# DYNAMIC STRUCTURE OF MATRICES OVER FINITE FIELDS

E. Ventura*

March 1997

**Abstract**

Given an endomorphism of a finite dimensional vector space $\mathbb{F}_q^n$ over a finite field, $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$, we describe the dynamic structure of the function $\varphi$ (that is, the decomposition in cycles of the permutation $\varphi$, in the bijective case) in terms of the elementary divisors of the endomorphism $\varphi$.

**Key-words:** Graph, Finite Field, Endomorphism, Elementary divisors.

## 1 The dynamical graph of a function

**Definition 1** A *graph*, $Z = (V, E, \iota, \tau)$, consists of two sets, $V = VZ$ called the set of *vertices* and $E = EZ$ called the set of *edges*, and two functions $\iota, \tau : E \to V$ called the *incident* functions. A graph is *finite* when $V$ and $E$ are both finite. A *loop* is an edge $e$ with $\iota e = \tau e$. The concepts of *graph morphism* and *graph isomorphism* (denoted $\simeq$) are the natural ones.

A *subgraph* of $Z = (V, E, \iota, \tau)$ is a graph of the form $(V', E', \iota', \tau')$ where $V' \subseteq V$, $E' \subseteq E$ and $\iota'$ and $\tau'$ are restrictions of $\iota$ and $\tau$ respectively. The *disjoint union* of two graphs $Z_1$ and $Z_2$ is denoted $Z_1 \vee Z_2$. We denote by $nZ$ the disjoint union of $n$ copies of $Z$. A graph $Z$ is *disconnected* when it is the disjoint union of two proper subgraphs. Otherwise, it is *connected*. The maximal connected subgraphs of $Z$ are called *connected components* of $Z$.

The *out-valence* of a vertex $v \in V$ is $|\iota^{-1}(v)|$, the *in-valence* of $v$ is $|\tau^{-1}(v)|$ and the *valence* of $v$ is $|\iota^{-1}(v)| + |\tau^{-1}(v)|$. A graph $Z$ is called a *finite core graph* if it is finite and has no vertices of valence 0 and 1 (in particular, the empty graph is a core graph, but the graph with a single vertex and no edges is not a core graph). The *core* of $Z$, denoted $c(Z)$, is the union of all the finite core subgraphs of $Z$. A graph $Z$ is a *forest* when $c(Z)$ is empty.

[1]Esc. Univ. Pol. de Manresa (Universitat Politècnica de Catalunya). e-mail: ventura@ma3.upc.es

And a *tree* is a connected forest. The concepts of *path*, *trivial* path and *closed* path are the natural ones.

Let $F \subseteq Z$ be a subforest of $Z$. The *quotient* $Z/F$ is the graph obtained from $Z$ by deleting the edges in $F$ and identifying all the vertices in the same component of $F$ to a single vertex. The incident functions are the natural ones.

Let $Z_1 = (V_1, E_1, \iota_1, \tau_1)$ and $Z_2 = (V_2, E_2, \iota_2, \tau_2)$ be two graphs. The *pull-back* of $Z_1$ and $Z_2$, denoted $Z_1 \wedge Z_2$, is the new graph $Z_1 \wedge Z_2 = (V_1 \times V_2, E_1 \times E_2, \iota_1 \times \iota_2, \tau_1 \times \tau_2)$. This definition is a particular case of that given in [5]. Note that $\wedge$ is commutative, associative and distributive respect to $\vee$. Note also that, for every graph $Z$, $Z \wedge C_1 \simeq Z$, where $C_1$ is the unique graph with a single vertex an a single edge.

The first examples of graphs are the cycle graphs and the bouquets. The *cycle graph* of $n$ vertices, denoted $C_n$, is the graph $C_n = (V, E, \iota, \tau)$ where $V = \mathbb{Z}/n\mathbb{Z}$, $E = \{e_1, \cdots e_n\}$, $\iota(e_i) = i$ and $\tau(e_i) = i + 1$, where the indices are modulo $n$. And the *bouquet* of $n$ vertices, denoted $R_n$, is the unique graph with a single vertex and $n$ (possibly infinit) edges.

Let $s \geq 1$, $n_1 \geq 2$ and $n_2, \cdots, n_s$ be positive integers such that $n_2 \leq n_1 - 1$ and $n_i \leq n_1 n_{i-1}$, $i = 3, \cdots, s$. We denote by $T_{n_1;n_2,\cdots,n_s}$ the graph constructed as follows. Let $V_0, V_1, \cdots, V_s$ be disjoint sets with $|V_0| = 1$, $|V_1| = n_1 - 1$ and $|V_i| = n_1 n_i$, for $i = 2, \cdots, s$. The set of vertices of $T_{n_1;n_2,\cdots,n_s}$ is $V = \cup_{i=0}^{s} V_i$. Furthermore, $T_{n_1;n_2,\cdots,n_s}$ contains a loop at the unique vertex in $V_0$, $n_1 - 1$ edges from the $n_1 - 1$ vertices in $V_1$ to the vertex in $V_0$ (the vertex in $V_0$ has in-valence $n_1$). Choose $n_2$ of the $n_1 - 1$ vertices in $V_1$ and for each one put $n_1$ different edges going from $n_1$ of the $n_1 n_2$ vertices in $V_2$ to the choosen vertex (every vertex in $V_1$ has in-valence either $n_1$ or 0). And again, for every $i = 3, \cdots, s$, choose $n_i$ of the $n_1 n_{i-1}$ vertices in $V_{i-1}$ and for each one put $n_1$ different edges going from $n_1$ of the $n_1 n_i$ vertices in $V_i$ to the choosen vertex (every vertex in $V_{i-1}$ has in-valence either $n_1$ or 0). It is clear that $T_{n_1;n_2,\cdots,n_s}$ has $1 + (n_1 - 1) + n_1 n_2 + \cdots + n_1 n_s$ vertices, all of them with out-valence 1, and in-valence either $n_1$ or 0. So, the number of edges is equal to the number of vertices. Furthermore, $T_{n_1;n_2,\cdots,n_s}$ is connected and, in fact, it is a tree with a loop attached the vertex in $V_0$.

The following lemma is straightforward to verify, and will be used later.

**Lemma 2** *For every two positive integers $n$, $m$, $C_n \wedge C_m \simeq gcd(n, m) C_{lcm(n,m)}$.*

**Definition 3** Let $A$ be a set and let $\varphi : A \to A$ be a function.

If $A$ is finite and $\varphi$ belongs to the symmetric group on $A$ (i.e. $\varphi$ is bijective), then it can be decomposed as a product (i.e. composition) of disjoint cycles. The unordered list of these cycles is canonically associated to $\varphi$ and, in fact, it determines $\varphi$. In the general case, this construction does not make sense. A graph is the natural object that we can associate to $\varphi$ in order to generalize the cycle decomposition of permutations in the finite bijective case. This graph will also be canonically associated to $\varphi$, and will determine $\varphi$ too.

We define the *dynamical graph* of $\varphi$, denoted $Z_\varphi$, to be $Z_\varphi = (V, E, \iota, \tau)$ where $V = A$, $E = \{e_a \mid a \in A\}$, $\iota(e_a) = a$ and $\tau(e_a) = \varphi(a)$. That is, we draw an edge from every element in $A$ to its image under $\varphi$.

Suppose that $A$ is finite and $\varphi$ is bijective. Clearly, $\varphi$ decomposes as a product of $\alpha_i$ disjoint cycles of length $k_i$, $i = 1, \cdots, s$ if and only if $Z_\varphi \simeq \bigvee_{i=1}^{r} \alpha_i C_{k_i}$. In general, the structure of $Z_\varphi$ is given by the following proposition (which is a particular case of Proposition 2 in [3] or Theorem I.3.8(iv) in [1]).

**Proposition 4** *Let $A$ be a set and let $\varphi : A \to A$ be a function. Every connected component of $Z_\varphi$ is either an infinite tree or a cycle graph with trees attached to its vertices.*

*Proof.* Take a maximal subforest of $Z_\varphi$ (i.e., a subforest $F \subseteq Z_\varphi$ containing $VZ_\varphi$) and consider the quotient $Z_\varphi/F$. Each connected component of $Z_\varphi/F$ contains exactly one vertex, that is, it is a bouquet. But, by definition, every vertex of $Z_\varphi$ has out-valence at most one (in fact, exactly one), and this property is preserved by collapsing subforests. So, each component of $Z_\varphi/F$ is isomorphic to either $R_0$ or $R_1$. This means that $c(Z_\varphi)$ is the disjoint union of cycle graphs and so, $Z_\varphi$ is the disjoint union of trees and cycle graphs with some trees attached to its vertices. Furthermore, if a tree component of $Z_\varphi$ was finite then it should contain a vertex with zero out-valence, which is not the case.

## 2 Polynomials over finite fields

For the rest of the paper, let $p$ be a prime number, $q = p^m$ and $\mathbb{F}_q$ be the field with $q$ elements.

**Definition 5** Let $p(x) \in \mathbb{F}_q[X]$ be a polynomial with $p(0) \neq 0$ and degree $r$. The ring $\mathbb{F}_q[X]/p(x)\mathbb{F}_q[X]$ contains $q^r - 1$ non-zero elements and so there exist two integers $0 \leq s_1 < s_2 \leq q^r - 1$ such that $x^{s_1} \equiv x^{s_2}$ modulo $p(x)$, that is, $p(x)$ divides $x^{s_1} - x^{s_2}$. The fact $p(0) \neq 0$ says that $p(x)$ divides $x^{s_2 - s_1} - 1$. We define the *order* of $p(x)$, denoted $\mathrm{ord}(p(x))$, to be the minimum positive integer $e$ such that $p(x)$ divides $x^e - 1$ (in general, $\mathrm{ord}(p(x)) \leq q^r - 1$).

The order of a given polynomial $p(x) \in \mathbb{F}_q[X]$ is the minimum positive integer $e$ such that $x^e \equiv 1$ modulo $p(x)$. So, an easy algorith to compute the order of $p(x)$ consists on recursively calculating the powers $x$, $x^2$, $x^3$, $\cdots$ modulo $p(x)$ until the first time we obtain 1 (note that if $x^i$ is the first power congruent to a constant polynomial then $\mathrm{ord}(p(x))$ is multiple of $i$).

The following are well-known facts in finite fields (see, for example, [4]) which we collect here for later reference:

*(i)* In a field of characteristic $p$, $(a + b)^p = a^p + b^p$.

*(ii)* $x^r - 1$ has no multiple roots in the corresponding splitting field if and only if $p$ does not divide $r$.

*(iii)* $x^r - 1$ divides $x^s - 1$ if and only if $r$ divides $s$. So, an arbitrary polinomial $p(x) \in \mathbb{F}_q[X]$ with $p(0) \neq 0$ divides $x^s - 1$ if and only if $\mathrm{ord}(p(x))$ divides $s$.

*(iv)* Let $p(x) \in \mathbb{F}_q[X]$ be an irreducible polynomial with $p(0) \neq 0$ and degree $r$. All the roots of $p(x)$ have the same multiplicative order in the corresponding splitting field. And $p(x)$ divides $x^s - 1$ if and only if some root $\alpha$ of $p(x)$ satisfies $\alpha^s = 1$. So, $\mathrm{ord}(p(x))$ coincides with the multiplicative order of the roots of $p(x)$, which is a divisor of $q^r - 1$. In particular, the order of an irreducible polynomial over a field is not multiple of the characteristic of the field.

We introduce the following notation. Given a prime number $p$ and a positive integer $n$, we define $[n]_p$ to be the shortest positive integer $h$ such that $p^h$ is not less that $n$ (we will write $[n]$ if there are no risc of confusion). That is, $[1] = 0$ and $p^{[n]-1} < n \leq p^{[n]}$ for $n \geq 2$.

**Lemma 6** *Let $p(x) \in \mathbb{F}_q[X]$ be an irreducible polynomial of order $e$. Then, the order of $p(x)^h$ is $ep^{[h]}$.*

*Proof.* Let $k = \mathrm{ord}(p(x)^h)$. By one hand, we have that $p(x)^h$, and so $p(x)$ divides $x^k - 1$. Thus, by *(iii)*, $e$ divides $k$. By another hand, $p(x)$ divides $x^e - 1$ and so $p(x)^h$ divides $(x^e - 1)^h$ and $(x^e - 1)^{p^{[h]}} = x^{ep^{[h]}} - 1$. Thus, $k$ divides $ep^{[h]}$, that is $k = ep^t$ for some $0 \leq t \leq [h]$. Now, by *(ii)* and *(iv)*, all the roots of $x^e - 1$ are simple and so, all the roots of $x^k - 1 = (x^e - 1)^{p^t}$ have multiplicity exactly $p^t$. But all the roots of $p(x)^h$ have multiplicity at least $h$, so $h \leq p^t$ which implies $t = [h]$ and $k = ep^{[h]}$.

## 3 The dynamical structure of a matrix over $\mathbb{F}_q$

Let $K$ be a field and $M$ a $n \times n$ matrix over $K$. We say that $M$ is in *normal form* when it has the form

$$M = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & M_t \end{pmatrix} \quad , \quad M_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_{i,0} \\ 1 & 0 & \cdots & 0 & -a_{i,1} \\ 0 & 1 & \cdots & 0 & -a_{i,2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{i,r_i-1} \end{pmatrix}$$

where $x^{r_i} + a_{i,r_i-1}x^{r_i-1} + \cdots + a_{i,1}x + a_{i,0}$ is a power of a monic irreducible polynomial in $K[X]$, say $p_i^{s_i}(x)$, $i = 1, \cdots, t$. In this case, the characteristic and the minimal polynomial of $M_i$ (called the *companion* matrix for $p_i^{s_i}(x)$, and denoted $M(p_i^{s_i}(x))$ is $p_i^{s_i}(x)$. The

characteristic polynomial of $M$ is $p_1^{s_1}(x)\cdots p_t^{s_t}(x)$ and the minimal polynomial of $M$ is $\operatorname{lcm}(p_1^{s_1}(x), \cdots, p_t^{s_t}(x))$. It is well known (see, for example, chapter 7 of [2]) that for every endomorphism $\varphi : K^n \to K^n$ there exist a basis in which the matrix of $\varphi$ is in normal form. This normal form is uniquely determined by $\varphi$ up to reordering, and the unordered list of polinomials $\{p_i(x) \,|\, i = 1, \cdots, t\}$ are called the *elementary divisors* of $M$. Furthermore, the normal form gives a decomposition $K^n = E_1 \oplus \cdots \oplus E_t$ in $\varphi$-invariant subspaces $E_i$, and the restriction $\varphi_{E_i} : E_i \to E_i$ has matrix $M(p_i^{s_i}(x))$ in the corresponding basis.

Given $\varphi : K^n \to K^n$, we can extend the $K$-linear structure of $K^n$ to a $K[X]$-module structure by defining $xv = \varphi(v)$, $v \in K^n$. It is also well known that $K^n$ is cyclic as $K[X]$-module if and only if the characteristic and the minimal polynomials of $\varphi$ coincides (denote them by $p(x) \in K[X]$). In this case, $K^n$ can be identified with $K[X]/p(x)K[X]$ as $K[X]$-module, and $\varphi$ becomes multiplication by $x$, $g(x) \mapsto xg(x)$.

**Proposition 7** *Let $\varphi : \mathbb{F}_q^n \to F_q^n$ be an endomorphism, let $E$ be a $\mathbb{F}_q$-vector space and let $\alpha : \mathbb{F}_q^n \to E$ be an automorphism. Then, $Z_\varphi \simeq Z_{\alpha^{-1}\varphi\alpha}$.*

*Proof.* It is easy to check that $v \mapsto \alpha(v)$, $e_v \mapsto e_{\alpha(v)}$ is a graph isomorphism from $Z_\varphi$ to $Z_{\alpha^{-1}\varphi\alpha}$. So, $Z_\varphi \simeq Z_{\alpha^{-1}\varphi\alpha}$.

**Proposition 8** *Let $\varphi : \mathbb{F}_q^n \to F_q^n$ be an endomorphism and let $E_1$ and $E_2$ be two $\varphi$-invariant subspaces such that $\mathbb{F}_q^n = E_1 \oplus E_2$. Consider $\varphi_{E_1}$ and $\varphi_{E_2}$ the restrictions of $\varphi$ to $E_1$ and $E_2$ respectively. Then, $Z_\varphi \simeq Z_{\varphi_{E_1}} \wedge Z_{\varphi_{E_2}}$.*

*Proof.* Let $Z_\varphi = (\mathbb{F}_q^n, EZ_\varphi, \iota_\varphi, \tau_\varphi)$ and $Z_{\varphi_{E_1}} \wedge Z_{\varphi_{E_2}} = (E_1 \times E_2, EZ_{\varphi_{E_1}} \times EZ_{\varphi_{E_2}}, \iota_{\varphi_{E_1}} \times \iota_{\varphi_{E_2}}, \tau_{\varphi_{E_1}} \times \tau_{\varphi_{E_2}})$. It is easy to check that $E_1 \times E_2 \to \mathbb{F}_q^n$, $(u, v) \mapsto u + v$ and $EZ_{\varphi_{E_1}} \times EZ_{\varphi_{E_2}} \to EZ_\varphi$, $(e_u, e_v) \mapsto e_{u+v}$ is a graph isomorphism from $Z_{\varphi_{E_1}} \wedge Z_{\varphi_{E_2}}$ to $Z_\varphi$. So, $Z_\varphi \simeq Z_{\varphi_{E_1}} \wedge Z_{\varphi_{E_2}}$.

**Theorem 9** *Let $p(x) \in \mathbb{F}_q[X]$, $p(x) \neq x$, be a monic irreducible polynomial of order $e$ and degree $r$, and let $\varphi : \mathbb{F}_q^{rs} \to F_q^{rs}$ be an endomorphism with characteristic and minimal polynomial $p(x)^s$. Then,*

$$\begin{aligned} Z_\varphi \;\simeq\; & C_1 \vee \alpha_1 C_e \vee (\alpha_2 + \cdots + \alpha_p) C_{ep} \vee (\alpha_{p+1} + \cdots + \alpha_{p^2}) C_{ep^2} \vee \cdots \\ & \cdots \vee (\alpha_{p^{[s]-2}+1} + \cdots + \alpha_{p^{[s]-1}}) C_{ep^{[s]-1}} \vee (\alpha_{p^{[s]-1}+1} + \cdots + \alpha_s) C_{ep^{[s]}} \end{aligned}$$

*where $\alpha_i = \frac{q^{ri} - q^{r(i-1)}}{ep^{[i]}}$, $i = 1, \cdots, s$, and the unique possible repetition is $e = 1$ which only occurs when $p(x) = x - 1$.*

*Proof.* As we discussed above, $\mathbb{F}_q^{rs}$ is isomorphic to $\mathbb{F}_q[X]/p(x)^s\mathbb{F}_q[X]$ as $\mathbb{F}_q[X]$-module, and $\varphi$ corresponds to multiplication by $x$. So, by Proposition 7, $Z_\varphi \simeq Z_\phi$ where $\phi : \mathbb{F}_q[X]/p(x)^s\mathbb{F}_q[X] \to \mathbb{F}_q[X]/p(x)^s\mathbb{F}_q[X]$, $g(x) \mapsto xg(x)$. Let us analize this second graph.

Under our hypothesis, $\phi$ is bijective and so $Z_\phi$ is a disjoint union of cycle graphs. Suppose that the connected component of $Z_\phi$ containing $0 \neq g(x) \in \mathbb{F}_q[X]/p(x)^s\mathbb{F}_q[X]$ is a cycle graph of length $k \geq 1$. Then, $k$ is the shortest power of $\phi$ that fixes $g(x)$. That is, $k$ is the shortest positive integer such that $g(x)x^k \equiv g(x)$ modulo $p(x)^s$ or, in other words, the shortest positive integer such that $p(x)^s$ divides $g(x)(x^k-1)$. Write $g(x) = g'(x)p(x)^d$ for some $0 \leq d < s$ and some $g'(x) \in \mathbb{F}_q[X]$ coprime with $p(x)$. The previous assertion is now equivalent to say that $k$ is the shortest positive integer such that $p(x)^{s-d}$ divides $x^k - 1$, that is, $k$ is the order of $p(x)^{s-d}$. This proves that every component of $Z_\phi$ is a cycle graph of length either $k_0 = 1$ (for the zero vector) or $k_i = \mathrm{ord}(p(x)^i)$ for some $i = 1, \cdots, s$ (furthermore, note that, by lemma 6, $k_i = ep^{[i]}$, $i = 1, \cdots, s$). Denote by $\mathcal{P}_i$ the set of non-zero polynomials $g(x) \in \mathbb{F}_q[X]$ with degree less than $rs$ and $\gcd(g(x), p(x)^s) = g(x)^{s-i}$. Each one of these polynomials gives a vertex in $Z_\phi$ which belongs to a cycle component of length $k_i$. But if $g(x) \in \mathcal{P}_i$ then $xg(x) \in \mathcal{P}_i$ modulo $p(x)^s$. So, $\mathcal{P}_i$ is the set of vertices of some family of cycle components of $Z_\phi$ with length $k_i$. In particular, $k_i$ divides $|\mathcal{P}_i|$. Let $\alpha_i = |\mathcal{P}_i|/k_i$. It is now clear that $Z_\phi \simeq C_1 \vee \bigvee_{i=1}^s \alpha_i C_{k_i}$. But $ep^{[1]} = e$ and $ep^{[i]} = ep^j$ for every $p^{j-1} < i \leq p^j$, $j \geq 1$. So,

$$\begin{aligned} Z_\varphi &\simeq Z_\phi \simeq C_1 \vee \textstyle\bigvee_{i=1}^s \alpha_i C_{ep^{[i]}} \\ &\simeq C_1 \vee \alpha_1 C_e \vee (\alpha_2 + \cdots + \alpha_p) C_{ep} \vee (\alpha_{p+1} + \cdots + \alpha_{p^2}) C_{ep^2} \vee \cdots \\ &\quad \cdots \vee (\alpha_{p^{[s]-2}+1} + \cdots + \alpha_{p^{[s]-1}}) C_{ep^{[s]-1}} \vee (\alpha_{p^{[s]-1}+1} + \cdots + \alpha_s) C_{ep^{[s]}} \end{aligned}$$

It remains to calculate $\alpha_i$ for $i = 1, \cdots, s$. It is clear that the number of polynomials $g(x) \in p(x)^{s-i}\mathbb{F}_q[X]$ with degree less than $rs$ is equal to the number of polynomials in $\mathbb{F}_q[X]$ with degree less than $ri$, that is, $q^{ri}$. So, $|\mathcal{P}_i| = q^{ri} - q^{r(i-1)}$ and $\alpha_i = \frac{q^{ri}-q^{r(i-1)}}{k_i} = \frac{q^{ri}-q^{r(i-1)}}{ep^{[i]}}$, $i = 1, \cdots, s$.

By the normal form properties, all the endomorphisms with characteristic and minimal polynomial $p(x)^s$ are equal up to a change of basis. So, by Proposition 7, the isomorphism type of the graph $Z_\varphi$ in the previous theorem is determined by the polynomial, and will be denoted $Z(p(x)^s)$.

**Theorem 10** *Let $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an endomorphism and denote by $p_1(x)^{s_1}, \cdots, p_t(x)^{s_t}$ its elementary divisors. Then, $Z_\varphi \simeq \bigwedge_{i=1}^t Z(p_i(x)^{s_i})$.*

*Proof.* We have a decomposition into $\varphi$-invariant direct summands, $\mathbb{F}_q^n = E_1 \oplus \cdots \oplus E_t$, such that the restriction $\varphi_{E_i} : E_i \to E_i$ has characteristic and minimal polynomial $p_i(x)^{s_i}$, $i = 1, \cdots, t$. So, by Theorem 9, $Z_{\varphi_{E_i}} \simeq Z(p_i(x)^{s_i})$. Now, the proof is completed by using Proposition 8 and induction on $t$.

**Theorem 11** *Let $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an endomorphism and denote by $p_1(x)^{s_1}, \cdots, p_t(x)^{s_t}$ its elementary divisors.*

*(i) If $\varphi$ is bijective then $p_i(x) \neq x$ for every $i = 1, \cdots, t$ and $Z_\varphi$ is a disjoint union of some cycle graphs whose lengths are precisely the numbers $lcm(e_1 p^{j_1}, \cdots, e_t p^{j_t})$ where $e_i = ord(p_i(x))$ and $j_i = -\infty, 0, 1, \cdots, [s_i]$, $i = 1, \cdots, t$ (with the convention that $e_i p^{-\infty} = 1$).*

*(ii) If $\varphi$ is nilpotent then $p_i(x) = x$ for every $i = 1, \cdots, t$ and*

$$Z_\varphi \simeq T_{q^{d_1}; q^{d_2-d_1}-1,\, q^{d_3-d_1}-q^{d_2-d_1}, \cdots, q^{d_s-d_1}-q^{d_{s-1}-d_1}}$$

*where $d_i$ is the dimension of $\ker \varphi^i$, $i = 1, \cdots, s = \max\{s_i\}$.*

*(iii) Otherwise, there are elementary divisors of the two types. Take those of the first (resp. second) type and consider the graph described in (i) (resp. (ii)) with respect to them, say $C$ (resp. $T$); let $v$ denote the initial and terminal vertex of the unique loop in $T$, and let $T'$ denote $T$ with this loop removed. Then, $Z_\varphi$ is isomorphic to $C$ with a copy of $T'$ attached to every vertex, through $v$.*

*Proof.* Suppose $\varphi$ is bijective. By Theorem 10, $Z_\varphi \simeq \bigwedge_{i=1}^{t} Z(p_i(x)^{s_i})$, and Theorem 9 gives us a description of $Z(p_i(x)^{s_i})$, say

$$Z(p_i(x)^{s_i}) \simeq C_{e_i p^{-\infty}} \vee \beta_{i,0} C_{e_i p^0} \vee \beta_{i,1} C_{e_i p^1} \vee \cdots \vee \beta_{i,[s_i]} C_{e_i p^{[s_i]}}$$

where $e_i = \mathrm{ord}(p_i(x))$. Now, using Lemma 2 and induction on $t$, we obtain that $Z_\varphi$ is a disjoint union of cycle graphs of lengths precisely $\mathrm{lcm}(e_1 p^{j_1}, \cdots, e_t p^{j_t})$ where $j_i$ runs inthe set $\{-\infty, 0, 1, \cdots, [s_i]\}$, $i = 1, \cdots, t$.

Suppose that $\varphi$ is nilpotent; the nilpotency index is $s = \max\{s_1, \cdots, s_t\}$. The dimension of $\ker \varphi$ is $d_1$, so every vertex in $Z_\varphi$ has in-valence either 0 or $q^{d_1}$. If there exist a non-trivial closed path in $Z_\varphi$ which does not crosses the zero vector then some power of $\varphi$ fixes a non-zero vector, i.e. it has an eigenvector of eigenvalue 1 which is impossible. So, the unique non-trivial closed paths in $Z_\varphi$ are repetitions of the loop at 0. Thus, deleting this loop we get a tree, say $T$. But 0 is the unique vertex in $T$ with out-valence zero, so, for every other vertex $v$ there exist a unique path in $T$ from $v$ to 0. And the length of this path is $k$ if and only if $v \in \ker \varphi^k$ and $v \notin \ker \varphi^{k-1}$. Take now $V = \{0\}$ and $V_i = \ker \varphi^i - \ker \varphi^{i-1}$, $i = 1, \cdots, s$. It is clear that every edge in $Z_\varphi$ is either the loop at 0, or has its initial vertex in $V_i$ and its terminal vertex in $V_{i-1}$ for some $i = 1, \cdots, s$. So, $Z_\varphi$ is isomorphic to the graph defined in Definition 1 with suitable parameters. But $|V_0| = 1$, $|V_1| = |\ker \varphi| - 1 = q^{d_1} - 1$, and $|V_i| = |\ker \varphi^i| - |\ker \varphi^{i-1}| = q^{d_i} - q^{d_{i-1}}$, $i = 2, \cdots, s$. So, the parameters in the construction of $Z_\varphi$ are $n_1 = q^{d_1}$, $n_2 = \frac{q^{d_2} - q^{d_1}}{q^{d_1}} = q^{d_2 - d_1} - 1$, and $n_i = \frac{q^{d_i} - q^{d_{i-1}}}{q^{d_1}} = q^{d_i - d_1} - q^{d_{i-1} - d_1}$, $i = 3, \cdots, s$ (it is straightforward to verify that they satisty the necessary conditions). This completes the proof of *(ii)*.

Suppose that $\varphi$ is neither bijective nor nilpotent and that $C$, $T$ and $T'$ are as in the statement. By Theorem 10, we know that $Z_\varphi \simeq C \wedge T$. Let $e$ denote the loop in $T$. The

vertices and edges of $C \wedge T$ with second component equal to $v$ and $e$ respectively, form a copy of $C$ inside $C \wedge T$, say $C'$. And it is clear that, for every vertex in $C'$, there is a copy of $T'$ attached to it through $v$. At this moment we have $|VC||VT|$ vertices which are the total number of vertices in $C \wedge T$; and no one of them is isolated. So, the addition of another edge will violate Proposition 4. Thus, the description above is a complete description of $C \wedge T$ and *(iii)* is proven.

# 4 Example

Consider the field with 3 elements and let $\varphi : \mathbb{F}_3^{16} \to \mathbb{F}_3^{16}$ be an endomorphism with characteristic polynomial $(x^2+1)^4(x^3+2x+2)^2x^2$ and minimal polynomial $(x^2+1)^4(x^3+2x+2)x^2$. The list of its elementary divisors will be $(x^2+1)^4$, $x^3+2x+2$, $x^3+2x+2$, $x^2$.

The polynomial $x^2+1 \in \mathbb{F}_3[X]$ is irreducible and has degree $r=2$ and order $e=4$ (in fact, $x^4-1=(x+1)(x+2)(x^2+1)$ and $x^2+1$ does not divide $x^2-1$). Aplying Theorem 9 with $s=4$, we obtain:

$$\alpha_1 = \frac{3^2-3^0}{4\cdot 3^0} = 2, \quad \alpha_2 = \frac{3^4-3^2}{4\cdot 3^1} = 6, \quad \alpha_3 = \frac{3^6-3^4}{4\cdot 3^1} = 54, \quad \alpha_4 = \frac{3^8-3^6}{4\cdot 3^2} = 162$$

so, $Z((x^2+1)^4) \simeq C_1 \vee 2C_4 \vee 60C_{12} \vee 162C_{36}$ (in fact, $1+2\cdot 4+60\cdot 12+162\cdot 36 = 6561 = 3^8$).

The polynomial $x^3+2x+2 \in \mathbb{F}_3[X]$ is irreducible and has degree $r=3$ and order $e=13$ (in fact, $e$ divides $3^3-1=26$ and $x^{13}-1=(x+2)(x^3+2x+2)(x^3+x^2+2)(x^3+x^2+x+2)(x^3+2x^2+2x+2)$). Aplying again Theorem 9, now with $s=1$, we obtain:

Fig. 1

$$\alpha_1 = \frac{3^3-3^0}{13\cdot 3^0} = 2$$

so, $Z(x^3+2x+2) \simeq C_1 \vee 2C_{13}$ (in fact, $1+2\cdot 13 = 27 = 3^3$).

By Theorem 11*(ii)*, we obtain that $Z(x^2)$ is the graph depicted in Fig 1.
Now, aplying Theorem 10 and Lemma 2 we obtain

$$Z((x^2+1)^4) \wedge Z(x^3+2x+2) \wedge Z(x^3+2x+2) \simeq$$
$$\simeq (C_1 \vee 2C_4 \vee 60C_{12} \vee 162C_{36}) \wedge (C_1 \vee 2C_{13}) \wedge (C_1 \vee 2C_{13}) \simeq$$
$$\simeq (C_1 \vee 2C_4 \vee 60C_{12} \vee 162C_{36}) \wedge (C_1 \vee 56C_{13}) \simeq$$
$$\simeq ((C_1 \vee 2C_4 \vee 60C_{12} \vee 162C_{36}) \wedge C_1) \vee ((C_1 \vee 2C_4 \vee 60C_{12} \vee 162C_{36}) \wedge 56C_{13}) \simeq$$
$$\simeq C_1 \vee 2C_4 \vee 60C_{12} \vee 56C_{13} \vee 162C_{36} \vee 112C_{52} \vee 3360C_{156} \vee 9072C_{468}$$

(in fact, $1+2\cdot 4+60\cdot 12+56\cdot 13+162\cdot 36+112\cdot 52+3360\cdot 156+9072\cdot 468 = 4782969 = 3^{14}$). So, by Theorem 11*(iii)*, $Z(\varphi)$ is the previous graph with a tree like in Fig.1 deletting the loop, attached to every vertex (the total number of vertices is $3^{14} \cdot 9 = 3^{16}$).

## References


[1] W. Dicks and E. Ventura. *The Group Fixed by a Family of Injective Endomorphisms of a Free Group*. Cont. Math., vol.195, (81 pages). (1996)

[2] F.R. Gantmacher. *Théorie des Matrices*, vol 1. Dunod, Paris, 1966.

[3] R.Z. Goldstein and E.C. Turner. *Fixed Subgroups of Homomorphisms of Free Groups*. Bull. London Math. Soc, vol.18, pp. 468-470. (1986)

[4] R.J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Klumer Academic Publishers, 1987.

[5] J.R. Stallings. *Topology of Finite Graphs*. Invent. Math., vol.71, pp. 551-565. (1983)