

LABORATOIRE



INFORMATIQUE, SIGNAUX ET SYSTÈMES
DE SOPHIA ANTIPOLIS
UMR 6070

CONCERNING TWO CONJECTURES ON THE SET OF FIXED
POINTS OF A COMPLETE ROTATION OF A CAYLEY
DIGRAPH

N. Lichiardopol

Projet RECIF

Rapport de recherche
I3S/RR-2002-44-FR

Septembre 2002

RÉSUMÉ :

En 1996, J-C Bermond, T. Kodate et S. Perennes ont conjecturé que l'ensemble des points fixes de l'une des rotation complète de la grille torique n'est pas séparateur. Ils ont aussi conjecturé que l'ensemble des points fixes de toute rotation complète d'un graphe de Cayley n'est pas séparateur. Dans ce papier, nous prouvons la première conjecture et donnons un contre-exemple pour la seconde.

MOTS CLÉS :

Graphe de Cayley, rotation complète, points fixes, ensemble séparateur

ABSTRACT:

In 1996, J-C bermond, T. Kodate, N. Marlin and S. Perennes conjectured that the set of fixed points of some complete rotation of the toroidal mesh is not separating. They also conjectured that the set of fixed points of any complete rotation of any Cayley digraph is not separating. In this paper, we prove the first conjecture and disprove the second one.

KEY WORDS :

Cayley digraph, complete rotation, fixed points, separating set

Concerning two conjectures on the set of fixed points of a complete rotation of a Cayley digraph

Nicolas Lichiardopol¹

13S², ESSI, 930, route des Colles, BP 145, 06903 Sophia Antipolis

Abstract

In 1996, J.C Bermond, T. Kodate, N. Marlin and S. Perennes conjectured that the set F_σ of fixed points of some complete rotation σ of the toroidal mesh $T.M(p)^k$ is not separating (that is F_σ does not disconnect $T.M(p)^k$).

They also conjectured that the set F_ω of fixed points of any complete rotation ω of any Cayley digraph is not separating.

In this paper, we prove the first conjecture and disprove the second one.

Keywords : Cayley digraph, complete rotation, fixed points, separating set.

Introduction

In [1] J.C Bermond, T. Kodate, S. Perennes consider a gossiping problem. They prove that for any Cayley digraph G with a complete rotation ω , the minimum gossiping time of G is optimal if the set F_ω of fixed points of ω is not separating and independent.

J.C Bermond, T. Kodate, S. Perennes and N. Marlin then proposed the following conjectures :

Conjecture 1: The set F_σ of fixed points of some complete rotation σ of the toroidal mesh $T.M(p)^k$ is not separating.

Conjecture 2 : The set F_ω of fixed points of any complete rotation ω of a Cayley digraph is not separating.

In this paper, we prove Conjecture 1 and as F_σ is an independent set, this implies that the minimum gossiping time of the toroidal mesh is optimal. We also invalidate Conjecture 2.

¹ *E-mail address* : lichiar@club-internet.fr

² This work was done while the author was at Inria Sophia Antipolis.

The invalidating example for Conjecture 2, shows that even when the gossiping time of a rotational Cayley digraph is optimal, the set of fixed points may be separating.

2. Definitions and notation

Definition 2.1. Let Γ be a group, and S be a generating set of Γ such that :

- $e \notin S$, e being the identity in Γ .

- $s \in S \Leftrightarrow s^{-1} \in S$.

The associated Cayley digraph $\text{Cay}(\Gamma, S)$ is the digraph whose vertices are the elements of Γ and whose arcs are the couples (x, sx) for $x \in \Gamma$ and $s \in S$.

With this definition, $\text{Cay}(\Gamma, S)$ is a connected symmetric digraph (in fact a strongly connected digraph). Therefore we may also consider it as a connected regular undirected graph, where each vertex has degree $d = |S|$.

If $S = \{s_0, \dots, s_{d-1}\}$, then for $t \in \mathbb{Z}$ we consider $s_t = s_r$, where r is the unique element of $\{0, \dots, d-1\}$ such that $t \equiv r \pmod{d}$.

We now recall the definition of a toroidal mesh :

Definition 2.2. For $p \in \mathbb{N}$, $p \geq 3$ and $k \in \mathbb{N}^*$, the toroidal mesh $T.M(p)^k$ is the Cayley digraph $\text{Cay}(\mathbb{Z}_p^k, S)$, where $S = \{s_0, \dots, s_{2k-1}\}$ with :

$s_0 = (1, 0, \dots, 0), \dots, s_{k-1} = (0, \dots, 0, 1)$ and $s_{k+i} = -s_i$ for $0 \leq i \leq k-1$.

The toroidal mesh $T.M(p)^k$ is a regular digraph of degree $2k$ with p^k vertices. Its diameter is $k \left\lceil \frac{p}{2} \right\rceil$ and its vertex-connectivity is $2k$.

Definition 2.3. Let $G = \text{Cay}(\Gamma, S)$ be a Cayley digraph with $|S| = d$.

A complete rotation of G is an automorphism ω of Γ such that for some ordering s_0, \dots, s_{d-1} of the elements of S , we have :

$\omega(s_t) = s_{t+1}$ for every $t \in \mathbb{Z}$.

A Cayley digraph with a complete rotation is called a rotational Cayley digraph. The toroidal mesh is a rotational Cayley digraph. Indeed, the mapping $\sigma : \mathbb{Z}_p^k \rightarrow \mathbb{Z}_p^k$ defined by :

$\sigma(x_0, \dots, x_{k-1}) = (-x_{k-1}, x_0, \dots, x_{k-2})$

is a complete rotation of the Cayley digraph $T.M(p)^k$ with $\sigma(s_t) = s_{t+1}$ for $t \in \mathbb{Z}$.

Remark : If ω is a complete rotation of a Cayley digraph $G = \text{Cay}(\Gamma, S)$ with $|S| = d$, we have $\omega^l(s_t) = s_{t+l}$ for $l, t \in \mathbb{Z}$. We also have $\omega^d(x) = x$ for each vertex $x \in \Gamma$.

Definition 2.4. Let $G = \text{Cay}(\Gamma, S)$ be a Cayley digraph with $|S| = d$ and let ω be a complete rotation of G .

An element $x \in \Gamma$ is said to be a fixed point of ω , if $x \neq e$ and if there exists $i \in \{1, \dots, d-1\}$ such that $\omega^i(x) = x$.

We note F_ω the set of fixed points of ω and $F'_\omega = F_\omega \cup \{e\}$.

It is obvious that for all t , $0 \leq t \leq d-1$, s_t is not a fixed point.

For $x \in F'_\omega$ let $i = \text{Min}\{j \in \mathbb{N}^* ; \omega^j(x) = x\}$. Clearly, $i < d$ and $i | d$.

For $i \in \mathbb{N}^*$ we note $W_{\omega,i} = \{x \in \Gamma ; \omega^i(x) = x\}$.

Clearly, $W_{\omega,i}$ is a subgroup of Γ , $W_{\omega,d} = \Gamma$ and $F'_\omega = \bigcup_{i|d, i < d} W_{\omega,i}$.

We can also verify that if $x \in W_{\omega,i}$, then for every $l \in \mathbb{Z}$ we have $\omega^l(x) \in W_{\omega,i}$.

We now determine the sets $W_{\omega,i}$ in the particular case of the toroidal mesh :

Proposition 2.5. For the toroidal mesh $T.M(p)^k = \text{Cay}(Z_p^k, S)$ with its complete rotation σ , and for $i | 2k$, $i < 2k$:

a) If i is not a divisor of k (then $2 | i$) we have :

$$W_{\sigma,i} = \left\{ (U, -U, \dots, U, -U, U); U \in Z_p^{\frac{i}{2}} \right\}$$

and therefore $|W_{\sigma,i}| = p^{\frac{i}{2}}$.

b) If $i | k$ and if p is even, we have :

$$W_{\sigma,i} = \left\{ (U, \dots, U); U \in \left\{ 0, \frac{p}{2} \right\}^i \right\}$$

and therefore $|W_{\sigma,i}| = 2^i$ and $2x = 0$ for $x \in W_{\sigma,i}$.

c) If $i | k$ and if p is odd, then $W_{\sigma,i} = \{0\}$ and so $|W_{\sigma,i}| = 1$.

Proof. a) We have $i = 2j$, $2k = l \times 2j$.

Note that l is not even, as otherwise we have $2j | k$ and hence $i | k$, which is false by hypothesis.

Therefore, l is odd and we have $k = (2m+1)\frac{i}{2}$ with $m \geq 1$ (because $i < 2k$).

Consider now a vertex $x \in W_{\sigma, i}$.

We have $x = (U_1, \dots, U_{2m+1})$ where $U_r \in \mathbb{Z}_p^{\frac{i}{2}}$ for $1 \leq r \leq 2m+1$.

Since $\sigma^i(x) = x$, we have :

$$(U_1, U_2, \dots, U_{2m+1}) = (-U_{2m}, -U_{2m+1}, U_1, \dots, U_{2m-1})$$

Hence :

$$U_1 = U_3, \dots, U_{2m-1} = U_{2m+1}, \text{ and also } U_1 = -U_{2m} \text{ and } U_2 = -U_{2m+1}.$$

This implies : $U_1 = U_3 = \dots = U_{2m+1} = -U_{2m}$ and also $U_2 = \dots = U_{2m}$.

Then putting $U_1 = U$, we obtain $x = (U, -U, \dots, U, -U, U)$ with $U \in \mathbb{Z}_p^{\frac{i}{2}}$.

Conversely, it is clear that every element x of this form is in $W_{\sigma, i}$, and so the assertion is proved.

b) As $i \mid k$, we note $k = ji$ with $j \in \mathbb{N}^*$.

Let $x \in W_{\sigma, i}$. We note $x = (U_1, \dots, U_j)$, with $U_r \in \mathbb{Z}_p^i$ for $1 \leq r \leq j$. Then we have $\sigma^i(x) = (-U_j, U_1, \dots, U_{j-1})$.

As $\sigma^i(x) = x$, we get $U_1 = \dots = U_j$ and $U_1 = -U_j$. Then putting $U_1 = U$, we obtain

$$x = (U, \dots, U), \text{ with } U = -U \text{ which means } U \in \left\{0, \frac{p}{2}\right\}^i.$$

Conversely, it is clear that a vertex x of the above form is in $W_{\sigma, i}$. Consequently

$$W_{\sigma, i} = \left\{ (U, \dots, U); U \in \left\{0, \frac{p}{2}\right\}^i \right\}.$$

Obviously $|W_{\sigma, i}| = 2^i$ and $2x = 0$ for $x \in W_{\sigma, i}$ and so the assertion is proved.

c) Obvious, as $U = -U$ in \mathbb{Z}_p^i implies $U = 0$.

3. Proof of Conjecture 1.

For $p \geq 3$ and $k \geq 1$, let us consider the toroidal mesh $T.M(p)^k = \text{Cay}(\mathbb{Z}_p^k, S)$ with its complete rotation σ . We note $\Gamma = \mathbb{Z}_p^k$.

We must prove that the set F_σ of fixed points of σ is not separating.

By Proposition 2.5 if $k = 1$ and if p is odd, we have $F'_\sigma = \{0\}$ and $F_\sigma = \emptyset$ and so F_σ is not separating (F'_σ is also not separating because the vertex-connectivity of a

cycle is 2) and if $k = 1$ and p is even, we have $F'_\sigma = \left\{0, \frac{p}{2}\right\}$, $F_\sigma = \left\{\frac{p}{2}\right\}$ and

again F_σ is not separating (but no F'_σ).

Thus, for $k = 1$, Conjecture 1 is true, and so we consider the case $k \geq 2$.

Several intermediate results are necessary. We start with:

Proposition 3.1. *Let i, j be elements of \mathbb{N}^* .*

$W_{\sigma,i} - W_{\sigma,j} = \{x - y; x \in W_{\sigma,i}, y \in W_{\sigma,j}\}$ is a subgroup of Γ , invariant by σ .

Proof. Since $W_{\sigma,i}$ and $W_{\sigma,j}$ are subgroups of the abelian group Γ and since they are invariant by σ this result is obvious. \square

Proposition 3.2. *If x is an element of F'_σ , for every $t \in \{0, \dots, 2k-1\}$ we have $x + s_t \notin F'_\sigma$.*

Proof. Proposition 3.2 is obvious for $x = 0$. Let us suppose $x \neq 0$.

Since $x \in F'_\sigma$, there exists i , a proper divisor of $2k$ such that $x \in W_{\sigma,i}$.

Let us suppose that there exists $t_0 \in \{0, \dots, 2k-1\}$ such that $x + s_{t_0} \in F'_\sigma$. Then there exists an integer j verifying $j \mid 2k$, $j < 2k$ such that $x + s_{t_0} \in W_{\sigma,j}$.

Five cases may occur :

Case 1. p is odd.

Since $x \neq 0$ and $x + s_{t_0} \neq 0$ (otherwise we have $x \notin F'_\sigma$), x and $x + s_{t_0}$ are non null fixed points and by Proposition 2.5, i and j are not divisors of k .

Since we have $x + s_{t_0} \in W_{\sigma,j}$ and $x \in W_{\sigma,i}$, we deduce $s_{t_0} \in W_{\sigma,j} - W_{\sigma,i}$.

Since $s_t = \sigma^{t-t_0}(s_{t_0})$, and since $W_{\sigma,j} - W_{\sigma,i}$ is invariant by σ , then for every $t \in \{0, \dots, 2k-1\}$, we have $s_t \in W_{\sigma,j} - W_{\sigma,i}$ and $S \subseteq W_{\sigma,j} - W_{\sigma,i}$.

This implies $W_{\sigma,j} - W_{\sigma,i} = \mathbb{Z}_p^k$ and therefore $|W_{\sigma,j} - W_{\sigma,i}| = p^k$.

But $|W_{\sigma,j}| = p^{\frac{j}{2}}$, $|W_{\sigma,i}| = p^{\frac{i}{2}}$ and as the mapping $\phi: W_{\sigma,j} \times W_{\sigma,i} \rightarrow W_{\sigma,j} - W_{\sigma,i}$ defined by $\phi(u, v) = u - v$ is surjective, we have $|W_{\sigma,j} - W_{\sigma,i}| \leq |W_{\sigma,j} \times W_{\sigma,i}|$ that is

$$p^k \leq p^{\frac{i+j}{2}}.$$

Furthermore, as i and j are proper divisors of $2k$, both distinct from k , we have :

$$i < k \text{ and } j < k, \text{ hence } \frac{i}{2} + \frac{j}{2} < k \text{ and then } p^{\frac{i+j}{2}} < p^k.$$

By transitivity, we obtain $p^k < p^k$, a contradiction.

Case 2. p is even, i and j are not divisors of k .

The same proof as that of Case 1 applies.

Case 3. p is even, $i \mid k$, $j \mid k$.

By Proposition 2.5.b, we have $2x=0$, $2(x+s_{t_0})=0$, hence $2s_{t_0}=0$ which means $2=0$ in Z_p , impossible (as $p > 2$).

Case 4. p is even, i is a divisor of k and j is not.

Then $2x=0$ and $x+s_{t_0} \in W_{\sigma,j}$ implies $2(x+s_{t_0}) \in W_{\sigma,j}$ that is $2s_{t_0} \in W_{\sigma,j}$.

Since j is not a divisor of k , by Proposition 2.5.a we have :

$2s_{t_0} = (U, -U, \dots, U, -U, U)$ with $U \in Z_p^{\frac{j}{2}}$, and since $U \neq 0$ (because $2s_{t_0} \neq 0$), $2s_{t_0}$ contains at least three nonzero co-ordinates, which is a contradiction as $2s_{t_0}$ contains exactly one nonzero co-ordinate.

Case 5. p is even, i is not a divisor of k and $j|k$.

Same as Case 4 by exchanging the roles of x and $x+s_{t_0}$.

In all cases, we obtain a contradiction. Consequently for every $t \in \{0, \dots, 2k-1\}$, we can state $x+s_t \notin F'_\sigma$. □

This proposition means that F'_σ is an independent set of $T.M(p)^k$.

For positive integers i and j , recall that $i \vee j$ denotes the lowest common multiple of i and j .

The next two propositions concern the case $p \neq 4$.

Proposition 3.3. *We suppose here that $p \neq 4$.*

Let t and t' be two distinct elements of $\{0, \dots, 2k-1\}$ and let $x \in \Gamma$.

If there are integers i and j , proper divisors of $2k$ such that $x+s_t \in W_{\sigma,i}$ and $x+s_{t'} \in W_{\sigma,j}$, then $i \vee j = 2k$.

Proof. Let us note $m = i \vee j$. Since $i|2k$ and $j|2k$, we deduce $m|2k$.

Let us suppose $m < 2k$. Since $x+s_t \in W_{\sigma,i}$, $x+s_{t'} \in W_{\sigma,j}$, $i|m$ and $j|m$, we have :

$x+s_t \in W_{\sigma,m}$ and $x+s_{t'} \in W_{\sigma,m}$, and that implies $s_t - s_{t'} \in W_{\sigma,m}$.

This is impossible if m is not a divisor of k , because an element $x \neq 0$ of $W_{\sigma,m}$ is of the form : $x = (U, -U, \dots, U, -U, U)$ with $U \neq 0$, and so it contains at least three nonzero co-ordinates, while $s_t - s_{t'}$ contains at most two nonzero co-ordinates.

If m is a divisor of k , by Proposition 2.5 we have $2(s_t - s_{t'}) = 0$ and that implies $4=0$ in Z_p , which is impossible because $p \neq 2$ and $p \neq 4$.

Consequently, $m = 2k$ and $i \vee j = 2k$. □

For $x \in \Gamma$, we note $A_x = \{t \in \{0, \dots, 2k-1\}; x + s_t \in F'_\sigma\}$ and for $t \in A_x$, i_t is the smallest of the integer $j > 0$ such that $x + s_t \in W_{\sigma, j}$. Of course i_t is a proper divisor of $2k$.

For $n \in \mathbb{N}^*$, $\varphi(n)$ is the Euler's totient of n . It is known that $n = \sum_{d|n} \varphi(d)$ (see [3])

Now we can state :

Proposition 3.4. *We suppose again that $p \neq 4$.*

If x and y are distinct elements of Γ , then there exists $t_0 \in \{0, \dots, 2k-1\}$ such that :

$$x + s_{t_0} \notin F'_\sigma \text{ and } y + s_{t_0} \notin F'_\sigma.$$

Proof. By Proposition 3.3, for $t, t' \in A_x$, $t \neq t'$, we have $i_t \vee i_{t'} = 2k$ and that implies $i_t \neq i_{t'}$. If $|A_x| \geq 2$ we have also $i_t > 1$ for every $t \in A_x$.

Let us suppose $|A_x| \geq k$.

Since $k \geq 2$, $|A_x| \geq 2$ and then $2k$ has at least k proper divisors distinct from 1.

It is easy to verify that for $k \in \{2, 3\}$ this is impossible. And if $k \geq 4$, we have :

$$2k = \sum_{d|2k} \varphi(d), \text{ which implies } 2k \geq \varphi(2k) + \sum_{t \in A_x} \varphi(i_t).$$

Since $\varphi(n) \geq 2$, for $n \geq 3$, we obtain $2k \geq 2 + \varphi(2) + 2(k-1)$, that is $2k \geq 2k+1$, which is false.

Consequently, $|A_x| < k$ and we have also $|A_y| < k$, hence $|A_x \cup A_y| < 2k$ and so $A_x \cup A_y \subset \{0, \dots, 2k-1\}$.

Then, there exists $t_0 \in \{0, \dots, 2k-1\}$ such that $t_0 \notin A_x \cup A_y$, that is $x + s_{t_0} \notin F'_\sigma$ and $y + s_{t_0} \notin F'_\sigma$. □

Both following results concern a particular case :

Proposition 3.5. *We suppose here that $p = 4$. Let $x \in \Gamma$ and $t_0 \in \{0, \dots, 2k-1\}$. If $x + s_{t_0} \in W_{\sigma, k}$ then we have $x - s_{t_0} \in W_{\sigma, k}$ and for every $t \in \{0, \dots, 2k-1\}$ such that k does not divide $t - t_0$, we have $x + s_t \notin F'_\sigma$.*

Proof. We can write $x - s_{t_0} = x + s_{t_0} - 2s_{t_0}$ and if we have $x + s_{t_0} \in W_{\sigma, k}$ then, since $2s_{t_0} \in W_{\sigma, k}$, we deduce $x - s_{t_0} \in W_{\sigma, k}$.

Let us suppose that for some $t \in \{0, \dots, 2k-1\}$ such that k does not divide $t - t_0$ we have $x + s_t \in F'_\sigma$. Then there exists $j | 2k$, $j < 2k$ such that $x + s_t \in W_{\sigma, j}$.

If $j \mid k$ we have $2(x + s_{t_0}) = 2(x + s_t) = 0$, hence $2(s_{t_0} - s_t) = 0$. Since $t \neq t_0$ and $t \neq t_0 + k$ in Z_{2k} , we deduce $2 = 0$ in Z_4 , a contradiction.

If j is not a divisor of k , since $2(x + s_{t_0}) = 0$, we deduce :

$2(s_{t_0} - s_t) = 2(x + s_{t_0}) - 2(x + s_t) = -2(x + s_t) = 2(x + s_t)$. since $x + s_t \in W_{\sigma, j}$ we have $2(s_{t_0} - s_t) \in W_{\sigma, j}$.

Now, this is impossible, because $2(s_{t_0} - s_t)$ has exactly two nonzero co-ordinates, while a nonzero element of $W_{\sigma, j}$ has at least three nonzero co-ordinates.

So $x + s_t \in F'_\sigma$ is no possible and consequently the result is proved. \square

We continue with :

Proposition 3.6. *We suppose again $p = 4$. Let $x \in \Gamma$ and let $t_0 \in \{0, \dots, 2k - 1\}$. If $x + s_{t_0} \in F'_\sigma \setminus W_{\sigma, k}$, we have $|A_x| < k$.*

Proof. For every $t \in A_x$ we have $x + s_t \in F'_\sigma \setminus W_{\sigma, k}$

Indeed, if for an element $t \in A_x$, we have $x + s_t \in W_{\sigma, k}$, then by Proposition 3.5 either $x + s_{t_0} \in W_{\sigma, k}$ or $x + s_{t_0} \notin F'_\sigma$ and both cases are excluded (by hypothesis).

Then, for $t, t' \in A_x$, $t \neq t'$, we have $x + s_t \in W_{\sigma, i_t}$, $x + s_{t'} \in W_{\sigma, i_{t'}}$.

Let us remark that i_t and $i_{t'}$ are proper divisors of $2k$ but not divisors of k (otherwise $x + s_t \in W_{\sigma, k}$ or $x + s_{t'} \in W_{\sigma, k}$).

Let us note $m = i_t \vee i_{t'}$.

It is clear that m is not a divisor of k . We have $x + s_t \in W_{\sigma, m}$ and $x + s_{t'} \in W_{\sigma, m}$, hence $s_t - s_{t'} \in W_{\sigma, m}$. Again arguing on the number of nonzero co-ordinates, it is easy to conclude that for $m < 2k$, this is not possible.

Consequently, $m = 2k$ and $i_t \vee i_{t'} = 2k$. Then, as in the proof of Proposition 3.4 we obtain $|A_x| < k$. \square

Here is now a synthesis of three previous results :

Proposition 3.7. *If $p \neq 4$, $k \geq 2$ and if x, y are distinct elements of Γ , there exists $t_0 \in \{0, \dots, 2k - 1\}$ such that $x + s_{t_0} \notin F'_\sigma$ and $y + s_{t_0} \notin F'_\sigma$.*

This result also holds for $p = 4$ and $k > 2$.

Proof. For $p \neq 4$, $k \geq 2$, the result is already proved.

For $p = 4$ and $k > 2$, the two previous propositions imply that, for $x \in \Gamma$, we have either $|A_x| < k$ or $|A_x| = 2$ and therefore $|A_x| < k$.

The remaining part may be proved as in the final part of the proof of Proposition 3.4. \square

We can state that this proposition is false for $p = 4$ and $k = 2$. For example if we take $x = (1, 2)$ and $y = (2, 1)$ we can very easily verify that there exists no s_{t_0} such that $x + s_{t_0} \notin F'_\sigma$ and $y + s_{t_0} \notin F'_\sigma$.

Before proving Conjecture 1, we give a slightly stronger result :

Theorem 3.8. *For $p \geq 3$ and $k \geq 2$, F'_σ is not a separating set of the toroidal mesh $T.M(p)^k$.*

Proof. For $p = 4$ and $k = 2$, we have $F'_\sigma = \{(0, 0), (0, 2), (2, 0), (2, 2)\}$ and it is easy to verify that this set is not separating.

Consequently we now consider $(p, k) \neq (4, 2)$.

We only have to prove that the digraph $T.M(p)^k - F'_\sigma$ is strongly connected. As $G = T.M(p)^k$ is a symmetric digraph, we only have to prove that for distinct elements x, y of Γ/F'_σ , there exists a directed path from x to y in $G - F'_\sigma$, that is, a path using no vertex of F'_σ .

We prove it by induction on the distance $m = d_G(x, y)$ between x and y (so $m \leq D(G)$).

For $m = 1$, it is obvious.

For $m = 2$, if x and y are vertices of Γ/F'_σ such that $d_G(x, y) = 2$, then there exists a directed path $C = (x, x + s_{t_1}, x + s_{t_1} + s_{t_2} = y)$ of G .

If $x + s_{t_1} \notin F'_\sigma$, C is a directed path in $G - F'_\sigma$ and then the assertion is proved for $m = 2$.

Suppose now that $x + s_{t_1} \in F'_\sigma$. By Proposition 3.7, there exists $t \in \{0, \dots, 2k - 1\}$ such that $x + s_t \notin F'_\sigma$ and $y + s_t \notin F'_\sigma$ and since $x + s_{t_1} \in F'_\sigma$, by Proposition 3.2, we have $x + s_{t_1} + s_t \notin F'_\sigma$.

Therefore $C_1 = (x, x + s_t, x + s_{t_1} + s_t, x + s_{t_1} + s_t + s_{t_2} = y + s_t, y)$ is a directed path in $G - F'_\sigma$ and the assertion is proved for $m = 2$.

Let us suppose that the assertion is true up to $m - 1$, $3 \leq m \leq D(G)$ and let us prove it for m .

So, if $d_G(x, y) = m$, there exists a directed path :

$C = (x, x + s_{t_1}, x + s_{t_1} + s_{t_2}, x + s_{t_1} + s_{t_2} + s_{t_3}, \dots, x + s_{t_1} + \dots + s_{t_1} = y)$ of length m .

If $x + s_{t_1} \notin F'_\sigma$, since $d_G(x + s_{t_1}, y) = m - 1$, by induction hypothesis, there exists a directed path from $x + s_{t_1}$ to y in $G - F'_\sigma$. If this path uses x , then we can extract from it a directed path of $G - F'_\sigma$ linking x to y .

And if this directed path does not use the vertex x , assembling it with the arc $(x, x + s_{t_1})$, we again obtain a directed path of $G - F'_\sigma$ linking x to y .

If $x + s_{t_1} \in F'_\sigma$, by Proposition 3.2 we have $x + s_{t_1} + s_{t_2} \notin F'_\sigma$.

Since $d_G(x, x + s_{t_1} + s_{t_2}) = 2$ and $d_G(x + s_{t_1} + s_{t_2}, y) = m - 2$, then, by induction hypothesis, there exists a directed path C_1 from x to $x + s_{t_1} + s_{t_2}$ and a directed path C_2 from $x + s_{t_1} + s_{t_2}$ to y , both in $G - F'_\sigma$.

Assembling these paths (while possibly eliminating some vertices), we obtain a directed path in $G - F'_\sigma$ linking x to y and the assertion is still verified. Being verified for m , the assertion holds for every $m \leq D(G)$, and consequently the theorem is proved. \square

We now prove Conjecture 1 :

Theorem 3.9. *For $p \geq 3$ and $k \geq 1$ the set F_σ of fixed points of the complete rotation σ does not disconnect the toroidal mesh $T.M(p)^k$.*

Proof. The case $k = 1$ has already been seen. So, we consider $k \geq 2$.

Let x, y , be distinct elements of $\Gamma \setminus F_\sigma$.

If $x \neq 0$ and $y \neq 0$, x and y are in $\Gamma \setminus F'_\sigma$ and by Theorem 3.9., there exists a directed path of $G - F'_\sigma$ linking x to y . This path is also a path of $G - F_\sigma$, hence x and y are linked in $G - F_\sigma$.

If $x = 0$, $s_0 \in \Gamma \setminus F'_\sigma$ and $y \in \Gamma \setminus F'_\sigma$ are linked by a path in $G - F'_\sigma$ and then, assembling with the arc $(0, s_0)$, we obtain a directed path in $G - F_\sigma$ linking x to y .

Similar reasoning holds if $y = 0$.

So, we can always link x to y in $G - F_\sigma$ and consequently the theorem is proved.

4. Invalidation of Conjecture 2.

We start with some results from number theory.

For $p \in \mathbb{N}$, $p \geq 2$ and $a \in \mathbb{N}^*$, we note $Val_p(a)$ the greatest integer m such that $p^m \mid a$.

We note $a \wedge b$ the greatest common divisor of a and b .

Lemma 4.1. *Let a and b be integer with $a \wedge b = 1$.*

If $3 \mid a - b$, then $Val_3(a^2 + ab + b^2) = 1$.

Proof. From $a^2 + ab + b^2 = (a-b)^2 + 3ab$ and the conditions of Lemma 4.1, it is easy to prove that while 3 divides $a^2 + ab + b^2$, 3^2 does not. \square

Lemma 4.2. For any $k \in \mathbb{N}$ we have $\text{Val}_3\left(2^{2 \times 3^k} - 1\right) = k + 1$.

Proof. We have $2^{2 \times 3^{k+1}} - 1 = \left(2^{2 \times 3^k} - 1\right)\left(2^{4 \times 3^k} + 2^{2 \times 3^k} + 1\right)$

Using Lemma 4.1 with $a = 2^{2 \times 3^k}$ and $b = 1$, it is easy to prove the assertion by induction on k . \square

Proposition 4.3 For $n \geq 1$:

- a) $2^{2 \times 3^{n-1}} - 1 = 0$ in Z_{3^n} .
- b) $2^{3^{n-1}} + 1 = 0$ in Z_{3^n} .
- c) For every l verifying $1 \leq l < 2 \times 3^{n-1}$, $2^l - 1 \neq 0$ in Z_{3^n} .

Proof. a) By Lemma 4.2, we have $\text{Val}_3\left(2^{2 \times 3^{n-1}} - 1\right) = n$.

This implies $3^n \mid 2^{2 \times 3^{n-1}} - 1$ and so $2^{2 \times 3^{n-1}} - 1 = 0$ in Z_{3^n} .

b) We have $2^{2 \times 3^{n-1}} - 1 = \left(2^{3^{n-1}} - 1\right)\left(2^{3^{n-1}} + 1\right)$

As $2 \equiv -1 \pmod{3}$ we get $2^{3^{n-1}} \equiv (-1)^{3^{n-1}} \pmod{3}$ that is $2^{3^{n-1}} \equiv (-1) \pmod{3}$ and then $2^{3^{n-1}} - 1 \equiv (-2) \pmod{3}$.

Consequently, 3 does not divide $2^{3^{n-1}} - 1$.

As by Proposition 4.3.a, $3^n \mid \left(2^{3^{n-1}} - 1\right)\left(2^{3^{n-1}} + 1\right)$, we deduce $3^n \mid 2^{3^{n-1}} + 1$ and so $2^{3^{n-1}} + 1 = 0$ in Z_{3^n} .

c) Let d be the smallest of the integers $m > 0$ such that $3^n \mid 2^m - 1$.

Since $2 \equiv -1 \pmod{3}$, we obtain $2^d \equiv (-1)^d \pmod{3}$ and $2^d - 1 \equiv 0 \pmod{3}$ implies that d is even.

As usually we note $Z_{3^n}^*$ the multiplicative group of nonzero elements of Z_{3^n} . We know that $\left|Z_{3^n}^*\right| = \varphi(3^n) = 2 \times 3^{n-1}$

As d is the order of 2 in $Z_{3^n}^*$ by Cauchy's theorem we have $d \mid 2 \times 3^{n-1}$ and then we get $d = 2 \times 3^k$ where $k \leq n-1$.

Since $3^n \mid 2^{2 \times 3^k} - 1$ and $\text{Val}_3(2^{2 \times 3^k} - 1) = k + 1$, we deduce $n \leq k + 1$. Hence $k \geq n - 1$ and then $k = n - 1$. Consequently $d = 2 \times 3^{n-1}$.
 Consequently, for $1 \leq l < 2 \times 3^{n-1}$ we have $2^l - 1 \neq 0$ in Z_{3^n} and so the assertion is proved. \square

We now consider the additive group $\Gamma_n = Z_{3^n}$ for $n \geq 3$.
 For each $a \in Z$ we note \hat{a} the class of a in Z_3 and \bar{a} the class of a in Z_{3^n} .
 It is clear that $\theta_n : \bar{a} \mapsto \hat{a}$ define a surjective morphism from Z_{3^n} into Z_3 .

We define the elements $s_{n,i} \in \Gamma_n$, $0 \leq i \leq 2 \times 3^{n-2} - 1$ by $s_{n,i} = \overline{2^{3i}}$.
 For $0 \leq i \leq 2 \times 3^{n-2} - 1$, $0 \leq j \leq 2 \times 3^{n-2} - 1$ with $i < j$ we have :
 $0 < 3(j-i) < 2 \times 3^{n-1} - 1$.
 By Proposition 4.3, we have $2^{3j-3i} \neq 1$ in Z_{3^n} that is $\overline{2^{3i}} \neq \overline{2^{3j}}$.
 Consequently, the elements $s_{n,i}$, $0 \leq i \leq 2 \times 3^{n-2} - 1$ are all distinct.
 Since $s_{n,0} = \bar{1}$ is a generator of the group Γ_n , $S_n = \{s_{n,i} ; 0 \leq i \leq 2 \times 3^{n-2} - 1\}$ is a generating set of Γ_n .

Using Proposition 4.3.b, for $0 \leq i \leq 3^{n-2} - 1$ we have :

$$s_{n,i} + s_{n,i+3^{n-2}} = \overline{2^{3i}} + \overline{2^{3(i+3^{n-2})}} = \overline{2^{3i} (2^{3^{n-1}} + 1)} = \bar{0}.$$

Therefore $s_{n,i+3^{n-2}} = -s_{n,i}$ and consequently $s \in S_n \Leftrightarrow -s \in S_n$.

Clearly, $\bar{0} \notin S_n$. Therefore for $n \geq 3$ we can define the Cayley digraph $G_n = \text{Cay}(\Gamma_n, S_n)$.

For $i \in \{0, \dots, 2 \times 3^{n-2} - 1\}$ we have $2^3 \equiv -1 \pmod{9}$ whence $2^{3i} \equiv (-1)^i \pmod{9}$.
 Consequently, $s_{n,i}$ is of the form $\overline{9k + (-1)^i}$ and moreover $\theta_n(s_{n,i}) = (-1)^i$.
 The $2 \times 3^{n-2}$ elements of S_n are of the form $\overline{9k \pm 1}$ and since they are $2 \times 3^{n-2}$ elements of this type, we conclude that S_n is exactly the set of elements of the form $\overline{9k \pm 1}$

For $t \in Z$ we note $s_{n,t} = s_{n,r}$ where r is the unique element of $\{0, \dots, 2 \times 3^{n-2} - 1\}$ such that $t \equiv r \pmod{2 \times 3^{n-2}}$. It is easy to prove that $s_{n,t} = \left(\overline{2^3}\right)^t$.

Let $\omega_n : \Gamma_n \rightarrow \Gamma_n$, be the mapping defined by $\omega_n(x) = 2^3 x$. Clearly ω_n is a group automorphism and for $t \in Z$, we have : $\omega_n(s_{n,t}) = 2^3 \overline{2^{3t}} = \overline{2^{3(t+1)}} = s_{n,t+1}$.

Consequently, ω_n is a complete rotation of Γ_n .

It is easy to prove that if i is a positive integer, then for every element $x \in \Gamma_n$ we have $\omega_n^i(x) = 2^{3i}x$.

Now, we characterise the fixed points of ω_n :

Proposition 4.4. *The set of fixed points of ω_n is :*

$$F_{\omega_n} = \{\bar{x}; 0 < x \leq 3^n - 1, 3 \mid x\}.$$

Proof. Let \bar{a} , be an element of F_{ω_n} .

There exists $i \in \{1, \dots, 2 \times 3^{n-2} - 1\}$ such that $\omega_n^i(\bar{a}) = \bar{a}$, that is, $2^{3i}\bar{a} = \bar{a}$.

This means that $3^n \mid a(2^{3i} - 1)$. As $i \in \{1, \dots, 2 \times 3^{n-2} - 1\}$ we get the inequality $0 < 3i < 2 \times 3^{n-1} - 1$. Then, by Proposition 4.3.c, we have $\text{Val}_3(2^{3i} - 1) < n$ which implies $3 \mid a$.

So we have $F_{\omega_n} \subseteq \{\bar{x}; 0 < x \leq 3^n - 1, 3 \mid x\}$.

Conversely, let \bar{a} be an element of $\{\bar{x}; 0 < x \leq 3^n - 1, 3 \mid x\}$.

We have $\bar{a} = 3\bar{b}$ with $1 \leq b \leq 3^{n-1} - 1$ and $\omega^{2 \times 3^{n-3}}(\bar{a}) = 2^{2 \times 3^{n-2}}\bar{a} = 3 \times 2^{2 \times 3^{n-2}}\bar{b}$.

By Proposition 4.2.a, we have $3^{n-1} \mid 2^{2 \times 3^{n-2}} - 1$ which implies $3^n \mid 3 \times 2^{2 \times 3^{n-2}}\bar{b} - 3\bar{b}$

and therefore $3 \times 2^{2 \times 3^{n-2}}\bar{b} = 3\bar{b}$ that is $\omega^{2 \times 3^{n-3}}(\bar{a}) = \bar{a}$. Since $2 \times 3^{n-3} < 2 \times 3^{n-2}$, \bar{a} is a fixed point and therefore $\{\bar{x}; 0 < x \leq 3^n - 1, 3 \mid x\} \subseteq F_{\omega_n}$.

Both inclusions imply our assertion. □

With this proposition, it is clear that $|F'_{\omega_n}| = 3^{n-1}$.

It is also clear that $F_{\omega_n} = \{\bar{x} \neq \bar{0}; \theta_n(\bar{x}) = \hat{0}\}$.

Lemma 4.5 *Let \bar{u} and \bar{v} , be distinct elements of $\Gamma_n \setminus F'_{\omega_n}$.*

Let $(\bar{u}, \bar{u} + s_{n,t_1}, \dots, \bar{u} + s_{n,t_1} + \dots + s_{n,t_m} = \bar{v})$, be a directed path from \bar{u} to \bar{v} using no vertex of F'_{ω_n} . Then :

- a) $\theta_n(s_{n,t_1}) = \theta_n(\bar{u})$ and $\theta_n(s_{n,t_m}) = -\theta_n(\bar{v})$
- b) If $m \geq 2$, for $1 \leq i \leq m-1$ we have $\theta_n(s_{n,t_{i+1}}) = -\theta_n(s_{n,t_i})$
- c) For $1 \leq i \leq m$, we have $\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_i}) = (-1)^i \theta_n(\bar{u})$

Proof. a) Since $\bar{u} \notin F'_{\omega_n}$ we have $\theta_n(\bar{u}) \in \{-\bar{1}, \bar{1}\}$ and as $\theta_n(s_{n,t_1}) \in \{-\bar{1}, \bar{1}\}$, we have either $\theta_n(s_{n,t_1}) = -\theta_n(\bar{u})$ or $\theta_n(s_{n,t_1}) = \theta_n(\bar{u})$.

The first equality implies $\theta_n(\bar{u} + s_{n,t_1}) = \hat{\theta}$, which is false by hypothesis.

Consequently, we have $\theta_n(s_{n,t_1}) = \theta_n(\bar{u})$.

Similarly, we prove $\theta_n(s_{n,t_m}) = -\theta_n(\bar{v})$.

b) If $m = 2$, it is obvious.

If $m \geq 3$, for $2 \leq i \leq m-1$ by Lemma 4.5.a we have:

$\theta_n(s_{n,t_{i+1}}) = \theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_i})$ hence

$$\theta_n(s_{n,t_{i+1}}) = \theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_{i-1}}) + \theta_n(s_{n,t_i}) = 2\theta_n(s_{n,t_i}).$$

This yields $\theta_n(s_{n,t_{i+1}}) = -\theta_n(s_{n,t_i})$ and this equality is also true for $i = 1$.

c) If $m = 1$ it is obvious.

If $m \geq 2$, for $2 \leq i \leq m$ we have :

$\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_i}) = \theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_{i-1}}) + \theta_n(s_{n,t_i})$ hence:

$$\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_i}) = 2\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_{i-1}})$$

This yields $\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_i}) = -\theta_n(\bar{u} + s_{n,t_1} + \dots + s_{n,t_{i-1}})$.

Now, the assertion can easily be proved by induction on i . □

Corollary 4.6 *Let \bar{u} and \bar{v} be distinct elements of $\Gamma_n \setminus F'_{\omega_n}$. Then :*

a) *If $\theta_n(\bar{u}) = -\theta_n(\bar{v})$, any directed path of even length from \bar{u} to \bar{v} , contains at least one vertex of F'_{ω_n} .*

b) *If $\theta_n(\bar{u}) = \theta_n(\bar{v})$, any directed path of odd length from \bar{u} to \bar{v} , contains at least one vertex of F'_{ω_n} .*

Proof. **a)** Let $C = (\bar{u}, \bar{u} + s_{n,t_1}, \dots, \bar{u} + s_{n,t_1} + \dots + s_{n,t_{2m}} = \bar{v})$ be a directed path of even length linking \bar{u} to \bar{v} . Suppose that C does not contain any vertex of F'_{ω_n} .

Then by Lemma 4.5.c we have $\theta_n(\bar{v}) = (-1)^{2m} \theta_n(\bar{u})$, that is $\theta_n(\bar{v}) = \theta_n(\bar{u})$, which is false by hypothesis. Consequently, C contains at least one element of F'_{ω_n} and so the assertion is proved.

b) The proof is similar. □

We finish with:

Proposition 4.7 *Let \bar{v} , be a vertex of G_n with $v \equiv 4 \pmod{9}$ or $v \equiv 5 \pmod{9}$.*

Any directed path from $\bar{0}$ to \bar{v} contains at least one vertex of F_{ω_n} .

Proof. First, suppose that $v \equiv 4 \pmod{9}$. Then we have $v = 9r + 4$ where r is an integer.

Suppose on the opposite, that there exists a directed path :

$C = (\bar{0}, s_{n,t_1}, \dots, s_{n,t_1} + \dots + s_{n,t_m} = \bar{v})$ from $\bar{0}$ to \bar{v} using no vertex of F_{ω_n} .

We know that the elements of S_n are of the form $\overline{9k \pm 1}$ and so $(\bar{0}, \bar{v})$ can not be an arc of G_n .

Consequently, $m \geq 2$ and so $C_I = (s_{n,t_1}, \dots, s_{n,t_1} + \dots + s_{n,t_m} = \bar{v})$ is a directed path of length $m - 1$ using no vertex of F'_{ω_n} (because $\bar{0}$ is not a vertex of C_I).

For $1 \leq i \leq m$ one can write $s_{n,t_i} = \overline{9k_i + (-1)^{t_i}}$ and then we have :

$$\bar{v} = \overline{9(k_1 \dots + k_m) + (-1)^{t_1} + \dots + (-1)^{t_m}}.$$

Two cases are possible :

Case 1 : $\theta_n(s_{n,t_1}) = \hat{1}$.

Then we have $s_{n,t_1} = \overline{9k_1 + 1}$. Since $\theta_n(\bar{v}) = 1 = \theta_n(s_{n,t_1})$, by Corollary 4.6.b, $m - 1$ is even and so m is odd.

By Proposition 4.5.b, we have $\theta_n(s_{n,t_2}) = \theta_n(s_{n,t_1}) = \hat{1}$ and then $s_{n,t_2} = \overline{9k_2 + 1}$.

Furthermore, for $i \geq 2$ we have $\theta_n(s_{n,t_i}) = \hat{1}$ if i is even and $\theta_n(s_{n,t_i}) = -\hat{1}$ if i is odd.

That means : $s_{n,t_i} = \overline{9k_i + 1}$ if i is even and $s_{n,t_i} = \overline{9k_i - 1}$ if i is odd.

As m is odd, we deduce : $(-1)^{t_1} + \dots + (-1)^{t_m} = 1$ and then $\bar{v} = \overline{9(k_1 \dots + k_m) + 1}$, a contradiction with $\bar{v} = \overline{9r + 4}$.

Case 2 : $\theta_n(s_{n,t_1}) = \hat{1}$

Then $s_{n,t_1} = \overline{9k_1 - 1}$. Since $\theta_n(\bar{v}) = 1 = -\theta_n(s_{n,t_1})$, by Corollary 4.6.a, $m - 1$ is odd and so m is even.

By Proposition 4.5.b, we have $\theta_n(s_{n,t_2}) = \theta_n(s_{n,t_1}) = -\hat{1}$ and so $s_{n,t_2} = \overline{9k_2 - 1}$.

Furthermore, for $i \geq 2$ we have $\theta_n(s_{n,t_i}) = \hat{1}$ if i is odd and $\theta_n(s_{n,t_i}) = -\hat{1}$ if i is even.

That means $s_{n,t_i} = \overline{9k_i + 1}$ if i is odd, and $s_{n,t_i} = \overline{9k_i - 1}$ if i is even.

As m is even, we get : $(-1)^{t_1} + \dots + (-1)^{t_m} = -1$ and then $\bar{v} = \overline{9(k_1 \dots + k_m) - 2}$, a contradiction with $\bar{v} = \overline{9r + 4}$.

In both cases we have a contradiction, consequently any directed path from $\bar{0}$ to \bar{v} contains at least one vertex of F_{ω_n} .

Suppose now that $v \equiv -4 \pmod{9}$.

Let $C = (\bar{0}, \bar{v}_1, \dots, \bar{v}_m = \bar{v})$ be a directed path from $\bar{0}$ to \bar{v} .

Then $C' = (\bar{0}, -\bar{v}_1, \dots, -\bar{v}_m = -\bar{v})$ is a directed path from $\bar{0}$ to $-\bar{v}$ and since $-v \equiv 4 \pmod{9}$, there exists an integer $i \in \{1, \dots, m - 1\}$ such that $-\bar{v}_i \in F_{\omega_n}$.

This implies $\bar{v}_i \in F_{\omega_n}$ and consequently the directed path C contains at least one vertex of F_{ω_n} . \square

We have proved that for $n \geq 3$ the set F_{ω_n} of fixed points of the complete rotation ω_n , disconnects the Cayley digraph $G_n = \text{Cay}(Z_{3^n}, S_n)$ and so Conjecture 2 is invalidated.

Moreover, we can prove that the minimum gossiping time of G_n is optimal, while the set F_{ω_n} of fixed points of ω_n is separating.

Acknowledgements

I would like to thank Claudine Peyrat and the referees for their helpful comments.

References

- [1] J.C Bermond, T. Kodate, S. Perennes, Gossiping in Cayley graphs by packets. In Conf. CCS95 (8 th Franco-Japanese and 4 th Franco-Chinese Conf. Combin. Comput. Sci. (Brest July 1995)), Lecture Notes in Comput. Sci. Vol.1120, Springer Verlag, 1995, pp. 301-305.
- [2] B. Ducourthal, M.C Heydemann, Cayley Graphs and Interconnection Networks, Vol. N.A.T.O , A.S.L of Kluiver.Academic Publishers, 1997.
- [3] E. Landau, Elementary number theory, Chelsea Publishing Company, New York, 1966
- [4] N. Marlin, Rotations complètes dans les graphes de Cayley, D.E.A of Nice-Sophia Antipolis University, France, 1996.
- [5] N. Marlin, Communications structurées dans les réseaux, Ph.D. Thesis of Nice-Sophia Antipolis University, France, 2000