New Communication Properties of Knödel Graphs

Calin Dan Morosan

A thesis

in

The Department

of

Computer Science

Presented in partial Fulfilment of the Requirements

for the Degree of Master of Computer Science at

Concordia University

Montreal, Quebec, Canada

October 2003

Your file Votre référence
ISBN: 0-612-91088-1
Our file Notre référence
ISBN: 0-612-91088-1

Abstract

New communication properties of Knödel graphs

Calin Dan Morosan

Knödel graphs $W_{d,n}$ of even order n and degree d, $1 \le d \le \lfloor \log_2 n \rfloor$, have been introduced by W. Knödel as a result of their good properties in terms of broadcasting and gossiping information in interconnected networks. In particular, Knödel graphs of order 2^d and degree d have been widely studied because of their remarkable number of vertices to diameter ratio characteristic, which competes with hypercubes and circulant graphs of the same order.

In this thesis, a general definition of the Knödel graphs is given, based on a theorem of isomorphism, and a new family of complete rotations is found. Based on the Cayley graph definition of the Knödel graph, a new hierarchical structure is defined and its rotational properties are studied.

Although Knödel graphs have high symmetry properties, the diameter of the Knödel graphs is known only for $W_{d,2^d}$, and the shortest path problem in logarithmic time, is an open problem. In this thesis, a logarithmic algorithm for the shortest path in $W_{d,2^d}$ is proposed, for a subset of the set of vertices, and a heuristic is given for the remaining vertices. The method described here opens the way of finding the shortest path in general and for solving the general problem of finding the diameter in every Knödel graph.

Acknowledgements

Thank God for giving me *the light* and Dr. Hovhannes A. Harutyunyan for *setting it* in the right angle.

Contents

List of Figures

Chapter I

1 Introduction

The dissemination of information is not a new field but the development of new type of networks as ad-hoc wireless, satellite communications, supercomputers, Internet, etc., brought not only the need for new and powerful algorithms but also for new and reliable network architectures. Among these, the regular networks play a key role in implementing powerful algorithms for routing, broadcasting, parallel and distributed computing.

From the point of view of dissemination of information the Knödel graph stands as one of the most suitable network architectures. Therefore, in this thesis, new properties of Knödel graphs are studied.

1.1 Dissemination of information

1.1.1 Definitions and notations

In order to define the problem of dissemination of information, a network can be modeled as a graph $G = (V, E)$, where V is the set of vertices (nodes) and E is the set of edges (communication lines). Throughout this thesis we will consider only the undirected graphs as model of communication and we will not specify this, unless a possibility of confusion may arise.

Two vertices, $u, v \in V$, are *adjacent* if there is an edge $e \in E$, such that $e = (u, v)$. In this case we say that u and v are *neighbours*. The *degree of a vertex v*, $\delta(v)$, is the number of neighbours of this vertex. The *degree of the graph G*, $\Delta(G)$ is the maximum degree among all vertices: $\Delta(G) = \max\{\delta(v) \mid v \in V\}$. A graph G with all vertices of same degree is called a *regular graph*. A *path P* in a graph G is a sequence of nodes of the form $P = (v_1, v_2, ..., v_n)$, $n > 1$, so that every $(v_i, v_{i+1}) \in E$, $1 \le i < n$. The *length* of the path is the number of edges of P. The length of the shortest path between two vertices v and u, is the *distance* between them, $d(v,u)$. The *diameter* $D(G)$ of the graph G is the maximum distance among distances between all pairs of nodes of the graph: $D_G = \max\{d(v,u) \mid v, u \in V\}$. A graph $G = (V, E)$ is *connected* if there is a path between every two nodes in G.

1.1.2 Models of dissemination of information

Communication in networks can be classified regarding the ability of the vertices to communicate simultaneously with their neighbours in [7]:

- **Processor-bound** called 1-*port* or *whispering*, in which a vertex can communicate only with one neighbour at a time.
- **Link-bound**, called *n-ports* or *shouting*, in which a vertex can call all its neighbours simultaneously.

Obviously, between these two extremes we can have the case in which one vertex can use only a part of its links at a time.

Another issue in characterizing the communication in networks is the necessary

time for a message to be prepared, to travel along an edge and to be received. There are two models widely used in the literature:

- *constant model*, in which the time needed to transmit and receive a message is constant $T = const$.
- *linear model* in which the time needed to communicate is modeled as $T = \beta + L\tau$, where β is the cost of preparing the message, L the length of the message, and τ the propagation time of a data unit length.

In this thesis we consider the 1-port constant model, in which the time of communication between every two vertices is equal to one time unit. This model is simple and can be efficiently utilized when small messages are exchanged and over a small distances. Also we consider here that the whole network acts synchronously, that is, all vertices will transmit and receive at well defined moments of time, called *time-slots*.

A *protocol* or a *communication strategy* in such a network will consist in defining the vertices which will transmit and receive the information, and the time slots for each action.

There are four main problems, regarding information dissemination, widely studied in the literature [6,10]: *broadcasting*, *accumulation*, *gossiping*, and *multicasting*.

- **Broadcast problem**

  Let $G = (V, E)$ be a graph and let v be a vertex in G. Consider now that v knows a piece of information, $I(v)$, which is unknown to all other vertices in $V \setminus \{v\}$. The broadcasting problem is to find a communication strategy, called *broadcast protocol*, such that all nodes from G learn the piece of information $I(v)$ in minimum time possible.

- **Accumulation problem**

  Let $G=(V,E)$ be a graph and let $v \in V$ be a vertex in G. Let each vertex $u \in V$ know a piece of information $I(u)$, and let, for every $x, y \in V$, the piece of information $I(x)$ and $I(y)$ be "disjoint" (independent). The set $I(G)$ where $I(G)=\{I(w) \mid w \in V\}$ is called the *cumulative message* of G. The problem is to find a communication strategy, called *accumulation protocol*, such that the node v learns the cumulative message of G. It is clear that the accumulation problem is the inverse of the broadcast problem.

- **Gossip problem**

  Let $G=(V,E)$ be a graph and let, for all vertices $v \in V$, $I(v)$ be a piece of information residing in v. The gossip problem is to find a communication strategy, called *gossip protocol*, such that all vertices in V learn the whole cumulative message in minimum time possible. A gossip protocol will exhibit also a broadcasting protocol since we can consider that all the vertices from V, except v, know the "null" information and then suspend all the calls from the gossip protocol which carry "null" information.

- **Multicasting problem**

  Let $G=(V,E)$ be a graph, let $v \in V$ be a vertex in G, and let $I(v)$ be a piece of information residing in v. The multicasting problem is to find a communication strategy, called *multicasting protocol*, such that some vertices from G, $u \in S' \subseteq V$, learn the message $I(v)$ in minimum time possible.

1.1.3 Minimum broadcast graph problem

Let $G = (V, E)$ be a graph and v be the originator for the broadcast problem. Let $b(v)$ be the minimum time necessary to broadcast the information $I(v)$ to the rest of vertices of G, called *broadcast time* of v. The *broadcast time of the graph G*, $b(G)$, will be the maximum broadcast time among all vertices of G, that is: $b(G) = \max\{b(v) | v \in V\}$.

The problem of finding the minimum broadcasting time for an arbitrary vertex in an arbitrary graph is NP-complete, as is proved in [8] by showing to be equivalent to another NP-complete problem: the three-dimension matching (3DM) [9].

A broadcast protocol, for a particular vertex v from G, consists of constructing a spanning tree in G, rooted at v. Each edge of this tree can be labelled according to the time-slot in which will be used in order to communicate. If we have d time-slots, and we consider that in each time-slot every informed vertex will announce a new one, the maximum number of informed vertices can be $n = 2^d$. Thus, a natural lower bound for the broadcast time of a graph with n vertices is:

$$b(G) \geq \lceil \log_2 n \rceil \tag{1.1}$$

A graph $G = (V, E)$ with the broadcast time $b(G) = \lceil \log_2 n \rceil$ is called a *broadcast graph*, or shortly, a *bg*. Let us consider now the following problem (*minimum broadcast graph problem*): given a number of vertices n, find a graph G, with minimum number of edges, which has the broadcast time $b(G) = \lceil \log_2 n \rceil$. Such a graph is called *minimum broadcast graph*, or shortly an *mbg*.

The number of edges of a minimum broadcast graph is denoted by $B(n)$, where n represents the number of vertices. There are only two known infinite families of *mbg*'s,

for $n = 2^d$ with $B(2^d) = d2^{d-1}$ and for $n = 2^d - 2$ with $B(2^d - 2) = (d-1)(2^{d-1} - 1)$. The exact value of $B(n)$ is known only for a very limited number of values of $n \leq 63$ [21,42].

Various heuristics and methods have been proposed for obtaining new minimum broadcast graphs or upper bounds for the value of $B(n)$. Some of them are based on compounding previous known broadcast graphs, which consist of taking two or more copies of known minimum broadcast graphs and join some of the non-adjacent vertices [11,15,16,17,18,19,20,28,29]. Other upper bounds for $B(n)$ has been obtained by direct constructions [13,20].

1.2 Knödel graphs survey

Besides hypercubes and recursive circulant graphs, Knödel graphs $W_{d,n}$ of even order n and degree d, $1 \leq d \leq \lfloor \log_2 n \rfloor$, are among the most powerful regular networks from the dissemination of information point of view. They have been introduced by W. Knödel in [1] as a result of their properties regarding broadcasting and gossiping the information in interconnected networks [3], and many of the graphs given later as examples of minimum broadcast (gossiping) graphs [15,14,23] were in fact isomorphic to Knödel graphs [4]. They have been formally defined as follows [2]:

Definition 1 (Knödel graph – one-layer representation)

The Knödel graph $W_{d,n}$ of order n and degree d is the graph $G = (V, E)$ with an even number of vertices, $|V| = n$ and:

$$E = \{(i, j) \mid i + j = 2^r - 1 \bmod n, 0 \leq i, j \leq n-1, 1 \leq r \leq d\} \tag{1.2}$$

We can see from the definition above that Knödel graphs are regular graphs of degree *d*. Throughout this thesis we will refer to this definition as *one-layer representation* (fig. 1) or also "*classic*" representation.

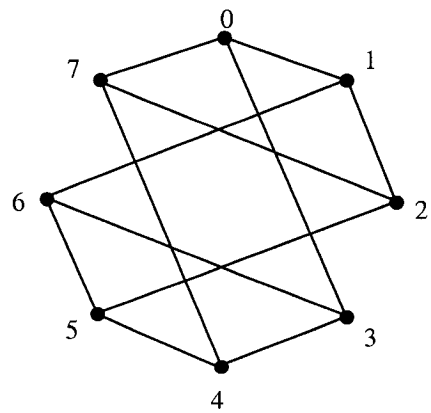

Figure 1 - Knödel graph of dimension 3 and order 8, $W_{3,8}$ – one-layer representation

Table 1 - Broadcast and gossip properties of Knödel graphs

Type of graph	Properties
$W_{k,2^k}$	Minimum broadcast graph [12] Minimum gossip graph [1] Minimum linear gossip graph [2]
$W_{k-1,2^k-2}$	Minimum broadcast graph [15,14] Minimum gossip graph [23] Minimum linear gossip graph [2]
$W_{k-1,2^k-4}$	Minimum gossip graph [23] Minimum linear gossip graph [2]
$W_{k-1,2^k-6}$	Minimum linear gossip graph [2]
$W_{k-2,n}$ $2^{k-1}+2 \le n \le 3 \cdot 2^{k-2}-4$	Broadcast graph [24] Linear gossip graph [25] Gossip graph [24]
$W_{k-1,n}$ $3 \cdot 2^{k-2}-4 \le n \le 2^k-4$	Broadcast graph [24] Linear gossip graph [25] Gossip graph [24]

In particular, for every $n = 2^d$, and for every $n = 2^{d+1} - 2$, Knödel graphs of order n and degree d, turn out to be minimum broadcast, gossip, and linear gossip graphs. Table 1 is a survey of some Knödel graphs and their properties, in terms of broadcasting and gossiping.

From definition 1, the bipartite character of the Knödel graph is not very obvious. We can formally give another definition which is more suitable to exhibit this characteristic:

Definition 2 (Knödel graph – two-layer representation)

The Knödel graph on $n \geq 2$ vertices (n even) and of maximum degree d, $1 \leq d \leq \lfloor \log_2 n \rfloor$ is denoted by $W_{d,n}$. The vertices of $W_{d,n}$ are the pairs (i, j) with $i = 0,1$ and $0 \leq j \leq \frac{n}{2} - 1$, and the set of edges:

$$E = \left\{ ((0,i),(1,j)) \mid j = i + 2^r - 1 \bmod \frac{n}{2}, 0 \leq i, j \leq \frac{n}{2} - 1,\ 0 \leq r \leq d-1 \right\} \qquad (1.3)$$

Throughout this thesis we will refer to this definition as *two-layer representation* (fig. 2).

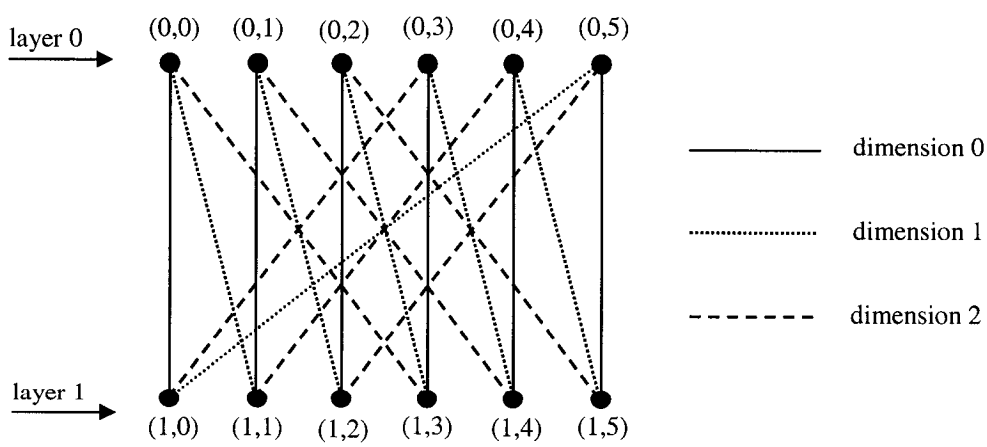

Figure 2 - Knödel graph of dimension 3 and order 12, $W_{3,12}$ – two-layer representation

We can translate the labelling between one-layer representation and two layer representation by following mapping:

$$(0, y) \to (1-2y) \bmod n = i \tag{1.4}$$

$$(1, y') \to 2y' = j \tag{1.5}$$

Indeed, summing i and j we obtain the one-layer definition:

$$i + j = (1 - 2y + 2y') \bmod n$$

$$= (1 - 2y + 2((y + 2^r - 1) \bmod n/2)) \bmod n$$

$$= (2^{r+1} - 1) \bmod n \tag{1.6}$$

We can also define Knödel graphs in terms of Cayley graphs:

Definition 3 (Knödel graphs as Cayley graphs) [27]

For every even n and $1 \le d \le \lfloor \log_2 n \rfloor$, $W_{d,n}$ is a Cayley graph on the semi-direct product $G = Z_2 \times Z_{n/2}$ with the set of generators $S = \{(1,2^i), 0 \le i \le d-1\}$ and the multiplicative law $(x, y)(x', y') = (x + x', y + (-1)^x y')$, where $x, x' \in Z_2$ and $y, y' \in Z_{n/2}$.

Knödel graph has good compound properties. For example we can construct $W_{d+1,2n}$ from two copies W_1 and W_2 of $W_{d,n}$, by the following procedure [26]:

a) Re-label the vertices of W_1:

- $f(0,i) = (0,2i)$ for every $i \in \left[0, \frac{n}{2} - 1\right]$;

- $f(1,i) = (1,2i+1)$ for every $i \in \left[0, \frac{n}{2} - 1\right]$.

b) Re-label the vertices of W_1:

- $f(0,i) = (0,2i+1)$ for every $i \in \left[0, \frac{n}{2} - 1\right]$;

- $f(1,i) = (1,2i+2)$ for every $i \in \left[0, \frac{n}{2} - 1\right]$.

c) Do a perfect matching between the vertices of W_1 and W_2, that is, add the edges $(f(0,i), f(1,i))$, for every $i \in \left[0, \frac{n}{2} - 1\right]$.

We observe that the edges from dimension i in $W_{d,n}$ will become edges of dimension $i + 1$ in $W_{d+1,2n}$ (figure 5). Note that, in particular, if $2n = 2^k$ and $d + 1 = k$, this give a recursive construction of $W_{k,2^k}$ starting with K_2.

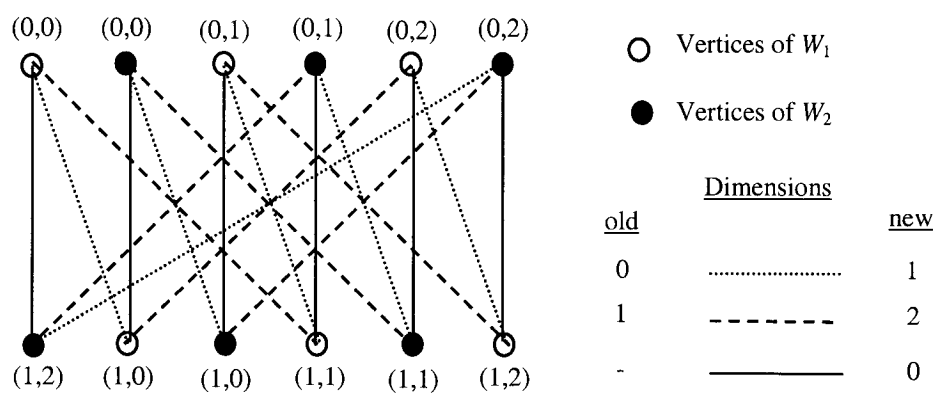

Figure 3 - Constructing $W_{3,12}$ from two copies of $W_{2,6}$

We can extract this compound property from a more general definition:

Definition 4 (Compound graph)

A compound graph of a graph G and a graph H, denoted by $G[H]$, is a graph obtained in the following way: we replace the vertices of G by copies of H, and add edges to some of the vertices of two of these copies iff the corresponding vertices of G are adjacent.

By this definition we observe that $W_{d+1,2n} = K_2[W_{d,n}]$, for every even n and $1 \le d \le \lfloor \log_2 n \rfloor$. In particular, $W_{k,2^k} = K_2[W_{k-1,2^{k-1}}] = \underbrace{K_2[K_2[K_2[\ldots[K_2]]]]}_{k\ -\ times}$ for every $k \ge 2$

Finally, among other properties of Knödel graphs, we mention below some of them, which are connected with this thesis subject:

a) For every $d \geq 2$, the diameter of $W_{d,2^d}$ is $D_d = \left\lceil \frac{d+2}{2} \right\rceil$ [5].

b) For every even n and $1 \leq d \leq \lfloor \log_2 n \rfloor$, $W_{d,n}$ is vertex transitive, since Cayley graphs are vertex transitive.

c) For all even n, such that $n \neq 2^d - 2$, $W_{\lfloor \log_2 n \rfloor, n}$ is not edge transitive [30], while in the case $n = 2^d - 2$, $W_{k-1,2^k-2}$ is edge transitive [27].

We note here that a graph G is vertex transitive if there is a map $f : V(G) \to V(G)$, such that $\{u,v\} \in E(G)$ iff $\{f(u), f(v)\} \in E(G)$.

1.3 Thesis outline

In the first chapter definitions and general properties of Knödel graphs are given. The first section considers the broadcasting and gossiping phenomena, models, and previous results. Section 1.2 is focused on Knödel graphs, their previous definitions, general properties, and previous results, from the point of view of dissemination of information.

In chapter 2 a Knödel graphs drawing theorem is given, a more general definition of Knödel graphs is proposed, based on a theorem of isomorphism, and a previous sufficiency theorem is tested against broadcast protocols in Knödel graphs.

In chapter 3 a new family of complete rotations of Knödel graphs is described, a new hyper structure based on Knödel graphs is defined, and its rotational properties are studied.

In chapter 4 a logarithmic minimum path routing algorithm is proposed, for a subset of vertices in Knödel graphs, and its correctness is proved. Also, a heuristic is described for the remaining vertices and its effectiveness is analyzed.

Chapter II

2 Generalized Knödel graphs

2.1 Drawing Knödel graphs

Drawing graphs, beside embeddings, planarity and patterns in graphs, is a problem often considered in graph theory. It has many applications in geometry, network design, electrical engineering, etc. Also, a "good" drawing could reveal symmetry and isomorphism properties that are not very transparent in an algebraic formalism*.

According to the "classic" definition of Knödel graphs (1-2), the set of edges is defined:

$$E = \{(i, j) \mid i + j = 2^r - 1 \bmod n, 0 \le i, j \le n-1, 1 \le r \le d\} \tag{2.1}$$

In order to draw the Knödel graph of order n and dimension d, one should solve $N = \frac{dn}{2}$ equations of the form:

$$i + j = 2^r - 1 \bmod n,\ 0 \le i, j \le n-1,\ 1 \le r \le d \tag{2.2}$$

For example, for the Knödel graph $W_{d,2^d}$ we have $N = d2^{d-1}$ equation to solve, which is exponential in terms of d. In general, for the Knödel graph $W_{d,n}$, we found that we can do this drawing solving only d equations and then applying a special procedure described in the theorem below:

* I found myself the isomorphism described in the next section just drawing the Knödel graph in a "nice" way

Theorem 1

Let $\{0,1,...,n-1\}$ be the set of vertices of $W_{d,n}$, with $1 \le d \le \lfloor \log_2 n \rfloor$, in this order. We take the following steps:

i) Spread the nodes along a circle line, in order, at equidistance, clockwise.

ii) Find the d pairs of nodes $(0, j)$, with $1 \le j \le 2^d - 1$, which are adjacent in the graph, that is, which respect the relation $0 + j = 2^r - 1$, where $r \in \{1,...,d\}$, and union them.

iii) Draw all possible parallel segments with the segments from step **ii)**, that bind, each, a pair of nodes.

After step **iii)**, the graph is complete.

Proof:

ii) This search is equivalent to finding all the j labelled nodes that respect the general definition of edge set and it takes d steps. After this step we have d edges of form $(0, j)$, more precisely $(0, 2^r - 1)$, with $r \in \{1,...,d\}$.

iii) Let $(0, j)$ be an edge obtained in step **ii)**. Then, all possible pairs of the form $(-p, j+p)$, with $p \in \{-2^{d-1}+1,...,0,1,...,n-2\}$, will satisfy equation (2.2), (all additions and subtractions are done modulo n):

$$(-p) \bmod n + (j + p) \bmod n = j = (2^r - 1) \bmod n, \text{ with } r \in \{1,...,k\} \quad (2.3)$$

At the same time, because we add and subtract the same number p, we move forward or backward along the circle, depending on the p sign, with the same arc length. That means that all the resulted edges $((-p) \bmod n, (j+p) \bmod n)$ will be geometrically parallel each other.

The number of segments generated at step **ii)** is d and the number of parallels

generated at step **iii**), for each initial segment from step **ii**), will be $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ (since n is always even), thus, total number of edges will be $\frac{dn}{2}$ which is the number of edges in our graph $W_{d,n}$. □

The following example illustrates the procedure of drawing for $W_{3,16}$ (figure 4).

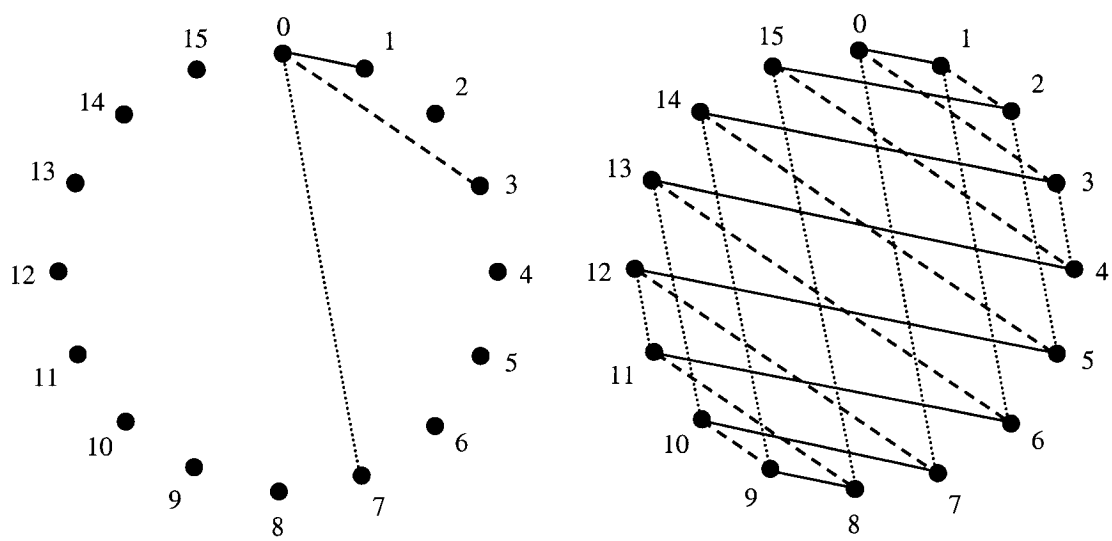

Figure 4 - $W_{3,16}$ after the second step ii) (left) and after the third step iii) (right)

2.2 Previous definitions

In the previous chapter we saw four definitions for the set of edges in Knödel graphs:

– One-layer representation:

$$E = \{(i, j) \mid i + j = 2^r - 1 \bmod n,\ 0 \le i, j \le n-1,\ 1 \le r \le d\} \tag{2.4}$$

– Two-layer representation:

$$E = \left\{ ((0,i),(1,j)) \mid j = i + 2^r - 1 \bmod \frac{n}{2}, 0 \le i, j \le \frac{n}{2} - 1,\ 0 \le r \le d-1 \right\} \tag{2.5}$$

– As Cayley graphs [27]:

$$E = \{ (g, gs) \mid g \in Z_2 \times Z_{n/2}; s \in S \}, \tag{2.6}$$

with $S = \{ (1,2^i) \mid 0 \le i \le \lfloor \log_2 n \rfloor \}$, and the multiplicative law

$$(x,y)(x',y') = (x + x', y + (-1)^x y'), \tag{2.7}$$

where $x, x' \in Z_2$ and $y, y' \in Z_{n/2}$.

– Modified Knödel graphs [3]:

$$E = \left\{ ((0,i),(1,j)) \mid j = i + 2^r \bmod \frac{n}{2}, 0 \le i, j \le \frac{n}{2} - 1,\ 0 \le r \le \lfloor \log_2 n \rfloor \right\} \tag{2.8}$$

2.3 Generalized definition

Let us represent first, in a two-layer representation the same Knödel graph as yields from (2.2) and (2.5), say, for example, for $n = 14$ and $d = 3$ (figure 5):

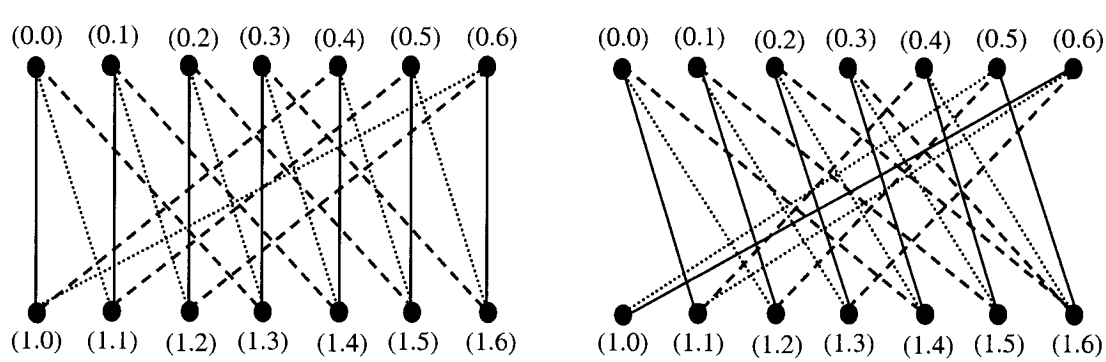

Figure 5 - "Classic" (left) and "modified" (right) Knödel graph on 14 vertices, $W_{3,14}$

Now we shift to the left with one position the vertices from layer 1 in the modified Knödel graph and we set the location of vertex (1,0) in the previous location of (1,6). After that, we do a re-labelling in layer one:

$$(1,i) \rightarrow \left(1,(i-1)\bmod\frac{n}{2}\right) \tag{2.9}$$

We can see the result in figure 6:

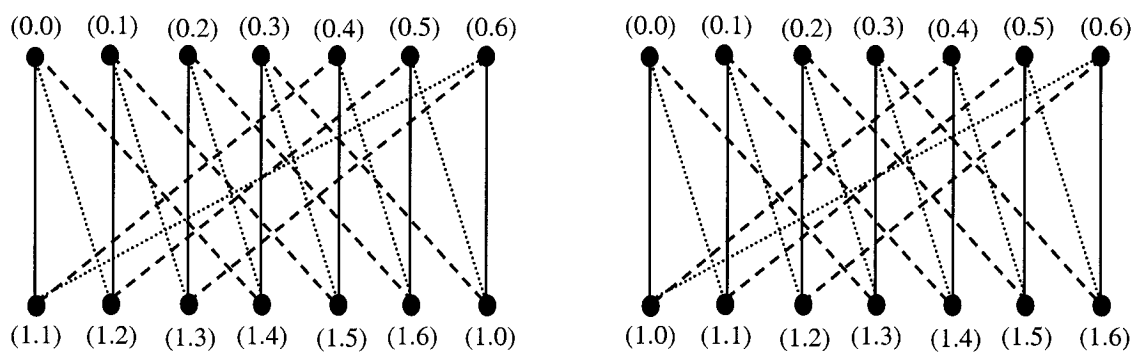

Figure 6 - The modified Knödel graph after "shifting" (left) and re-labelling (right)

We observe that the last figure is identical to the "classic" Knödel graph on the same order and dimension. We can also formally prove the isomorphism between the "classic" and the modified Knödel graph on the same order and dimension using the following vertex mapping in the modified Knödel graph:

$$f(i,j) = \begin{cases} (0,j) \ \ if \ \ i=0 \\ \left(1,(j-1)\bmod\frac{n}{2}\right) \ \ if \ \ i=1 \end{cases} \tag{2.10}$$

This observation suggests a more general definition of the Knödel graphs:

Definition 5 (Generalized Knödel graph; two-layer representation)

The generalized Knödel graph, $GK_{d,n}$, on even order n and dimension d, $1 \le d \le \lfloor \log_2 n \rfloor$, is the graph with the vertices of form (l,j), with $l \in \{0,1\}$ and $0 \le j \le \frac{n}{2}-1$, and the set

of edges:

$$E=\left\{\left((0,i),(1,j)\right)\mid j=i+2^r-s\bmod\frac{n}{2};\ 0\le i,j\le\frac{n}{2}-1;\ 0\le r\le d-1;\ \forall s\in Z\right\} \qquad (2.11)$$

Theorem 2

The generalized Knödel graph $GK_{d,n}$ on even order n and dimension d, $1\le d\le\lfloor\log_2 n\rfloor$, as defined in (2.11), is isomorphic to Knödel graph on same order and dimension.

Proof:

We can do the following mapping that will affect the vertices from layer 1:

$$f(i,j)=\begin{cases}(0,j) & if\ \ i=0\\ \left(1,(j+s-1)\bmod\frac{n}{2}\right) & if\ \ i=1\end{cases} \qquad (2.12)$$

We observe that the re-labelling is consistent since the new labels cover the whole set of vertices from layer 1, $\{0,\ldots,n/2-1\}$, and, after that, we meet the usual Knödel graph edges definition:

$$E=\left\{\left((0,y),\left(1,y+2^r-1\bmod n/2\right)\right)\middle|0\le y\le n/2-1;\ 0\le r\le k-1;\ s\in Z\right\}\ \square \qquad (2.13)$$

As we will see in the next section and, especially, in the next chapter, the modified Knödel graph definition seems to be the most suitable for Knödel graphs study because of the strong connection between binary representation of the vertices labels and the routing problems, including broadcasting and gossiping.

Also, we can extend this general definition (2.11) from the two-layer to one-layer representation:

Definition 6 (Generalized Knödel graph – one-layer representation)

The generalized Knödel graph, $GK_{d,n}$, on even order n and dimension d, $1\le d\le\lfloor\log_2 n\rfloor$,

is the graph with the vertices i, with $0 \le i \le n-1$, and the set of edges:

$$E = \left\{ (i,j) \middle| i + j = 2^r - q \bmod n/2;\ 0 \le i, j \le \frac{n}{2} - 1;\ 1 \le r \le k;\ q \in Z,\ q - odd \right\} \tag{2.14}$$

Indeed, we can map the two-layer representation in one-layer representation as follows:

$$(0, y) \to 1 - 2y \bmod n = i \tag{2.15}$$

$$(1, y') \to 2y' = j \tag{2.16}$$

We can verify now that i and j satisfy the relation (2.11):

$$i + j = (1 - 2y + 2y') \bmod n$$

$$= (1 - 2y + 2((y + 2^r - s) \bmod n/2)) \bmod n.$$

$$= 2^{r+1} - (2s - 1) \bmod n, \text{ with } q = 2s - 1 \tag{2.17}$$

2.4 Broadcasting and gossiping in modified Knödel graphs

One of the main characteristic of the modified Knödel graphs, denoted by KG_n, is that the number of dimensions is $d = \lfloor \log_2 n \rfloor$, where $2^d < n < 2^{d+1}$. It has been introduced in [3] as result of a consistent algebraic description of the gossip and, implicitly, broadcast phenomena, using a special set matrix representation, whose elements are sets. Multiplication of these elements will be replaced by set addition and addition of the resulting products will be replaced by set union. By the definition, two calls in dimensions i and j will be represented by the matrices:

$$M_i = \begin{pmatrix} \{0\} & \{-2^i\} \\ \{2^i\} & \{0\} \end{pmatrix}, \text{ and} \tag{2.18}$$

$$M_j = \begin{pmatrix} \{0\} & \{-2^j\} \\ \{2^j\} & \{0\} \end{pmatrix} \tag{2.19}$$

A sequence of calls in dimensions i and j will be then represented by:

$$M_{i,j} = M_j \cdot M_i = \begin{pmatrix} \{0\} & \{-2^j\} \\ \{2^j\} & \{0\} \end{pmatrix} \begin{pmatrix} \{0\} & \{-2^i\} \\ \{2^i\} & \{0\} \end{pmatrix} =$$

$$= \begin{pmatrix} \{0, 2^i - 2^j\} & \{-2^i, -2^j\} \\ \{2^i, 2^j\} & \{0, 2^j - 2^i\} \end{pmatrix} \tag{2.20}$$

Thus, a set of calls, say in dimensions $i_1, \ldots, i_t$, denoted by $\varpi(i_1, i_2, \ldots, i_t)$, will be a valid gossip (broadcast) protocol if:

$$M(\varpi) = M_{i_t} \cdot M_{i_{t-1}} \cdot \ldots \cdot M_{i_2} \cdot M_{i_1} = \begin{pmatrix} X & X \\ X & X \end{pmatrix}, \text{ where } X = \left\{ 0, 1, \ldots, \frac{n}{2} - 1 \right\} \tag{2.21}$$

Using these properties, in [3] are presented general results regarding gossip (broadcast) protocols for modified Knödel graphs and, implicitly, due to the isomorphism theorem 2, for generalized Knödel graphs on same order and dimension.

We have to mention here some specific notations and properties regarding gossiping (broadcasting) protocols in modified Knödel graphs, consistent with those presented in [3]:

Definition 7 (dimensional gossip protocol)

We will call $s(\pi_1, \pi_2, \ldots, \pi_d)$ a gossip protocol in KG_n, with $d = \lfloor \log_2 n \rfloor$, if, in the t time-slots, with $1 \le t \le d$, every informed vertex will transmit all the messages that it knows to its π_t*-dimensional* neighbour, and, in the last time slot, i.e. time-slot d + 1, every informed vertex will transmit its information to its π_1*-dimensional* neighbour, that is, the

first call will be repeated.

We call here u a π_t*-dimensional* neighbour of a vertex v, if $v = u + 2^t \bmod n/2$ or $u = v + 2^t \bmod n/2$. As we mentioned in section 1.1.2, every gossip protocol can be translated into a broadcast protocol, respecting the same "dimensionality" property as described in the definition above.

Definition 8 (valid permutation)

We will say that $s(\pi_1, \pi_2, ..., \pi_d)$ is a valid gossip (broadcast) protocol, called also a *valid permutation*, in KG_n, with $d = \lfloor \log_2 n \rfloor$, if, after $d + 1$ calls, all the vertices are informed.

The term permutation comes from the fact that $s(\pi_1, \pi_2, ..., \pi_d)$ is a permutation of $(0,1,...,d-1)$. We recall here some of the most important results needed from [3]:

Lemma 1 [3] The permutation $(0,1,...,d-1)$, is a valid permutation for KG_n.

Lemma 2 [3] Every cyclic shift of a valid permutation is also a valid permutation.

Lemma 3 [3] The reverse of every valid permutation is also a valid permutation.

The most general result from [3] is the following theorem, which gives a sufficiency condition for a permutation to be valid:

Theorem 3 [3] The permutation $(\pi_1, \pi_2, ..., \pi_d)$ is a valid permutation for KG_n if:

1) $2^{\pi_d} - 2^{\pi 1}$ is relatively prime to $\frac{n}{2}$, and

2) $\left\{ 2^{\pi_1} - 2^{\pi_2}, 2^{\pi_2} - 2^{\pi_3}, ..., 2^{\pi_{d-1}} - 2^{\pi_d}, 2^{\pi_d} - 2^{\pi_1} \right\} =$

$$= \left\{ 2^{\pi_d} - 2^{\pi_1} \right\} * \left\{ 2^0, 2^1, ..., 2^{d-1} \right\} \tag{2.22}$$

Since condition 1) gives some families of gossip protocols for particular values of n (see theorem 4 from [3]), we found that condition 2) is too strong, even for the well

known gossip (broadcast) protocol $(0,1,...,d-1)$.

Theorem 4

There is no valid gossip (broadcast) protocol that satisfies condition 2) (2.22), if $n \neq 2^{d+1} - 2$.

Proof:

Assume that we found a valid protocol $(\pi_1, \pi_2, ..., \pi_d)$ which satisfies condition 2). Then, by lemma 2, mentioned above, we can assume that $\pi_1 = 0$, since, otherwise we can circularly shift the protocol until $\pi_1 = 0$.

Depending on the value of $\frac{n}{2}$ we distinguish two cases:

Case 1 - $\frac{n}{2}$ even

We can split the condition 2) into two sets, left part, denoted with S_L and right part denoted with S_R. In this case, the left part will be:

$$S_L = \left\{ 2^{\pi_1} - 2^{\pi_2}, 2^{\pi_2} - 2^{\pi_3}, ..., 2^{\pi_{d-1}} - 2^{\pi_d}, 2^{\pi_d} - 2^{\pi_1} \right\} =$$

$$= \left\{ 2^0 - 2^{\pi_2}, 2^{\pi_2} - 2^{\pi_3}, ..., 2^{\pi_{d-1}} - 2^{\pi_d}, 2^{\pi_d} - 2^0 \right\} =$$

$$= \left\{ 1 - 2^{\pi_2}, 2^{\pi_2} - 2^{\pi_3}, ..., 2^{\pi_{d-1}} - 2^{\pi_d}, 2^{\pi_d} - 1 \right\} =$$

$$= \left\{ \underbrace{\frac{n}{2} + 1 - 2^{\pi_2}}_{odd}, 2^{\pi_2} - 2^{\pi_3}, ..., 2^{\pi_{d-1}} - 2^{\pi_d}, \underbrace{2^{\pi_d} - 1}_{odd} \right\} \tag{2.23}$$

According to condition 2), this set must be identical to:

$$S_R = \left\{ 2^{\pi_d} - 2^{\pi_1} \right\} * \left\{ 2^0, 2^1, ..., 2^{d-1} \right\} =$$

$$=\left\{2^{\pi_d}-2^0\right\}*\left\{2^0,2^1,\ldots,2^{d-1}\right\}=$$

$$=\left\{2^{\pi_d}-1\right\}*\left\{2^0,2^1,\ldots,2^{d-1}\right\}=$$

$$=\left\{\left(2^{\pi_d}-1\right)2^0,\left(2^{\pi_d}-1\right)2^1,\ldots,\left(2^{\pi_d}-1\right)2^{d-1}\right\}=$$

$$=\left\{\underbrace{2^{\pi_d}-1}_{odd},\left(2^{\pi_d}-1\right)2^1,\ldots,\left(2^{\pi_d}-1\right)2^{d-1}\right\} \tag{2.24}$$

We obtain a contradiction since S_L has two odd members and S_R has only one.

Case 2 - $\frac{n}{2}$ odd

We will split again the condition 2) into two sets, left part, denoted with S_L and right part denoted with S_R. In this case, the right part will remain the same as in previous case. The left part can be written as:

$$S_L=\left\{2^{\pi_1}-2^{\pi_2},2^{\pi_2}-2^{\pi_3},\ldots,2^{\pi_{d-1}}-2^{\pi_d},2^{\pi_d}-2^{\pi_1}\right\}=$$

$$=\left\{2^0-2^{\pi_2},2^{\pi_2}-2^{\pi_3},\ldots,2^{\pi_{d-1}}-2^{\pi_d},2^{\pi_d}-2^0\right\}=$$

$$=\left\{\underbrace{1-2^{\pi_2}}_{odd<0},2^{\pi_2}-2^{\pi_3},\ldots,2^{\pi_{d-1}}-2^{\pi_d},\underbrace{2^{\pi_d}-1}_{odd>0}\right\}=$$

$$=\left\{\underbrace{\frac{n}{2}+1-2^{\pi_2}}_{even},2^{\pi_2}-2^{\pi_3},\ldots,2^{\pi_{d-1}}-2^{\pi_d},\underbrace{2^{\pi_d}-1}_{odd>0}\right\} \tag{2.25}$$

Since the right part, S_R, has only one odd member, the only possible case is when all the members of S_L, except the last one, are even, thus, positive. That means:

$$2^{\pi_2}-2^{\pi_3}>0$$

$$2^{\pi_3}-2^{\pi_4}>0$$

$$\ldots$$

$$2^{\pi_{d-1}} - 2^{\pi_d} > 0 \tag{2.26}$$

Since $\pi_1 = 0$, we must have:

$$\pi_2 > \pi_3 > \ldots > \pi_{d-1} > \pi_d \tag{2.27}$$

Because $\{\pi_1, \pi_2, \ldots, \pi_d\} = \{0, 1, \ldots, d-1\}$, the only possibility is:

$$\pi_1 = 0;$$

$$\pi_2 = d - 1;$$

$$\ldots$$

$$\pi_d = 1 \tag{2.28}$$

Let us assume that the protocol $(0, d-1, d-2, \ldots, 1)$ satisfy condition 2). The left part:

$$S_L = \{ 2^0 - 2^{d-1}, 2^{d-1} - 2^{d-2}, \ldots, 2^2 - 2^1, 2^1 - 2^0 \} =$$

$$= \{ 2^0 - 2^{d-1}, 2^{d-2}, \ldots, 2^1, 2^0 \} \tag{2.29}$$

The right part will be:

$$S_R = \{ 2^1 - 2^0 \} * \{ 2^0, 2^1, \ldots, 2^{d-1} \} =$$

$$= \{ 2^0, 2^1, \ldots, 2^{d-1} \} \tag{2.30}$$

Since we must have, $S_L = S_R$:

$$\{ 2^0 - 2^{d-1}, 2^{d-2}, \ldots, 2^1, 2^0 \} = \{ 2^0, 2^1, \ldots, 2^{d-1} \} \tag{2.31}$$

That is equivalent to the following set of equations:

$$2^0 - 2^{d-1} = 2^{d-1} \bmod \frac{n}{2} \tag{2.32}$$

$$\frac{n}{2} + 1 - 2^{d-1} = 2^{d-1} \tag{2.33}$$

$$\frac{n}{2} = 2^d - 1 \tag{2.34}$$

$$n = 2^{d+1} - 2 \tag{2.35}$$

But this contradicts the theorem's hypothesis which states that $n \neq 2^{d+1} - 2$. Thus, there is no valid protocol that will pass condition 2) from theorem 3. □

We have to mention here that for the case $n = 2^{d+1} - 2$, theorem 5 from [3] states a strong result, based on the same algebraic description of modified Knödel graphs:

Theorem 5 [3]

The only valid permutations for $KG_{2^{d+1}-2}$ are the cyclic shifts (and reverses) of the form $0, k, 2k, \ldots, (d-1)k$, where $2^k - 1$ is relatively prime to $2^d - 1$.

It still remains open the interesting problem of finding a necessary condition for a gossip (broadcast) scheme to be valid, based on this algebraic description of dissemination of information in Knödel graph. Also, an interesting problem remains open, if such a description can be applied to Knödel graphs on smaller dimensions.

Chapter III

3 Algebraic properties of Knödel graphs

3.1 Complete rotations in Knödel graphs

Knödel graphs, as Cayley graphs, present some general properties of symmetry. One of these properties, called complete rotation, has been used in [31] and [32] to derive algorithms or properties of the underlining graphs, such as optimal gossip protocols and construction of edge disjoint spanning trees.

The notion of rotation in graph theory was first introduced in the context of embeddings (see [33], [34], and a good survey can be also found in [35]), and it consists of a special graph automorphism generated by a cyclic permutation of all the vertices adjacent to a vertex, corresponding, in the Cayley graphs, to a cyclic permutation of the elements of the generator set.

In order to extend the notion of complete rotation and to present a new family of complete rotation over the Knödel graphs, we give some definitions below:

Definition 9 [27] (Cayley graph)

Let G be a group with unit I and S a subset such that $I \notin S$ and the inverse of elements of S belong to S. The Cayley graph $Cay(G,S)$ is the graph with vertex set G and with edges set $\{(g,gs) \mid g \in G, s \in S\}$.

We can see that $W_{d,n} = Cay(Z_2 \times Z_{n/2}, S)$ with $S = \{(1,2^i) \mid 0 \le i \le d-1\}$. Also we mention that if G is generated by S, denoted by $G = \langle S \rangle$, then $Cay(G,S)$ is connected.

Definition 10 [27] (complete rotation)

Let $Cay(G,S)$ be a Cayley graph with $G=\langle S\rangle$. A mapping $\varpi: G \to G$ is a complete rotation of $Cay(G,S)$ if it is bijective and satisfies the following two properties for some ordering of $S=\{s_i \mid 0 \le i \le d-1\}$:

$$\varpi(I)=I \tag{3.1}$$

$$\varpi(gs_i)=\varpi(g)s_{i+1}, \text{ for every } x \in G \text{ and } i \in Z_d \tag{3.2}$$

It has been found in [27] that the Knödel graph $W_{d,2^{d+1}-2}$ has the following complete rotation:

$$\varpi(x,y)=(x,2y) \tag{3.3}$$

Indeed, for the natural order of $S=\{(1,2^0),(1,2^1),\ldots,(1,2^{d-1})\}$, we have:

$$\varpi(0,0)=(0,0), \text{ and} \tag{3.4}$$

$$\begin{aligned}\varpi(gs_i)&=\varpi\left((x,y)(1,2^i)\right)=\varpi\left(y+1,x+(-1)^y 2^i\right)=\\&=\left(y+1,2x+(-1)^y 2^{i+1}\right)=(x,2y)(1,2^{i+1})=\varpi(x,y)s_{i+1}\end{aligned} \tag{3.5}$$

We can generalize this result to a family of complete rotations of Knödel graphs, under certain conditions:

Theorem 6

The mapping $\varpi: W_{d,n} \to W_{d,n}$ defined as $\varpi(x,y)=(x,2^p y)$ is a complete rotation of $W_{d,n}$ if p is relatively prime to d, and 2^p is relatively prime to $n/2$.

Proof:

First we have to find an appropriate order for set S. For this, we consider the following set S':

$$S' = \left\{ \left(1, 2^{ip \bmod d}\right) \middle| \, 0 \le i \le d-1 \right\} \tag{3.6}$$

To show that $S = S'$, we have to prove that:

$$\{0,1,\ldots,d-1\} = \{0 \cdot p \bmod d,\ 1 \cdot p \bmod d, \ldots,\ (d-1)p \bmod d\} \tag{3.7}$$

Assume that there exist i and j, $1 \le i, j \le d-1$, with $i \ne j$, such that:

$$ip \bmod d = jp \bmod d \tag{3.8}$$

$$(i-j)p \bmod d = 0 \tag{3.9}$$

Since $i - j \ne d$, and p and d are relatively prime then $i = j$ (contradiction). Thus, the two sets must have the same cardinality and, by the pigeonhole principle they must be the same.

The condition from (3.1) is always satisfied. Let us verify condition (3.2):

$$\varpi(gs_i) = \varpi\left((x,y)\left(1, 2^{ip \bmod d}\right)\right) = \varpi\left(y+1, x + (-1)^y\, 2^{ip \bmod d}\right) =$$

$$= \left(y+1, 2^p x + (-1)^y\, 2^{(i+1)p \bmod d}\right) = \left(x, 2^p y\right)\left(1, 2^{(i+1)p \bmod d}\right) = \varpi(x,y)s_{i+1} \tag{3.10}$$

We can prove the injection by contradiction. Assume that exist there are g_1 and g_2 in $W_{d,n}$ such that $g_1 \ne g_2$, with and $\varpi(g_1) = \varpi(g_2)$. Thus, we have:

$$\left(2^p x_1, y_1\right) = \left(2^p x_2, y_2\right) \tag{3.11}$$

$$2^p x_1 = 2^p x_2 \bmod \frac{n}{2} \tag{3.12}$$

$$2^p (x_1 - x_2) = 0 \bmod \frac{n}{2} \tag{3.13}$$

Because 2^p is relatively prime to $\frac{n}{2}$ by hypothesis, and $x_1 - x_2 \ne \frac{n}{2}$, we may conclude that $x_1 = x_2$. Since $y_1 = y_2$, we obtain $g_1 = g_2$ (contradiction).

To show the surjection, we have to show that for every $g=(x,y)\in W_{d,n}$, there exist $g'=(x',y')\in W_{d,n}$, such that $\varpi(g')=g$. But this is obvious since, according to the definition of Cayley graphs, we can label the edges according to the set of generators. Because the Knödel graphs are regular, each vertex has d incident edges, labelled, in this case, by $\{0, p \bmod d,..., (d-1)p \bmod d\}$. Thus, g' will be the vertex from the opposite layer connected with g by the edge labelled " $p \bmod d$ ". □

We mentioned that, in [27], the $\varpi(x,y)=(x,2y)$ complete rotation of $W_{d,n}$ has been proved for $n=2^k-2$ and $d=k-1$. Based on theorem above, we can extend this particularly complete rotation for every $d>1$:

Corollary 1

The mapping $\varpi: W_{d,n}\to W_{d,n}$ defined as $\varpi(x,y)=(x,2y)$ is a complete rotation of $W_{d,n}$ if $n/2$ is odd.

Proof:

Considering $p=1$ in theorem 4, the second condition from the hypothesis imposes that 2 to be relatively prime to $\frac{n}{2}$, which is equivalent to condition $\frac{n}{2}$ - odd. □

An interesting question remains open if these extensions of the complete rotations in Knödel graphs of every order could yield to new gossip and broadcast protocols since in [3] has been proved that, for $n=2^{d+1}-2$, the only valid protocol will be of form $(0,p,2p,...,(d-1)p)$, where p is relatively prime to d and, for all $n<2^{d+1}-2$, the protocol $(0,1,2,...,d-1)$ is a valid protocol.

3.2 Hyper-Knödel graphs

As it is mentioned in chapter 1, one method to obtain new broadcast graphs is by compounding known broadcast graphs using different methods: perfect matching, vertex cover matching, etc. In this section it is proposed a new structure based on Knödel graphs, which preserve some of the basic Knödel graphs properties, in particular, the complete rotation.

For the beginning, as a particular case, let us consider the Knödel graph $W_{d,n}$ in a two-layer representation and defined as $Cay(Z_2 \times Z_{n/2}, S)$, with $S = \{(1,2^i) | 0 \le i \le d-1\}$. For example, the vertex $(0,0)$, from the layer 0, will be connected with the vertices $\{(1,2^0),(1,2^1),...,(1,2^{d-1})\}$, from the layer 1. Take now $n/2$ copies of $W_{d,n}$ and add to the end of the old label a number between 0 and $\frac{n}{2}-1$, corresponding to the new level. Connect the vertex (x,y,z) with all vertices (x',y,z') such that $z' = z + (-1)^x 2^i$, where $0 \le i \le d-1$. We will call this, the 2-hyper Knödel graph, denoted by $2HW_{d,n}$.

It turns out that this structure is also a Cayley graph $Cay(Z_2 \times Z_{n/2} \times Z_{n/2}, S)$, where the generators set is:

$$S = \left\{ s_{i,j} \left| \begin{array}{l} s_{i,j} = (1,2^i,0) \; if \;\; j=0 \\ s_{i,j} = (1,0,2^i) \; if \;\; j=1 \end{array} \right. and \; 0 \le i \le d-1 \right\}, \tag{3.14}$$

and the composition law is:

$$(x,y,z)(x',y',z') = (x+x', y+(-1)^x y', z+(-1)^x z') \tag{3.15}$$

As an example, you can see in figure 7 the $2HW_{2,6}$ layout and some representative edges.

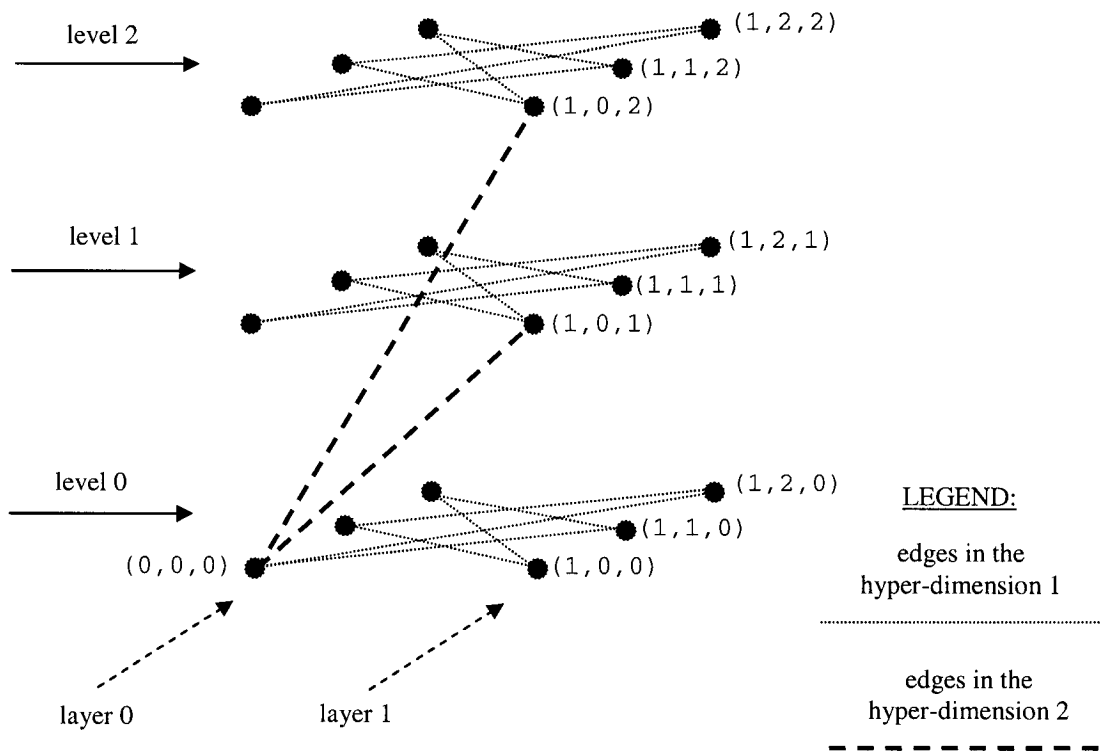

Figure 7 - The $2HW_{2,6}$, 2-hyper Knödel graph and some representative edges

Following the definition of $2HW_{d,n}$ we can generalize this structure for h hyper dimensions:

Definition 11 (hyper Knödel graph)

The h-Knödel graph denoted by $hHW_{d,n}$ of order n and dimension d, with n-even and $1 \le d \le \lfloor \log_2 n \rfloor$, is defined as $Cay\left(Z_2 \times (Z_{n/2})^h, S\right)$, where the generators set is:

$$S = \left\{ s_{\alpha,\beta} \middle| s_{\alpha,\beta} = \left(1,0,\ldots,\underbrace{2^{\alpha}}_{\beta},\ldots,0\right) \quad 0 \le \alpha \le d-1;\ 0 \le \beta \le h-1 \right\}, \tag{3.16}$$

and the composition law is:

$$(x, y_0,\ldots, y_{h-1})(x', y_0',\ldots, y'_{h-1}) = \left(x + x', y_0 + (-1)^x y'_0,\ldots, y_{h-1} + (-1)^x y'_{h-1}\right) \tag{3.17}$$

with $x, x' \in Z_2$ and $y_1,\ldots, y_h, y'_1,\ldots, y'_h \in Z_{n/2}$.

We denote here $(Z_{n/2})^h = Z_{n/2} \times \ldots \times Z_{n/2}$, h times.

Let us note that, in particular, for $Cay\left(Z_2 \times (Z_{n/2})^h, S\right)$, the set of generators can be also written as:

$$S = \left\{ s_i \middle| s_i = \left(1,0,\ldots,\underbrace{2^\beta}_{\alpha},\ldots,0\right),\ \alpha = \left\lfloor \frac{i}{d} \right\rfloor \ and\ \beta = i \bmod d;\ 0 \le i \le hd-1 \right\}, \quad (3.18)$$

where α represents the position of 2^β in the sequence $\left(0,\ldots,2^\beta,\ldots,0\right)$ starting with position 0 from the left side.

3.3 Rotational properties of the hyper Knödel graphs

Using the same technique as in section 3.1 we can find a complete rotation for the hyper Knödel graph. First we have to define an appropriate order for the set of generators which is different as that given in 3-16 and 3-18:

$$S = \left\{ s_i \middle| s_i = \left(1,0,\ldots,\underbrace{2^\beta}_{\alpha},\ldots,0\right),\ \beta = \left\lfloor \frac{i}{h} \right\rfloor \ and\ \alpha = i \bmod h;\ 0 \le i \le hd-1 \right\} \quad (3.19)$$

Now we can define a complete rotation Ω for the new structure:

Theorem 7

The mapping $\Omega : hW_{d,n} \to hW_{d,n}$, defined as $\Omega(x, y_0,\ldots, y_{h-1}) = (x, 2y_{h-1}, y_0,\ldots, y_{h-2})$, with the generator set as in 3-19, is a complete rotation of $hW_{d,n}$.

Proof:

Considering $g \in hW_{d,n}$, let us verify condition 3-2:

$$\Omega(gs_i) = \Omega\left((x, y_0,\ldots, y_{h-1})\left(1,0,\ldots,\underbrace{2^\beta}_{\alpha},\ldots 0\right)\right) =$$

$$= \Omega\left(x, y_0, \ldots, \underbrace{y_\alpha + (-1)^x 2^\beta}_{\alpha}, \ldots, y_{h-1} \right) =$$

$$= \left(x, 2y_{h-1}, y_0, \ldots, \underbrace{y_\alpha + (-1)^x 2^\beta}_{\alpha+1}, \ldots, y_{h-2} \right) =$$

$$= \left(x, 2y_{h-1}, y_0, \ldots, y_{h-2} \right) \left(1, 0, \ldots, \underbrace{2^\beta}_{\alpha+1}, \ldots 0 \right) =$$

$$= \Omega\left(x, y_0, \ldots, y_{h-1} \right) \left(1, 0, \ldots, \underbrace{2^\beta}_{\alpha+1}, \ldots 0 \right) = \Omega(g) s_{i+1} \tag{3.20}$$

The injection can be similarly proven as in theorem 4 and the surjection is a direct consequence of edge labelling in Cayley graphs. □

This rotational property can be extended in a similar manner as in theorem 4 to $\Omega(x, y_0, \ldots, y_{h-1}) = (x, 2^p y_{h-1}, y_0, \ldots, y_{h-2})$ whenever p is relatively prime to d, and 2^p is relatively prime to $n/2$, with an appropriate order relation for the set of generators.

We note that this structure also presents interesting partial rotations for each hyper-dimension, similar to the rotations around the axes in the 3-dimensional space geometry.

We have to mention that the structure can be degenerated, preserving its property as Cayley graph but not the property of complete rotation:

Definition 12 (Degenerated hyper Knödel graph)

The degenerated Knödel graph denoted by $hHW^{d_0,\ldots,d_{h-1}}_{n_0,\ldots,n_{h-1}}$ of order $(n_0, \ldots, n_{h-1})$ and dimension $(d_0, \ldots, d_{h-1})$, with n_i-even and $d_i \geq 1$, $0 \leq i \leq h-1$, is defined as:

$Cay\left(Z_2 \times Z_{\frac{n_0}{2}} \times \ldots \times Z_{\frac{n_{h-1}}{2}}, S \right)$, where the generators set is:

$$S = \left\{ s_{\alpha,\beta} \middle| s_{\alpha,\beta} = \left(1,0,\ldots,\underbrace{2^{\alpha_i}}_{\beta},\ldots,0\right) \quad 0 \le \alpha_i \le d_i - 1;\ 0 \le \beta \le h-1;\ 0 \le i \le h-1 \right\} \tag{3.21}$$

and the composition law:

$$\left(x, y_0, \ldots, y_{h-1}\right)\left(x', y_0', \ldots, y'_{h-1}\right) = \left(x + x', y_0 + (-1)^x y'_0, \ldots, y_{h-1} + (-1)^x y'_{h-1}\right) \tag{3.22}$$

with $x, x' \in Z_2$ and $y_i, y'_i \in Z_{n_i/2}$, $0 \le i \le h-1$.

Chapter IV

4 Shortest path problem in Knödel graphs

4.1 Problem description

Let $Cay(G,S)$ be a Cayley graph over a group G, with the set of generators S, and $g, g' \in G$ two vertices. If $g' = gs_1s_2...s_t$ with $s_i \in S$, $1 \le i \le t$, then the sequence $s_1, s_2, ..., s_t$ defines a path from vertex g to vertex g', with the edges labelled by $s_1, s_2, ..., s_t$ [35]. Thus, finding a path from g to g' is equivalent to finding a path from $g^{-1}g' = s_1s_2...s_t$ to I. This problem is equivalent to the *minimal word problem* in groups: for a given element $g \in G$, find $s_1, s_2, ..., s_t$ with $s_i \in S$, $1 \le i \le t$, and t minimal, such that $gs_1s_2...s_t = I$. This problem has been proven to be NP-complete in [36] if the set of generators is not fixed in advance.

Although Knödel graphs have been introduced 28 years ago as an interconnection network, its diameter is not known in general. In particular, for 2^d vertices and degree d, it has been proven recently in [5] that $D\left(W_{d,2^d}\right) = \left\lceil \frac{d+2}{2} \right\rceil$. Their proof method (by contradiction) does not yield an algorithm for computing the minimum path between two vertices in $W_{d,2^d}$, and hence the problem of finding such a path remains open.

In general, let $\Gamma = Cay(G,S)$ be a Cayley graph of order $n = 2^d$ and degree d. Since Γ is vertex transitive, the minimum path between every two vertices and, implicitly, the diameter can be obtained by constructing a breath-first search tree from the

vertex I. This can be computed in $O(dn) = O(d2^d)$ time complexity and with the same space complexity, which remains exponential in terms of d. In section 4.4 we present an algorithm for finding the minimum path between vertex (0,0) and a subset of vertices in $W_{d,2^d}$ in $O(d)$ time and space complexity.

4.2 Paths in Knödel graphs and binary representation of vertices

In the following descriptions we will use the generalized definition of the Knödel graphs as described in definition 5 (2.11) with $s = 0$, where the set of vertices is described by:

$$E = \left\{ ((0,i),(1,j)) \mid j = i + 2^r \bmod \frac{n}{2};\ 0 \le i, j \le \frac{n}{2} - 1;\ 0 \le r \le d-1 \right\} \tag{4.1}$$

This two-layer representation has the great advantage of dealing only with powers of two. Every time we move from layer 0 to layer 1 we have to add to the vertex label a power of two and every time when we move from layer 1 to layer 0 we have to subtract from the vertex label a power of two, corresponding to the dimension of the edge. Note that all the additions and subtractions are done modulo $n/2$ and the labels go, in each layer, from 0 to $\frac{n}{2} - 1$.

For example, in figure 8, for $W_{4,16}$, in order to move from vertex $(0,0)$ to $(1,2)$ we have to add 2^1 (i.e. $0 + 2^1 = 2$) and to move from $(1,2)$ to $(0,2)$ we have to subtract 2^3 (i.e. $(2 - 2^3) \bmod 8 = (-6) \bmod 8 = 2$). Also, in order to move from vertex $(0,0)$ to $(1,0)$ we have to add 2^3 (i.e. $(0 + 2^3) \bmod 8 = 0$) and to move from $(1,0)$ to $(0,4)$ we have to

subtract 2^2 (i.e. $(0-2^2)\bmod 8=(-4)\bmod 8=4$).

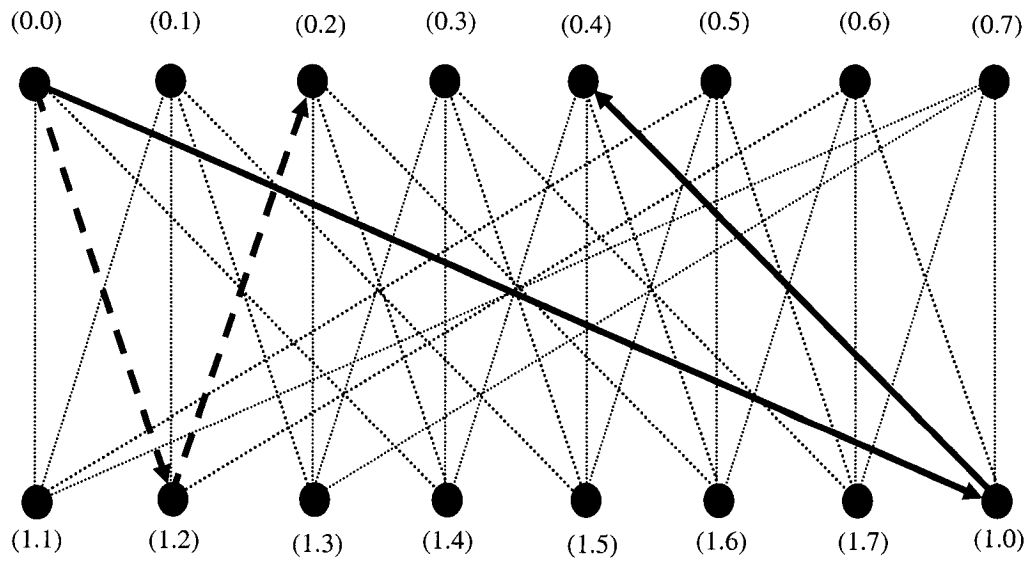

Figure 8 - Two paths in $W_{4,16}$: $(0,0)\to(1,2)\to(0,2)$ and $(0,0)\to(1,0)\to(0,4)$

We generalize the path expression in Knödel graphs in the following lemma:

Lemma 4

Let be $W_{d,2^d}$ the Knödel graph of order 2^d and dimension *d*. Then, there exist *t* and *w*, with $0\le t\le d$, and $0\le w\le d-1$, such that:

1) Any vertex from layer 0, $(0,v)\neq(0,0)$, can be written as: $v=\left(\sum_{r=1}^{t}\left(2^{i_r}-2^{j_r}\right)\right)\bmod 2^{d-1}$,

with $0\le i_r, j_r\le d-1$ and $i_r\neq j_r$.

2) Any vertex from layer 1, $(1,v)$, can be written as $v=\left(2^w+\sum_{r=1}^{t}\left(2^{i_r}-2^{j_r}\right)\right)\bmod 2^{d-1}$,

with $0\le i_r, j_r, w\le d-1$ and $i_r\neq j_r$.

Proof:

Let $b(v)$ be the binary representation of *v*. Note than $v<2^{d-1}$ and we need maximum

$d-1$ digits to write $b(v)$.

1) If v is in layer 0, we can write it as:

$$v=\left(\sum_{r=1}^{t}2^{m_r}\right)\bmod 2^{d-1}=\left(\sum_{r=1}^{t}\left(2^{m_r+1}-2^{m_r}\right)\right)\bmod 2^{d-1} \tag{4.2}$$

1) If v is in layer 1, we can write it as:

$$v=\left(\sum_{r=1}^{t}2^{m_r}\right)\bmod 2^{d-1}=\left(2^{m_t}+\sum_{r=1}^{t-1}\left(2^{m_r+1}-2^{m_r}\right)\right)\bmod 2^{d-1} \quad \square \tag{4.3}$$

We will call this kind of decomposition, in which the number of positive powers of two is equal with the number of negative powers of two, *symmetric decomposition*, respective *quasi-symmetric decomposition* for (4.3). We have to stress here that, in general, the symmetric decomposition is not unique.

For example, $6=\overline{0110}_2$ can have the following symmetric decompositions: $6=\left(2^3-2^2\right)+\left(2^2-2^1\right)$ or $6=\left(2^3-2^1\right)$. Each of them corresponds to a path in the Knödel graph $W_{4,16}$, as you can see in the figure below:

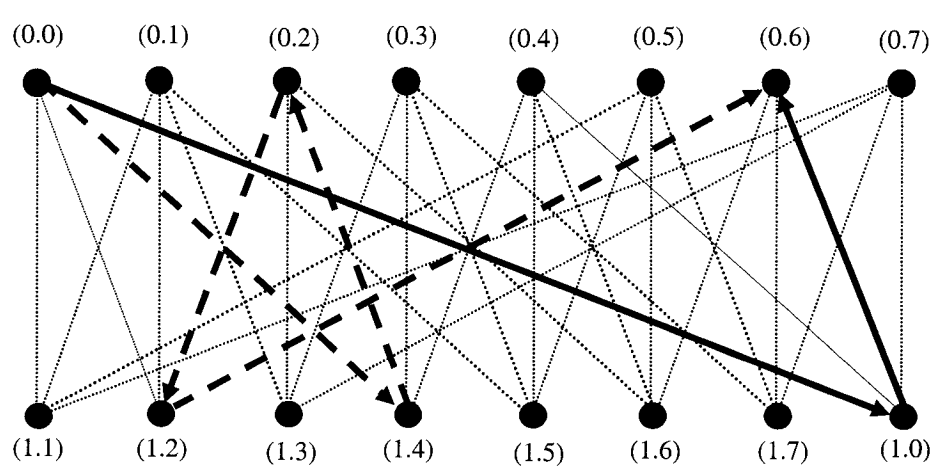

Figure 9 - Two different paths $(0,0)\rightarrow(0,6)$ in $W_{4,16}$

Analogous, a path between $(0,0)$ and a vertex from layer 1 can be drawn based on

quasi-symmetric decomposition (4.3). For example, the vertex $(1,7)$ can be written as $7 = \overline{0111}_2$ and could have the following quasi-symmetric decompositions: $7 = 2^2 + (2^2 - 2^0)$ or $7 = 2^0 + (2^3 - 2^1)$. Each of them corresponds to a path in the Knödel graph $W_{4,16}$, as you can see in the figure below:

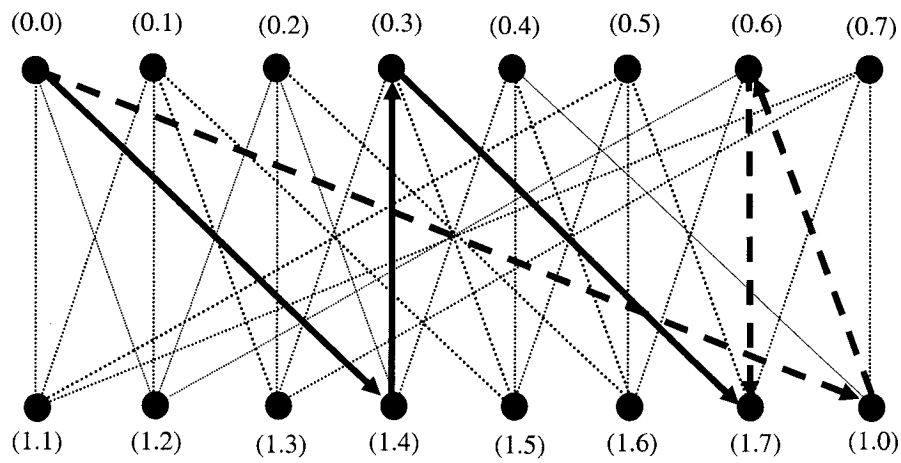

Figure 10 - Two different paths $(0,0) \rightarrow (1,7)$ in $W_{4,16}$

Every path between two vertices in Knödel graph will correspond to a symmetric (quasi-symmetric) decomposition of the label of vertices. Thus, we can reduce the problem of finding the minimum path to the problem of finding the minimal symmetric (quasi-symmetric) decomposition. As we will see in the next section, this last problem is closely related with that of minimal redundant expansion of integers.

4.3 Minimal redundant expansion of integers

In order to understand the redundant expansion of an integer and its connection with the minimum path problem in Knödel graphs we give the following definitions:

Definition 13 (redundant expansion of an integer) [37]

For every integer n, the redundant expansion of n in base q is :

$$R_q(n) = \left\{ \varepsilon = (\varepsilon_t, \ldots, \varepsilon_0) \,\middle|\, t \in N, \varepsilon_i \in Z,\ n = \sum_{i=0}^{t} \varepsilon_i q^i \right\} \tag{4.4}$$

Definition 14 (cost of representation) [37]

The cost of a representation $\varepsilon \in R_q(n)$ is defined as:

$$c(\varepsilon) = c(\varepsilon_0, \ldots, \varepsilon_t) = t + 1 + \sum_{i=0}^{t} |\varepsilon_i| \tag{4.5}$$

Definition 15 (relaxed cost of representation) [37]

The relaxed cost of a representation $\varepsilon \in R_q(n)$ is defined as:

$$c'(\varepsilon) = c'(\varepsilon_0, \ldots, \varepsilon_t) = \sum_{i=0}^{t} |\varepsilon_i| \tag{4.6}$$

For example, the number $99 = \overline{1100011}_2$ has one of the redundant expansions in the system $\{-1,0,1\}$: $\overline{10-10010-1}$. Indeed, $99 = 1 \cdot 2^7 + (-1) \cdot 2^5 + 1 \cdot 2^2 + (-1) \cdot 2^0$. For the notation convenience, we replace -1 with $\bar{1}$ in the redundant expansion. Thus, we will write: $99 = 10\bar{1}0010\bar{1}$ in the redundant base 2. Note that, in general, this representation is not unique. For example, we can write $99 = 110010\bar{1}$, with the same relaxed cost.

The problem of optimizing the costs *c* or *c*' has applications in the optimal design of arithmetical hardware [38], in coding theory [39], and especially in cryptography [40]. It has first been studied in [38] for $q = 2$ and was generalised for every q in [37]. Although there are many algorithms for optimizing the relaxed cost *c*' [40, 41], the one presented in [37] by Heuberger and Prodinger is one of the most simple and powerful. It gives a minimum relaxed redundant representation of an integer n in $O(\log n)$ time and space for every base q, and is proven to have the minimum relaxed cost, even this representation is not unique.

Their algorithm scans the usually binary representation of an integer n at which a "0" digit is appended artificially at the left side, from right to left, and has as output the digits of the relaxed redundant representation which can be with at most one digit longer than the binary representation.

We adapted here lemma 3 from [37] and the relaxed representation algorithm (algorithm 2 in [37]) for redundant base 2:

Lemma 5 (Heuberger-Prodinger relaxed representation [37])

Let n be a fixed integer (input) and $\varepsilon \in R_2(n) = (\varepsilon_s, \varepsilon_{s-1}, ..., \varepsilon_1, \varepsilon_0)$ the relaxed reduced representation (output) in base 2. Let:

$$a = n \bmod 2 \tag{4.7}$$

$$b = \frac{n-a}{2} \bmod 2 \tag{4.8}$$

Then, the first output digit will be:

$$\varepsilon_0 = \begin{cases} a & \text{if } a < 1 \text{ or } (a = 1 \text{ and } b < 1) \\ a - 1 & \text{otherwise} \end{cases} \tag{4.9}$$

Heuberger-Prodinger relaxed algorithm for base 2 (q = 2) [37]

```
        ε ← ( )
        m ← n
        while m > 0 do
            a ← (m mod 2)
(*)         if ((a = 1) and ({m/4} ≥ 1/2) ) then
                a ← a − 2
            end if
```

(**) $m \leftarrow (m-a)/2$

$\varepsilon \leftarrow a \,\&\, \varepsilon$

end while

Note that, $\{x\}$ represents the fractional part of x, $\{x\} = x - \lfloor x \rfloor$, and $a \,\&\, \varepsilon$ means that a is concatenated with ε, at the left side.

4.4 Minimum path algorithm

In order to find the minimum symmetric decomposition (lemma 4) our intention is to use the Heuberger-Prodinger algorithm for redundant base 2 in special conditions. We will consider first the case of minimum path between $(0,0)$ and a vertex from layer 0. The symmetric decomposition will be of form: $v = \sum_{r=1}^{t} \left(2^{i_r} - 2^{j_r}\right) \bmod 2^{d-1}$ (4.2). Thus, we have to ensure that the number of 1's will be equal to the number of -1's in the algorithm's output. We can easily see that this is not the case for all vertices. For example, $21 = \overline{10101}_2$, will generate an identical relaxed minimum redundant expansion via Heuberger-Prodinger algorithm (10101).

Let n be an integer with the binary representation $b(n)$. We define the *extended binary representation* $b'(n)$, the number obtained from $b(n)$ appending a 0 on the rightmost side and a 0 on the leftmost side: $b'(n) = \overline{0b(n)0}$. The next two theorems will ensure a symmetric (quasi-symmetric) output in some cases.

Theorem 8

Let n be an integer with the extended binary representation $b'(n)$. The output of

Heuberger-Prodinger algorithm for $b(n)$ will be symmetric if $b'(n)$ does not contain neither $\overline{101}$ nor $\overline{010}$ as a sub-block.

Proof:

First we must note that, always throughout the algorithm's run, the last two digits in the m's binary representation are taken into account because of the test: $\{m/4\} \geq 1/2$. Let us analyse the first output of the algorithm. We can group the last two digits in three cases:

Case 1 ($\overline{00}$ and $\overline{10}$)

Every time when a = 0 (last digit in m's binary representation), a "0" will be appended because the test $(a = 1)$ will be evaluated to FALSE. That means that a block of 0's as input will always generate the same block of 0's as output.

Case 2 ($\overline{01}$)

A $\overline{01}$ block as input will generate "01" as output because the test $\{m/4\} \geq 1/2$ will be evaluated to FALSE (i.e. $\{m/4\} = 1/4 < 1/2$), a =1 and will remain 1 after (*). Thus, the last tow digits of m will be revaluated to: $\overline{m'01} = \frac{(\overline{m'01} - 1)}{2} = \overline{m'0}$ and case 1) follows.

Case 3 ($\overline{11}$)

A $\overline{00\underbrace{1.....1}_{r-digits}1}$ block will generate $\overline{01\underbrace{0.....0}_{r-digits}-1}$ as output if $r \geq 2$ (if $r = 1$ we are in the case 2). Indeed, at the first occurrence of 1, the statement (*) is evaluated to TRUE (a = 1 and $\{m/4\} = \overline{11}/4 = 3/4 \geq 1/2$). Thus, a will be revaluated to -1 and m will be revaluated by (**) to (m + 1)/2. That means:

$$(**) \qquad m \leftarrow \frac{\overline{00\underbrace{1.....1}_{r-digits}}+1}{2} = \frac{\overline{01\underbrace{0.....0}_{r-digits}}}{2} = \overline{01}\,\underbrace{\overline{0.....0}}_{(r-1)\ digits} \qquad (4.10)$$

After $(r-1)$ iterations, in which a will be "0" conform case 1), we meet again the case 2) and the last two digits of the output will be "01".

Now we can see that the conditions from hypothesis will exclude all the numbers that have blocs of 1's or blocs of 0's with length 1. For example the numbers $\overline{110001110}$ and $\overline{011100110011}$ are valid inputs but $\overline{11000100}$ and $\overline{11101110}$ are not, the first for a $\overline{010}$ occurrence and the second for a $\overline{101}$ occurrence. If these occurrences are excluded, we cannot be in the cases 1) and 2). The case 3) will ensure us a symmetric decomposition. □

Theorem 9

Let n be an integer with the binary representation $b(n)$ and extended binary representation $b'(n)$. The output of Heuberger-Prodinger algorithm for $b(n)$ will be quasi-symmetric if:

1) $b'(n)$ contains exactly one $\overline{010}$ as a sub-block and does not contain $\overline{101}$ in the remaining digits, or

2) $b'(n)$ contains exactly one $\overline{101}$ as a sub-block, which is not contained in a $\overline{0110110}$ sub-block, and also does not contain $\overline{010}$ in the remaining digits.

Note that two $\overline{010}$ sub-blocks or two $\overline{101}$ sub-blocks may overlap in maximum one digit in order to be excluded.

Proof:

Let us separately consider $b'(n)$ in the above cases:

1) In this case we will subtract from $b'(n)$ the power of two corresponding to the position of the 1 from $\overline{010}$. The obtained number will satisfy the conditions from theorem 1, which means that there is a symmetric decomposition for it. Adding the subtracted power of two to this symmetric decomposition we obtain a quasi-symmetric decomposition.

2) In this case, since we cannot have a $\overline{010}$ sub-block in the remaining digits, the $\overline{101}$ sub-block can be contained in the following sub-block: $\overline{\underbrace{1...1}_{x}0\underbrace{1...1}_{y}}$, with $x > 2$ or $y > 2$.

We have two cases:

a) If $x > 2$, we subtract the power of two corresponding to the rightmost 1 from the left sub-block.

b) If $y > 2$, we subtract the power of two corresponding to the leftmost 1 from the right sub-block.

In both cases, the conditions of theorem 8 are satisfied for the number obtained after subtraction, and we obtain again a quasi-symmetric decomposition. □

For example $\overline{1001110}$ is a valid inputs for theorem 2 since $\overline{10100111}$ is not.

4.4.1 Layer 0 $\rightarrow$ layer 0 minimum path

First, let us assume that we are in the conditions of theorem 8. In this case a symmetric decomposition is ensured and we obtain a minimum path of even length. For example, an input $102 = \overline{1100110}$ will generate the output $(10\bar{1}010\bar{1}0)$. This can be translated in a minimum path in Knödel graphs as follows: in every Knödel graph $W_{d,2^d}$, with $d \geq 8$, the minimum path between vertices $(0,0)$ and $(0, 102)$ will follow the edges in dimensions $7 \rightarrow 5 \rightarrow 3 \rightarrow 1$, in this order. We have to note that we can always permute

the edges of same sign and the result will be the same. For example, in the previous case the $7 \to 1 \to 3 \to 5$ path also connects $(0,0)$ with $(0, 102)$.

If we are in the conditions of theorem 9, we can obtain a symmetric decomposition of length $2t+1$ as follows (we skip the modulo operations for simplicity):

$$b(n) = 2^w + \sum_{r=1}^{t}\left(2^{i_r} - 2^{j_r}\right) = 2^{w+1} - 2^w + \sum_{r=1}^{t}\left(2^{i_r} - 2^{j_r}\right) = \sum_{r=1}^{t+1}\left(2^{i_r} - 2^{j_r}\right) \tag{4.11}$$

Thus, we obtain a path of length $2(t+1)$, which is one longer that the length of a minimum path guaranteed by the Heuberger-Prodinger theorem. Any symmetrical decomposition smaller then $2(t+1)$ will have at most $2t$ terms. This will contradict the mentioned theorem, which claims a minimum decomposition with $2t+1$ terms. For example, an input $307 = \overline{100110011}$ will generate as output $(1010\bar{1}010\bar{1})$. That means that the minimum symmetric decomposition is: $307 = (2^9 - 2^8) + (2^6 - 2^4) + (2^2 - 2^0)$ and the minimum path will follow the dimensions $9 \to 8 \to 6 \to 4 \to 2 \to 0$ or any permutations of dimensions of same sign.

4.4.2 Layer 0 $\to$ layer 1 minimum path

In this case, we are looking for a minimum quasi-symmetric decomposition since all the paths have odd length. If we are in the conditions of theorem 1 we obtain a symmetric decomposition. For transforming it in a quasi-symmetric decomposition, we proceed as follows (we skip the modulo operations for simplicity):

$$b(n) = \sum_{r=1}^{t}\left(2^{i_r} - 2^{j_r}\right) = \sum_{r=1}^{t-1}\left(2^{i_r} - 2^{j_r}\right) + \left(2^{i_t} - 2^{j_t}\right) =$$

$$= \sum_{r=1}^{t-1}\left(2^{i_r} - 2^{j_r}\right) + \left(2^{i_t-1} - 2^{j_t}\right) + 2^{i_t-1} = 2^{i_t-1} + \sum_{r=1}^{t}\left(2^{i'_r} - 2^{j_r}\right) \tag{4.12}$$

We obtain a path with cost $2t+1$. Any quasi-symmetric representation, smaller than $2t+1$, will have at most $2t-1$ terms. This contradicts the Heuberger-Prodinger theorem, which states that the representation with $2t$ terms is the minimal representation for this case. If we are in the conditions of theorem 9 we obtain directly a minimum quasi-symmetric decomposition.

A natural question arises: how many cases are covered by this algorithm? The problem of sub-block occurrences in redundant representation was considered in [37] and [43] and there is no exact formula for the sub-block occurrences. In [43] they obtained an average frequency of occurrences of a given sub-block amongst the numbers $0,\ldots,n-1$ described by $const \cdot \log_2 n + \delta(\log_2 n) + o(1)$, with a multiplicative constant of $\log_2 n$, and a periodic function, $\delta(\log_2 n)$, of period one, depending on the given sub-block.

4.4.3 A heuristic for the minimum path

The minimum redundant decomposition, as it comes from the Heuberger-Prodinger algorithm can give us a path for all the rest of vertices, which did not pass the conditions from theorems 8 and 9.

Note that the algorithm output must contain at least one positive power of two. Assume that we have x of 1's and y of -1's in output: $b(n)=\sum_{r=1}^{x} 2^{i_r} - \sum_{r=1}^{y} 2^{j_r}$. We have three cases:

a) $x > y$. In this case we can obtain a symmetrical decomposition as follows:

$$b(n)=\sum_{r=1}^{x} 2^{i_r} - \sum_{r=1}^{y} 2^{j_r} = \sum_{r=1}^{y} 2^{i_r} - \sum_{r=1}^{y} 2^{j_r} + \sum_{r=y+1}^{x} 2^{i_r} = \sum_{r=1}^{y} \left(2^{i_r} - 2^{j_r}\right) + \sum_{r=y+1}^{x} \left(2^{i_r+1} - 2^{i_r}\right) \qquad (4.13)$$

b) $x < y$. In this case we can obtain a symmetrical decomposition as follows:

$$b(n)=\sum_{r=1}^{x}2^{i_r}-\sum_{r=1}^{y}2^{j_r}=\sum_{r=1}^{x}2^{i_r}-\sum_{r=1}^{x}2^{j_r}-\sum_{r=x+1}^{y}2^{j_r}=\sum_{r=1}^{x}\left(2^{i_r}-2^{j_r}\right)+\sum_{r=x+1}^{y}\left(2^{j_r}-2^{j_r+1}\right) \qquad (4.14)$$

c) $y=0$. In this case, we produce first a negative term as follows:

$$b(n)=\sum_{r=1}^{x}2^{i_r}=\sum_{r=1}^{x-1}2^{i_r}+2^{i_x}=\sum_{r=1}^{x-1}2^{i_r}+2^{i_x+1}-2^{i_x}=\sum_{r=1}^{x}2^{i_r}-\sum_{r=1}^{1}2^{j_r}. \qquad (4.15)$$

The obtained form follows case a).

This method of expanding will give us a logarithmic heuristic for the vertices excluded by the theorems 8 and 9.

Note that the length of the path obtained from heuristic, can be at most $|x-y|+1$ greater then the length of a minimum path. Since the diameter of Knödel graph $W_{d,2^d}$ is $\lceil (d+2)/2 \rceil$, the difference between the actual length of a minimum path and the length of the path obtained from our heuristic is at most $\lceil (d+2)/2 \rceil + 1$.

Both, the algorithm and the heuristic, take as input the binary representation of the vertex label and analyse each digit from right to left. Thus, the time complexity of the algorithm is $O(\log n)$ for $W_{d,2^d}$, which is logarithmic in terms if n, the number of vertices in graph. Since the only number needed to be stored is the vertex label, the space complexity is $O(\log n)$ as well.

Observations:

a) We can extend the algorithm for all Knödel graphs $W_{\lfloor \log_2 n \rfloor, n}$ but, in this case, we have to analyse the binary decomposition of both, positive and negative forms of the vertex label l: $b(l)$ or $(-b(l))$ mod $\frac{n}{2}$. For example, $819=\overline{1100110011}$ yields to a

symmetric decomposition $10\bar{1}010\bar{1}010\bar{1}$, which means a path of length 6. Taking $(-819)\bmod 847 = \overline{11100}$, we obtain a symmetric decomposition $1000\bar{1}00$, which means a path of length 2.

b) The lower bound for the diameter of Knödel graph $W_{d,2^d}$ is a consequence of the method presented in this paper. The maximum relaxed cost, as yields from this algorithm, for a d digits number, is $\lceil d/2 \rceil$, for a binary form $\overline{101...101}$ or $\overline{0101...101}$. Assuming that $\lceil d/2 \rceil$ is even and we want a path between different layers, we obtain a length of $\lceil d/2 \rceil + 1$. If $\lceil d/2 \rceil$ is odd, and we want a path between same layers, we obtain a length of $\lceil d/2 \rceil + 1$. Thus, the diameter must be at least $\lceil d/2 \rceil + 1$.

Conclusions and future work

Although Knödel graphs have been introduced 28 years ago, there are still many open questions regarding their algebraic and routing properties. In this thesis we partially solve three of them:

- the general definition of Knödel graphs
- the families of complete rotation in Knödel graphs
- minimum path routing algorithm for $W_{d,2^d}$.

Among the remained open problems we mention here:

- minimum path routing in Knödel graphs $W_{d,n}$
- the diameter of Knödel graphs $W_{d,n}$, for $n \neq 2^d$.

Because of their remarkable number of vertices to diameter ratio characteristic, which competes with hypercubes and circulant graphs of same order, Knödel graphs

become a useful candidate for communication networks, especially in supercomputing, where parallel algorithms are heavily employed.

Bibliography

[1] W. Knödel. New gossips and telephones. *Discrete Mathematics*, 13:95, 1975.

[2] P. Fraigniaud and J.G. Peters, Minimum linear gossip graphs and maximum linear (Δ, k)-gossip graphs. *Networks*, Volume 38, Number 3, October 2001.

[3] J.-C. Bermond, H.A. Harutyunyan, A.L. Liestman, and S. Perennes. A note on the dimensionality of modified Knödel graphs. *IJFCS: International Journal of Foundations of Computer Science*, 8(2):109-116, 1997.

[4] G. Fertin and A. Raspaud, Families of graphs having broadcasting and gossiping properties. *In Proc. of the 24-th International Workshop on Graph-Theoretic Concepts in Computer Science* (WG '98), *Smolenice. Lecture Notes in Computer Science*, 1517:63-77, 1998.

[5] G. Fertin, A. Raspaud, O. Sýkora, H. Schröder, and I. Vrto. Diameter of Knödel graph. *26th International Workshop on Graph-Theoretic Concepts in Computer Science (WG 2000), Lecture Notes in Computer Science*, 1928:149-160. Springer-Verlag, 2000.

[6] J. Hromovic, R. Klasig, B. Monien, R. Peine. Dissemination of information in interconnection networks (broadcasting & gossiping). *Combinatorial Network Theory*, 125-212, ed.: Ding-Zhu Du, D. Frank Hsu, Kluwer Academic Publishers

[7] P. Fraigniaud and E. Lazard, Methods and problems of communication in usual networks. *Discrete Appl. Math.*, 53:79-133, 1994.

[8] P.J. Slater, E.J. Cockayne and S.T. Heditniemi, Information dissemination in trees. *SIAM Journal of Computing*, vol. 10, no. 4:692-701, 1981.

[9] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. F. Freeman, San Francisco, 1979.

[10] S.T. Hedetniemi, S.M. Hedetniemi, A.L. Liestman. A survey of broadcasting and gossiping in communication networks. *Networks*, 18:319-349, 1988.

[11] J.-C. Bermond, P. Hell, A.L. Liestman, and J. Peters. Sparse broadcast graphs. *Discrete Appl. Math.*, 36:97-130, 1992.

[12] A. Farley, S. Hedetniemi, S. Mitchel, A. Proskurowski, Minimum Broadcast Graphs. *Discrete Mathematics* 25:189-193: 1979.

[13] L. Gargano, U. Vaccaro. On the construction of minimal broadcast networks. *Networks*, 19:673-689, 1989.

[14] M.J. Dinnen, M.R. Fellows, and V. Faber. Algebraic construction of efficient broadcast networks. *Proc. of Applied Algebra, Algorithms and Error Correcting Codes (AAECC'91), Lecture Notes in Computer Science*, 539:152-158, 1991

[15] L.H. Khachatrian and H.A. Harutyunyan. Construction of new classes of minimal broadcast networks. *Proc. Third International Colloquium on Coding Theory*, pg. 69-77, 1990

[16] J.-C. Bermond, P. Fraigniaud, J. Peters. Antepenultimate broadcasting, *Networks* 26:125-137, 1995

[17] S.C. Chau, A.L. Liestman. Constructing minimal broadcast networks. *J. Combin. Inform. Systems Sci.* 10:110-122, 1985

[18] M.J. Dinneen, J.A. Ventura, M.C. Wilson, G. Zakeri. Compound constructions of minimal broadcast networks, *Technical Report CDMTCS-026*, 1997

[19] A. Farley. Minimal broadcast networks. *Networks* 9:313-332, 1979

[20] H.A. Harutyunyan, A.L. Liestman. More broadcast graphs. *Discrete Applied Mathematics* 98:81-102, 1999.

[21] R. Labahn. A minimum broadcast graph on 63 vertices. *Discrete Applied Mathematics* 53:247-250, 1994

[22] M. Grigni, D. Peleg. Tight bounds on minimum broadcast networks. *SIAM Journal of Discrete Math.* 4:207-222, 1991.

[23] R. Labahn. Some minimum gossip graphs. *Networks*, 23:333-341, 1993

[24] G. Fertin. A study of minimum gossip graphs. *Discrete Mathematics*, 1-3(215):33-57, 2000

[25] G. Fertin and R. Labahn. Compounding of gossip graphs. Networks, 36(2):126-137, 2000

[26] G.Fertin, A. Raspaud. A survey on Knödel graphs. *Discrete Applied Mathematics*, 137:173–195 (2004).

[27] M-C. Heydemann, N. Marlin, and S. Perennes. Cayley graphs with complete rotations. *Technical report, Laboratiore the Recherche en Informatique* (Orsay), 1997. TR-1155.

[28] H.S. Haroutunian. New minimal broadcast networks, *Proceedings of the Fourth International Colloquium on Coding Theory*. 1991, pp. 36-40.

[29] J.-C. Bermond, P. Hell, A.L. Liestman, and J. Peters. Broadasting in bounded degree graphs. *SIAM J. Discrete Math.*, 5 :10-24, 1992.

[30] J. Cohen, P. Fraigniaud, and C. Gavoille. Recognizing bipartite incident-graphs of circulant graphs. In 25th *International Workshop on Group-Theoretic Concepts in*

Computer Science (WG'99), Lecture Notes in Computer Science, 1665:215-227, 1999.

[31] J.-C. Bermond, T. Kodate, and S. Perennes. Gossiping in Cayley graphs by packets. In *Conf. CCS95) 8th Franco-Japanese and 4th Franco-Chinese Conf. Combin. Comput. Sci. Brest, July 1995), Lecture Notes in Computer Science*, 1120:301-305, 1996.

[32] P. Fragopolou and S.G. Akl. Spanning subgraphs with applications to communication on a subclass of the Cayley graph based network. *Discrete Applied Math.*, 83:76-96, 1998.

[33] N. Biggs and A. White. Permutation groups and combinatorial structures. London Mathematical Society, *Lecture Notes Series, Cambridge University Press*, 1979.

[34] A. White. Graphs, groups and surfaces. *North Holland Mathematical Studies, Netherlands*, 1984.

[35] M.-C. Heydemann and B. Ducourthial. Cayley graphs and interconnection networks. In *Graph Symmetry, Algebraic Methods and Applications*, "*NATO ASI C*", 497:167-226, 1997.

[36] S. Even and O. Goldreich. The minimal-length generating sequence problem is NP-hard. *J. Algorithms*, 2:311-313, 1981.

[37] C. Heuberger and H. Prodinger. On minimal expansions in redundant number systems: Algorithms and quantitative analysis. *Computing*, 66:377-393, 2001.

[38] G.W. Reitwieser. Binary arithmetic. *Advances in Computers*, 1:231-308, 1960.

[39] J.L. Massey and O.N. Garcia. Error-correcting codes in computer arithmetic. *Advances Inform. Syst. Sci.*, 4:273-326, 1972.

[40] F. Morain and J. Olivios. Speeding up the computations on an elliptic curve using addition-subtraction chains. *RAIRO Inform. Théor. Appl.*, 24:531-543, 1990.

[41] J. Demetrovics, A. Pethő, and L. Rónzai. On the ± 1-representation of integers. *Acta Cybernetica*, 14:27-36, 1999.

[42] M. Maheo, J.-F. Sacle. Some minimum broadcast graphs. *Discrete Appl. Math*, 53:275-285, 1994.

[43] P.J. Grabner, C. Heuberger, and H. Prodinger. Subblock occurrences in signed digit representations. *Glasgow mathematical journal*. 45:427—440, 2003.