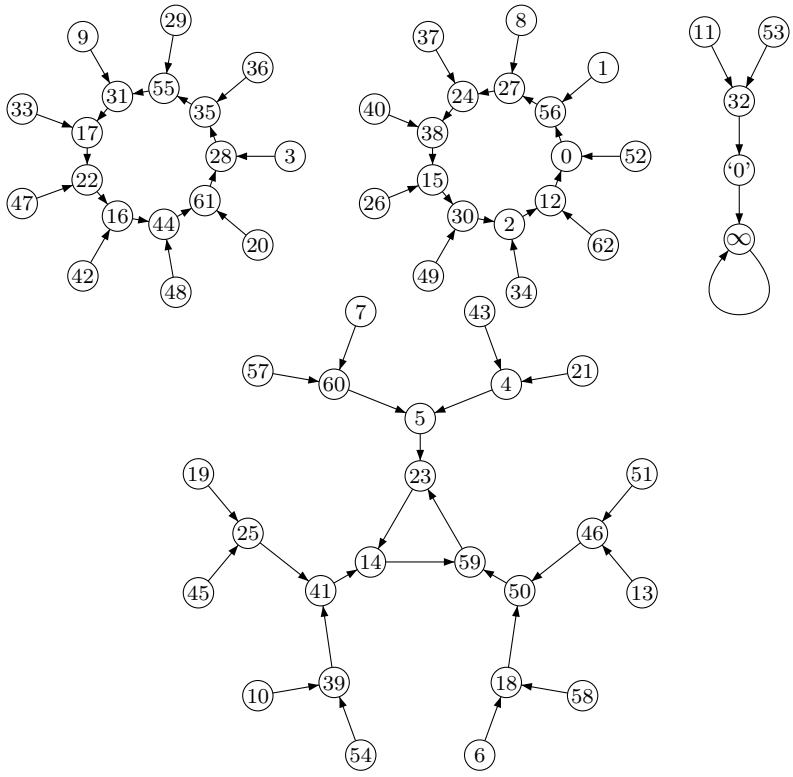
2. The structure of the graphs $\mathrm{Gr}_s(\alpha)$

Since all graphs $\mathrm{Gr}_s(\alpha)$ are isomorphic to $\mathrm{Gr}_s(1)$, from [9] we deduce the following, for a chosen element $\alpha \in \mathbb{F}_{2^s}^*$:

- ▷ every connected component of $\mathrm{Gr}_s(\alpha)$ is formed by a cycle whose vertices are roots of binary trees of the same depth;
- ▷ either all the trees of a connected component of $\mathrm{Gr}_s(\alpha)$ have depth 1 or they have depth $l+2$, where l is positive integer such that 2^l is the greatest power of 2 which divides s (see [9], Lemma 4.3, Lemma 4.4).

Example 2.1. In this example we construct the graph $\mathrm{Gr}_6(\alpha)$, where α is a root of the Conway polynomial $x^6+x^4+x^3+x+1$, which is primitive in $\mathbb{F}_2[x]$. The labels of the vertices are ∞, "0" (the zero of $\mathbb{F}_2$) and the exponents i of the powers α^i for $0 \leqslant i \leqslant 62$.

We notice that the graph $\mathrm{Gr}_6(\alpha)$ is isomorphic to the graph $\mathrm{Gr}_6(1)$, which the reader can find in [8], Example 4.2. Since the greatest power of 2 dividing 6 is 1, the trees belonging to a connected component of $\mathrm{Gr}_6(\alpha)$ either have depth 3 or 1.



3. The synthesis of irreducible polynomials via the (Q, α)-transforms

The following lemma about the irreducibility of the polynomials $f^{(Q,\alpha)}$ holds in analogy with [5], Lemma 4.

Lemma 3.1. *If f is an irreducible monic polynomial of degree n in $\mathbb{F}_{2^s}[x]$ for some positive integers n and s, and $\alpha \in \mathbb{F}_{2^s}^*$, then either $f^{(Q,\alpha)}$ is an irreducible monic polynomial of degree $2n$ in $\mathbb{F}_{2^s}[x]$ or $f^{(Q,\alpha)}$ splits into the product of a pair of irreducible monic polynomials g_1, g_2 of degree n in $\mathbb{F}_{2^s}[x]$. In the latter case at least one of g_1 and g_2 has no θ_α-periodic roots.*

P r o o f. Let $\beta \in \mathbb{F}_{2^{sn}}$ be a root of f and γ a solution of the equation $\theta_\alpha(x) = \beta$. Then $f^{(Q,\alpha)}(\gamma) = \gamma^n f(\gamma + \alpha\gamma^{-1}) = 0$. Since $\theta_\alpha(\gamma) = \beta$, either γ belongs to $\mathbb{F}_{2^{sn}}$ or γ belongs to $\mathbb{F}_{2^{2sn}} \setminus \mathbb{F}_{2^{sn}}$. In the latter case $f^{(Q,\alpha)}$ is irreducible of degree $2n$ over $\mathbb{F}_{2^s}$, while in the former case $f^{(Q,\alpha)}$ splits into the product of a pair of irreducible monic polynomials g_1, g_2 of degree n.

Suppose now that $f^{(Q,\alpha)}(x) = g_1(x)g_2(x)$, where g_1 and g_2 have degree n. We proceed by proving that one of g_1 and g_2 has no θ-periodic roots. First we notice that $\theta_\alpha(x) = \beta$ if and only if $x \in \{\gamma, \alpha\gamma^{-1}\}$. If β is not θ_α-periodic, then the same holds for γ too. If β is θ_α-periodic then, up to a renaming, γ belongs to the first level of the binary tree of $\mathrm{Gr}_{sn}(\alpha)$ rooted in β. Since $f^{(Q,\alpha)}(\gamma) = 0$, we conclude that either $g_1(\gamma) = 0$ or $g_2(\gamma) = 0$.

Suppose, without loss of generality, that $g_1(\gamma) = 0$. If δ is any root of g_1, then $\gamma = \delta^{2^{si}}$ for some integer i. Therefore, $\theta_\alpha^k(\delta) = \delta$ for some positive integer k if and only if $(\theta_\alpha^k(\delta))^{2^{si}} = \delta^{2^{si}} = \gamma$. Since $(\theta_\alpha^k(\delta))^{2^{si}} = \theta_\alpha^k(\gamma)$, we conclude that δ is θ_α-periodic if and only if γ is θ_α-periodic. Hence, none of the roots of g_1 is θ_α-periodic. □

The following theorem describes the iterative procedure for the construction of irreducible polynomials over finite fields of even characteristic via the (Q, α)-transforms.

Theorem 3.2. *Let $f_0 \in \mathbb{F}_{2^s}[x]$, where s is a positive integer, be an irreducible monic polynomial of positive degree n. Suppose that 2^{l_s} is the greatest power of 2 which divides s, while 2^{l_n} is the greatest power of 2 which divides n. Fix an element α in $\mathbb{F}_{2^s}^*$.*

Let f_1 be one of the at most two irreducible monic polynomials which factor $f_0^{(Q,\alpha)}$. Suppose also that the roots of f_1 are not θ_α-periodic.

Consider the sequence of polynomials $\{f_i\}_{i \geqslant 0}$ constructed inductively setting f_i equal to one of the irreducible monic factors of $f_{i-1}^{(Q,\alpha)}$ for $i \geqslant 2$.

Then there exists a positive integer $t \leqslant l_s + l_n + 3$ such that f_t has degree $2n$, while f_{t+1} has degree $4n$. Moreover, for any $i \geqslant t$, the polynomial $f_i^{(Q,\alpha)}$ is irreducible in $\mathbb{F}_{2^s}[x]$ and the degree of f_{i+1} is twice the degree of f_i.

P r o o f. Since f_0 is an irreducible polynomial of degree n in $\mathbb{F}_{2^s}[x]$, all its roots are in $\mathbb{F}_{2^{sn}}$. Let $\beta_0 \in \mathbb{F}_{2^{sn}}$ be a root of f_0. Then it is possible to construct inductively a sequence of elements $\{\beta_i\}_{i\geqslant 0}$, where any β_i belongs to an appropriate extension of $\mathbb{F}_{2^{sn}}$, such that

▷ any β_i is a root of f_i;
▷ $\beta_i = \theta_\alpha(\beta_{i+1})$.

Since $\beta_0 \in \mathbb{F}_{2^{sn}}$ and β_1 is not θ_α-periodic, all the elements β_i for $i \geqslant 1$, belong to a tree of the graph $\mathrm{Gr}_{2sn}(\alpha)$. In particular, such a tree has depth at least 2 in $\mathrm{Gr}_{2sn}(\alpha)$. Indeed, there are two possibilities for β_1: either $\beta_1 \in \mathbb{F}_{2^{sn}}$ or $\beta_1 \in \mathbb{F}_{2^{2sn}} \setminus \mathbb{F}_{2^{sn}}$. In the former case β_1 lies on a level not smaller than 1 of a tree in $\mathrm{Gr}_{sn}(\alpha)$ and consequently β_2 lies on a level not smaller than 2 of a tree in $\mathrm{Gr}_{2sn}(\alpha)$. In the latter case, β_0 is a leaf of a tree in $\mathrm{Gr}_{sn}(\alpha)$. Such a tree has depth at least 1.

Consequently, β_2 lies on a level not smaller than 2 of a tree in $\mathrm{Gr}_{2sn}(\alpha)$. In both cases we conclude that such a tree has not depth 1 in $\mathrm{Gr}_{2sn}(\alpha)$, namely it has depth $(1 + l_n + l_s) + 2$ in $\mathrm{Gr}_{2sn}(\alpha)$ (see Section 2). Hence, there exists a positive integer $t \leqslant l_n + l_s + 3$ such that $\beta_t \in \mathbb{F}_{2^{2sn}}$, while $\beta_{t+j} \in \mathbb{F}_{2^{2^{j+1}sn}}$ for any $j \geqslant 1$. For such an integer t we have that f_t has degree $2n$, while $f_t^{(Q,\alpha)}$ has degree $4n$. In general, for any $i \geqslant t$, we have that $f_{i+1} = f_i^{(Q,\alpha)}$ and the degree of f_{i+1} is twice the degree of f_i. □

Remark 3.3. In the hypotheses of Theorem 3.2 we require that the roots of f_1 are not θ_α-periodic. Indeed, this is true if $f_1 = f_0^{(Q,\alpha)}$, since in this circumstance the degree of f_1 is twice the degree of f_0 and consequently the roots of f_0 are leaves of $\mathrm{Gr}_{sn}(\alpha)$.

Consider now the case that $f_0^{(Q,\alpha)}(x) = g_1(x)g_2(x)$ for some irreducible monic polynomials g_1, g_2 of degree n in $\mathbb{F}_{2^s}[x]$. According to Lemma 3.1, at least one of g_1 and g_2 has no θ_α-periodic roots. Suppose that g_2 has no θ_α-periodic roots. If we set $f_1 := g_1$ and all the polynomials f_i have degree n for $0 \leqslant i \leqslant l_s + l_n + 3$, then we break the iterations and set $f_1 := g_2$. Since g_2 has no θ_α-periodic roots, the hypotheses of Theorem 3.2 are satisfied and we can construct inductively a sequence of irreducible monic polynomials, as explained in the theorem.

Example 3.4. In this example we construct a sequence of irreducible monic polynomials over $\mathbb{F}_8[x]$ starting from the polynomial $f_0(x) = x^4 + x + a^3$, being a a root of the primitive polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$. We notice that f_0 is irreducible in $\mathbb{F}_8[x]$ (see [2], Table 5).

We set $\alpha := a$ and proceed as explained in Theorem 3.2. Adopting the notation of the theorem, in the current example we have that $s = 3$, $n = 4$, $l_s = 0$ and $l_n = 2$. Since $f_0^{(Q,\alpha)}$ is not irreducible, it splits into the product of two irreducible monic polynomials of degree 4. We set f_1 equal to one of the two factors of $f_0^{(Q,\alpha)}$, namely

$$f_1(x) := x^4 + a^4x^3 + x^2 + a^2x + a^6.$$

We notice that $f_1^{(Q,\alpha)}$ is irreducible of degree 8 and set $f_2 := f_1^{(Q,\alpha)}$. Since $f_2^{(Q,\alpha)}$ is irreducible of degree 16 in $\mathbb{F}_8[x]$, implying that f_3 has degree $4n = 16$, according to Theorem 3.2 all the polynomials $f_i^{(Q,\alpha)}$ are irreducible for $i \geqslant 2$. Hence, no more factorization is required and we can generate an infinite sequence of irreducible monic polynomials of increasing degree.

Acknowledgement. The author is grateful to the anonymous reviewer for her/his useful comments which contributed to improving the article.

References

[1] *S. D. Cohen*: The explicit construction of irreducible polynomials over finite fields. Des. Codes Cryptography *2* (1992), 169–174.
[2] *D. H. Green, I. S. Taylor*: Irreducible polynomials over composite Galois fields and their applications in coding techniques. Proc. Inst. Elec. Engrs. *121* (1974), 935–939.
[3] *M. K. Kyuregyan*: Iterated constructions of irreducible polynomials over finite fields with linearly independent roots. Finite Fields Appl. *10* (2004), 323–341.
[4] *M. K. Kyuregyan*: Recurrent methods for constructing irreducible polynomials over GF(2). Finite Fields Appl. *8* (2002), 52–68.
[5] *H. Meyn*: On the construction of irreducible self-reciprocal polynomials over finite fields. Appl. Algebra Eng. Commun. Comput. *1* (1990), 43–53.
[6] *G. L. Mullen, D. Panario*: Handbook of Finite Fields. Discrete Mathematics and Its Applications, CRC Press, Boca Raton, 2013.
[7] *S. Ugolini*: Sequences of irreducible polynomials without prescribed coefficients over odd prime fields. Des. Codes Cryptography *75* (2015), 145–155.
[8] *S. Ugolini*: Sequences of binary irreducible polynomials. Discrete Math. *313* (2013), 2656–2662.
[9] *S. Ugolini*: Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two. Theory and Applications of Finite Fields. Conf. on finite fields and their applications, Ghent, Belgium, 2011 (M. Lavrauw et al., eds.). American Mathematical Society, Contemporary Mathematics 579, Providence, 2012, pp. 187–204.
[10] *R. R. Varšamov, G. A. Garakov*: On the theory of selfdual polynomials over a Galois field. Bull. Math. Soc. Sci. Math. Répub. Soc. Roum., Nouv. Sér. *13* (1969), 403–415. (In Russian.)

Author's address: Simone Ugolini, Dipartimento di Matematica, Università di Trento, Via Sommarive 14, I-38123 Povo, Trento, Italy, e-mail: `s.ugolini@unitn.it`.