Journal of Number Theory 133 (2013) 1207–1228

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic three and five

S. Ugolini

*Via Indentro, 32, Verona, VR, Italy*

ARTICLE INFO

*Article history:*
Received 13 May 2012
Revised 31 August 2012
Accepted 4 September 2012
Available online 4 December 2012
Communicated by David Goss

*Keywords:*
Arithmetic dynamical systems
Finite fields
Elliptic curves

ABSTRACT

*Text.* In a previous paper the graphs associated with the iterations of the map $\vartheta$ which takes an element $x$ of a finite field of characteristic two to $x + x^{-1}$ were studied, exploiting the relation between $\vartheta$ and the duplication map over Koblitz curves. While in odd characteristic the graphs associated with $\vartheta$ seem not to present notable symmetries, these are present in characteristic three and five. In fact, while in characteristic three the map $\vartheta$ is conjugated to the inverse of the square mapping, in characteristic five it is related to an endomorphism of a certain elliptic curve. Relying on these considerations we describe the structure of the graphs in finite fields of characteristic three and five and present a computational procedure for constructing examples in any characteristic.

*Video.* For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=nnH53jawJaQ.



## 1. Introduction

Over the last years some studies about iterations of maps over finite fields appeared. For example, in [Rog96] the author concentrates on the square mapping over prime fields, while in [VS04] the authors deal with other quadratic maps and in [CS04] the authors study the cyclic structure of repeated exponentiation modulo a prime. The map which takes an element $x$ of a finite field to $x + x^{-1}$, studied in this paper, is of interest too. For example, it is involved in the construction of self-reciprocal polynomials via the so-called $Q$-transform (cf. [Mey90]). Moreover, the relations between the multiplicative order of an element $\gamma$ and $\gamma + \gamma^{-1}$ over finite fields have been studied too (cf. [Shp01]).

*E-mail address:* sugolini@gmail.com.

0022-314X/$ – see front matter 
http://dx.doi.org/10.1016/j.jnt.2012.09.007

While this paper focuses on finite fields of characteristic three and five, summarizing the results proved in characteristic two, the problem can be described over a finite field of arbitrary characteristic. If $\mathbf{F}_q$ is a finite field with $q$ elements for some prime power $q$, then we can define a map $\vartheta$ on $\mathbf{P}^1(\mathbf{F}_q) = \mathbf{F}_q \cup \{\infty\}$ in such a way:

$$\vartheta(x) = \begin{cases} x + x^{-1} & \text{if } x \neq 0 \text{ and } x \neq \infty, \\ \infty & \text{if } x = 0 \text{ or } \infty. \end{cases}$$

We associate a graph with the map $\vartheta$ over $\mathbf{P}^1(\mathbf{F}_q)$, labeling the vertices of the graph by the elements of $\mathbf{P}^1(\mathbf{F}_q)$ and connecting a vertex $\alpha$ with a vertex $\beta$ if $\vartheta(\alpha) = \beta$. We notice in passing that, if $\beta \in \mathbf{P}^1(\mathbf{F}_q)$, then $\vartheta(x) = \beta$ for at most two elements $x \in \mathbf{P}^1(\mathbf{F}_q)$.

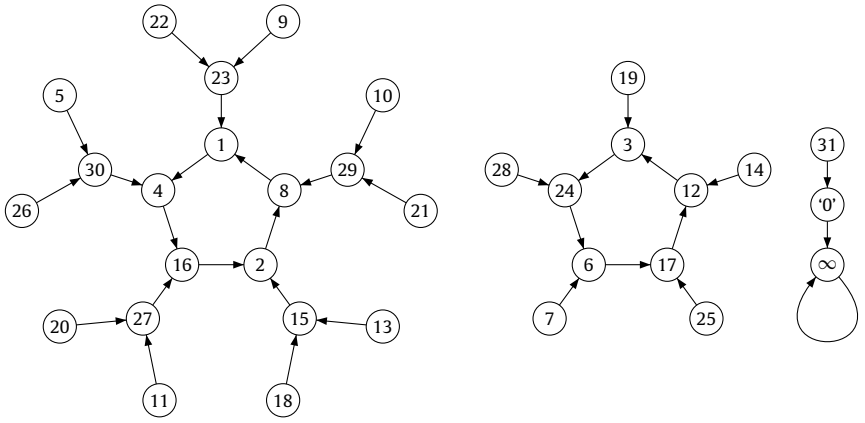
An element $\gamma \in \mathbf{P}^1(\mathbf{F}_q)$ can be periodic or not with respect to the action of the map $\vartheta$. Nevertheless, even when $\gamma$ is not periodic, it is preperiodic, namely there exists a certain iterate of $\gamma$, say $\vartheta^k(\gamma)$, which is periodic. Consider now an element $\gamma$ which is periodic. In this case, $\vartheta^k(\gamma) = \gamma$, for some positive integer $k$, namely $\gamma$ belongs to a cycle of length $k$ or a divisor of $k$. The smallest among these integers $k$ is the period $l$ of $\gamma$ with respect to the map $\vartheta$ and the set $\{\vartheta^i(\gamma)\colon\ 0 \leqslant i < l\}$ is the cycle of length $l$ containing $\gamma$. An element $\gamma$ belonging to a cycle can be the root of a reversed directed binary tree, provided that $\gamma = \vartheta(\alpha)$, for some $\alpha$ which is not contained in any cycle.

While it is possible to construct the graph associated with $\vartheta$ over any finite field, the experimental evidence suggests that such graphs in general present no particular symmetries. For example, the trees rooted at the elements of a same cycle do not have the same depth. Notwithstanding, in finite fields of characteristic two, three and five the graphs present remarkable symmetries and a complete description is possible.

### 1.1. Characteristic two

In [Ugo12] we dealt with the graphs associated with the map $\vartheta$ in characteristic two. There we noticed that this map is related to the duplication map over Koblitz curves. For the reader's convenience we present here an example taken from [Ugo12].

**Example 1.1.** In this example we construct the graph associated with the map $\vartheta$ in the field $\mathbf{F}_{2^5}$, viewed as the splitting field over $\mathbf{F}_2$ of the polynomial $x^5 + x^2 + 1 \in \mathbf{F}_2[x]$. If $\alpha$ is a root of such a polynomial in $\mathbf{F}_{2^5}$, then $\mathbf{P}^1(\mathbf{F}_{2^5}) = \{0\} \cup \{\alpha^i\colon\ 1 \leqslant i \leqslant 31\} \cup \{\infty\}$. We will label the nodes denoting the elements $\alpha^i$ by the exponent $i$ and the zero element by '0'.




While the length of the cycles in finite fields of characteristic two depends on the multiplicative order of a certain endomorphism in the endomorphism ring of the Koblitz curve defined by the