A NOTE ON THE DIMENSIONALITY OF MODIFIED KNÖDEL GRAPHS

JEAN-CLAUDE BERMOND
Project SLOOP, INRIA Sophia Antipolis, 2004 Route des Lucioles
BP 93 F-06902 Sophia-Antipolis, France

and

HOVHANNES A. HARUTYUNYAN
School of Computing Science, Simon Fraser University
Burnaby, B.C. V5A 1S6, Canada

and

ARTHUR L. LIESTMAN
School of Computing Science, Simon Fraser University
Burnaby, B.C. V5A 1S6, Canada

and

STEPHANE PERENNES
Project SLOOP, INRIA Sophia Antipolis, 2004 Route des Lucioles
BP 93 F-06902 Sophia-Antipolis, France

Received 5 November 1995
Revised 20 September 1996
Communicated by D. F. Hsu, M. Palis and D. S. L. Wei

ABSTRACT

We show that the edges of the modified Knödel graph can be grouped into dimensions which are similar to the dimensions of hypercubes. In particular, routing, broadcasting and gossiping, can be done easily in modified Knödel graphs using these dimensions.

Keywords: routing, broadcasting, gossiping, hypercubes.

1. Introduction

One of the reasons that the hypercube is such a popular network topology is its parameter called *dimension*. The value of this parameter determines the number of vertices and the number of edges of the hypercube. Dimension can be used, in a natural way, to label vertices and to facilitate routing between an arbitrary pair of vertices. (See, for example, [4,8].) It has long been known that broadcasting and gossiping can be easily accomplished in a hypercube, by using dimension. (See [2] for references on these problems.) However, hypercubes can only be constructed for $n = 2^d$ vertices. In this paper, we show that a set of graphs, constructable for any even n, which were used implicitly in a proof of Knödel [3] also have dimension - although the notion of dimension is somewhat weaker than that of hypercubes.

In this paper, we consider *modified Knödel graphs* on n vertices (for any even n which is not a power of 2). Let KG_n denote the modified Knödel graph on $n \geq 2$

vertices where n is even and not a power of 2 and let $d = \lfloor \log n \rfloor$. The vertices of KG_n are labeled (x, j) where $x \in Z_{\frac{n}{2}}$ and $j \in Z_2$. In this paper, the values of x will be those representatives of $Z_{\frac{n}{2}}$ between 0 and $\frac{n}{2} - 1$, the values of j will be 0 and 1, and the operations are modulo $\frac{n}{2}$ or modulo 2. The edges of KG_n are $[(x, 0), (x + 2^i, 1)]$ for all x and all i where $0 \leq i \leq d - 1$ (recall $d = \lfloor \log n \rfloor$). The edges of the form $[(x, 0), (x + 2^i, 1)]$ compose a perfect matching and are called *edges of dimension i*. (The graphs used by Knödel [3] are essentially the same, except that he also included edges of the form $[(x, 0), (x, 1)]$. We refer to those graphs as "Knödel graphs" and to our graphs as "modified Knödel graphs".)

The edges of a d-dimensional hypercube can be partitioned into d sets - each set corresponding to a particular dimension. In a hypercube, we can choose any permutation of the dimensions, say $\pi_1, \pi_2, \ldots, \pi_d$. Given such a permutation of dimensions, there is a unique route between any pair of vertices a and b which corresponds to moving in the necessary dimensions in the order implied by the permutation. To broadcast a message from any source, any informed vertex simply forwards the message to its neighbor in the π_ith dimension at each time i (where $1 \leq i \leq d$). To gossip, each vertex exchanges information with its neighbor in the π_ith dimension at each time i (where $1 \leq i \leq d$).

In the modified Knödel graph KG_n, we show that there exist permutations of the dimensions, say $\pi_1, \pi_2, \ldots, \pi_d$, which can be used similarly. However, given such a permutation, we use the sequence of dimensions $\pi_1, \pi_2, \ldots, \pi_d, \pi_1$; that is, the first dimension is repeated again at the end of the sequence. Given such a sequence, there is a route (not necessarily unique) between any pair of vertices a and b which corresponds to moving in the necessary dimensions in the order implied by the sequence. To broadcast a message from any source, any informed vertex simply forwards the message to its neighbor in the π_ith dimension at each time i (where $1 \leq i \leq d+1$ and $\pi_{d+1} = \pi_1$). To gossip, each vertex exchanges information with its neighbor in the π_ith dimension at each time i (where $1 \leq i \leq d+1$ and $\pi_{d+1} = \pi_1$). Thus, the dimensions in these graphs are quite similar to dimensions of hypercubes. This property allows an efficient perpetual gossip scheme [7] on these graphs and is also of use in implementing communication routines with variable data lengths [9].

In particular, we will focus on demonstrating that these permutations exist for the gossiping problem. The routing and broadcast results follow immediately.

1.1. Set Definitions

For sets A and B, we will use $A + B$, $A - B$, $A * B$, and A/B to denote $\{a + b \mid a \in A, b \in B\}$ (set addition), $\{a - b \mid a \in A, b \in B\}$ (set subtraction), $\{a * b \mid a \in A, b \in B\}$ (set multiplication), and $\{a/b \mid a \in A, b \in B\}$ (set division), respectively. We will also compute products of matrices 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. It is important to note that set union is distributive over set addition.

In order to describe gossip schemes in these graphs, we must be able to describe sets of vertices which are informed of particular messages after a sequence of time units. In all of our schemes, in a given time unit, calls will be made in exactly one dimension with each informed vertex calling its neighbor in that particular dimension.

Consider a set of vertices that know a particular piece of information at time t. In particular, if $(x,0)$ and $(y,1)$ know this information and we make calls in dimension i at the next time unit $(t+1)$, the set of informed vertices will also include $(x+2^i,1)$ and $(y-2^i,0)$.

We will use the matrix $M_i = \begin{pmatrix} \{0\} & \{-2^i\} \\ \{2^i\} & \{0\} \end{pmatrix}$ to represent a set of calls in dimension i.

Now consider a second set of calls in dimension j to be made at time $t+2$. After this set of calls, vertices $(x+2^j,1)$, $(y-2^j,0)$, $(x+2^i-2^j,0)$, and $(y-2^i+2^j,1)$ are also informed. Multiplying the corresponding matrices for dimensions i and j, we get $\begin{pmatrix} \{0\} & \{-2^j\} \\ \{2^j\} & \{0\} \end{pmatrix} \cdot \begin{pmatrix} \{0\} & \{-2^i\} \\ \{2^i\} & \{0\} \end{pmatrix} = \begin{pmatrix} \{0, 2^i-2^j\} & \{-2^i,-2^j\} \\ \{2^i,2^j\} & \{0,2^j-2^i\} \end{pmatrix} =$

$\begin{pmatrix} A & A-\{2^i\} \\ \{2^i\}-A & -A \end{pmatrix}$.

Observe that if $(x,0)$ is informed at time t and then calls are made in dimensions i and j at times $t+1$ and $t+2$, respectively, then vertices $(x+a,0)$ and $(x+c,1)$, where $a \in A, c \in \{2^i\}-A$, are informed after these calls. Similarly, if $(y,1)$ is informed at time t and then calls are made in dimensions i and j at times $t+1$ and $t+2$, respectively, then vertices $(y+b,0)$ and $(y+d,1)$, where $b \in A-\{2^i\}, d \in -A$, are informed after these calls. Note that the set A represents the set of vertices reachable from $(x,0)$ by a path of either zero or two calls (that is, a path of even length) and set $\{2^i\}-A$ represents the set of vertices reachable from $(x,0)$ by a path of exactly one call (that is, a path of odd length). $A-\{2^i\}$ and $-A$ similarly represent vertices reachable from $(y,1)$ by paths of odd and even length, respectively.

Extending this idea, we see that we can represent the outcome of a sequence of calls in dimensions $i_1, i_2, \ldots, i_k$ as a matrix M which is the matrix product $M(i_1,i_2,\ldots,i_k) = M_{i_k} \cdot M_{i_{k-1}} \cdots M_{i_1}$. In particular, the matrix product is easily expressed given the value of A. We use $s(i_1,i_2,\ldots,i_k)$ to denote the value (of the set A) for the sequence of calls in dimensions $i_1,i_2,\ldots,i_k$. That is, $s(i_1,i_2,\ldots,i_k) = \{y \in Z_{\frac{n}{2}} \mid (x+y,0)$ is reachable from $(x,0)$ by a path of even length from the dimensions$i_1,i_2,\ldots,i_k\}$. (Later, we will be particularly interested in those sequences which are permutations of the dimensions, but initially we will consider more general sequences of calls.)

2. Results

Lemma 1 *After any sequence of calls in dimensions $i_1, i_2, \ldots, i_k$,*

$$M_{i_k} \cdot M_{i_{k-1}} \cdots M_{i_1} = \begin{pmatrix} s(i_1, i_2, \ldots, i_k) & s(i_1, i_2, \ldots, i_k) - \{2^{i_1}\} \\ \{2^{i_1}\} - s(i_1, i_2, \ldots, i_k) & -s(i_1, i_2, \ldots, i_k) \end{pmatrix}.$$

Proof. The proof is by induction on k. When $k = 1$,

$$M_1 = \begin{pmatrix} \{0\} & \{0\} - \{2^{i_1}\} \\ \{2^{i_1}\} - \{0\} & -\{0\} \end{pmatrix} = \begin{pmatrix} \{0\} & \{-2^{i_1}\} \\ \{2^{i_1}\} & \{0\} \end{pmatrix} \text{ and } s(i_1) = \{0\}.$$

Then, $M_{i_k} \cdot M_{i_{k-1}} \cdots M_{i_1} =$

$$M_{i_k} \cdot \begin{pmatrix} s(i_1, i_2, \ldots, i_{k-1}) & s(i_1, i_2, \ldots, i_{k-1}) - \{2^{i_1}\} \\ \{2^{i_1}\} - s(i_1, i_2, \ldots, i_{k-1}) & -s(i_1, i_2, \ldots, i_{k-1}) \end{pmatrix} =$$

$$\begin{pmatrix} \{0\} & \{-2^{i_k}\} \\ \{2^{i_k}\} & \{0\} \end{pmatrix} \cdot \begin{pmatrix} s(i_1, i_2, \ldots, i_{k-1}) & s(i_1, i_2, \ldots, i_{k-1}) - \{2^{i_1}\} \\ \{2^{i_1}\} - s(i_1, i_2, \ldots, i_{k-1}) & -s(i_1, i_2, \ldots, i_{k-1}) \end{pmatrix} =$$

$$\begin{pmatrix} s(i_1, i_2, \ldots, i_k) & s(i_1, i_2, \ldots, i_k) - \{2^{i_1}\} \\ \{2^{i_1}\} - s(i_1, i_2, \ldots, i_k) & -s(i_1, i_2, \ldots, i_k) \end{pmatrix}.$$

Note that $s(i_1, i_2, \ldots, i_k) = s(i_1, i_2, \ldots, i_{k-1}) \cup (\{2^{i_1} - 2^{i_k}\} - s(i_1, i_2, \ldots, i_{k-1}))$. □

Let ω be any sequence of dimensions. The following three properties are easy to show from Lemma 1.

Properties

1. $s(i_1 \omega i_t) = s(i_1 \omega) \cup (\{2^{i_1} - 2^{i_t}\} - s(i_1 \omega))$.
2. $s(i_1 i_2 \omega) = s(i_2 \omega) \cup (s(i_2 \omega) + \{2^{i_1} - 2^{i_2}\})$.
3. $s(i_1 i_2 \ldots i_t) = \{0, 2^{i_1} - 2^{i_2}\} + \{0, 2^{i_2} - 2^{i_3}\} + \cdots + \{0, 2^{i_{t-1}} - 2^{i_t}\}$.

Proof. Property 1 is proved in Lemma 1. Property 2 can be obtained by computing the product $\begin{pmatrix} s(i_2\omega) & s(i_2\omega) - \{2^{i_2}\} \\ \{2^{i_2}\} - s(i_2\omega) & -s(i_2\omega) \end{pmatrix} \cdot M_{i_1}$. Property 3 is obtained by induction from Property 2. □

Gossip is completed in KG_n by any sequence of calls ω if and only if $M(\omega) = \begin{pmatrix} X & X \\ X & X \end{pmatrix}$, where $X = \{0, 1, \ldots, \frac{n}{2} - 1\}$. That is, when $s(\omega) = X$. We are interested in finding permutations of the dimensions $\pi_1, \pi_2, \ldots, \pi_d$ such that the sequence $\pi_1, \pi_2, \ldots, \pi_d, \pi_1$ completes gossiping. We define such a permutation to be a *valid permutation* for KG_n.

Knödel showed that gossip is completed by a sequence of calls in dimensions $0, 1, ..., d$ in the Knödel graphs [3]. More recently, it has been shown that gossip is completed by a sequence of calls in dimensions $0, 1, ..., d-1, 0$ in the modified Knödel graphs [1,5]. We restate this latter result as a lemma in the terms of this paper. (Note that this also follows directly from Property 3.)

Lemma 2 *The permutation $0, 1, ..., d-1$ is a valid permutation for KG_n.*

Lemma 3 *Any cyclic shift of a valid permutation is also a valid permutation.*

Proof. $s(\pi_1, \pi_2, \ldots, \pi_d, \pi_1) = \{0, 2^{\pi_1} - 2^{\pi_2}\} + \{0, 2^{\pi_2} - 2^{\pi_3}\} + \cdots + \{0, 2^{\pi_d} - 2^{\pi_1}\} = \{0, 2^{\pi_2} - 2^{\pi_3}\} + \cdots + \{0, 2^{\pi_d} - 2^{\pi_1}\} + \{0, 2^{\pi_1} - 2^{\pi_2}\} = s(\pi_2, \pi_3, \ldots, \pi_d, \pi_1, \pi_2)$. □

Lemma 4 *The reverse of a valid permutation is also a valid permutation.*

Proof. Let $\pi_1, \pi_2, \ldots, \pi_d$ be a valid permutation. Thus, $s(\pi_1, \pi_2, \ldots, \pi_d, \pi_1) = X$. Since the reverse of any gossiping scheme on any graph is also a gossiping scheme for the graph [6] we know that $s(\pi_1, \pi_d, \pi_{d-1} \ldots, \pi_2, \pi_1) = X$. From the proof of Lemma 3, we know that $s(\pi_1, \pi_d, \pi_{d-1}, \ldots, \pi_2, \pi_1) = s(\pi_d, \pi_{d-1}, \ldots, \pi_1, \pi_d)$. Thus, $\pi_d, \pi_{d-1}, \ldots, \pi_1$ is a valid permutation. □

From these lemmas, we get

Theorem 1 *The permutation $0, 1, 2, \ldots, d-1$ is a valid permutation for KG_n and any cyclic shift (or the reversal of such a cyclic shift) of $0, 1, 2, \ldots, d-1$ is also a valid permutation for KG_n.*

In particular, this means that gossip can be performed in KG_n as follows: At time $i+1$, where $0 \leq i \leq d$, every vertex calls its neighbor in dimension $i+k \pmod d$ where k is any value $0 \leq k \leq d-1$. Similarly, the following are also gossip schemes for KG_n: At time $i+1$, where $0 \leq i \leq d$, every vertex calls its neighbor in dimension $(d-1-i)+k \pmod d$ where k is any value $0 \leq k \leq d-1$.

In addition to the above permutations, some other permutations may yield gossip schemes for KG_n. It is worth noting, however, that for some n (such as $n = 58$ - obtained by an exhaustive search with a computer program) there are no other valid permutations. The following result gives a sufficient condition for a permutation to be valid.

Theorem 2 *The permutation $\pi_1, \pi_2, \ldots, \pi_d$ is a valid permutation for KG_n if*
1.) $2^{\pi_d} - 2^{\pi_1}$ is relatively prime to $\frac{n}{2}$ and
2.) $\{2^{\pi_1} - 2^{\pi_2}, 2^{\pi_2} - 2^{\pi_3}, \ldots, 2^{\pi_{d-1}} - 2^{\pi_d}, 2^{\pi_d} - 2^{\pi_1}\} = \{2^{\pi_d} - 2^{\pi_1}\} * \{2^0, 2^1, \ldots, 2^{d-1}\}$.

Proof. $s(\pi_1, \pi_2, \ldots, \pi_d, \pi_1)$

$$\begin{aligned}
&= \{0, 2^{\pi_1} - 2^{\pi_2}\} + \{0, 2^{\pi_2} - 2^{\pi_3}\} + \cdots + \{0, 2^{\pi_d} - 2^{\pi_1}\} \quad \text{(by property 3)} \\
&= \{0, (2^{\pi_d} - 2^{\pi_1}) \cdot 2^0\} + \{0, (2^{\pi_d} - 2^{\pi_1}) \cdot 2^1\} + \cdots + \{0, (2^{\pi_d} - 2^{\pi_1}) \cdot 2^{d-1}\} \\
&\qquad \text{(by 2.)} \\
&= \{2^{\pi_d} - 2^{\pi_1}\} * (\{0, 2^0\} + \{0, 2^1\} + \cdots + \{0, 2^{d-1}\}) \\
&= \{2^{\pi_d} - 2^{\pi_1}\} * X \\
&= X \quad \text{(by 1.)}
\end{aligned}$$

Thus, $\pi_1, \pi_2, \ldots, \pi_d$ is a valid permutation for KG_n. □

In the special case of $KG_{2^{d+1}-2}$, we can show that the sufficient condition of Theorem 2 is also a necessary condition for a permutation to be valid. In general, we can not completely characterize the set of valid permutations for any n. We note that there are permutations which are not valid for some particular n. For example, when $n = 26$, the permutation 3, 1, 2, 0 is not valid. In this case, the information from vertex $(0,0)$ (in particular) does not reach vertices $(5,0)$, $(8,0)$, $(0,1)$, or $(3,1)$.

Theorem 3 *The permutation $\pi_1, \pi_2, \ldots, \pi_d$ is a valid permutation for $KG_{2^{d+1}-2}$ if and only if*
1.) $2^{\pi_d} - 2^{\pi_1}$ is relatively prime to $\frac{n}{2}$ and
2.) $\{2^{\pi_d}-2^{\pi_1}, 2^{\pi_2}-2^{\pi_3}, \ldots, 2^{\pi_{d-1}}-2^{\pi_d}, 2^{\pi_d}-2^{\pi_1}\} = \{2^{\pi_d}-2^{\pi_1}\}*\{2^0, 2^1, \ldots, 2^{d-1}\}$.

Proof. Given Theorem 2, it remains to show that if $\frac{n}{2} = 2^d - 1$ and $\pi_1, \pi_2, \ldots, \pi_d$ is a valid permutation, then conditions 1.) and 2.) hold.

Since $\pi_1, \pi_2, \ldots, \pi_d$ is valid, we know that $s(\pi_1, \pi_2, \ldots, \pi_d, \pi_1) = \{0, 2^{\pi_1} - 2^{\pi_2}\} + \{0, 2^{\pi_2} - 2^{\pi_3}\} + \cdots + \{0, 2^{\pi_d} - 2^{\pi_1}\} = X$. Consider $S = s(\pi_1, \pi_2, \ldots, \pi_d) = \{0, 2^{\pi_1} - 2^{\pi_2}\} + \{0, 2^{\pi_2} - 2^{\pi_3}\} + \cdots + \{0, 2^{\pi_{d-1}} - 2^{\pi_d}\}$. By definition, $|S| \le 2^{d-1}$. Note that 0 and $2^{\pi_1} - 2^{\pi_d}$ are both in S. Let $\bar{S} = X - S$. We have $\bar{S} \subseteq S + \{2^{\pi_d} - 2^{\pi_1}\}$, so $|\bar{S}| \le |S|$. But, $|S \cup \bar{S}| = \frac{n}{2} = 2^d - 1$. So, $2^d - 1 \le 2|S|$ which implies that $|S| \ge 2^{d-1}$ and, in fact, $|S| = 2^{d-1}$ and $|\bar{S}| = 2^{d-1} - 1$. Furthermore, as $2^{\pi_1} - 2^{\pi_d} \in S$, then $0 \in S + \{2^{\pi_d} - 2^{\pi_1}\}$. Thus, if $S_1 = S \setminus (2^{\pi_d} - 2^{\pi_1})$, then $\bar{S} = S_1 + \{2^{\pi_d} - 2^{\pi_1}\}$. In other words, for each $x \in \bar{S}$, there exists a unique $y \in S_1$ such that $y + 2^{\pi_d} - 2^{\pi_1} = x$.

Let k be the greatest common divisor of $2^{\pi_d} - 2^{\pi_1}$ and $\frac{n}{2}$ and let $\lambda = \frac{n}{2k}$. Note that as $\frac{n}{2}$ is odd, k and λ are also odd.

Consider the sequence V_h, $0 \le h \le k-1$ of vertices $x_j^h = h + j(2^{\pi_d} - 2^{\pi_1})$ where $j = 0, 1, \ldots, \lambda - 1$. Note that if $x_j^h \in S_1$, then $x_{j+1}^h \in \bar{S}$. Note also that $2^{\pi_1} - 2^{\pi_d}$ belongs to V_0 ($x_{\lambda-1}^0 = 2^{\pi_1} - 2^{\pi_d}$). In other words, a sequence V_h does not contain two consecutive elements in S, and for $h \ge 1$, $x_{\lambda-1}^h$ and x_0^h are not both in S. So, as $|X|$ is odd, for $h \ge 1$, V_h contains at least $\frac{\lambda+1}{2}$ elements of $\bar{S}$ and for $h = 0$, V_0 contains at least $\frac{\lambda-1}{2}$ elements of S. Therefore, we obtain $|\bar{S}| \ge |S| + k - 2$. But, $|\bar{S}| = |S| - 1$, so the only possibility is that $k = 1$, that is, $2^{\pi_d} - 2^{\pi_1}$ and $\frac{n}{2}$ are relatively prime. Furthermore, $x_j^0 = j(2^{\pi_d} - 2^{\pi_1})$ should belong to S for $j = 0, 2, 4, \ldots, \frac{n}{2} - 1$ (and $x_j^0 \in \bar{S}$ for $j = 1, 3, 5, \ldots, \frac{n}{2} - 2$). Therefore, $S = \{2p(2^{\pi_d} - 2^{\pi_1}) \,|\, 0 \le p \le \frac{n-2}{4}\}$. Let $S' = S/(2^{\pi_d} - 2^{\pi_1})$ and let $\delta_i = (2^{\pi_i} - 2^{\pi_{i+1}})/(2^{\pi_d} - 2^{\pi_1})$ for $1 \le i \le d-1$. Then, we have $S' = \{0, \delta_1\} + \{0, \delta_2\} + \ldots \{0, \delta_{d-1}\}$. Therefore, $\{0, \delta_1\} + \{0, \delta_2\} + \cdots \{0, \delta_{d-1}\} = \{0, 2, 4, \ldots, \frac{n}{2} - 1\}$. Recall that the δ_i are even (they belong to S') and that $\frac{n}{2}$ is odd. Suppose that $\delta_1 + \delta_2 + \cdots + \delta_{d-1} > \frac{n}{2}$. Then, consider the smallest sum of the form $\delta_{i_1} + \delta_{i_2} + \cdots + \delta_{i_k}$ which is larger than $\frac{n}{2}$. This sum is odd $(\bmod \frac{n}{2})$, a contradiction. Thus, $\delta_1 + \delta_2 + \cdots + \delta_{d-1} \le \frac{n}{2}$. Since such sums must account for all even integers $\{0, 2, \ldots, \frac{n}{2} - 1\}$, $\{\delta_1, \delta_2, \ldots, \delta_{d-1}\} = \{2^1, 2^2, \ldots, 2^{d-1}\}$. □

In fact, we can specify exactly which permutations are valid in the case of $KG_{2^{d+1}-2}$.

Theorem 4 *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 $2^d - 1$.*

Proof. First, we show that if $2^k - 1$ is relatively prime to $2^d - 1$ (note that $2^d - 1 = \frac{n}{2}$), then k is relatively prime to d. Suppose, to the contrary, that $2^k - 1$ is relatively prime to $\frac{n}{2}$, and k is not relatively prime to d. In that case, let a be the smallest integer such that $ak \equiv 0 \pmod d$. (We know that $a < d$.) It follows that $2^{ak} \equiv 1 \,(\bmod \frac{n}{2})$. From $2^{ak} - 1 = (2^k - 1)(2^{(a-1)k} + 2^{(a-2)k} + \cdots + 2^k + 1)$, we get

$(2^k-1)(2^{(a-1)k}+2^{(a-2)k}+\cdots+2^k+1)=0$. Since the second term of this product cannot be 0, we know that 2^k-1 is not a unit in $Z_{\frac{n}{2}}$. Thus, if 2^k-1 is relatively prime to $\frac{n}{2}$, then k is relatively prime to d.

Let $\pi_1, \pi_2, \ldots, \pi_d$ be any valid permutation. As a cyclic shift is also a valid permutation, we can assume that $\pi_1 = 0$. We will prove that the permutation is of the form $0, k, 2k, \ldots, (d-1)k$ by showing that $\pi_i - \pi_{i+1} \equiv \pi_d \pmod d$ (here $k = -\pi_d$). In the proof we will frequently use the fact that $2^d \equiv 1 \pmod{\frac{n}{2}}$ and so, for example, $2^{-i} = 2^{d-i}$ for $0 \le i \le d-1$.

By Theorem 3, we have $2^{\pi_i} - 2^{\pi_{i+1}} = (2^{\pi_d} - 2^{\pi_1})2^{c_i}$ for some c_i, $0 \le c_i \le d-1$. As $\pi_1 = 0$, we obtain the equality (modulo $\frac{n}{2}$) $2^{\pi_i-\pi_{i+1}} - 1 = 2^{\pi_d+c_i-\pi_{i+1}} - 2^{c_i-\pi_{i+1}}$. There are two cases to consider. Consider the case: $2^{\pi_d+c_i-\pi_{i+1}} > 2^{c_i-\pi_{i+1}}$. The first member of the equality is odd and the second can be odd only if $c_i = \pi_{i+1}$ which implies that $2^{\pi_i} - 2^{\pi_{i+1}} = 2^{\pi_d}$ or $\pi_i - \pi_{i+1} \equiv \pi_d \pmod d$. Consider the case: $2^{\pi_d+c_i-\pi_{i+1}} < 2^{c_i-\pi_{i+1}}$. In this case, the equality becomes $2^{\pi_i-\pi_{i+1}} - 1 = 2^{\pi_d+c_i-\pi_{i+1}} - 2^{c_i-\pi_{i+1}} + 2^d - 1$ or $2^{\pi_i-\pi_{i+1}} - 2^{\pi_d+c_i-\pi_{i+1}} = -2^{c_i-\pi_{i+1}} + 2^d$. Let us divide the two members of this equality by $\min(2^{\pi_i-\pi_{i+1}}, 2^{\pi_d+c_i-\pi_{i+1}})$. After division, the second member is still even as $2^{\pi_d+c_i-\pi_{i+1}} < 2^{c_i-\pi_{i+1}}$. After division, the first member is odd unless $2^{\pi_i-\pi_{i+1}} = 2^{\pi_d+c_i-\pi_{i+1}}$ in which case its value is 0. That implies that $2^{c_i-\pi_{i+1}} = 2^d$ so $c_i = \pi_{i+1}$ and again $\pi_i - \pi_{i+1} \equiv \pi_d \pmod d$.

So, any valid permutation is a cyclic shift of the form $0, k, 2k, \ldots, (d-1)k$. As it is a permutation, all of the values ik, $0 \le i \le d-1$, should be distinct and so k is relatively prime with d. Furthermore, by Theorem 2, $2^{\pi_d} - 1$ is relatively prime to $\frac{n}{2}$, that is $2^k - 1$ is relatively prime to $\frac{n}{2}$.

Finally, it is easy to check that any permutation of the form $0, k, 2k, \ldots, (d-1)k$ satisfying the conditions of Theorem 4 is valid. Indeed, condition (1) of Theorem 3 is satisfied and condition (2) is also satisfied as $2^{\pi_i} - 2^{\pi_{i+1}} = 2^{\pi_{i+1}-k} - 2^{\pi_{i+1}} = (2^{-k}-1)\cdot 2^{\pi_{i+1}} = (2^{\pi_d} - 2^{\pi_1})\cdot 2^{\pi_{i+1}}$ and as the set $\{2^{\pi_{i+1}} \mid 0 \le i \le d-1\} = \{2^j \mid 0 \le j \le d-1\}$. $\square$

Acknowledgements

Bermond and Perennes were supported by the French cooperation program PICS. Harutyunyan and Liestman were supported by the Natural Sciences and Engineering Research Council of Canada.

References

1. P. Fraigniaud and J. G. Peters, Maximum Linear (Δ, k)-Gossip Graphs, Simon Fraser University tech. report TR-94-06, 1994.
2. S. T. Hedetniemi,S. M. Hedetniemi, and A. L. Liestman, A Survey of Broadcasting and Gossiping in Communication Networks, *Networks* 18, pp. 319–349, 1988.
3. W. Knödel, New Gossips and Telephones, *Discr. Math.* 13, p. 95, 1975.
4. F. T. Leighton, Introduction to Parallel Algorithms and Archtectures, Morgan Kauffman, San Mateo, 1992.
5. R. Labahn and A. L. Liestman, Minimum Periodic Gossip Graphs, manuscript, 1996.

6. A. L. Liestman and D. Richards, Toward Optimal Gossiping Schemes with Conference Calls, *Discr. Appl. Math.* 7, pp. 183–189, 1984.
7. A. L. Liestman and D. Richards, More Perpetual Gossiping, manuscript, 1996.
8. D. A. Reed and R. M. Fujimoto, Multicomputer Networks: Message-Based Parallel Processing, MIT Press, Cambridge, 1987.
9. E. Upfal, private communication.