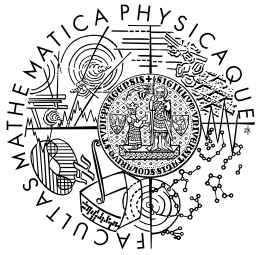

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Jan Čížek

Looking for Weak States of RC4 by Means of Waiting Tables

Department of Algebra

Supervisor of the bachelor thesis:	prof. RNDr. Aleš Drápal, CSc., DSc.
Study programme:	Mathematics
Study branch:	Mathematical Methods of Information Security

Prague 2018

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In Prague, 20th of July 2018 Jan Čížek

Title: Looking for Weak States of RC4 by Means of Waiting Tables

Author: Jan Čížek

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc.

Abstract: Waiting Tables were introduced by Drápal and Hojsík in 2006 to study weak states of the stream cipher RC4. This thesis revisits Waiting Tables and some of their most important properties. An equivalent model from graph theory, called Waiting Paths, is established in this work and the equivalence of the two models is proved. Afterwards, Waiting Matrices are defined and used for the analysis of a subclass of Waiting Paths.

Keywords: RC4, weak state, waiting table, waiting path, waiting matrix

Název práce: Hledání slabých stavů RC4 pomocí čekacích tabulek

Autor: Jan Čížek

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc.

Abstrakt: Čekací tabulky zavedli Drápal a Hojsík v roce 2006 kvůli zkoumání slabých stavů proudové šifry RC4. Tato práce se znovu vrací k čekacím tabulkám a některým jejich důležitým vlastnostem. Dále je v práci popsán ekvivalentní model z teorie grafů, tzv. čekací cesty, a je dokázána ekvivalence obou modelů. Poté jsou definovány tzv. čekací matice a ty jsou využity k analýze podtřídy čekacích cest.

Klíčová slova: RC4, slabý stav, čekací tabulka, čekací graf, čekací matice

Contents

1. Introduction

RC4 is a stream cipher designed by Ron Rivest in 1987. The cipher was kept as a trade secret until it was leaked out in 1994. It was praised by many cryptanalysts for being extremely fast and having a very simple design (e.g. [6, Introduction]). Among other works, RC4 was described and analysed in 2001 by Mantin, later the same year by Paul and Preneel and in 2006 by Hojsík [3, 6, 1].

Incorrect usage of RC4 led to development of insecure cryptographic protocols, such as WEP, a protocol aimed to secure wireless networks in 1997. A cryptanalytic attack against WEP was published in 2001 by Fluhrer, Mantin and Shamir [4]. Later the same year, an improved version of the attack was published by Stubblefield, Ioannidis and Rubin, showing the protocol is completely insecure [5].

RC4 can be described via various means; let us use an algebraic description. The inner state of RC4 is determined by a triple $(c,\, r,\, \pi)$, where $c, r \in \mathbb{Z}_N$ and $\pi \in S_N$ (here S_N is the symmetric group on the set $\{0, 1, \ldots, N-1\}$); RC4 uses $N = 256$ but other values can also be considered for theoretical purposes, even the *infinitary* variant $N = \infty$. The RC4 algorithm consists of two parts: the Key-Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA).

The first part, KSA, which is used to set up the permutation π for the following keystream generation, will not be discussed in the present work. The KSA has been, however, heavily studied since RC4 became popular. Recently, it has been analysed by Sladký, who described methods of reconstruction of the initial key from the inner state of RC4 [7]. The two attacks on WEP mentioned above also uses the analysis of KSA.

This work is motivated by the second part of RC4, PRGA. The change of an inner state $s = (c,\, r,\, \pi)$ to its successor inner state $s' = (c',\, r',\, \pi')$ is described by the following:

- $c' = \Big(c + 1\Big) \bmod N$;
- $r' = \Big(r + \pi(c')\Big) \bmod N$; and
- $\pi' = \pi \circ (c'\; r')$.

The last rule refers to a composition of the permutation π with the cycle $(c'\; r')$. The change of an inner state s to s' creates one keystream value $x \in Z_N$, determined as

$$x = \pi'\Big(\Big(\pi'(r') + \pi'(c')\Big) \bmod N\Big).$$

This thesis builds on the theory by Hojsík [1]. The theory was later revisited and reformulated into un unpublished paper by Drápal and Hojsík [2]. I have mainly followed on from the latter source, which might, however, be not easily accessible. Therefore, I am usually citing these two sources next to one another. The unpublished paper is not needed to read this thesis.

Drápal and Hojsík introduced a tabular model called Waiting Tables (originally, Hojsík used a term Table Triple) and they showed the model is equivalent to the infinitary version of RC4 (although other, "modullar" versions of RC4 were also considered). This thesis reintroduces and revisits the model, and also

a new model based on graph theory, called Waiting Paths, is introduced here. The equivalence of Waiting Paths and Waiting Tables is shown as well.

Drápal and Hojsík concentrated mainly on Injective Periodic Waiting Paths, which are also described in this work. This work focuses on a subclass of them, the so-called (Injective) Column-Periodic Waiting Tables.

The thesis contains a chapter about Waiting Tables, where they are defined and some of their essential properties are discussed. Then, a similar chapter about Waiting Paths follows. Next is the chapter where equivalence of the models is proved. The proofs are constructive and can therefore be used to create a Waiting Table from a Waiting Path and vice versa. Finally, the longest chapter is about looking for the Injective Vertex-Periodic Waiting Paths (which are equivalent to Injective Column-Periodic Waiting Tables). The searching is made via an analysis of newly introduced Injective Periodic Waiting Matrices. These matrices are, however, not an equivalent model to the previous two. Every Waiting Path (or Table) can be transformed into a Waiting Matrix, but not necessarily the other way around. But these matrices proved to be a useful tool for analyses of Waiting Paths.

2. Waiting Tables

2.1 Definition and Elementary Properties

In this chapter, we will define waiting tables and look at some of their properties. We will be especially interested in waiting tables which are both injective and infinitary.

Definition 2.1 (Waiting Table)**.** Consider integers $h \geq 0$ and $k \geq 1$. A *waiting table* of *height* h and *width* k is a triple $\mathcal{T} = (T, \rho, \mu)$ consisting of a rectangular array $T = (t_{i,j})$ of positive integers, $0 \leq i \leq h$ and $1 \leq j \leq k$, a mapping ρ from $\{1, 2, \ldots, k\}$ to $\mathbb{Z}$, and a mapping μ from $\{0, 1, \ldots, h\}$ to $\{1, 2, \ldots, k\}$, where for all $i \in \{0, 1, \ldots, h-1\}$ the following properties hold:

(T1) There exists exactly one $j \in \{1, 2, \ldots, k\}$ such that $t_{i,j} = 1$.

(T2) If $j \in \{1, 2, \ldots, k\}$ and $t_{i,j} = 1$, then $\mu(i+1) = j$ and $t_{i+1,j} = \rho(j) + t_{i,\mu(i)}$.

(T3) If $j \in \{1, 2, \ldots, k\}$ and $t_{i,j} \neq 1$, then $t_{i+1,j} = t_{i,j} - 1$.

The mapping ρ will be referred to as the *header* and the mapping μ as the *register*.

Definition 2.2 (Modular Waiting Table)**.** A *modular waiting table* is a waiting table where the rules for the header ρ and for the table values $(t_{i,j})$ in Definition 2.1 in (T1-3) are considered modulo an integer $N > 1$ called the *modulus* of the waiting table.

An equivalent model, called the *table triple*, was first introduced by Hojsík [1, Definition 19].

Lemma 2.3. *Let $\mathcal{T} = (T, \rho, \mu)$ be a waiting table of height h and width k. Let $i \in \{0, 1, \ldots, h-1\}$ and $j = \mu(i+1)$. Then $\rho(j) = t_{i+1,\mu(i+1)} - t_{i,\mu(i)}$.*

Proof. This follows directly from (T2) in Definition 2.1. □

Let $\mathcal{T}$ be a waiting table of height h and width k. By the ith *row* of $\mathcal{T}$, we will understand the k-tuple $(t_{i,1}, t_{i,2}, \ldots, t_{i,k})$, and by the jth *column* of $\mathcal{T}$, we will understand the h-tuple $(t_{0,j}, t_{1,j}, \ldots, t_{h,j})$. If further rows may be added to $\mathcal{T}$, forming thus a new waiting table $\mathcal{T}'$ of height $h' \geq h$, say that $\mathcal{T}$ is *extendable* into $\mathcal{T}'$.

Waiting table $\mathcal{T} = (T, \rho, \mu)$ of height h and width k is called

- *infinitary* if it may be extended by addition of infinitely many rows;
- *periodic* if there exists a positive integer $P \leq h$ such that $\mu(P) = \mu(0)$ and $t_{0,j} = t_{P,j}$ for all $j \in \{1, 2, \ldots, k\}$.

  The least possible value of P is called the *period* of $\mathcal{T}$;
- *periodically extendable* if it may be extended into a periodic waiting table;
- *complete* if it is periodic or if no further row may be added to it; and
- *injective* if the header ρ is an injective mapping.

–9	10	–3	5	3
1	2	[11]	4	5

Table 2.1: A waiting table which can be extended by addition of further rows. For the complete variant of this table, see Table 2.2.

–9	10	–3	5	3
1	2	[11]	4	5
[2]	1	10	3	4
1	[12]	9	2	3
[3]	11	8	1	2
2	10	7	[8]	1
1	9	6	7	[11]
[2]	8	5	6	10

Table 2.2: A waiting table which is injective but not infinitary.

3	0	–3	3	0
1	2	[3]	4	5
[6]	1	2	3	4
5	[6]	1	2	3
4	5	[3]	1	2
3	4	2	[6]	1
2	3	1	5	[6]
1	2	[3]	4	5

Table 2.3: A waiting table which is periodic (with period $P = 6$) but not injective.

4	0	8	3	5
1	2	[3]	4	5
[7]	1	2	3	4
6	[7]	1	2	3
5	6	[4]	1	2
4	5	3	[7]	1
3	4	2	6	[1]
2	3	1	5	[6]
1	2	[3]	4	5

Table 2.4: A modular waiting table (with modulus $N = 11$) that is both injective and periodic (with period $P = 7$).

Observation 2.4 (Extension of Waiting Tables)**.** *If a waiting table $\mathcal{T} = (T, \rho, \mu)$ of height h is extendable into a waiting table $\mathcal{T}'$ of height $h{+}1$, then the added $(h{+}1)$st row is uniquely determined by the hth row, by the header ρ and by the register value $\mu(h)$.*

Our main interest is in infinitary waiting tables. (Hojsík called these *persistent table triples* [1, Definition 20].) For this reason, Drápal and Hojsík added one more rule to the definition of waiting table for all $i \in \{0, 1, \ldots, h{-}1\}$:

(T4) If $j_1, j_2 \in \{1, 2, \ldots, k\}$ and $t_{i,j_1} = t_{i,j_2}$, then $j_1 = j_2$ [2].

Every periodically-extendable waiting table is infinitary. The converse is also true, which has been proved by Hojsík [1, Proposition 30], or by Drápal and Hojsík [2, Corollary 1.5]:

Claim 2.5. *A waiting table is infinitary if and only if it is periodically extendable.*

Examples of waiting tables are in Tables 2.1 to 2.4. The mapping ρ is indicated by the header of the table. The register value $\mu(i)$ is for each i expressed by a frame around $t_{i,\mu(i)}$. The same graphical representation was used by Drápal and Hojsík [1, 2].

Observation 2.6. *Let $\mathcal{T} = (T, \rho, \mu)$ be a periodic waiting table of height h and width k, with period P. Then the following is true for all $i_1, i_2 \in \{0, 1, \ldots, h\}$ and $j \in \{1, 2, \ldots, k\}$:*

$$t_{i_1,j} = t_{i_2,j} \text{ whenever } i_1 \equiv i_2 \pmod{P}; \text{ and}$$
$$\mu(i_1) = \mu(i_2) \text{ whenever } i_1 \equiv i_2 \pmod{P}.$$

Definition 2.7 (P–table)**.** Consider a positive integer $P > 1$. A periodic waiting table of height P and width k, with period P, is called a *P–table* (of width k).

2.2 Column-Periodic Waiting Tables

In periodic waiting tables, the values repeat periodically in each column (and the period of each value in each column divides the period P of the waiting table). However, in a given column, different values may have different periods. We will now look at a special class of periodic waiting tables, where in each column, all values repeat with the same period.

Definition 2.8 (Column-Periodic Waiting Table)**.** Let $\mathcal{T} = (T, \rho, \mu)$ be a periodic waiting table of height h and width k. Call $\mathcal{T}$ *column-periodic* if for all $j \in \{1, 2, \ldots, k\}$ there exists an integer $p = p(j) > 0$ such that if $j = \mu(i_1)$ and $i_2 \in \{0, 1, \ldots, h\}$, then

$$\mu(i_1) = \mu(i_2) \iff i_1 \equiv i_2 \pmod{p}.$$

Call $p(j)$ the *period* of the jth *column* in $\mathcal{T}$.

Tables 2.1 to 2.4 are not column-periodic. Table 2.5 is column-periodic with $p(1) = 4$, $p(2) = 2$ and $p(3) = 4$.

2	–2	2
$\boxed{4}$	1	2
3	$\boxed{2}$	1
2	1	$\boxed{4}$
1	$\boxed{2}$	3
$\boxed{4}$	1	2

Table 2.5: A column-periodic waiting table.

Observation 2.9. *If $\mathcal{T} = (T, \rho, \mu)$ is a column-periodic waiting table of height h and width k, with period P, then*

(i) $P = \text{l.c.m.}\Big(p(1), p(2), \ldots, p(k)\Big)$; *and*

(ii) $\forall\, i \in \{0, 1, \ldots, h\}\, \forall\, j \in \{1, 2, \ldots, k\} : \mu(i) = j \iff t_{i,j} = p(j)$.

Lemma 2.10. *Let $\mathcal{T} = (T, \rho, \mu)$ be a vertex-periodic P–table of width k. Let $i \in \{0, 1, \ldots, P{-}1\}$ and suppose that $j_1, j_2 \in \{1, 2, \ldots, k\}$ are such that $j_1 = \mu(i)$ and $j_2 = \mu(i{+}1)$. Then $\rho(j_2) = p(j_2) - p(j_1)$.*

Proof. According to Lemma 2.3 and Observation 2.9,

$$\rho(j) = t_{i+1,\,\mu(i+1)} - t_{i,\,\mu(i)} = t_{i+1,\,j_2} - t_{i,\,j_1} = p(j_2) - p(j_1).$$

□

3. Waiting Paths

Let us first introduce several terms from graph theory. Define a *graph* as a quadruple $G = (V, A, \alpha, \omega)$, where V is a set of vertices, A is a set of *arrows* (or *directed edges*), and α and ω are mappings from A to V. If $e \in A$, say the arrow e *starts* at the vertex $u = \alpha(e)$ and *ends* at the vertex $v = \omega(e)$.

For $v \in V$, denote the *indegree* of v (i.e. the number of arrows ending at v) by $\deg_{in}(v)$; that is,

$$\deg_{in}(v) \coloneqq \left|\left\{e \in A : v = \omega(e)\right\}\right|;$$

denote the *outdegree* of v (i.e. the number of arrows starting at v) by $\deg_{out}(v)$; that is,

$$\deg_{out}(v) \coloneqq \left|\left\{e \in A : v = \alpha(e)\right\}\right|.$$

The graph G is called *balanced* if $\deg_{in}(v) = \deg_{out}(v)$ for all $v \in V$. If G is balanced and $v \in V$, define the *degree* of v as the indegree of v (which equals its outdegree); that is,

$$\deg(v) \coloneqq \deg_{in}(v) = \deg_{out}(v).$$

The graph G is called *doubly-balanced* if it is balanced and if for all $u, v \in V$, $\deg(u) = \deg(v)$ whenever there exist $w \in V$ and $e, f \in A$ such that $u = \alpha(e)$, $v = \alpha(f)$, and $w = \omega(e) = \omega(f)$. This can be expressed by saying that confluence induces degree equality in doubly-balanced graphs.

A *path* of length $h{+}1$ on the graph G is a sequence $E = (e_0, e_1, \ldots, e_h)$ of arrows from A such that $\omega(e_i) = \alpha(e_{i+1})$ for all $i \in \{0, 1, \ldots, h{-}1\}$. Say that the path E *contains*

- *an arrow* $e \in A$ if $e = e_i$ for some $i \in \{0, 1, \ldots, h\}$; and
- *a vertex* $v \in V$ if

  $v = \alpha(e_0)$, i.e. the path E *starts* at the vertex v; or
  $v = \omega(e_h)$, i.e. the path E *ends* at the vertex v; or if
  $v = \omega(e_i) = \alpha(e_{i+1})$ for some $i \in \{0, 1, \ldots, h{-}1\}$.

The path E is said to be

- *closed* if $\omega(e_h) = \alpha(e_0)$; and
- *Eulerian* if E contains every arrow $e \in A$ exactly once.

Call the graph G

- *weakly connected* if for all $u, v \in V$ there exists a path which starts at u and ends at v, *or* a path which starts at v and ends at u; and
- *strongly connected* if for all $u, v \in V$ there exists a path which starts at u and ends at v, *and* a path which starts at v and ends at u.

Call a vertex $v \in V$ *isolated* if $\deg_{in}(v) = \deg_{out}(v) = 0$.

Note. A graph $G = (V, A)$ may contain multiple directed edges going from a vertex $u \in V$ to a vertex $v \in V$. The graph may even contain edges starting and ending at the same vertex. Such kind of objects are sometimes called *directed multigraphs*.

A path may contain any vertices multiple times. Such kind of objects are sometimes called *walks*.

3.1 Definition and Elementary Properties

In this chapter, we will define waiting paths and look at some of their properties. We will be especially interested in waiting paths which are both injective and infinitary. Notice that the chapter is intentionally written in a very similar way as the previous one. In the next chapter, we will show that waiting tables can be transformed into waiting paths and vice versa.

Definition 3.1 (Waiting Path)**.** Consider a graph $G = (V, A, \alpha, \omega)$ and an integer $h \geq 0$. A *waiting path* of *length* h on G is a triple $\mathcal{E} = (E, \rho, \pi)$ consisting of an Eulerian path $E = (e_0, e_1, \ldots, e_{h-1})$ on G, a mapping ρ from V to $\mathbb{Z}$, and a mapping π from A to $\{1, 2, \ldots\}$, where the following properties hold:

(E1) If $0 \leq i < h-1$ and if $v \in V$ is such that $v = \omega(e_i) = \alpha(e_{i+1})$, then

$$\rho(v) = \pi(e_{i+1}) - \pi(e_i).$$

(E2) If $0 \leq i_1 \leq i_2 \leq h-1$, then

$$\pi(e_{i_1}) = i_2 - i_1 + 1$$

if and only if there exists $v \in V$ such that $v = \alpha(e_{i_1})$, $v = \omega(e_{i_2})$ and $v \neq \alpha(e_i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$.

The mapping ρ will be referred to as the (*vertex*) *evaluation* and the mapping π as the (*edge*) *weights*.

Definition 3.2 (Modular Waiting Path)**.** A *modular waiting path* is a waiting path where the rules for the vertex evaluation ρ and for the edge weights π in Definition 3.1 in (E1-2) are considered modulo an integer $N > 1$ called the *modulus* of the waiting path.

Lemma 3.3. *Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be a waiting path of length h on G. Then for all $v \in V$ the following property holds:*

(E2') *If $0 \leq i_1 < i_2 \leq h-1$, then*

$$\pi(e_{i_1}) = i_2 - i_1$$

if and only if there exists $v \in V$, where $v = \alpha(e_{i_1}) = \alpha(e_{i_2})$ and $v \neq \alpha(e_i)$ for all $i \in \mathbb{Z}$, $i_1 < i < i_2$.

Proof. This follows directly from (E2) in Definition 3.1. □

If further edges may be added to a waiting path $\mathcal{E}$ of length h on a graph $G=(V,A)$, forming thus a new waiting path $\mathcal{E}'$ of length $h' \geq h$ on a graph $G'=(V,A')$, say that $\mathcal{E}$ is *extendable* into $\mathcal{E}'$.

Waiting path $\mathcal{E} = (E, \rho, \pi)$ of length h on a graph $G = (V, A, \alpha, \omega)$ is called

- *infinitary* if it may be extended by addition of infinitely many edges;
- *periodic* if there exists a positive integer $P \leq h$ such that $\omega(e_{P-1}) = \alpha(e_0)$, and $\pi(e_i) = i' - i$ for all $i \in \{0, 1, \ldots, h-1\}$, where

$$i' \coloneqq \min\Big\{m \in \mathbb{Z},\, m > i : \alpha(e_i) = \alpha(e_{m \bmod P})\Big\}.$$

  The least possible value of P is called the *period* of $\mathcal{E}$;
- *periodically extendable* if it is extendable into a periodic waiting path;
- *complete* if it is periodic or if no further edge may be added to it; and
- *injective* if the evaluation ρ is an injective mapping.

Examples of waiting paths are in Figs. 3.1 to 3.4. The vertex evaluation ρ is indicated by the values inside the vertices (which are drawn as circles). The edge weight $\pi(e_i)$ is for each arrow e_i expressed by a value in a frame on the top of the arrow e_i.

Lemma 3.4 (Extension of Waiting Paths)**.** *Let $G = (V, A, \alpha, \omega)$ be a graph. If a waiting path $\mathcal{E} = (E, \rho, \pi)$ of length h on G can be extended into a waiting path $\mathcal{E}'$ of length $h+1$ (on a graph G', created from G by addition of a new arrow) and if we denote the newly-added arrow by e_h, then the vertex $v = \omega(e_h)$*

- *either is isolated in G, and then any other isolated vertex in G may be chosen in place of v,*
- *or is not isolated in G, and then v is uniquely determined by the mappings α, ω and π.*

Proof. First, consider a vertex $v \in V$, $v = \omega(e_h)$, isolated in G. Then, E does not contain v, and so the vertex v (as well as the edge e_h) trivially follows the rules in Definition 3.1. That would also be true for any other vertex isolated in G, in place of v.

Now, consider vertices $u, v \in V$, non-isolated in G, such that it is possible to define $\omega(e_h)$ as $\omega(e_h) \coloneqq u$ or as $\omega(e_h) \coloneqq v$. Put:

$$i_u \coloneqq \max\{0 \leq i < h : \alpha(e_i) = u\};\ \text{and}$$
$$i_v \coloneqq \max\{0 \leq i < h : \alpha(e_i) = v\}.$$

Since both u and v are non-isolated in G, both i_u and i_v are well defined. $\omega(e_h)$ may be defined as $\omega(e_h) \coloneqq u$, so $\pi(e_{i_u}) = h - i_u + 1$, and so (from Definition 3.1) $u = \omega(e_h)$. But $\omega(e_h)$ may also be defined as $\omega(e_h) \coloneqq v$, so $\pi(e_{i_v}) = h - i_v + 1$, and so (from Definition 3.1) $v = \omega(e_h)$. Therefore, $u = v$. □

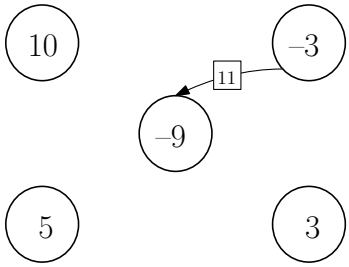

Figure 3.1: A waiting path which can be extended by addition of further arrows. For a possible extension of this graph, see Fig. 3.2.

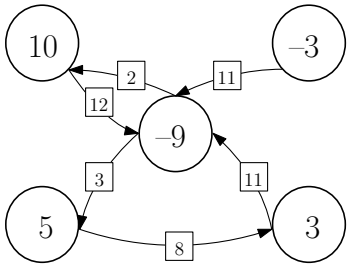

Figure 3.2: A waiting path which is injective but not infinitary.

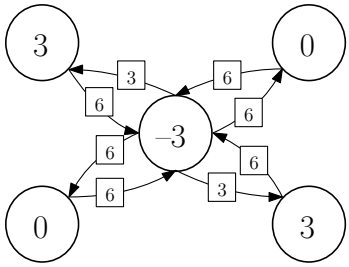

Figure 3.3: A waiting path which is periodic (with period $P = 6$) but not injective.

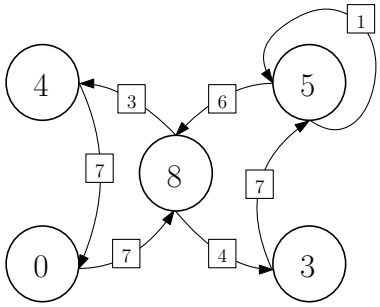

Figure 3.4: A modular waiting path (with modulus $N = 11$) that is both injective and periodic (with period $P = 7$).

Observation 3.5. *Let G be a graph without isolated vertices.*

(i) *If there exists a waiting path on G, then G is weakly connected.*

(ii) *If there exists a periodic waiting path on G, then G is strongly connected.*

Observation 3.6. *Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be a periodic waiting path of length h on G, with period P. Then the following is true for all $i_1, i_2 \in \{0, 1, \ldots, h-1\}$:*

$$\alpha(e_{i_1}) = \alpha(e_{i_2}) \text{ whenever } i_1 \equiv i_2 \pmod{P}; \text{ and}$$
$$\pi(e_{i_1}) = \pi(e_{i_2}) \text{ whenever } i_1 \equiv i_2 \pmod{P}.$$

Definition 3.7 (P–path)**.** Consider a positive integer $P > 1$. A periodic waiting path of length P on a graph G, with period P, is called a *P–path* (on G).

Observation 3.8. *If $\mathcal{E} = (E, \rho, \pi)$ is a P–path on a graph G, then the graph G is balanced and the path E is closed.*

3.2 Vertex-Periodic Waiting Paths

In periodic waiting paths, the vertices repeat periodically on the Eulerian path (and the period of each vertex divides the period P of the waiting path). However, for a given vertex, different subcycles (i.e. closed paths in the graph) containing the vertex exactly once may have different lengths. We will now look at a special class of periodic waiting paths, where for each vertex, all such subcycles have the same length.

Definition 3.9 (Vertex-Periodic Waiting Path)**.** Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be a periodic waiting path of length h on G. Call $\mathcal{E}$ *vertex-periodic* if for all $v \in V$ there exists an integer $p = p(v) > 0$ such that if $v = \alpha(e_{i_1})$ and $i_2 \in \{0, 1, \ldots, h-1\}$, then

$$\alpha(e_{i_1}) = \alpha(e_{i_2}) \iff i_1 \equiv i_2 \pmod{p}$$

Call $p(v)$ the *period of the vertex v* in $\mathcal{E}$.

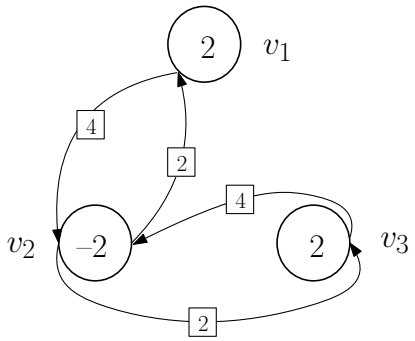

Figure 3.5: A vertex-periodic waiting path.

Figs. 3.1 to 3.4 are not vertex-periodic. Fig. 3.5 is vertex-periodic with $p(v_1) = 4$, $p(v_2) = 2$ and $p(v_3) = 4$.

Observation 3.10. *If $G = (V, A, \alpha, \omega)$ is a graph and $\mathcal{E} = (E, \rho, \pi)$ is a vertex-periodic waiting path of height h on G, with period P, then*

(i) $P = \text{l.c.m.}\big(p(1), p(2), \ldots, p(k)\big)$; *and*

(ii) $\forall\, i \in \{0, 1, \ldots, h-1\}\, \forall\, v \in V : \alpha(e_i) = v \implies \pi(e_i) = p(v)$.

Lemma 3.11. *Let $G = (V, A, \alpha, \omega)$ be a graph and $\mathcal{E}$ be a vertex-periodic P–path on G. Then $P = \deg(v)\, p(v)$ for all $v \in V$.*

Proof. For $v \in V$ consider a set $S = \Big\{ i \in \mathbb{Z},\, 0 \le i < P : \alpha(e_i) = v \Big\}$ and put

$$m \coloneqq \min S,\ p \coloneqq p(v) \text{ and } d \coloneqq \deg(v).$$

Then

$$|S| = \deg_{out}(v) = \deg(v) = d,$$

and from the vertex periodicity of $\mathcal{E}$,

$$S = \Big\{ m,\, m + p,\, \ldots,\, m + (d-1)\, p \Big\}.$$

Since the waiting path $\mathcal{E}$ is periodic with period P,

$$\begin{aligned} m + d\, p &= m + P; \text{ and} \\ d\, p &= P. \end{aligned}$$

□

Lemma 3.12. *Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be a vertex-periodic P–path on G. Let $i \in \{1, 2, \ldots, P-1\}$ and suppose that $v_1, v_2 \in V$ are such that $v_1 = \alpha(e_{i-1})$ and $v_2 = \alpha(e_i)$. Then $\rho(v_2) = p(v_2) - p(v_1)$.*

Proof. According to Definition 3.1 and Observation 3.10,

$$\rho(v_2) = \pi(e_i) - \pi(e_{i-1}) = p(v_2) - p(v_1).$$

□

Drápal and Hojsík showed that column-periodic waiting tables are equivalent to directed doubly-balanced (multi)graphs with vertex-periodic Eulerian cycles (i.e. closed Eulerian paths which have the property from Definition 3.9) [2, Proposition 5.1].

We will show our model is not weaker, i.e. our vertex-periodic waiting paths are also doubly-balanced:

Lemma 3.13. *Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be a vertex-periodic P–path on G. Then the graph G is doubly-balanced.*

Proof. Consider vertices $u, v, w \in V$ and arrows $e, f \in A$ such that $u = \alpha(e)$, $v = \alpha(f)$ and $w = \omega(e) = \omega(f)$. We need to prove $\deg(u) = \deg(v)$.

From Lemma 3.12, we have $\rho(w) = p(w) - p(u)$ as well as $\rho(w) = p(w) - p(v)$, and therefore $p(u) = p(v)$. From Lemma 3.11, we have $P = \deg(u)p(u)$ as well as $P = \deg(v)p(v)$, and therefore $\deg(u) = \deg(v)$. □

4. Equivalence of Waiting Tables and Waiting Paths

In this chapter, we will show that waiting tables and waiting paths can be converted into one another. For simplicity, in order for the header $\rho_{\mathcal{T}}$ (of a waiting table $\mathcal{T}$ of width k) to have the same domain as the evaluation $\rho_{\mathcal{E}}$ (of a waiting path $\mathcal{E}$ on a graph with a set V of k vertices), suppose throughout this chapter that $V = \{1, 2, \ldots, k\}$.

Note that the proofs of Theorems 4.5 and 4.6 are constructive and can therefore be used to create waiting paths from waiting tables and vice versa.

Definition 4.1 (Equivalence of a waiting table and a waiting path)**.** Let $\mathcal{T}_0$ be a waiting table and $\mathcal{E}_0$ be a waiting path. Say that $\mathcal{T}_0$ and $\mathcal{E}_0$ are *equivalent* if they can be extended into a complete waiting table $\mathcal{T} = (T, \rho, \mu)$ of height h and width k, and a complete waiting path $\mathcal{E} = (E, \rho, \pi)$ of length h on a graph $G = (V, A, \alpha, \omega)$ on k vertices, such that for all $i \in \{0, 1, \ldots, h-1\}$ the following properties hold:

(i) $\alpha(e_i) = \mu(i)$;

(ii) $\omega(e_i) = \mu(i+1)$; and

(iii) $\pi(e_i) = t_{i,\,\mu(i)}$.

Observation 4.2. *Let $\mathcal{T}$ be a waiting table of height h, extendable into a waiting table $\mathcal{T}'$ of height $h' \geq h$. Let $\mathcal{E}$ be a waiting path of length h, extendable into a waiting path $\mathcal{E}'$ of height $h' \geq h$. Then $\mathcal{T}$ and $\mathcal{E}$ are equivalent if and only if $\mathcal{T}'$ and $\mathcal{E}'$ are equivalent.*

Lemma 4.3. *Let $\mathcal{T} = (T, \rho, \mu)$ be a waiting table of height h and width k. If $0 \leq i_1 \leq i_2 \leq h$ and $1 \leq j \leq k$, then*

$$t_{i_1,\,j} - t_{i_2,\,j} = i_2 - i_1$$

if and only if $j \neq \mu(i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$.

Proof. First, suppose $j \neq \mu(i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$. Proceed by induction for $n := i_2 - i_1$. If $n = 1$, then (as $\mu(i_2) \neq j$ and so $t_{i_1,\,j} \neq 1$) from Definition 2.1,

$$t_{i_2,\,j} = t_{i_1,\,j} - 1; \text{ and}$$
$$t_{i_1,\,j} - t_{i_2,\,j} = 1.$$

Let the statement be true for some $n \geq 1$ and assume $i_2 < h$ and $j \neq \mu(i_2 + 1)$. From the previous step, $t_{i_2,\,j} - t_{i_2+1,\,j} = 1$. From the induction presumption, $t_{i_1,\,j} - t_{i_2,\,j} = n$. Together,

$$t_{i_1,\,j} - t_{i_2+1,\,j} = (t_{i_1,\,j} - t_{i_2,\,j}) + (t_{i_2,\,j} - t_{i_2+1,\,j}) = n + 1.$$

Suppose now $t_{i_1,\,j} - t_{i_2,\,j} = i_2 - i_1$. For contradiction, assume there exists $i \in \mathbb{Z}$, $i_1 < i \leq i_2$, such that $j = \mu(i)$. Consider the least such i. From Definition 2.1, $t_{i-1,\,j} = 1$, and according to the previous part of the proof,

$$t_{i_1,\,j} - t_{i-1,\,j} = (i-1) - i_1.$$

Therefore, we arrive at a contradiction:

$$t_{i_1,j} - t_{i_2,j} \leq t_{i_1,j} - 1 = t_{i_1,j} - t_{i-1,j} = i - 1 - i_1 < i - i_1 \leq i_2 - i_1.$$

□

Lemma 4.4. *Let $\mathcal{T} = (T, \rho, \mu)$ be a waiting table of height h and width k. If $0 \leq i_1 \leq i_2 \leq h-1$ and $1 \leq j \leq k$, then*

$$t_{i_1,j} = i_2 - i_1 + 1$$

if and only if $j = \mu(i_2 + 1)$ and $j \neq \mu(i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$.

Proof. First, suppose $j = \mu(i_2 + 1)$ and $j \neq \mu(i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$. According to Definition 2.1, $t_{i_2,j} = 1$ because $\mu(i_2 + 1) = j$. From Lemma 4.3,

$$t_{i_1,j} = t_{i_1,j} - t_{i_2,j} + t_{i_2,j} = i_2 - i_1 + 1.$$

Suppose now $t_{i_1,j} = i_2 - i_1 + 1$. According to Definition 2.1,

$$\begin{aligned} t_{i_1+1,j} &= t_{i_1,j} - 1 = (i_2 - i_1 + 1) - 1 = i_2 - i_1, \\ t_{i_1+2,j} &= t_{i_1+1,j} - 1 = (i_2 - i_1) - 1, \\ &\vdots \\ t_{i_2,j} = t_{i_1+(i_2-i_1),j} &= \ldots = (i_2 - i_1) - (i_2 - i_1 - 1) = 1 \end{aligned}$$

So from (T2) and (T3) in Definition 2.1,

$$j = \mu(i_2 + 1) \text{ and } j \neq \mu(i) \text{ for all } i \in \mathbb{Z},\ i_1 < i \leq i_2.$$

□

Theorem 4.5. *Let $\mathcal{T} = (T, \rho, \mu)$ be a complete waiting table of height h and width k. Then there exists a graph G on k vertices with a waiting path $\mathcal{E}$ such that $\mathcal{T}$ and $\mathcal{E}$ are equivalent.*

Proof. Put $V := \{1, 2, \ldots, k\}$ and let $A = \{e_0, e_1, \ldots, e_{h-1}\}$ be a set of h elements. Define $\alpha(e_i) := \mu(i)$ and $\omega(e_i) := \mu(i+1)$ for all $i \in \{0, 1, \ldots, h-1\}$. Then $G := (V, A, \alpha, \omega)$ is a (well-defined) graph.

Consider a sequence $E = (e_0, e_1, \ldots, e_{h-1})$ and observe that E is an Eulerian path on the graph G. Define $\pi(e_i) := t_{i,\mu(i)}$ for all $i \in \{0, 1, \ldots, h-1\}$. We will show now that $\mathcal{E} := (E, \rho, \pi)$ is a well-defined waiting path, i.e. it has the required properties from Definition 3.1:

(E1) Let $0 \leq i < h-1$ and put $v = \omega(e_i) = \alpha(e_{i+1}) = \mu(i+1)$. Then we get from Lemma 2.3:

$$\rho(v) = t_{i+1,\mu(i+1)} - t_{i,\mu(i)} = \pi(e_{i+1}) - \pi(e_i).$$

(E2) Let $0 \leq i_1 \leq i_2 \leq h-1$. Then we get from Lemma 4.4:

$$\pi(e_{i_1}) = t_{i_1,\mu(i_1)} = i_2 - i_1 - 1$$

if and only if there exists $v \in \mathbb{Z}$, $1 \leq v \leq k$, such that $v = \mu(i_1) = \alpha(e_{i_1})$, $v = \mu(i_2 + 1) = \omega(e_{i_2})$ and $v \neq \alpha(e_i)$ for all $i \in \mathbb{Z}$, $i_1 < i \leq i_2$.

□

Theorem 4.6. *Let $G = (V, A, \alpha, \omega)$ be a graph on k vertices. Let G be without isolated vertices. Let $\mathcal{E} = (E, \rho, \pi)$ be a complete waiting path of length h on G. Then there exists a waiting table $\mathcal{T}$ of height h and width k such that $\mathcal{T}$ and $\mathcal{E}$ are equivalent.*

Proof. Put

$$\mu(i) := \begin{cases} \alpha(e_i) & \text{if } 0 \le i < h; \text{ and} \\ \omega(e_{h-1}) & \text{if } i = h. \end{cases}$$

Then $\omega(e_i) = \mu(i{+}1)$ for all $i \in \{0, 1, \ldots, h{-}1\}$.

If $0 \le i \le h$ and $1 \le j \le k$, define a set $S_{i,j} := \{m \in \mathbb{Z},\ i < m \le h : j = \mu(m)\}$. Put

$$t_{0,j} := \begin{cases} \pi(e_0) & \text{if } j = \mu(0) = \alpha(e_0); \text{ and} \\ \min S_{0,j} & \text{if } j \ne \mu(0) = \alpha(e_0) \end{cases}$$

for all $j \in \{1, 2, \ldots, k\}$.

Note that if $1 \le j \le k$, the vertex j is not isolated in the graph G, and so $j = \alpha(e_0) = \mu(0)$ or $j = \omega(i) = \mu(i{+}1)$ for some $i \in \{0, 1, \ldots, h{-}1\}$ (and then $S_{0,j} \ne \emptyset$). Therefore, $t_{0,j}$ is well defined for all $j \in \{1, 2, \ldots, k\}$.

Put now

$$t_{i+1,j} := \begin{cases} t_{i,\mu(i)} + \rho(j) & \text{if } t_{i,j} = 1; \text{ and} \\ t_{i,j} - 1 & \text{if } t_{i,j} \ne 1 \end{cases}$$

for all $i \in \{0, 1, \ldots, h{-}1\}$ and all $j \in \{1, 2, \ldots, k\}$. Consider a rectangular array $T := (t_{i,j})$, $0 \le i \le h$ and $1 \le j \le k$. We will now show that $\mathcal{T} = (T, \rho, \mu)$ is a well-defined waiting table.

We need to prove that each row of T only contains positive integers, exactly one of them being equal to 1. To prove this, we will show for all $i \in \{0, 1, \ldots, h{-}1\}$ and $j \in \{1, 2, \ldots, k\}$ that either $t_{i,j} > h - i$ or $t_{i,j} = \min S_{i,j} - i$. At the same time, we will show $\pi(e_i) = t_{i,\mu(i)}$ for all $i \in \{0, 1, \ldots, h{-}1\}$.

Proceed by induction. First, suppose $i = 0$. We only need to consider the case $t_{0,\mu(0)} = \pi(e_0)$ when $\pi(e_0) = t$ for some $t \le h$. Then, according to Definition 3.1, there exists $j \in \{1, 2, \ldots, k\}$ such that $j = \alpha(e_0) = \omega(e_{t-1})$ and $j \ne \alpha(e_i)$ for all $i \in \mathbb{Z}$, $0 < i \le t{-}1$. Therefore, $\mu(t) = \omega(t{-}1)$, and therefore

$$t_{0,\mu(0)} = \pi(e_0) = \min S_{0,\mu(0)} - 0 = \min S_{0,\mu(0)}.$$

Now, for $i \in \mathbb{Z}$, $0 < i < h{-}1$, suppose $\pi(e_i) = t_{i,\mu(i)}$ and either $t_{i,j} > h - i$ or $t_{i,j} = \min S_{i,j} - i$; we will prove the same is true for $i{+}1$. If $t_{i,j} > h - i$, then

$$t_{i+1,j} = t_{i,j} - 1 > h - i - 1 = h - (i + 1).$$

Note that if $j = \mu(i) = \pi(e_i)$ and thus

$$1 < h - i < t_{i,j} = t_{i,\mu(i)} = \pi(e_i),$$

then $j \ne \mu(i{+}1)$ by Definition 3.1.

Consider the latter case, i.e. $t_{i,\,j} = \min S_{i,\,j} - i$. If $t_{i,\,j} \neq 1$, then $j \neq \mu(i{+}1)$, and therefore

$$\begin{aligned} t_{i+1,\,j} &= t_{i,\,j} - 1 \\ &= (\min S_{i,\,j} - i) - 1 \\ &= \min S_{i,\,j} - (i+1) \\ &= \min \left\{ m \in \mathbb{Z},\, i < m \leq h : j = \mu(m) \right\} - \Big(i+1\Big) \\ &= \min \left\{ m \in \mathbb{Z},\, i{+}1 < m \leq h : j = \mu(m) \right\} - \Big(i+1\Big) \\ &= \min\, S_{i+1,\,j} - (i{+}1). \end{aligned}$$

Else, if $t_{i,\,j} = 1$, then $j = \mu(i{+}1)$ and

$$t_{i+1,\,j} = t_{i+1,\,\mu(i+1)} = t_{i,\,\mu(i)} + \rho(j).$$

By the induction assumption, $t_{i,\,\mu(i)} = \pi(e_i)$. From this and from Definition 3.1, we get

$$\rho(j) = t_{i+1,\,\mu(i+1)} - t_{i,\,\mu(i)} = \pi(e_{i+1}) - \pi(e_i),$$

and therefore $t_{i+1,\,j} = t_{i+1,\,\mu(i+1)} = \pi(e_{i+1})$. If $\pi(e_{i+1}) \leq h - (i{+}1)$, then (by Definition 3.1) there exists $i' \in \mathbb{Z}$, $i < i' \leq h{-}1$, such that $j = \omega(e_{i'}) = \mu(i'{+}1)$ and $j \neq \alpha(m) = \mu(m)$ for all $m \in \mathbb{Z}$, $i < m \leq i'$, and that

$$\begin{aligned} \pi(e_{i+1}) &= i' - (i{+}1) + 1 \\ &= (i'{+}1) - (i{+}1) \\ &= \min \left\{ m \in \mathbb{Z},\, i{+}1 < m \leq h{-}1 : j = \mu(m) \right\} - \Big(i+1\Big) \\ &= \min S_{i+1,\,j} - (i{+}1). \end{aligned}$$

The waiting table $\mathcal{T} = (T,\, \rho,\, \mu)$ is thus well-defined and it is also equivalent to the waiting path $\mathcal{E} = (E,\, \rho,\, \pi)$ because all properties from Definition 4.1 hold. □

Note (about isolated vertices)**.** Waiting paths with isolated vertices could be viewed as objects equivalent to waiting tables having (infinitely) high values in the corresponding columns. This issue could be solved by addition of the following requirement to Definition 3.1:

(E3) If $v \in V$, there exists an integer $t = t(v) > 0$ such that

$$t < h \implies v = \alpha(e_t)$$

The value $t(v) = t_{0,\,v}$ from a corresponding waiting table would satisfy this requirement. Adding such requirement would however also complicate the definition of waiting path without bringing sufficient benefits to the model.

Theorem 4.7. *Let $\mathcal{T} = (T,\, \rho,\, \mu)$ be a waiting table of height h and width k. Let $\mathcal{E} = (E,\, \rho,\, \pi)$ be a waiting path of length h on a graph $G = (V,\, A,\, \alpha,\, \omega)$ with k vertices. If $\mathcal{T}$ and $\mathcal{E}$ are equivalent, then the following properties hold:*

(i) *$\mathcal{T}$ is injective if and only if $\mathcal{E}$ is injective.*

(ii) *$\mathcal{T}$ is periodic with period P if and only if $\mathcal{E}$ is periodic with period P.*

Proof.

(i) $\mathcal{T}$ is injective $\iff$ the mapping ρ is injective $\iff$ $\mathcal{E}$ is injective.

(ii) First, suppose that $\mathcal{T}$ is periodic with period P. Then

$$\omega(e_{P-1}) = \mu\Big((P-1)+1\Big) = \mu(P) = \mu(0) = \alpha(e_0).$$

Let $i \in \{1, 2, \ldots, P-1\}$ and denote

$$i' \coloneqq \min\Big\{m \in \mathbb{Z},\, m > i : \alpha(e_i) = \alpha(e_{m \bmod P})\Big\}.$$

Without loss of generality, suppose $i' \leq h$ (else consider a waiting table $\mathcal{T}'$ of height $h' \geq i'$ such that $\mathcal{T}$ can be extended into $\mathcal{T}'$). Then $\alpha(e_i) = \alpha(e_{i'})$ and so $\mu(i) = \mu(i')$. According to Lemma 4.4

$$\pi(e_i) = t_{i,\,\mu(i)} = i' - i.$$

Suppose now that $\mathcal{E}$ is periodic with period P. Then

$$\mu(P) = \omega(e_{P-1}) = \alpha(e_0) = \mu(0).$$

Let $j \in \{1, 2, \ldots, k\}$ and suppose $t_{0,\,j} \neq t_{P,\,j}$, for example $t_{0,\,j} < t_{P,\,j}$. Denote $i_1 \coloneqq t_{0,\,j}$ and $i_2 \coloneqq t_{0,\,j} + P$. Without loss of generality, suppose $i_2 < h$ (else consider a waiting path $\mathcal{E}'$ of length $h' > i_2$ such that $\mathcal{E}$ can be extended into $\mathcal{E}'$). Then, $i_1 \equiv i_2 \pmod{P}$, and yet, because $\mathcal{T}$ and $\mathcal{E}$ are equivalent,

$$\alpha(e_{i_1}) = \mu(i_1) \neq \mu(i_2) = \alpha(e_{i_2}),$$

which (according to Observation 3.6) contradicts with the periodicity of $\mathcal{E}$. Therefore, $t_{0,\,j} = t_{P,\,j}$.

□

Corollary 4.8. *Suppose the requirements of Theorem 4.7 are satisfied. Then the following properties hold:*

(i) *$\mathcal{T}$ is infinitary if and only if $\mathcal{E}$ is infinitary.*

(ii) *$\mathcal{T}$ is periodically extendable if and only if $\mathcal{E}$ is periodically extendable.*

(iii) *$\mathcal{T}$ is column periodic if and only if $\mathcal{E}$ is vertex periodic.*
In that case, the period $p_{\mathcal{T}}(j)$ of the jth column in $\mathcal{T}$ is equal to the period $p_{\mathcal{E}}(j)$ of the vertex j in $\mathcal{E}$ for all $j \in \{1, 2, \ldots, k\}$.

Corollary 4.9. *A waiting path is infinitary if and only if it is periodically extendable.*

5. Looking for Injective Vertex-Periodic Waiting Paths

We will now introduce compressed graphs, i.e. objects created from balanced graphs by grouping all vertices of the same degree together into a new "compressed vertex". We will also define indicator matrices (indicating whether there is at least one arrow between two given vertices), which are similar to adjacency matrices from graph theory (which also tell how many such arrows are there).

Definition 5.1 (Indicator Matrix)**.** Consider a graph $G = (V, A, \alpha, \omega)$ with a set of vertices $V = \{v_1, v_2, \ldots\}$. The *indicator matrix* of the graph G is a square matrix $M = (m_{i,j})$ defined as

$$m_{i,j} := \begin{cases} 1 & \text{if } \exists\, e \in A : \alpha(e) = v_i \text{ and } \omega(e) = v_j; \\ 0 & \text{otherwise.} \end{cases}$$

Definition 5.2 (Compressed Graph)**.** Let $G = (V, A, \alpha, \omega)$ be a balanced graph. Denote the degrees of its vertices $d_1, d_2, \ldots, d_n$, where $d_1 < d_2 < \ldots < d_n$. Define:

$$\begin{aligned} &F_i := \{v \in V : \deg(v) = d_i\},\ 1 \le i \le n; \\ &\widetilde{V} := \{F_1, F_2, \ldots, F_n\}; \\ &\widetilde{\alpha} \colon A \to \widetilde{V},\ e \mapsto F_i \iff \alpha(e) \in F_i; \\ &\widetilde{\omega} \colon A \to \widetilde{V},\ e \mapsto F_i \iff \omega(e) \in F_i; \text{ and} \\ &f_i := |F_i|. \end{aligned}$$

Call $\widetilde{G} = (\widetilde{V}, A, \widetilde{\alpha}, \widetilde{\omega})$ the *compressed graph* for the graph G. In the context of a compressed graph, the numbers $d_1, \ldots, d_n$ will be referred to as *degree values* and the numbers $f_1, \ldots, f_n$ as *degree frequencies*.

Note. A compressed graph $\widetilde{G}$ can be viewed as a graph created from a graph G by "compressing" vertices of the same degree to a single vertex, with arrows induced by the original vertices.

Lemma 5.3. *Let $G = (V, A, \alpha, \omega)$ be a graph and let $\mathcal{E} = (E, \rho, \pi)$ be an injective vertex-periodic P–path on G. Let $e, f \in A$ and put $u_1 := \alpha(e)$, $u_2 := \alpha(f)$, $v_1 := \omega(e)$ and $v_2 := \omega(f)$. If $\deg(u_1) = \deg(u_2)$ and $\deg(v_1) = \deg(v_2)$, then $v_1 = v_2$.*

Proof. The mapping ρ is injective, so $v_1 = v_2$ whenever $\rho(v_1) = \rho(v_2)$. According to Lemmas 3.11 and 3.12,

$$\begin{aligned} \rho(v_1) &= p(v_1) - p(u_1) \\ &= \frac{P}{\deg(v_1)} - \frac{P}{\deg(u_1)} \\ &= \frac{P}{\deg(v_2)} - \frac{P}{\deg(u_2)} \\ &= p(v_2) - p(u_2) \\ &= \rho(v_2) \end{aligned}$$

□

Lemma 5.4. *Let $G = (V, A, \alpha, \omega)$ be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph corresponding to G, with degree values $d_1, d_2, \ldots, d_n$ and degree frequencies $f_1, f_2, \ldots, f_n$. Let $(m_{i,j})$ be the indicator matrix of the compressed graph $\widetilde{G}$. Then for all $i \in \{1, 2, \ldots, n\}$ the following holds:*

(i) $\sum_{k=1}^{n} m_{k,\,i} = f_i$; *and*

(ii) $\sum_{k=1}^{n} m_{i,\,k}\, d_k = f_i\, d_i$.

Proof. Suppose $i \in \{1, 2, \ldots, n\}$ and consider the compressed vertex $F_i \in \widetilde{V}$.

(i) Count the number of arrows incoming into vertices in F_i. On the one hand, every arrow ending at a vertex $v \in F_i$ starts inside the same compressed vertex F_k, because G is doubly balanced. According to Lemma 5.3, all arrows going from any given compressed vertex F_k into F_i end at the same vertex $v \in F_i$. Therefore, if there exists an arrow from F_k to F_i, then there are d_i such arrows (every vertex in F_i has degree d_i). So there are $\sum_{k=1}^{n} m_{k,i} d_i$ incoming arrows. On the other hand, there are f_i vertices of the degree d_i in F_i, which makes $f_i\, d_i$ incoming arrows. Hence $\sum_{k=1}^{n} m_{k,i} d_i = f_i d_i$, and so $\sum_{k=1}^{n} m_{k,i} = f_i$.

(ii) Use similar arguments. Count the number of outgoing arrows from the vertices in F_i. If there exists an arrow from F_i into a compressed vertex F_k, then there are d_k such arrows (every vertex in F_k has degree d_k). So there are $\sum_{k=1}^{n} m_{i,k} d_k$ outgoing arrows. There are f_i vertices of the degree d_i in F_i, which makes $f_i\, d_i$ outgoing arrows. Therefore, $\sum_{k=1}^{n} m_{i,k} d_k = f_i d_i$.

□

Corollary 5.5. *Suppose the requirements of Lemma 5.4 are satisfied. Then the following properties hold:*

(i)
$$\begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & & \\ \vdots & & \ddots & \\ m_{n,1} & & & m_{n,n} \end{pmatrix} = \begin{pmatrix} f_1 & f_2 & \cdots & f_n \end{pmatrix}$$

(ii)
$$\begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & & \\ \vdots & & \ddots & \\ m_{n,1} & & & m_{n,n} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} = \begin{pmatrix} f_1 d_1 \\ f_2 d_2 \\ \vdots \\ f_n d_n \end{pmatrix}$$

Lemma 5.6. *Let $G = (V, A, \alpha, \omega)$ be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph corresponding to G, with degree values $d_1, d_2, \ldots, d_n$ and degree frequencies $f_1, f_2, \ldots, f_n$. Let $(m_{i,j})$ be the indicator matrix of the compressed graph $\widetilde{G}$. If there exists $i \in \{1, 2, \ldots, n\}$ such that $f_i = 1$, then $m_{i,\,j} = 0$ for all $j \in \{i, i{+}1, \ldots, n\}$.*

Proof. Suppose $f_i = 1$ for some $i \in \{1, 2, \ldots, n\}$. Then, according to Lemma 5.4, the following holds:

$$\begin{aligned} \sum_{k=1}^{n} m_{k,\,i} &= 1; \text{ and} \\ \sum_{k=1}^{n} m_{i,\,k}\, d_k &= d_i. \end{aligned} \tag{5.1}$$

If $j > i$, then $d_j > d_i$, so $m_{i,\,j} = 0$. If $j = i$, assume, for a contradiction, that $m_{i,\,i} = 1$. Then, from Eq. (5.1), $m_{i,\,k} = 0$ for all $k \in \{1, 2, \ldots, i-1\}$. It follows from Definitions 5.1 and 5.2 that the (compressed) vertex F_i is not connected to other vertices, a contradiction. □

Corollary 5.7. *Let $G = (V,\, A,\, \alpha,\, \omega)$ be a graph with an injective vertex-periodic P–path. Consider a compressed graph corresponding to G, with degree frequencies $f_1,\, f_2,\, \ldots,\, f_n$, $n \geq 2$. Then*

(a) $f_1 > 1$; and

(b) $f_2 > 1$.

Corollary 5.8. *Let $G = (V,\, A,\, \alpha,\, \omega)$ be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph corresponding to G, with degree values $d_1,\, d_2,\, \ldots,\, d_n$ and degree frequencies $f_1,\, f_2,\, \ldots,\, f_n$. If $f_i = 1$ for some integer $i > 2$, then there exists an integer $r < i$ and there exist integers $i_1,\, i_2,\, \ldots,\, i_r$ such that $1 \leq i_1 < i_2 < \ldots < i_r < i$ and the following holds:*

$$d_{i_1} + d_{i_2} + \ldots + d_{i_r} = d_i.$$

Lemma 5.9. *Let $G = (V,\, A,\, \alpha,\, \omega)$ be a graph with an injective vertex-periodic P–path $\mathcal{E} = (E,\, \rho,\, \pi)$. Let $u, v \in V$ be such that all arrows starting at v end at u or all arrows ending at v start at u (i.e. v is connected to only a single vertex u via its incoming edges or via its outgoing edges). Then*

$$\begin{aligned} p(u) \,|\, p(v);&\ \textit{and} \\ \deg(v) \,|\, \deg(u).& \end{aligned}$$

Proof. According to Lemma 3.11,

$$P = \deg(u)\, p(u) = \deg(v)\, p(v),$$

so $p(u) \,|\, p(v)$ if and only if $\deg(v) \,|\, \deg(u)$. G is vertex-periodic, so $p(u) \,|\, p(v)$. □

Now, we will establish theory for further analyses of injective vertex-periodic waiting paths. We will introduce *injective waiting matrices* and enumerate all of these matrices of size up to 4×4. This will eventually lead us to a conclusion that "simple" injective vertex-periodic waiting paths do not exist.

Say that $\{\Delta,\, \Delta'\}$ is a partition of a set S if the following properties hold:

(i) $\emptyset \neq \Delta \subseteq S$, $\emptyset \neq \Delta' \subseteq S$;

(ii) $\Delta \cup \Delta' = S$; and

(iii) $\Delta \cap \Delta' = \emptyset$.

Consider a square matrix $A = (a_{i,j})$ of order n. Call it (*strongly*) *connected* if

$$\sum_{\substack{i\in\Delta\\ j\in\Delta'}} a_{i,j} > 0$$

for each partition $\{\Delta,\, \Delta'\}$ of the set $\{1, 2, \ldots, n\}$. Call it *cut-balanced* if

$$\sum_{\substack{i\in\Delta\\ j\in\Delta'}} a_{i,j} = \sum_{\substack{i\in\Delta'\\ j\in\Delta}} a_{i,j}.$$

for each partition $\{\Delta,\, \Delta'\}$ of the set $\{1, 2, \ldots, n\}$. Call it *sum-divisible* if

$$a_{i,j} \text{ divides } \sum_{\substack{1\le r\le n\\ 1\le s\le n}} a_{r,\,s}$$

whenever $a_{i,j} \neq 0$. Call it *column-monotone* if for all $i_1, i_2 \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$,

$$a_{i_1,\,j} = a_{i_2,\,j}$$

whenever $a_{i_1,\,j} \neq 0$ and $a_{i_2,\,j} \neq 0$.

We are thus looking for a square matrix D, which would be:

- nonnegative;
- column-monotone;
- connected;
- sum-divisible; and
- cut-balanced.

Call such a matrix $D = (d_{i,j})$ of order n a *periodic waiting matrix*, or *PW–matrix*. If $1 \le j \le n$, denote the nonzero value in the jth column by d_j and the number of those values (in the jth column) by f_j, and put

$$p_j := \frac{P}{d_j}, \text{ where } P := \sum_{\substack{1\le r\le n\\ 1\le s\le n}} d_{r,\,s}$$

If $d_1 < d_2 < \ldots < d_n$, call D an *injective* periodic waiting matrix, or *IPW–matrix*.

Let G be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph of the graph G, with degree values d_1, d_2, …, d_n. Let $M = (m_{i,j})$ be the indicator matrix of the compressed graph $\widetilde{G}$. Put

$$d_{i,j} := \begin{cases} d_j & \text{if } m_{i,j} = 1;\\ 0 & \text{if } m_{i,j} = 0. \end{cases}$$

Call the matrix $D = (d_{i,j})$ the *PW–matrix of the graph G*.

Observation 5.10. *The matrix D from the previous paragraph is the adjacency matrix of the compressed graph $\widetilde{G}$.*

Lemma 5.11. *Let G be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph of the graph G, with degree values $d_1, d_2, \ldots, d_n$ and degree frequencies $f_1, f_2, \ldots, f_n$. Let $D = (d_{i,j})$ be the PW–matrix of the graph G. Then the matrix D has all properties from the definition of a PW matrix (i.e. it is nonnegative, column-monotone, connected, sum-divisible and cut-balanced.)*

Proof. D is apparently nonnegative and column-monotone. If F_i and F_j are compressed vertices of $\widetilde{G}$, there are $d_{i,j}$ arrows from F_i to F_j. If $\{\Delta, \Delta'\}$ is a partition of $\{1, 2, \ldots, n\}$, then the number of arrows from $\bigcup_{i\in\Delta} F_i$ to $\bigcup_{j\in\Delta'} F_j$ is equal to the number of arrows going in the opposite direction (so D is cut-balanced). This number is nonzero since the graph G is Eulerian (so D is connected). There are f_j nonzero values in the jth column of D. Hence $P = \sum_{j=1}^{n} f_j d_j = d_i p_i$ for all $i \in \{1, 2, \ldots, n\}$ (so D is sum-divisible). □

Observation 5.12. *Let D be an IPW–matrix. Define:*

$$\delta := \text{g.c.d.}(d_{i,j};\ 1 \le i, j \le n) > 1;\ \textit{and}$$
$$D' := (d'_{i,j}),\ \textit{where } d'_{i,j} = \frac{d_{i,j}}{\delta}.$$

Then D' is also an IPW–matrix.

Lemma 5.13. *Let G be a graph with an injective vertex-periodic P–path. Let $\widetilde{G}$ be the compressed graph of the graph G, with degree values $d_1, d_2, \ldots, d_n$ and degree frequencies $f_1, f_2, \ldots, f_n$. Let $D = (d_{i,j})$ be the PW–matrix of the graph G. If $f_i = 1$ for some $i \in \{1, 2, \ldots, n\}$, then there exists $J \subseteq \{1, 2, \ldots, n\} \setminus \{i\}$ such that $d_i = \sum_{j\in J} d_j$.*

Proof. Put $J := \{j \in \mathbb{Z} : d_{i,j} \neq 0 \text{ and } 1 \le j \le n\}$. Then $i \notin J$, as otherwise there would be no arrow going from F_i to other vertices. Since $\deg(F_i) = d_i$, it follows that $d_i = \sum_{j\in J} d_{i,j} = \sum_{j\in J} d_j$. □

Corollary 5.14. *Suppose the requirements of Lemma 5.13 are satisfied. If $f_i = 1$, then $i \ge 3$.*

Observation 5.15. *Let $D = (d_{i,j})$ be an IPW–matrix. Then D is connected if for all partitions $\{\Delta, \Delta'\}$ of the set $\{1, 2, \ldots, n\}$ there exists $i \in \Delta$ and $j \in \Delta$ such that $d_{i,j} > 0$.*

The following is a well-known property from graph theory. Note that our definition of weakly-connected graphs is more strict than definitions of weakly-connected graphs in other sources (i.e. we want that every two vertices are connected via an oriented path, whereas other sources usually want that every two vertices are connected via a "non-oriented" path in the oriented graph).

Claim 5.16. *Let G be a balanced graph. Then G is strongly connected if and only if it is weakly connected.*

Lemma 5.17. *Let $D = (d_{i,j})$ be an IPW–matrix. Then D is cut-balanced if and only if*

$$\sum_{j \neq i} d_{i,j} = \sum_{j \neq i} d_{j,i} \tag{5.2}$$

for all $i \in \{1, 2, \ldots, n\}$.

Proof. D is cut-balanced if and only if

$$\sum_{\substack{i \in \Delta \\ j \in \Delta'}} a_{i,j} = \sum_{\substack{i \in \Delta' \\ j \in \Delta}} a_{i,j} \tag{5.3}$$

for each partition $\{\Delta, \Delta'\}$ of the set $\{1, 2, \ldots, n\}$. If Eq. (5.3) holds, then Eq. (5.2) clearly holds as well. Assume now that Eq. (5.2) holds and choose $\Delta := \{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$ arbitrarily. Consider the system of equations

$$\sum_{j \neq i_s} d_{i_s,j} = \sum_{j \neq i_s} d_{j,i_s} \tag{5.4}$$

for $s \in \{1, 2, \ldots, t\}$. The sum of all equations in Eq. (5.4) equals Eq. (5.3). □

5.1 Enumeration of Injective Periodic Waiting Matrices

Let us now look at IPW–matrices of small sizes. For an IPW–matrix D of order $n = 1, \ldots, 4$, we will be using the following properties of D:

- in every row and every column, there exists a nonzero value (as D is connected);
- if $1 \leq i \leq n$, then $\sum_{j=1}^{n} d_{i,j} = \sum_{j=1}^{n} d_{j,i}$ (as D is cut-balanced);
- $d_1 < d_2 < \ldots$ (as D is injective, column-monotone); and
- if $l = \text{l.c.m.}(d_1, d_2, \ldots, d_n)$, then $l \mid P$, where P is the period of the matrix (as D is sum-divisible).

Call the matrix D' from Observation 5.12 the *canonical* IPW–matrix. Call the vector $(d_1, d_2, \ldots, d_n)$ of column values of a canonical matrix D the *canonical solution* of the matrix D.

5.1.1 IPW–matrices of sizes 1×1 and 2×2

The only IPW–matrix of order 1 is $D = (d_1)$, with the canonical matrix $D = (1)$. No matrix of order 2 exists because the equation

$$d_1 = d_{2,1} = d_{1,2} = d_2$$

does not hold.

5.1.2 IPW–matrices of size 3×3

(a) $d_{1,3} = d_{2,3} = d_3$

$$2d_3 = d_{1,3} + d_{2,3} = d_{3,1} + d_{3,2} \leq d_1 + d_2 < 2d_3,$$

a contradiction.

(b) $d_{1,3} = d_3$ and $d_{2,3} = 0$

$$d_2 < d_3 = d_{1,3} + d_{2,3} = d_{3,1} + d_{3,2} \in \{d_1,\, d_2,\, d_1 + d_2\}$$

Therefore, $d_{3,1} = d_1$ and $d_{3,2} = d_2$. But then

$$d_2 > d_1 \geq d_{2,1} + d_{2,3} = d_{1,2} + d_{3,2} \in \{d_2,\, 2d_2\},$$

which cannot be.

(c) $d_{1,3} = 0$ and $d_{2,3} = d_3$

$$d_2 < d_3 = d_{1,3} + d_{2,3} = d_{3,1} + d_{3,2} \in \{d_1,\, d_2,\, d_1 + d_2\}$$

Therefore, $d_{3,1} = d_1$ and $d_{3,2} = d_2$. The matrix D is connected, and therefore $d_{1,2} = d_2$.

$$d_1 < d_2 = d_{1,2} + d_{1,3} = d_{2,1} + d_{3,1} \in \{d_1,\, 2d_1\}$$

Therefore, $d_{2,1} = d_1$.

$$d_2 < d_3 = d_{1,3} + d_{2,3} = d_{3,1} + d_{3,2} \in \{d_1,\, d_2,\, d_1 + d_2\}$$

Therefore, $d_{3,1} = d_1$ and $d_{3,2} = d_2$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 \\ d_1 & \bullet & d_3 \\ d_1 & d_2 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ d_3 &= d_1 + d_2 \end{aligned}$$

We get $d_2 = 2d_1$ and $d_3 = 3d_1$, so the canonical solution is $\boldsymbol{d} = (1, 2, 3)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3) = 6$. Then, $9 \leq P \leq 15$ and $l \mid P$, and therefore $P = 12$. That yields the following matrices:

$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 3 \\ 1 & 2 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 2 & 0 \\ 1 & 0 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

5.1.3 IPW–matrices of size 4×4

(a) $d_{1,4} = d_{2,4} = d_{3,4} = d_4$

$$3d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \leq d_1 + d_2 + d_3 < 3d_4,$$

a contradiction.

(b) $d_{1,4} = d_4$, $d_{2,4} = d_4$ and $d_{3,4} = 0$

$$d_2 + d_3 < 2d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3}$$

Therefore, $d_{4,1} = d_1$, $d_{4,2} = d_2$ and $d_{4,3} = d_3$.

$$2d_3 > d_1 + d_2 \geq d_{3,1} + d_{3,2} + d_{3,4} = d_{1,3} + d_{2,3} + d_{4,3} \in \{d_3,\, 2d_3,\, 3d_3\}$$

Therefore, $d_{1,3} = d_{2,3} = 0$ and $d_3 = d_1 + d_2$, and so

$$2d_4 = d_1 + d_2 + d_3 = d_3 + d_3 = 2d_3,$$

a contradiction.

(c) $d_{1,4} = d_4$, $d_{2,4} = 0$ and $d_{3,4} = d_4$

$$d_2 + d_3 < 2d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3}$$

Therefore, $d_{4,1} = d_1$, $d_{4,2} = d_2$ and $d_{4,3} = d_3$.

$$d_1 < d_2 \leq d_{1,2} + d_{3,2} + d_{4,2} = d_{2,1} + d_{2,3} + d_{2,4} \in \{d_1,\, d_3,\, d_1 + d_3\}$$

Therefore, $d_{2,3} = d_3$. Note that

$$d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \leq 3d_1 < d_2 + d_3 + d_4,$$

and so $d_{1,2} = 0$ or $d_{1,3} = 0$.

(c.a) $d_{1,2} = 0$ and $d_{1,3} = d_3$

$$d_2 < d_3 \leq d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2\}$$

Therefore, $d_{3,2} = d_2$.

$$2d_1 < d_3 + d_4 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\},$$

and so $d_{2,1} = d_{3,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & d_3 & d_4 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_3 + d_4 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_1 + d_2 + d_4 \\ 2d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{8}{7}d_1$, $d_3 = \frac{9}{7}d_1$ and $d_4 = \frac{12}{7}d_1$, the canonical solution is $\boldsymbol{d} = (7, 8, 9, 12)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(7, 8, 9, 12) = 504$. Then $88 \leq P \leq 124$ and $l \mid P$, a contradiction.

(c.b) $d_{1,2} = d_2$ and $d_{1,3} = 0$

$$2d_1 < d_2 + d_4 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\},$$

and so $d_{2,1} = d_{3,1} = d_1$.

$$d_1 + d_2 + d_4 > d_1 + d_2 + d_3 = 2d_4 > 2d_3 = d_{1,3} + d_{2,3} + d_{4,3} = \\ = d_{3,1} + d_{3,2} + d_{3,4} \in \{d_1 + d_4,\, d_1 + d_2 + d_4\}$$

Therefore, $d_{3,2} = 0$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & d_4 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 + d_4 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_4 \\ 2d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{6}{5}d_1$, $d_3 = \frac{7}{5}d_1$ and $d_4 = \frac{9}{5}d_1$, so the canonical solution is $\boldsymbol{d} = (5, 6, 7, 9)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(5, 6, 7, 9) = 630$. However, $59 \leq P \leq 86$ and $l \mid P$, a contradiction.

(c.c) $d_{1,2} = d_{1,3} = 0$

$$d_2 < d_3 \leq d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2\}.$$

Therefore, $d_{3,2} = d_2$.

$$d_1 + d_2 + d_4 > d_1 + d_2 + d_3 = 2d_4 > 2d_3 = d_{1,3} + d_{2,3} + d_{4,3} = \\ = d_{3,1} + d_{3,2} + d_{3,4} \in \{d_2 + d_4,\, d_1 + d_2 + d_4\}$$

Therefore, $d_{3,1} = 0$.

$$d_1 < d_4 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1\},$$

and so $d_{2,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & 0 & d_4 \\ d_1 & \bullet & d_3 & 0 \\ 0 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_4 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_2 + d_4 \\ 2d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{4}{3}d_1$, $d_3 = \frac{5}{3}d_1$ and $d_4 = 2d_1$, so the canonical solution is $\boldsymbol{d} = (3, 4, 5, 6)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(3, 4, 5, 6) = 60$. However, $36 \leq P \leq 54$ and $l \mid P$, a contradiction.

(d) $d_{1,4} = 0$, $d_{2,4} = d_4$ and $d_{3,4} = d_4$

$$d_2 + d_3 < 2d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3}$$

Therefore, $d_{4,1} = d_1$, $d_{4,2} = d_2$ and $d_{4,3} = d_3$. Note that

$$d_3 < d_4 \leq d_{3,1} + d_{3,2} + d_{3,4} = d_{1,3} + d_{2,3} + d_{4,3} \in \{d_3,\, 2d_3,\, 3d_3\},$$

and so $d_{1,3} = d_3$ or $d_{2,3} = d_3$.

(d.a) $d_{1,3} = d_3$, $d_{2,3} = 0$
Note that

$$d_2 < d_4 \leq d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2\, 3d_2\},$$

and so $d_{1,2} = d_2$ or $d_{3,2} = d_2$.

(d.a.a) $d_{1,2} = d_2$ and $d_{3,2} = 0$

$$2d_1 < d_2 + d_3 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$$

Therefore, $d_{2,1} = d_{3,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & 0 & d_4 \\ d_1 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

But then $2d_2 = d_1 + d_4 = 2d_3$, which cannot be.

(d.a.b) $d_{1,2} = 0$ and $d_{3,2} = d_2$
If $d_{3,1} = d_1$, then

$$2d_3 = d_1 + d_2 + d_4 > d_1 + d_2 + d_3 = 2d_4,$$

which cannot be. Therefore, $d_{3,1} = 0$.

$$d_1 < d_3 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1\}.$$

Therefore, $d_{2,1} = d_1$. From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_3 \\ 2d_2 &= d_1 + d_4 \\ 2d_3 &= d_2 + d_4 \\ 2d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{5}{3}d_1$, $d_3 = \frac{6}{3}d_1$ and $d_4 = \frac{7}{3}d_1$, the canonical solution is $\boldsymbol{d} = (3, 5, 6, 7)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(3, 5, 6, 7) = = 210$. However, $42 \leq P \leq 63$ and $l \mid P$, a contradiction.

(d.a.c) $d_{1,2} = d_{3,2} = d_2$

$2d_1 < d_2+d_3 = d_{1,2}+d_{1,3}+d_{1,4} = d_{2,1}+d_{3,1}+d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$

Therefore, $d_{2,1} = d_{3,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

But then $2d_3 = d_1 + d_2 + d_4 > d_1 + d_2 + d_3 = 2d_4$, which cannot be.

(d.b) $d_{1,3} = 0$, $d_{2,3} = d_3$

$2d_2 < d_3 + d_4 \leq d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4_2} \in \{d_2,\, 2d_2,\, 3d_2\}$

Therefore, $d_{1,2} = d_{3,2} = d_2$. If $d_{3,1} = d_1$, then

$$2d_3 = d_1 + d_2 + d_4 > d_1 + d_2 + d_3 = 2d_4,$$

which cannot be. Therefore, $d_{3,1} = 0$.

$$d_1 < d_2 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1\},$$

and so $d_{2,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & d_4 \\ 0 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_1 + d_3 + d_4 \\ 2d_3 &= d_2 + d_4 \\ 2d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{6}{3}d_1$, $d_3 = \frac{7}{3}d_1$ and $d_4 = \frac{8}{3}d_1$, so the canonical solution is $\boldsymbol{d} = (3, 6, 7, 8)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(3, 6, 7, 8) = 168$. However, $54 \leq P \leq 78$ and $l \mid P$, a contradiction.

(d.c) $d_{1,3} = d_{2,3} = d_3$

$2d_2 < d_3 + d_4 \leq d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2,\, 3d_2\}$

Therefore, $d_{1,2} = d_{3,2} = d_2$.

$2d_2 < d_2 + d_3 \leq d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$

Therefore, $d_{2,1} = d_{3,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & d_3 & d_4 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

But then $3d_2 = d_1 + d_3 + d_4 > d_1 + d_2 + d_4 = 3d_3$, which cannot be.

(e) $d_{1,4} = d_4$, $d_{2,4} = 0$ and $d_{3,4} = 0$

Note that

$$2d_3 > d_1 + d_2 \geq d_{3,1} + d_{3,2} + d_{3,4} = d_{1,3} + d_{2,3} + d_{4,3} \in \{d_3,\, 2d_3,\, 3d_3\}$$

and so either $d_{1,3} = d_3$, or $d_{2,3} = d_3$, or $d_{4,3} = d_3$.

$$d_1 < d_2 \leq d_{1,2} + d_{3,2} + d_{4,2} = d_{2,1} + d_{2,3} + d_{2,3} \in \{d_1,\, d_3,\, d_1 + d_3\}$$

Therefore, $d_{2,3} = d_3$ and $d_{1,3} = d_{4,3} = 0$. On the other hand,

$$d_2 < d_3 = d_{1,3} + d_{2,3} + d_{4,3} = d_{3,1} + d_{3,2} + d_{3,4} \in \{d_1,\, d_2,\, d_1 + d_2\},$$

so $d_{3,1} = d_1$ and $d_{3,2} = d_2$. But then

$$d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \leq d_1 + d_2 = d_3,$$

which cannot be.

(f) $d_{1,4} = 0$, $d_{2,4} = d_4$ and $d_{3,4} = 0$

Note that

$$2d_3 > d_1 + d_2 \geq d_{3,1} + d_{3,2} + d_{3,4} = d_{1,3} + d_{2,3} + d_{4,3} \in \{d_3,\, 2d_3,\, 3d_3\}$$

and so either $d_{1,3} = d_3$, or $d_{2,3} = d_3$, or $d_{4,3} = d_3$. If $d_{4,3} = 0$, then

$$d_4 = d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \leq d_1 + d_2 = d_3,$$

which cannot be. Therefore, $d_{4,3} = d_3$ and $d_{1,3} = d_{2,3} = 0$. On the other hand,

$$d_2 < d_3 = d_{1,3} + d_{2,3} + d_{4,3} = d_{3,1} + d_{3,2} + d_{3,4} \in \{d_1,\, d_2,\, d_1 + d_2\},$$

so $d_{3,1} = d_1$ and $d_{3,2} = d_2$. And since the matrix D is connected, $d_{1,2} = d_2$. Note that

$$d_1 < d_2 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$$

and so $d_{2,1} = d_1$ or $d_{4,1} = d_1$.

(f.a) $d_{2,1} = d_1$ and $d_{4,1} = 0$

$$d_3 < d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \in \{d_3,\, d_2 + d_3\}$$

Therefore, $d_{4,2} = d_2$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & 0 \\ 0 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_1 + d_4 \\ d_3 &= d_1 + d_2 \\ d_4 &= d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 5d_1$, so the canonical solution is $\boldsymbol{d} = (1, 2, 3, 5)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 5) = 30$. However, $16 \leq P \leq 27$ and $l \mid P$, a contradiction.

(f.b) $d_{4,1} = d_1$ and $d_{4,2} = 0$

(f.b.a) $d_{2,1} = 0$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ 0 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & 0 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_4 \\ d_3 &= d_1 + d_2 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 4d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 3, 4)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 4) = 12$. However, $13 \leq P \leq 23$ and $l \mid P$, a contradiction.

(f.b.b) $d_{2,1} = d_1$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & 0 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 \\ 2d_2 &= d_1 + d_4 \\ d_3 &= d_1 + d_2 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 3d_1$, $d_3 = 4d_1$ and $d_4 = 5d_1$, the canonical solution is $\boldsymbol{d} = (1, 3, 4, 5)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 3, 4, 5) = 60$. However, $18 \leq P \leq 31$ and $l \mid P$, a contradiction.

(f.c) $d_{4,1} = d_1$ and $d_{4,2} = d_2$

(f.c.a) $d_{2,1} = 0$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ 0 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & 0 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_4 \\ d_3 &= d_1 + d_2 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 6d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 3, 6)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 6) = 6$. Then, $17 \leq P \leq 29$ and $l \mid P$, and therefore $P = 18$ or $P = 24$. That yields the following matrices:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

(f.c.b) $d_{2,1} = d_1$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & 0 & d_4 \\ d_1 & d_2 & \bullet & 0 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 \\ 3d_2 &= d_4 \\ d_3 &= d_1 + d_2 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 3d_1$, $d_3 = 4d_1$ and $d_4 = 8d_1$, the canonical solution is $\boldsymbol{d} = (1, 3, 4, 8)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 3, 4, 8) = 24$. Then, $24 \leq P \leq 40$ and $l \mid P$, and therefore $P = 24$. That yields the following matrix:

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 8 \\ 1 & 3 & 0 & 0 \\ 1 & 3 & 4 & 0 \end{pmatrix}$$

(g) $d_{1,4} = 0$, $d_{2,4} = 0$ and $d_{3,4} = d_4$

Assume $d_{4,3} = 0$. Then

$$d_3 < d_4 \leq d_{3,1} + d_{3,2} + d_{3,4} = d_{1,3} + d_{2,3} + d_{4,3} \in \{d_3,\, 2d_3\}$$

and so $d_{1,3} = d_3$ and $d_{2,3} = d_3$. Also,

$$d_2 < d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \in \{d_1,\, d_2,\, d_1 + d_2\}$$

and so $d_{4,1} = d_1$ and $d_{4,2} = d_2$. But then

$$d_4 = d_1 + d_2 < 2d_3 = d_4,$$

which cannot be. Therefore, $d_{4,3} = d_3$.

$$d_1 < d_2 \leq d_{1,2} + d_{3,2} + d_{4,2} = d_{2,1} + d_{2,3} + d_{2,4} \in \{d_1,\, d_3,\, d_1 + d_3\}$$

Therefore, $d_{2,3} = d_3$. Note that

$$d_3 < d_4 = d_{1,4} + d_{2,4} + d_{3,4} = d_{4,1} + d_{4,2} + d_{4,3} \in \{d_3,\, d_1 + d_3,\, d_2 + d_3,\, d_1 + d_2 + d_3\}$$

and so $d_{4,1} = d_1$ or $d_{4,2} = d_2$.

(g.a) $d_{4,1} = d_1$ and $d_{4,2} = 0$

$$d_2 < d_3 = d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2\}$$

Therefore, $d_{1,2} = d_{3,2} = d_2$.

(g.a.a) $d_{1,3} = d_3$

$$2d_1 < d_2 + d_3 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$$

Therefore, $d_{2,1} = d_{3,1} = d_1$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 + d_3 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = \frac{4}{3}d_1$, $d_3 = \frac{5}{3}d_1$ and $d_4 = \frac{8}{3}d_1$, the canonical solution is $\boldsymbol{d} = (3, 4, 5, 8)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(3, 4, 5, 8) = = 120$. However, $40 \leq P \leq 60$ and $l \mid P$, a contradiction.

(g.a.b) $d_{1,3} = 0$
Note that

$$d_1 < d_2 = d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1,\, 3d_1\}$$

and so $d_{2,1} = d_1$ or $d_{3,1} = d_1$.

(g.a.b.a) $d_{2,1} = d_1$ and $d_{3,1} = 0$
The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ 0 & d_2 & \bullet & d_4 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_2 + d_4 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 4d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 3, 4)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 4) = 12$. Then, $16 \leq P \leq 26$ and $l|P$,

and therefore $P = 24$. That yields the following matrix:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 2 & 3 & 4 \\ 1 & 0 & 3 & 4 \end{pmatrix}$$

(g.a.b.b) $d_{2,1} = 0$ and $d_{3,1} = d_1$
The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ 0 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_3 \\ 2d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 4d_1$ and $d_4 = 5d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 4, 5)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 4, 5) = 20$. Then, $19 \leq P \leq 31$ and $l|P$, and therefore $P = 20$. That yields the following matrix:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 1 & 2 & 0 & 5 \\ 1 & 0 & 4 & 0 \end{pmatrix}$$

(g.a.b.c) $d_{2,1} = d_{3,1} = d_1$
The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & 0 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_3 \end{aligned}$$

We get $d_2 = 3d_1$, $d_3 = 5d_1$ and $d_4 = 6d_1$, the canonical solution is $\boldsymbol{d} = (1, 3, 5, 6)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then

$l = \text{l.c.m.}(1,3,5,6) = 30$. Then, $25 \leq P \leq 40$ and $l|P$, and therefore $P = 30$. That yields the following matrix:

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 1 & 3 & 5 & 6 \\ 1 & 0 & 5 & 0 \end{pmatrix}$$

(g.b) $d_{4,1} = 0$ and $d_{4,2} = d_2$

Note that

$$d_1 < d_2 \leq d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1} \in \{d_1,\, 2d_1\}$$

and so $d_{2,1} = d_{3,1} = d_1$. On the other hand,

$$d_2 + d_3 > 2d_1 = d_{2,1} + d_{3,1} + d_{4,1} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_1 + d_2\}$$

and so either $d_{1,2} = 0$, or $d_{1,3} = 0$.

(g.b.a) $d_{1,2} = 0$ and $d_{1,3} = d_3$

$$d_2 < d_1 + d_3 = d_{2,1} + d_{2,3} + d_{2,4} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_2,\, 2d_2\}$$

Therefore, $d_{3,2} = d_2$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ 0 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_3 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{3}{2}d_1$, $d_3 = 2d_1$ and $d_4 = \frac{7}{2}d_1$, the canonical solution is $\boldsymbol{d} = (2,3,4,7)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(2,3,4,7) = = 84$. However, $29 \leq P \leq 45$ and $l \mid P$, a contradiction.

(g.b.b) $d_{1,2} = d_2$ and $d_{1,3} = 0$

(g.b.b.a) $d_{3,2} = 0$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & 0 & \bullet & d_4 \\ 0 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_4 \\ d_4 &= d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 5d_1$, so the canonical solution is $\boldsymbol{d} = (1, 2, 3, 5)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 5) = 30$. However, $17 \leq P \leq 28$ and $l|P$, a contradiction.

(g.b.b.b) $d_{3,2} = d_2$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ 0 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 5d_1$ and $d_4 = 7d_1$, so the canonical solution is $\boldsymbol{d} = (1, 2, 5, 7)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 5, 7) = 70$. However, $25 \leq P \leq 40$ and $l \mid P$, a contradiction.

(g.c) $d_{4,1} = d_1$ and $d_{4,2} = d_2$

Note that

$$d_2 < d_3 \leq d_{2,1} + d_{2,3} + d_{2,3} = d_{1,2} + d_{3,2} + d_{4,2} \in \{d_2,\, 2d_2,\, 3d_2\}$$

and so $d_{1,2} = d_2$ or $d_{3,2} = d_2$. Also, note that

$$d_1 < d_2 \leq d_{1,2} + d_{1,3} + d_{1,4} = d_{2,1} + d_{3,1} + d_{4,1}$$

and so $d_{2,1} = d_1$ or $d_{3,1} = d_1$

(g.c.a) $d_{1,2} = d_2$ and $d_{3,2} = 0$, $d_{2,1} = d_1$ and $d_{3,1} = 0$

$$d_2 + d_3 > 2d_1 = d_{2,1} + d_{3,1} + d_{4,1} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_2,\, d_2 + d_3\}$$

Therefore, $d_{1,3} = 0$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ 0 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 6d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 3, 6)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 6) = = 6$. Then, $18 \leq P \leq 30$ and $l \mid P$, and therefore $P = 18$ or $P = 24$ or $P = 30$. That yields the following matrices:

$$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 3 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 3 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

(g.c.b) $d_{1,2} = d_2$ and $d_{3,2} = 0$, $d_{2,1} = 0$ and $d_{3,1} = d_1$

$d_2 + d_3 > 2d_1 = d_{2,1} + d_{3,1} + d_{4,1} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_2,\, d_2 + d_3\}$

Therefore, $d_{1,3} = 0$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ 0 & \bullet & d_3 & 0 \\ d_1 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 2d_2 &= d_3 \\ 2d_3 &= d_1 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 4d_1$ and $d_4 = 6d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 4, 7)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 4, 7) = = 28$. Then, $21 \leq P \leq 35$ and $l \mid P$, and therefore $P = 28$. That yields the following matrices:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 1 & 0 & 4 & 7 \\ 1 & 2 & 4 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 1 & 0 & 0 & 7 \\ 1 & 2 & 4 & 7 \end{pmatrix}$$

(g.c.c) $d_{1,2} = d_2$ and $d_{3,2} = 0$, $d_{2,1} = d_{3,1} = d_1$

(g.c.c.a) $d_{1,3} = 0$ The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 \\ 2d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 3d_1$, $d_3 = 5d_1$ and $d_4 = 9d_1$, so the canonical solution is $\boldsymbol{d} = (1, 3, 5, 9)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 3, 5, 9) = 45$. Then, $28 \leq P \leq 46$ and $l|P$, and therefore $P = 45$. That yields the following matrix:

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 3 & 5 & 0 \\ 1 & 0 & 5 & 9 \\ 1 & 3 & 5 & 9 \end{pmatrix}$$

(g.c.c.b) $d_{1,3} = d_3$
The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & 0 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 + d_3 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_1 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{4}{3}d_1$, $d_3 = \frac{5}{3}d_1$ and $d_4 = 4d_1$, so the canonical solution is $\boldsymbol{d} = (3, 4, 5, 12)$. Put $l := \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(3, 4, 5, 12) = 60$. Then, $44 \leq P \leq 68$ and $l|P$, and therefore $P = 60$. That yields the following matrix:

$$\begin{pmatrix} 0 & 4 & 5 & 0 \\ 3 & 4 & 5 & 0 \\ 3 & 0 & 0 & 12 \\ 3 & 4 & 5 & 12 \end{pmatrix}$$

(g.c.d) $d_{1,2} = 0$ and $d_{3,2} = d_2$, $d_{2,1} = d_1$ and $d_{3,1} = 0$
The matrix D is connected, and therefore $d_{1,3} = d_3$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ 0 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_3 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_2 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = \frac{3}{2}d_1$, $d_3 = 2d_1$ and $d_4 = \frac{9}{2}d_1$, the canonical solution is $\boldsymbol{d} = (2, 3, 4, 9)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(2, 3, 4, 9) = = 36$. Then, $31 \leq P \leq 49$ and $l \mid P$, and therefore $P = 36$. That yields the following matrix:

$$\begin{pmatrix} 2 & 0 & 4 & 0 \\ 2 & 3 & 4 & 0 \\ 0 & 3 & 0 & 9 \\ 2 & 3 & 4 & 0 \end{pmatrix}$$

(g.c.e) $d_{1,2} = 0$ and $d_{3,2} = d_2$, $d_{2,1} = 0$ and $d_{3,1} = d_1$
The matrix D is connected, and therefore $d_{1,3} = d_3$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & d_3 & 0 \\ 0 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

But then $2d_1 = d_3 = 2d_2$, which cannot be.

(g.c.f) $d_{1,2} = 0$ and $d_{3,2} = d_2$, $d_{2,1} = d_{3,1} = d_1$
The matrix D is connected, and therefore $d_{1,3} = d_3$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & 0 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_3 \\ 2d_2 &= d_1 + d_3 \\ 3d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 3d_1$ and $d_4 = 6d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 3, 6)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 3, 6) = 6$. Then, $20 \leq P \leq 32$ and $l \mid P$, and therefore $P = 24$ or $P = 30$. That yields the following matrices:

$$\begin{pmatrix} 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 2 & 3 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 2 & 3 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

(g.c.g) $d_{1,2} = d_{3,2} = d_2$, $d_{2,1} = d_1$ and $d_{3,1} = 0$

$d_2 + d_3 > 2d_1 = d_{2,1} + d_{3,1} + d_{4,1} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_2,\ d_2 + d_3\}$

Therefore, $d_{1,3} = 0$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ 0 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_1 + d_3 \\ 2d_3 &= d_2 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 5d_1$ and $d_4 = 8d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 5, 8)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 5, 8) = = 40$. Then, $26 \leq P \leq 42$ and $l \mid P$, and therefore $P = 40$. That yields the following matrix:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 0 & 2 & 5 & 8 \\ 1 & 2 & 5 & 8 \end{pmatrix}$$

(g.c.h) $d_{1,2} = d_{3,2} = d_2$, $d_{2,1} = 0$ and $d_{3,1} = d_1$

$d_2 + d_3 > 2d_1 = d_{2,1} + d_{3,1} + d_{4,1} = d_{1,2} + d_{1,3} + d_{1,4} \in \{d_2,\ d_2 + d_3\}$

Therefore, $d_{1,3} = 0$. The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ 0 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 2d_1 &= d_2 \\ 3d_2 &= d_3 \\ 2d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 2d_1$, $d_3 = 6d_1$ and $d_4 = 9d_1$, the canonical solution is $\boldsymbol{d} = (1, 2, 6, 9)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 2, 6, 9) = = 18$. Then, $29 \leq P \leq 47$ and $l \mid P$, and therefore $P = 36$. That yields the following matrix:

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 1 & 2 & 6 & 9 \\ 1 & 2 & 6 & 0 \end{pmatrix}$$

(g.c.i) $d_{1,2} = d_{3,2} = d_2$, $d_{2,1} = d_{3,1} = d_1$

(g.c.i.a) $d_{1,3} = 0$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & 0 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

From the matrix D, we obtain the following system of equations:

$$\begin{aligned} 3d_1 &= d_2 \\ 3d_2 &= d_1 + d_3 \\ 2d_3 &= d_1 + d_2 + d_4 \\ d_4 &= d_1 + d_2 + d_3 \end{aligned}$$

We get $d_2 = 3d_1$, $d_3 = 8d_1$ and $d_4 = 12d_1$, the canonical solution is $\boldsymbol{d} = (1, 3, 8, 12)$. Put $l \coloneqq \text{l.c.m.}(\boldsymbol{d})$; then $l = \text{l.c.m.}(1, 3, 8, 12) = 24$. Then, $40 \leq P \leq 64$ and $l|P$, and therefore $P = 48$. That yields the following matrix:

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 8 & 0 \\ 1 & 3 & 8 & 12 \\ 1 & 3 & 8 & 0 \end{pmatrix}$$

(g.c.i.b) $d_{1,3} = d_3$

The matrix D looks as follows:

$$\begin{pmatrix} \bullet & d_2 & d_3 & 0 \\ d_1 & \bullet & d_3 & 0 \\ d_1 & d_2 & \bullet & d_4 \\ d_1 & d_2 & d_3 & \bullet \end{pmatrix}$$

But then

$$3d_1 = d_2 + d_3 > d_1 + d_3 = 3d_2,$$

which cannot be.

5.1.4 Compression graphs for the found IPW–matrices

We will now go through all IPW–matrices of order greater than one (we aew not interested in the trivial solution of size 1) from the previous section. For each of them, we will make the corresponding compression graph using Observation 5.10. We will show that none of the compressed graphs can be "decompressed" into a graph with an injective vertex-periodic waiting path.

(f.c.a.1)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

We have $P = 18$ and $\boldsymbol{p} = (p_1, p_2, p_3, p_4) = (\frac{P}{d_1}, \frac{P}{d_2}, \frac{P}{d_3}, \frac{P}{d_4}) = (18, 9, 6, 3)$. Consider the shortest closed path containing the F_1 loop (the arrow starting and ending at F_1) going through the compressed vertex F_4. The length of the path is ≥ 4, but the vertex in F_4 has period $p_4 = 3 < 4$, which cannot be.

(f.c.a.2)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 12, 8, 4)$. The "decompressed" graph must be doubly-balanced according to Lemma 3.13, so all loops in F_4 goes from a single vertex to the other remaining vertex. Therefore, the shortest closed path going through F_4 and containing the F_1 loop has length ≥ 5, but the vertices in F_4 have period $p_4 = 4 < 5$, which cannot be.

(f.c.b)

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 8 \\ 1 & 3 & 0 & 0 \\ 1 & 3 & 4 & 0 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 8, 6, 3)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the arrow from F_3 to F_1 has length ≥ 4, but the vertex in F_4 has period $p_4 = 3 < 4$, which cannot be.

(g.a.b.a)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 2 & 3 & 4 \\ 1 & 0 & 3 & 4 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 12, 8, 6)$. The "decompressed" graph must be doubly-balanced, therefore all F_4 loops go from a single vertex in F_4 to the other vertex in F_4, and all arrows from this other vertex going into F_3 end at the same vertex (because the "decompressed" graph must be "injective"), so $6 = p_4 | p_3 = 8$, which cannot be.

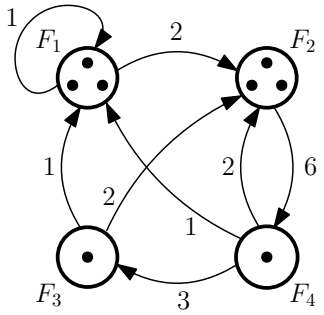

Figure 5.1: (f.c.a.1)

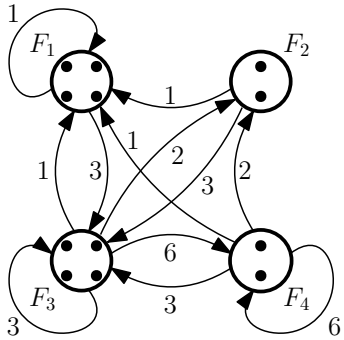

Figure 5.2: (f.c.a.2)

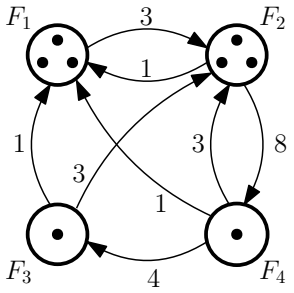

Figure 5.3: (f.c.b)

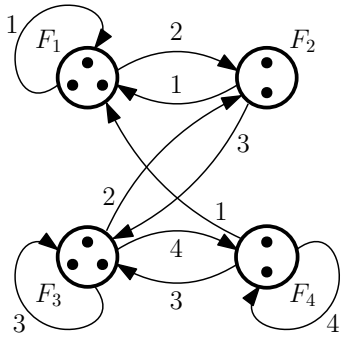

Figure 5.4: (g.a.b.a)

(g.a.b.b)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 1 & 2 & 0 & 5 \\ 1 & 0 & 4 & 0 \end{pmatrix}$$

We have $P = 20$ and $\boldsymbol{p} = (20, 10, 5, 4)$. The "decompressed" graph must be doubly-balanced according to Lemma 3.13, so all arrows from the vertex in F_4 into F_3 end at the same vertex. By Lemma 5.9, $4 = p_4 | p_3 = 5$, which cannot be.

(g.a.b.c)

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 1 & 3 & 5 & 6 \\ 1 & 0 & 5 & 0 \end{pmatrix}$$

We have $P = 30$ and $\boldsymbol{p} = (30, 10, 6, 5)$. Similarly to Section 5.1.4, all arrows from the vertex in F_4 into F_3 end at the same vertex, so $5 = p_4 | p_3 = 6$, which cannot be.

(g.c.a.1)

$$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

We have $P = 18$ and $\boldsymbol{p} = (18, 9, 6, 3)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the arrow from F_4 to F_1 has length ≥ 4, but the vertex in F_4 has period $p_4 = 3 < 4$, which cannot be.

(g.c.a.2)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 3 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 12, 8, 4)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the F_1 loop has length ≥ 5, but the vertex in F_4 has period $p_4 = 4 < 5$, which cannot be.

(g.c.a.3)

$$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 12, 8, 4)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the arrow from F_4 to F_1 has length ≥ 5, but the vertex in F_4 has period $p_4 = 4 < 5$, which cannot be.

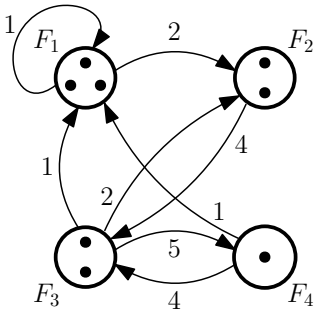

Figure 5.5: (g.a.b.b)

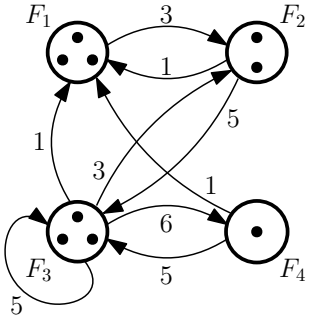

Figure 5.6: (g.a.b.c)

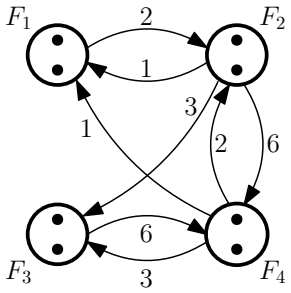

Figure 5.7: (g.c.a.1)

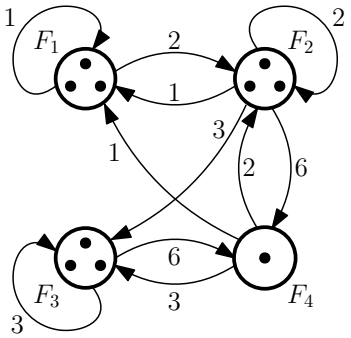

Figure 5.8: (g.c.a.2)

(g.c.a.4)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 3 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

We have $P = 30$ and $\boldsymbol{p} = (30, 15, 10, 5)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the F_1 loop has length ≥ 6, but the vertex in F_4 has period $p_4 = 5 < 6$, which cannot be.

(g.c.b.1)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 1 & 0 & 4 & 7 \\ 1 & 2 & 4 & 0 \end{pmatrix}$$

We have $P = 28$ and $\boldsymbol{p} = (28, 14, 7, 4)$. Similarly to Section 5.1.4, all arrows from the vertex in F_4 into F_3 end at the same vertex, so $4 = p_4 | p_3 = 7$, which cannot be.

(g.c.b.2)

$$\begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 1 & 0 & 0 & 7 \\ 1 & 2 & 4 & 7 \end{pmatrix}$$

We have $P = 28$ and $\boldsymbol{p} = (28, 14, 7, 4)$. Analogically to Section 5.1.4, the shortest path going through F_4 and containing the arrow from F_4 to F_1 has length ≥ 5, but the vertex in F_4 has period $p_4 = 4 < 5$, which cannot be.

(g.c.c.a)

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 3 & 5 & 0 \\ 1 & 0 & 5 & 9 \\ 1 & 3 & 5 & 9 \end{pmatrix}$$

We have $P = 45$ and $\boldsymbol{p} = (45, 15, 9, 5)$. The "decompressed" graph must be doubly-balanced according to Lemma 3.13, so all loops in F_4 goes from a single vertex to the other remaining vertex. The same is true for F_3. Therefore, the shortest closed path going through F_4 and containing the arrow from F_4 to F_1 has length ≥ 6, but the vertices in F_4 have period $p_4 = 5 < 6$, which cannot be.

(g.c.c.b)

$$\begin{pmatrix} 0 & 4 & 5 & 0 \\ 3 & 4 & 5 & 0 \\ 3 & 0 & 0 & 12 \\ 3 & 4 & 5 & 12 \end{pmatrix}$$

We have $P = 60$ and $\boldsymbol{p} = (20, 15, 12, 5)$. The "decompressed" graph must be doubly-balanced, therefore all F_4 loops go from a single vertex in F_4 to the other vertex in F_4, and all arrows from this other vertex going into F_3 end at the same vertex, so $5 = p_4 | p_3 = 12$, which cannot be.

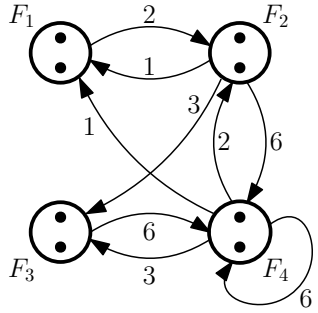

Figure 5.9: (g.c.a.3)

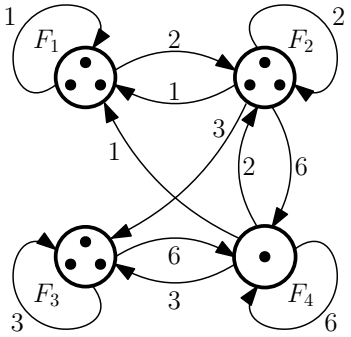

Figure 5.10: (g.c.a.4)

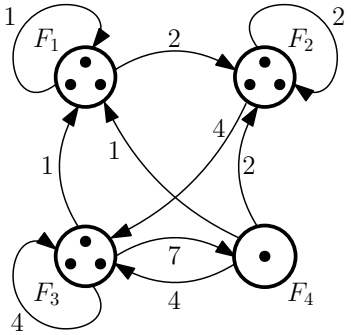

Figure 5.11: (g.c.b.1)

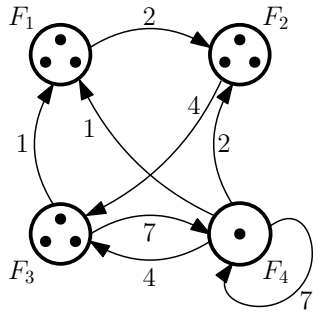

Figure 5.12: (g.c.b.2)

(g.c.d)

$$\begin{pmatrix} 2 & 0 & 4 & 0 \\ 2 & 3 & 4 & 0 \\ 0 & 3 & 0 & 9 \\ 2 & 3 & 4 & 0 \end{pmatrix}$$

We have $P = 36$ and $\boldsymbol{p} = (18, 12, 9, 4)$. Similarly to Section 5.1.4, all arrows from the vertex in F_4 into F_3 end at the same vertex, so $4 = p_4 | p_3 = 9$, which cannot be.

(g.c.f.1)

$$\begin{pmatrix} 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 2 & 3 & 6 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

We have $P = 24$ and $\boldsymbol{p} = (24, 12, 8, 4)$. The "decompressed" graph must be doubly-balanced, therefore all arrows from F_3 into F_2 end at the same vertex, so $8 = p_3 | p_2 = 12$, which cannot be.

(g.c.f.2)

$$\begin{pmatrix} 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 2 & 3 & 6 \\ 1 & 2 & 3 & 6 \end{pmatrix}$$

We have $P = 30$ and $\boldsymbol{p} = (30, 15, 10, 5)$. The "decompressed" graph must be doubly-balanced, therefore all arrows from F_3 into F_2 end at the same vertex, so $10 = p_3 | p_2 = 15$, which cannot be.

(g.c.g)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 5 & 0 \\ 0 & 2 & 5 & 8 \\ 1 & 2 & 5 & 8 \end{pmatrix}$$

We have $P = 40$ and $\boldsymbol{p} = (40, 20, 8, 5)$. The "decompressed" graph must be doubly-balanced, therefore all F_4 loops go from a single vertex in F_4 to the other vertex in F_4, and all arrows from this other vertex going into F_3 end at the same vertex (because the "decompressed" graph must be "injective"), so $5 = p_4 | p_3 = 8$, which cannot be.

(g.c.h)

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 1 & 2 & 6 & 9 \\ 1 & 2 & 6 & 0 \end{pmatrix}$$

We have $P = 36$ and $\boldsymbol{p} = (36, 18, 6, 4)$. Similarly to Section 5.1.4, all arrows from the vertex in F_4 into F_3 end at the same vertex, so $4 = p_4 | p_3 = 6$, which cannot be.

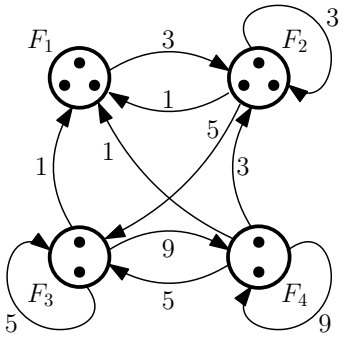

Figure 5.13: (g.c.c.a)

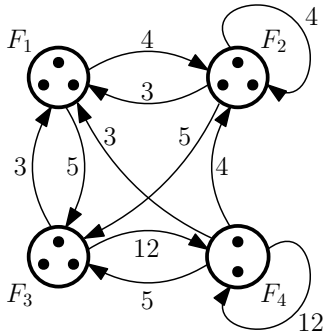

Figure 5.14: (g.c.c.b)

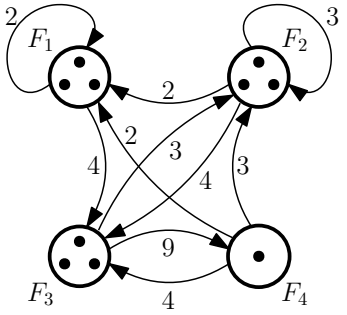

Figure 5.15: (g.c.d)

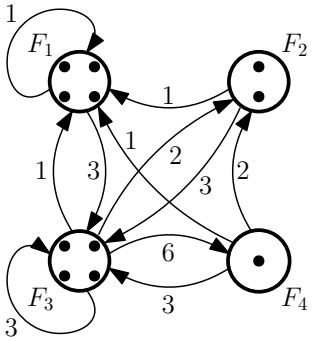

Figure 5.16: (g.c.f.1)

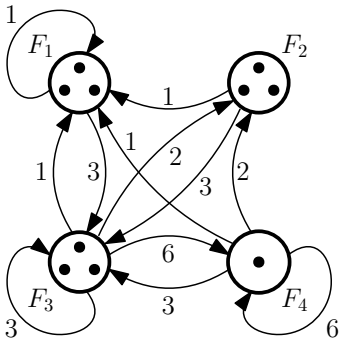

Figure 5.17: (g.c.f.2)

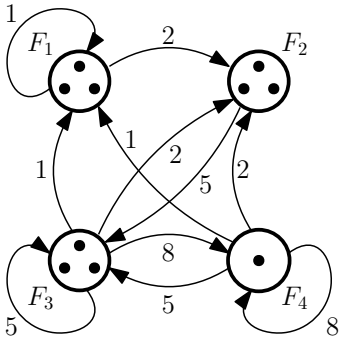

Figure 5.18: (g.c.g)

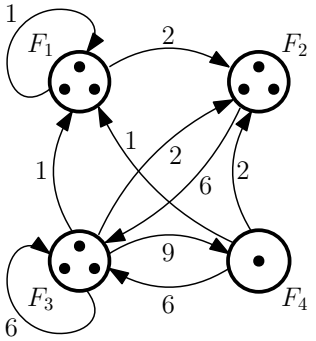

Figure 5.19: (g.c.h)

(g.c.i.a)

$$\begin{pmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 8 & 0 \\ 1 & 3 & 8 & 12 \\ 1 & 3 & 8 & 0 \end{pmatrix}$$

We have $P = 48$ and $\boldsymbol{p} = (48, 12, 6, 3)$. Analogically to Section 5.1.4,

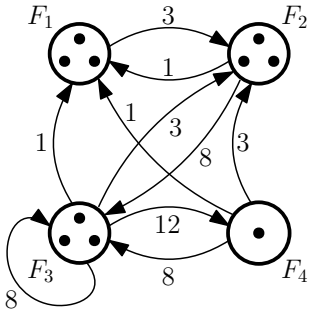

Figure 5.20: (g.c.i.a)

the shortest path going through F_4 and containing the arrow from F_4 to F_1 has length ≥ 4, but the vertex in F_4 has period $p_4 = 3 < 4$, which cannot be.

6. Conclusion

It remains open whether there exists a waiting path (or waiting table) which is injective and periodic. Because the search for such a waiting path is motivated by the eventual existence of corresponding weak inner states in the infinitary version of the RC4 cipher, finding the answer to this question could have a huge impact on usage of the cipher; it could even mean the end of RC4. A special case of the question is if there exists an injective vertex-periodic waiting path (or injective column-periodic waiting table). The answer to this second question remains unknown as well.

This thesis has tried to find an answer to the second question and it was partially successful. By proving that no IPW–matrices of order 2 to 4 exist, we have shown that injective vertex-periodic waiting paths (with more than one vertex) have at least 5 vertices with mutually distinct degrees, and therefore with distinct vertex periods (see Lemma 3.11). Especially, they have at least 5 vertices. Consequently, injective column-periodic waiting tables (with more than one column) have at least 5 columns with mutually distinct column periods. The thesis has also established a new theory which could be used for subsequent searching.

As a follow-up work, IPW–matrices of higher orders could be studied. Searching for these matrices with computer algorithms might help, although I did not manage to find a good use for it with the currentlydeveloped theory. One could also try to come up with better or more strict properties for "generating" matrices than those of IPW–matrices.

Hojsík showed an equivalence relationship between injective periodic waiting tables and weak inner states of the infinitary version of RC4 [1, Proposition 26]. He also showed the equivalence of injective periodic waiting tables and the so-called *matrices induced by equivalences on linearly ordered sets* [1, Proposition 52]. (The fact that these three models are equivalent was also shown by Drápal and Hojsík [2].) We have shown the equivalence of waiting tables and waiting paths introduced in the present work. The problem of weak inner states of RC4 can thus be viewed from many different perspectives, using various models and theories.

I could at least express my personal opinion about the question of existence of injective vertex-periodic waiting paths, the opinion which I have made after months of studying this topic. I believe it is reasonable to expect these kind of waiting paths do not exist. On an intuitive level, the requirement of injectivity prevents the graph to be very symmetric, whereas the requirement of vertex periodicity will rarely be met by non-symmetric graphs. However, I would not be surprised if waiting paths which would be injective and periodic but not vertex-periodic were found in the future.

Bibliography

[1] M. Hojsík. The Stream Cipher RC4. Master's thesis, Charles University in Prague, Faculty of Mathematics and Physics, 2006.

[2] A. Drápal and M. Hojsík. A Riddle Introduced by Persistent States of RC4. Preprint.

[3] I. Mantin. Analysis of the Stream Cipher RC4. Master's thesis, The Weizmann Institute of Science, Faculty of Mathematics and Computer Science, 2001.

[4] S. R. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Schedulling Algorithm of RC4. In *SAC '01 Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 1–24, 2001.

[5] A. Stubblefield, J. Ioannidis, and A. D. Rubin. Using the Fluhrer, Mantin and Shamir Attack to Break WEP. In *Technical Report TD – 4ZCPZZ, AT&T Labs*, 2001.

[6] S. Paul and B. Preneel. Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator. In *Progress in Cryptology – INDOCRYPT 2003: 4th International Conference on Cryptology in India*, 2003.

[7] L. Sladký. Key reconstruction from the inner state of RC4. Master's thesis, Charles University in Prague, Faculty of Mathematics and Physics, 2016.