Growth and its Applications in Graph Theory

Thomas Bridge
Edward Cumberlege
Harry Peaker
Joshua Prettyman

Year 4 Project
School of Mathematics
University of Edinburgh
2013

Abstract

Growth is a fundamental concept at the heart of modern mathematics. Whether it be by modelling the growth of sets governed by an underlying principle, forming recursive definitions or defining generating functions - there are numerous ways to study growth. In this report, the fundamental results and ideas that underpin the theory of growth are analysed with full rigour.

Throughout this report, we will be illustrating different patterns of growth by considering a particular problem in graph theory. Namely, whether we can explicitly determine the growth of the number of paths of any given length for a given digraph. We will focus on digraphs that contain loops, a form that we will later see arises when considering certain problems in the field of non-commutative algebra, and analyse methods for counting paths of any given length. It will be shown that the functions counting paths within digraphs of our considered form are quasipolynomial and we will analyse how the quasiperiod for functions associated to similar digraphs are related. In this report, we propose and develop a classification system for categorising the quasiperiods associated to an infinite family of graphs by considering a finite subset of its members.

We will also explore the correspondence between these graphs and binary strings, along with a fundamental link to Fibonacci Sequences. Finally, we will conclude by applying our analysis of graphs to the problems of classifying the growth of the dimension of a finitely presented monomial algebra.

Acknowledgements

We owe a debt of gratitude to Tom Lenagan for his supervision throughout this project; we greatly appreciate the guidance and thorough feedback he has provided at all stages. We also extend our thanks to those who attended our workshop, through their responses they have made a valuable contribution to our report.

Notation

$\mathbb{N}$	The set of non-negative integers, $0, 1, 2, \ldots$
$\mathbb{N}_+$	The set of positive integers, $1, 2, \ldots$
k	An arbitrary field
φ	The golden ratio, or the positive root of $f(x) = x^2 - x - 1$
$F(x)$	The generating function for a function f
Δf	Backward finite difference of f
$\Delta_N^d f$	The dth iteration of the N-step difference of f
G	Any directed graph
v_i	Vertex i in a given graph
a_{ij}	The entry in the ith row and jth column of an adjacency matrix
$a_{ij}^{(n)}$	The number of paths of length n from v_i to v_j
L_k	A minor of an adjacency matrix representing a k-loop graph
$c_k(n)$	The $k \times 1$ column vector where the nth entry is 1 and all other entries 0
$r_k(n)$	The $1 \times k$ row vector where the nth entry is 1 and all other entries 0
N	An arbitrary quasiperiod
$q(G)$	The minimal quasiperiod of the $f(n)$ associated to a graph G
$\Phi_n(x)$	The nth cyclotomic polynomial
$\mathcal{G}$	The family of all graphs of the form $[l_0, t_1, l_1, t_2, \ldots, t_d, l_d]$
$\bar{G}$	The reduction of G modulo L
$\bar{\mathcal{G}}$	The family of all $\bar{G}$
$\mathcal{P}, \mathcal{Q}$	Partitions on $\mathcal{G}$
Σ	A given alphabet
Σ^*	All words of arbitrary length formed from Σ
ε	The unique word of length 0
$k\langle x\rangle$	Free algebra over the field k
w	A word, or monomial, in $k\langle x\rangle$
Γ	An Ufnarovski graph

Contents

Chapter 1

Introduction

1.1 Why Consider Growth?

To begin, we provide motivation for the significance of considering growth in modern mathematics. Consider the algebra $k[x_1, x_2, \ldots, x_m]$ where k is a field and let V^n be the vector space of polynomials from $k[x_1, x_2, \ldots, x_m]$ up to degree n. We can explore properties of V^n, such as how the dimension grows in n as we vary m. For example, taking $m = 1$ we see

$$\begin{aligned} V^0 &= k \cdot 1 \\ V^1 &= k \cdot 1 + kx_1 \\ V^2 &= k \cdot 1 + kx_1 + kx_1^2 \\ V^3 &= k \cdot 1 + kx_1 + kx_1^2 + kx_1^3 \\ &\vdots \end{aligned}$$

At this point we wonder *how* exactly the dimension grows as we increase n. Problems like this are important in algebra and it is to allow for a rigourous analysis of this growth that we establish the material in the following chapters. We will use recurrence relations and generating functions to establish new results based on familiar theorems. We will then establish links between concepts of growth in a multitude of contexts, including graph theory, abstract algebra and combinatorics. Throughout the report we will be primarily concerned with two types of growth.

Definition 1.1. [8] We say that f has polynomial growth of degree d if there exist real numbers $a, b > 0$ such that $an^d \leq f(n) \leq bn^d$ for $n \gg 0$.

Definition 1.2. [8] We say that f has exponential growth if $f(n) \geq c^n$ for some $c > 1$ and $n \gg 0$.

The main focus of this report will be to analyse the growth of a particular family of digraphs, which will be denoted by $\mathcal{G}$. This will be achieved by evaluating the results from our experimental research using established theory.

1.2 Recurrence Relations

The growth of a sequence of sets can be analysed in many ways - one such method is by considering a recurrence relation on the sequence. For this report we restrict these sets to singletons - more simply we are concerned with sequences of numbers.

Definition 1.3. A *recurrence relation* is an equation that defines a sequence through an iterative process by relating every term $f(n)$ to a set of $m \leq n$ terms preceding it, combined with m initial conditions.

We note that clearly $n \in \mathbb{N}$ since this parameter represents the index of each term in the sequence. We consider a simple example to motivate this material.

Example 1.4. Consider the recurrence relation

$$f(n) = 2f(n-1) \text{ subject to } f(0) = 1$$

Then we use an inductive process to solve the recurrence and obtain a closed form as follows;

$$f(n) = 2f(n-1) = 2^2 f(n-2) = 2^3 f(n-3) = \ldots = 2^n f(0) = 2^n$$

Remark 1.5. It is sometimes difficult, or often even impossible, to find a closed formula for an arbitrary $f(n)$ that is defined by a recurrence relation.

We illustrate the previous remark by considering a non-trivial example of a recurrence relation.

Example 1.6. The following recurrence defines the well-known Catalan Numbers. [5]

$$f(n+1) = \sum_{i=0}^{n} f(n)f(n-i)$$

This is not a linear recurrence and it requires some more advanced techniques to solve than the previous example. It can be shown after some work, however, that $f(n)$ has the following closed form solution

$$f(n) = \frac{1}{n+1}\binom{2n}{n}$$

Definition 1.7. [11] *Lucas Sequences of the First Kind* are sequences of integers that satisfy a second order recurrence relation of the form

$$f(n) = Pf(n-1) - Qf(n-2) \qquad \text{with } P, Q \in \mathbb{Z}.$$

Example 1.8. The Fibonacci Sequence $f(n) = f(n-1) + f(n-2)$ is a particular case of the Lucas Sequences. Given initial conditions $f(0) = 0$ and $f(1) = 1$, $f(n)$ has a closed form solution called *Binet's Formula.* [2]

$$f(n) = \frac{\varphi^n - (1-\varphi)^n}{\varphi - (1-\varphi)} = \frac{\varphi^n - (1-\varphi)^n}{\sqrt{5}} \text{ where } \varphi = \frac{1+\sqrt{5}}{2} \text{ is the } \textit{Golden Ratio}.$$

We can generalise this result by solving $f(n) = f(n-1) + f(n-2)$ subject to any given initial conditions. We will return to the Fibonacci Sequence in Chapter 5.

Remark 1.9. There is a fundamental link between recurrence relations and differential equations and this notion extends to the terminology: recurrence relations can be linear, non-linear, homogeneous, separable, etc.

We see that examples 1.6 and 1.8 demonstrate that even seemingly simple recurrence relations can yield unexpectedly complicated solutions. In general however, we can solve any linear recurrence relation of the following form

$$f(n) = a_1 f(n-1) + a_2 f(n-2) + \ldots + a_d f(n-d)$$

provided $a_i \in \mathbb{R}$ for all i, which will be an important idea throughout the next chapter. We will go on to use recurrence relations to motivate theory on generating functions, which we will use to analyse the growth of f.

1.3 Generating Functions

When dealing with large amounts of information, it is often useful to find a method of expressing it in a concise form. In a mathematical context, generating functions are these neat forms that encodes various information.

Consider $(S_0, S_1, S_2, \ldots)$ an infinite sequence of subsets of a set X, indexed by $\mathbb{N}$. Before we can define a generating function fully, we first define a growth function denoted by $a(n)$.

Definition 1.10. The *growth function* assigns to each n an output $a(n) = |S_n|$, which is a non-negative integer.

Example 1.11. Consider the following sequence of subsets of $[0, \infty)$ indexed by $\mathbb{N}$.

$$\emptyset \subseteq \{2,3,5,7\} \subseteq \{2,3,5,7,11,13,17,19\} \subseteq \{2,3,5,7,11,13,17,19,23,29\} \subseteq \dots$$

In this example $a(n)$ encodes the number of prime numbers in $[0, 10n]$. Hence, $a(0) = 0$, $a(1) = 4$, $a(2) = 8$, $a(3) = 10$ and so on. We see there is no discernible pattern in these outputs. This provides some evidence that we cannot obtain a formula for the spread of prime numbers in this fashion, at least not in any readily apparent manner. Allowing such insights is what makes growth functions useful.

At this stage however, we note that $a(n)$ is an infinite sequence and not in a concise form that is easy to manipulate. This motivates the construction of generating functions.

Definition 1.12. We define the *ordinary generating function* for $a(n)$ on an infinite sequence of subsets $S_0, S_1, \dots$ contained in X, as the following formal power series in x.

$$F(x) = \sum_{n=0}^{\infty} a(n)x^n$$

We will henceforth refer to this simply as a *generating function*.

Remark 1.13. For the purpose of this report, we have restricted our definitions of growth functions and generating functions so that $a(n)$ admits only non-negative integer values. Informally this is equivalent to every $a(n)$ being the cardinality of some set, which follows reasonably from the assumption that we are 'counting' something in some sense. In full generality we can extend definitions 1.10 and 1.12 to allow $a(n) \in \mathbb{C}$ for all n, however, this report will only consider growth functions and generating functions as explicitly defined. [5]

Remark 1.14. A formal power series of x can sometimes be written in a closed form using the properties of the geometric series. This allows for easier manipulation of the information that $a(n)$ encodes.

Remark 1.15. The information is just encoded by the coefficients of the terms in the power series and x is simply an indeterminate. However, we will see in a later chapter that evaluating f at certain values can recover the coefficients.

Remark 1.16. Let $S_0, S_1, S_2, \dots, S_d$ be a finite sequence of subsets of a set X. Then this sequence can be extended to an infinite sequence with $S_i = \emptyset$ for all $i > d$ and $a(i) = 0$ for all $i > d$. Hence we can use generating functions to encode information that consists of a finite sequence of $a(n)$, but we must extend the domain of the growth function indefinitely, since the generating function is a formal power series by definition. By convention this technicality is often omitted and shall be assumed implicitly from this point in the report.

Additionally, for the purpose of simplicity, all generating functions will be denoted by a capital letter. Moving on to Chapter 2, we will consider the fundamental link between recurrence relations and generating functions.

Chapter 2

Theory of Generating Functions

In this chapter we will show that the generating function for a given recurrence relation is a rational function if and only if the recurrence relation is linear. Before we state the main theorem, we will first introduce some results concerning combinatorics and difference operators that will be useful during our analysis.

2.1 Preliminaries

Throughout this section we will be repeatedly using the binomial formula

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \qquad \text{for all integers } n, k > 0,$$

with initial conditions

$$\binom{n}{0} = 1, \quad \text{for all } n \geq 0, \qquad \binom{0}{k} = 0, \quad \text{for all } k > 0.$$

Proposition 2.1. *We can express* $\binom{n}{k}$ *as a linear combination of* $\binom{n-s}{t}$ *for a fixed* $s \leq n$ *and* $0 \leq t \leq n-s$*, for all integers* $n, k > 0$*. More precisely*

$$\binom{n}{k} = \sum_{i=0}^{s} \binom{s}{i} \binom{n-s}{k-i}$$

Proof. Let $P(s)$ be the proposition as above for $s \in \mathbb{N}$.

We see that the base case $P(0)$ is verified as follows.

$$\sum_{i=0}^{0} \binom{0}{i} \binom{n-0}{k-i} = \binom{n}{k} \text{ as required.}$$

Now let us assume that $P(r)$ is true for some $r \in \mathbb{N}$. Using this inductive hypothesis we will verify that $P(r+1)$ is true by twice employing the binomial identity with the given initial conditions.

$$\begin{aligned}
\binom{n}{k} &= \sum_{i=0}^{r} \binom{r}{i}\binom{n-r}{k-i} \\
&= \sum_{i=0}^{r} \binom{r}{i}\left[\binom{n-(r+1)}{k-i} + \binom{n-(r+1)}{k-1-i}\right] \\
&= \binom{r}{0}\binom{n-(r+1)}{k} + \sum_{i=1}^{r}\left[\binom{r}{i-1} + \binom{r}{i}\right]\binom{n-(r+1)}{k-i} + \binom{r}{r}\binom{n-(r+1)}{k-(r+1)} \\
&= \binom{r}{0}\binom{n-(r+1)}{k} + \sum_{i=1}^{r}\binom{r+1}{i}\binom{n-(r+1)}{k-i} + \binom{r}{r}\binom{n-(r+1)}{k-(r+1)} \\
&= \sum_{i=0}^{r+1}\binom{r+1}{i}\binom{n-(r+1)}{k-i}
\end{aligned}$$

Hence we see $P(r+1)$ is true and so by the principle of mathematical induction $P(s)$ is true for all $s \in \mathbb{N}$. □

Definition 2.2. Let $f : \mathbb{N} \to \mathbb{C}$ be a given function. Then for any $N \in \mathbb{N}$, we define a new function Δf_N, the *N-step difference of f*, as $\Delta_N f(n) = f(n) - f(n-N)$.

Remark 2.3. In the $N = 1$ case, we simply write Δf.

Definition 2.4. Let $\Delta_N^d f$ denote the d^{th} *iteration of the N-step difference*, which is defined as $\Delta_N^d f = \Delta_N(\Delta_N^{d-1} f)$.

Remark 2.5. The 0^{th} iteration of the N-step difference $\Delta_N^0 f$ is simply $f(n)$.

We can formulate the following recursion in d for the d^{th} iteration of the N-step difference $\Delta_N^d f(n) = \Delta_N^{d-1} f(n) - \Delta_N^{d-1} f(n-N)$ with initial conditions $\Delta_N^0 f(n) = f(n)$ and $\Delta_N^1 f(n) = f(n) - f(n-N)$. From repeated back substitution it follows that

$$\begin{aligned}
\Delta_N^d f(n) &= \Delta_N^{d-1} f(n) - \Delta_N^{d-1} f(n-N) \\
\Delta_N^d f(n) &= \Delta_N^{d-2} f(n) - 2\Delta_N^{d-2} f(n-N) + \Delta_N^{d-2} f(n-2N) \\
\Delta_N^d f(n) &= \Delta_N^{d-3} f(n) - 3\Delta_N^{d-3} f(n-N) + 3\Delta_N^{d-3} f(n-2N) - \Delta_N^{d-3} f(n-3N) \\
&\vdots
\end{aligned}$$

By this inductive reasoning we establish the following result, which shall be proven as a theorem.

Theorem 2.6 (Shifted Iterative Difference). *The d^{th} iteration of the N-step difference $\Delta_N^d f$ can be expressed as a sum of r^{th} iterations $\Delta_N^r f$ for any $0 \leq r \leq d$ in the following way*

$$\Delta_N^d f(n) = \sum_{i=0}^{d-r} \binom{d-r}{i} (-1)^i \Delta_N^r f(n - iN)$$

Proof. Let $P(r)$ be the proposition as above for a fixed $d \in \mathbb{N}$ and $0 \leq r < d$. Recalling that $\binom{0}{0} = 1$, we verify the base case $P(d)$ as follows.

$$\Delta_N^d f(n) = \sum_{i=0}^{0} \binom{0}{i} (-1)^i \Delta_N^d f(n - iN)$$

Now assume that $P(m)$ is true for some $1 \leq m \leq d$ to establish an inductive hypothesis. Recalling the result that $\Delta_N^m f(n) = \Delta_N^{m-1} f(n) - \Delta_N^{m-1} f(n)$ we rewrite the hypothesis as follows.

$$\begin{aligned}
\Delta_N^d f(n) &= \sum_{i=0}^{d-m} \binom{d-m}{i} (-1)^i \Delta_N^m f(n - iN) \\
&= \sum_{i=0}^{d-m} \binom{d-m}{i} (-1)^i \left[\Delta_N^{m-1} f(n - iN) - \Delta_N^{m-1} f(n - (i+1)N)\right]
\end{aligned}$$

Let us denote the first and last summand as A and B respectively, then

$$A = \binom{d-m}{0} (-1)^0 \Delta_N^{m-1} f(n), \quad B = \binom{d-m}{d-m} (-1)^{d-m} \Delta_N^{m-1} f(n - (d - (m-1))N)$$

Expanding out the sum, separating the first and last term, then grouping consecutive terms together yields the following result for $\Delta_N^d f(n)$.

$$\begin{aligned}
\Delta_N^d f(n) &= A + \sum_{i=1}^{d-m} \left[\binom{d-m}{i} + \binom{d-m}{i-1}\right] (-1)^i \Delta_N^{m-1} f(n - iN) + B \\
&= A + \sum_{i=1}^{d-m} \binom{d-(m-1)}{i} (-1)^i \Delta_N^{m-1} f(n - iN) + B \\
&= \sum_{i=0}^{d-(m-1)} \binom{d-(m-1)}{i} (-1)^i \Delta_N^{m-1} f(n - iN)
\end{aligned}$$

This is precisely the proposition $P(m-1)$ as required. We have seen that $P(d)$ is true and shown that if $P(m)$ is true, then so is $P(m-1)$. Therefore by the principle of backward induction, $P(r)$ is true for all $0 \leq m \leq d$. $\square$

Corollary 2.7. *For all $d \geq 1$, we can express the N-step difference in terms of $f(n)$ in the following way.*

$$\Delta_N^d f(n) = \sum_{i=0}^{d} \binom{d}{i} (-1)^i f(n - iN)$$

Proof. Recall that $\Delta_N^0 f(n) = f(n)$ for any $n, N \in \mathbb{N}$. Now using Theorem 2.6 with $r = 0$, we get the required result.

$$\Delta_N^d f(n) = \sum_{i=0}^{d} \binom{d}{i} (-1)^i \Delta_N^0 f(n - iN) = \sum_{i=0}^{d} \binom{d}{i} (-1)^i f(n - iN)$$

$\square$

Theorem 2.6 and the resulting corollary are very useful results. They allow full manipulation of $\Delta_N^d f$, which makes computation of finite differences easier and we will go on to apply them in our analysis in the following chapters.

2.2 Rational Generating Functions

In this section we will show that the generating function for a given recurrence relation is a rational function if and only if the recurrence relation is linear. This will be useful for us in the following sections, where we will analyse the growth rate of the number of paths of length n for directed graphs.

Theorem 2.8 (Stanley [12]). *Let $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$ be a fixed sequence of complex numbers, $d \geq 1$ a fixed natural number and $\alpha_d \neq 0$. The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ are equivalent:*

1. *For all $n \geq 0$,*

$$f(n + d) + \alpha_1 f(n + d - 1) + \alpha_2 f(n + d - 2) + \cdots + \alpha_d f(n) = 0.$$

2. *For $P, Q \in \mathbb{C}(x)$,*

$$\sum_{n=0}^{\infty} f(n) x^n = \frac{P(x)}{Q(x)}$$

   where $Q(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_d x^d$ and $\deg(P) < d$.

Proof. Suppose

$$\sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}$$

Then

$$\begin{aligned} P(x) &= Q(x)\sum_{n=0}^{\infty} f(n)x^n \\ &= (1+\alpha_1+\alpha_2x^2+\cdots+\alpha_dx^d)\sum_{n=0}^{\infty} f(n)x^n \\ &= \sum_{n=0}^{\infty} f(n)x^n + \alpha_1\sum_{n=0}^{\infty} f(n)x^{n+1}+\cdots+\alpha_d\sum_{n=0}^{\infty} f(n)x^{n+d} \end{aligned}$$

Since $\deg(P) < d$, we can compare coefficients of x^{n+d} to get

$$f(n+d)+\alpha_1f(n+d-1)+\alpha_2f(n+d-2)+\cdots+\alpha_df(n)=0$$

Hence (1.) $\Rightarrow$ (2.).

Since $\deg(P) < d$, then P is of the form $P(x) = c_0+c_1x+\cdots+c_{d-1}x^{d-1}$ where $c_0,\ldots,c_{d-1} \in \mathbb{C}$. Now define the vector space V as

$$V = \{f : \mathbb{N} \to \mathbb{C} | \sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}, Q(x) \text{ is fixed}\}$$

and define the set B as

$$B = \{b_k(x) = \frac{c_kx^k}{Q(x)} : k = 0,\ldots,d-1\}$$

We want to show that B is a basis for V. Let $g(x) \in V$, then $g(x)$ is of the form

$$g(x) = \frac{a_0+a_1x+\cdots+a_{d-1}x^{d-1}}{Q(x)}$$

By writing $a_i = \frac{a_i}{c_i}c_i$ for all i, we get

$$g(x) = \frac{\frac{a_0}{c_0}c_0+\frac{a_1}{c_1}c_1x+\cdots+\frac{a_{d-1}}{c_{d-1}}c_{d-1}x^{d-1}}{Q(x)} = \sum_{i=0}^{d-1}\lambda_ib_i(x)$$

Therefore we can express an arbitrary element $g(x)$ of V as linear combination of b_i's.

Hence B, a set consisting of d distinct elements, spans the d-dimensional vector space V. It follows from the Dimension Theorem [1] that the b_i must be linearly independent, otherwise $|B| < \dim(V)$, giving a contradiction. Hence $|B| = d$ and B is a basis for V. Similarly, consider the vector space W where

$$W = \{f : \mathbb{N} \to \mathbb{C} | f(n+d) + \alpha_1 f(n+d-1) + \cdots + \alpha_d f(n) = 0\}$$

Any choice of complex numbers for $f(0), f(1), \ldots, f(d-1)$ specifies a unique $f(d)$, from which we can establish an inductive argument. Hence, $\dim W = d$.

Since we have already shown that $V \subseteq W$ and $\dim V = \dim W$, we deduce that $V = W$. So we have proved (2.) $\Rightarrow$ (1.) and hence (1.) $\Leftrightarrow$ (2.). $\square$

Remark 2.9. Whilst Theorem 2.8 establishes a fundamental result, we note that it applies only to rational functions for which the denominator is of higher degree than the numerator. It may be of interest to consider cases where this condition does not hold. For these cases we proceed as follows. Suppose that

$$\sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}, \qquad \deg(P) > \deg(Q) \tag{2.1}$$

Then there exists unique polynomials $L, R \in \mathbb{C}[x]$ such that

$$\frac{P(x)}{Q(x)} = L(x) + \frac{R(x)}{Q(x)}, \qquad \deg(R) < \deg(Q)$$

Moreover, let $m = \deg(L) = \deg(P) - \deg(Q)$ and define

$$\sum_{n=0}^{\infty} g(n)x^n = \frac{R(x)}{Q(x)}$$

Then, by comparing coefficients, it follows that $g(n) = f(n)$ for $n > m$. Hence, we can apply Theorem 2.8 to a rational function of the form shown in (2.1) above, but we must be careful to note that the equations derived from the theorem only necessarily hold for $n > m$.

2.3 Dimension of a Vector Space

Throughout this project, we are interested in analysing the growth of functions. So far, we have introduced recurrence relations and generating functions as a way of analysing this growth and Theorem 2.8 has linked the two together. We will now apply the theory to an example.

Lemma 2.10. *Consider an algebra of polynomials $k[x_1, \ldots, x_m]$, where k is a field and V^n is a vector space of the polynomials from $k[x_1, \ldots, x_m]$ up to degree n. Then the dimension of V^n is given by*

$$f(n) = \binom{m+n}{m}$$

Proof. Let B be a basis for V^n generated by $1, x_1, \ldots, x_m$ and let Λ be the set of all m-tuples $(\lambda_1, \ldots, \lambda_m)$ such that $0 \leq \lambda_i \leq m+n$ and the λ_i are all distinct. Now define $g : \Lambda \to B$ by

$$g((\lambda_1, \ldots, \lambda_m)) = 1^{\lambda_1 - 1} x_1^{\lambda_2 - \lambda_1 - 1} x_2^{\lambda_3 - \lambda_2 - 1} \ldots x_{m-1}^{\lambda_m - \lambda_{m-1} - 1} x_m^{m+n-\lambda_m}$$

Note that the indices sum to n. This map is surjective because given any element $b \in B$, we can write b in the following form.

$$b = 1^{i_0} x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$$

We can calculate λ_i using forward induction, by first calculating $\lambda_1 = i_0 + 1$, then λ_2 and so on.

Since all the $\lambda_i \in (\lambda_1, \ldots, \lambda_m)$ are distinct, the map must be injective and hence g is bijective. This means that the number of elements in B equals that of Λ. Since the λ_i's are distinct,

$$|\Lambda| = \binom{m+n}{m} = |B|$$

□

As noted by Stanley [12], there are several natural choices of a basis for the vector space of polynomials $f : \mathbb{N} \to \mathbb{C}$ with degree at most m, over $\mathbb{C}$. We now introduce three of these bases and illustrate their usage by applying them to f calculated in Lemma 2.10.

1. n^i, $0 \leq i \leq m$. This is the normal basis for a polynomial.

$$f(n) = \frac{1}{m!}(n+m)(n+(m-1)) \ldots (n+1)$$

2. $\binom{n+m-i}{m}$, $0 \leq i \leq m$. This basis is particularly useful for our example, and as proved in Lemma 2.10,

$$f(n) = \binom{n+m}{m}$$

3. $\binom{n}{i}$, $0 \leq i \leq m$. By recalling $\binom{n}{m} = 0$ for $m > n$, we see that this basis is well defined. By applying Proposition 2.1 to $f(n)$ under basis (2.) it follows that

$$f(n) = \binom{m}{0}\binom{n}{m} + \binom{m}{1}\binom{n}{m-1} + \cdots + \binom{m}{m}\binom{n}{0}$$

Example 2.11. Under basis (2.) we can easily deduce a closed formula for Δf.

$$\Delta f(n) = f(n) - f(n-1) = \binom{n+m}{m} - \binom{n+m-1}{m} = \binom{n+m-1}{m-1}$$

Proposition 2.12. *Consider an algebra of polynomials $k[x_1, \ldots, x_m]$, where k is a field and V^n is the vector space of polynomials from $k[x_1, \ldots, x_m]$ up to degree n. Then the recurrence relation for the dimension of V^n, denoted by $f(n)$, has the form*

$$\sum_{k=0}^{m+1} \binom{m+1}{k} (-1)^{m+1-k} f(n+k) = 0$$

Furthermore, the generating function for the dimension of V^n is given by

$$\sum_{n=0}^{\infty} f(n) x^n = \sum_{n=0}^{\infty} \binom{m+n}{m} x^n = \frac{1}{(1-x)^{m+1}}$$

Proof. From Lemma 2.10 above, we have $f(n) = \binom{m+n}{m}$ and, as we saw in Example 2.11, it follows that

$$\Delta f(n) = f(n) - f(n-1) = \binom{n+m}{m} - \binom{n+m-1}{m} = \binom{n+m-1}{m-1}$$

Therefore, continuing by induction, we have

$$\Delta^m f(n) = \binom{n+m-m}{m-m} = \binom{n}{0} = 1$$

This means that

$$\Delta^{m+1} f(n) = \Delta^m f(n) - \Delta^m f(n-1) = 0 \tag{2.2}$$

Furthermore, from Corollary 2.7 applied at $N = 1$, we also have

$$\Delta^m f(n) = \sum_{k=0}^{m} \binom{m}{k} (-1)^k f(n-k) \tag{2.3}$$

So by combining equations (2.2) and (2.3), we deduce a recurrence relation

$$\sum_{k=0}^{m+1} \binom{m+1}{k} (-1)^k f(n-k) = 0 \tag{2.4}$$

By taking the coefficients from (2.4), as described in Theorem 2.8, we get

$$Q(x) = \sum_{k=0}^{m+1} \binom{m+1}{k} (-x)^k = (1-x)^{m+1}$$

Furthermore, we calculate $P(x)$ as

$$P(x) = F(x)Q(x) = \left(\sum_{n=0}^{\infty} \binom{m+n}{m} x^n \right) \left(\sum_{i=0}^{m+1} \binom{m+1}{i} (-x)^i \right) = 1$$

Therefore, by Theorem 2.8 we have

$$\sum_{n=0}^{\infty} f(n)x^n = \sum_{n=0}^{\infty} \binom{m+n}{m} x^n = \frac{1}{(1-x)^{m+1}}$$

$\square$

Remark 2.13. Although Proposition 2.12 follows straight away from known results about the binomial coefficient, the proof above is a nice illustration of how we can apply Theorem 2.8 to calculate generating functions.

Example 2.14. Consider vector spaces V^n of polynomials from $k[x_1, x_2]$ up to degree n. Then we have

$$\begin{aligned}
V^0 &= k.1 \\
V^1 &= k.1 + kx_1 + kx_2 \\
V^2 &= k.1 + kx_1 + kx_2 + kx_1^2 + kx_2^2 + kx_1x_2 \\
V^3 &= k.1 + kx_1 + kx_2 + kx_1^2 + kx_2^2 + kx_1^3 + kx_1^3 + kx_1x_2 + kx_1^2x_2 + kx_1x_2^2
\end{aligned}$$

Then, by Proposition 2.12, $f(n)$ is defined by the recurrence relation

$$f(n+3) - 3f(n+2) + 3f(n+1) - f(n) = 0$$

with initial conditions $f(0) = 1$, $f(1) = 3$ and $f(2) = 6$.

Furthermore, its generating function is given by

$$\sum_{n=0}^{\infty} f(n)x^n = \frac{1}{(1-x)^3}$$

Example 2.15. From the well known generating function for the constant sequence

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

and from Proposition 2.12, we can inductively find generating functions for $f(n) = n^d$, $d \in \mathbb{N}$ as follows. First of all note that

$$\begin{aligned}\binom{n+d}{d} &= \frac{1}{d!}(n+d)(n+(d-1))\cdots(n+1)\\ d!\binom{n+d}{d} &= n^d + \alpha_1 n^{d-1} + \cdots + \alpha_d \quad \text{for some } \alpha_i \in \mathbb{Z}.\end{aligned}$$

Therefore

$$n^d = d!\binom{n+d}{d} - \alpha_1 n^{d-1} - \cdots - \alpha_d$$

and so

$$\sum_{n=0}^{\infty} n^d x^n = d!\frac{P_b(x)}{Q_b(x)} - \alpha_1\frac{P_{d-1}(x)}{Q_{d-1}(x)} - \cdots - \alpha_d\frac{P_0(x)}{Q_0(x)} = \frac{P_d(x)}{Q_d(x)}$$

where $\frac{P_b(x)}{Q_b(x)}$ is the generating function for $\binom{n+d}{d}$ and $\frac{P_i(x)}{Q_i(x)}$ is the generating function for n^i, for each $i = 1, 2, \ldots, d$. From Proposition 2.12, we calculated $\frac{P_b(x)}{Q_b(x)}$ for any d and furthermore

$$\sum_{n=0}^{\infty} n^0 x^n = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x} = \frac{P_0(x)}{Q_0(x)}$$

We now have a base case and can proceed inductively to find the generating function for any n^d. Also, by construction, we have that $Q_d(x) = (1-x)^{d+1}$. Proceeding as detailed, the first few $P_d(x)$ are found to be

$$P_0(x) = 1\ ,\ P_1(x) = x\ ,\ P_2(x) = x(x+1)\ ,\ P_3(x) = x(x^2+4x+1)$$

Remark 2.16. Once generating functions for $n^0, n^1, \cdots, n^d$ are known, one can construct a generating function for any polynomial in n of degree less than or equal to d. Furthermore, by construction, we know that the generating function will have $Q(x) = (1-x)^{\sigma+1}$, where σ is the degree of the polynomial.

Remark 2.17. In the previous sections we have introduced the notion of generating functions and considered several applications for them. In these examples we often obtained a function of the form

$$G(x) = \sum_{n=0}^{\infty} a(n)x^n = \frac{P(x)}{Q(x)}$$

where $a(n)$ is the given growth function and $P(x), Q(x) \in \mathbb{C}[x]$. Often we may want to recover the coefficients, and there are several methods to do this, for example basic calculus gives us the following lemma.

Lemma 2.18 (Maclaurin Evaluation). *Let $G(x)$ be the generating function for the sequence $g(n)$. Then we have*

$$g(n) = \frac{1}{n!}G^{(n)}(0) \text{ for all non-negative integers } n.$$

Maclaurin Evaluation is useful for extracting coefficients from the closed form of a generating function. However, calculating multiple derivatives of a rational function becomes computationally intensive, so this method has its limitations.

Chapter 3

Digraph Properties

In this chapter we will consider digraphs of a certain form and the generating function $F(x) = \sum_{n=0}^{\infty} f(n)x^n$ where $f(n)$ is the number of paths of length n in the considered digraph. We aim to find a general formula to determine $F(x)$ for a given digraph.

First, we look at some examples and define some notation.

Definition 3.1. Throughout this chapter, we will denote vertex i in a given digraph by v_i.

3.1 Recurrence Relations

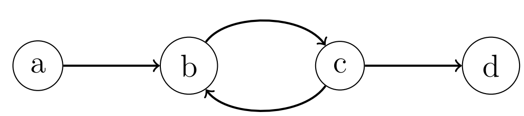


Figure 3.1: Simple 2-loop graph

Example 3.2. Consider the digraph in Figure 3.1, we can define a recurrence relation for each v_i where $f_i(n)$ is the number of paths of length n starting from that vertex. If a vertex is connected to another by a directed edge, then the number of paths of length n from the first vertex will depend on the number of paths of length $(n-1)$ starting from the second vertex; for example, in the above graph $f_a(n) = f_b(n-1)$ for $n \geq 1$. Therefore, for $n \geq 1$

we can write the relation for each vertex in the above graph as follows

$$
\begin{aligned}
f_a(n) &= f_b(n-1) \\
f_b(n) &= f_c(n-1) \\
f_c(n) &= f_b(n-1) + f_d(n-1) \\
f_d(n) &= 0
\end{aligned}
$$

with initial conditions $f_i(0) = 1$ for $i \in \{a, b, c, d\}$. Note that f_a and f_c depend only on f_b and f_d. Hence

$$
\begin{aligned}
f(n) &= f_a(n) + f_b(n) + f_c(n) + f_d(n) \\
&= f_b(n-1) + f_b(n) + [f_b(n-1) + f_d(n-1)] + 0 \\
&= f_b(n) + 2f_b(n-1) + f_d(n-1)
\end{aligned}
$$

Now $f_b(n+2) = f_c(n+1) = f_b(n) + f_d(n) = f_b(n)$ and also $f_b(n+1) = f_c(n) = f_b(n-1) + f_d(n-1)$. This gives us the following relation for f.

$$
\begin{aligned}
f(n+2) &= f_b(n+2) + 2f_b(n+1) + f_d(n+1) \\
&= f_b(n) + 2[f_b(n-1) + f_d(n-1)] \\
&= f(n) + f_d(n-1)
\end{aligned}
$$

Hence

$$f(n+2) = f(n) \quad \text{for } n \geq 2. \tag{3.1}$$

Remark 3.3. We can generalise this for loops including k vertices, such as in Figure 3.2, for which we get the following recurrence relation

$$
\begin{aligned}
f_s(n) &= f_1(n-1) \\
f_i(n) &= f_{i+1}(n-1) \text{ for } i = 1, 2, ..., k-1 \\
f_k(n) &= f_1(n-1) + f_t(n-1) \\
f_t(n) &= 0
\end{aligned}
$$

with initial conditions $f_s(0) = f_i(0) = f_t(0) = 1$ for $i = 1, 2, \ldots, k$.

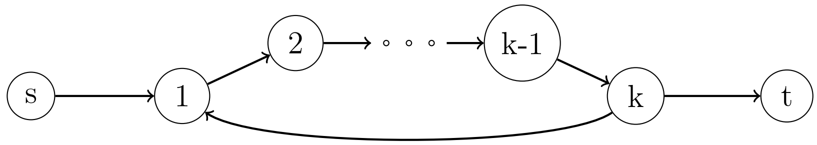


Figure 3.2: k-loop

3.2 Adjacency Matrices

We will now consider the adjacency matrix A of a graph G where the entries a_{ij} are the number of edges from v_i to v_j. For the purpose of indexing, we will number the vertices in ascending order from left to right and clockwise around the loops.

Example 3.4. For the digraph in Figure 3.1 we obtain the adjacency matrix

$$A = \left[\begin{array}{c|cc|c} 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \end{array}\right] \tag{3.2}$$

Definition 3.5. We define the function $\Sigma : \mathrm{Mat}_m(\mathbb{N}) \to \mathbb{N}$, by

$$\Sigma(A) := \sum_{0 \le i,j \le m} a_{ij}$$

Lemma 3.6. *Let G be a directed graph with m vertices and adjacency matrix A. Let $a_{ij}^{(n)}$ denote the ij^{th} element of A^n. Then the number of paths of length n from v_i to v_j is $a_{ij}^{(n)}$.*

Proof. We will prove the statement using induction. Let $P(n)$ be the proposition that $a_{ij}^{(n)}$ is the number paths of length n from v_i to v_j. By definition we have that $a_{ij}^{(1)}$ is the number paths of length 1. Hence $P(1)$ is true. Now assume that $P(k)$ is true. By matrix multiplication we have the following

$$a_{ij}^{(k+1)} = \sum_{l=1}^{m} a_{il}^{(k)} a_{lj}$$

Observe that $a_{il}^{(k)} a_{lj}$ is the number of paths from v_i to v_j that visit v_l exactly one step before v_j. Therefore, summing over all l gives the total number of paths from v_i to v_j of length $k+1$. Since $P(1)$ is true and $P(k) \Rightarrow P(k+1)$ we have that $P(n)$ is true for all $n \ge 1$. $\square$

From Lemma 3.6 above, we can immediately deduce the following corollary.

Corollary 3.7. *The number of paths of length n in G is equal to the sum of the elements of A^n. More formally, $f(n) = \sum(A^n)$.*

We would like to generalise our findings for any graph. First, we concentrate on graphs constructed by connecting smaller graphs with edges. The graph in Figure 3.1 can be considered as the combination of a single vertex, a 2-loop and another single vertex (as in Figure 3.3). This idea is evident from the upper block-triangular form of the adjacency matrix in equation (3.2), where each diagonal block corresponds to the adjacency matrix of a single element of the graph.

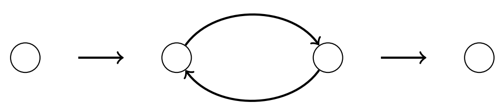


Figure 3.3: Construction of a graph

Definition 3.8. Before we look at any more examples, let us first define some notation:

- Let L_k denote the adjacency matrix of a k-loop cycle graph. The 1-loop is simply a vertex connected to itself and so $L_1 = [1]$, a 1×1 matrix. In general the $k \times k$ matrix L_k

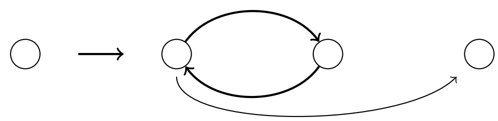
$$L_k = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix}$$

- Let $c_k(n)$ denote the $k \times 1$ column where the n^{th} entry is equal to 1.

- Let $r_k(n)$ denote the $1 \times k$ row where the n^{th} entry is equal to 1.

We consider the arguments of $r_k(\cdot)$ and $c_k(\cdot)$ modulo k, for example $r_3(5) = r_3(2) = (0, 1, 0)$ and $c_3(-2) = c_3(1) = (1, 0, 0)^T$.

If we look again at the adjacency matrix in equation (3.2), we see that the 1×1 zero matrices in the top left and bottom right corners are L_1, corresponding to the two non-loop vertices. Additionally, the remaining 2×2 block is L_2, the adjacency matrix for the 2-loop. For graphs of this form we will have a column vector $c_k(n)$ to the right of each $k \times k$ diagonal block, the '1' in the column vector represents the edge connecting the element (either a loop or a non-loop vertex) to the next element in sequence. In Figure 3.3, the edge connecting the 2-loop to the final vertex is represented by $c_2(2)$, as can be noted in the adjacency matrix in equation (3.2). In the graph pictured below, the same edge is represented by $c_2(1)$, reflecting the different manner in which the loop is connected to the next vertex.



Therefore, the adjacency matrix for this graph is given by

$$A = \left[\begin{array}{c|cc|c} 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right]$$

Note that the characteristic equation, which depends only upon the block-diagonal entries, will be exactly the same as for the previous matrix in equation (3.2). We will go on to show that this means the recurrence relation for $f(n)$ will be the same for both graphs, except for initial conditions.

Remark 3.9. It will be helpful when reading the next section to make a note of the following identities:

- $\Sigma(L_k^n) = \Sigma(L_k^m)$ for any n and m.
- $L_k^k = I_k$ the identity matrix.
- $r_k(n)c_k(m) = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{otherwise} \end{cases}$
- $r_k(n)L_k = r_k(n+1)$.
- $L_k c_k(n) = c_k(n-1)$.

3.2.1 Single Loops

We are now well equipped to study some graphs in further detail. First we deal with graphs such as that in Figure 3.4, with all vertices connected in a straight line from source to sink but for a single edge 'looping' back to a previous vertex. We will be primarily concerned with this form of digraph so, for clarity, we now introduce the following notation.

Definition 3.10. Let $[l_0, k, l_1]$ denote a graph in which l_0 is the number of vertices before the loop, k is the number of vertices included in the loop and l_1 is the number occurring after the loop.

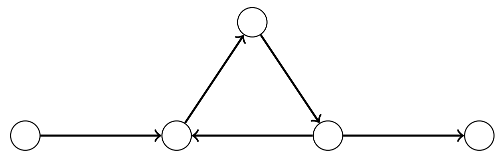


Figure 3.4: 3-loop graph

Consider the graph in Figure 3.4, which will henceforth be referred to as [1, 3, 1], then we obtain the adjacency matrix A and take its powers as follows;

$$A = \left[\begin{array}{c|c|c} 0 & r_3(1) & 0 \\ \hline 0 & L_3 & c_3(3) \\ \hline 0 & 0 & 0 \end{array}\right] \quad A^2 = \left[\begin{array}{c|c|c} 0 & r_3(2) & 0 \\ \hline 0 & L_3^2 & c_3(2) \\ \hline 0 & 0 & 0 \end{array}\right] \quad A^3 = \left[\begin{array}{c|c|c} 0 & r_3(3) & 0 \\ \hline 0 & I_3 & c_3(1) \\ \hline 0 & 0 & 0 \end{array}\right]$$

$$A^4 = \left[\begin{array}{c|c|c} 0 & r_3(1)L_3^3 & r_3(1)c_3(1) \\ \hline 0 & L_3^4 & L_3c_3(1) \\ \hline 0 & 0 & 0 \end{array}\right] = \left[\begin{array}{c|c|c} 0 & r_3(1) & 1 \\ \hline 0 & L_3 & c_3(3) \\ \hline 0 & 0 & 0 \end{array}\right]$$

Note that A^4 is the same as A but for a 1 in the top right corner. On further multiplication this 1 will make no difference since the first column and last row of each matrix are all zeros; for example $A^6 = A^2A^4 = A^2A = A^3$. More generally we can write that $A^{n+3} = A^n$ for $n \geq 2$, noting that $A^4 \neq A$. In fact $\Sigma(A^4) = \Sigma(A) + 1$; that is $f(4) = f(1) + 1$, an initial condition to the recurrence relation $f(n + 3) = f(n)$.

We can find a general form for powers of the adjacency matrix

$$A^{n+1} = \left[\begin{array}{c|c|c} 0 & r_3(1)L_3^n & r_3(1)c_3(1-n) \\ \hline 0 & L_3^{n+1} & L_3c_3(1-n) \\ \hline 0 & 0 & 0 \end{array}\right]$$

Notice that we do not actually use the property that $k = 3$ here. In fact we can consider a more general graph of this form with any size loop, as shown in Figure 3.2, and write down a matrix with a similar structure.

$$A = \left[\begin{array}{c|c|c} 0 & r_k(1) & 0 \\ \hline 0 & L_k & c_k(k) \\ \hline 0 & 0 & 0 \end{array}\right] \qquad A^{n+1} = \left[\begin{array}{c|c|c} 0 & r_k(1)L_k^n & r_k(1)c_k(1-n) \\ \hline 0 & L_k^{n+1} & L_kc_k(1-n) \\ \hline 0 & 0 & 0 \end{array}\right]$$

Consider the entry in the top right corner of the matrix A^{n+1} and observe that

$$r_k(1)c_k(1-n) = \begin{cases} 1 & \text{if } (n-1) \equiv 1 \mod k \\ 0 & \text{otherwise} \end{cases}$$

It is clear that an extra 1 will appear in the top right corner of A^n when $(2-n) \equiv 1 \mod k$ so that we will have $r_k(1)c_k(1) = 1$ in that position. That is, when $n \equiv 1 \mod k$ and, by construction, not when n is actually equal to 1 since then we have a zero in the top right corner. It follows that the recurrence relation for this graph will be $A^{n+k} = A^n$ and hence

$$f(n+k) = f(n) \quad \text{for all } n \geq 2 \tag{3.3}$$

which agrees with our earlier calculations.

3.2.2 Single Loops of Different Order

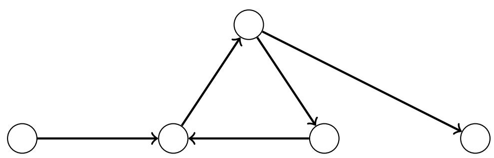


Figure 3.5: Altered 3-loop graph

Now we consider the graph in Figure 3.5 with the following adjacency matrix:

$$B = \left[\begin{array}{c|c|c} 0 & r_3(1) & 0 \\ \hline 0 & L_3 & c_3(2) \\ \hline 0 & 0 & 0 \end{array}\right] \qquad B^{n+1} = \left[\begin{array}{c|c|c} 0 & r_3(1)L_3^n & r_3(1)c_3(3-n) \\ \hline 0 & L_3^{n+1} & L_3c_3(3-n) \\ \hline 0 & 0 & 0 \end{array}\right]$$

Here we expect to see no difference in the recurrence relation for the sequence $f(n)$ from equation (3.3), except for the initial conditions. This difference is due to the different values of n for which the top right entry of B^n is 1. In this case, the top right entry of B^n is 1 when $n \equiv 0 \mod 3$. In other words, one power *earlier* than in the previous case.

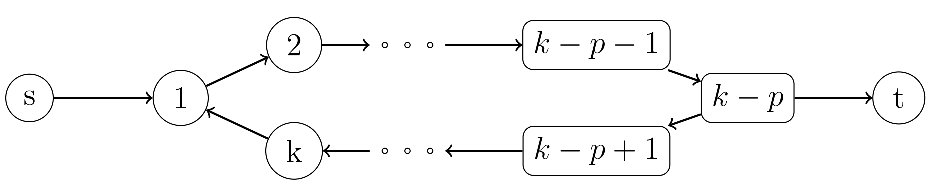


Figure 3.6: k-loop of order p

Generalising to any size loop, consider the graph in Figure 3.6; call the loop in this graph a k-loop of order p. Thus the graph in Figure 3.4 contains a 3-loop of order 0 and the graph in Figure 3.5 contains a 3-loop of order 1. To make things simpler later on we will refer to the case where $p = k$ as being order 0. It is a simple extension of the previous cases to find the adjacency matrix B given below.

$$B = \left[\begin{array}{c|c|c} 0 & r_k(1) & 0 \\ \hline 0 & L_k & c_k(p-1) \\ \hline 0 & 0 & 0 \end{array}\right] \qquad B^{n+1} = \left[\begin{array}{c|c|c} 0 & r_k(1)L_k^n & r_k(1)c_k(1-p-n) \\ \hline 0 & L_k^{n+1} & L_k c_k(1-p-n) \\ \hline 0 & 0 & 0 \end{array}\right]$$

The entry in the top right corner of B^n will be equal to 1 when $r_k(1)c_k(2-p-n) = 1$, which is when $(2-p-n) \equiv 1 \mod k$, or when $n \equiv (1-p) \mod k$.

It is clear that matrix multiplication will become very complicated, especially when we start to consider graphs with more than one loop. Rather than explicitly calculating the powers of the adjacency matrix, it will be convenient to analyse the intrinsic properties of these matrices before continuing.

3.2.3 Deriving Recurrence Relations

Definition 3.11. We define the characteristic polynomial of an $n \times n$ matrix M by $p(\lambda) = \det(\lambda I_n - M)$.

Theorem 3.12 (Cayley-Hamilton [9])**.** *Any matrix $M \in \mathrm{Mat}_n(\mathbb{C})$ is a root of its own characteristic polynomial, that is, $p(M) = 0$.*

This will be particularly useful here because it will allow us to more easily find a recurrence relation on the function $f(n)$ for a given graph.

Proposition 3.13. *Let A be the adjacency matrix for a graph G. Suppose that the characteristic polynomial of A is given by*

$$p(\lambda) = \lambda^d + \alpha_1\lambda^{d-1} + \cdots + \alpha_d$$

then, for all $n \geq 0$, $f(n)$ satisfies the recurrence relation

$$f(n+d) + \alpha_1 f(n+d-1) + \ldots + \alpha_d f(n) = 0$$

Proof. By applying the Cayley-Hamilton Theorem, we have

$$p(A) = A^d + \alpha_1 A^{d-1} + \cdots + \alpha_d = 0$$

Continuing by induction we get

$$A^{n+d} + \alpha_1 A^{n+d-1} + \cdots + \alpha_d A^n = 0$$

Now we apply the sigma function, defined in Definition 3.5, to get

$$\sum(A^{n+d}) + \alpha_1 \sum(A^{n+d-1}) + \cdots + \alpha_d \sum(A^n) = 0$$

Therefore, by Corollary 3.7, we deduce the recurrence relation

$$f(n+d) + \alpha_1 f(n+d-1) + \ldots + \alpha_d f(n) = 0$$

□

Example 3.14. Consider again the 2-loop graph in Figure 3.1 and its adjacency matrix A in equation (3.2) represented in upper block triangular form. The characteristic polynomial is given by

$$p(\lambda) = \det(\lambda I_4 - A) = \lambda^2(\lambda^2 - 1) = \lambda^4 - \lambda^2$$

By applying Proposition 3.13, it follows that

$$f(n+2) - f(n) = 0, \qquad \text{for all } n \geq 2.$$

We thus have a recurrence relation, wanting of initial conditions, for the number of paths of length n in $[1, 2, 1]$. Note that this agrees with equation (3.1), which we obtained by considering the reccurence relations on the four vertices.

3.2.4 Double Loops

We will now concentrate on graphs containing two non-intersecting loops where both loops are of order 0. Much of what we study in the following chapters will concern these types of graphs. Extending our notation introduced in Definition 3.10 we denote such graphs by $[l_0, t_1, l_1, t_2, l_2]$ where l_1 is the number of vertices occurring in between the two loops of sizes t_1 and t_2. When $l_1 = 0$ the two loops are connected by a single edge.

Lemma 3.15. *Consider the general two loop graph $G = [l_0, t_1, l_1, t_2, l_2]$, then the characteristic polynomial of the adjacency matrix A for G is given by*

$$p(\lambda) = \lambda^{l_0+l_1+l_2}(\lambda^{t_1} - 1)(\lambda^{t_2} - 1) \tag{3.4}$$

Proof. Using the preceeding analysis, it follows that the adjacency matrix A will be of the form

$$A = \left[\begin{array}{c|c|c|c|c} \mathbf{J}_{l_0} & \mathbf{K}_{l_0,t_1} & 0 & 0 & 0 \\ \hline 0 & L_{t_1} & \mathbf{K}_{t_1,l_1} & 0 & 0 \\ \hline 0 & 0 & \mathbf{J}_{l_1} & \mathbf{K}_{l_1,t_2} & 0 \\ \hline 0 & 0 & 0 & L_{t_2} & \mathbf{K}_{t_2,l_2} \\ \hline 0 & 0 & 0 & 0 & \mathbf{J}_{l_2} \end{array}\right]$$

where $\mathbf{J}_n$ is the $n \times n$ matrix with 1's on the off-diagonal and 0's everywhere else, and $\mathbf{K}_{n,m} = c_n(n)r_m(1)$ is the $n \times m$ matrix with a single 1 in the bottom left corner and 0's everywhere else. It can be shown that the determinant of an upper block triangular matrix is equal to the product of the determinants of the diagonal blocks. The result then follows by calculation. □

Corollary 3.16. *Let $G = [l_0, t_1, l_1, t_2, l_2]$, then a recurrence relation for $f(n)$ is given by*

$$f(n + t_1 + t_2) - f(n + t_1) - f(n + t_2) + f(n) = 0 \quad \text{for all } n \geq l_0 + l_1 + l_2. \tag{3.5}$$

Proof. We deduce the recurrence relation by applying Proposition 3.13 to Lemma 3.15. □

Remark 3.17. Note that equation (3.5) implies that the recurence relation on $f(n)$ will be the same, up to initial conditions, regardless of how the 'non-loop' vertices are arranged. Given two graphs $[l_0, t_1, l_1, t_2, l_2]$ and $[l'_0, t_1, l'_1, t_2, l'_2]$, we will always get the relation given in equation (3.5) provided $l'_0 + l'_1 + l'_2 = l_0 + l_1 + l_2$. Note that this does not imply that the growth of f will be the same in both cases. In fact we will see later that the initial conditions can change the behaviour of $f(n)$ as n increases, even when only a very subtle change is made in the arrangement of the non-loop vertices.

3.3 Generating Functions for Digraphs

In the previous section, we deduced a recurrence relation that we can use to examine the growth of f for any directed graph, but it may be necessary to encode this information in a generating function before we can observe any interesting behaviour. In the following sections we will see that considering the generating function for f yields some interesting results.

Example 3.18. Consider the graph $[1, 3, 1]$ in Figure 3.4. From elementary calculations, $f(0) = f(1) = f(2) = f(3) = 5$ and recall the conditions that $f(4) = f(1) + 1 = 6$ and $f(n + 3) = f(n)$ for $n \geq 2$. Therefore by applying Theorem 2.8, we can deduce the generating function

$$F(x) = \frac{5 + 5x + 5x^2 + x^4}{1 - x^3}$$

Using the same argument as above, we obtain the following generating function for the more general graph $[1, k, 1]$

$$F(x) = \frac{(k+2) + \cdots + (k+2)x^{k-1} + x^{k+1}}{1 - x^k} \tag{3.6}$$

We can also find the generating function in the case of the general k-loop, order p, graph in Figure 3.6

$$\begin{aligned} F(x) =& \sum_{n=0}^{\infty} f(n)x^n \\ =&(k+2) + (k+2)x + \cdots + (k+3)x^{k+1-p} + \\ &+ (k+2)x^{k+2-p} + \cdots + (k+3)x^{2k+1-p} + \dots \\ (1 - x^k)F(x) =&(k+2) + \cdots + (k+2)x^{k-p} + (k+3)x^{k+1-p} + \cdots + (k+2)x^{k-1} \end{aligned}$$

It follows that

$$\begin{aligned} F(x) =& \frac{(k+2) + \cdots + (k+3)x^{k+1-p} + \cdots + (k+2)x^{k-1}}{1 - x^k} \\ =& \frac{k+2}{1-x} + \frac{x^{k+1-p}}{1-x^k} \end{aligned}$$

This agrees with the function that we had for the case $p = 0$.

More generally, we can apply the results from Chapter 2 to deduce the form of the generating function for any of the graphs we are considering.

Proposition 3.19. *Let $G = [l_0, t_1, l_1, t_2, l_2]$, then the generating function F for f associated to G will be of the form*

$$F(x) = \frac{P(x)}{(1 - x^{t_1})(1 - x^{t_2})}$$

where $\deg(P) \leq l_0 + t_1 + l_1 + t_2 + l_2$.

Proof. From Corollary 3.16, $f(n)$ has the recurrence relation

$$f(n + t_1 + t_2) - f(n + t_1) - f(n + t_2) + f(n) = 0 \text{ for all } n \geq l_0 + l_1 + l_2$$

The result then follows immediately from Theorem 2.8. Note that $\deg(P) \leq l_0 + t_1 + l_1 + t_2 + l_2$ since the recurrence relation has up to $l_0 + t_1 + l_1 + t_2 + l_2$ initial conditions. $\square$

3.4 Introduction to Quasipolynomials

Definition 3.20 (Stanely [12])**.** A *quasipolynomial* of degree d is, informally, a polynomial of degree d that takes periodic functions (with integer period) as coefficients instead of constants.
More formally a *quasipolynomial* of degree d is a function $f : \mathbb{N} \to \mathbb{C}$ of the form

$$f(n) = c_d(n)n^d + c_{d-1}(n)n^{d-1} + \cdots + c_0(n),$$

where each $c_j(n)$ is a periodic function (with integer period), and where $c_d(n)$ is not identically zero.

Equivalently, f is a *quasipolynomial* of degree d if there exists an integer $N > 0$ and polynomials $f_0, f_1, \ldots, f_{N-1}$ with $\deg(f_i) \leq d$ and at least one i with $\deg(f_i) = d$ such that

$$f(n) = f_i(n) \text{ if } n \equiv i \mod N$$

We call f_i the constituents of f. Furthermore, this integer N is called a *quasiperiod* of f.

Proposition 3.21. *The two definitions for a quasipolynomial function given above are indeed equivalent.*

Proof. Suppose we have

$$f(n) = c_d(n)n^d + c_{d-1}(n)n^{d-1} + \ldots + c_0(n)$$

where each $c_j(n)$ is a periodic function with integer period and c_d is not identically zero. Let p_j denote the minimal period for c_j. Let $N = \operatorname{lcm}(p_0, p_1, \cdots, p_d)$, then $c_j(n + N) = c_j(n)$ for all j. Now for $i = 0, 1, \cdots, N-1$ set

$$f_i(n) = c_d(i)n^d + c_{d-1}(i)n^{d-1} + \ldots + c_0(i)$$

so that each f_i has degree at most d and at least one has degree equal to d. Now we have

$$f(n) = f_i(n) \text{ if } n \equiv i \mod N$$

which is the second definition. Conversely, by letting $c_j(i)$ take coefficients from the n^j

term in f_i and extending each c_j periodically by $c_j(n+N) = c_j(n)$ the reverse direction is quickly proved. □

Remark 3.22. Note that N in the second definition is a common period of the c_j in the first definition and is therefore not unique. However, in the proof the minimum such N was found by taking the minimum periods of each c_j and, by the construction of N, each of these minimum periods will divide N.

An extension of Theorem 2.8 can now be given, which will be applied when analysing the growth of the number of paths in the digraphs introduced earlier.

Theorem 3.23 (Stanely [12]). *The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ and integer $N > 0$ are equivalent.*

1. *A function f is a quasipolynomial of quasiperiod N.*

2. $$\sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}$$

   where $P(x), Q(x) \in \mathbb{C}[x]$ and every zero α of $Q(x)$ satisfies $\alpha^N = 1$.

Proof. Let us start with (2.) $\Rightarrow$ (1.). Let $Q(x) = 1 + \alpha_1 x + \cdots + \alpha_d x^d$, with roots $x = a_1, \ldots, a_d$ then by Theorem 2.8 we have

$$f(n+d) + \alpha_1 f(n+d-1) + \cdots + \alpha_d f(n) = 0$$

This recurrence has characteristic polynomial

$$r^d + \alpha_1 r^{d-1} + \cdots + \alpha_d$$

which can be factorised $\prod_{i=1}^{k}(r - \gamma_i)^{d_i}$ where each γ_i is a distinct root and d_i is its multiplicity. It then follows that we can find an expression for $f(n)$ of the form

$$f(n) = \sum_{i=1}^{k} P_i(n)\gamma_i^n$$

where each $P_i(n)$ is a polynomial in n with $\deg(P_i) < d_i$. Let $d = \max d_i$ and write each $P_i(n) = \beta_{i_1} n^{d-1} + \cdots + \beta_{i_{d-1}} n + \beta_{i_d}$ and so we have

$$f(n) = \sum_{i=1}^{k} \beta_{i_1}\gamma_i^n n^{d-1} + \cdots + \sum_{i=1}^{k} \beta_{i_{d-1}}\gamma_i^n n + \sum_{i=1}^{k} \beta_{i_d}\gamma_i^n$$

Now note that solving $Q(\frac{1}{r}) = 0$ gives the roots $\gamma_1, \cdots, \gamma_k$ and so each $\gamma_i = a_j^{-1}$. For each a_j we have $a_j^N = 1$ and so we also must have $(a_j^{-1})^N = \gamma_i^N = 1$ for some integer N.

Let $c_l(n) = \sum_{i=1}^{k} \beta_{i_l} \gamma_i^n$ then

$$c_l(n+N) = \sum_{i=1}^{k} \beta_{i_l} \gamma_i^{n+N} = \sum_{i=1}^{k} \beta_{i_l} \gamma_i^n \gamma_i^N = \sum_{i=1}^{k} \beta_{i_l} \gamma_i^n = c_l(n)$$

so each c_l is periodic with integer period N and we have

$$f(n) = c_1 n^{d-1} + \cdots + c_{d-1} n + c_d$$

Therefore f is a quasipolynomial and following the proof for Proposition 3.21 we get that f has quasiperiod N.

For (1.)⇒(2.), let f be a quasipolynomial with quasiperiod N. Then we can write f in the form

$$f(n) = c_d(n)n^d + \cdots + c_1(n)n + c_0$$

where each c_j is such that $c_j(n+N) = c_j(n)$. Therefore we can write the generating function,

$$\sum_{n=0}^{\infty} f(n)x^n = \sum_{j=0}^{d} \sum_{n=0}^{\infty} c_j(n)n^j x^n = \sum_{j=0}^{d} \frac{P_j(x)}{Q_j(x)}$$

Now fix j, then we have that $c_j(i) = \lambda_{ji}$ for $i = 0, 1, \cdots, N-1$ and each $\lambda_{ji} \in \mathbb{C}$. Hence

$$\frac{P_j(x)}{Q_j(x)} = \sum_{n=0}^{\infty} c_j(n)n^j x^n = \sum_{i=0}^{N-1} [\lambda_{ji} \sum_{n=0}^{\infty} (Nn+i)^j x^{Nn+i}] = \sum_{i=0}^{N-1} [\lambda_{ji} x^i \sum_{n=0}^{\infty} (Nn+i)^j (x^N)^n]$$

Then for a fixed i, we can write

$$\lambda_{ji} x^i \sum_{n=0}^{\infty} (Nn+i)^j (x^N)^n = \lambda_{ji} x^i \frac{P_{j_i}(x^N)}{Q_{j_i}(x^N)}$$

Therefore, combining the results above, it follows that

$$\sum_{n=0}^{\infty} f(n)x^n = \sum_{j=0}^{d} \frac{P_j(x)}{Q_j(x)} = \sum_{j=0}^{d} \sum_{i=0}^{N-1} \lambda_{ji} x^i \frac{P_{j_i}(x^N)}{Q_{j_i}(x^N)}$$

From Example 2.15 and Remark 2.16, we have $Q_{j_i}(x) = (1-x)^{j_i+1}$ for each j_i. Hence

$$\sum_{n=0}^{\infty} f(n)x^n = \sum_{j=0}^{d} \frac{P_j(x)}{(1-x^N)^{j+1}} = \frac{\sum_{j=0}^{d}(1-x^N)^{d-j}P_j(x)}{(1-x^N)^{d+1}}$$

where $P_j(x) = \sum_{i=0}^{N-1} P_{j_i}(x^N)$. This expression is of the form $\frac{P(x)}{Q(x)}$ and every zero of $Q(x)$, α say, is an N^{th} root of unity and therefore satisfies $\alpha^N = 1$. □

Remark 3.24. Less constructive proofs are possible but they are less illuminating. More constructive still would be to note that N is not necessarily the least common period for every c_j, and a similar argument to that for (1.)⇒(2.) could be followed taking the least periods of each c_j.

Remark 3.25. When considering f of a graph G, we will see that there exists an n_0 such that $f(n)$ will be quasipolynomial with quasiperiod N for all $n \geq n_0$. For simplicity, we will now refer to this *eventual quasiperiod* of f as the quasiperiod of f.

Remark 3.26. Additionally, for brevity in explanations, when we say the quasiperiod of a graph G, we are referring to the quasiperiod of f associated to G.

Example 3.27. From the analysis in this chapter so far, we have shown that the generating functions F' and F^*, for graphs $G' = [l_0, k, l_1]$ and $G^* = [l_0, t_1, l_1, t_2, l_2]$ respectively, are of the form

$$F'(x) = \frac{P'(x)}{1-x^k} \qquad \text{and} \qquad F^*(x) = \frac{P^*(x)}{(1-x^{t_1})(1-x^{t_2})}$$

Therefore, by Theorem 3.23, G' has quasiperiod k and G^* has quasiperiod $\text{lcm}(t_1, t_2)$. However, this may not be the minimal quasiperiod since we may be able to reduce F' or F^* to simpler forms, altering the roots of the denominator. This motivates the following definition.

Definition 3.28. For a graph G we define $q(G)$ as the minimal quasiperiod of G.

In order to analyse the quasiperiod of the graphs, we now introduce some theory relating to cyclotomic polynomials. We will see that this insight forms a bound on $q(G)$ for a graph G.

3.4.1 Cyclotomic Polynomials [4]

Recall an n^{th} root of unity is a complex number z such that $z^n = 1$. An n^{th} root of unity is said to be primitive if $z^n = 1$ and $z^k \neq 1$ for all $k \in \{1, 2, \cdots, n-1\}$. It is easy then to see that the n^{th} primitive roots of unity are of the form $e^{2\pi i \frac{k}{n}}$ where k and n are coprime.

Definition 3.29. The n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined as

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n-1 \\ \gcd(k,n)=1}} (x - e^{2\pi i \frac{k}{n}})$$

Note that $\deg(\Phi_n) = \varphi(n)$ where φ is Euler's totient function.

The following relations lead to a quick way for calculating cyclotomic polynomials.

Lemma 3.30. *Let n be a positive integer. Then*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Proof. For k such that $1 \le k \le n$, we have that $\gcd(k, n) = m$ where m divides n. Letting d run through the divisors of n we obtain

$$\prod_{d|n} \Phi_d(x) = \prod_{k=1}^{n} (x - e^{2\pi i \frac{k}{n}}) = x^n - 1$$

From this result it follows that

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{d|n, d \neq n} \Phi_d(x)}$$

Noting that $\Phi_1(x) = x - 1$ can easily be calculated, this result gives a quick inductive way of calculating $\Phi_n(x)$. We can now argue inductively to show that the coefficients of $\Phi_n(x)$ are certainly rational. They are in fact always integers but a little more work is needed to show this. $\square$

Remark 3.31. As before, let $F(x) = P(x)/Q(x)$ denote the generating function for $f(n)$, the number of paths of length n, associated with a graph. If we apply the theory of cyclotomic polynomials to the graphs we have introduced so far, we discover that $Q(x)$ is in fact a product of several cyclotomic polynomials. We can argue, informally, that if $P(x)$ and $Q(x)$ have a common factor then it must be an entire cyclotomic polynomial. The argument for this is that if only part of a cyclotomic polynomial were to cancel, we would be left with $Q(x)$ and $P(x)$ taking some non-real coefficients. Therefore f would be likely to take some imaginary values, which is not well-defined for a function counting paths in a graph.

3.5 Further Results

Proposition 3.32. *Let $G = [l_0, k, l_1]$, then $q(G)$ divides k for all $n \ge l = l_0 + l_1$.*

Proof. By the result from Lemma 3.15 the adjacency matrix A of G has characteristic polynomial

$$p(\lambda) = \lambda^l (\lambda^k - 1)$$

Then, by applying Proposition 3.13, it follows that

$$f(n+k) - f(n) = 0 \qquad \forall\ n \geq l$$

Therefore, by Theorem 2.8, we get that the generating function is

$$F(x) = \sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{1 - x^k}$$

By applying Lemma 3.30, we can express $F(x)$ as

$$F(x) = \frac{-P(x)}{\prod\limits_{d|k} \Phi_d(x)}$$

It may happen that $P(x)$ can be divided by some of the cyclotomic polynomials, reducing $F(x)$ to a simpler form. Suppose the most reduced form of $F(x)$ is given by

$$F(x) = \frac{P'(x)}{\Phi_{d_1}(x) \dots \Phi_{d_r}(x)}$$

where d_i divides k for each i. Therefore, it follows from Proposition 3.23 that the quasiperiod divides k. Since $F(x)$ is assumed to be in its most reduced form, this must be the minimum quasiperiod and hence $q(G)$ divides k. $\square$

Proposition 3.33. *Let* $G = [l_0, t_1, l_1, t_2, l_2]$, *then* $q(G)$ *divides* $L = \operatorname{lcm}(t_1, t_2)$ *for all* $n \geq l = l_0 + l_1 + l_2$.

Proof. By Proposition 3.19, we get that the generating function is

$$F(x) = \sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{(1 - x^{t_1})(1 - x^{t_2})}$$

Therefore, by applying the theory of cyclotomic polynomials above, it follows that

$$F(x) = \frac{P(x)}{\prod\limits_{j|t_1} \Phi_j(x) \prod\limits_{k|t_2} \Phi_k(x)}$$

It may happen that $P(x)$ can be divided by some of the cyclotomic polynomials. Then $F(x)$ can be reduced to a simpler form, in which case we have

$$F(x) = \frac{P(x)}{\Phi_{j_1}(x) \dots \Phi_{j_r}(x) \Phi_{k_1}(x) \dots \Phi_{k_s}(x)}$$

Hence, $q(G) = \mathrm{lcm}(j_1, \ldots, j_r, k_1, \ldots, k_s)$. But we know that $j_1, \ldots, j_r$ all divide t_1 and $k_1, \ldots, k_s$ all divide t_2. Thus, $q(G)$ divides $L = \mathrm{lcm}(t_1, t_2)$ as required. $\square$

Chapter 4

Fully Classifying Graph Families

The aim of this chapter is to introduce a set of sufficient and necessary conditions to guarantee that a function f will be quasiploynomial with quasiperiod N. We will then analyse a particular graph family $\mathcal{G}$ in detail, deriving some key results related to the growth of their associated f and establish a full classification of all G in this given family by exhibiting a finite partition.

4.1 Quasipolynomials and Quasiperiods

In this section, we will consider the theory of quasipolynomials in more depth and focus on establishing a result to identify whether a function is quasipolynomial. However, before we do that, we establish a result to determine a necessary condition under which a given function f is polynomial. The reader should note that this is the special case where f is quasipolynomial of minimal quasiperiod 1.

Theorem 4.1 (Polynomial)**.** *A polynomial f is of degree d if and only if the finite difference Δf is a polynomial of degree $d-1$.*

Proof. Suppose f has degree d, then utilising the results from Chapter 2, we can represent f and Δf under a change of basis. This yields $f(n) = b_d\binom{n}{d} + b_{d-1}\binom{n}{d-1} + \ldots + b_1\binom{n}{1} + b_0\binom{n}{0}$ where b_d is non-zero. Now we substitute this into the formula for Δf.

$$\begin{aligned}\Delta f(n) &= b_d\tbinom{n}{d} + b_{d-1}\tbinom{n}{d-1} + \cdots + b_0\tbinom{n}{0} - b_d\tbinom{n-1}{d} - b_{d-1}\tbinom{n-1}{d-1} - \cdots - b_0\tbinom{n-1}{0} \\ &= b_d[\tbinom{n}{d} - \tbinom{n-1}{d}] + b_{d-1}[\tbinom{n}{d-1} - \tbinom{n-1}{d-1}] + \ldots + b_0[\tbinom{n}{0} - \tbinom{n-1}{0}]\end{aligned}$$

Recalling the binomial identity $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for $k \leq n-1$, and that $\binom{t}{0} = 1$ for all $t \in \mathbb{N}$, we simplify the above expression as

$$\Delta f(n) = b_d\binom{n-1}{d-1} + b_{d-1}\binom{n-1}{d-2} + \ldots + b_1\binom{n-1}{0}$$

Therefore, f and Δf both have leading coefficient b_d. Hence, $\deg(\Delta f) = d-1$ if $b_d \neq 0$, which follows from the assumption that $\deg(f) = d$. This completes the proof for the forward implication. The proof for the reverse implication follows in a similar manner with the argument reversed. □

Theorem 4.2. *A function f is a quasipolynomial with quasiperiod N if and only if Δf is a quasipolynomial with quasiperiod N.*

Proof. Omitted. It proceeds in the same way as Theorem 4.1. □

Remark 4.3. Theorem 4.2 was used throughout our research as a sufficient condition for determining the minimial quasiperiod of a given graph. For example, it can be shown that f associated to a two loop graph is a linear function, which means that if the constituents of f have the same leading coefficient, Δf will be a quasipolynomial of order zero. Therefore, we can apply Theorem 4.2 to calculate $q(G)$ from Δf, which is often easier to determine since Δf has a smaller degree.

Theorem 4.4 (Quasipolynomial)**.** *Suppose that*

$$\sum_{i=1}^{N} \Delta f(n+i) = \sum_{i=1}^{N} \Delta f(n+i+N)$$

Then the function f has quasiperiod N.

Proof. Let us assume

$$\sum_{i=1}^{N} \Delta f(n+i) = \sum_{i=1}^{N} \Delta f(n+i+N)$$

By expanding Δf, it follows that

$$f(n+N) - f(n) = f(n+2N) - f(n+N)$$

and so

$$f(n+2N) - 2f(n+N) + f(n) = 0$$

Now we apply Theorem 2.8 to deduce that the denominator of the rational generating function for $f(n)$ is of the form $Q(x) = x^{2N} - 2x^N + 1 = (x^N - 1)^2$. Hence every root α of $Q(x)$ satisfies $\alpha^N = 1$ and f has quasiperiod N by Theorem 3.23. □

Remark 4.5. Theorem 4.4 was a useful sufficient condition for identifying the quasiperiod of a graph during our research.

4.2 Graph Families

In this section we will attempt to formalise some of the key results from our experimental research using our programme 'Digraph Creata', as outlined in Appendices A and B. Before we move on to the main content, we introduce some new concepts and establish preliminary results. We will continue using the notation for graphs that was defined in Chapter 3.

Definition 4.6. We define a *graph family* as the set of graphs

$$\mathcal{G} = \{[l_0, t_1, l_1, t_2, \ldots, t_d, l_d] \mid l_i \in \mathbb{N} \text{ for all } 0 \leq i \leq d\}$$

where $[l_0, t_1, l_1, t_2, \ldots, t_d, l_d]$ is an extension of the notation introduced in Definition 3.10 and denotes a graph with d loops where $t_i \in \mathbb{N}$ is the given length of the i^{th} loop.

Definition 4.7. Fix r with $0 \leq r \leq d$. Set $\hat{\eta} = \{\eta_0, \ldots, \eta_{r-1}, \eta_{r+1}, \ldots, \eta_d\}$ for some fixed $\eta_0, \ldots, \eta_d \in \mathbb{N}$ and also set $\hat{\zeta} = \{\zeta_1, \zeta_2, \ldots, \zeta_d\}$ for some fixed $\zeta_1, \ldots, \zeta_d \in \mathbb{N}$. Then we define a *graph subfamily* of $\mathcal{G}$ as the set of graphs

$$G_{\hat{\eta}}^{\hat{\zeta}}(r) = \{[\eta_0, \zeta_1, \ldots \eta_{r-1}, \zeta_{t-1}, l_r, \zeta_r, \ldots, \eta_d, \zeta_d] \mid l_r \in \mathbb{N}\}$$

Informally, a graph subfamily of $\mathcal{G}$ is the infinite collection of graphs in which every t_i is fixed and every l_i is fixed except l_r. The fixed $l_i = \eta_i$ and the fixed $t_i = \zeta_i$. The subfamily then consists of all graphs with distinct l_r.

Definition 4.8. Let $\mathcal{G}$ be a given graph family with a subfamily $G_{\hat{\eta}}^{\hat{\zeta}}(r)$. Then we define the *signature* of $\mathcal{G}$ at $G_{\hat{\eta}}^{\hat{\zeta}}(r)$, denoted by $\Omega(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(r))$, as the sequence of quasiperiods obtained from the subfamily $G_{\hat{\eta}}^{\hat{\zeta}}(r)$ by considering $l_r = 0, 1, 2, \ldots$

Graph	Quasiperiod
[0,2,1,3,1]	3
[1,2,1,3,1]	6
[2,2,1,3,1]	3
[3,2,1,3,1]	6
[4,2,1,3,1]	3
[5,2,1,3,1]	6
[l_0,2,1,3,1]	

Graph	Quasiperiod
[0,2,0,3,1]	3
[1,2,0,3,1]	1
[2,2,0,3,1]	3
[3,2,0,3,1]	3
[4,2,0,3,1]	1
[5,2,0,3,1]	3
[l_0,2,0,3,1]	

Figure 4.1: Signatures from examples 4.9 and 4.10

This concept is best illustrated with a couple of examples. The reader may also wish to consult Table 1 in Appendix B while reading this section, to lend a firm example to the ideas that are presented.

Example 4.9. Consider the graph family $\mathcal{G} = [l_0, 2, l_1, 3, l_2]$ and subfamily $G_{\hat{\eta}}^{\hat{\zeta}}(0) = [l_0, 2, 1, 3, 1]$ where $\hat{\eta} = \{1, 1\}$ and $\hat{\zeta} = \{2, 3\}$. Let l_0 take values $0, 1, 2, \ldots$ and consider the quasiperiods of the resulting graphs. From Figure 4.1, we have the sequence $3, 6, 3, 6, 3, 6$. Therefore $\Omega(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(0)) = 3, 6, 3, 6, 3, 6, \ldots$

Example 4.10. Consider a different subfamily of $\mathcal{G}$, the subfamily $\hat{G}_{\hat{\eta}}^{\hat{\zeta}}(0) = [l_0, 2, 0, 3, 1]$ where $\hat{\eta} = \{0, 1\}$ and $\hat{\zeta} = \{2, 3\}$. From Figure 4.1, we see that $\Omega(\mathcal{G}, \hat{G}_{\hat{\eta}}^{\hat{\zeta}}(0)) = 3, 1, 3, 3, 1, 3, \ldots$

Remark 4.11. In both of the examples above, we found that the signature appeared to be determined by a recurring subsequence, that is, the sequence of quasiperiods of graphs in the same subfamily form a uniform pattern. This motivates the following conjecture.

Conjecture 4.12 (Invariance of Quasiperiod)**.** *Let $G = [l_0, t_1, l_1, t_2, \ldots, t_d, l_d]$. Suppose that $L = \operatorname{lcm}(t_1, t_2, \ldots, t_d)$ and $G' = [l_0 + Lm_0, t_1, l_1 + Lm_1, t_2, \ldots, t_d, l_d + Lm_d]$ for some $m_i \in \mathbb{N}$, then $q(G) = q(G')$.*

Even though every result from our computational experimentation satisfies this conjecture, we have thus far only established a proof of the conjecture in certain cases, including the case $d = 1$ (see Theorem 4.14). Before we begin the proof, we first introduce an essential lemma.

Lemma 4.13. *Let G be a one loop graph of the form $G = [l_0, t_1, l_1]$ and let $f(n)$ be the total number of paths of length n. Let v_g denote the 'choice' vertex in the loop, as shown in Figure 4.2, and $g(n)$ be the number of paths of length n starting from v_g. Then,*

$$f(n) = g(n) + g(n-1) + \cdots + g(n - l_0 - t_1 + 1)$$

for n sufficiently large. Furthermore, for $r_n \equiv (t_1 - n) \mod t_1$,

$$g(n) = \left\lfloor \frac{l_1 + r_n}{t_1} \right\rfloor + 1$$

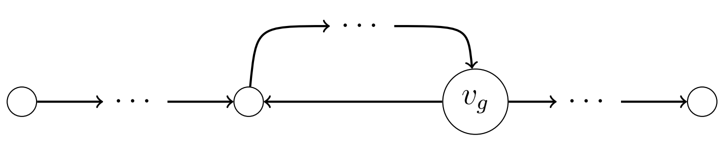


Figure 4.2: $G = [l_0, t_1, l_1]$

Proof. Assuming n is sufficiently large, a path from any vertex before v_g has no choice in direction until it reaches v_g, and then takes any possible path from v_g with its remaining 'moves'. Therefore, there are $g(n - i)$ paths of length n from the vertex located i vertices prior to v_g. Noting that for n sufficiently large there will be no paths of length n from any of the vertices beyond v_g, it follows that

$$f(n) = g(n) + g(n-1) + \cdots + g(n - l_0 - t_1 + 1)$$

To find an expression for $g(n)$, note that there are two cases. Case 1: the path from v_g remains in the loop. There is only 1 path in this case. Case 2: the path from v_g leaves the loop and finishes in the tail of the graph. To express case 2 more formally, let $r_n \equiv (t_1 - n) \mod t_1$ with $0 \leq r_n \leq t_1 - 1$. We express r_n in this way because it means that we can start counting the paths that finish outside the loop as follows. Let k be the number of paths that finish at a vertex past v_g, then k is the largest integer such that $kt_1 - r_n \leq l_1$. Intuitively, this counts the number of times we can 'unwrap' the path from the loop and still finish within the tail. Therefore $k = \lfloor \frac{l_1 + r_n}{t_1} \rfloor$. By combining the cases, it follows that

$$g(n) = \left\lfloor \frac{l_1 + r_n}{t_1} \right\rfloor + 1$$

Furthermore, since $r_n \in \{0, 1, \cdots, t_1 - 1\}$, then there exists a unique $r_0 \in \{0, 1, \cdots, t_1 - 1\}$ such that,

$$\left\lfloor \frac{l_1 + r}{t_1} \right\rfloor = \begin{cases} \frac{l_1 + r_0}{t_1} - 1 & \text{if } r_n < r_0 \\ \frac{l_1 + r_0}{t_1} & \text{if } r_n \geq r_0 \end{cases}$$

□

Using this lemma, we can now prove Conjecture 4.12 for the one loop case.

Theorem 4.14. *Let $G = [l_0, t_1, l_1]$, $G' = [l_0 + t_1, t_1, l_1]$ and $G^* = [l_0, t_1, l_1 + t_1]$. Then $q(G) = q(G') = q(G^*)$.*

Proof. For each of the graphs respectively, let $f(n)$, $f'(n)$ and $f^*(n)$ be the number of paths of length n and $g(n), g'(n)$ and $g^*(n)$ be the number of paths of length n from the choice vertex. Since $g(n)$ only depends on t_1 and l_1 it immediately follows that, $g(n) = g'(n)$. Furthermore, since $r_n \equiv (t_1 - n) \mod t_1 \equiv (kt_1 - n) \mod t_1$, for some $k \in \mathbb{Z}$, it also follows that $g(n + kt_1) = g(n)$. Therefore,

$$\begin{aligned} f'(n) &= g(n) + g(n-1) + \cdots + g(n - l_0 - t_1 + 1) + \\ &\qquad + g(n - l_0 - t_1) + \cdots + g(n - l_0 - 2t_1 + 1) \\ &= f(n) + g(n - l_0 - t_1) + \cdots + g(n - l_0 - 2t_1 + 1) \\ &= f(n) + g(n) + g(n-1) + \cdots + g(n - t_1 + 1) \\ &= f(n) + r_0\Big(\frac{l_1 + r_0}{t_1}\Big) + (t_1 - r_0)\Big(\frac{l_1 + r_0}{t_1} + 1\Big) \\ &= f(n) + l_1 + t_1 \end{aligned}$$

Hence, for n sufficiently large, $f'(n)$ differs from $f(n)$ by a fixed constant for each n. Therefore $q(G') = q(G)$.

Now consider $g^*(n) = \lfloor \frac{l_1+t_1+r_n}{t_1} \rfloor + 1 = \lfloor \frac{l_1+r_n}{t_1} \rfloor + 2 = g(n) + 1$, then

$$\begin{aligned} f^*(n) &= g^*(n) + g^*(n-1) + \cdots + g^*(n - l_0 - t_1 + 1) \\ &= g(n) + g(n-1) + \cdots + g(n - l_0 - t_1 + 1) + l_0 + t_1 \\ &= f(n) + l_0 + t_1 \end{aligned}$$

Hence, for n sufficiently large, we have that $f^*(n)$ differs from $f(n)$ by a fixed constant for each n and so $q(G^*) = q(G)$. Therefore by transitivity, $q(G) = q(G') = q(G^*)$. $\square$

Proposition 4.15. *Let $G = [l_0, t_1, l_1, t_2, l_2]$ and set $L = \mathrm{lcm}(t_1, t_2)$. Define $G' = [l_0 + Lm_0, t_1, l_1 + Lm_1, t_2, l_2 + Lm_2]$, for some $m_i \in \mathbb{N}$, then $q(G) = q(G')$.*

Proof. (Sketch) Having proven Conjecture 4.12 for the one loop case one might hope that there may be some way of analogously extending the argument to the two loop case and this is, at least in some sense, possible.

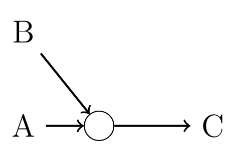


Figure 4.3

Consider the digraph in Figure 4.3 where A, B and C are any digraphs. It is clear that you cannot move between A and B or return to either A or B once you have left them. Therefore, when considering the number of paths of length n in this graph, we may count the number of paths in C with A appended and the number of paths in C with B appended and then take off the paths in C, which we have counted twice. Now consider a graph of the form $[l_0, t_1, l_1, t_2, l_2]$, as shown in Figure 4.4.

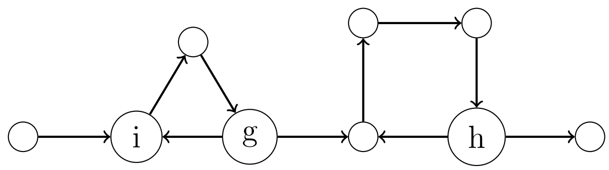


Figure 4.4: Choices vertices for $[1, 3, 0, 4, 1]$

Denote the vertices labelled g, h and i by v_g, v_h and v_i respectively. Lemma 4.13 tells us that the number of paths of length n from v_h is $h(n) = \lfloor \frac{l_2+r_n}{t_2} \rfloor + 1$. Now we consider all the ways a path of length n might reach vertex v_h by moving backwards from v_h through the graph. From Theorem 4.14, we can implement this process until we reach v_i at which point we are presented with a choice that can be represented as a branch. One branch represents the choice to continue the path around the loop and one represents the choice to move out of the loop. Figure 4.5 shows this process applied to the graph in Figure 4.4.

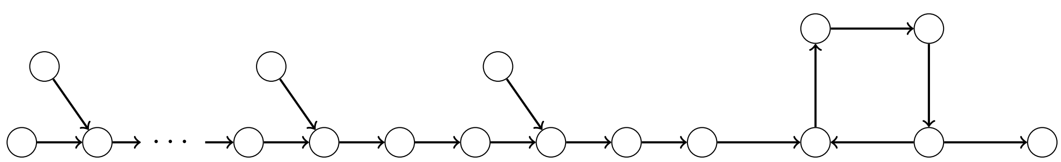


Figure 4.5: Splitting the graph

In Figure 4.5 we terminated a branch either when we reached a 'dead end' when tracing the graph backwards or when we had counted back n steps. The number of paths of length n in this graph will be the same as the number of paths of length n in $[l_0, t_1, l_1, t_2, l_2]$ which reach v_h. Following the explanation for Figure 4.3, we can count the number of paths in the graph in Figure 4.5 by splitting it into finitely many 1-loop graphs either of the form $[l_0 + at_1 + l_1, t_2, l_2]$ or $[at_1 + l_1, t_2, l_2]$ where $a \in \mathbb{N}$. There will, of course, be paths which do not reach v_h and to count these we must also consider the graph $[l_0, t_1, l_1 + t_2 - 1]$.

We have now split the problem of counting the number of paths in a 2-loop graph into counting the number of paths in finitely many 1-loop graphs. Furthermore, from Theorem 4.14 we know that adding $L = \mathrm{lcm}(t_1, t_2)$ to the front or end of any of these graphs will preserve the quasiperiod. Given $G = [l_0, t_1, l_1, t_2, l_2]$ and $G' = [l_0 + Lm_0, t_1, l_1 + Lm_1, t_2, l_2 +$

Lm_2] it is then possible to deduce that $q(G) = q(G')$. However, to do so rigorously requires a great deal of calculation considering $[l_0 + Lm_0, t_1, l_1, t_2, l_2]$, $[l_0, t_1, l_1 + Lm_1, t_2, l_2]$ and $[l_0, t_1, l_1, t_2, l_2 + Lm_2]$ as separate cases. Following extensive calculations, the case $d = 2$ for Conjecture 4.12 then follows. We omit these technical details in this sketch. $\square$

Informally we offer the following intuitive justification for the conjecture for the remaining cases. We see that L is the shortest length of path necessary to ensure that all paths not leaving a given loop, starting at a vertex within that given loop, will end at the same vertex within the loop. We also note that any path originating from a non-loop vertex or leaving a loop remains fixed since the edges are directed on the graph and all cycles are non-intersecting. This remains of course, purely an informal justification.

4.3 Forming Partitions

There are enough cases above and sufficient experimental evidence to justify investigating the ramifications of Conjecture 4.12. The results in this section are only proven for graph families $\mathcal{G}$ belonging to a proven case of Conjecture 4.12, although we are yet to find a counter example.

Definition 4.16. We define the *rank* of the signature to be the number of terms in the shortest recurring subsequence, and denote the rank of a signature by $\Lambda(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(r))$.

Employing Conjecture 4.12 in combination with the previous definition establishes the following corollary.

Proposition 4.17. *For a graph family* $\mathcal{G} = [l_0, t_1, l_1, t_2, \dots, t_d, l_d]$*, we have* $\Lambda(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(r))$ *divides* $L = \operatorname{lcm}(\zeta_1, \zeta_2, \dots, \zeta_d)$*, for all* $0 \le r \le d$.

Proof. Assume that $\Lambda(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(r)) = s \nmid L$. Then there does not exist a positive integer s' such that $ss' = L$, which contradicts the result of Conjecture 4.12. Therefore $\Lambda(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(r))$ divides L as required. $\square$

Example 4.18. For the graph families considered in examples 4.9 and 4.10, we have that $\Lambda(\mathcal{G}, G_{\hat{\eta}}^{\hat{\zeta}}(0)) = 2$ and $\Lambda(\mathcal{G}, \hat{G}_{\hat{\eta}}^{\hat{\zeta}}(0)) = 3$. Therefore, despite $G_{\hat{\eta}}^{\hat{\zeta}}(0)$ and $\hat{G}_{\hat{\eta}}^{\hat{\zeta}}(0)$ both being subfamilies of $\mathcal{G}$, their corresponding ranks are not equal; that is $\Lambda(\mathcal{G}_1, L_0) \neq \Lambda(\mathcal{G}_2, L_0)$. However, they both divide $6 = \operatorname{lcm}(2, 3)$, as proved in Proposition 4.17.

It will be useful to establish notation for the ideas presented in Conjecture 4.12 and Proposition 4.17. We introduce the following definition.

Definition 4.19. For any graph $G = [l_0, t_0, l_1, \dots, t_d, l_d]$, we define the graph G *modulo* L as $\bar{G} = [l_0 \mod L, t_1, l_1 \mod L, \dots, t_d, l_d \mod L]$, where $L = \operatorname{lcm}(t_1, \dots, t_k)$.

Using this notation, we can restate Conjecture 4.12 as the following corollary for certain cases.

Corollary 4.20. *In the proven cases of Conjecture 4.12, for any $G \in \mathcal{G}$, we have that $q(G) = q(\bar{G})$.*

Proof. Let $G = [l_0 + Lm_0, t_1, l_1 + Lm_1, t_2, \ldots, t_d, l_d + Lm_d]$, for some $m_i \in \mathbb{N}$ and $L = \operatorname{lcm}(t_1, t_2, \ldots, t_d)$. Then $\bar{G} = [l_0, t_1, l_1, t_2, \ldots, t_d, l_d]$ and by Conjecture 4.12 we see that $q(G) = q(\bar{G})$ as required. □

Example 4.21. Let $G = [7, 2, 12, 3, 9]$. Then $L = \operatorname{lcm}(2, 3) = 6$ and we see that $\bar{G} = [1, 2, 0, 3, 3]$. Hence, by Corollary 4.20, these two graphs will have the same quasiperiod.

Remark 4.22. The previous example shows that Corollary 4.20 can greatly simplify the task of calculating $q(G)$.

Definition 4.23. Let $\mathcal{G}$ be a given graph family. We define $\bar{\mathcal{G}}$ as the set of graphs, $\bar{\mathcal{G}} = \{\bar{G} \mid G \in \mathcal{G}\}$.

Proposition 4.24. *The set $\bar{\mathcal{G}}$ is a finite subset of the family of graphs $\mathcal{G}$, which is an infinite set of graphs. Furthermore, $|\bar{\mathcal{G}}| = L^{d+1}$.*

Proof. From the definition of $\bar{G}$, we can also express $\bar{\mathcal{G}}$ as

$$\bar{\mathcal{G}} = \{[l_0, t_1, l_1, \ldots, t_d, l_d] \mid 0 \leq l_i \leq L - 1 \text{ for all } 0 \leq i \leq d\}$$

where t_i are fixed for all i. The result follows. □

We see that $\bar{G}$ is uniquely defined for each $G \in \mathcal{G}$ and thus we form a partition $\mathcal{P}$ by considering the equivalence relation $G \sim H$ if and only if $\bar{G} = \bar{H}$.

Theorem 4.25 (The Residue Classification)**.** *We can classify the minimal quasiperiod of every $G \in \mathcal{G}$ by classifying the minimal quasiperiod of every $\bar{G} \in \bar{\mathcal{G}}$. In other words, we can categorise the growth of every $G \in \mathcal{G}$ by catergorising the growth of every $\bar{G} \in \bar{\mathcal{G}}$.*

Proof. We know that the equivalence classes $[\bar{G}_i]$ form a partition over $\mathcal{G}$. Using the properties of a partition, we see that the following two statements are true

$$[\bar{G}_i] \cap [\bar{G}_j] = \emptyset \text{ for any } i \neq j \qquad\qquad G = \bigsqcup_{i=1}^{L^{d+1}} [\bar{G}_i]$$

Therefore every $G \in \mathcal{G}$ is contained in a unique $[\bar{G}_i]$. By Corollary 4.20 we see that $q(G) = q(\bar{G}_i)$ for all $G \in [\bar{G}_i]$.

Hence by calculating $q(\bar{G}_i)$ we know the quasiperiod of every graph in this class $[\bar{G}_i]$. Repeating this process for all $1 \leq i \leq L^{d+1}$, we see that we can understand the growth of any graph $G \in \mathcal{G}$ just by considering the growth of the graphs contained in $\bar{\mathcal{G}}$, which is a finite subset. $\square$

In essence, this theorem allows us to analyse the growth of an infinite family of graphs by considering a finite subset of the family members.

Remark 4.26. The partition $\mathcal{P}$ does not partition $\mathcal{G}$ by quasiperiod in general. More precisely, it is possible that $q(\bar{G}_i) = q(\bar{G}_j)$ for $i \neq j$. However, the Residue Classification does provide an upper bound for the number of cases we must consider to fully classify the growth of all $G \in \mathcal{G}$.

Example 4.27. Consider the graph family with a single loop of length 2. Then it follows that $\mathcal{G} = \{[l_0, 2, l_1] \mid l_0, l_1 \in \mathbb{N}\}$ and $\bar{\mathcal{G}} = \{[l_0, 2, l_1] \mid 0 \leq l_i \leq 1\}$. Let us calculate the quasiperiod of all $\bar{G} \in \bar{\mathcal{G}}$.

$\bar{G}$	$q(\bar{G})$
[0,2,0]	1
[1,2,0]	1
[0,2,1]	1
[1,2,1]	2

Furthermore, by using the Residue Classification we can use the table to determine the quasiperiod of any graph in the family $\mathcal{G} = \{[l_0, 2, l_1] \mid l_0, l_1 \in \mathbb{N}\}$.

We can coarsen our partition $\mathcal{P}$ so that each part contains all graphs with the same quasiperiod.

Definition 4.28. Let $\mathcal{G}$ be a given graph family. Define $\mathcal{Q}_N = \{G \in \mathcal{G} \mid q(G) = N\}$ and $\bar{\mathcal{Q}}_N = \{\bar{G} \in \bar{\mathcal{G}} \mid q(\bar{G}) = N\}$.

Proposition 4.29. *The partition $\mathcal{P}$ can be coarsened to be a partition over $\mathcal{G}$ on the quasiperiods of G, denoted by $\mathcal{Q}$.*

Proof. Recall that $\mathcal{P} = \{[\bar{G}_1], [\bar{G}_2], \ldots [\bar{G}_{L^{d+1}}]\}$. Now group together all $[\bar{G}_i]$ sharing the same quasiperiod. More formally let

$$\begin{aligned}
\bar{\mathcal{Q}}_{N_1} &= \{[\bar{G}] \mid q(\bar{G}) = N_1\} \\
\bar{\mathcal{Q}}_{N_2} &= \{[\bar{G}] \mid q(\bar{G}) = N_2\} \\
&\vdots \\
\bar{\mathcal{Q}}_{N_r} &= \{[\bar{G}] \mid q(\bar{G}) = N_r\}
\end{aligned}$$

where $N_1, N_2, \ldots, N_r$ are the quasiperiods that at least one $\bar{G} \in \mathcal{G}$ assumes - this ensures that $\bar{\mathcal{Q}}_{N_j} \neq \emptyset$ for any j. By construction we see that each $\bar{\mathcal{Q}}_{N_j}$ is nonempty. These sets are also mutually disjoint and their union covers $\mathcal{G}$. Hence we see that $\mathcal{Q} = \{\mathcal{Q}_{N_1}, \mathcal{Q}_{N_2}, \ldots, \mathcal{Q}_{N_r}\}$ is a partition over $\mathcal{G}$ on the quasiperiods of G. □

Proposition 4.30. *Let $\mathcal{G}$ be a given graph family. Then $|\mathcal{Q}| \leq$ the number of divisors of L.*

Proof. From the properties of cyclotomic polynomials explored in Chapter 3, we see that $q(G)$ divides L. □

Remark 4.31. The aim of this section was to show that for an infinite graph family $\mathcal{G} = [l_0, t_1, l_1, t_2, \ldots, t_d, l_d]$ satisfying Conjecture 4.12, we can fully understand the properties and growth of any member by understanding the behaviour of all $\bar{G} \in \bar{\mathcal{G}}$, a finite subset of graphs. Therefore we can understand the behaviour of infinitely many graphs by understanding the behaviour of a known finite subset.

Chapter 5

Applications of Growth

In this chapter we aim to illustrate some of the applications of generating functions, recurrence relations and the graph theoretic material we covered in the previous chapters. The applications in the separate sections will be shown to be interlinked in a fundamental way.

5.1 Binary Strings [13]

5.1.1 Notation and Preliminary Results

Generating functions have many useful applications in algebraic coding and, in particular, binary string decompositions, which underpin the theory of modern cryptography. We will show that such functions can be used to count the number of strings satisfying a fixed condition as we vary n, the length of the string. Before we do this, we will first define a few basic concepts which will also be used in later sections of this chapter.

Definition 5.1. An *alphabet* $\Sigma = s_1, s_2, s_3, \ldots, s_r$ is a set of elements from which we draw the letters of our word. Informally they are the symbols that make up the word.

Definition 5.2. A *word* $w_n = (g_1, g_2, g_3, \ldots, g_n)$ is an ordered n-tuple with all $g_i \in \Sigma$. In this sense we see $w_n \in \Sigma^n$.

Definition 5.3. For a fixed $n \in \mathbb{N}$, the *descendant word space* is the set of all distinct words of length n drawn from Σ and is denoted by Σ^n.

Definition 5.4. The *parent word space* is the set of all distinct words of any length drawn from Σ and is denoted by Σ^*.

Definition 5.5. The *empty word* ε is the unique word of length zero.

Definition 5.6. A *d-block* is a subword of length d consisting of d copies of the same letter.

In this section we will focus on particular types of words called *binary strings* but we will return to words in more generality in the next section. For binary strings, we define $\Sigma = \{0, 1\}$. Note that Σ^* is an infinite space but $|\Sigma^n| = 2^n$ for any $n \in \mathbb{N}$.

Definition 5.7. Let us consider the growth function $a_P(n) : \mathbb{N} \to \mathbb{N}$ to be the number of strings of length n that are contained in Σ^n and governed by some known underlying principle P. We will denote the generating function for all strings in a given subset $\Omega \subseteq \Sigma^*$ subject to a condition P by $F_{\Omega_P}(x)$. From this we define the parent word space using the following generating function

$$F_{\Sigma_P^*}(x) = \sum_{n=0}^{\infty} a_P(n) x^n$$

Now that we have defined these objects called words, we will define operations on them to give Σ^n algebraic properties and some form of mathematical structure.

Definition 5.8. For $a \in \Sigma^{d_1}$ and $b \in \Sigma^{d_2}$ with $a = (a_1, a_2, \ldots, a_{d_1})$ and $b = (b_1, b_2, \ldots, b_{d_2})$, we define the concatenation of a by b as

$$ab = (a_1, a_2, \ldots, a_{d_1}, b_1, b_2, \ldots, b_{d_2}) \in \Sigma^{d_1+d_2}$$

Definition 5.9. If $A, B \in \Sigma^*$ then we define the concatenation of A by B as $AB = \{ab \mid a \in A, b \in B\}$. Informally it is the set of all words resulting from appending elements in B to elements in A.

Example 5.10. Let $A = \{1, 101\}$ and $B = \{1, 011, 100\}$ then

$$AB = \{11, 1011, 1100, 101011, 101100\}$$

We see that the string 1011 is not created uniquely from A and B, for example $1011 = (1)(011) = (101)(1)$. This motivates the definition for uniqueness.

Definition 5.11. We say a string in AB is *created uniquely* from A and B if and only if it is the concatenation of a unique $a \in A$ and a unique $b \in B$.

The notions of the parent word space and the descendent word space extend to subsets of a given alphabet since they are, by definition, also alphabets. We can use the concatenation operation to define both of these spaces more formally.

Definition 5.12. The parent word space of $A \subseteq \Sigma$ is denoted by A^* and defined formally as

$$A^* = \varepsilon \cup A \cup AA \cup AAA \cup \ldots = \bigcup_{n=0}^{\infty} A^n$$

For the descendent word space, we consider a finite union up to some $d \in \mathbb{N}$. Finally we introduce two key lemmas that will be built upon in the following sections.

Lemma 5.13 (Yip [13]). *If elements in AB are created uniquely from A and B, then $F_{AB}(x) = F_A(x)F_B(x)$.*

Lemma 5.14 (Yip [13]). *The generating function for A^* is $F_{A^*}(x) = \dfrac{1}{1-F_A(x)}$.*

These lemmas will be used frequently and often implicitly throughout the remainder of this section.

5.1.2 The Block Decomposition

Now we have defined some core concepts, we move on to finding explicit formulae for these generating functions. Therefore, it would be of use to first find a way of expressing Σ^* in terms of its disjoint subsets such that every $\gamma \in \Sigma^*$ is created uniquely from the concatenation of those subsets. We start by observing that for $\Sigma = \{0, 1\}$

$$F_{\Sigma^*}(x) = \frac{1}{1-F_\Sigma(x)} = \frac{1}{1-2x} = \sum_{i=0}^{\infty} 2^i x^i$$

Remark 5.15. It is clear from the form of the generating function that $|\Sigma^n| = 2^n$ for any $n \in \mathbb{N}$, thus reaffirming our earlier assertion.

It is obvious that $\{0, 1\}^*$ determines uniquely every string in Σ^n but there is no way of discerning structural properties of these strings using this decomposition. A natural question to consider at this point is whether there are other ways to represent every string. There are in fact several different ways to represent every string but let us consider one decomposition in detail. This decomposition is called the *Block Decomposition*.

Theorem 5.16 (Block Decomposition [13]). $\{0, 1\}^* = \{0\}^*(\{1\}\{1\}^*\{0\}\{0\}^*)^*\{1\}^*$ *gives unique representation of all strings $\gamma \in \Sigma^*$.*

Proof. Every string $\gamma \in \Sigma^*$ has the form $\rho\sigma\tau$ where $\rho \in \{0\}^*$ and $\tau \in \{1\}^*$. The substrings ρ and τ are unique and disjoint by construction. Let $a_j = 1r_{j_1}$ and $b_j = 0r_{j_2}$ with $r_{j_1} \in \{1\}^*$ and $r_{j_2} \in \{0\}^*$. If σ is empty then we rewrite $\rho\sigma\tau$ as $\rho\tau$ and if σ is non-empty we see that we can express σ as

$$\sigma = \sigma_1\sigma_2\sigma_3\sigma_4 \ldots \sigma_{2d-1}\sigma_{2d} \text{ where } \sigma_i = \begin{cases} a_{\frac{i+1}{2}}, & \text{if } i \text{ is odd} \\ b_{\frac{i}{2}}, & \text{if } i \text{ is even} \end{cases}$$

We see that every σ_i is a non-empty substring alternating between 1's and 0's. We know that since 1 is not an element of $\{0\}^*$ and 0 is not an element of $\{1\}^*$ it follows that for all ρ, σ and τ in their respective subsets, $\rho \neq \sigma$ and $\tau \neq \sigma$. So σ is generated independently of ρ and τ. So $\gamma = \rho\sigma\tau$ must be uniquely generated by concatenation of the subsets given. Hence $\{0,1\}^* = \{0\}^*(\{1\}\{1\}^*\{0\}\{0\}^*)^*\{1\}^*$ gives unique representation of all strings $\gamma \in \Sigma^*$. We observe that by symmetry the following is also true: $\{0,1\}^* = \{1\}^*(\{0\}\{0\}^*\{1\}\{1\}^*)^*\{0\}^*$. □

Informally every γ has the form $\rho\sigma\tau$ where ρ is a block of 0's and τ is a block of 1's, both of which can be empty. The substring σ is either empty or consists of alternating non-empty blocks of 1's and 0's. [13]

Example 5.17. We illustrate the block decomposition for $\gamma = 0010110$. We have $\gamma = (00)(1)(\varepsilon)(0)(\varepsilon)(1)(1)(0)(\varepsilon)(\varepsilon) = \rho\sigma\tau$ where $\rho = 00$, $\sigma = (1\varepsilon)(0\varepsilon)(11)(0\varepsilon)$ and $\tau = \varepsilon$.

Using this decomposition, we can count the number of strings that do not contain *exactly* 3 consecutive identical letters.

Example 5.18. Let Q_3 be the property that no block of 1's or 0's has length exactly 3. These are all strings of the form

$$\{\varepsilon, 0, 00, 0000, \ldots\}(\{1, 11, 1111, \ldots\}\{0, 00, 0000, \ldots\})^*\{\varepsilon, 1, 11, 1111, \ldots\}$$

Let $F_A(x)$ be the generating function for $A = \{\varepsilon, 0, 00, 0000, \ldots\}$, $F_B(x)$ be the generating function for $B = \{1, 11, 1111, \ldots\}$, $F_C(x)$ be the generating function for $C = \{0, 00, 0000, \ldots\}$ and $F_D(x)$ be the generating function for $D = \{\varepsilon, 1, 11, 1111, \ldots\}$.

Using our definition of generating functions we have $F_A(x) = F_D(x) = 1 + x + x^2 + x^4 + \ldots$ and we also have $F_B(x) = F_C(x) = x + x^2 + x^4 + \ldots$. We see $F_{BC}(x) = (x + x^2 + x^4 + \ldots)^2$ and it follows that $F^*_{(BC)}(x) = \frac{1}{1-(x+x^2+x^4+\ldots)^2}$. Hence, by Lemma 5.14, we deduce that

$$\begin{aligned} F_{\Sigma^*_{Q_3}}(x) = F_A(x)F_{(BC)^*}(x)F_D(x) &= \frac{(1 + x + x^2 + x^4 + \ldots)^2}{1 - (x + x^2 + x^4 + \ldots)^2} \\ = \frac{(1 + x + x^2 + \frac{x^4}{1-x})^2}{1 - (x + x^2 + \frac{x^4}{1-x})^2} &= \frac{x^8 - 2x^7 + x^6 + 2x^4 - 2x^3 + 1}{-x^8 + 2x^7 - x^6 - 2x^5 + 2x^4 - 2x + 1} \end{aligned}$$

Although this is a closed formula for the generating function, it becomes problematic to extract the coefficient of a particular x^n in the current form. Regarding the generating function as a formal power series, it follows from routine manipulations, using the properties of the infinite geometric series and the binomial theorem, that the following equation holds.

$$F_{\Sigma^*_{Q_3}}(x) = (x^8 - 2x^7 + x^6 + 2x^4 - 2x^3 + 1)\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}(j+1)x^{2i+j}(1+x+x^3+\ldots)^{2i}$$

We now have a closed form and a power series for the generating function. In the example below, we show that both give the same results by using $F_{\Sigma^*_{Q_3}}(x)$ to calculate the number of strings of length 3 satisfying Q_3.

Example 5.19. Consider the ordered pairs $(0,0)$,$(0,1)$,$(0,2)$,$(0,3)$,$(1,0)$,$(1,1)$ and $(1,2)$. These are all of the form (i,j). We see that substituting these pairs into $F_{\Sigma^*_{Q_3}}(x)$ gives 6 strings of length 3 satisfying Q_3. We can verify this is the correct result because we know there are $2^3 = 8$ binary strings of length 3, and only 000 and 111 violate Q_3 leaving 6 strings satisfying the condition. Additionally, using the method of *Maclaurin Evaluation* mentioned in Chapter 2, we see that the number of strings of length 3 is

$$\frac{1}{3!}F'''_{\Sigma^*_{Q_3}}(0) = \frac{(-12)(-3)}{3!} = 6$$

Our final aim is to generalise the previous result to find a generating function for strings that do not contain blocks of length exactly d.

Proposition 5.20. *The generating function for condition Q_d over all binary strings is*

$$F_{\Sigma^*_{Q_d}}(x) = \Psi(x)\sum_{j=0}^{\infty}\sum_{i=0}^{\infty}(j+1)x^{2i+j}(1+x+\ldots+x^{d-2}+x^d+\ldots)^{2i}$$

where $\Psi(x) = x^{2d+2} - 2x^{2d+1} + x^{2d} + 2x^{d+1} - 2x^d + 1$ is a fixed polynomial over $\mathbb{N}$ for a fixed $d \in \mathbb{N}$.

Proof. Fix $d \geq 1$ and let Q_d be the property that no block of 0's or 1's has length exactly d. Using the block decomposition, we decompose the string into four pieces. Let $A = \{0\}^* \setminus \{0^d\}$, $B = \{1\}^* \setminus \{\varepsilon, 1^d\}$, $C = \{0\}^* \setminus \{\varepsilon, 0^d\}$ and $D = \{1\}^* \setminus \{1^d\}$. We see that the strings satisfying Q_d are all strings of the form

$$A(BC)^*D$$

We proceed by letting $F_A(x), F_B(x), F_C(x)$ and $F_D(x)$ be the generating functions for A, B, C and D respectively. We note the following identities; $B = D\setminus\{\varepsilon\}$ and $C = A\setminus\{\varepsilon\}$, which make the computation of the generating functions easier. We see that $F_A(x) = F_D(x) = 1+x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots$ and $F_B(x) = F_C(x) = x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots$

and so using the same manipulation as in Example 5.18, we see that

$$F_{\Sigma^*_{Q_d}}(x) = F_A(x)F_{(BC)^*}(x)F_D(x) = \frac{(1+x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots)^2}{1-(x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots)^2}$$

Expanding this expression yields the generating function

$$F_{\Sigma^*_{Q_d}}(x) = \frac{x^{2d+2}-2x^{2d+1}+x^{2d}+2x^{d+1}-2x^d+1}{-x^{2d+2}+2x^{2d+1}-x^{2d}-2x^{d+2}+2x^{d+1}-2x+1}$$

We again use properties of the infinite geometric series to manipulate $F_{\Sigma^*_{Q_d}}(x)$ as a formal power series. The manipulation begins as follows

$$\begin{aligned}
F_{(BC)^*} &= \frac{1}{1-(x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots)^2} \\
&= \sum_{i=0}^{\infty}(x+x^2+\ldots+x^{d-1}+x^{d+1}+\ldots)^{2i} \\
&= \sum_{i=0}^{\infty}x^{2i}(1+x+\ldots+x^{d-2}+x^d+\ldots)^{2i}
\end{aligned}$$

Now we will manipulate $F_A(x)F_D(x)$ by rewriting $x^{d+1}+x^{d+2}+\ldots$ as an infinite geometric series in closed form

$$\begin{aligned}
F_A(x)F_D(x) &= (1+x+\ldots+x^{d-1}+x^{d+1}+\ldots)^2 \\
&= (1+x+\ldots+x^{d-1}+\frac{x^{d+1}}{1-x})^2 \\
&= \frac{(1-x^d+x^{d+1})^2}{(1-x)^2}
\end{aligned}$$

Combining our results yields

$$F_{\Sigma^*_{Q_d}}(x) = \frac{(1-x^d+x^{d+1})^2}{(1-x)^2}\sum_{i=0}^{\infty}x^{2i}(1+x+\ldots+x^{d-2}+x^d+\ldots)^{2i}$$

Expanding the numerator, expressing the denominator as an infinite sum indexed by $j \in \mathbb{N}$ and observing that $\binom{j+1}{j} = j+1$ for all j gives

$$F_{\Sigma^*_{Q_d}}(x) = \Psi(x)\sum_{j=0}^{\infty}\sum_{i=0}^{\infty}(j+1)x^{2i+j}(1+x+\ldots+x^{d-2}+x^d+\ldots)^{2i}$$

where $\Psi(x) = x^{2d+2}-2x^{2d+1}+x^{2d}+2x^{d+1}-2x^d+1$ as required. $\square$

We see that the number of strings subject to Q_d grows exponentially in n. This makes the property Q_d of some use in cyptography. In the next section we consider abstract algebra and explore a link between binary strings, so called *finitely presented monomial algebras* and the graph theoretic results from the previous chapters.

5.2 Abstract Algebra

5.2.1 Finitely Presented Monomial Algebras

The purpose of this section is to demonstrate the fundamental way in which we can apply the results of growth, obtained from the graph theoretic context in the previous chapters, to the growth of the dimension of a finitely presented monomial algebra. We begin by considering some basic definitions to motivate the material.

Definition 5.21. The *free algebra* $F = k\langle x_1, x_2, ..., x_d\rangle$ is a non-commutative polynomial ring over a field k consisting of elements of the form

$$\sum_i a_i x_1^{\alpha_{1_i}} \dots x_s^{\alpha_{d_i}}$$

where all $a_i \in k$ and all but finitely many are zero.

A free algebra can be notionally considered a non commutative analogue of the polynomial ring. In particular we have $x_i x_j \neq x_j x_i$ for $i \neq j$ for any x_i, x_j in a free algebra. Recalling the definition from the previous section, we define ab to be the concatenation of a by b for any $a, b \in F$.

Definition 5.22. For $I \triangleleft F$ we say that I is *finitely generated* as an ideal if it is generated by finitely many elements $f \in F$. More formally this means that any finitely generated ideal can be written in the form $I = \langle f_1(x_1, x_2, ..., x_d), \dots, f_r(x_1, x_2, ..., x_d)\rangle$ where $f_i \in F$. [3]

Definition 5.23. We say that A is a *finitely presented* algebra if it isomorphic to $\frac{F}{I}$ where F is a free algebra and I is a finitely generated ideal of F.

We illustrate this idea with an example.

Example 5.24. Let $A = k[x, y, z]$ and $F = k\langle x, y, z\rangle$ where k is a field. The ideal $I \triangleleft A$ where $I = \langle xy - yx, xz - zx, yz - zy\rangle$ is clearly a finitely generated ideal. We see $A \cong \frac{F}{I}$.

More generally, letting $A = k[x_1, x_2, \dots, x_d]$ be a commutative polynomial ring and $F = k\langle x_1, x_2, \dots, x_d\rangle$ be the associated free algebra. We can construct an onto homomorphism

$\phi : F \to A$ such that $\ker(\phi) = I$, where I is a finitely generated ideal of F. Using the first isomophism theorem for rings we see that

$$\frac{F}{I} \cong A$$

Remark 5.25. This is an important result: in full generality it says that any finitely presented algebra is isomorphic to a finitely presented free algebra in the same number of indeterminates, that is then factored by a finitely generated ideal. We consider a further particular case relating to finite presentation by introducing the following definition.

Definition 5.26. A *finitely presented monomial algebra*, denoted by $A \cong \frac{F}{I}$, is the quotient of a free algebra F, and an ideal $I \triangleleft F$ which is finitely generated by monomials.

For the remainder of this chapter we restrict our attention to finitely presented monomial algebras - henceforth referred to as FPM algebras. In this context the monomials of a free algebra F are equivalent to words formed from the alphabet $\{x_1, x_2, \dots, x_d\}$.

5.2.2 Growth of Vector Space Dimension

In this section we will make frequent reference to a precise mathematical structure associated to every FPM algebra A. For brevity we introduce the following definition.

Definition 5.27. Let $A \cong \frac{F}{I}$ where $F = k\langle x_1, x_2, ..., x_d\rangle$ and $I = \langle w_1, w_2, ..., w_r\rangle$. Define the *'associated vector space of A'* as the vector space over k that generates the elements of A up to degree n. Let this be denoted by V^n.

Consider the FPM algebra $A \cong \frac{F}{I}$, where $F = k\langle x_1, x_2, ..., x_d\rangle$ and $I = \langle w_1, w_2, ..., w_r\rangle$ with each w_i being a distinct word of length u_i. Consider the associated vector space V^n. An important point to consider is how to determine the growth function for $\dim(V^n)$ as we vary n. There exists a method for analysing this property, but first we must introduce the notion of the Ufnarovski graph.

Let $m = \max_i(u_i)$ and construct Υ, the set of all words of length m containing any w_i as a subword. Since m is finite, Υ must also be finite and can therefore be indexed by $\{1, 2, ..., s\}$ for some $s \in \mathbb{N}$, more precisely $\Upsilon = \{w'_1, w'_2, ..., w'_s\}$. Noticing that $I' = \langle w'_1, w'_2, ..., w'_s\rangle$ is a finitely generated ideal of F, we construct the FPM algebra $B \cong \frac{F}{I'}$ and let $\overline{w}$ denote an arbitrary monomial in B. From our knowledge of FPM algebras, we know the following facts:

1. For all $\overline{w} \in B$ we know $\overline{w} = 0$ if and only if w contains some $w_i \in I$ as a subword.

2. For all non-zero $\alpha_j \in k$ we know $\sum_j \alpha_j \overline{w}_j = 0$ if and only if $\overline{w} = 0$ for all j.

We can now construct the Ufnarovski graph Γ of an FPM algebra. [7]

Definition 5.28. The *Ufnarovski Graph* $\Gamma = (V, E)$ is a directed graph that represents some of the properties of the FPM algebra B - as defined in the previous material. Using the notation from this section, we define the vertices v_j of Γ to be words of length $m-1$ in F. Let v_j be connected to v_k by a directed edge if and only if there exists a non-zero $\overline{w} \in B$ such that the first $m-1$ letters of w are v_j and the last $m-1$ letters in w are v_k. In other words, v_j is connected to v_k if and only if $v_j\alpha = w = \beta v_k$ for some $\alpha, \beta \in \{x_1, x_2, ..., x_d\}$.

Non-zero words of length n in B correspond to paths of length $n-(m-1)$ in Γ. We have that $\dim(V^n)$ is equal to the number of non-zero words of length n in B. Let $v(n)$ be the function that gives the dimension of V^n and $f(n)$ be the function for the number of paths of length n in Γ. Then we have that $v(n) = f(n-(m-1))$ for all $n \geq m-1$.

Now we have defined the Ufnarovski graph of an FPM algebra, we will explore the properties of these graphs and how they relate to the properties of FPM algebras. We will see that some Ufnarovski graphs take the form $[l_0, t_1, l_1, t_2, \ldots, t_k, l_k]$, similar to the graphs we have analysed in previous chapters. Therefore we can investigate the growth of V^n by applying some of the results we have already established.

Theorem 5.29 (Ufnarovski's Theorem [7])**.** *The growth of a finite directed graph is:*

- *Exponential if and only if the graph contains distinct intersecting cycles.*
- *Polynomial of degree d if and only if the graph does not contain overlapping cycles and d is the maximal number of distinct cycles a path may intersect.*

We note that exponential and polynomial growth are as defined in Chapter 1.1. We illustrate the power of this theorem with an example.

Example 5.30. Let $F = k\langle x, y, z\rangle$ be a free algebra where k is a field and $w \in F$ are words of arbitrary length. Consider the finitely generated ideal $I = \langle x^2, y^2, z^2, yz, zy, zxy\rangle$ and construct both the FPM algebra $A \cong \frac{k\langle x,y,z\rangle}{I}$ and the associated vector space V^n. We will prove that $\dim(V^n)$ grows polynomially with degree 2.

We begin by observing that the elements of I are not all of equal length, so we construct $I' \lhd F$ as follows:

$$\begin{aligned}
&I' = \langle I_1 \cup I_2 \cup I_3\rangle \text{ where}\\
&I_1 = \{x^3, y^3, z^3\}\\
&I_2 = \{yx^2, x^2y, zx^2, x^2z, xy^2, y^2x, zy^2, y^2z, yz^2, z^2y, xz^2, z^2x\}\\
&I_3 = \{xyz, zyx, xzy, yzx, zyz, yzy, \}
\end{aligned}$$

We can now consider the FPM algebra $B \cong \frac{F}{I'}$ and observe that the only non-zero words of length 3 in B are $\{xyx, yxy, yxz, xzx, zxz\}$. Let V_1 denote the vector space of B over k. To construct the Ufnarovski graph Γ, let the vertices be the words of length 2 in B, namely $x^2, y^2, z^2, xy, yx, xz, zx, yz$ and zy. Now consider all non-zero words of length 3 in B and construct the directed edges of the graph. For example, the word xyx is non-zero in B, so there will be a directed edge from xy to yx in Γ. Similarly there will be directed edges from yx to xy, yx to xz, xz to zx and zx to xz. It can be verified that this graph does not contain distinct intersecting cycles and any path will intersect at most 2 distinct cycles.

In fact, the resulting Ufnarovski graph is precisely $\Gamma = [0, 2, 0, 2, 0]$ which we know from experimentation to have polynomial growth. Let V_1 be the associated vector space of B and we see that $\dim(V_1^n)$ grows polynomially in n using the correspondence between Γ and B. We know that A is asymptotic to B, so for sufficiently large n we can conclude that $\dim(V^n)$ grows polynomially. Furthermore, by invoking Theorem 5.29 we deduce that this quantity grows quadratically for n sufficiently large.

5.2.3 Applications of Ufnarovski Graphs

In this section we aim to link together the material from previous sections to prove some key results that build on our previous work. First we will establish an essential result in the form of Proposition 5.31.

Proposition 5.31. *The 2nd order Fibonacci Sequence $f(n) = f(n-1) + f(n-2)$ with generalised initial conditions grows exponentially in n.*

Proof. We know f will grow exponentially if $Q(x)$, the denominator of the rational generating function for f, has a root within the unit circle [7]. We know that $\varphi - 1$ is a root of Q and $|\varphi - 1| < 1$, where φ is the golden ratio. Hence f grows exponentially as required. $\square$

Proposition 5.32. *The Generalised Fibonacci Sequence of order d, denoted by $g(n)$, grows exponentially in n.*

Proof. We know that $g(n)$ is the sum of the previous d terms and $f(n)$ is the sum of the previous 2 terms. For any initial conditions, there will exist a finite $n_0 \in \mathbb{N}$ such that $g(n_0 - i) > f(n_0 - i)$ for $i = 0, 1, 2$. For all $n > n_0$ we see that $g(n)$ will grow faster than $f(n)$ because $g(n) \geq f(n)$. Proposition 5.31 establishes that f grows exponentially. Hence the result follows. $\square$

Using this result, we will illustrate the Ufnarovski correspondence by exhibiting a full example.

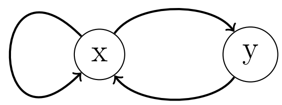


Figure 5.1: Γ_2

Example 5.33. Consider the FGM algebra $U_2 \cong \frac{k\langle x,y\rangle}{\langle y^2\rangle}$ where k is a field. We construct the Ufnarovski graph Γ_2 given above. We see that Γ_2 consists of an intersecting 1-loop and 2-loop. By Theorem 5.29, the number of paths of length n must grow exponentially in n - we verify this explicitly using the theory from the previous sections. The adjacency matrix for this graph is given by

$$A_{\Gamma_2} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

The characteristic polynomial for A_{Γ_2} is $P_{\Gamma_2}(\lambda) = \lambda^2 - \lambda - 1$. Therefore, by applying Proposition 3.13, we deduce a recurrence relation of the form $f(n+2) = f(n+1) + f(n)$, which is a generalised order 2 Fibonacci Sequence with initial conditions $f(0) = 2$ and $f(1) = 3$. By Proposition 5.31 we know that f will grow exponentially and we deduce that the number of paths of length n in Γ_2 also grows exponentially. Hence, if we consider the associated vector space of U_2 denoted as V_2, then $\dim(V_2^n)$ grows exponentially for n sufficiently large. We see that our analysis corroborates the result from Theorem 5.29.

Remark 5.34. We can relate the theory of Ufnarovski graphs to the earlier mention of binary strings. Letting x and y represent 0 and 1 respectively, we associate to every binary string in $\{0,1\}^*$ a word in $\{x,y\}^*$ which are monomials in the FPM algebra.

Example 5.35. Consider the algebra $U_3 \cong \frac{k\langle x,y\rangle}{\langle y^3\rangle}$, under the aforementioned relabelling, we see that this is equivalent to all binary strings that do not contain the substring 111. From the results obtained in the earlier section on binary strings and from Theorem 5.29, we know that the associated vector space of U_3 must grow exponentially for n sufficiently large. We verify that Γ_3, the Ufnarovski graph for U_3, does indeed contain intersecting cycles. Figure 5.2 shows Γ_3 and we see that the cycle $yx - x^2 - xy - yx$ intersects the cycle $xy - y^2 - yx - xy$.
Furthermore, if we apply the same analysis as in the previous example, we extract the recurrence relation $f(n+3) = f(n+2) + f(n+1) + f(n)$ valid for all $n \geq 3$, with initial conditions $f(0) = 4, f(1) = 7$ and $f(2) = 13$. This is a generalised Fibonacci Sequence of order 3. We can fully generalise this result.

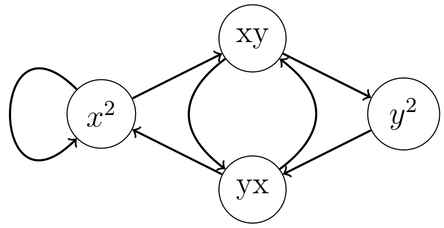


Figure 5.2: Γ_3 the Ufnarovski graph for U_3

Proposition 5.36. *Let V_d^n be the associated vector space of the FPM algebra $U_d = \frac{k\langle x,y\rangle}{\langle y^d\rangle}$ over k. Then $\dim(V_d^n)$ grows exponentially for $d \geq 2$.*

Proof. We have already proven the proposition explicitly for the case $d = 2$. Clearly there exists an onto map defined as

$$\theta : \frac{k\langle x,y\rangle}{\langle y^d\rangle} \twoheadrightarrow \frac{k\langle x,y\rangle}{\langle y^2\rangle} \qquad \theta : f + \langle y^d\rangle \longrightarrow f + \langle y^2\rangle$$

This map is well defined and we see that the image of U_d under θ is a FPM algebra that grows exponentially. Therefore we see that the growth of U_d must be both; at least exponential, and no greater than exponential. We conclude that the growth of U_d is exponential and hence, by the Ufnarovski correspondence $\dim(V_d^n)$, grows exponentially for $d \geq 2$ as required.

□

Remark 5.37. The result from Proposition 5.36 can be interpreted as showing that the number of strings satisfying property Q_d, for a fixed d, grows exponentially as we increase the length of the strings.

Definition 5.38. A *composition* of an integer n, is an ordered partition of n. [6]

Example 5.39. There are 4 compositions of $n = 3$. Explicitly we have $3 = 2 + 1 = 1 + 2 = 1 + 1 + 1$. We see that $2 + 1$ and $1 + 2$ are different compositions.

Remark 5.40. It is a known result that the n^{th} Fibonacci number is the number of integer compositions of $n+1$ into parts greater than 1, or equivalently, compositions of n into odd parts. Note that we have initial conditions $f(0) = 0$ and $f(1) = 1$. [10]

We offer a brief and informal discussion on these compositions. We note that it is unsurprising that the initial conditions for $f(n)$ in the previous examples will correspond to integer compositions of d in some way. In turn, this is fundamentally linked to binary string decompositions. The recurrence obtained in Proposition 1.13 represents the growth of the number of strings not containing d consecutive 1's as a substring; that is, satisfying Q_d. Recalling that a block is a series of consecutive letters, we see that in general terms the parts of the composition relate to the lengths of the blocks in the strings. For example, if d_1 were a part of a composition, then this would relate to a block of length d_1 in the corresponding string in some manner. Compositions are of course ordered; that is, the composition $1 + 2 \neq 2 + 1$. This is also represented in the ordered structure of words, with $011 \neq 110$. The precise nature of this relationship is not immediately obvious, but nonetheless we should not be surprised to learn that there is an observable relationship of some kind.

Using an analogy with binary strings, the examples we have considered in this section illustrate the link between recurrence relations and Ufnarovski graphs as well as the link the between Ufnarovski correspondence and FPM algebras. It is our hope that in this section we have conveyed some sense of the beauty we see in these results.

Chapter 6

Summary

To summarise our report, we now consider some of the key milestones and results obtained in the course of our experimentation and research.

We began by providing motivation for why studying growth is of significance in modern algebra with an example of the growth of dimension of vector spaces. We then moved on to an introduction of recurrence relations and generating functions in full generality.

Chapter 2 focused on recurrence relations of a particular form, and exhibited Stanley's Theorem as a key result to build upon. We explored the implications of this theorem by returning to the problem considered at the beginning of Chapter 1 and foreshadowed some material that would be considered in Chapter 5, albeit in a different context. It was in this chapter that we also established methods for manipulating difference operators - a useful tool for analysing the behaviour of quasipolynomials in later chapters.

Chapter 3 primarily provided the groundwork for Chapter 4. Using the Cayley-Hamilton Theorem, we derived results concerning the basic properties of $\mathcal{G}$. Establishing a generalised method to extract the recurrence relation and generating function for a given f from the associated graph was also a key focus. The theory of quasipolynomials was introduced, along with the notion of cyclotomic polynomials, which facilitated the analysis of some of the more fundamental behaviour of these graphs. In particular, our results establish properties of the minimal quasiperiod of the path counting function f, which is associated to a graph G.

Chapter 4 aimed to generalise many results from previous chapters and provide rigour to many arguments and ideas we had presented - in particular, to the notion of quasipolynomials. The concepts of signatures, graph residues and graph families were created to help our efforts in analysing the behaviour of $\mathcal{G}$. We derived the *Residue Classification* - a fundamental result proving that the behaviour of $\mathcal{G}$ can be understood by considering a finite subset $\bar{\mathcal{G}} \subset \mathcal{G}$. By constructing a partition on $\mathcal{G}$, we provided a method for fully classifying the growth of a given graph family that could be implemented in real terms.

In Chapter 5, we demonstrated some of the alternative applications of generating functions by first providing an analysis of their application in cryptography. The material of the previous chapters was fundamentally linked to abstract algebra through the Ufnarovski Correspondence, which established a connection between FPM algebras and digraphs and thus linking our work with abstract algebra. We then established some form of correspondence between binary strings satisfying a given condition Q and the growth of factor algebras of a certain form. Using this analysis, the material on recurrence relations from Chapter 2 and the material in Chapter 3, we obtained results on the growth of Fibonacci Sequences and formulated a proof for their exponential growth rate. This chapter culminated in a proposition that in some sense established, through the Ufnarovski correspondence, a connection between binary strings, the Fibonacci sequence and $\mathcal{G}$ - the family of digraphs that we have been studying. This proposition on the growth of dimension of a vector space provided a response to the problem considered at the very beginning of Chapter 1 and concludes our exploration of growth.

Throughout this project we have explored many areas of investigation. There are some results that we have gathered that lead us to make several conjectures. These results, particularly those concerning the quantification of quasiperiods, are motivated by the data we have collected and included in Appendix B. We conjecture the following, leaving them as open problems.

Conjecture 6.1. *For $G = [l_0, t_1, l_1, \dots, t_d, l_d]$ in $\mathcal{G}$, there is a function involving the l_i and t_i giving the quasiperiod of the graph. More formally there exists a function Θ such that*

$$q(G) = \Theta(l_0, t_1, l_1, \dots, t_d, l_d)$$

for any $G \in \mathcal{G}$. We anticipate this function not being a simple polynomial, nay 'simple' in any respect.

Conjecture 6.2. *For a fixed graph family $\mathcal{G}$, the number of graphs $G \in \mathcal{G}$ satisfying $q(G) = N_i$ approaches a fixed proportion as n tends to infinity. More formally, for every i we have*

$$\lim_{n \to \infty} \frac{|\mathcal{Q}_{N_i}|}{|\mathcal{G}|} = \delta_i$$

for a corresponding fixed $\delta_i \in [0, 1]$.

Conjecture 6.3 (Quasiperiod Frequency)**.** *Consider a fixed graph family $\mathcal{G} = [l_0, t_1, l_1, \dots, t_d, l_d]$.*

The different quasiperiods occur at differeing frequencies. Let $\mathcal{Q}_{\chi_i} = \{G \in \mathcal{G} \mid q(G) \in \chi_i\}$ *where*

$$\begin{aligned}
\chi_\infty &= \{1, t_1, t_2, \ldots, t_d, L\} \\
\chi_{d-1} &= \{N \mid N \text{ divides exactly } d-1 \text{ of the } t_i\} \\
&\vdots \\
\chi_0 &= \{N \mid N \text{ does not divide any } t_i\}
\end{aligned}$$

then $|\mathcal{Q}_{\chi_i}| \leq |\mathcal{Q}_{\chi_{i+1}}|$ *for all* i. *Informally quasiperiod that divide a greater number of the* t_i *occur more frequently than those quasiperiods that divide a smaller number of the* t_i.

Appendix A

DiGraph Creata

We have created a programme called Digraph Creata to help us with our analysis of digraphs. The programme is written in BBC BASIC for Windows. The features are explained below, accompanied by screenshots.

A.1 Mode 1

This mode lets you draw any digraph by first placing the nodes and then joining them up with the edges. The program generates the adjacency matrix, a table containing $f(n)$ and $\Delta f(n)$, and a plot of $f(n)$.

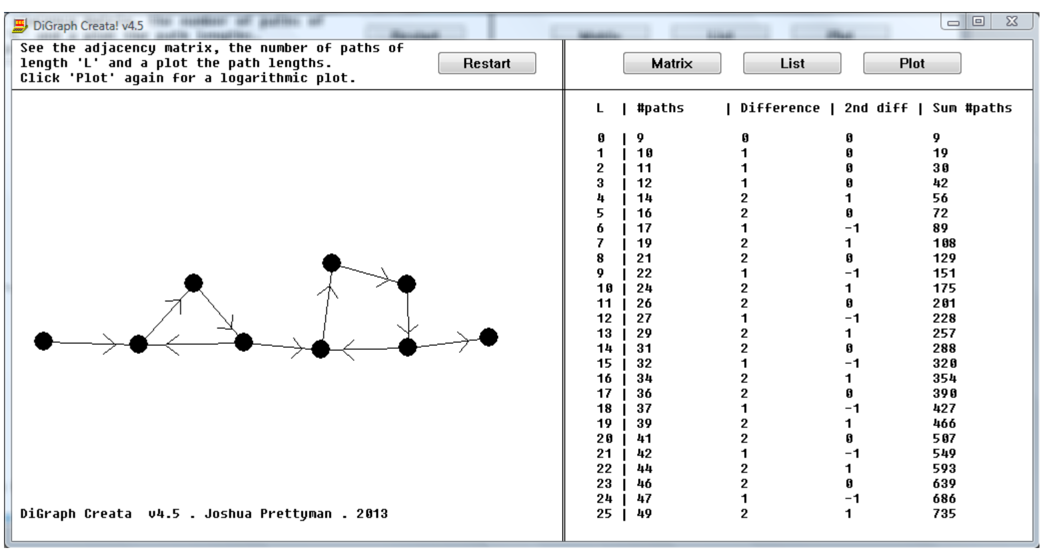


Figure A.1: Mode 1

A.2 Mode 2

Mode 2 lets you quickly analyse graphs of a certain form by inputing the structure of the graph. The graphs it can analyse are those of the form $[l_0, t_1, l_1]$, $[l_0, t_1, l_1, t_2, l_2]$ and $[l_0, t_1, l_1, t_2, l_2, t_3, l_3]$. The programme calculates the quasiperiod of $f(n)$ and its explicit form, as well as a list of $f(n)$ and $\Delta f(n)$ for n from 1 to 100, and plots of $f(n)$. The 'Properties' tab displays the quasiperiod of f and gives closed formula for $f(n)$, as shown in the figure below.

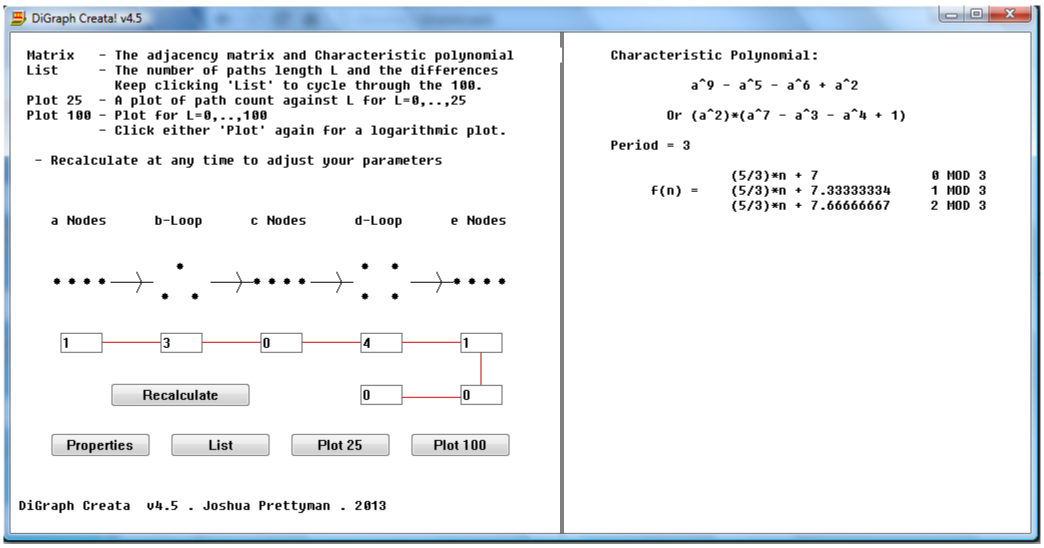


Figure A.2: Mode 2

A.3 Mode 3

Mode 3 lets you analyse the different quasiperiods of a given two loop digraph and can find graphs with a given quasiperiod. Fixing the size of the two loops, the program considers all permutations of non-loop nodes, up to a fixed number, and outputs the number of graphs found of each quasiperiod. The program also outputs the explicit form of graphs with the specified quasiperiod that it found during its search.

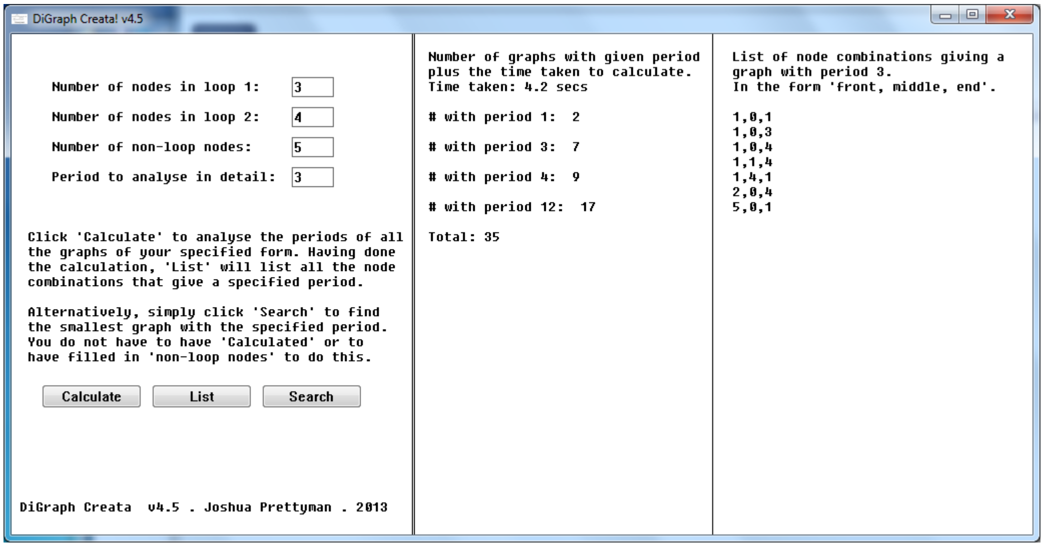


Figure A.3: Mode 3

Appendix B

Tables of Results

Table 1 shows the minimal quasiperiods of all 216 distinct $\bar{G} \in \mathcal{G} = [l_0, 2, l_1, 3, l_2]$. For example to find $q([2, 2, 1, 3, 5])$ we look in the row corresponding to $l_0 = 2$, then in the subrow $l_1 = 1$ and then in the column $l_2 = 5$ to get $q([2, 2, 1, 3, 5]) = 3$. The signatures can be easily identified using this table. Each row of quasiperiods is a signature on G_2. Each column of 6 entries within a fixed l_0 is a signature on G_1. Finally, each sequence of quasiperiods obtained by jumping 6 rows in a fixed column represents the signature on G_2. Consider the following example.

i The red highlight shows $\Omega(\mathcal{G}, [3, 2, 1, 3, l_2])$ - a signature in which l_0 and l_1 are fixed. We see $\Lambda(\mathcal{G}, [3, 2, 1, 3, l_2]) = 3$

ii The blue highlight shows $\Omega(\mathcal{G}, [1, 2, l_1, 3, 3])$ - a signature in which l_0 and l_2 are fixed. We see $\Lambda(\mathcal{G}, [1, 2, l_1, 3, 3]) = 2$

iii The green highlight shows $\Omega(\mathcal{G}, [l_0, 2, 1, 3, 4])$ - a signature in which l_1 and l_2 are fixed. We see $\Lambda(\mathcal{G}, [l_0, 2, 1, 3, 4]) = 1$

Using DiGraph Creata we have compiled Tables 2 and 3 which show the quasiperiods for graphs in the family $\mathcal{G} = [l_0, t_1, l_1, t_2, l_2]$. Here $t_1$and t_2 represent the lengths of the first and second loops respectively. The quantity E represents the maximum total number of extra vertices in a graph not contained in a loop. For example $E = 5$ means all graphs containing up to 5 extra vertices have been considered in the calculation. The corresponding entry in the table then lists the number of graphs having the quasiperiod given by the column. Again we illustrate with a few examples of ordered triples (t_1, t_2, E).

i For $(2, 5, 10)$ we see that there are 105 graphs having quasiperiod 5.

ii For $(4, 5, 20)$ we see that there are only 12 graphs of quasiperiod 3.

iii For $(3, 8, 30)$ we see that there are no graphs of quasiperiod 6.

We observe that the total number of graphs considered for a given E is fixed independently of the t_i. For example the total number of graphs in $(3, 4, 15)$ is the same as in $(2, 12, 15)$.

From this table it is quite clear that the most frequently occurring quasiperiods for a given (t_1, t_2, E) are $1, t_1, t_2$ and L. The other quasiperiods are notably rarer in every case. For example consider $(3, 4, 20)$, there are hundreds of graphs of quasiperiod $1, 3, 4$ and 12, but only 25 graphs of period 2, and a mere 15 graphs of period 6. These tables provide much evidence in support of our conjectures in Chapter 6.

Table 1

l_0	l_1	l_2					
		0	1	2	3	4	5
0	0	1	3	3	1	3	3
	1	1	3	3	1	3	3
	2	1	3	3	1	3	3
	3	1	3	3	1	3	3
	4	1	3	3	1	3	3
	5	1	3	3	1	3	3
1	0	2	1	2	1	2	1
	1	2	6	6	2	6	6
	2	2	3	6	1	6	3
	3	2	2	2	2	2	2
	4	2	3	6	1	6	3
	5	2	6	6	2	6	6
2	0	1	3	3	1	3	3
	1	1	3	3	1	3	3
	2	1	3	3	1	3	3
	3	1	3	3	1	3	3
	4	1	3	3	1	3	3
	5	1	3	3	1	3	3
3	0	2	3	6	1	6	3
	1	2	6	6	2	6	6
	2	2	3	6	1	6	3
	3	2	6	6	2	6	6
	4	2	3	6	1	6	3
	5	2	6	6	2	6	6
4	0	1	1	1	1	1	1
	1	1	3	3	1	3	3
	2	1	3	3	1	3	3
	3	1	1	1	1	1	1
	4	1	3	3	1	3	3
	5	1	3	3	1	3	3
5	0	2	3	6	1	6	3
	1	2	6	6	2	6	6
	2	2	3	6	1	6	3
	3	2	6	6	2	6	6
	4	2	3	6	1	6	3
	5	2	6	6	2	6	6

Table 2

Vertices				Number of Graphs having given Quasiperiod													Total
t_1	t_2	E		1	2	3	4	5	6	7	8	9	10	12	15	24	
4	6	5		4	0	0	3	-	4	-	-	-	-	24		-	35
4	6	10		12	6	2	18	-	38	-	-	-	-	144		-	220
4	6	15		44	14	6	57	-	120	-	-	-	-	439		-	680
4	6	20		110	35	12	143	-	291	-	-	-	-	949		-	1540
3	4	5		2	0	7	9	-	0	-	-	-	-	17		-	35
3	4	10		19	4	42	53	-	1	-	-	-	-	101		-	220
3	4	15		73	10	123	174	-	4	-	-	-	-	296		-	680
3	4	20		171	25	272	398	-	15	-	-	-	-	659		-	1540
2	3	5		9	5	14	-	-	7	-	-	-	-	-	-	-	35
2	3	10		49	35	81	-	-	55	-	-	-	-	-	-	-	220
2	3	15		162	93	266	-	-	159	-	-	-	-	-	-	-	680
2	3	20		374	235	561	-	-	370	-	-	-	-	-	-	-	1540
2	5	5		5	1	-	-	19	-	-	-	-	10	-	-	-	35
2	5	10		27	14	-	-	105	-	-	-	-	74	-	-	-	220
2	5	15		103	41	-	-	331	-	-	-	-	205	-	-	-	680
2	5	20		226	112	-	-	720	-	-	-	-	482	-	-	-	1540
2	4	5		3	3	-	29	-	-	-	-	-	-	-	-	-	35
2	4	10		24	28	-	168	-	-	-	-	-	-	-	-	-	220
2	4	15		97	77	-	506	-	-	-	-	-	-	-	-	-	680
2	4	20		211	199	-	1130	-	-	-	-	-	-	-	-	-	1540
2	6	5		3	1	2	-	-	29	-	-	-	-	-	-	-	35
2	6	10		21	12	9	-	-	178	-	-	-	-	-	-	-	220
2	6	15		81	34	17	-	-	548	-	-	-	-	-	-	-	680
2	6	20		164	99	32	-	-	1245	-	-	-	-	-	-	-	1540
2	8	5		2	0	-	2	-	-	-	31	-	-	-	-	-	35
2	8	10		25	6	-	6	-	-	-	183	-	-	-	-	-	220
2	8	15		98	17	-	15	-	-	-	550	-	-	-	-	-	680
2	8	20		177	53	-	30	-	-	-	1280	-	-	-	-	-	1540
3	6	5		1	-	2	-	-	32	-	-	-	-	-	-	-	35
3	6	10		4	-	22	-	-	194	-	-	-	-	-	-	-	220
3	6	15		21	-	70	-	-	589	-	-	-	-	-	-	-	680
3	6	20		58	-	163	-	-	1319	-	-	-	-	-	-	-	1540
3	8	5		5	0	0	2	-	0	-	7	-	-	0	-	21	35
3	8	10		17	0	9	6	-	0	-	61	-	-	0	-	127	220
3	8	15		62	0	39	12	-	0	-	185	-	-	3	-	379	680
3	8	20		140	0	92	22	-	0	-	466	-	-	7	-	813	1540
3	8	25		284	0	192	34	-	0	-	872	-	-	19	-	1524	2925
3	8	30		500	0	335	55	-	0	-	1442	-	-	33	-	2595	4960

Table 3

Vertices				Number of Graphs having given Quasiperiod													
t_1	t_2	E		1	2	3	4	5	6	7	8	9	10	12	15	24	
4	8	5		1	0	-	2	-	-	-	32	-	-	-	-	-	35
4	8	10		4	1	-	11	-	-	-	204	-	-	-	-	-	220
4	8	15		43	4	-	38	-	-	-	595	-	-	-	-	-	680
4	8	20		88	12	-	98	-	-	-	1342	-	-	-	-	-	1540
2	12	5		13	0	-	-	-	0	-	-	-	-	22		-	35
2	12	10		24	7	-	-	-	3	-	-	-	-	186		-	220
2	12	15		135	24	-	-	-	6	-	-	-	-	515		-	680
2	12	20		219	44	-	-	-	15	-	-	-	-	1262		-	1540
2	2	5		11	24	-	-	-	-	-	-	-	-	-	-	-	35
2	2	10		60	160	-	-	-	-	-	-	-	-	-	-	-	220
2	2	15		196	484	-	-	-	-	-	-	-	-	-	-	-	680
2	2	20		420	1120	-	-	-	-	-	-	-	-	-	-	-	1540
3	3	5		1	-	34	-	-	-	-	-	-	-	-	-	-	35
3	3	10		12	-	208	-	-	-	-	-	-	-	-	-	-	220
3	3	15		50	-	630	-	-	-	-	-	-	-	-	-	-	680
3	3	20		126	-	1414	-	-	-	-	-	-	-	-	-	-	1540
4	4	5		0	0	-	35	-	-	-	-	-	-	-	-	-	35
4	4	10		6	8	-	206	-	-	-	-	-	-	-	-	-	220
4	4	15		34	18	-	628	-	-	-	-	-	-	-	-	-	680
4	4	20		80	40	-	1420	-	-	-	-	-	-	-	-	-	1540
3	5	5		4	-	3	-	10	-	-	-	-	-	-	18	-	35
3	5	10		23	-	27	-	67	-	-	-	-	-	-	103	-	220
3	5	15		67	-	88	-	199	-	-	-	-	-	-	326	-	680
3	5	20		156	-	195	-	466	-	-	-	-	-	-	723	-	1540
3	9	5		1	-	0	-	-	-	-	-	34	-	-	-	-	35
3	9	10		16	-	7	-	-	-	-	-	197	-	-	-	-	220
3	9	15		38	-	30	-	-	-	-	-	612	-	-	-	-	680
3	9	20		98	-	79	-	-	-	-	-	1363	-	-	-	-	1540

Appendix C

Workshop

As part of our project, we held a workshop during Innovative Learning Week to showcase our work to our fellow students. The workshop was 2 hours long and 13 students attended. Throughout the workshop, we alternated between a presentation and carefully designed tasks to illustrate the material. The students were split up into 4 smaller groups so that each one of us could act as a tutor to each of the groups. This was very effective and it helped the students grasp the main ideas behind the project. During the second half of the workshop, the students were invited to explore properties of digraphs using a specially designed educational version of the DiGraph Creata.

C.1 DiGraph Creata - Educational Version

The following screenshots depict the 3 modes available to the students. As shown below, the home screen has a function which computes powers of matrices. This was used by the students to explore properties of adjacency matrices.

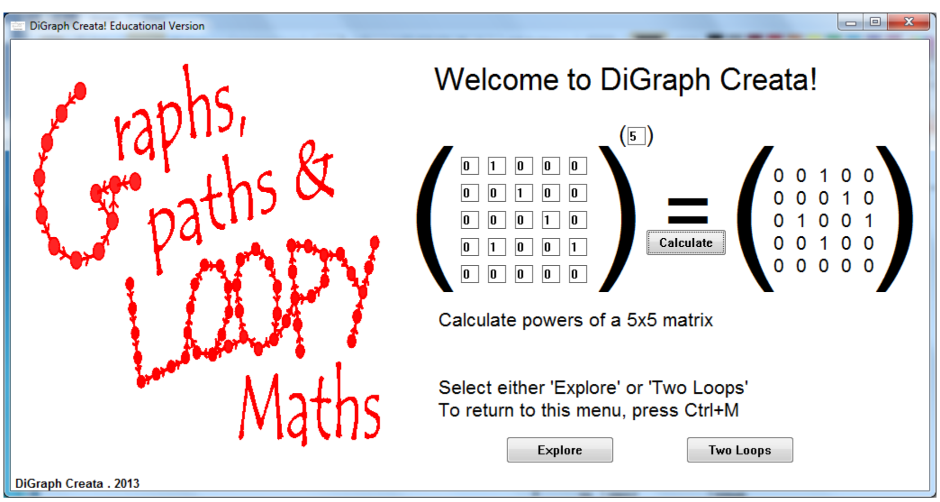


Figure C.1: Home screen

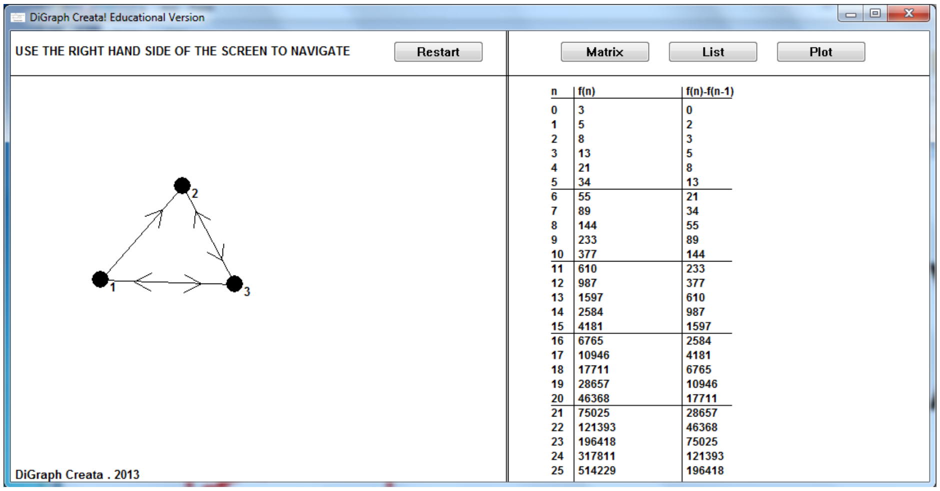


Figure C.2: Explore mode

The 'Explore' mode allowed the students to construct their own graphs and explore its properties. The programme generates the graph's corresponding adjacency matrix, a list of $f(n)$ and $\Delta f(n)$ for n up to 25 and also a plot of $f(n)$. The 'Two Loops' mode takes the vertex structure of a graph as the input and outputs the corresponding properties. This was used by the students to find the quasiperiod of given graphs.

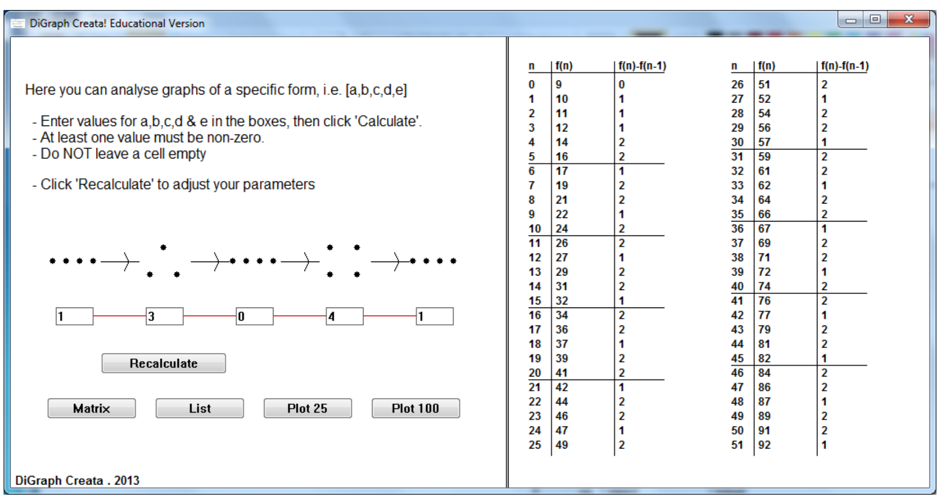


Figure C.3: Two Loops mode

C.2 Slides and Poster

For reference, we attach the workshop presentation slides and the poster used to advertise the event.

Graphs, paths and loopy maths: An introduction to abstract graph theory

Thomas Bridge, Edward Cumberlege, Harry Peaker, Joshua Prettyman

University of Edinburgh

20/02/2013

Overview

Notation

Single loop Notation

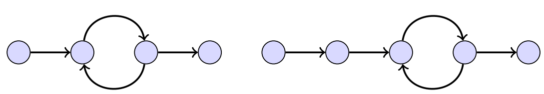


Figure: G_1= [1,2,1] (left) and G_2= [2,2,1] (right)

Double loop Notation

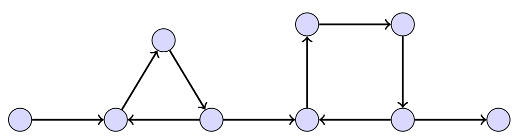


Figure: G_3=[1,3,0,4,1]

Introduction

Aim

In this workshop we will be analysing the growth of $f(n)$ for graphs containing one or two loops.

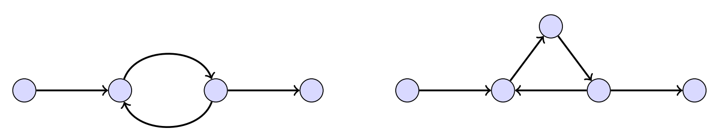


Figure: Simple 2-loop and 3-loop graphs

Task 1

Task 1

For G_1 and G_2 in the figure below, calculate $f(i)$ for $i = 0, 1, 2, 3, 4, 5$. What patterns emerge? What difference does the extra starting vertex make?

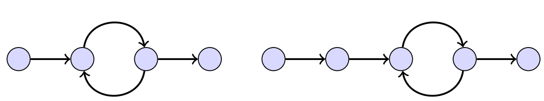


Figure: G_1= [1,2,1] (left) and G_2= [2,2,1] (right)

Task 1

Solution

For $G_1 = [1, 2, 1]$ we have

n	0	1	2	3	4	5
$f(n)$	4	4	4	5	4	5

For $G_2 = [2, 2, 1]$ we have

n	0	1	2	3	4	5
$f(n)$	5	5	5	6	6	6

Note: For G_1, $f(n)$ alternates but for G_2, $f(n)$ is constant. This shows that adding an extra vertex can change the growth of the number of paths of length n.

Adjacency Matrices

Example

The adjacency matrix for $G_1 = [1, 2, 1]$ is given by

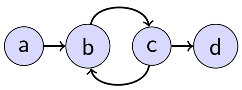


Figure: G_1= [1,2,1]

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$a_{ij} = \text{number of edges from vertex } i \text{ to vertex } j$$

Observations

Notation

Let us denote the sum of all elements of a matrix A by $\sum(A)$, i.e.

$$\sum(A) := \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij}$$

Observations

From the definition of A, it follows that $\sum(A) = f(1)$.
Can we find a link between $\sum(A)$ and $f(n)$?

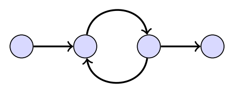


Figure: G_1= [1,2,1]

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Lemma 1

Lemma 1

Let G be a directed graph with adjacency matrix A. Consider A^n. Then

$$a_{ij}^{(n)} = \text{number of paths from vertex } i \text{ to vertex } j \text{ of length } n$$

Hence,

$$f(n) = \sum(A^n)$$

That is, the number of paths of length n is equal to the sum of the entries of A^n.

Task 2

Task 2

Recall the graph $G_2 = [2, 2, 1]$.

1. Write down the adjacency matrix A_2 for G_2. How does it differ from A_1?
2. Use the computer to calculate A_2^i for $i = 0, 1, 2, 3, 4, 5$ and check $\sum(A_2^i)$ with your answers for $f(i)$ from the previous task.
3. Draw the graph associated with the adjacency matrix A_3 below.

$$A_3 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Task 2

Solution

1. $A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

2. $A_2^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ $A_2^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

   $A_2^4 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ $A_2^5 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

Task 2

Solution

3. $G = [1, 3, 2]$

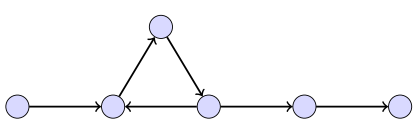


Figure: G=[1,3,2]

Recurrence Relations

Example

We saw patterns emerge in $f(n)$ for $G_1 = [1,2,1]$

n	0	1	2	3	4	5	6	7	8	9	10
$f(n)$	4	4	4	5	4	5	4	5	4	5	4

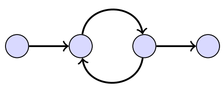


Figure: G_1= [1,2,1]

Characteristic Polynomial

Example

Recall A_1, the adjacency matrix for $G_1 = [1,2,1]$

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \lambda \mathbf{I}_4 - A_1 = \left[\begin{array}{c|cc|c} \lambda & -1 & 0 & 0 \\ \hline 0 & \lambda & -1 & 0 \\ 0 & -1 & \lambda & -1 \\ \hline 0 & 0 & 0 & \lambda \end{array}\right]$$

Since $\lambda \mathbf{I}_4 - A_1$ is almost a block diagonal matrix, the determinant is easy to compute

$$p(\lambda) = \det(\lambda \mathbf{I}_4 - A) = \lambda^2(\lambda^2 - 1)$$

Cayley-Hamilton Theorem

Theorem (Cayley-Hamilton Theorem)

Let A be an $m \times m$ matrix. Define the characteristic polynomial as $p(\lambda) = \det(\lambda \mathbf{I}_m - A)$. Then A satisfies $p(A) = 0$.

Example

Recall that for $G_1 = [1,2,1]$

$$p(\lambda) = \det(\lambda \mathbf{I}_4 - A) = \lambda^2(\lambda^2 - 1)$$

We apply the Cayley-Hamilton Theorem to get

$$A^4 - A^2 = 0$$

Continuing by induction we get

$$A^{n+2} - A^n = 0 \qquad \forall\, n \geq 2$$

Cayley-Hamilton Theorem

Example continued

$$A^{n+2} - A^n = 0 \qquad \forall\, n \geq 2$$

The equality must hold when we sum all the elements

$$\sum(A^{n+2}) - \sum(A^n) = 0 \qquad \forall\, n \geq 2$$

Finally, we apply lemma 1 to deduce a recurrence relation for $f(n)$

$$f(n+2) - f(n) = 0 \qquad \forall\, n \geq 2$$

With the following initial conditions

$$f(0) = 4, f(1) = 4, f(2) = 4, f(3) = 5$$

Task 3

Task 3

1. Apply the Cayley-Hamilton Theorem to the characteristic polynomial of the adjacency matrix corresponding to $G_2 = [2,2,1]$.
2. Deduce a recurrence relation for $f(n)$ using lemma 1: $\sum(A^n) = f(n)$
3. How does the recurrence relation compare to that for $G_1 = [1,2,1]$?

Task 3

Solution

1. $p(\lambda) = \lambda^3(\lambda^2 - 1)$
2. $$\begin{aligned} A^3(A^2 - 1) &= 0 \\ A^5 - A^3 &= 0 \\ A^{n+2} - A^n &= 0 \qquad \forall n \geq 3 \\ f(n+2) - f(n) &= 0 \qquad \forall n \geq 3 \end{aligned}$$
3. Looks to be the same recurrence relation. But the paths grow differently - must have different initial conditions.

Generating Functions

Definition
We define the *generating function* for $f(n)$ to be the function

$$F(x) = \sum_{n=0}^{\infty} f(n)x^n$$

Example
For $G_1 = [1, 2, 1]$

$$\sum_{n=0}^{\infty} f(n)x^n = 4 + 4x + 4x^2 + 5x^3 + 4x^4 + \cdots$$

Theorem 2

Theorem (Stanley)
Suppose we have a recurrence relation

$$f(n+d) + \alpha_1 f(n+d-1) + \cdots + \alpha_{d-1} f(n+1) + \alpha_d f(n) = 0$$

Then the generating function for $f(n)$ is of the form

$$F(x) = \sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}$$

where $Q(x) = 1 + \alpha_1 x + \cdots + \alpha_{d-1}x^{d-1} + \alpha_d x^d$

Example

Recall that for $G_1 = [1, 2, 1]$ we deduced the recurrence relation

$$f(n+2) - f(n) = 0 \qquad \forall\ n \geq 2$$

Then by Theorem 2, $Q(x) = 1 - x^2$. Now we can find $P(x)$, and hence $F(x)$, by solving

$$\sum_{n=0}^{\infty} f(n)x^n = 4 + 4x + 4x^2 + 5x^3 + 4x^4 + \cdots = \frac{P(x)}{1 - x^2}$$

It then follows that the generating function for G_1 is

$$F(x) = \frac{x^3 + 4(x+1)}{1 - x^2}$$

Task 4

Task 4
1. Use your results from the previous task to write down $Q(x)$ for $G_2 = [2, 2, 1]$.
2. Calculate $P(x)$ and therefore deduce $F(x)$ for the graph G_2. Is $F(x)$ in its most reduced form?
   (*Hint*: Using your previous calculations for $f(i)$, $i = 1, \ldots, 5$, solve $P(x) = Q(x) \sum f(n)x^n$).
3. Compare your answer with the generating function for G_1:

$$F(x) = \frac{x^3 + 4(x+1)}{1 - x^2}$$

Task 4

Solution
1. Same as for G_1, that is $1 - x^2$
2.
$$P(x) = (1 - x^2)(5 + 5x + 5x^2 + 6x^3 + 6x^4 + \ldots)$$
$$P(x) = x^4 + x^3 + 5(x+1)$$
$$F(x) = \frac{(x^3 + 5)(x+1)}{1 - x^2} = \frac{x^3 + 5}{1 - x}$$
3. It initially has the same denominator but the initial conditions admit a common factor in the numerator, which then cancels

Conclusion

Conclusion
The number of vertices outside of the loop effects the growth of $f(n)$.

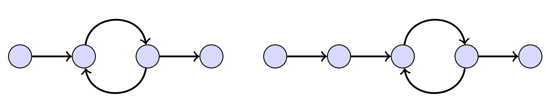


Figure: G_1= [1,2,1] (left) and G_2= [2,2,1] (right)

Introducing Quasipolynomials

Definition
A function f is *quasipolynomial* if there exists an integer $N > 0$ and polynomials $f_0, f_1, \ldots, f_{N-1}$ such that

$$f(n) = f_i(n) \text{ if } n \equiv i \mod N$$

N is called the *quasiperiod* of f.

Example
We can again consider $f(n)$ for the graph $G_1 = [1, 2, 1]$

$$f(n) = \begin{cases} 4 & \text{if } n \equiv 0 \mod 2 \\ 5 & \text{if } n \equiv 1 \mod 2 \end{cases}$$

Proposition 3

Theorem (Stanley)
f is quasipolynomial with quasiperiod N if and only if it has a generating function of the form

$$\sum_{n=0}^{\infty} f(n)x^n = \frac{P(x)}{Q(x)}$$

where every root α of $Q(x)$ satisfies $\alpha^N = 1$

Example
We saw that for $G_1 = [1, 2, 1]$ and $G_2 = [2, 2, 1]$

$$F_1(x) = \frac{x^3 + 4(x+1)}{1 - x^2} \qquad F_2(x) = \frac{x^3 + 5}{1 - x}$$

Introduction

In this section we will give you the chance to carry out your own experiments with our specially designed software.

Aim
To explore questions about the quasiperiod of a graph:

1. How do the sizes of the loops effect the quasiperiod?
2. How does adding vertices and edges outside of the loop effect the quasiperiod?
3. If we know the quasiperiod of a given graph, can we deduce the quasiperiod of another graph?

Indentifying The Quasiperiod

Example

n	$f(n)$	$\Delta f(n)$
20	40	2
21	44	4
22	47	3
23	49	2
24	53	4
25	56	3
26	58	2
27	62	4
28	65	3
29	67	2

Task 5

Find the quasiperiod for the following graphs:

1. $G_1 = [7, 2, 1, 3, 4]$
2. $G_2 = [1, 4, 2, 2, 1]$
3. $G_3 = [7, 3, 3, 4, 1]$
4. $G_4 = [4, 4, 1, 9, 1]$

Task 5

Solution

1. $G_1 = [7, 2, 1, 3, 4]$ has quasiperiod 6
2. $G_2 = [1, 4, 2, 2, 1]$ has quasiperiod 4
3. $G_3 = [7, 3, 3, 4, 1]$ has quasiperiod 6
4. $G_4 = [4, 4, 1, 9, 1]$ has quasiperiod 9

Key Results

Proposition 4

Let $G = [l_0, t_1, l_1, t_2, l_2]$. Then $Q(x) = (1 - x^{t_1})(1 - x^{t_2})$

Corollary 5

Then the quasiperiod N divides $L = \text{lcm}(t_1, t_2)$.

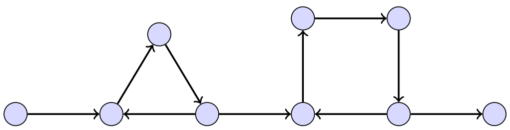


Figure: G=[1,3,0,4,1]

Task 6

1. Write down the possible quasiperiods for graphs of the form (i) $G_1 = [l_0, 3, l_1, 4, l_2]$ (ii) $G_2 = [l_0, 4, l_1, 6, l_2]$
2. Generate graphs of the form $G_1 = [l_0, 3, l_1, 4, l_2]$ & $G_2 = [l_0, 4, l_1, 6, l_2]$ and also record the quasiperiods that you find.
3. Compare your findings with the quasiperiods you predicted. Are some quasiperiods harder to find than others?
4. Can you find any patterns? Try repeatedly adding $L = \text{lcm}(t_0, t_1)$ to l_0 and see how it effects the quasiperiod. How about l_1 and l_2?

Key Results

Proposition 6

The quasiperiod of $G = [l_0, t_0, l_1, t_1, l_2]$ is equal to the quasiperiod of $G' = [l_0 + k_0 L, t_0, l_1 + k_1 L, t_1, l_2 + k_2 L]$, where $L = \text{lcm}(t_0, t_1)$ and $k_0, k_1, k_2 \in \mathbb{N}$.

Consequence

We can find out all the information about the graph just by analysing $G = [l_0, t_0, l_1, t_1, l_2]$ for all l_i such that $0 \leq l_i \leq \text{lcm}(t_0, t_1)$.

Prize Task

Prize Task

To win a prize, be the first group to find a graph of the form $[l_0, 3, l_1, 4, l_2]$ which has quasiperiod 2.

Research Questions

This workshop has covered material that our project has been exploring but there remains much more to be investigated:

1. Extra vertices added to a graph
2. Leaving the loop at different vertices

Applications

Abstract Algebra

We can apply our theory to Ufnarovski graphs, which represent the structure of factor algebras. The growth of $f(n)$ for the Ufnarovski graph represents the growth of the dimension of the factor algbra.

Growth of functions

We can apply the theory about recurrence relations and polynomial growth to more general examples:

1. Dimension of a vector space
2. Tiling a wall
3. Binary strings

Graphs, paths & LOOPY Maths

FROM GRAPH THEORY

TO ALGEBRA!

AND BACK AGAIN

How many paths are there through a graph?

Find out what a final -year project entails and discover some interesting results.

And **WIN** prizes!

Suitable for <u>all</u> maths students

INNOVATIVE LEARNING WEEK

WEDNESDAY 20th FEB 11am-1pm

Appleton Tower, Room M2

Book **NOW**: MyEd > MyStuff > Event Bookings

Bibliography

[1] M.R. Cullen, D.G. Zill; *'Advanced Engineering Mathematics', 3rd ed.,* Jones and Bartlett, Sudbury, MA, 2006, pg 332 - 338.

[2] E.L Flapan, T.K. Marks, J.E. Pommersheim; *'Number Theory: A Lively Introduction with Proofs, Applications and Stories'*, John Wiley and Sons Inc., USA, 2010, pg. 69.

[3] B. George, L.A. Herrera Flores, B. Schlomer; *'Growth of Algebras'*, presentation at Universidad Autónoma del Estado de Hidalgo, July 16th 2009.

[4] Y. Gallot; 'Cyclotomic Polynomials and Prime Numbers', Mathematics Subject Classification, 2000, rev 2001. Available online at

http://galloty.chez.com/papers/cyclotomic.pdf

[5] R. Grimaldi; *'Discrete and Combinatorial Mathematics : An Applied Introduction', 5th ed.*, Pearson, New York, 2003, pg. 488.

[6] V.E. Hoggat, Jr., and D.A. Lind; 'Compositions and Fibonacci Numbers', The Fibonacci Quarterly Volume 7, 1969, pg. 253 - 267. Available online at

http://www.fq.math.ca/Scanned/7-3/hoggatt.pdf

[7] G. Krause, T.H. Lenagan; *'Growth of Algebras and Gelfand-Kirillov Dimension' 2nd ed.*, American Mathematical Society, Providence, 2000, pg. 175.

[8] W. Imrich, N. Seifter; 'A survey on paths with polynomial growth', Discrete Mathematics Volume 95, 1991, pg. 101 - 117.

[9] A. Morris; *'Linear Algebra: an introduction'*, Chapman and Hall, London, 1982, pg. 163.

[10] A. Sills; Compositions, Partitions, and Fibonacci Numbers, The Fibonacci Quarterly Volume 40, 2011, pg. 348 - 354. Available online at

http://math.georgiasouthern.edu/~asills/comps/CompositionsFQRev.pdf

[11] C. Smyth 'The Terms in Lucas Sequences Divisible by their Indices', Journal of Integer Sequences Volume 13, 2010. Available online at
https://cs.uwaterloo.ca/journals/JIS/vol13.html

[12] R. Stanley; *'Enumerative Combinatorics Volume 1', 2nd ed.*, Cambridge University Press, New York, 2012, Chapter 4, pg. 535 - 547.

[13] M. Yip; *'Math 340 Notes'*, University of Pennsylvania, Philadelphia, 2011.