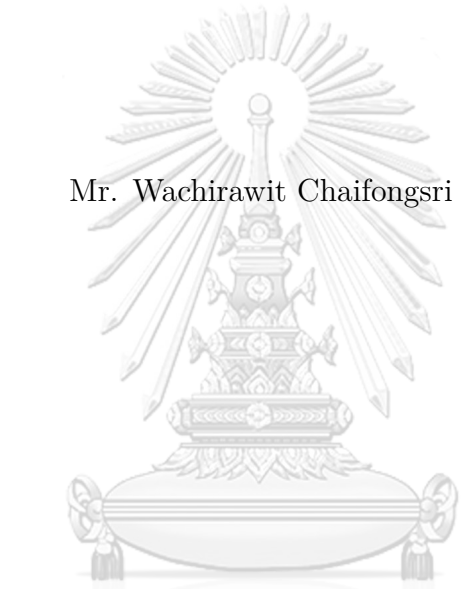
วัฏจักรแฮมิลตันของกราฟเชิงสมการเหนือฟิลด์จำกัด

นาย วชิรวิทย์ ไชยฟองศรี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2564

HAMILTONIAN CYCLES OF EQUATIONAL GRAPHS OVER FINITE FIELDS

Mr. Wachirawit Chaifongsri



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science Chulalongkorn University
Academic Year 2021

Thesis Title	HAMILTONIAN CYCLES OF EQUATIONAL GRAPHS OVER FINITE FIELDS
By	Mr. Wachirawit Chaifongsri
Field of Study	Mathematics
Thesis Professor	Professor Yotsanan Meemark, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master's Degree.

..... Dean of the Faculty of Science
(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

..... Chairman
(Associate Professor Sajee Pianskool, Ph.D.)

..... Thesis Advisor
(Professor Yotsanan Meemark, Ph.D.)

..... Committee
(Associate Professor Tuangrat Chaichana, Ph.D.)

..... External Examiner
(Professor Patanee Udomkavanich, Ph.D.)

วชิรวิทย์ ไชยฟองศรี: วัฏจักรแฮมิลตันของกราฟเชิงสมการเหนือฟิลด์จำกัด. (HAMILTONIAN CYCLES OF EQUATIONAL GRAPHS OVER FINITE FIELDS
อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ศาสตราจารย์ ดร. ยศนันต์ มีมาก, 29 หน้า.

กำหนดให้ $\mathbb{F}_q$ เป็นฟิลด์จำกัดที่มีสมาชิก q ตัว สำหรับแต่ละสมการ $E(X,Y)=0$ เหนือ $\mathbb{F}_q$ กราฟเชิงสมการที่สอดคล้องกับสมการนี้เป็นไดกราฟที่มีเซตของจุดยอดเป็น $\mathbb{F}_q$ และ สำหรับ x และ y ใน $\mathbb{F}_q$ มีเส้นเชื่อมจาก x ไปยัง y ก็ต่อเมื่อ $E(x,y)=0$ ในงานวิจัยครั้งนี้ เราสมมติให้ $q-1\geq k$ และศึกษากราฟเชิงสมการ $\mathcal{G}^{(k)}(\lambda,f)$ ที่สอดคล้องกับสมการ

$$(Y^k-f(X))(\lambda Y^k-f(X))\dots(\lambda^{k-1}Y^k-f(X))=0$$

เมื่อ X และ Y เป็นตัวแปร $f(t)$ เป็นพหุนามใน $\mathbb{F}_q[t]$ และ λ เป็นสมาชิกใน $\mathbb{F}_q^\times$ ที่มีอันดับอย่างน้อย k เราศึกษาความเชื่อมโยงอย่างเข้มและการมีอยู่ของวัฏจักรแฮมิลตันของกราฟ $\mathcal{G}^{(k)}(\lambda,f)$ นอกจากนี้เราสามารถจำแนกกราฟเชิงสมการ $\mathcal{G}^{(3)}(\lambda,f)$ เชิงสมสัณฐานเมื่อ $f(t)$ เป็นพหุนามใน $\mathbb{F}_q[t]$ และหาเงื่อนไขบางอย่างของการมีอยู่ของส่วนประกอบที่มีจำนวนจุดยอดไม่มาก

ภาควิชา . . คณิตศาสตร์และวิทยาการคอมพิวเตอร์ . . ลายมือชื่อนิสิต . . . . . .
สาขาวิชา . . คณิตศาสตร์ . . ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก . . . . . .
ปีการศึกษา . . . . . 2564 . . . . .

##6370180823 : MAJOR MATHEMATICS.
KEYWORDS: EQUATIONAL GRAPHS / FINITE FIELDS / HAMILTONIAN CYCLE / POWER MAPPING / STRONGLY CONNECTIVITY
WACHIRAWIT CHAIFONGSRI: HAMILTONIAN CYCLES OF EQUATIONAL GRAPHS OVER FINITE FIELD
ADVISOR: PROFESSOR YOTSANAN MEEMARK, Ph.D., 29 pp.

Let $\mathbb{F}_q$ be the finite field of q elements. For any equation $E(X,Y)=0$ over $\mathbb{F}_q$, the equational graph of this equation is a digraph whose vertex set is $\mathbb{F}_q$ and for $x,y\in\mathbb{F}_q$ there is the edge from x to y if $E(x,y)=0$. In this work, we assume that $q-1\geq k$ and work on the equational graph $\mathcal{G}^{(k)}(\lambda,f)$ associated with the equation

$$(Y^k-f(X))(\lambda Y^k-f(X))\dots(\lambda^{k-1}Y^k-f(X))=0$$

with variables X and Y, where $f(t)\in\mathbb{F}_q[t]$ and λ is an element in $\mathbb{F}_q^\times$ of order at least k. We study strongly connectivity and the existence of Hamiltonian cycle of the graph $\mathcal{G}^{(k)}(\lambda,f)$. Moreover, we classify the equational graph $\mathcal{G}^{(3)}(\lambda,f)$ up to isomorphism where $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$ and find some conditions for the existence of components with small vertices.

Department	Mathematics and Computer Science	Student's Signature	.....
Field of Study	Mathematics	Advisor's Signature	.....
Academic Year	2021		

Acknowledgements

I would like to express my special thanks of gratitude to my advisor, Professor Yotsanan Meemark, Ph.D. who gives me an opportunity to do this thesis. It also helps me in doing a lot of research and I come to know about so many new things I am really thankful to them. Also, I would like to express my thanks to thesis committee: Associate Professor Sajee Pianskool, Ph.D., Associate Professor Tuangrat Chaichana, Ph.D. and Professor Patanee Udomkavanich, Ph.D. for their great suggestions and comments. Finally, I would like to thank my parents and friends who help me a lot in finalizing this thesis within the limited time frame.

Wachirawit Chaifongsri

Contents

CHAPTER I
PRELIMINARIES

1.1 Directed graphs and equational graphs

A *directed* graph (digraph) G consists of a vertex set $V(G)$ and an *arc* set $E(G)$ where a directed edge is an ordered pair of vertices in $V(G)$, a direction of an edge is indicated with an arrow, as in Figure 1.1 below. This might happen that an edge connects a vertex to itself and we obtain a *loop*.

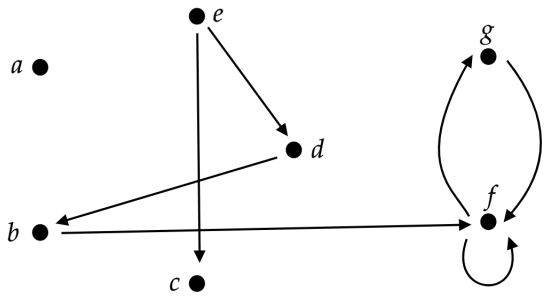


Figure 1.1: A directed graph G

For a directed graph, a vertex x is a *predecessor* of y if there is an edge from x to y. Otherwise, x is a *successor* of y if there is an edge from y to x. The *in-degree* of a vertex is the number of its predecessors and the *out-degree* of a vertex is the number of its successors. Two directed graphs G_1 and G_2 are *isomorphic* if there is a bijection τ from $V(G_1)$ to $V(G_2)$ which preserves adjacency conditions, that is, there is an edge from u to v in G_1 if and only if there is an edge from $\tau(u)$ in to $\tau(v)$ in G_2. A (directed) *path* of length r from x to y in a directed graph is a sequence of $r+1$ distinct vertices $x = a_1, a_2, \ldots, a_{r+1} = y$ such that for every $s \in \{1, 2, \ldots, r\}$ there is an edge from a_s to a_{s+1}. A *cycle* in a directed graph is a

directed path (with at least one edge) whose first and last vertices are the same. If a path in a directed graph visits each vertex exactly once, we call this *Hamiltonian path*. A *Hamiltonian cycle* is a Hamiltonian path that is a cycle. For example, the graph G in Figure 1.2 has a Hamiltonian cycle, its Hamiltonian path is as follows: $a_1 \to a_2 \to a_3 \to a_4 \to a_1$.

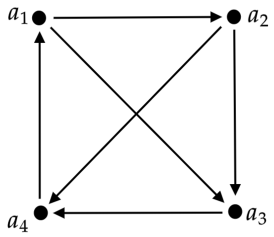


Figure 1.2: The directed graph G with a Hamiltonian cycle

Note that a directed graph containing a Hamiltonian path may not have a Hamiltonian cycle. For instance, the directed graph H in Figure 1.3 has no out-degree of the vertex b_0, so a Hamiltonian cycle does not exist. But its Hamiltonian path is as follows: $b_1 \to b_2 \to b_3 \to b_4 \to b_5 \to b_6 \to b_0$.

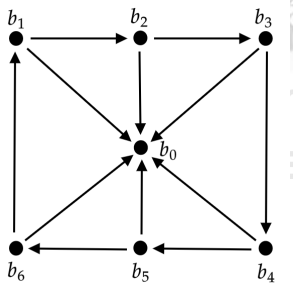


Figure 1.3: The directed graph H without Hamiltonian cycles

A directed graph is *bipartite* if its vertex set can be partitioned into two sets G_1 and G_2, where every edge in the graph goes from a vertex in G_1 to a vertex in G_2 and there is no adjacent edge between two vertices in the G_1 or G_2. For example, the graph $\mathcal{G}$ whose vertex set can be partitioned into two sets $\mathcal{G}_1 = \{a, b\}$ and $\mathcal{G}_2 = \{c, d, e\}$ (see Figure 1.4).

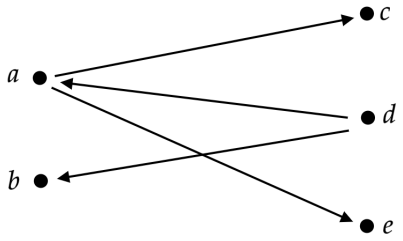


Figure 1.4: The bipartite graph $\mathcal{G}$

A *weak path* in any digraph is a sequence $a_0, a_1, \ldots, a_r$ of distinct vertices for which there is an undirected edge between a_{i-1} and a_i for each $i = 1, 2, \ldots, r$. A digraph is said to be *weakly connected* if any two vertices can be joined by a weak path. We say that a directed graph is *strongly connected* if it is possible to reach any vertex starting from any vertex in a graph. A *weakly connected component* of a directed graph is a maximal weakly connected subgraph. It is well known that a directed graph can be partitioned into a disjoint union of weakly connected components. For the notation, we abbreviate a *component* for a weakly connected component. A strongly connected directed graph is always weakly connected, but a weakly connected directed graph may not be strongly connected (see Figure 1.5).

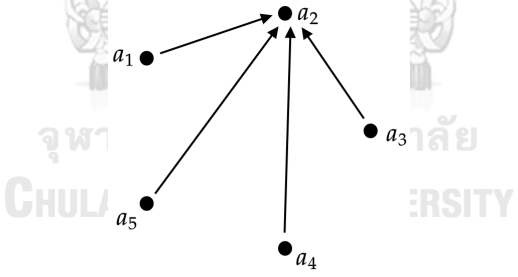


Figure 1.5: A non-strongly connected directed graph

Let $\mathbb{F}_q$ be the finite field of q elements. For a function f on $\mathbb{F}_q$, we define the *functional graph* of f as a digraph of q vertices labeled by the elements of $\mathbb{F}_q$, where there is an edge from u to v if and only if $f(u) = v$. By working on polynomials over $\mathbb{F}_q$, Knoyagin et al. [4] found algorithms to estimate the number of non-isomorphism functional graphs and provided an upper bound on the number of functional graphs. Later, Mans et al. [5] provided algorithms on quadratic polynomials over finite

fields to approximate the number of connected functional graphs, the number of graphs having a maximal cycle, the number of cycles of fixed size and the number of components of fixed size.

Mans et al. [5] suggested that almost all of the functional graphs generated by the polynomial $f(t) = t^2 + a \in \mathbb{F}_q[t]$ are weakly connected.

More generally, for an equation over $\mathbb{F}_q$:

$$E(X, Y) = 0$$

with variables X and Y, we may define a digraph by letting elements in $\mathbb{F}_q$ as vertices and drawing an edge from u to v in $\mathbb{F}_q$ if and only if $E(u, v) = 0$. We call this graph an *equational graph* associated with the above equation.

Mans et al. [6] studied the equational graph associated with the equation

$$E(X, Y) = (Y^2 - f(X))(\lambda Y^2 - f(X)) = 0$$

with variables X and Y, $f(t)$ is a polynomial over $\mathbb{F}_q$, where q is odd and λ is a non-square element in $\mathbb{F}_q$. It is denoted by $\mathcal{G}^{(2)}(\lambda, f)$ (see Figure 1.6).

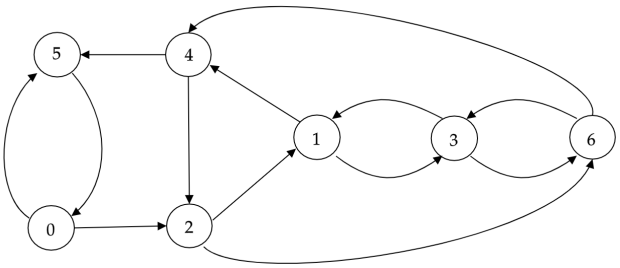


Figure 1.6: The equational graph $\mathcal{G}^{(2)}(3, 2t + 4)$ over $\mathbb{Z}_7$

A polynomial $f(t)$ in $\mathbb{F}_q[t]$ is a *permutation polynomial* if the map $x \mapsto f(x)$ gives a bijection from $\mathbb{F}_q$ onto itself. Mans et al. obtained properties on vertices when $f(t)$ is a permutation polynomial as follows.

Proposition 1.1.1. *[6] Let $f(t)$ be a permutation polynomial over $\mathbb{F}_q$ where q is odd. For the graph $\mathcal{G}^{(2)}(\lambda, f)$,*

1. *if $f(0) \neq 0$, then the vertex 0 has in-degree 1 and out-degree 2, the vertex $f^{-1}(0)$ has in-degree 2 and out-degree 1, and the vertex x ($x \neq 0$ and $x \neq f^{-1}(0)$) has in-degree 2 and out-degree 2, and*

2. *if* $f(0) = 0$*, then the vertex* 0 *has in-degree* 1 *and out-degree* 1*, and the vertex* x $(x \neq 0)$ *has in-degree* 2 *and out-degree* 2.

It follows from the above proposition that every vertex lies in a cycle and also every edge lies in a cycle. It also implies that every Mans' graph is not a bipartite graph. Note that there is a strongly connected digraph whose some component does not have a Hamiltonian cycle (see Corollary 3.8.2 of [2]). Mans et al. showed that

Theorem 1.1.2. *[6] If* $f(t)$ *is a permutation polynomial in* $\mathbb{F}_q[t]$ *where* q *is odd, then every component of the graph* $\mathcal{G}^{(2)}(\lambda, f)$ *has a Hamiltonian cycle.*

Some examples for the non-permutation polynomials were also provided in [6]. Mans et al. also analyzed the graphs and obtained some algorithms for searching Hamiltonian cycles when $f(t)$ is of degree $1, 2$ or 3. In addition, they [6] classified the equational graphs $\mathcal{G}^{(2)}(\lambda, f)$ up to isomorphism where $f(t)$ is a permutation polynomial of degree one (a linear polynomial). They showed that $\mathcal{G}^{(2)}(\lambda, at + b)$ is isomorphic to $\mathcal{G}^{(2)}(\lambda, t + a^{-1}b)$ for any $a \neq 0$ and $b \in \mathbb{F}_q$. Thus, they studied components with $2, 3$ or 4 vertices of $\mathcal{G}^{(2)}(\lambda, t + b)$ for every $b \in \mathbb{F}_q$. Their results suggested that almost of graphs $\mathcal{G}^{(2)}(\lambda, f)$ are connected where $f(t)$ is a linear polynomial in $\mathbb{F}_q[t]$.

1.2 The kth power mapping on finite fields

Let $\mathbb{F}_q$ be the finite fields of q elements. We write $\mathbb{F}_q^\times$ for its multiplicative group of nonzero elements. Let $k \geq 2$ be a positive integer. Consider the kth power mapping φ_k on $\mathbb{F}_q^\times$ given by $\varphi_k(a) = a^k$ for all $a \in \mathbb{F}_q^\times$. The kernel of φ_k is $\{a \in \mathbb{F}_q^\times : a^k = 1\}$ and the image of φ_k is $\{a^k : a \in \mathbb{F}_q^\times\}$, the set of the kth power elements. The following result gives the structure of the multiplicative group $\mathbb{F}_q^\times$.

Theorem 1.2.1. *[1] The multiplicative group* $\mathbb{F}_q^\times$ *is a cyclic of order* $q - 1$*. Its generators are called primitive elements of* $\mathbb{F}_q$*.*

Next, we discuss some basic tools in group theory. Let ϕ be the *Euler* ϕ*-function*, that is, a function counting positive integers up to a given natural number n that are relatively prime to n.

Theorem 1.2.2. *[3] Let G be a cyclic group of order n generated by a.*

1. *For each positive divisor d of n, the group G has exactly one subgroup of order d, namely $\langle a^{n/d} \rangle$.*

2. *If d is a positive divisor of n, then the number of elements of order d in a cyclic group G of order n is $\phi(d)$.*

3. $\sum_{d|n} \phi(d) = n$.

We proceed to compute the size of $\ker \varphi_k$. By Theorem 1.2.2, if $d \mid q-1$, then the number of elements of order d in $\mathbb{F}_q^\times$ is $\phi(d)$ and there are no elements of order d in $\mathbb{F}_q^\times$ otherwise. Since $\ker \varphi_k$ consists of elements in $\mathbb{F}_q^\times$ of order a divisor of k, by Theorem 1.2.2 (3), we have

$$|\ker \varphi_k| = \sum_{d|k} |\{a \in \mathbb{F}_q^\times : \circ(a) = d\}| = \sum_{d|\gcd(k,q-1)} \phi(d) = \gcd(k, q-1).$$

It follows that

$$|\operatorname{im} \varphi_k| = |\mathbb{F}_q^\times / \ker \varphi_k| = \frac{q-1}{\gcd(k, q-1)}.$$

In particular, we have φ_k is injective if and only if $\gcd(k, q-1) = 1$, and in this case, every element in $\mathbb{F}_q^\times$ is the kth power. On the other hand, if $k \mid q-1$, then $|\ker \varphi_k| = k$ and the polynomial $t^k - 1$ splits into monic linear factors in $\mathbb{F}_q[t]$ and $\mathbb{F}_q^\times / \operatorname{im} \varphi_k$ is a cyclic group of order k. We can apply these observations to study the generalized equational graphs introduced in Section 1.1 of Mans et al. [6].

1.3 Our graphs

Let $k \geq 2$ be a positive integer. Assume that $k \leq q-1$. Then there is an element λ in $\mathbb{F}_q^\times$ of order at least k. A directed graph whose vertex set is $\mathbb{F}_q$ and for $x, y \in \mathbb{F}_q$ there is a directed edge from x to y if

$$(y^k - f(x))(\lambda y^k - f(x)) \dots (\lambda^{k-1} y^k - f(x)) = 0.$$

is called *the digraph associated with the polynomial* $f(t) \in \mathbb{F}_q[t]$. It is denoted by $\mathcal{G}^{(k)}(\lambda, f)$. If q is odd and $k = 2$, it is a Mans' graph. Mans et al. suggested the above equation in their comments in Section 7 of [6].

In this thesis, we use the kth power mapping to study the graph $\mathcal{G}^{(k)}(\lambda, f)$ where $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$. The work is organized as follows. In Chapter 2, we assume that $\lambda \operatorname{im} \varphi_k$ generates the quotient group $\mathbb{F}_q^\times / \operatorname{im} \varphi_k$ and prove that every vertex has a positive in-degree and out-degree in Section 2.1. This implies the strong connectivity of the graph. Moreover, if $k \mid (q-1)$, then a Hamiltonian cycle exists. This proof is presented in Section 2.2 together with some examples. In Section 3.1, we classify the equational graphs $\mathcal{G}^{(3)}(\lambda, f)$ up to isomorphism where $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$. Finally, we find some conditions for the existence of components with three or four vertices in Section 3.2.

CHAPTER II
CONNECTIVITY AND HAMILTONIAN CYCLES

2.1 In-degree, out-degree and strongly connectivity

Assume that $\lambda \operatorname{im} \varphi_k$ generates the quotient group $\mathbb{F}_q^\times / \operatorname{im} \varphi_k$. This can easily hold if λ is a primitive element of $\mathbb{F}_q$ or the size of $\mathbb{F}_q^\times / \operatorname{im} \varphi_k$ is a small prime. First, we study the in-degrees and out-degrees of every vertex of $\mathcal{G}^{(k)}(\lambda, f)$ where $f(t) \in \mathbb{F}_q[t]$ is a permutation polynomial. It follows that every component of the graph $\mathcal{G}^{(k)}(\lambda, f)$ is strongly connected and the graph is not bipartite. We begin with an algebraic lemma.

Lemma 2.1.1. *Assume that* $\gcd(k, q-1) = d$. *Let* $f(t)$ *be a polynomial in* $\mathbb{F}_q[t]$ *and let* $x \in \mathbb{F}_q$ *with* $f(x) \neq 0$. *Then there exists* $l \in \{0, 1, \ldots, d-1\}$ *such that* $\lambda^{-l} f(x) \in \operatorname{im} \varphi_k$. *Moreover, for* $j \in \{0, 1, \ldots, k-1\}$, *there exists* $y \in \mathbb{F}_q^\times$ *such that* $\lambda^j y^k = f(x)$ *if and only if* $j = l + md$ *for some* $m \in \{0, 1, \ldots, k/d - 1\}$. *In particular, the number of* y*'s in* $\mathbb{F}_q$ *such that*

$$(y^k - f(x))(\lambda y^k - f(x)) \ldots (\lambda^{k-1} y^k - f(x)) = 0$$

is k.

Proof. Let $j \in \{0, 1, \ldots, k-1\}$. Suppose that there exists $y \in \mathbb{F}_q^\times$ such that $\lambda^j y^k = f(x)$. Since $\lambda^{-l} f(x) \in \operatorname{im} \varphi_k$, $f(x) = \lambda^l g^k$ for some $g \in \mathbb{F}_q^\times$. Then $\lambda^j y^k = \lambda^l g^k$, so $\lambda^{j-l} = (gy^{-1})^k \in \operatorname{im} \varphi_k$. Since the order of $\lambda \operatorname{im} \varphi_k$ is $d = |\mathbb{F}_q^\times / \operatorname{im} \varphi_k|$, we have $d \mid (j - l)$.

Conversely, we suppose that $j = l + md$ for some $m \in \{0, 1, \ldots, k/d - 1\}$. Since the order of $\lambda \operatorname{im} \varphi_k$ is d, we have

$$\lambda^{-j} f(x) \operatorname{im} \varphi_k = \lambda^{-l} f(x) \operatorname{im} \varphi_k = \operatorname{im} \varphi_k.$$

Then $\lambda^{-j} f(x) \in \operatorname{im} \varphi_k$, so $\lambda^{-j} f(x) = y^k$ for some $y \in \mathbb{F}_q^\times$.

Finally, for each $j \equiv l \mod d$, the number of y's such that $\lambda^j y^k = f(x)$ is d because $|\ker \varphi_k| = d$. Since the number of j's in $\{0, 1, \ldots, k-1\}$ such that $j \equiv l \mod d$ is k/d, it follows that our desired number is k. □

Proposition 2.1.2. *Let $f(t)$ be a permutation polynomial in $\mathbb{F}_q[t]$. For the graph $\mathcal{G}^{(k)}(\lambda, f)$,*

1. *if $f(0) = 0$, then the vertex 0 has in-degree 1 and out-degree 1, and the vertex x ($x \neq 0$) has in-degree k and out-degree k, and*

2. *if $f(0) \neq 0$, then the vertex 0 has in-degree 1 and out-degree k, the vertex $f^{-1}(0)$ has in-degree k and out-degree 1, and the vertex x ($x \neq 0$ and $x \neq f^{-1}(0)$) has in-degree k and out-degree k.*

Proof. 1. Assume that $f(0) = 0$. We first count the in-degree and out-degree of the vertex 0. Let u be a successor of the vertex 0. Then,

$$\lambda^{k(k-1)/2} u^{k^2} = (u^k - f(0))(\lambda u^k - f(0)) \ldots (\lambda^{k-1} u^k - f(0)) = 0,$$

and so $u = 0$. Hence, the vertex zero has in-degree 1. Let v be a predecessor of the vertex 0. Then, $f(v) = 0 = f(0)$. Since f is a one-to-one, $v = 0$. The vertex 0 has out-degree 1. Next, we let x be a nonzero vertex in $\mathbb{F}_q$. Since f is one-to-one and $f(0) = 0$, we have $f(x) \neq 0$. By Lemma 2.1.1, there are k successors of x. Now, we let s be a predecessor associated with x. Then

$$(x^k - f(s))(\lambda x^k - f(s)) \ldots (\lambda^{k-1} x^k - f(s)) = 0.$$

Therefore, $s = f^{-1}(\lambda^j x^k)$ where $j \in \{0, 1, \ldots, k-1\}$ gives k solutions.

2. Assume that $f(0) \neq 0$. By Lemma 2.1.1, there are k successors of the vertex 0. Let v be a predecessor of the vertex 0. Then $f(v) = 0$ and so $v = f^{-1}(0) \neq 0$ because f is one-to-one. Therefore, there is only one predecessor of the vertex 0.

Now, we let c be a successor of $f^{-1}(0)$. Then, $\lambda^{k(k-1)/2}c^{k^2} = 0$, so $c = 0$. Next, we let h be a predecessor of $f^{-1}(0)$. Then,

$$((f^{-1}(0))^k - f(h))(\lambda(f^{-1}(0))^k - f(h)) \dots (\lambda^{k-1}(f^{-1}(0))^k - f(h)) = 0,$$

so $h = f^{-1}(\lambda^{-j}(f^{-1}(0))^k)$ where $j \in \{0, 1, \dots, k-1\}$. Since $f(0) \neq 0, f^{-1}(0) \neq 0$. Hence, the vertex $f^{-1}(0)$ has in-degree 1 and out-degree k.

Lastly, let x be a vertex such that $x \neq 0$ and $x \neq f^{-1}(0)$. Then $f(x) \neq 0$. By Lemma 2.1.1, there are k successors of x. Let s be a predecessor associated with x. Then

$$(x^k - f(s))(\lambda x^k - f(s)) \dots (\lambda^{k-1}x^k - f(s)) = 0.$$

Thus, $s = f^{-1}(\lambda^j x^k)$ where $j \in \{0, 1, \dots, k-1\}$. Since $x \neq 0$, the vertex s varies k solutions. □

Remark. From the above proposition, if $k \geq 3$ and $f(t) \in \mathbb{F}_q[t]$, then there is no components of $\mathcal{G}^{(3)}(\lambda, f)$ with two vertices. Mans et al. gave a condition in which $\mathcal{G}^{(2)}(\lambda, f)$ has a component with two vertices (see Proposition 4.5 of [6]).

Lemma 2.1.3. *Let $f(t)$ be a permutation polynomial in $\mathbb{F}_q[t]$. Then every vertex of $\mathcal{G}^{(k)}(\lambda, f)$ lies in a cycle, and every edge of $\mathcal{G}^{(k)}(\lambda, f)$ lies in a cycle. Moreover, every component of the graph is strongly connected.*

Proof. Let $\mathcal{C}$ be a connected component of $\mathcal{G}^{(k)}(\lambda, f)$. By Proposition 2.1.2, every vertex must be adjacent to some vertex in $\mathbb{F}_q$. Thus, we will show that, if there is an edge from x to y, then there is a path from the vertex y to the vertex x and thus we obtain our desired cycle. Proposition 2.1.2 also says that every vertex in $\mathbb{F}_q$ has positive in-degree as well as out-degree. Let G_1 be a subgraph of $\mathcal{G}^{(k)}(\lambda, f)$ that we start from x, then we draw the predecessors of x, and the predecessors of the predecessors of x, and so on. On the other hand, we let G_2 be a subgraph of $\mathcal{G}^{(k)}(\lambda, f)$ that we start from y, then we draw the successors of y, and the successors of the successors of y, and so on.

Next, we show that there is a common vertex in the subgraphs G_1 and G_2. Suppose that G_1 and G_2 have no common vertex. Then, the edge from x to y is not in G_1, and also not in G_2.

Case 1. G_2 does not contain the vertex 0. So $y \neq 0$ and $y \neq f^{-1}(0)$. By Proposition 2.1.2, in G_2, the vertex y has out-degree k and in-degree at most $k-1$. Nonetheless, any other vertex in G_2 has out-degree k and in-degree at most k. Therefore, the sum of out-degrees in G_2 is not equal to the sum of in-degrees in G_2, a contradiction.
Case 2. G_2 contains the vertex 0. If $f(0) = 0$, then $\mathcal{C}$ contains only the vertex 0 which is impossible. So $f(0) \neq 0$. If $y = 0$, then $x = f^{-1}(0)$ is not in G_2, and hence any other vertex in G_2 has in-degree at most k and out-degree k. It follows that

$$\begin{aligned} k + k(|V(G_2)| - 1) &= \text{the sum of out-degrees in the subgraph } G_2 \\ &= \text{the sum of in-degrees in the subgraph } G_2 \\ &\leq 0 + k(|V(G_2)| - 1) \end{aligned}$$

which is absurd. For the case $y = f^{-1}(0)$, we have a successor of y must be a vertex 0, $|V(G_2)| \geq 2$, and in G_2, the vertex $f^{-1}(0)$ has in-degree at most $k-1$ and out-degree 1. By Proposition 2.1.2, we obtain the sum of in-degrees in the subgraph G_2 is at most $(k-1) + 1 + k(|V(G_2)| - 2)$ and the sum of out-degrees in the subgraph G_2 equals to $1 + k(|V(G_2)| - 1)$. Since, in G_2, the sum of in-degrees is equal to the sum of out-degrees, we have

$$1 + k(|V(G_2)| - 1) \leq k + k(|V(G_2)| - 2),$$

so $1 \leq 0$ which is a contradiction. Thus, we may assume that $y \neq 0$ and $y \neq f^{-1}(0)$, so any other vertex z in the subgraph G_2 which is not 0 and $f^{-1}(0)$ has out-degree k and in-degree at most k. Hence,

$$\begin{aligned} k + k + 1 + k(|V(G_2)| - 3) &= \text{the sum of out-degrees in the subgraph } G_2 \\ &= \text{the sum of in-degrees in the subgraph } G_2 \\ &\leq (k-1) + 1 + k + k(|V(G_2)| - 3) \end{aligned}$$

which is also a contradiction, and we can conclude that G_1 and G_2 have a common vertex. □

Proposition 2.1.4. *Assume that q is odd. If $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$, then the graph $\mathcal{G}^{(k)}(\lambda, f)$ is not a bipartite graph.*

Proof. Assume that the graph $\mathcal{G}^{(k)}(\lambda, f)$ is a bipartite graph. Then the vertex set is divided into two disjoint subsets, say G_1 and G_2, where there is no adjacent edge between two vertices in the same vertex subset G_1 or G_2. Thus, there is no loops in $\mathcal{G}^{(k)}(\lambda, f)$ and so $f(0) \neq 0$. Without loss of generality, we suppose that $f^{-1}(0) \in G_1$ and $0 \in G_2$. Let $|G_1| = m$ and $|G_2| = n$. By Proposition 2.1.2, the sum of out-degrees of the vertices in G_1 equals $k(m-1)+1$, and the sum of in-degree of the vertices in G_2 is equal to $k(n-1)+1$. Since $\mathcal{G}^{(k)}(\lambda, f)$ is a bipartite graph, the sum of out-degrees of the vertices in G_1 and the sum of in-degrees of the vertices in G_1 are equal. Hence, $m = n$ and $q = m+n$ is an even integer which is a contradiction. □

2.2 Existence of Hamiltonian cycles

Next, we obtain some conditions for the existence of a Hamiltonian cycle in the graph $\mathcal{G}^{(k)}(\lambda, f)$.

Theorem 2.2.1. *If $k \mid (q-1)$ and $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$, then every component of the graph $\mathcal{G}^{(k)}(\lambda, f)$ has a Hamiltonian cycle.*

Proof. Suppose on the contrary that there exists a component $\mathcal{C}$ in $\mathcal{G}^{(k)}(\lambda, f)$ which does not have a Hamiltonian cycle. By Lemma 2.1.3, we can choose a maximal cycle, say M, in $\mathcal{C}$. So the cycle M cannot be enlarged and does not go through all vertices of $\mathcal{C}$. Also, there is a vertex in M whose successor is outside M. Let x_0 be a vertex in M such that y_0 is a successor of x_0 outside the cycle M. If $y_0 = 0$, then x_0 has out-degree at least 2 which is impossible. Thus, $y_0 \neq 0$, and so the in-degree of y_0 is k.

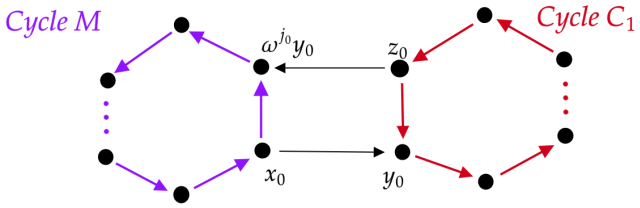
Next, we show that y_0 has a predecessor outside M. Suppose that all predecessors of y_0 are inside the cycle M. Let u_0 be a predecessor of y_0. Then

$$(y_0^k - f(u_0))(\lambda y_0^k - f(u_0)) \dots (\lambda^{k-1} y_0^k - f(u_0)) = 0.$$

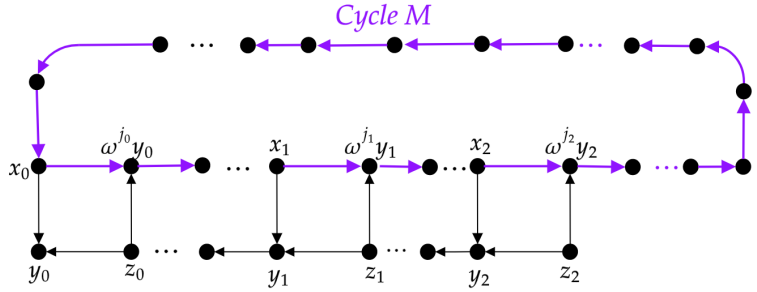
Since f is one-to-one, $u_0 = f^{-1}(\lambda^l y_0^k)$ for some $l \in \{0, 1, \dots, k-1\}$. Since $k \mid (q-1)$, there is a primitive kth root of unity ω in $\mathbb{F}_q$. Then, for each $i \in \{0, 1, \dots, k-1\}$,

$$((\omega^i y_0)^k - f(u_0))(\lambda(\omega^i y_0)^k - f(u_0)) \dots (\lambda^{k-1}(\omega^i y_0)^k - f(u_0)) = 0.$$

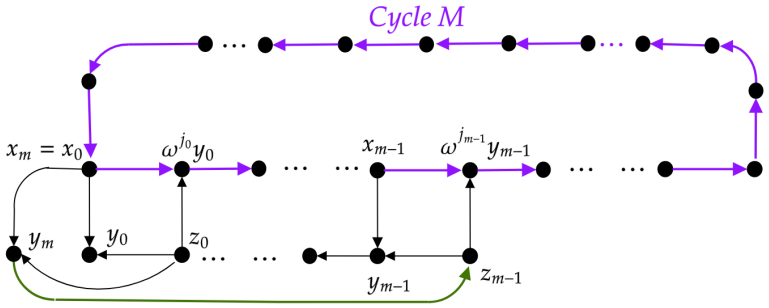
Thus, k vertices $f^{-1}(y_0^k), f^{-1}(\lambda y_0^k), \ldots, f^{-1}(\lambda^{k-1} y_0^k)$ have common successors $y_0, \omega y_0$, $\omega^2 y_0, \ldots, \omega^{k-1} y_0$ and $x_0 = f^{-1}(\lambda^l y_0^k)$ for some $l \in \{0, 1, \ldots, k-1\}$. Since the vertex y_0 is outside the cycle M, the successor of x_0 inside the cycle M is $\omega^{j_0} y_0$ for some $j_0 \in \{1, 2, \ldots, k-1\}$. Since $y_0, \omega y_0, \omega^2 y_0, \ldots, \omega^{k-1} y_0$ are common successors of $f^{-1}(y_0^k), f^{-1}(\lambda y_0^k), \ldots, f^{-1}(\lambda^{k-1} y_0^k)$, there is a predecessor of y_0 whose out-degree is at least $k+1$, a contradiction. Hence, there is a predecessor of y_0 outside the cycle M, say z_0. By Lemma 2.1.3, the edge from z_0 to y_0 lies in a cycle, say C_1. If the cycle C_1 does not intersect M, then we can enlarge the cycle M by cutting edges by edges from x_0 to $\omega^{j_0} y_0$ and from z_0 to y_0 (see the figure below), which contradicts the maximality of M, so C_1 must intersect M.



Let x_1 be a vertex in C_1 and also in M such that, along with the cycle C_1, the path from x_1 to y_0 does not intersect with M, except the vertex x_1. Similarly, we can find a successor $y_1 \neq 0$ of x_1 outside the cycle M, and there exists a predecessor of y_1 outside M, say z_1. By Lemma 2.1.3, the edge from z_1 to y_1 lies in a cycle, say C_2. As before, the cycle C_2 must intersect M, and there exist a vertex say x_2, in C_2 and also in M such that along the cycle C_2, the path from x_2 to y_1 does not intersect M except the vertex x_2. Then we draw vertices $y_2, \omega^{j_2} y_2, z_2$ and the edges among them as before. Repeating this previous process, we obtain a sequence of vertices in M, $x_0, x_1, x_2, \ldots$ in a similar manner (see the next figure).



Since M is a finite cycle, $x_n = x_m$ for some $n < m$. Without loss of generality, we assume that $n = 0$. Since $\omega^{j_m} y_m$ is a successor of x_m in the cycle M, we have $y_m = \omega^l y_0$ for some $l \in \{0, 1, \ldots, k-1\}$. Also, there is a path from y_m to z_{m-1} and there is an edge from z_0 to $y_m = \omega^l y_0$, shown in the next figure.



Thus $C : x_0, \omega^{j_0} y_0, \ldots, x_{m-1}, y_{m-1}, \ldots, z_0, y_m = \omega^l y_0, z_{m-1}, \omega^{j_{m-1}} y_{m-1}$ is a cycle in $\mathcal{C}$ extending M which contradicts the maximality of M. Therefore, every component has a Hamiltonian cycle. □

Example 2.2.2. Consider the finite field $\mathbb{Z}_3[i]$, where $i^2 = -1$ in $\mathbb{Z}_3$, $\lambda = 1 + i$ and $f(t) = t$. Indeed, $f(t)$ is a permutation polynomial over $\mathbb{Z}_3[i]$ and $\gcd(4, 9-1) = 4$. From Figure 2.1, the graph $\mathcal{G}^{(4)}(1+i, t)$ over $\mathbb{Z}_3[i]$ has two components and its Hamiltonian paths are as follows: $0 \to 0$ and $1 - i \to 1 \to -1 \to -1 - i \to 1 + i \to -i \to i \to -1 + i \to 1 - i$.

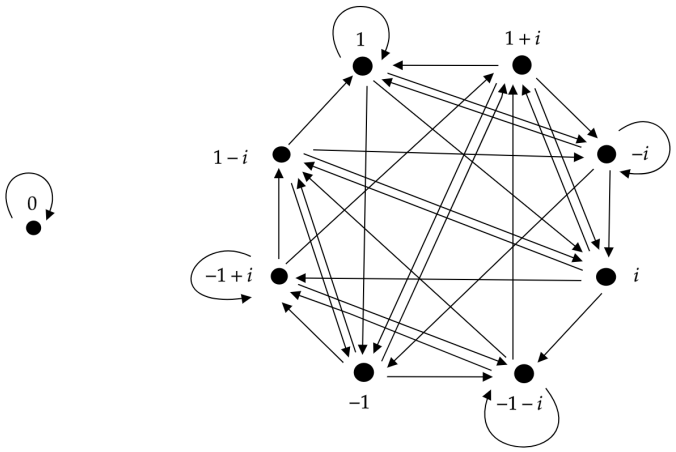


Figure 2.1: The graph $\mathcal{G}^{(4)}(1+i, t)$ over $\mathbb{Z}_3[i]$

Example 2.2.3. If $f(t) \in \mathbb{F}_q[t]$ is not a permutation polynomial, then there is a graph $\mathcal{G}^{(k)}(\lambda, f)$ whose component does not have a Hamiltonian cycle. For example, in $\mathbb{Z}_7$, $f(t) = t^3 + 1 \in \mathbb{Z}_7[t]$ is not a permutation polynomial and we consider $\lambda = 3$. From Figure 2.2, the graph $\mathcal{G}^{(3)}(3, t^3 + 1)$ has only one component and there is no predecessor of vertices $3, 5$ and 6. Hence, the Hamiltonian cycle does not exist. On the other hand, $f(t) = t^3 \in \mathbb{Z}_7[t]$ is not a permutation polynomial but every component of the graph $\mathcal{G}^{(3)}(2, t^3)$ over $\mathbb{Z}_7$ has a Hamiltonian cycle (see Figure 2.3).

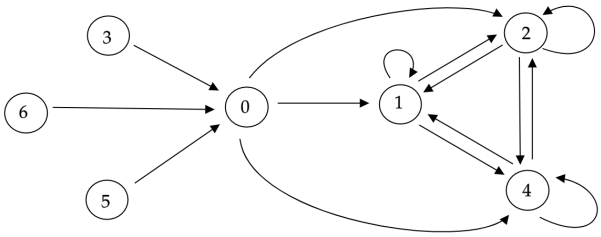


Figure 2.2: The graph $\mathcal{G}^{(3)}(3, t^3 + 1)$ over $\mathbb{Z}_7$

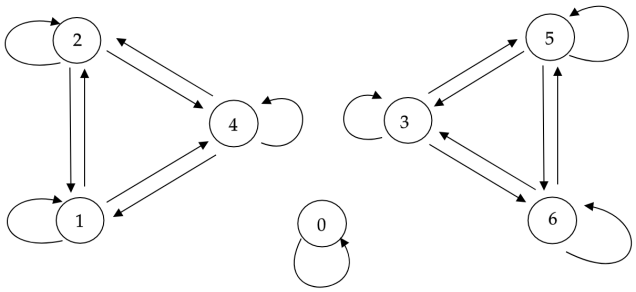


Figure 2.3: The graph $\mathcal{G}^{(3)}(3, t^3)$ over $\mathbb{Z}_7$

CHAPTER III
FURTHER RESULTS

3.1 Isomorphism Classses

Throughout this section, we assume that q is odd and fix a non-square element c in $\mathbb{F}_q$. We work on isomorphism classes of the graph $\mathcal{G}^{(3)}(\lambda, at+b)$ where $a, b \in \mathbb{F}_q$ with $a \neq 0$. We shall distinguish $a \neq 0$ in two cases, namely, square and non-square, as follows.

Proposition 3.1.1. *Let $\alpha \neq 0$ in $\mathbb{F}_q$ and $b \in \mathbb{F}_q$, the graph $\mathcal{G}^{(3)}(\lambda, \alpha^2 t + b)$ is isomorphic to the graph $\mathcal{G}^{(3)}(\lambda, t + \alpha^{-3}b)$.*

Proof. Let τ be the bijection map on $\mathbb{F}_q^\times$ defined by $\tau(x) = \alpha^{-1}x$ for all $x \in \mathbb{F}_q$. To show that τ preserves the adjacency conditions, we let u and v be in $\mathbb{F}_q$ and compute

$$\begin{aligned}
&\left(v^3 - (\alpha^2 u + b)\right)\left(\lambda v^3 - (\alpha^2 u + b)\right)\left(\lambda^2 v^3 - (\alpha^2 u + b)\right) = 0 \\
&\Leftrightarrow \alpha^{-3}\left(v^3 - (\alpha^2 u + b)\right)\alpha^{-3}\left(\lambda v^3 - (\alpha^2 u + b)\right)\alpha^{-3}\left(\lambda^2 v^3 - (\alpha^2 u + b)\right) = 0 \\
&\Leftrightarrow \left((\alpha^{-1}v)^3 - (\alpha^{-1}u + \alpha^{-3}b)\right)\left(\lambda(\alpha^{-1}v)^3 - (\alpha^{-1}u + \alpha^{-3}b)\right)\left(\lambda^2(\alpha^{-1}v)^3 - (\alpha^{-1}u + \alpha^{-3}b)\right) = 0 \\
&\Leftrightarrow \left((\tau(v))^3 - (\tau(u) + \alpha^{-3}b)\right)\left(\lambda(\tau(v))^3 - (\tau(u) + \alpha^{-3}b)\right)\left(\lambda^2(\tau(v))^3 - (\tau(u) + \alpha^{-3}b)\right) = 0.
\end{aligned}$$

Hence, τ is an isomorphism from the graph $\mathcal{G}^{(3)}(\lambda, \alpha^2 t + b)$ onto the graph $\mathcal{G}^{(3)}(\lambda, t + \alpha^{-3}b)$. □

Proposition 3.1.2. *Assume that a is a non-square element in $\mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Then ac is a square element and the graph $\mathcal{G}^{(3)}(\lambda, at + b)$ is isomorphic to the graph $\mathcal{G}^{(3)}(\lambda, c^{-1}t + \beta^{-3}b)$ where $\beta \in \mathbb{F}_q$ and $\beta^2 = ac$.*

Proof. Consider the square mapping φ_2. Since $\ker \varphi_2 = \{1, -1\}$, $|\mathbb{F}_q^\times / \operatorname{im} \varphi_2| = 2$, so $a \operatorname{im} \varphi_2 = c \operatorname{im} \varphi_2 = c^{-1} \operatorname{im} \varphi_2$. Then $ac \in \operatorname{im} \varphi_2$, so $ac = \beta^2$ for some $\beta \in \mathbb{F}_q^\times$. Let

τ be the bijection map on $\mathbb{F}_q$ defined by $\tau(x) = \beta^{-1}x$ for all $x \in \mathbb{F}_q$. To show that τ preserves the adjacency conditions, we let u and v be in $\mathbb{F}_q$. Since

$$\begin{aligned}
&\left(v^3 - (au+b)\right)\left(\lambda v^3 - (au+b)\right)\left(\lambda^2 v^3 - (au+b)\right) = 0 \\
&\Leftrightarrow \left(cv^3 - [(\beta^2 u) + cb]\right)\left(c\lambda(v)^3 - [(\beta^2 u) + bc]\right)\left(c\lambda^2(v)^3 - [(\beta^2 u) + bc]\right) = 0 \\
&\Leftrightarrow \beta^{-3}\left(cv^3 - [(\beta^2 u) + cb]\right)\beta^{-3}\left(c\lambda(v)^3 - [(\beta^2 u) + bc]\right)\beta^{-3}\left(c\lambda^2(v)^3 - [(\beta^2 u) + bc]\right) = 0 \\
&\Leftrightarrow \left(c(\beta^{-1}v)^3 - [(\beta^{-1}u) + \beta^{-3}cb]\right)\left(c\lambda(\beta^{-1}v)^3 - [(\beta^{-1}u) + \beta^{-3}bc]\right)\left(c\lambda^2(\beta^{-1})^3 - [(\beta^{-1}u) + \beta^{-3}bc]\right) = 0 \\
&\Leftrightarrow \left((\beta^{-1}v)^3 - [c^{-1}(\beta^{-1}u) + \beta^{-3}b]\right)\left(\lambda(\beta^{-1}v)^3 - [c^{-1}(\beta^{-1}u) + \beta^{-3}b]\right)\left(\lambda^2(\beta^{-1})^3 - [c^{-1}(\beta^{-1}u) + \beta^{-3}b]\right) = 0 \\
&\Leftrightarrow \left((\tau(v))^3 - [c^{-1}(\tau(u)) + b\beta^{-3}]\right)\left(\lambda(\tau(v))^3 - [c^{-1}(\tau(u)) + b\beta^{-3}]\right)\left(\lambda^2(\tau(v))^3 - [c^{-1}(\tau(u)) + b\beta^{-3}]\right) = 0,
\end{aligned}$$

τ is an isomorphism from the graph $\mathcal{G}^{(3)}(\lambda, at+b)$ onto the graph $\mathcal{G}^{(3)}(\lambda, t+\beta^{-3}b)$. □

By Propositions 3.1.1 and 3.1.2, we may focus the study on the graphs $\mathcal{G}^{(3)}(\lambda, t+b)$ and $\mathcal{G}^{(3)}(\lambda, ct+b)$ where $b \in \mathbb{F}_q$. In addition, we have

Proposition 3.1.3. *The graphs $\mathcal{G}^{(3)}(\lambda, t)$ and $\mathcal{G}^{(3)}(\lambda, ct)$ are not isomorphic.*

Proof. Consider the equation

$$(X^3 - X)(\lambda X^3 - X)(\lambda^2 X^3 - X) = 0.$$

If λ is a square element in $\mathbb{F}_q$, then there are seven solutions associated with the equation, and if λ is non-square, then there are five solutions of the equation. It follows that there are at least five fixed vertices in $\mathcal{G}^{(3)}(\lambda, t)$. Next, we consider another equation

$$(X^3 - cX)(\lambda X^3 - cX)(\lambda^2 X^3 - cX) = 0.$$

Since $X^2 = \lambda^{-2}c$ and $X^2 = c$ are insolvable, the equation has at most three solutions. Thus, there are at most three fixed vertices of the graph $\mathcal{G}^{(3)}(\lambda, ct)$. Hence, the number of fixed vertices of $\mathcal{G}^{(3)}(\lambda, t)$ and $\mathcal{G}^{(3)}(\lambda, ct)$ are different, so they are not isomorphic. □

Proposition 3.1.4. *Let $a \neq 0$ and $h \in \mathbb{F}_q$. Then the graph $\mathcal{G}^{(3)}(\lambda, at+h)$ is isomorphic to the graph $\mathcal{G}^{(3)}(\lambda, at-h)$.*

Proof. Let τ be the bijection on $\mathbb{F}_q$ defined by $\tau(x) = -x$ for all $x \in \mathbb{F}_q$. To show that τ preserves the adjacency conditions, we let u and v be in $\mathbb{F}_q$ and compute

$$\left(v^3 - (au+h)\right)\left(\lambda v^3 - (au+h)\right)\left(\lambda^2 v^3 - (au+h)\right) = 0$$

$$\Leftrightarrow \left(-v^3-(-au-h)\right)\left(-\lambda v^3-(-au-h)\right)\left(-\lambda^2 v^3-(-au-h)\right)=0$$
$$\Leftrightarrow \left((-v)^3-(a(-u)-h)\right)\left(\lambda(-v)^3-(a(-u)-h)\right)\left(\lambda^2(-v)^3-(a(-u)-h)\right)=0$$
$$\Leftrightarrow \left((\tau(v))^3-[a(\tau(u))-h]\right)\left(\lambda(\tau(v))^3-[a(\tau(u))-h]\right)\left(\lambda^2(\tau(v))^3-[a(\tau(u))-h]\right)=0.$$

Thus, we have the proposition. □

Proposition 3.1.5. *If $a_1, a_2 \in \mathbb{F}_q^\times$, then the graph $\mathcal{G}^{(3)}(\lambda, a_1 t)$ and $\mathcal{G}^{(3)}(\lambda, a_2 t+b)$ with $b \neq 0$ are not isomorphic.*

Proof. Since $b \neq 0$, $\mathcal{G}^{(3)}(\lambda, a_2 t+b)$ has no vertex with in-degree 1 and out-degree 1 by Proposition 2.1.2 (2). However, the vertex 0 in $\mathcal{G}^{(3)}(\lambda, a_1 t)$ has in-degree 1 and out-degree 1, so both graphs are not isomorphic. □

Proposition 3.1.6. *Assume that $3 \mid (q-1)$. Let $a \neq 0$ and $i, j \in \{0,1,2\}$. If λ is an element of order 3 in $\mathbb{F}_q^\times$, then the graph $\mathcal{G}^{(3)}(\lambda, at+\lambda^i)$ is isomorphic to $\mathcal{G}^{(3)}(\lambda, at+\lambda^j)$.*

Proof. Let τ be the bijection map on $\mathbb{F}_q$ defined by $\tau(x) = \lambda^{j-i}x$ for $x \in \mathbb{F}_q$. To show that τ preserves the adjacency conditions, we let u and v be in $\mathbb{F}_q$. Since

$$\left(v^3-(au+\lambda^i)\right)\left(\lambda v^3-(au+\lambda^i)\right)\left(\lambda^2 v^3-(au+\lambda^i)\right)=0$$
$$\Leftrightarrow \lambda^{j-i}\left(v^3-(au+\lambda^i)\right)\lambda^{j-i}\left(\lambda v^3-(au+\lambda^i)\right)\lambda^{j-i}\left(\lambda^2 v^3-(au+\lambda^i)\right)=0$$
$$\Leftrightarrow \left((\tau(v))^3-(a\tau(u)+\lambda^j)\right)\left(\lambda(\tau(v))^3-(a\tau(u)+\lambda^j)\right)\left(\lambda^2(\tau(v))^3-(a\tau(u)+\lambda^j)\right)=0,$$

we have the proposition. □

Proposition 3.1.7. *If $q \equiv 3 \mod 4$, then the graphs $\mathcal{G}^{(3)}(\lambda, -t+1)$ and $\mathcal{G}^{(3)}(\lambda, t+1)$ are not isomorphic.*

Proof. Suppose that both graphs are isomorphic with an isomorphism τ. By Proposition 2.1.2 (2), 0 is the only vertex in $\mathcal{G}^{(3)}(\lambda, -t+1)$ whose in-degree is 1 and out-degree is 3. Then only the vertex $\tau(0)$ in $\mathcal{G}^{(3)}(\lambda, t+1)$ has in-degree 1 and out-degree 3, so $\tau(0) = 0$. Moreover, 1 is only vertex in $\mathcal{G}^{(3)}(\lambda, -t+1)$ whose in-degree is 3 and out-degree is 1. Thus, only the vertex $\tau(1)$ in $\mathcal{G}^{(3)}(\lambda, t+1)$ has in-degree 1 and out-degree 3, so $\tau(1) = -1$. Since

$$\left(1^3-(-0+1)\right)\left(\lambda(1)^3-(-0+1)\right)\left(\lambda^2(1)^3-(-0+1)\right)=0,$$

there exists an edge from the vertex 0 to 1 in $\mathcal{G}^{(3)}(\lambda, -t+1)$. Since $q \equiv 3 \mod 4$, we know that -1 is non-square, so $\lambda^2 + 1 \neq 0$. On the other hand, we note that

$$\begin{aligned}\left((-1)^3 - (0+1)\right)\left(\lambda(-1)^3 - (0+1)\right)\left(\lambda^2(-1)^3 - (0+1)\right) \\ = (-2)(-\lambda-1)(-\lambda^2-1) \neq 0,\end{aligned}$$

there is no edges from the vertex 0 to -1 in $\mathcal{G}^{(3)}(\lambda, t+1)$. However, since τ preserves the adjacency condition, there is an edge from $\tau(0) = 0$ to $\tau(1) = -1$ in $\mathcal{G}^{(3)}(\lambda, t+1)$. Hence, we have a contradiction, so both graphs are not isomorphic. □

Example 3.1.8. In $\mathbb{Z}_7$ with $\lambda = 2$, by Propositions 3.1.1 to 3.1.5, we have at most eight isomorphism classes of the graph $\mathcal{G}^{(3)}(\lambda, at+b)$ where $a, b \in \mathbb{Z}_7$ with $a \neq 0$ as shown in the following table.

$\mathcal{G}^{(3)}(2, -t)$	$\mathcal{G}^{(3)}(2, t)$
$\mathcal{G}^{(3)}(2, -t+1)$	$\mathcal{G}^{(3)}(2, t+1)$
$\mathcal{G}^{(3)}(2, -t+2)$	$\mathcal{G}^{(3)}(2, t+2)$
$\mathcal{G}^{(3)}(2, -t+4)$	$\mathcal{G}^{(3)}(2, t+4)$

Since the order of λ is 3, by Proposition 3.1.6, the number of isomorphism classes is at most four, and it equals four by Proposition 3.1.7 as shown in the next table.

$\mathcal{G}^{(3)}(2, -t)$	$\mathcal{G}^{(3)}(2, t)$
$\mathcal{G}^{(3)}(2, -t+1)$	$\mathcal{G}^{(3)}(2, t+1)$

3.2 Components with small number of vertices

In this section, we first study the number of vertices in a component of $\mathcal{G}^{(k)}(\lambda, f)$ where $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$ and $k \mid (q-1)$. This allows us to study the components of $\mathcal{G}^{(3)}(\lambda, f)$ of small vertices. We show some conditions for the existence of a component with three or four vertices of our desired graphs.

Lemma 3.2.1. *Assume that $k \mid (q-1)$ and $f(t)$ is a permutation polynomial in $\mathbb{F}_q[t]$. Let $\mathcal{C}$ be a component in $\mathcal{G}^{(3)}(\lambda, f)$ with the number of vertices $n_{\mathcal{C}}$. Then*

1. *if 0 is not a vertex of $\mathcal{C}$, then $n_{\mathcal{C}}$ is divisible by k, and*

2. if 0 *is a vertex of* $\mathcal{C}$*, then* $n_{\mathcal{C}} - 1$ *is divisible by* k*.*

Proof. Define

$$\mathcal{E} = \{(x, y) : x, y \in V(\mathcal{C}) \text{ and } y^k = f(x)\}.$$

For $y \in V(\mathcal{C})$, we write

$$\mathcal{A}_y = \{(x, y) : x \in V(\mathcal{C}) \text{ and } y^k = f(x)\}.$$

Then

$$\mathcal{E} = \bigcup_{y \in V(\mathcal{C})} \mathcal{A}_y = \bigcup_{y \in V(\mathcal{C})} \{(f^{-1}(y^k), y)\}$$

because f is one-to-one. Hence $|\mathcal{E}| = \sum_{y \in V(\mathcal{C})} 1 = n_{\mathcal{C}}$. For $x \in V(\mathcal{C})$, we write

$$\mathcal{B}_x = \{(x, y) : y \in V(\mathcal{C}) \text{ and } y^k = f(x)\},$$

and so $\mathcal{E} = \bigsqcup_{x \in V(\mathcal{C})} \mathcal{B}_x$, a disjoint union.

1. Let $x \in V(\mathcal{C})$. Assume that $\mathcal{B}_x \neq \emptyset$. Then there exists $y \in V(\mathcal{C})$ such that $y^k = f(x)$, so $f(x) = (y\omega^j)^k$ for all $j \in \{0, 1, \ldots, k-1\}$ and ω is an element of order k in $\mathbb{F}_q^\times$. Since $x \in V(\mathcal{C}), y\omega^j \in V(\mathcal{C})$ for all $j \in \{0, 1, \ldots, k-1\}$. Thus, $|\mathcal{B}_x| = k$ because $y \neq 0$. Hence, we have shown that $|\mathcal{B}_x|$ is either 0 or k, so $n_{\mathcal{C}} = \sum_{x \in V(\mathcal{C})} |\mathcal{B}_x|$ is divisible by k.

2. If $f(0) = 0$, then $|V(\mathcal{C})| = 1$ by Proposition 2.1.2 (1). Suppose that $f(0) \neq 0$. Then $|\mathcal{B}_{f^{-1}(0)}| = 1$. Let $z \in V(\mathcal{C}) \backslash \{f^{-1}(0)\}$. Assume that $\mathcal{B}_z \neq \emptyset$. Then there exists $y \in V(\mathcal{C})$ such that $y^k = f(z)$, so $f(z) = (y\omega^j)^k$ for all $j \in \{0, 1, \ldots, k-1\}$ and ω is an element of order k in $\mathbb{F}_q^\times$. Since $z \in V(\mathcal{C}), y\omega^j \in V(\mathcal{C})$ for all $j \in \{0, 1, \ldots, k-1\}$. Thus, $|\mathcal{B}_z| = k$ because $f(z) \neq 0$. Hence, we have shown that $|\mathcal{B}_z|$ is either 0 or k, so $n_{\mathcal{C}} - 1 = \sum_{z \in V(\mathcal{C}) \backslash \{f^{-1}(0)\}} |\mathcal{B}_z|$ is divisible by k. □

Example 3.2.2. Lemma 3.2.1 may not hold if $k \nmid (q-1)$. For example, the graph $\mathcal{G}^{(3)}(2, t+2)$ over $\mathbb{Z}_5$ has a component with five vertices whereas the vertex 0 is in this component (see Figure 3.1).

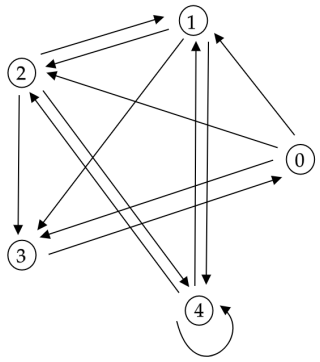
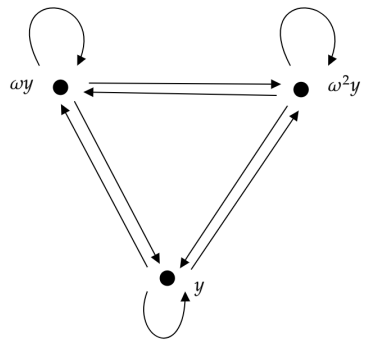


Figure 3.1: The graph $\mathcal{G}^{(3)}(2, t+2)$ over $\mathbb{Z}_5$

Proposition 3.2.3. *Assume that* $3 \mid (q-1)$. *If* $a \in \mathbb{F}_q$, *then the graph* $\mathcal{G}^{(3)}(\lambda, t+a)$ *has a component with three vertices if and only if* $a = 0$ *and the order of* λ *is* 3.

Proof. Let $\mathcal{C}$ be a component of the graph $\mathcal{G}^{(3)}(\lambda, t+a)$ with three vertices. By Lemma 3.2.1, $0 \notin V(\mathcal{C})$ and so $f^{-1}(0) \notin V(\mathcal{C})$. By Proposition 2.1.2, each vertex of $\mathcal{C}$ has in-degree 3 and out-degree 3. Since $3 \mid (q-1)$, we can let ω be a primitive 3rd root of unity in $\mathbb{F}_q^\times$. Let x be a vertex of $\mathcal{C}$ and y be a successor of x. By Lemma 2.1.1, $y^3 = \lambda^{-l}(x+a)$ for some $l \in \{0,1,2\}$, so $y, \omega y$ and $\omega^2 y$ are vertices of $\mathcal{C}$. We have only one possibility of $\mathcal{C}$ displayed below.



Also, we have three predecessors of y, namely $y^3 - a, \lambda y^3 - a$ and $\lambda^2 y^3 - a$. Hence, we obtain system of equations

$$y^3 - a = \omega^i y \tag{3.2.1}$$

$$\lambda y^3 - a = \omega^j y \tag{3.2.2}$$

$$\lambda^2 y^3 - a = \omega^k y \tag{3.2.3}$$

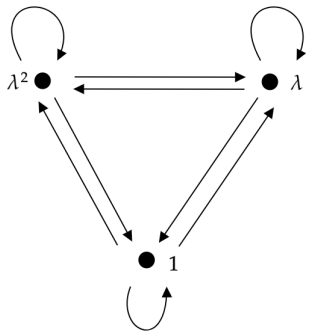
where $\{i, j, k\} = \{0, 1, 2\}$. By (3.2.1) and (3.2.2), we have

$$(\lambda - 1)y^3 = (\omega^j - \omega^i)y. \tag{3.2.4}$$

By (3.2.2) and (3.2.3), we have

$$\lambda(\lambda - 1)y^3 = (\omega^k - \omega^j)y. \tag{3.2.5}$$

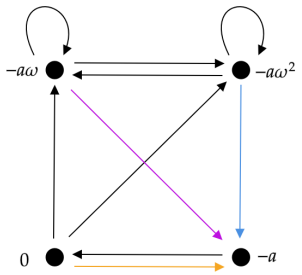
So, by (3.2.4) and (3.2.5), we obtain $\lambda = \dfrac{\omega^k - \omega^j}{\omega^j - \omega^i}$, and hence $\lambda^3 = 1$. By (3.2.1), (3.2.2) and (3.2.3), we have $a = \frac{1}{3}(1+\lambda+\lambda^2)y^3 = 0$. For the converse, the component



of $\mathcal{G}^{(3)}(\lambda, t)$ has three vertices. □

Proposition 3.2.4. *Assume that q is odd and $3 \mid (q-1)$. For each $a \in \mathbb{F}_q$, there is no component of the graph $\mathcal{G}^{(3)}(\lambda, t+a)$ with four vertices.*

Proof. Suppose on a contrary that the graph $\mathcal{G}^{(3)}(\lambda, t+a)$ has a component with four vertices, say $\mathcal{C}$. By Lemma 3.2.1, the vertex $0 \in V(C)$ and $a \neq 0$. Let y be a successor of the vertex 0. By Lemma 2.1.1, $y^3 = \lambda^{-l}a$ for some $l \in \{0, 1, 2\}$, so $y, \omega y$ and $\omega^2 y$ are vertices of $\mathcal{C}$. Since $-a$ is a nonzero predecessor of the vertex 0, we have $-a = y\omega^j$ for some $j \in \{0, 1, 2\}$ and so all successors of the vertex 0 are $-a, -a\omega$ and $-a\omega^2$ where ω is a primitive 3rd root of unity in $\mathbb{F}_q$. By Lemma 2.1.1 the vertex 0 has in-degree 1, and so the vertices $-a\omega$ as well as $-a\omega^2$ have three common successors $-a, -a\omega$ and $-a\omega^2$. We have only one possibility of $\mathcal{C}$ displayed below.



In addition, there are three predecessors of $-a$, namely $-a^3 - a, -\lambda a^3 - a$ and $-\lambda^2 a^3 - a$. Hence, we obtain

$$\lambda^i(-a)^3 = 0 + a \tag{3.2.6}$$

$$\lambda^j(-a)^3 = -a\omega + a \tag{3.2.7}$$

$$\lambda^k(-a)^3 = -a\omega^2 + a \tag{3.2.8}$$

where $\{i, j, k\} = \{0, 1, 2\}$. By the above equations, we have

$$\lambda^k - \lambda^j = (\omega - 1)(\lambda^j - \lambda^i). \tag{3.2.9}$$

We next permute i, j, k in six cases as follows.

Case 1. $i = 0, j = 1$ and $k = 2$. By (3.2.9), we have $\lambda = \omega - 1$. But, from (3.2.6) and (3.2.7), we have $\lambda = -\omega + 1$ which implies that $2 = 0$, a contradiction.

Case 2. $i = 0, j = 2$ and $k = 1$. By (3.2.9), we have $\lambda = \omega$. But, from (3.2.6) and (3.2.8), we have $\lambda = -\omega^2 + 1$ and thus $2 = 0$ which is a contradiction.

Case 3. $i = 1, j = 0$ and $k = 2$. By (3.2.9), we have $\lambda = -\omega$. But, from (3.2.6) and (3.2.7), we have $\lambda = \frac{1}{1-\omega}$ and so $2 = 0$ which is impossible.

Case 4. $i = 1, j = 2$ and $k = 0$. By (3.2.9), we have $\lambda = -\omega^2$. But, from (3.2.6) and (3.2.8), we have $\lambda = \frac{1}{1-\omega^2}$ and thus $2 = 0$ which is impossible.

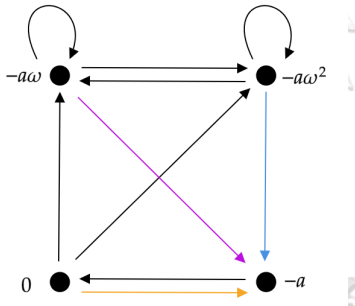
Case 5. $i = 2, j = 0$ and $k = 1$. By (3.2.9), we have $\lambda = \frac{\omega}{1-\omega}$. But from (3.2.7) and (3.2.8), we have $\lambda = \omega + 1$ and so $2 = 0$ which is absurd.

Case 6. $i = 2, j = 1$ and $k = 0$. By (3.2.9), we have $\lambda = \frac{1}{\omega-1}$. But from (3.2.7) and (3.2.8), we have $\lambda = \frac{1}{1+\omega}$ which also implies that $2 = 0$, a contradiction.

Hence, we obtain a contradiction and so there is no components with four vertices. □

Proposition 3.2.5. *Assume that q is even and $3 \mid (q-1)$. If $a \in \mathbb{F}_q$, then the graph $\mathcal{G}^{(3)}(\lambda, t+a)$ has a component with four vertices if and only if the order of λ is 3 and $a = \lambda^i$ for some $i \in \{0,1,2\}$.*

Proof. Since $\mathrm{char}\mathbb{F}_q = 2$, we have $\ker \varphi_2 = \{1\}$. Let $\mathcal{C}$ be a component of the graph $\mathcal{G}^{(3)}(\lambda, t+a)$ with four vertices. By Lemma 3.2.1, $0 \notin \mathcal{C}$ and $a \neq 0$. Let y be a successor of the vertex 0. By Lemma 2.1.1, $y^3 = \lambda^{-l}a$ for some $l \in \{0,1,2\}$, so $y, \omega y$ and $\omega^2 y$ are vertices of $\mathcal{C}$. Since $-a$ is a nonzero predecessor of the vertex 0, we have $-a = y\omega^j$ for some $j \in \{0,1,2\}$ and so all successors of the vertex 0 are $-a, -a\omega$ and $-a\omega^2$ where ω is a primitive 3rd root of unity in $\mathbb{F}_q$. By Lemma 2.1.1 the vertex 0 has in-degree 1, and so the vertices $-a\omega$ as well as $-a\omega^2$ have three common successors $-a, -a\omega$ and $-a\omega^2$. We have only one possibility of $\mathcal{C}$ displayed below.



In addition, there are three predecessors of $-a$, namely $-a^3 - a, -\lambda a^3 - a$ and $-\lambda^2 a^3 - a$. Hence, we obtain

$$\lambda^i(-a)^3 = 0 + a \tag{3.2.10}$$

$$\lambda^j(-a)^3 = -a\omega + a \tag{3.2.11}$$

$$\lambda^k(-a)^3 = -a\omega^2 + a \tag{3.2.12}$$

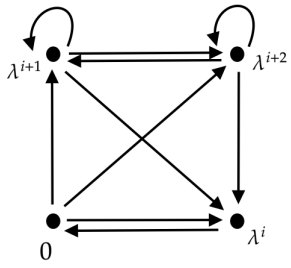
where $\{i,j,k\} = \{0,1,2\}$. By the above equations, we have

$$(1 + \lambda + \lambda^2)(-a^3) = 4a = 0$$

because $\mathrm{char}\mathbb{F}_q = 2$. So, we have $\lambda^3 = 1$. By equations (3.2.10), (3.2.11) and (3.2.12), we again have

$$\lambda^3(-a^9) = (a^3)(1-\omega)(1-\omega^2) = 3a^3 = a^3,$$

so $a^6 = 1$ and hence $a^3 = 1$ because $|\ker \varphi_2| = 1$. For the converse, the component



has four vertices. □

Example 3.2.6. Let $\mathbb{F}_4 = \{a+b\alpha : a, b \in \mathbb{Z}_2 \text{ and } \alpha^2+\alpha+1 = 0\} \cong \mathbb{Z}_2[t]/\langle t^2+t+1\rangle$. Let $f(t) = t + a$ be a linear permutation polynomial in $\mathbb{F}_4[t]$. Let $\mathcal{C}$ be a component in $\mathcal{G}^{(3)}(\lambda, f)$ not containing the vertex 0. By Lemma 3.2.1, the number of vertices in $\mathcal{C}$ is a multiple of 3. Let $\mathcal{D}$ be a component containing the vertex 0. Then the number of vertices in $\mathcal{D}$ is $3d+1$ for some $d \in \{0, 1\}$. If $d = 0$, then there is a graph containing a component with three vertices, for example, $\mathcal{G}^{(3)}(\alpha, t)$ (see Figure 3.2). If $d = 1$, then there is a graph containing a component with three vertices such as $\mathcal{G}^{(3)}(\alpha, t + \alpha)$ (see Figure 3.2). Our desired λ is provided by Proposition 3.2.5. Hence, any graph $\mathcal{G}^{(3)}(\lambda, t + a)$ is isomorphic to the graph in Figure 3.2 or Figure 3.3.

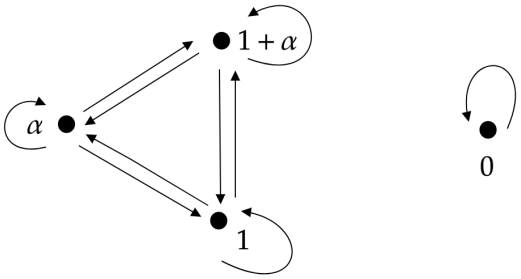


Figure 3.2: The graph $\mathcal{G}^{(3)}(\alpha, t)$ over $\mathbb{F}_4$

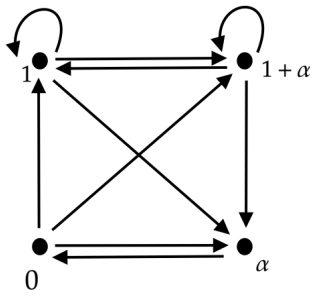


Figure 3.3: The graph $\mathcal{G}^{(3)}(\alpha, t+\alpha)$ over $\mathbb{F}_4$

Example 3.2.7. Let $f(t) = t + a$ be a permutation polynomial in $\mathbb{Z}_7[t]$. Let $\mathcal{C}$ be a component in $\mathcal{G}^{(3)}(\lambda, f)$ not containing the vertex 0. By Lemma 3.2.1, the number of vertices in $\mathcal{C}$ is a multiple of 3. Let $\mathcal{D}$ be a component containing the vertex 0. Then the number of vertices in $\mathcal{D}$ is $3d + 1$ for some $d \in \{0, 1, 2\}$. The graph $\mathcal{G}^{(3)}(\lambda, f)$ does not have a component with four vertices by Proposition 3.2.4, so d is 0 or 2. If $d = 0$, then there are two possibilities of our desired graphs. The first one is a graph containing a component with six vertices, for example $\mathcal{G}^{(3)}(3, t)$ (see Figure 3.4). Another one is a graph containing two components with three vertices such as $\mathcal{G}^{(3)}(4, t)$ (see Figure 3.5). This desired λ is given by Proposition 3.2.3 as well. If $d = 2$, then there is an equational graph $\mathcal{G}^{(3)}(\lambda, f)$ with 7 vertices, for instance $\mathcal{G}^{(3)}(3, t+1)$ (see Figure 3.6). Hence, by working on small components, we find that the graph $\mathcal{G}^{(3)}(\lambda, t + a)$ is isomorphic to the graph in Figure 3.4 or Figure 3.5 or Figure 3.6.

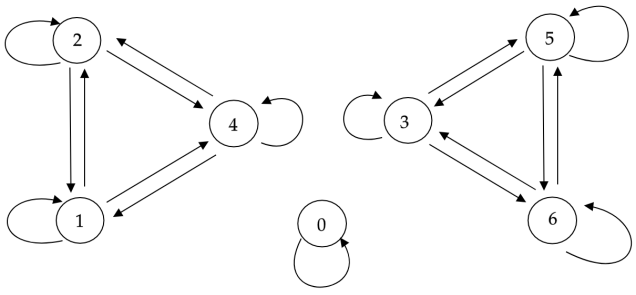


Figure 3.4: The graph $\mathcal{G}^{(3)}(4, t)$ over $\mathbb{Z}_7$

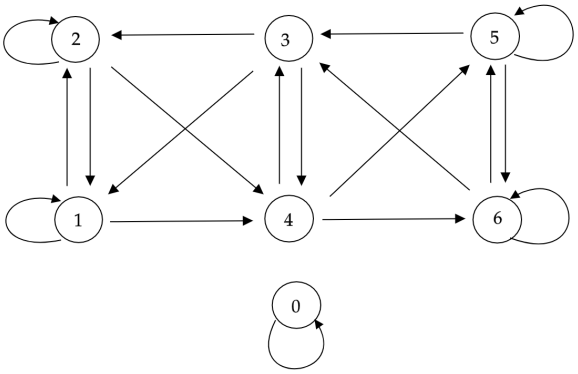


Figure 3.5: The graph $\mathcal{G}^{(3)}(3,t)$ over $\mathbb{Z}_7$

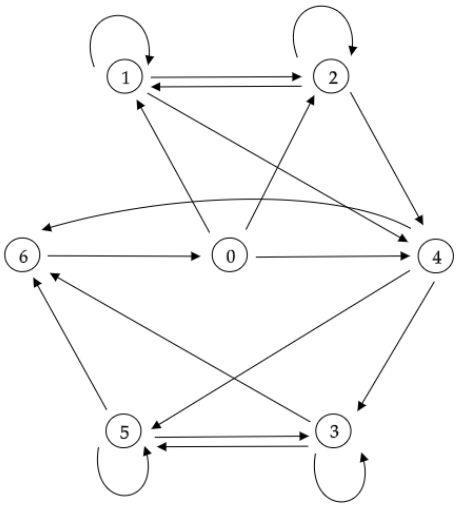


Figure 3.6: The graph $\mathcal{G}^{(3)}(3,t+1)$ over $\mathbb{Z}_7$

BIBLIOGRAPHY

[1] D. S. Dummit, R. M. Foote, *Abstract Algebra*, 2nd edn, Prentice-Hall Inc., London, 1999.

[2] C. Godsil, G. Royle, *Algebraic Graph Theory*, Springer, New York, 2001.

[3] A.G. Joseph, *Contemporary Abstract Algebra*, 10th edn, Taylor & Francis Group, LLC, 2021.

[4] S.V. Knoyagin, F. Luca, B. Mans, L. Mathieson, M. Sha, I.E. Shparlinski, Functional graphs of polynomials over finite fields, *J. Comb. Theory*, Ser. B **116** (2016), 87–122.

[5] B. Mans, M. Sha, I.E. Shparlinski, D. Sutantyo, On functional graphs of quadratic polynomials, *Exp. Math.*, **28** (2019), 292–300.

[6] B. Mans, M. Sha, J. Smith, D. Sutantyo, On the equational graphs over finite fields, *Finite Fields Appl.*, **64** (2020), 1–31.

VITA

Name	Mr. Wachirawit Chaifongsri
Date of Birth	May 30, 1998
Place of Birth	Chiang Rai, Thailand
Education	B.Sc. (Mathematics), Chulalongkorn University, 2020