ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 24, Number 3, Summer 1994

ALGEBRAIC DYNAMICS OF POLYNOMIAL MAPS ON THE ALGEBRAIC CLOSURE OF A FINITE FIELD, II

ANJULA BATRA AND PATRICK MORTON

ABSTRACT. We study the dynamics of polynomial maps on the algebraic closure of the finite field $\mathbf{F}_q$ by associated to a polynomial $\sigma(x)$ in $\mathbf{F}_q[x]$ a graph G_σ on the irreducible polynomials over $\mathbf{F}_q$ which reflects the algebraic properties of the mapping $\alpha \to \sigma(\alpha)$. For additive polynomials σ we show that many of the connected components of G_σ are isomorphic to the connected component of x, and we determine the structure of all of the connected components of G_σ over $\mathbf{F}_p$ explicitly when $\sigma(x) = x^p \pm x$ and p is prime. We also describe the connection between the graph G_σ for $\sigma(x) = x^p - x$ and Artin-Schreier theory.

1. Introduction. In Part I of this paper we have defined a graph G_σ on the monic, irreducible polynomials over a finite field $\mathbf{F}_q$ which reflects the dynamics of the mapping $a \to \sigma(a)$ on the algebraic closure of $\mathbf{F}_q$, where $\sigma(x)$ is a nonconstant polynomial with coefficients in $\mathbf{F}_q$ (the same definitions work for an arbitrary field). In that paper we also proved a number of theorems about the cycles in the graph G_σ, and gave special consideration to the polynomials of the form $\sigma(x) = x^q + ax$.

In this part of the paper we will first investigate the structure of the connected components of this graph for general additive (separable) polynomials and then give more detailed results for two special families of polynomials, the maps $\sigma(x) = x^p \pm x$, considered over the prime field $\mathbf{F}_p$. When we want to emphasize the ground field κ, we use the notation $G_\sigma(\kappa)$. The connected component of a polynomial f in G_σ will be denoted by $C_\sigma(f)$ or by $C_\sigma(f;\kappa)$ if the field κ needs to be emphasized.

We recall that for two irreducible polynomials f and g over $\mathbf{F}_q$, the edge $g \to f$ is in the graph G_σ if and only if the map $\sigma(x)$ takes a root of g to a root of f. In part 1 we show that $g \to f$ for a unique

Received by the editors on May 13, 1993, and in revised form on October 12, 1993.
1991 AMS *Mathematics Subject Classification.* 12E20, 5C20.
The second author was supported by a Brachman-Hoffman grant from Wellesley College, and both authors were supported by NSF Grant DMS-9200575, during the period in which this article was written.

irreducible f, so there is an induced map $\hat{\sigma}$ on irreducible polynomials defined by: $\hat{\sigma}(g) = f$, if α has minimal polynomial g and $\sigma(\alpha) = \beta$ has minimal polynomial f. We showed further that the polynomials f in cycles of G_σ, which are just the periodic points of $\hat{\sigma}$, are exactly the irreducible factors of the polynomials $\Phi_{m,\sigma}(x)$ defined by the formula

$$\Phi_{m,\sigma}(x) = \prod_{d|m} (\sigma^d(x) - x)^{\mu(m/d)}.$$

Our main results show that many of the connected components of G_σ are isomorphic to the connected component of x, when σ is an additive, separable polynomial over $\mathbf{F}_q$, i.e., a polynomial in $\phi(x) = x^p$ in which the coefficient of x is nonzero. Let p be the characteristic of $\mathbf{F}_q$.

Theorem 1 (see Theorems 3.1, 3.2). *Let $\sigma(x)$ be an additive, separable, polynomial over $\mathbf{F}_q$, and let κ be the splitting field of $\sigma(x)$ over $\mathbf{F}_q$. If $f(x)$ is a fixed point of $\hat{\sigma}$ for which $(\deg f, [\kappa : \mathbf{F}_q]p) = 1$, then the connected component $C_\sigma(f)$ of f in G_σ is isomorphic to the connected component $C_\sigma(x)$.*

In Theorems 3.3 and 3.4 we extend this result to any periodic point f of $\hat{\sigma}$ for which $(\deg f, [\kappa : \mathbf{F}_q]) = 1$. Define, for a polynomial f in a cycle, $C^*_\sigma(f)$ to be the subgraph of $C_\sigma(f)$ consisting of the vertices whose distance to f in the graph is less than the distance to any other vertex in the cycle. These are the vertices from which any path to the cycle hits f first in the cycle, and can be visualized by imagining the cycle as the center of a wheel and $C^*_\sigma(f)$ as one of the spokes. (See the third diagram in Section 3 of Part I.) Then for $\deg f = p^r m$, where $(m, p[\kappa : \mathbf{F}_q]) = 1$, we have the isomorphism $C^*_\sigma(f) \cong C^*_\sigma(x; \mathbf{F}_{q'})$, with $q' = q^{p^r}$. In particular, all of the "spokes" of $C_\sigma(f)$ are isomorphic graphs, so that this connected component has a nontrivial cyclic group of automorphisms whenever f has period ≥ 2 with respect to $\hat{\sigma}$.

These results show that over the splitting field κ of σ, each of the connected components of $G_\sigma(\kappa)$ is determined by the cycle it contains and by the structure of $C_\sigma(x; \mathbf{F}_{q'})$. In Sections 4 and 5 we determine the structure of $C_\sigma(x)$ completely for each of the polynomials $\sigma(x) = x^p \pm x$ over $\mathbf{F}_p$. For the map $\sigma(x) = x^p - x$, the vertices in $C_\sigma(x)$ are all the irreducible polynomials over $\mathbf{F}_p$ whose degrees are powers of p: each

of these polynomials has roots which are pre-periodic with respect to σ. In contrast, for the map $\sigma(x) = x^p + x$ (with p odd) the irreducible polynomials of degree p^r lie in cycles of G_σ and therefore have roots which are periodic. This indicates that these two maps have very different dynamics. In particular, the determination of $C_\sigma(x)$ is much more difficult for $\sigma(x) = x^p + x$ than for $x^p - x$ (see Section 5). In computing $C_\sigma(x)$ we make use of some of the main results of Part I [**3**].

One nice application of the graph G_σ is that it gives an interesting way of visualizing the algebraic closure $\hat{\mathbf{F}}_p$ of $\mathbf{F}_p$. For example, the connected component $C_\sigma(x)$ for the map $\sigma(x) = x^p - x$ gives a "layering" of elements of degree p^r over $\mathbf{F}_p$. (See the second diagram in Section 3 of Part I, which gives the initial part of this layering for $p = 2$.) The following theorem, which describes this "layering" more precisely, uses the notation "level" of a vertex, which is defined to be the length of the shortest path from that vertex to a cycle, in this case the length of the shortest path to x. (The symbol $\varphi(n)$ denotes the Euler φ-function.)

Theorem 2. (See Theorems 4.3, 4.4). a) *If $k \geq 1$, the irreducible polynomials of degree p^k over $\mathbf{F}_p$ occur in $\varphi(p^k)$ levels of $C_{x^p-x}(x)$, starting with $(p-1)p^{p^{k-1}-k}$ polynomials at level $p^{k-1}+1$, branching to p times the previous number in each successive level, for $\varphi(p^k)$ levels. Each polynomial in the last row of irreducibles of degree p^k (at level p^k) is connected to a single irreducible of degree p^{k+1} at level $p^k + 1$.*

b) *For $n \geq 0$, the set of roots V_n of polynomials at levels n or less in $C_{x^p-x}(x)$ is a vector space of dimension n over $\mathbf{F}_p$ and coincides with the set of solutions α in $\hat{\mathbf{F}}_p$ of $\sigma^n(\alpha) = 0$, where $\sigma(x) = x^p - x$. The spaces V_n give a layering (filtration; composition series)*

$$V_0 \subset V_1 \subset \cdots \subset V_n \subset \cdots \subset V_\infty$$

of the subfield V_∞ of $\hat{\mathbf{F}}_p$ consisting of the elements which have degree p^r, $r \geq 0$, over $\mathbf{F}_p$. In particular, the roots of polynomials at level n comprise $p-1$ cosets $k\alpha + V_{n-1}$ of V_{n-1}, $k = 1, 2, \ldots, p-1$, and are therefore invariant under translation by elements of V_{n-1}.

The map $\sigma(x) = x^p - x$ is also interesting because of its connection to Artin-Schreier theory. In Section 4 we use the graph G_σ to locate poly-

nomials whose roots generate p-power extensions of a given groundfield $\mathbf{F}_q$.

Theorem 3 (see Theorem 4.5). *Let $\sigma(x) = x^p - x$. For any integer d relatively prime to p, there exists an irreducible polynomial f in $\mathbf{F}_p[x]$ of degree d which lies in a cycle of G_σ. For such an f, let σ be any root of a polynomial at level 1 in $C_\sigma(f)$. Then any root of $\sigma^{p^{k-1}} - \alpha$ generates the unique extension of degree p^k of $\mathbf{F}_{p^d}$.*

For $k = 1$, this is the usual result, that a root of $x^p - x - \alpha$ (for suitable α) generates a cyclic extension of $\mathbf{F}_{p^d}$ of degree p (cf. [**1**]). It would be interesting to generalize this result about finite fields to arbitrary fields of characteristic p, but it doesn't seem clear how to do this.

Finally, in another paper we will discuss an application of the graphs G_σ over $\mathbf{F}_p$ to algebraic number theory. These graphs are related to the splitting behavior of a prime p in towers of algebraic number fields generated by pre-periodic points of a map $\sigma(x)$ defined over $\mathbf{Q}$. (See also [**2**].)

2. Properties of additive maps. Let σ be an additive, separable polynomial over a field κ of characteristic p, i.e., a polynomial in the Frobenius map $\phi(x) = x^p$:

$$\sigma(x) = (a_0\phi^k + a_1\phi^{k-1} + \cdots + a_k)(x), \qquad a_k \neq 0, \tag{1}$$

and assume that the groundfield κ contains all the roots of $\sigma(x) = 0$.

If g and f are monic and irreducible and $g \to f$, then g is a divisor of $f(\sigma(x))$. It is not hard to show that

$$f(\sigma(x)) = \prod_a g(x + a),$$

where a runs over a subset of the roots of $\sigma(x) = 0$. We show this by considering the function field extension $\kappa(x)/\kappa(\sigma(x))$. This is an extension whose degree is $\deg \sigma = p^k$ (see [**7**, page 217]). The extension is also normal and separable, since the minimal polynomial of x over $\kappa(\sigma(x))$, namely $\sigma(y) - \sigma(x)$, splits completely over $\kappa(x)$:

$$\sigma(y) - \sigma(x) = \sigma(y - x) = \prod_{\sigma(a)=0} (y - x - a).$$

(Compare with [**4**, Theorem 3].) Hence the conjugates of x over $\kappa(x)$ are the linear polynomials $x+a$, where a is a root of σ, so that if V is the additive group of roots of $\sigma(x)$ in κ,

$$\Gamma = \mathrm{Gal}\,(\kappa(x)/\kappa(\sigma(x))) \cong V.$$

It follows that a polynomial $h(x)$ is a polynomial in $\sigma(x)$ if and only if h is invariant under all the automorphisms of Γ, i.e., if and only if

$$h(x+a) = h(x), \qquad \text{for all } a \text{ for which } \sigma(a) = 0.$$

Now consider $f(\sigma(x))$. This polynomial is invariant under Γ. Let H be the subgroup of Γ which leaves the polynomial g invariant. If $\tau_1, \ldots, \tau_r$ are a set of coset representatives for H in Γ, and if $\tau_i(x) = x + a_i$, then the product

$$P = \prod_{i=1}^{r} \tau_i(g) = \prod_{i=1}^{r} g(x+a_i)$$

is a product of distinct irreducibles and is invariant under Γ. Since $f(\sigma(x))$ is invariant under Γ and divisible by $g(x)$, it must also be divisible by P. On the other hand, writing $P(x) = h(\sigma(x))$ implies that $h(x)$ divides $f(x)$, which gives that $h(x) = f(x)$ by the irreducibility of f. This proves the following theorem.

Theorem 2.1. *Assume κ has characteristic p and contains all the roots of the additive, separable polynomial $\sigma(x)$. If f is monic and irreducible and g is a monic, irreducible factor of $f(\sigma(x))$, then*

$$f(\sigma(x)) = \prod_{i=1}^{r} g(x+a_i), \tag{2}$$

where the a_i are a subset of the roots of $\sigma(x) = 0$, and where the automorphisms $x \to x+a_i$ are coset representatives in Γ of the subgroup which fixes the polynomial $g(x)$. In particular, all the irreducible factors of $f(\sigma(x))$ have the same degree, and the number of irreducible factors is a power of p.

The last assertion follows from the fact that $[\Gamma : H]$ is a power of p. Note that this power divides $\deg \sigma$.

In the arithmetic of algebraic function fields, $f(\sigma) = f(\sigma(x))$ corresponds to a prime divisor of the ground field $\kappa(\sigma) = \kappa(\sigma(x))$ and the factorization (2) gives the splitting of this prime divisor into prime divisors of the extension $\kappa(x)$. Since the field extension is normal, the new prime divisors all have the same degree.

This theorem also gives a method for computing f, given g. Just compute the product on the right side of equation (2) and write this as a polynomial in $\sigma(x)$. It isn't necessary to compute the group H, since f can be determined from

$$\prod_{\tau \text{ in } \Gamma} \tau(g) = f(\sigma(x))^{|H|}.$$

When the lefthand side of this equation is computed and written as a polynomial in $\sigma(x)$, it will be a power of f.

Corollary. *Let $\sigma(x) = x^p - x$. If f is an irreducible polynomial over a field κ of characteristc p, then $f(\sigma(x))$ is either irreducible or factors into a product of p irreducible factors with degree equal to $\deg f$. In the latter case*

$$f(x^p - x) = \prod_{a=0}^{p-1} g(x + a) \tag{3}$$

where g is any irreducible factor of $f(\sigma(x))$.

In terms of the splitting of the prime divisor $f(\sigma)$ in $\mathbf{F}_p(x)/\mathbf{F}_p(\sigma)$, with $\sigma(x) = x^p - x$, Theorem 3.6 of Part I shows that for infinitely many primes (i.e., irreducibles) $f(\sigma)$ in $\mathbf{F}_p(\sigma)$, one of the prime divisors of $f(\sigma)$ in $\mathbf{F}_p(x)$ is $f(x)$ itself.

Theorem 2.1 has important consequences for the graph G_σ, for a general σ of the form (1).

Theorem 2.2. *Let f be an irreducible polynomial over κ, a field of characteristic p, which contains the roots of the additive polynomial*

$\sigma(x)$, and consider the vertices g_i in $G_\sigma(\kappa)$ for which $g_i \to f$. Then the number of such vertices, r, is a power of p. Moreover, the degrees of the g_i are all equal, and they all belong to the same field extension of κ.

Proof. The assertions are all immediate from Theorem 2.1, the last being a consequence of the fact that the roots of $g_i(x) = g(x + a_i)$ can be expressed linearly in terms of the roots of any single $g = g_j$. □

Corollary 2.3. *If $\sigma(x) \in \mathbf{F}_q[x]$ is an additive polynomial with splitting field κ over $\mathbf{F}_q$ and f is an irreducible polynomial in $\mathbf{F}_q[x]$ whose degree is divisible by $[\kappa : \mathbf{F}_q]$, then the conclusions of Theorem* 2.2 *hold for the vertex f in the graph $G_\sigma(\mathbf{F}_q)$.*

Proof. Let $d = [\kappa : \mathbf{F}_q]$. The polynomial f splits into irreducibles of the same degree m over κ, where $\deg f = dm$. In fact

$$f(x) = \prod_{i=0}^{d-1} \phi^i(g(x)) = \operatorname{Norm} g(x),$$

where $g(x)$ is one of the irreducible factors of f over κ, $\phi(x) = x^q$ is the Frobenius automorphism and Norm denotes the norm from κ to $\mathbf{F}_q$. By Theorem 2.2, the polynomial $g(\sigma(x))$ splits over κ into irreducibles h_j of the same degree. It follows that

$$f(\sigma(x)) = \prod_j \prod_{i=0}^{d-1} \phi^i(h_j(x)) = \prod_j \operatorname{Norm} h_j(x).$$

Using the fact that σ maps roots of h_j to roots of g and that the coefficients of g generate κ over $\mathbf{F}_q$, it is not hard to see that each root of h_j generates the extension of degree $d(\deg h_j)$ over $\mathbf{F}_q$, and hence that $\operatorname{Norm} h_j(x)$ is irreducible over $\mathbf{F}_q$. It follows that $f(\sigma(x))$ splits over $\mathbf{F}_q$ into irreducibles of the same degree, where the number of irreducibles is a power of p. This proves the corollary. □

3. The graph G_σ for additive σ: isomorphisms between connected components. The structure of the connected component

of x determines a large part of the structure of G_σ, if σ is additive, as we show in this section. Let $C_\sigma(f)$ denote the connected component of f in the graph G_σ. We start with connected components of the form $C_\sigma(f)$, where f is a fixed point of the induced map $\hat{\sigma}$.

Theorem 3.1. *Let $\sigma(x)$ be any additive, separable polynomial over $\mathbf{F}_q$ (a map of the form (1) with $\phi(x) = x^p$). Let $f(x)$ be an irreducible factor of $\Phi_{n,\sigma}(x)$ whose degree over $\mathbf{F}_q$ is relatively prime to the degree of every irreducible in $C_\sigma(x)$, and assume $f(x)$ is a fixed point of $\hat{\sigma}$. Then the component $C_\sigma(f(x))$ of G_σ is isomorphic to $C_\sigma(x)$.*

Proof. Let β be a root of $f(x)$, and let $g(x)$ be an irreducible in $C_\sigma(x)$ with root α. Then for some minimal m, $\sigma^m(\alpha) = 0$, the root of x. We define a map

$$T : C_\sigma(x) \to C_\sigma(f(x))$$

by

$$T(g) = h, \quad \text{where } h \text{ is the minimal polynomial of } \alpha + \beta.$$

We must show that T is well-defined, i.e., that it doesn't depend on the particular roots α or β used to find h, and that T is an isomorphism of directed graphs.

First note that

$$\sigma^m(\alpha + \beta) = \sigma^m(\alpha) + \sigma^m(\beta) = \sigma^m(\beta). \tag{4}$$

Since σ permutes the roots of f, $\sigma^m(\beta)$ is a root of f, and it follows that the minimal polynomial $h(x)$ of $\alpha + \beta$ is in $C_\sigma(f(x))$. To show that $h = T(g)$ doesn't depend on α or β we show that

$$\mathrm{Gal}\,(\mathbf{F}_q(\alpha + \beta)/\mathbf{F}_q) = \mathrm{Gal}\,(\mathbf{F}_q(\alpha)/\mathbf{F}_q) * \mathrm{Gal}\,(\mathbf{F}_q(\beta)/\mathbf{F}_q). \tag{5}$$

We claim first that $\mathbf{F}_q(\alpha, \beta) = \mathbf{F}_q(\alpha + \beta)$. To see this, note from (4) that the field $\mathbf{F}_q(\alpha + \beta)$ contains $\sigma^m(\beta)$ and therefore β, since $\sigma^m(\beta)$ and β are in the same orbit under σ. Thus $\mathbf{F}_q(\alpha + \beta)$ contains α and β and must therefore coincide with $\mathbf{F}_q(\alpha, \beta)$. Since α and β have relatively prime degrees, $\mathbf{F}_q(\alpha)$ and $\mathbf{F}_q(\beta)$ intersect in the field $\mathbf{F}_q$, and

the assertion (5) now follows from standard results in Galois theory, using that $\mathbf{F}_q(\alpha)$ and $\mathbf{F}_q(\beta)$ are normal over $\mathbf{F}_q$.

The result in (5) shows that we get all the conjugates of $\alpha+\beta$ by adding together conjugates of α and conjugates of β in all possible ways. Thus $h(x)$ depends only on g and f and not on α or β.

In particular, we get that

$$\deg\,(Tg(x)) = (\deg f)(\deg g). \tag{6}$$

The map T is 1–1, for if $Tg = Tg'$, then $\alpha+\beta$ and $\alpha'+\beta$ must be conjugate over $\mathbf{F}_q$ for some roots α and α' of g and g'. By (6) g and g' have the same degree, so that α and α' generate the same field. If τ is an automorphism of $\mathbf{F}_q(\alpha,\beta)$ for which $\tau(\alpha+\beta)=\alpha'+\beta$, then by (4) $\tau(\sigma^m(\beta)) = \sigma^m(\beta)$ for some m, whence $\tau(\beta)=\beta$, since $\beta = \sigma^{n-m}(\sigma^m(\beta))$ for appropriate n. It follows that α and $\tau(\alpha)=\alpha'$ must be conjugate as well, giving $g=g'$.

The map T is also onto $C_\sigma(f(x))$, for if h is any irreducible in $C_\sigma(f(x))$, then for some root γ of h and some integer m, $\sigma^m(\gamma)$ is a root of f. By taking a conjugate of γ in place of γ we may assume this root is β. Let β' be a root of $f(x)$ for which $\sigma^m(\beta')=\beta$, and consider the number $\alpha=\gamma-\beta'$. This α satisfies

$$\sigma^m(\alpha) = \sigma^m(\gamma) - \sigma^m(\beta') = \beta - \beta = 0,$$

and therefore has a minimal polynomial g which is connected to x in G_σ. Since $\gamma = \alpha+\beta'$, we have $Tg=h$, which proves that T is onto.

To show that T is an isomorphism of graphs, we must show finally that $g \to g'$ in $C_\sigma(x)$ implies $Tg \to Tg'$ in $C_\sigma(f(x))$. Let α be a root of g. Then $\sigma(\alpha)$ is a root of g', and roots of Tg and Tg' are $\alpha+\beta$ and $\sigma(\alpha)+\beta$. But the above argument shows that the numbers $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$ and $\sigma(\alpha)+\beta$ are conjugates; this shows that σ takes roots of Tg to roots of Tg'. Hence $Tg \to Tg'$, and the theorem is proved. □

To see which polynomials satisfy the degree hypothesis in Theorem 3.1, we prove

Theorem 3.2. *Let σ be an additive, separable polynomial defined over $\mathbf{F}_q$, and let κ be the field generated over $\mathbf{F}_q$ by the roots of $\sigma(x)$.*

Then the degrees of the vertices in $C_\sigma(x)$ have the form dp^k, where d divides $[\kappa : \mathbf{F}_q]$. Thus the degrees of vertices in $C_\sigma(x)$ are only divisible by finitely many distinct primes.

Proof. Let $\sigma(x)$ be any additive map over $\mathbf{F}_q$ of the form (1), and consider the graph $G_\sigma(\kappa)$ and its component $C_\sigma(x;\kappa)$ defined over κ. The vertices in $C_\sigma(x;\kappa)$ are factors of the vertices in $C_\sigma(x)$, and all vertices in $C_\sigma(x;\kappa)$ are still connected to x. Let α be the root of a polynomial in $C_\sigma(x)$, and let h be the polynomial in $C_\sigma(x;\kappa)$ whose root is α. By Theorem 2.2 the vertices g in $C_\sigma(x;\kappa)$ which are 1-step connected to h all have the same degree (over κ). It follows that the root β of any such vertex g satisfies $\deg_\kappa \beta = \deg_\kappa \alpha * p^{r-s}$, where $p^r = \deg \sigma$ and p^s is the number of vertices 1-step connected to h (note $r \geq s$). Thus, except possibly for the factor p, $\deg_\kappa \beta$ has the same prime factors as $\deg_\kappa \alpha$. Applying this argument repeatedly shows that $\deg_\kappa \beta$ is a power of p, since the root 0 of the vertex x has degree 1 over κ. Now the equation

$$\deg_\kappa \beta * [\kappa : \mathbf{F}_q] = [\kappa(\beta) : \kappa][\kappa : \mathbf{F}_q] = [\kappa(\beta) : \mathbf{F}_q(\beta)][\mathbf{F}_q(\beta) : \mathbf{F}_q]$$

implies that $\deg_{\mathbf{F}_q} \beta = [\mathbf{F}_q(\beta) : \mathbf{F}_q]$ divides $\deg_\kappa \beta * [\kappa.\mathbf{F}_q]$. This proves the theorem. □

It is possible to extend the result of Theorem 3.1 to any factor of $\Phi_{n,\sigma}(x)$ with degree prime to the degrees of the irreducibles in $C_\sigma(x)$. We first recall the definition of the *level* of a vertex in G_σ for any σ. An irreducible polynomial g has *level* n if g is n-step connected to a polynomial f in a cycle of G_σ, but not k-step connected to any such polynomial, for $k < n$. All the polynomials whose level is n form a *level* or *row* of the graph G_σ. A polynomial f in a cycle has level 0.

Now let $f(x)$ belong to a cycle in G_σ. We denote by $C^*_\sigma(f)$ the subgraph of $C_\sigma(f)$ consisting of the vertices g for which $\hat{\sigma}^m(g) = f$, where m is the level of g, and call it the star connected component of f. Since $\hat{\sigma}^0(f) = f$, this subgraph contains f and all the polynomials in the "spoke" of $C_\sigma(f)$ which connects to the cycle at f.

Theorem 3.3. *Let $f(x) = f_1(x)$ be an irreducible factor of $\Phi_{n,\sigma}(x)$ whose degree is prime to p and to $[\kappa : \mathbf{F}_q]$, where κ is as in Theorem*

3.2. *Suppose also that f belongs to a cycle of length r in G_σ.*

$$f_1 \to f_2 \to \cdots \to f_r \to f_1, \qquad f_i \neq f_j \text{ for } 1 \leq i \neq j \leq r.$$

a) *Define the map $T_i : C_\sigma(x) \to C_\sigma(f)$ by the requirement that $h = T_i(g)$ is the minimal polynomial of $\alpha + \beta_i$, where α is a root of g and β_i is a root of f_i. Then T_i is a 1–1 map on vertices, and each polynomial h in $C_\sigma(f)$ is given by $h = T_i(g)$ for a unique i, $1 \leq i \leq r$, and g in $C_\sigma(x)$.*

b) *For any fixed i with $1 \leq i \leq r$, define the map $\hat{T}_i : C_\sigma(x) \to C_\sigma(f)$ by*

$$\hat{T}_i(g) = T_{i-m}(g) \quad (\textit{subscripts read modulo } r),$$

where $m = m(g)$ is the level of g in $C_\sigma(x)$. Then $\hat{T}_i$ is an isomorphism of $C^*_\sigma(x)$ with $C^*_\sigma(f_i)$. The disjoint subgraphs $\hat{T}_i(C^*_\sigma(x))$, for $1 \leq i \leq r$, give a partition of the set of vertices of $C_\sigma(f)$.

Proof. The map T_i is the same as the map T in Theorem 1.3 for the polynomial f_i. By the same arguments—in particular, using (5) with $\beta = \beta_i$–T_i is a well-defined map on $C_\sigma(x)$. If g is in $C_\sigma(x)$ and α is a root of g, then by (4) and the fact that (for some m) $\sigma^m(\beta_i)$ is the root of a polynomial in the cycle of f_i, it follows that T_i takes g to a polynomial in $C_\sigma(f)$. By the same argument as before, T_i is also 1–1.

A slight modification of the previous argument will also show that each h in $C_\sigma(f)$ is equal to $T_i(g)$ for some i and g. Just take $\sigma^m(\gamma) = \beta_i$ to be a root of f_i, where γ is a root of h, let β_j satisfy $\sigma^m(\beta_j) = \beta_i$, and put $\alpha = \gamma - \beta_j$. The same reasoning as before shows $T_j(g) = h$, where g is the minimal polynomial of α. Now assume

$$h = T_i(g) = T_j(g').$$

With the obvious notation it follows that $\alpha+\beta_i$ and $\alpha'+\beta_j$ are conjugate over $\mathbf{F}_q$. If m is the larger of the levels of g and g', we see as in (4) that $\sigma^m(\beta_i)$ and $\sigma^m(\beta_j)$ are conjugate, whence β_i and β_j are also conjugate. This shows that $i = j$, so $g = g'$ by the injectivity of T_i. This proves part a).

Now suppose g is at level $m \geq 1$ in $C_\sigma(x)$ and $g \to g'$. Let α and α' be roots of g and g' with $\alpha' = \sigma(\alpha)$. Since the polynomial g' is at level

$m-1$, and $\sigma(\alpha+\beta_{i-m}) = \alpha' + \beta_{i-m+1}$ is a root of $\hat{T}_i(g')$, we conclude that $\hat{T}_i(g) \to \hat{T}_i(g')$. Note that the subgraph $\hat{T}_i(C^*_\sigma(x))$ consists of a set of vertices which are all connected to f_i, since $\hat{T}_i(x) = f_i$. Part a) implies easily that $\hat{T}_i$ is also 1–1, so $\hat{T}_i$ is indeed an isomorphism of $C^*_\sigma(x)$ with a subgraph of $C^*_\sigma(f_i)$. Further, if $\hat{T}_i(g) = \hat{T}_j(g')$, then part a) implies $i - m(g) \equiv j - m(g') \pmod r$ and $g = g'$, hence $i = j$. The assertions of part b) now follow from the fact that every h in $C_\sigma(f)$ can be expressed as

$$h = T_i(g) = T_{i+m(g)-m(g)}(g) = \hat{T}_{i+m(g)}(g). \qquad \square$$

Corollary. *If* lev (h) *denotes the level of a polynomial* h *in* G_σ, *then for any* g *in* $C_\sigma(x)$, lev $(g) =$ lev $(\hat{T}_i(g))$.

Proof. This is immediate from the fact that $\hat{T}_i$ is an isomorphism and that $\hat{T}_i(x) = f_i$. $\square$

We finish this section by showing that the connected components $C_\sigma(x; \mathbf{F}_{q^{p^r}})$ determine the structure of G_σ completely over the splitting field κ of $\sigma(x)$.

Theorem 3.4. *Let* σ *be an additive, separable polynomial over* $\mathbf{F}_q$ *with splitting field* κ, *and let* f *be a polynomial in a cycle of* $G_\sigma(\mathbf{F}_q)$, *where* $\deg f = p^r m$ *and* $(m, [\kappa : \mathbf{F}_q]p) = 1$. *Then* $C^*_\sigma(f; \mathbf{F}_q)$ *is isomorphic to* $C^*_\sigma(x; \mathbf{F}_{q^{p^r}})$.

Proof. Let h be an irreducible factor of f over the field $\mathbf{F}_{q^{p^r}}$. Then $\deg h = m$ is prime to p and prime to $[\kappa' : \mathbf{F}_{q^{p^r}}]$, where $\kappa' = \kappa \mathbf{F}_{q^{p^r}}$ is the splitting field of σ over $\mathbf{F}_{q^{p^r}}$. Furthermore, h lies in a cycle of the graph $G_\sigma(\mathbf{F}_{q^{p^r}})$. Theorem 3.3 implies therefore that $C^*_\sigma(h; \mathbf{F}_{q^{p^r}}) \cong C^*_\sigma(x; \mathbf{F}_{q^{p^r}})$. On the other hand, we claim that

$$C^*_\sigma(h; \mathbf{F}_{q^{p^r}}) \cong C^*_\sigma(f; \mathbf{F}_q).$$

To prove this, note first that if g is any irreducible in $C^*_\sigma(h; \mathbf{F}_{q^{p^r}})$, then g divides a unique irreducible polynomial g' in $\mathbf{F}_q[x]$. Furthermore, if

α is a root of g, and $\sigma^n(\alpha)$ is a root of h, for suitable n, then $\sigma^n(\alpha)$ is also a root of f, which shows that g' is a vertex in $C^*_\sigma(f;\mathbf{F}_q)$. An easy argument gives that $g_1 \to g_2$ implies $g_1' \to g_2'$. Next, let g'' be any vertex in $C^*_\sigma(f;\mathbf{F}_q)$. For some root α of g'' and some n, $\sigma^n(\alpha)$ is a root of f, and $\sigma^k(\alpha)$ is pre-periodic for $k < n$. By taking a conjugate of α over $\mathbf{F}_q$ we may assume that $\sigma^n(\alpha)$ is a root of h. Hence the minimal polynomial g of α over $\mathbf{F}_{q^{p^r}}$ lies in $C^*_\sigma(h;\mathbf{F}_{q^{p^r}})$ and divides g''. It follows that $g' = g''$, so the map which takes g to g' is onto $C^*_\sigma(f;\mathbf{F}_q)$. Finally, to show this map is an isomorphism, let g_1 and g_2 be two polynomials in $C^*_\sigma(h;\mathbf{F}_{q^{p^r}})$ for which $g_1' = g_2'$. If α_i is a root of g_i $(i = 1, 2)$, then there is an automorphism τ of $\hat{\mathbf{F}}_p$ fixing $\mathbf{F}_q$ for which $\tau(\alpha_1) = \alpha_2$. Applying τ to the graph $C^*_\sigma(h;\mathbf{F}_{q^{p^r}})$ and using the fact that α_2 is the root of a unique vertex in $G_\sigma(\mathbf{F}_{q^{p^r}})$ shows that $\tau(h) = h$, and therefore that τ fixes $\mathbf{F}_{q^{p^r}}$ (a field generated by the coefficients of h) elementwise. Hence α_1 and α_2 are conjugate over $\mathbf{F}_{q^{p^r}}$ and $g_1 = g_2$. This proves the theorem. □

Corollary. *If all the roots of $\sigma(x)$ lie in the field $\mathbf{F}_q$, then all the star components of $G_\sigma(\mathbf{F}_q)$ are isomorphic to $C^*_\sigma(x;\mathbf{F}_{q^{p^r}})$ for some $r \geq 0$.*

This corollary shows that to understand the structure of levels ≥ 1 in $G_\sigma(\mathbf{F}_q)$, where $\mathbf{F}_q$ contains the roots of $\sigma(x)$, it is only necessary to know the connected component of x over p-extensions of $\mathbf{F}_q$. In the next two sections we shall compute these components for the two particular maps $\sigma(x) = x^p \pm x$.

4. The graph G_σ for $s(x) = x^p - x$: the connected component of x. In this section we consider the special additive map $\sigma(x) = x^p - x$ over $\mathbf{F}_p$. In preparation for considering the graph G_{x^p-x} we look at the special case $p = 2$, $\sigma(x) = x^2 + x$.

Theorem 4.1. *The vertices in the connected component $C_{x^2+x}(x)$ of x in the graph G_{x^2+x} over $\mathbf{F}_2$ are exactly the irreducible polynomials over $\mathbf{F}_2$ of degree 2^k, $k \geq 0$.*

Proof. First we show that only polynomials of degree 2^k can occur in the connected component of x. If f is a vertex in G_{x^2+x}, then

$f(\sigma(x)) = f(x^2 + x)$ is either irreducible with degree $2 * \deg f$ or it has two irreducible factors whose degrees are equal to $\deg f$, by the corollary to Theorem 2.1. Thus, if $g \to f$, $\deg g = 2^a \deg f$, where $a = 0$ or 1. Since $\deg x = 1$ and $x \to x$, this shows that all vertices f in $C_{x^2+x}(x)$ have degree equal to 2^k for some k.

Now we show that every irreducible polynomial over $\mathbf{F}_2$ of degree 2^k occurs as a vertex. We will give two proofs of this fact, both of which require the formula

$$\sigma^{2^k}(x) = x^{2^{2^k}} + x, \qquad \text{for } k \geq 0. \tag{7}$$

This formula is easily proved using induction.

1) *First proof.* Let f be any irreducible over $\mathbf{F}_2$ of degree 2^k. A root α of f lies in the field $\mathbf{F}_{2^{2^k}}$, and so (7) implies that $\sigma^{2^k}(\alpha) = 0$. Hence $\hat{\sigma}^{2^k}(f) = x$, showing that f is in the connected component of x.

2) *Second proof.* First we note from (7) that for α in $\mathbf{F}_{2^{2^{k+1}}}$

$$\operatorname{tr}_{\mathbf{F}_{2^{2^{k+1}}}/\mathbf{F}_{2^{2^k}}}(\alpha) = \sigma^{2^k}(\alpha), \tag{8}$$

since the extension $\mathbf{F}_{2^{2^{k+1}}}/\mathbf{F}_{2^{2^k}}$ is quadratic with generating automorphism $(\alpha \to \alpha^{2^{2^k}})$.

We show by induction that every irreducible polynomial f of degree 2^k occurs in the component of x. This is clear for $k = 0$, since $x+1 \to x$, and since x and $x+1$ are the only irreducible polynomials of degree 1.

Assume every polynomial of degree $\leq 2^k$ occurs in $C_{x^2+x}(x)$, and let g be a polynomial of degree 2^{k+1}. A root α of g lies in $\mathbf{F}_{2^{2^{k+1}}}$, so $\sigma(\alpha)$ lies in this field, as well, and has a minimal polynomial $f_1(x)$ of degree $\leq 2^{k+1}$. Thus $g \to f_1$. Similarly, $\sigma^2(\alpha)$ is a root of some irreducible polynomial $f_2(x)$ and $g \to f_1 \to f_2$.

Continuing in this way, we get $g \to f_1 \to f_2 \to \cdots \to f_{2^k}$, where $\sigma^{2^k}(\alpha)$ is a root of $f_{2^k}(x)$. By (8), $\sigma^{2^k}(\alpha)$ lies in the field $\mathbf{F}_{2^{2^k}}$. Thus $\deg f_{2^k}(x) \leq 2^k$. By our induction assumption, we know that $f_{2^k}(x)$ is connected to x, and therefore g is also connected to x. This proves the theorem. □

Using the corollary to Theorem 2.1, the first proof can be generalized to give

Theorem 4.2. *The vertices in the connected component $C_{x^p-x}(x)$ of x in the graph G_{x^p-x} over $\mathbf{F}_p$ are exactly the irreducible polynomials over $\mathbf{F}_p$ of degree p^k, $k \geq 0$.*

The proof uses the analogue of (7) for odd primes p:

$$\text{if} \quad \sigma(x) = x^p - x, \qquad \sigma^{p^k}(x) = x^{p^{p^k}} - x, \tag{9}$$

which can be proved using the equation $\sigma = \phi - 1$, where $\phi(x) = x^p$ is the Frobenius map. Note also that $x + a \to x$ in G_{x^p-x} for each $a = 0, 1, \ldots, p-1$.

The second proof of Theorem 4.1 is interesting because it gives a layering of the elements in fields of degree 2^k over $\mathbf{F}_2$ using the map $\sigma(x) = x^2 + x$. The following theorem describes this layering more precisely. We prove the theorem for the map $\sigma(x) = x^p - x$ over $\mathbf{F}_p$, but a similar result holds for the map

$$\begin{aligned}\sigma(x) &= (\phi^{p-1} + \phi^{p-2} + \cdots + \phi + 1)(x) \\ &= x^{p^{p-1}} + x^{p^{p-2}} + \cdots + x^p + x,\end{aligned}$$

which is the trace map for $\mathbf{F}_{p^p}/\mathbf{F}_p$ (cf. the second proof of Theorem 4.1).

Theorem 4.3. *If $k \geq 1$, the irreducible polynomials of degree p^k over $\mathbf{F}_p$ occur in $\varphi(p^k)$ levels of $C_{x^p-x}(x)$, starting wtih $(p-1)p^{p^{k-1}-k}$ polynomials at level $p^{k-1}+1$, branching to p times the previous number in each successive level, for $\varphi(p^k)$ levels. Each polynomial in the last row of irreducibles of degree p^k (at level p^k) is connected to a single irreducible of degree p^{k+1} at level $p^k + 1$.*

Remark. The result of the theorem also holds for $k = 0$ if p^{-1} is interpreted to be 0.

Proof. Recall that the level n of an irreducible polynomial g in $C_{x^p-x}(x)$ is the smallest n for which a root α of g satisfies $\sigma^n(\alpha) = 0$.

The irreducibles of degree p^k don't occur in more than $\varphi(p^k)$ levels of $C_{x^p-x}(x)$: this is a consequence of (9) and the formula

$$\begin{aligned}\sigma^{p^k}(x) &= \sigma^{p^{k-1}}(\sigma^{p^k-p^{k-1}}(x)) \\ &= \{\sigma^{p^k-p^{k-1}}(x)\}^{p^{p^{k-1}}} - \{\sigma^{p^k-p^{k-1}}(x)\},\end{aligned}$$

which shows that if α has degree p^k over $\mathbf{F}_p$, then $\sigma^{\varphi(p^k)}(\alpha)$ has degree at most p^{k-1}. Hence any irreducible of degree p^k is at most $\varphi(p^k)$-step connected to an irreducible of degree $\leq p^{k-1}$.

If $k = 1$, note that all first degree polynomials are 1-step connected to x, so that there are $p-1$ irreducibles of degree p at level 2. Now fix $k \geq 2$ and assume inductively that the first assertion of the theorem holds for degrees $\leq p^{k-1}$. The induction assumption implies that in the last row corresponding to degree p^{k-1} there are

$$(p-1)p^{p^{k-2}-(k-1)} \cdot p^{\varphi(p^{k-1})-1} = (p-1)p^{p^{k-1}-k}$$

irreducibles. Moreover, all the polynomials at any level $\leq p^{k-1}$ $(= 1 + \varphi(p) + \cdots + \varphi(p^{k-1}))$ have the same degree (namely, $\leq p^{k-1}$).

The last two facts imply that there must be $(p-1)p^{p^{k-1}-k}$ irreducibles of degree p^k at level $p^{k-1}+1$. From the corollary to Theorem 2.1 it follows that the total number of polynomials of degree p^k in $C_{x^p-x}(x)$ is at most

$$\begin{aligned}(p-1)p^{p^{k-1}-k}\sum_{j=0}^{\varphi(p^k)-1} p^j &= (p-1)p^{p^{k-1}-k} \cdot \frac{p^{\varphi(p^k)}-1}{p-1} \\ &= \frac{1}{p^k}(p^{p^k} - p^{p^{k-1}}).\end{aligned} \tag{10}$$

This is the maximal number possible because in the first row corresponding to degree p^k, all polynomials have degree p^k, and in each row thereafter there are at most p polynomials connected to the polynomials in the next lower row. But the number in (10) is exactly the total number of irreducible polynomials of degree p^k over $\mathbf{F}_p$. Since all these polynomials must occur in $C_{x^p-x}(x)$ (by the previous theorem), and since they must all occur in these $\varphi(p^k)$ levels, in fact all the

connections accounted for in formula (10) must occur. This proves the theorem. □

From this theorem it is easy to determine the structure of $C_{x^p-x}(x;\kappa)$, where $\kappa = \mathbf{F}_{p^{p^r}}$. This is because a vertex in C_{x^p-x} (over $\mathbf{F}_p$) of degree p^k splits into p^r vertices in $C_{x^p-x}(x;\kappa)$, each of degree p^{k-r}, if $k \geq r$. If $k < r$, such a vertex splits completely into linear factors. If f is a vertex in $C_{x^p-x}(x)$ and f' is any irreducible factor of f over κ, then the level of f' in $C_{x^p-x}(x;\kappa)$ must equal the level of f in $C_{x^p-x}(x)$. Furthermore, $f \to g$ if and only if $f' \to g'$ for some irreducible factors f' of f and g' of g over κ. From these remarks it follows that the edge $f \to g$ in $C_{x^p-x}(x)$, with $\deg f = p^k$, contributes p^k edges to $C_{x^p-x}(x;\kappa)$ if $0 \leq k \leq r$, and p^r edges if $k \geq r$. For example, the vertices with degree 1 occur in levels 0 to p^r of $C_{x^p-x}(x;\kappa)$, while the vertices of degree p^a occur in $\varphi(p^{a+r})$ levels, starting at level $p^{a+r-1}+1$, for $a > 0$. The last assertion of Theorem 4.3 (except for the mention of specific levels) remains valid over κ.

Thus Theorems 3.4 and 4.3 give a complete determination of the structure of the star-components of $G_\sigma(\mathbf{F}_p)$, where $\sigma(x) = x^p - x$.

By the last remark before Theorem 4.3, and the fact that the map σ^n is linear, the roots of the polynomials at level n or less form a vector space over $\mathbf{F}_p$, the nullspace of σ^n. This space is the subject of the next theorem.

Theorem 4.4. *Let $\sigma(x) = x^p - x$, and for $n \geq 0$ let V_n denote the set of roots of polynomials at levels n or less in the connected component $C_{x^p-x}(x)$ of $G_\sigma(\mathbf{F}_p)$. Then V_n is a vector space of dimension n over $\mathbf{F}_p$ and coincides with the set of solutions α in $\hat{\mathbf{F}}_p$ of $\sigma^n(\alpha) = 0$. The spaces V_n give a layering (filtration; composition series)*

$$V_0 \subset V_1 \subset \cdots \subset V_n \subset \cdots \subset V_\infty$$

of the subfield V_∞ of $\hat{\mathbf{F}}_p$ consisting of the elements which have degree p^k, $k \geq 0$, over $\mathbf{F}_p$. The roots of polynomials at level n comprise $p-1$ cosets $k\alpha + V_{n-1}$ of V_{n-1}, $k = 1, 2, \ldots, p-1$, and are therefore invariant under translation by elements of V_{n-1}.

Proof. Setting $\sigma = \phi - 1$, as before, where $\phi(x) = x^p$ is the Frobenius

map, we have

$$\sigma^n(x) = (\phi - 1)^n(x).$$

Using this it is easy to see that the derivative of $\sigma^n(x)$ is $(-1)^n$, so that $\sigma^n(x)$ has no multiple roots. Hence $\sigma^n(x)$ has exactly p^n distinct roots, and this proves the first assertion. The last assertion follows from the fact that V_{n-1} has index p in V_n. □

A similar theorem holds for any additive map with a nonvanishing x term.

Theorem 4.3 also has the following consequence, which gives a connection between Artin-Schreier theory (cf. [**1**]) and the graph G_{x^p-x} and shows how to explicitly find generators for extensions of degree p^k of finite fields of characteristic p.

Theorem 4.5. *Let $\sigma(x) = x^p - x$, and let d be an integer relatively prime to p. Then there is an irreducible polynomial f with degree d lying in a cycle of G_σ. If α is the root of any polynomial at level p^r in $C_\sigma(f)$, the polynomial $\sigma(x) - \alpha = x^p - x - \alpha$ is irreducible over $\mathbf{F}_{p^{dp^r}}$, and its roots generate the cyclic p-extension $\mathbf{F}_{p^{dp^{r+1}}}/\mathbf{F}_{p^{dp^r}}$. For the same α, the polynomial*

$$\sigma^{p^{r+k}-p^r}(x) - \alpha = (\phi^{p^r} - 1)^{p^k-1}(x) - \alpha \tag{11}$$

factors into irreducibles of degree p^k over $\mathbf{F}_{p^{dp^r}}$, so that its roots generate the unique extension of $\mathbf{F}_{p^{dp^r}}$ of degree p^k. The same is true of the polynomial

$$\sigma^{p^{r+k-1}-p^r+1}(x) - \alpha. \tag{12}$$

For the proof we require the following lemma.

Lemma 4.6. *Let $\sigma(x) = x^p - x$ over the field $\mathbf{F}_p$. Let $f(x)$ be an irreducible factor of $\Phi_{n,\sigma}$ of degree d prime to p. Then there are exactly p irreducible polynomials (all of degree d) which are 1-step connected to f in G_σ, one of which is a factor of $\Phi_{n,\sigma}$ and $p-1$ which are not.*

The roots of the latter factors are pre-periodic, but not periodic, points of σ.

Proof. By Part I, Lemma 3.4, there is exactly one factor $h(x)$ of $\Phi_{n,\sigma}$ which divides $f(\sigma(x))$, a polynomial of degree pd. Since there are $p-1$ linear polynomials at level 1 in $C_\sigma(x)$, it follows from Theorem 3.3b) that there are $p-1$ irreducibles g of degree d at level 1 in $C_\sigma(f)$ for which $g \to f$. (Note that $\kappa = \mathbf{F}_p$ in applying Theorem 3.3.) The roots of any such g cannot be periodic points, since otherwise g would have to be a factor of $\Phi_{n,\sigma}$ also (α and $\sigma(\alpha)$ would be roots of g and f, respectively, and would belong to the same orbit). □

Proof of Theorem 4.5. We first demonstrate the existence of the polynomial f. By Theorem 6.2 of Part I every irreducible polynomial whose degree d is prime to p occurs either at level 0 (i.e., in a cycle) or at level 1 in G_{x^p-x}. In fact there are always irreducibles of degree d in cycles of G_{x^p-x}. For if g is at level 1 and has degree d, then $g \to f$ for some f at level 0 with $\deg f \mid \deg g$. Since $\deg f$ is prime to p, Lemma 4.6 implies that $d = \deg g = \deg f$.

Now we appeal to Theorem 4.3. This shows that if α is the root of any polynomial at level p^r in $C_{x^p-x}(x)$, the polynomial $\sigma(x)-\alpha = x^p-x-\alpha$ is irreducible over $\mathbf{F}_{p^{p^r}}$, and its roots generate the cyclic p-extension $\mathbf{F}_{p^{p^{r+1}}}/\mathbf{F}_{p^{p^r}}$. Furthermore, if α is the root of any polynomial at level p^r, the roots of (11), which are roots of polynomials at level p^{r+k}, must have degree p^k over $\mathbf{F}_{p^{p^r}}$ so that (11) must factor over $\mathbf{F}_{p^{p^r}}$ into irreducibles of degree p^k. The same is true of the polynomial (12), as can be seen by considering roots of polynomials at levels $p^{r+k-1}+1$ and p^r in $C_{x^p-x}(x)$.

But by Theorem 4.3b), the component $C^*_\sigma(x)$ is isomorphic to $C^*_\sigma(f)$, in such a way that a vertex g in $C^*_\sigma(x)$ corresponds to a vertex h in $C^*_\sigma(f)$ for which $\deg h = \deg f * \deg g = d \deg g$. This isomorphism preserves levels, by the corollary to Theorem 3.3. Thus the considerations of the preceding paragraph also apply to the graph $C_\sigma(f;\mathbf{F}_p)$ and to the polynomials (11) and (12) over the field $\mathbf{F}_{p^{dp^r}}$, where α is a root of a polynomial at level p^r in $C_\sigma(f)$. This proves the theorem. □

5. The graph G_σ for $\sigma(x) = x^p + x$: the connected component

of x. The dynamics of the map $x^p - x$ are such that all the irreducible polynomials over $\mathbf{F}_p$ whose degrees are powers of p lie in the connected component of x; the roots of these polynomials are therefore pre-periodic with respect to σ. In this section we consider the map

$$\sigma(x) = x^p + x, \quad p \text{ an odd prime.} \tag{13}$$

The first result says that the irreducibles over $\mathbf{F}_p$ of degree p^k lie in cycles of G_σ and have roots that are always *periodic* points of σ. (For the results of this section see also [**2**].)

Theorem 5.1. *If α has degree p^k over $\mathbf{F}_p$, then α is a periodic point of $\sigma(x) = x^p + x$ with primitive period np^k, where n is the order of 2 modulo p.*

Proof. We note first that

$$\sigma^{p^k}(\alpha) = (\phi^{p^k} + 1)(\alpha) = \alpha + \alpha = 2\alpha, \tag{14}$$

where $\phi(x) = x^p$ is, as before, the Frobenius map. It follows that α is a periodic point of σ with primitive period d dividing np^k. Furthermore, (14) implies that α has primitive order n with respect to the map σ^{p^k}. Let $d = mp^r$, with $m|n$ and $r \leq k$. Then α is a root of $\Phi_{mp^r,\sigma}(x)$, and therefore also a root of

$$\Phi_{m,\sigma^{p^r}}(x) = \prod_{i=0}^{r} \Phi_{mp^i,\sigma}(x).$$

(See [**6**], Lemma 3.2] and [**3**, equation (12)].) By Part I, Theorem 4.4, applied to the map $\sigma^{p^r}(x) = x^q + x$ with $q = p^{p^r}$, the irreducible factors of $\Phi_{m,\sigma^{p^r}}(x)$ have degrees which are divisors of $q^e - 1$ over $\mathbf{F}_q$, where e is the order of q mod m. Hence the degree of α over $\mathbf{F}_p$ divides $p^r(q^e - 1)$, which implies that $r = k$ by the assumption that $\deg_{\mathbf{F}_p} \alpha = p^k$. Since α has primitive order n with respect to the map σ^{p^k}, it now follows that $m = n$ and the theorem is proved. □

The next lemma is a first step toward understanding the structure of the connected component $C_\sigma(x)$ in the graph G_σ.

Lemma 5.2. *The complete factorization of the polynomial $x^q + x$ over $\mathbf{F}_q$ is*

$$x^q + x = x \prod_{\alpha \neq \gamma^2} (x^2 - \alpha), \tag{15}$$

where the product is over all the nonsquares α in $\mathbf{F}_q$.

Proof. It is clear that the right side of (15) divides the left side, since

$$\sqrt{\alpha}^{(q-1)} = \alpha^{(q-1)/2} = -1$$

for all α in $\mathbf{F}_q$ which are not squares. Since both sides have the same degree their equality follows. □

In terms of the graph G_σ over $\mathbf{F}_p$ where $\sigma(x) = x^p + x$, Lemma 5.2 says that the polynomials at level 1 in $C_\sigma(x)$ are the binomial quadratic polynomials $x^2 - \alpha$. A similar assertion holds for the components of other linear polynomials:

Lemma 5.3. *For a in $\mathbf{F}_p$, there are $(p-1)/2$ polynomials at level 1 in $C_\sigma(x-a)$, all of which are quadratic. Furthermore, every irreducible quadratic over $\mathbf{F}_p$ occurs at level 1 in $C_\sigma(x-a)$ for some a.*

Proof. By Theorem 5.1, $x - a$ lies in a cycle of G_σ whose length is n, the order of 2 modulo p. Hence $\sigma(2^{n-1}a) = a$ implies that

$$\sigma(x) - a = \sigma(x - 2^{n-1}a)$$

factors the same way that $\sigma(x)$ factors. Thus Lemma 5.2 implies the first claim. The second claim follows from counting the number of quadratic polynomials we have just determined: this number is $p(p-1)/2 = (p^2 - p)/2$, which is the total number of irreducible quadratics over $\mathbf{F}_p$. □

In order to understand the structure of $C_\sigma(x)$, it turns out that we need to simultaneously determine the structure of all the components

$C^*_\sigma(f)$, where f is a polynomial of degree p^k, $k \geq 0$. The next theorem describes the first p^k levels of $C^*_\sigma(f)$, and generalizes the last lemma.

Theorem 5.4. *Let $f(x)$ be an irreducible polynomial of degree p^k over $\mathbf{F}_p$. In levels 1 to p^k of $C^*_\sigma(f)$ there are $(p^{p^k}-1)/2$ polynomials, all of degree $2p^k$.*

Proof. We first consider the connected component $C^*_\sigma(x-\alpha;\mathbf{F}_q)$, where $q = p^{p^k}$ and α is one of the p^k roots of $f(x)$ (lying in $\mathbf{F}_q$). The vertices in levels 1 to p^k of this component are factors of $\sigma^{p^k}(x) - \alpha$. By (14) we have that $\sigma^{p^k}(2^{n-1}\alpha) = \alpha$ (n = order of 2 mod p), and because σ^{p^k} is linear over $\mathbf{F}_q$ we have

$$\sigma^{p^k}(x) - \alpha = \sigma^{p^k}(x - 2^{n-1}\alpha).$$

On the other hand $\sigma^{p^k}(x - 2^{n-1}\alpha)$ factors the same way over $\mathbf{F}_q$ as does $\sigma^{p^k}(x) = x^q + x$. Lemma 5.2 shows that $\sigma^{p^k}(x) - \alpha$ factors into one linear polynomial $(x - 2^{n-1}\alpha)$ and $(q-1)/2$ irreducible quadratic polynomials over $\mathbf{F}_q$. Hence

$$f(\sigma^{p^k}(x)) = \prod_{i=1}^{p^k} (\sigma^{p^k}(x) - \alpha_i) \tag{16}$$

has p^k linear and $p^k(q-1)/2$ quadratic factors over $\mathbf{F}_q$. It is clear that the linear factors are all distinct. Since f lies in a cycle of G_σ, the product of the linear factors must be an irreducible polynomial of degree p^k over $\mathbf{F}_p$. Furthermore, the other irreducible factors of $f(\sigma^{p^k}(x))$ must have degrees which are divisible by p^k, since they are connected to f in G_σ. Equation (16) and the above discussion show that these factors must also have degrees which are divisible by 2. Since their roots have degree 2 over $\mathbf{F}_q$, these factors must all have degree equal to $2p^k$.

Now f lies in a cycle whose length r divides np^k by Theorem 5.1. Let this cycle be

$$f = f_r \to f_{r-1} \to \cdots \to f_1 \to f,$$

where subscripts are to be read modulo r (thus $f = f_r = f_0$). All of the polynomials in this cycle have degree p^k, so the foregoing discussion

applies to all of them. Thus $f_i(\sigma^{p^k}(x))$ factors the same way that $f(\sigma^{p^k}(x))$ does.

Clearly $f(\sigma(x))$ is f_1 times the product of the vertices at level 1 in $C^*_\sigma(f)$, $f(\sigma^2(x))$ is f_2 times the product of the vertices at level 1 in $C^*_\sigma(f_1)$ times the product of the vertices at level 2 in $C^*_\sigma(f)$, and in general, $f(\sigma^i(x))$ is f_i times the product of the vertices at level $i-j$ in $C^*_\sigma(f_j)$, as j ranges from 0 to i.

Since for all j, $f_j(\sigma^{p^k}(x))$ is a product of a single irreducible of degree p^k times a number of irreducibles of degree $2p^k$, it follows that all of the polynomials in $C^*_\sigma(f_i)$ at levels 1 to p^k must have degree $2p^k$ for any i. In particular, all of the star components $C^*_\sigma(f_i)$ are isomorphic to each other up to level p^k (this would also follow from Theorem 3.4) so the number of irreducible factors of $f(\sigma^{p^k}(x))$ of degree $2p^k$ is equal to the number of vertices in $C^*_\sigma(f)$ in levels 1 to p^k. The first part of the proof shows that this number is $(q-1)/2$, and this proves the theorem. □

To determine the structure of $C^*_\sigma(x)$, we shall inductively determine where in G_σ all the polynomials of degree $2p^k$ are located. The last theorem accounts for $(p^{p^k}-1)/2$ of these polynomials in the connected component of each irreducible of degree p^k. Since the number of irreducibles of degree p^k is $(p^{p^k}-p^{p^{k-1}})/p^k$, this accounts for a total of

$$\frac{1}{2}(p^{p^k}-1)\frac{1}{p^k}(p^{p^k}-p^{p^{k-1}}) = \frac{1}{2p^k}(p^{2p^k}-p^{p^k+p^{k-1}}-p^{p^k}+p^{p^{k-1}})$$

polynomials. As is well known, the total number of irreducibles of degree $2p^k$ is

$$N(2p^k;\mathbf{F}_p) = \frac{1}{2p^k}(p^{2p^k}-p^{2p^{k-1}}-p^{p^k}+p^{p^{k-1}}).$$

(See [**5**] or [**3**, equation (4)].) Thus there are

$$\frac{1}{2p^k}(p^{p^k+p^{k-1}}-p^{2p^{k-1}})$$

polynomials still to locate. We shall show that these remaining polynomials are all factors of the polynomial

$$h_k(x) = (\phi^{2p^{k-1}}-1)\circ\sigma^{\varphi(p^k)}(x), \qquad k\geq 1, \tag{17}$$

where $\phi(x) = x^p$ and φ denotes the Euler φ-function.

Lemma 5.5. *An element α of $\hat{\mathbf{F}}_p$ is a root of $h_k(x)$ if and only if $\alpha^q + \alpha \in \mathbf{F}_{p^{p^{k-1}}}$, where $q = p^{p^k}$. Further, $h_k(x)$ has no multiple roots.*

Proof. From (17) we have

$$\begin{aligned} h_k(x) &= (\phi^{p^{k-1}} - 1) \circ (\phi^{p^{k-1}} + 1) \circ \sigma^{\varphi(p^k)}(x) \\ &= (\phi^{p^{k-1}} - 1) \circ (\phi + 1)^{p^{k-1}} \circ (\phi + 1)^{p^k - p^{k-1}}(x) \\ &= (\phi^{p^{k-1}} - 1) \circ (\phi + 1)^{p^k}(x) \\ &= (\phi^{p^{k-1}} - 1) \circ (x^q + x). \end{aligned}$$

It follows that α is a root of $h_k(x)$ if and only if $\alpha^q + \alpha$ is fixed by $\phi^{p^{k-1}}$, which is the case exactly when $\alpha^q + \alpha \in \mathbf{F}_{p^{p^{k-1}}}$.

The fact that $h_k(x)$ has no multiple roots follows from $h_k'(x) = -1$, which can be easily checked using the last equation. □

We now prove

Theorem 5.6. (a) *For $k \geq 1$, the irreducible factors of $h_k(x)$ consist of all the irreducible polynomials whose degrees divide $2p^{k-1}$ and*

$$\frac{1}{2p^k}(p^{p^k + p^{k-1}} - p^{2p^{k-1}})$$

irreducible polynomials of degree $2p^k$.

(b) *For $k \geq 1$, the polynomials of degree $2p^k$ occur in levels $p^{k-1} + 1$ to p^k of the connected components of irreducibles whose degrees divide p^{k-1}, and in levels 1 to p^k of the irreducibles of degree p^k. Moreover, these levels consist entirely of polynomials of degree $2p^k$.*

(c) *Let f be irreducible with $\deg f = p^r$, $0 \leq r \leq k-1$. Then at level $p^{k-1} + 1$ of $C_\sigma^*(f)$, the first level at which polynomials of degree $2p^k$ occur, there are exactly*

$$p^r \cdot p^{p^{k-1} - k} \left(\frac{p-1}{2} \right) \tag{18}$$

irreducibles of degree $2p^k$.

Proof. We first prove parts (a) and (b) together by induction. For general k note that all the irreducible polynomials g whose degrees divide $2p^{k-1}$ are factors of $h_k(x)$. This is clear from Lemma 5.5 since a root α of g either lies in the field $\mathbf{F}_{p^{p^{k-1}}} = \mathbf{F}_q$ or is quadratic over this field, and since $\alpha^{q^p} + \alpha (q = p^{p^{k-1}})$ is the trace of α to $\mathbf{F}_q$ in the latter case.

We next check the case $k = 1$ of (a). We consider the roots α of $h_1(x)$ which are not linear or quadratic. By Lemma 5.5, $\alpha^{p^p} + \alpha = \sigma^p(\alpha)$ lies in $\mathbf{F}_p$. This shows the minimal polynomial g of α is at most p-step connected to a linear polynomial, and therefore at most $p-1$ step connected to a quadratic polynomial by Lemma 5.3. It follows that 2 divides $\deg g = \deg \alpha$. Furthermore, $\deg \alpha$ divides $2p$, since

$$\alpha^{p^{2p}} - \alpha = (\alpha^{p^p} + \alpha)^{p^p} - (\alpha^{p^p} + \alpha) = 0$$

($\alpha^{p^p} + \alpha$ is an element of $\mathbf{F}_p \subset \mathbf{F}_{p^p}$). Hence $\deg \alpha = 2p$. It follows that the number of irreducible factors of $h_1(x)$ of degree $2p$ is

$$\frac{1}{2p}(\deg h_1(x) - p^2) = \frac{1}{2p}(p^{p+1} - p^2),$$

proving (a) for $k = 1$.

Now consider (b) for $k = 1$. The last argument shows that there are $(p^{p+1} - p^2)/2p$ irreducibles of degree $2p$ above linear components $C_\sigma(x-a)$, and these occur in levels 2 to p. Since the linear components $C_\sigma(x-a)$ are all isomorphic (either by Theorem 3.4 or the argument in Theorem 5.4), there are $(p^{p-1} - 1)/2$ of these polynomials per component. By Lemma 5.3 and Corollary 2.3 (with $\kappa = \mathbf{F}_{p^2}$ and $d = 2$) there must be $(p-1)/2$ polynomials of degree p at level 2 in $C_\sigma(x-a)$, and then each vertex at level i must be connected to p vertices at level $i+1$ (for $2 \le i \le p-1$), in order for the total number of polynomials of degree $2p$ to be $(p^{p-1} - 1)/2$; this is because

$$\frac{p-1}{2}(1 + p + \cdots + p^{p-2}) = \frac{p^{p-1} - 1}{2}. \tag{19}$$

(This argument is similar to the argument used in Theorem 4.3.) This shows that all of the vertices at levels 2 to p in $C_\sigma(x-a)$ have degree

$2p$. (Alternatively, any polynomial g in $C_\sigma(x-a)$ at a level between 2 and p must be a factor of $h_1(x)$ by (17), since g is no more than $p-1$ step connected to a quadratic polynomial at level 1. This implies that $\deg g$ has to be $2p$.) The other assertions of (b) for $k=1$ follow from the case $k=1$ of Theorem 5.4.

Now assume that both (a) and (b) hold for $k-1$ in place of k, where $k \geq 2$. Consider (a) first. By the remarks at the beginning of the proof, all the irreducible polynomials g whose degrees divide $2p^{k-1}$ are factors of $h_k(x)$. Let α be a root of $h_k(x)$, and assume that the degree of α does not divide $2p^{k-1}$. By Lemma 5.5, $\alpha^{q^p} + \alpha = \sigma^{p^k}(\alpha)$ lies in $\mathbf{F}_q$, where $q = p^{p^{k-1}}$. This shows the minimal polynomial g of α is at most p^k-step connected to a polynomial of degree p^{k-1}, and therefore at most $(p^k - p^{k-1})$-step connected to a polynomial of degree $2p^{k-1}$, by part (b) (for $k-1$). It follows that $2p^{k-1}$ divides $\deg g = \deg \alpha$. Furthermore, $\deg \alpha$ divides $2p^k$, since

$$\alpha^{p^{2p^k}} - \alpha = (\alpha^{p^{p^k}} + \alpha)^{p^{p^k}} - (\alpha^{p^{p^k}} + \alpha) = 0$$

($\alpha^{p^{p^k}} + \alpha$ is an element of $\mathbf{F}_{p^{p^{k-1}}} \subset \mathbf{F}_{p^{p^k}}$). Hence $\deg \alpha = 2p^k$. It follows that the number of irreducible factors of $h_k(x)$ of degree $2p^k$ is

$$\nu_k = \frac{1}{2p^k}(\deg h_k(x) - p^{2p^{k-1}}) = \frac{1}{2p^k}(p^{p^k+p^{k-1}} - p^{2p^{k-1}}),$$

proving (a) for k.

Now we turn to the proof of (b) for k. The last argument shows that there are ν_k irreducibles of degree $2p^k$ above components $C_\sigma(f)$, where $\deg f$ divides p^{k-1}, and these occur in levels $p^{k-1}+1$ to p^k. Note also that any polynomial which lies in one of these levels is a factor of $h_k(x)$, by its defining formula (17), and by the induction assumption (part b). Thus all of the polynomials in one of the levels $p^{k-1}+1$ to p^k must have degree $2p^k$. The rest of part (b) follows from Theorem 5.4.

To prove part (c), let $r \geq 1$ be fixed. The first step of the induction is $k = r+1$. By Theorem 5.4 there are $(p^{p^r}-1)/2$ polynomials of degree $2p^r$ in levels 1 to p^r of $C_\sigma^*(f)$. Each polynomial at a level between 1 and $p^r - 1$ must branch to p polynomials at the next level, by Corollary 2.3. If s denotes the number of polynomials at level 1, then the equation

$$s(1 + p + \cdots + p^{p^r-1}) = \frac{p^{p^r}-1}{2}$$

implies that $s = (p-1)/2$. Hence, there are

$$p^{p^r-1}\left(\frac{p-1}{2}\right) = p^{p^{k-1}+r-k}\left(\frac{p-1}{2}\right)$$

polynomials at level $p^r + 1 = p^{k-1} + 1$. If the formula (18) holds for $k-1$, then there are

$$p^r \cdot p^{\varphi(p^{k-1})-1} p^{p^{k-2}-(k-1)}\left(\frac{p-1}{2}\right) = p^r \cdot p^{p^{k-1}-k}\left(\frac{p-1}{2}\right)$$

irreducibles of degree $2p^{k-1}$ at level p^{k-1}, and therefore the same number of polynomials of degree $2p^k$ at level $p^{k-1}+1$. This completes the proof. □

We summarize the result for $C_\sigma(x)$ separately.

Theorem 5.7. *Let $\sigma(x) = x^p + x$. The structure of $C_\sigma(x)$ can be described as follows: there are $(p-1)/2$ quadratic polynomials at level 1 in $C_\sigma(x)$. At level $p^{k-1}+j$, for $k \geq 1$ and $1 \leq j \leq \varphi(p^k)$, there are $p^{p^{k-1}-k+j-1}((p-1)/2)$ polynomials of degree $2p^k$. Thus all of the polynomials in $C_\sigma(x)$ have degree 1, 2 or $2p^k$, and all polynomials at a given level have the same degree.*

By Theorem 3.4, the results of Theorems 5.6 and 5.4 completely determine the structure of all of the fundamental components $C^*_\sigma(x; \mathbf{F}_{p^{p^r}})$, since the latter two theorems describe the structure of $C^*_\sigma(f)$, where $\deg f = p^r$. Thus we have determined the structure of the graph $G_\sigma(\mathbf{F}_{p^2})$, up to knowing cycle lengths. (Note that each vertex f in $G_\sigma(\mathbf{F}_p)$ contributes 1 or 2 vertices to $G_\sigma(\mathbf{F}_{p^2})$, according to whether $\deg f$ is odd or even. See the paragraph following Theorem 4.3 and Corollary 2.3.) The results of this section also give an independent proof that $C^*_\sigma(f_1)$ is isomorphic to $C^*_\sigma(f_2)$ whenever $\deg f_1 = \deg f_2 = p^r$.

Note added in proof. There is a slight error in the statement of the Reciprocity theorem (Theorem 6.3 and its corollary) in [**3**]. The word "roots" should be replaced everywhere in these results by "primitive roots".

REFERENCES

1. E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, in *The collected papers of Emil Artin*, Addison-Wesley, 1965, 289–295.

2. A. Batra, *Iterated maps on finite fields and applications to algebraic number theory*, Honors thesis, Wellesley College, 1993.

3. A. Batra and P. Morton, *Algebraic dynamics of polynomial maps on the algebraic closure of a finite field*, I, Rocky Mountain J. of Math. **24** (1994), 453–481.

4. A. Bremner and P. Morton, *Polynomial relations in characteristic p*, Quart. J. Math. Oxford **29** (1978), 335–347.

5. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of mathematics and its applications, vol. 20, Addison-Wesley Publ. Co., 1983.

6. P. Morton and P. Patel, *The Galois theory of periodic points of polynomial maps*, Proc. London Math. Soc., to appear.

7. B.L. van der Waerden, *Algebra*, vol. 1, Frederick Ungar Publishing Co., 1971.

Department of Mathematics, University of Illinois at Urbana–Champaign, Urbana, Illinois 61801

Department of Mathematics, Wellelsey College, Wellesley, MA 02181