A singular quartic curve over a finite field and the Trisentis game

Masakazu Yamagishi

Department of Mathematics,
Nagoya Institute of Technology,
Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
e-mail: yamagishi.masakazu@nitech.ac.jp
TEL: +81-52-735-5138
FAX: +81-52-735-5142

Abstract

The Trisentis game consists of a rectangular array of lights each of which also functions as a toggle switch for its (up to eight) neighboring lights. The lights are OFF at the start, and the object is to turn them all ON. We give explicit formulas for the dimension of the kernel of the Laplacian associated to this game as well as some variants, in some cases, by counting rational points of the singular quartic curve $(x + x^{-1} + 1)(y + y^{-1} + 1) = 1$ over finite fields. As a corollary, we have an affirmative answer to a question of Clausing whether the $n \times n$ Trisentis game has a unique solution if $n = 2 \cdot 4^k$ or $n = 2 \cdot 4^k - 2$.

Keywords: σ-game; σ^+-game; graph Laplacian; Lights Out; strong product; Kronecker product; Chebyshev polynomials.

MSC2010: 05C50, 11G20, 14G15, 31C20, 91A46.

1 Introduction

The $m \times n$ Trisentis game [2] consists of an $m \times n$ array of lights each of which also functions as a toggle switch for its (up to eight) neighboring lights. The lights are OFF at the start, and the object of this solitaire game is to turn them all ON, by switching some of the lights.

Theorem 1 (Clausing [2]). *(i) The $n \times n$ Trisentis game has no solution if n is odd.*

(ii) It has a solution if $n = 2 \cdot 4^k$ or $n = 2 \cdot 4^k - 2$ for some integer $k \geq 1$.

Conjecture 2 (ibid.). *(i) The $n \times n$ Trisentis game has a solution if n is even.*

(ii) The solution is unique if $n = 2 \cdot 4^k$ or $2 \cdot 4^k - 2$.

In this note, we give a proof of Conjecture 2(ii), thereby providing an alternative proof of Theorem 1(ii), by counting rational points of the singular quartic curve

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

over finite fields. Actually, we do more. We consider this game and its torus version, both with p colors where p is a prime number; each light can assume one of p colors instead of an ON/OFF state. The game has a unique solution if and only if the associated Laplacian is injective. For given m, n, and p, we can compute the kernel of the Laplacian by Gaussian elimination. But the numerical table of the dimension of the kernel gives very few indications as to the dependence on m, n, and p. We obtain explicit formulas for the dimension in some cases. See subsection 2.3 for precise statements.

It is known that the elliptic curve

$$x + x^{-1} + y + y^{-1} + 1 = 0 \tag{2}$$

plays an important role in the arithmetic of Lights Out puzzle, a similar solitaire game (cf. [4],[12]). In [4], we observed interesting patterns in the table of the dimension of the kernel of the Laplacian for Lights Out puzzle, and proved one of them by using the multiplication by 2 map on this elliptic curve. In the present note, the curve (1) plays a similar role as this elliptic curve.

In fact, these two games are just particular cases of the same scheme as follows (see [13] for the details). Let $\Lambda = \mathbb{Z}^2$ and let K be a field of positive characteristic. For a function $a : \Lambda \to K$ with finite support, consider the Laplacian (convolution operator) $f \mapsto \Delta_a(f) = f * a$ acting on the space of functions on Λ with values in K. A function is called a-harmonic if $\Delta_a(f) = 0$. If m and n are prime to the characteristic of K, then the dimension of the space of a-harmonic functions with period (m, n) is equal to the number of bi-torsion points of order (m, n) of an affine curve called the symbolic variety of a. The Lights Out game (on a torus, to be precise) is the case where $K = \mathbb{F}_2$ (the field with two elements) and the support of a is

$$\{(x, y) \in \mathbb{Z}^2 \,|\, |x| + |y| \leq 1\}.$$

The elliptic curve (2) is nothing but the symbolic variety for this a. The Trisentis game is the case where $K = \mathbb{F}_2$ and the support of a is

$$\{(x, y) \in \mathbb{Z}^2 \mid \max\{|x|, |y|\} = 1\},$$

for which the quartic curve (1) is the symbolic variety. This scheme works as well for higher dimensional lattices and for systems of convolution equations, where general affine varieties naturally appear.

The organization of this paper is as follows. In section 2, we begin with Sutner's σ-game and σ^+ game on a graph, and define the Laplacian. We then formulate the Trisentis game as well as some variants, and give statements of results. Section 3 is devoted to the proofs. After preparing about basic properties of Kronecker products, Chebyshev polynomials, and eigenstructure of adjacency matrices of some graphs, we are naturally lead to the quartic curve (1). We count rational points of this curve over an arbitrary finite field, and finally give proofs of the results.

We use the following notation.

- I is an identity matrix, whose degree will be clear from the context.
- p is a prime number.
- $\mathbb{F}_q$ is the finite field with q elements.
- P_n is a path graph with n vertices ($n \geq 2$), and C_n is a cycle graph with n vertices ($n \geq 3$).
- $\left(\frac{a}{q}\right)$ is the Jacobi symbol. We use this notation only for $q = p^f$ where p is an odd prime and $f \geq 1$. In this case $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)^f$ where $\left(\frac{a}{p}\right)$ is the Legendre symbol, hence we have

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } \gcd(a, p) = 1 \text{ and } \sqrt{a} \in \mathbb{F}_q, \\ -1 & \text{if } \gcd(a, p) = 1 \text{ and } \sqrt{a} \notin \mathbb{F}_q. \end{cases}$$

- $\#S$ is the cardinality of a set S.

2 Trisentis game

2.1 σ-game and σ^+-game on a graph

The σ-game and the σ^+-game were introduced by Sutner [10]. The following formulation is different from [10] in two respect. First, we only consider undirected graphs. Second, we allow p states instead of ON/OFF states. Let $G = (V(G), E(G))$ be a finite simple undirected graph, and p a prime number. A map from $V(G)$ to $\mathbb{F}_p$ is called a *configuration*. The set $\mathrm{Conf}_{G,p}$ of all configurations is a vector space over $\mathbb{F}_p$. Define the $\mathbb{F}_p$-linear map $\sigma_{G,p} : \mathrm{Conf}_{G,p} \to \mathrm{Conf}_{G,p}$ by

$$\sigma_{G,p}(f)(v) = \sum_{u \sim v} f(v),$$

where we write $u \sim v$ if there exists an edge joining u and v. Given a pair of configurations (f_s, f_t) (source configuration and target configuration, respectively), the goal of *the σ-game on G with p colors* is to find a configuration f, which we call a *solution* to (f_s, f_t), such that

$$f_s + \sigma_{G,p}(f) = f_t.$$

If f is a solution, then $f + \ker(\sigma_{G,p})$ is the set of all solutions. Define

$$d(G; p) = \dim_{\mathbb{F}_p} \ker(\sigma_{G,p}).$$

A configuration f_s is said to be *solvable* if $(f_s, 0)$ has a solution. Since the set of solvable configurations coincides with the image of $\sigma_{G,p}$, the ratio of solvable configurations to all configurations is $1/p^{d(G;p)}$. Thus $d(G; p)$ measures non-solvability of this game.

Likewise, we define

$$\sigma^+_{G,p}(f)(v) = f(v) + \sum_{u \sim v} f(v),$$

$$d^+(G; p) = \dim_{\mathbb{F}_p} \ker(\sigma^+_{G,p}).$$

The maps $\sigma_{G,p}$ and $\sigma^+_{G,p}$ are analogues of the Laplacian.

Fix an order in $V(G)$, and let $\mathrm{Adj}(G)$ be the adjacency matrix of G. Under an obvious identification $\mathrm{Conf}_{G,p} \cong \mathbb{F}_p^{\#V(G)}$, we have

$$\sigma_{G,p}(f) = \mathrm{Adj}(G)f, \quad \sigma^+_{G,p}(f) = (\mathrm{Adj}(G) + I)f,$$

and hence

$$d(G; p) = \mathrm{corank}_{\mathbb{F}_p} \mathrm{Adj}(G), \quad d^+(G; p) = \mathrm{corank}_{\mathbb{F}_p}(\mathrm{Adj}(G) + I).$$

Example 3. (i) Orbix is the σ-game on an icosahedron with two colors. All configurations are solvable; $d(G;2) = 0$.

(ii) The Lights Out puzzle is the σ^+-game on the Cartesian product $P_5 \times P_5$ with two colors. Exactly $1/4$ of the configurations are solvable; $d^+(P_5 \times P_5; 2) = 2$.

(iii) More generally, the σ-game and the σ^+-game on $P_m \times P_n$, $P_m \times C_n$, $C_m \times C_n$ etc. have been extensively investigated. See, for example, [1], [3], [4], [6], [9], [10], [11], [12], [13], [14]. For these graphs, the σ^+-game is mathematically much deeper than the σ-game.

See [7, 6.3] for detailed descriptions of (i) and (ii), as well as more examples which have been patented and marketed.

2.2 Trisentis game

The strong product $G \boxtimes H$ of graphs G, H is defined by:

$$V(G \boxtimes H) = V(G) \times V(H),$$

$$(v,w) \sim (v',w') \iff \begin{cases} v \sim v', w \sim w' & \text{or} \\ v = v', w \sim w' & \text{or} \\ v \sim v', w = w'. \end{cases}$$

Here is an example.

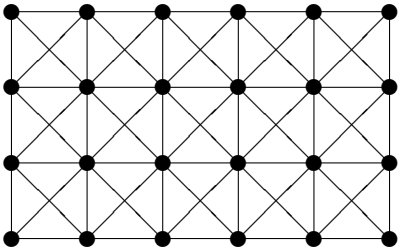

Figure 1: $P_6 \boxtimes P_4$

We can then rephrase that the $m \times n$ Trisentis game is the σ-game on $P_m \boxtimes P_n$ with two colors for the particular pair of configurations

$$f_s = {}^t(0\ 0\ \ldots\ 0), \quad f_t = {}^t(1\ 1\ \ldots\ 1).$$

n		2	3	4	5	6	7	8	9	10
d_n		0	3	4	1	0	7	0	9	0
n	11	12	13	14	15	16	17	18	19	20
d_n	3	0	1	12	15	16	1	0	19	0
n	21	22	23	24	25	26	27	28	29	30
d_n	1	0	7	4	1	0	3	0	25	0
n	31	32	33	34	35	36	37	38	39	40
d_n	31	0	33	4	3	0	1	0	39	0
n	41	42	43	44	45	46	47	48	49	50
d_n	1	0	3	12	1	0	15	0	9	16

Table 1: $d_n = d(P_n \boxtimes P_n; 2)$

We are concerned about the dimension $d(P_m \boxtimes P_n; p)$, especially its arithmetic behavior when we vary m, n, and p. Here is a table of $d_n = d(P_n \boxtimes P_n; 2)$ for $2 \le n \le 50$.

We also consider the following variants.

(i) The σ-game on $C_m \boxtimes C_n$.

(ii) The σ^+-game on $P_m \boxtimes P_n$ and $C_m \boxtimes C_n$.

We might also consider the σ-game and σ^+-game on $P_{n_1} \boxtimes P_{n_2} \boxtimes \cdots \boxtimes P_{n_r}$ and $C_{n_1} \boxtimes C_{n_2} \boxtimes \cdots \boxtimes C_{n_r}$. Some of the following results can be generalized to these cases, but we omit a description.

2.3 Statements of the results

Theorem 4. *Let* $q = 2^f$.

(i)

$$d(P_{q-2} \boxtimes P_{q-2}; 2) = \begin{cases} 0 & \text{if is odd}, f \ge 3, \\ q-4 & \text{if is even}, f \ge 2. \end{cases}$$

(ii)

$$d(P_q \boxtimes P_q; 2) = \begin{cases} 0 & \text{if is odd}, f \ge 1, \\ q & \text{if is even}, f \ge 2. \end{cases}$$

(iii)

$$d(C_{q-1} \boxtimes C_{q-1}; 2) = \begin{cases} 1 & \text{if is odd}, f \ge 3, \\ 2q-7 & \text{if is even}, f \ge 2. \end{cases}$$

(iv)

$$d(C_{q+1} \boxtimes C_{q+1}; 2) = \begin{cases} 1 & \text{if is odd}, f \geq 1, \\ 2q+1 & \text{if is even}, f \geq 2. \end{cases}$$

Since $d(G; p) = 0$ if and only if all configurations are solvable in the σ-game on G with p colors, Theorem 4 implies Conjecture 2(ii), and hence gives an alternative proof of Theorem 1(ii).

Combining Theorem 4 with Lemma 14 and Lemma 15 below, we obtain the following.

Corollary 5. *If* $\mathrm{lcm}(m, n)$ *divides* $2^f \pm 1$ *where* f *is odd, then we have*

$$d(P_{m-1} \boxtimes P_{n-1}; 2) = 0, \quad d(C_m \boxtimes C_n; 2) = 1.$$

For example, this corollary applies to $n = 2, 6, 8, 10, 18, 22, 26, 30, 32, 42, 46, 48$ in Table 1.

Theorem 6. *Let* $q = p^f$.

(i) If $p = 3$*, then for* $f \geq 2$*,*

$$d(P_{(q-3)/2} \boxtimes P_{(q-3)/2}; 3) = \frac{1}{4}\left(q - (-1)^f - 4\right).$$

(ii) If $p \geq 5, q \geq 7$*, then*

$$d(P_{(q-3)/2} \boxtimes P_{(q-3)/2}; p) = \frac{1}{4}\left(q - \left(\frac{-1}{q}\right) - 2\left(\frac{-2}{q}\right) - 4\left(\frac{-3}{q}\right) - 6\right).$$

(iii) If $p \geq 3, q \geq 5$*, then*

$$d(C_{q-1} \boxtimes C_{q-1}; p) = q - \left(\frac{-1}{q}\right) - 4\left(\frac{-3}{q}\right) - 3.$$

For the σ^+-game on $P_m \boxtimes P_n$ and $C_m \boxtimes C_n$, we have a general result. A remarkable fact is that the result is almost independent of the prime p. Another observation is that the σ^+-game is mathematically easier than the σ-game in the case of strong products $P_m \boxtimes P_n, C_m \boxtimes C_n$. This presents a striking contrast to the case of Cartesian products $P_m \times P_n, C_m \times C_n$, for which the σ^+-game is deeper than the σ-game.

Theorem 7. *(i)*

$$d^+(P_m \boxtimes P_n; p) = \begin{cases} m+n-1 & \text{if } m+1 \equiv n+1 \equiv 0 \pmod 3, \\ n & \text{if } m+1 \equiv 0 \pmod 3, n+1 \not\equiv 0 \pmod 3, \\ m & \text{if } m+1 \not\equiv 0 \pmod 3, n+1 \equiv 0 \pmod 3, \\ 0 & \text{if } (m+1)(n+1) \not\equiv 0 \pmod 3. \end{cases}$$

(ii)

$$d^+(C_m \boxtimes C_n; 3) = \begin{cases} 2m+2n-4 & \text{if } m \equiv n \equiv 0 \pmod 3, \\ m+2n-2 & \text{if } m \equiv 0 \pmod 3, n \not\equiv 0 \pmod 3, \\ 2m+n-2 & \text{if } m \not\equiv 0 \pmod 3, n \equiv 0 \pmod 3, \\ m+n-1 & \text{if } mn \not\equiv 0 \pmod 3. \end{cases}$$

If $p \neq 3$, then

$$d^+(C_m \boxtimes C_n; p) = \begin{cases} 2m+2n-4 & \text{if } m \equiv n \equiv 0 \pmod 3, \\ 2n & \text{if } m \equiv 0 \pmod 3, n \not\equiv 0 \pmod 3, \\ 2m & \text{if } m \not\equiv 0 \pmod 3, n \equiv 0 \pmod 3, \\ 0 & \text{if } mn \not\equiv 0 \pmod 3. \end{cases}$$

3 Proofs

3.1 Kronecker products

For two graphs G, H, we have

$$\mathrm{Adj}(G \boxtimes H) = (\mathrm{Adj}(G) + I) \otimes (\mathrm{Adj}(H) + I) - I,$$

where the Kronecker product of matrices

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix}$$

and Y is defined by

$$X \otimes Y = \begin{pmatrix} x_{11}Y & \cdots & x_{1n}Y \\ \vdots & \ddots & \vdots \\ x_{m1}Y & \cdots & x_{mn}Y \end{pmatrix}.$$

Here are some properties of Kronecker products. We omit the proof.

Lemma 8. *(i)* $(A \otimes B)(X \otimes Y) = (AX) \otimes (BY)$ *if the right hand side makes sense (i.e., the products* AX *and* BY *are defined).*

(ii) Let A *and* B *be square matrices of size* m *and* n *respectively. Let* $\lambda_1, \lambda_2, \ldots, \lambda_m$ *be the eigenvalues of* A *and* $\mu_1, \mu_2, \ldots, \mu_n$ *those of* B*, counting multiplicities. Then the eigenvalues of* $A \otimes B$ *are*

$$\lambda_i \mu_j \quad i = 1, 2, \ldots, m,\ j = 1, 2, \ldots, n.$$

(iii) $\operatorname{rank}(A \otimes B) = (\operatorname{rank} A)(\operatorname{rank} B)$.

3.2 Chebyshev polynomials

The normalized Chebyshev polynomials of the first, respectively, second kind are defined by

$$C_0(x) = 2,\ C_1(x) = x,\ C_n(x) = xC_{n-1}(x) - C_{n-2}(x)\ (n \geq 2),$$

$$S_0(x) = 1,\ S_1(x) = x,\ S_n(x) = xS_{n-1}(x) - S_{n-2}(x)\ (n \geq 2).$$

We follow the notation in [8], which is slightly different from that in [12]. We believe that there is no fear of confusion between the cycle graph C_n and the Chebyshev polynomial $C_n(x)$. Except for $C_0(x) = 2$, the polynomials $C_n(x)$ and $S_n(x)$ are monic of degree n with integer coefficients, and have the same parity as n in the sense that

$$C_n(-x) = (-1)^n C_n(x), \quad S_n(-x) = (-1)^n S_n(x).$$

These polynomials are characterized by the identities

$$C_n(2\cos\theta) = 2\cos n\theta, \quad S_n(2\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta} \tag{3}$$

for any θ.

Lemma 9. *(i) The characteristic polynomial of* $\operatorname{Adj}(P_n)$ $(n \geq 2)$ *is*

$$|xI - \operatorname{Adj}(P_n)| = \begin{vmatrix} x & -1 & & & \\ -1 & x & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & x & -1 \\ & & & -1 & x \end{vmatrix} = S_n(x),$$

and that of $\mathrm{Adj}(C_n)$ $(n \geq 3)$ *is*

$$|xI - \mathrm{Adj}(C_n)| = \begin{vmatrix} x & -1 & & & -1 \\ -1 & x & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & x & -1 \\ -1 & & & -1 & x \end{vmatrix} = C_n(x) - 2.$$

(ii) $C_n(1) = \begin{cases} (-1)^n 2 & \text{if } n \equiv 0 \pmod 3, \\ (-1)^{n-1} & \text{otherwise.} \end{cases}$

(iii) $S_n(1) = \begin{cases} (-1)^n & \text{if } n \equiv 0 \pmod 3, \\ (-1)^{n-1} & \text{if } n \equiv 1 \pmod 3, \\ 0 & \text{if } n \equiv 2 \pmod 3. \end{cases}$

3.3 Eigenstructure of adjacency matrices

In the following, ζ_n denotes a primitive nth root of unity in a field whose characteristic is either 0 or prime to n. Let K be an algebraically closed field.

Lemma 10. *(i) If the characteristic of* K *is either* 0 *or prime to* $2(n+1)$*, then the eigenvalues of* $\mathrm{Adj}(P_n)$ *over* K *are*

$$\zeta_{2(n+1)}^k + \zeta_{2(n+1)}^{-k},\ k = 1, 2, \ldots, n,$$

and $\mathrm{Adj}(P_n)$ *is diagonalizable by*

$$\left(\frac{\zeta_{2(n+1)}^{ij} - \zeta_{2(n+1)}^{-ij}}{\zeta_{2(n+1)}^{j} - \zeta_{2(n+1)}^{-j}} \right)_{1 \leq i,j \leq n}.$$

(ii) If the characteristic of K *is* 0 *or is prime to* n*, then the eigenvalues of* $\mathrm{Adj}(C_n)$ *over* K *are*

$$\zeta_n^k + \zeta_n^{-k},\ k = 0, 1, 2, \ldots, n-1,$$

and $\mathrm{Adj}(C_n)$ *is diagonalizable by*

$$\left(\zeta_n^{(i-1)(j-1)}\right)_{1 \leq i,j \leq n}.$$

Proof. In both cases, the first part follows from Lemma 9(i) and the property (3) of Chebyshev polynomials. The verification of the second part is then straightforward. □

Noting that, in characteristic zero, $-\zeta_{2(n+1)}$ is a primitive $(n+1)$st root of unity if n is even, we obtain the following.

Lemma 11. *If K has characteristic 2 and n is even, then the eigenvalues of $\mathrm{Adj}(P_n)$ over K are*

$$\zeta_{n+1}^k + \zeta_{n+1}^{-k}, \quad k = 1, 2, \ldots, n/2,$$

each with multiplicity 2.

Lemma 12. *The eigenspace of $\mathrm{Adj}(P_n)$ for each eigenvalue has dimension 1.*

Proof. This follows from the fact that the minimal polynomial of $\mathrm{Adj}(P_n)$ coincides with the characteristic polynomial $S_n(x)$. This fact is proved in [11, Lemma 4.1] when K has characteristic 2, but the proof is valid for arbitrary K. For the convenience of the reader, we reproduce the proof. Put $A = \mathrm{Adj}(P_n)$. It suffices to show that $f(A) \neq O$ for any nonzero polynomial f of degree $d < n$. Consider the column vector

$$v = {}^t(1\ 0\ \ldots\ 0)$$

of degree n, and let

$$A^i v = {}^t(a_1^{(i)}\ a_2^{(i)}\ \ldots\ a_n^{(i)}).$$

If $0 \leq i < n$, then $a_{i+1}^{(i)} = 1$ and $a_j^{(i)} = 0$ for $j > i+1$. It follows that the $(d+1)$st entry of $f(A)v$ is equal to the leading coefficient of f, which is nonzero. Hence $f(A) \neq O$. □

Lemma 13. *If $p \neq 2$ and $(m+1)(n+1) \not\equiv 0 \pmod{p}$, then*

$$\begin{aligned} d(P_m \boxtimes P_n; p) \;=\; & \frac{1}{4}\#\{(x,y) \in \bar{\mathbb{F}}_p^\times \times \bar{\mathbb{F}}_p^\times \,;\, (x+x^{-1}+1)(y+y^{-1}+1) = 1, \\ & x^{2(m+1)} = y^{2(n+1)} = 1,\ x \neq \pm 1, y \neq \pm 1\}. \end{aligned}$$

Proof. By definition, $d(G;p)$ is the dimension over $\mathbb{F}_p$ of the eigenspace of $\mathrm{Adj}(G)$ for the eigenvalue zero. By extension of scalars, we may replace $\mathbb{F}_p$ by $\bar{\mathbb{F}}_p$. By Lemma 8 and Lemma 10(i),

$$\mathrm{Adj}(P_m \boxtimes P_n) = (\mathrm{Adj}(P_m) + I) \otimes (\mathrm{Adj}(P_n) + I) - I$$

is diagonalizable over $\bar{\mathbb{F}}_p$ and the eigenvalue are, multiplicities taken into account,

$$\left(\zeta_{2(m+1)}^k + \zeta_{2(m+1)}^{-k} + 1\right)\left(\zeta_{2(n+1)}^l + \zeta_{2(n+1)}^{-l} + 1\right) - 1, \quad 1 \leq k \leq m, 1 \leq l \leq n.$$

Considering the range of k and l, we obtain the result. □

Lemma 14. *If m and n are even, then we have*

$$d(P_m \boxtimes P_n; 2) = \frac{1}{2}\#\{(x,y) \in \bar{\mathbb{F}}_2^\times \times \bar{\mathbb{F}}_2^\times \,;\, (x+x^{-1}+1)(y+y^{-1}+1) = 1, \\ x^{m+1} = y^{n+1} = 1,\ x \neq 1, y \neq 1\}.$$

Proof. It suffices to count the dimension over $\bar{\mathbb{F}}_2$ of the eigenspace of

$$\mathrm{Adj}(P_m \boxtimes P_n) + I = (\mathrm{Adj}(P_m) + I) \otimes (\mathrm{Adj}(P_n) + I)$$

for the eigenvalue 1. By Lemma 11 and Lemma 12, $\mathrm{Adj}(P_n) + I$ is similar to the Jordan canonical form

$$\mathrm{Adj}(P_n) + I \sim \begin{pmatrix} J_2(\alpha_{n+1}^{(1)}) & & & \\ & J_2(\alpha_{n+1}^{(2)}) & & \\ & & \ddots & \\ & & & J_2(\alpha_{n+1}^{(n/2)}) \end{pmatrix}$$

over $\bar{\mathbb{F}}_2$, where we put $\alpha_{n+1}^{(k)} = \zeta_{n+1}^k + \zeta_{n+1}^{-k} + 1$ and

$$J_2(\alpha) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

denotes a Jordan cell of degree 2. We have then

$$\mathrm{Adj}(P_m \boxtimes P_n) + I \sim \begin{pmatrix} \ddots & & \\ & J_2(\alpha_{m+1}^{(k)}) \otimes J_2(\alpha_{n+1}^{(l)}) & \\ & & \ddots \end{pmatrix}_{1 \le k \le m/2, 1 \le l \le n/2}.$$

We note that if $\alpha, \beta \in \bar{\mathbb{F}}_2, \alpha \neq 0$, then

$$P^{-1}(J_2(\alpha) \otimes J_2(\beta))P = \begin{pmatrix} J_2(\alpha\beta) & \\ & J_2(\alpha\beta) \end{pmatrix}$$

holds for

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha^{-1} & \beta & \alpha^{-1} \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

It follows that $d(P_m \boxtimes P_n; 2)$ is equal to two times the number of pairs (k,l) such that $\alpha_{m+1}^{(k)} \alpha_{n+1}^{(l)} = 1$, i.e.,

$$\left(\zeta_{m+1}^k + \zeta_{m+1}^{-k} + 1\right)\left(\zeta_{n+1}^l + \zeta_{n+1}^{-l} + 1\right) = 1$$

and $1 \le k \le m/2, 1 \le l \le n/2$. Considering the range of k and l, we obtain the result. □

Lemma 15. *If* $mn \not\equiv 0 \pmod{p}$*, then*

$$d(C_m \boxtimes C_n; p) = \#\{(x,y) \in \bar{\mathbb{F}}_p^\times \times \bar{\mathbb{F}}_p^\times \,;\, (x+x^{-1}+1)(y+y^{-1}+1) = 1,\ x^m = y^n = 1\}.$$

Proof. By Lemma 8 and Lemma 10(ii), $\mathrm{Adj}(C_m \boxtimes C_n)$ is diagonalizable over $\bar{\mathbb{F}}_p$ and the eigenvalues are

$$\left(\zeta_m^k + \zeta_m^{-k} + 1\right)\left(\zeta_n^l + \zeta_n^{-l} + 1\right) - 1, \quad 0 \le k \le m-1, 0 \le l \le n-1.$$

□

Corollary 16. *(i) If* m, n *are even, then*

$$d(C_{m+1} \boxtimes C_{n+1}; 2) = 2d(P_m \boxtimes P_n; 2) + 1.$$

(ii) If $2(m+1)(n+1) \not\equiv 0 \pmod{p}$*, then*

$$d(C_{2(m+1)} \boxtimes C_{2(n+1)}; p) = 4d(P_m \boxtimes P_n; p) + a_p(2(m+1)) + a_p(2(n+1)) + 1,$$

where

$$a_p(N) = \#\{x \in \bar{\mathbb{F}}_p^\times \,;\, 3(x + x^{-1} + 1) = 1, x^N = 1\}.$$

Proof. We give a proof of (ii). That of (i) is easier. Consider the set

$$\begin{aligned} S \;=\; & \{(x,y) \in \bar{\mathbb{F}}_p^\times \times \bar{\mathbb{F}}_p^\times \,;\, (x + x^{-1} + 1)(y + y^{-1} + 1) = 1, \\ & x^{2(m+1)} = y^{2(n+1)} = 1\}, \end{aligned}$$

whose cardinality is $d(C_{2(m+1)} \boxtimes C_{2(n+1)}; p)$ by Lemma 15. By Lemma 13, we have

$$d(P_m \boxtimes P_n; p) = \frac{1}{4} \# \left(S \cap \left((\bar{\mathbb{F}}_p^\times \setminus \{\pm 1\}) \times (\bar{\mathbb{F}}_p^\times \setminus \{\pm 1\}) \right) \right),$$

so that

$$\begin{aligned} d(C_{2(m+1)} \boxtimes C_{2(n+1)}; p) \;=\; & 4d(P_m \boxtimes P_n; p) \\ & + \# \left(S \cap (\{\pm 1\} \times \bar{\mathbb{F}}_p^\times) \right) + \# \left(S \cap (\bar{\mathbb{F}}_p^\times \times \{\pm 1\}) \right) \\ & - \# \left(S \cap (\{\pm 1\} \times \{\pm 1\}) \right). \end{aligned}$$

Since

$$\begin{aligned} \# \left(S \cap (\{1\} \times \bar{\mathbb{F}}_p^\times) \right) &= a_p(2(n+1)), \\ \# \left(S \cap (\bar{\mathbb{F}}_p^\times \times \{1\}) \right) &= a_p(2(m+1)), \end{aligned}$$

and

$$S \cap (\{-1\} \times \bar{\mathbb{F}}_p^\times) = S \cap (\bar{\mathbb{F}}_p^\times \times \{-1\}) = S \cap (\{\pm 1\} \times \{\pm 1\}) = \{(-1,-1)\},$$

we complete the proof. □

Remark 17. Clearly, $a_3(N) = 0$. For $p \geq 5$, let b_p be the order of $(-1 \pm 2\sqrt{-2})/3$ in $\bar{\mathbb{F}}_p^\times$, which is well-defined since

$$\frac{-1+2\sqrt{-2}}{3} \cdot \frac{-1-2\sqrt{-2}}{3} = 1.$$

Then we have

$$a_p(N) = \begin{cases} 2 & \text{if } b_p | N, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, for $q = p^f, p \geq 5$, we have

$$a_p(q-1) = \left(\frac{-2}{q}\right) + 1.$$

3.4 A quartic curve

It has thus turned out that counting the solutions of the equation

$$(x + x^{-1} + 1)(y + y^{-1} + 1) = 1$$

in a finite field is of significant importance. Let us consider the projective curve

$$\mathcal{C} : (x^2 + xz + z^2)(y^2 + yz + z^2) = xyz^2.$$

Whatever the base field is, $\mathcal{C}$ has exactly two points $(0 : 1 : 0), (1 : 0 : 0)$ at infinity, both of which are singular, and has a unique singular point $(-1 : -1 : 1)$ in the affine part $z \neq 0$. Let $\mathcal{C}(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points of $\mathcal{C}$. In this subsection, we give a formula for $\#\mathcal{C}(\mathbb{F}_q)$.

First we treat the case of characteristic two. The curve $\mathcal{C}$ is reducible over $\bar{\mathbb{F}}_2$ as

$$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2,$$

where

$$\mathcal{C}_i : xy + \zeta_3^i(x+y)z + z^2 = 0, \quad i = 1, 2,$$

are non-singular conics intersecting at the three singular points of $\mathcal{C}$.

Lemma 18. *Consider the curve $\mathcal{C}$ over $\bar{\mathbb{F}}_2$.*

(i) The points $(x : y : 1) \in \mathcal{C}$ with $xy = 0$ are $(\zeta_3^2 : 0 : 1), (0 : \zeta_3^2 : 1) \in \mathcal{C}_1$ and $(\zeta_3 : 0 : 1), (0 : \zeta_3 : 1) \in \mathcal{C}_2$.

(ii) Let Frob_q be the qth power Frobenius map, where $q = 2^f$. We have $\mathrm{Frob}_q(\mathcal{C}_i) \subset \mathcal{C}_i$ if f is even, $\mathrm{Frob}_q(\mathcal{C}_i) \subset \mathcal{C}_{3-i}$ if f is odd.

(iii) If $(x : y : 1) \in \mathcal{C}_i$ *with* $xy \neq 0$*, then* $(x^{-1} : y^{-1} : 1) \in \mathcal{C}_i$*.*

Proof. Straightforward. □

Proposition 19. *For* $q = 2^f$*, we have*

$$\#\mathcal{C}(\mathbb{F}_q) = \begin{cases} 3 & \text{if } f \text{ is odd}, \\ 2q-1 & \text{if } f \text{ is even}. \end{cases}$$

Proof. Suppose f is odd, and let $\mathcal{G} = \mathrm{Gal}(\bar{\mathbb{F}}_2/\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle$ be the Galois group. We have

$$\mathcal{C}(\mathbb{F}_q) = \mathcal{C}(\bar{\mathbb{F}}_2)^{\mathcal{G}} = \mathcal{C}_1 \cap \mathcal{C}_2$$

by Lemma 18(ii), so that $\#\mathcal{C}(\mathbb{F}_q) = 3$.

If f is even, then $\mathcal{C}_1, \mathcal{C}_2$ are defined over $\mathbb{F}_q$, so that we have

$$\#\mathcal{C}(\mathbb{F}_q) = \#\mathcal{C}_1(\mathbb{F}_q) + \#\mathcal{C}_2(\mathbb{F}_q) - \#(\mathcal{C}_1 \cap \mathcal{C}_2) = 2(q+1) - 3 = 2q - 1.$$

□

Proposition 20. *For* $q = p^f, p \geq 3$*, we have*

$$\#\mathcal{C}(\mathbb{F}_q) = q - \left(\frac{-1}{q}\right) - 2\left(\frac{-3}{q}\right) + 1.$$

Proof. Consider two rational maps

$$\mathcal{C} \to Q, \quad (x : y : z) \mapsto ((x+y)z : xy : z^2),$$
$$Q \to \mathbb{P}^1, \quad (X : Y : Z) \mapsto (Y - Z : X + 2Z),$$

where

$$Q : X^2 + XY + Y^2 + XZ - 2YZ + Z^2 = 0$$

is a non-singular conic, and $\mathbb{P}^1$ is the projective line. By composition, we obtain a rational map

$$\pi : \mathcal{C} \to \mathbb{P}^1, \quad (x : y : z) \mapsto (xy - z^2 : (x + y + 2z)z),$$

which is defined outside the set of singular points of $\mathcal{C}$. If follows from

$$\mathcal{C}(\mathbb{F}_q) = \{\text{singular points}\} \cup \bigcup_{\mathrm{P} \in \mathbb{P}^1(\mathbb{F}_q)} \pi^{-1}(\mathrm{P}) \cap \mathcal{C}(\mathbb{F}_q),$$

that

$$\#\mathcal{C}(\mathbb{F}_q) = \nu_0 + \sum_{\mathrm{P} \in \mathbb{P}^1(\mathbb{F}_q)} \nu(\mathrm{P}),$$

where we put

$$\nu_0 = 3, \quad \nu(\mathrm{P}) = \#\left(\pi^{-1}(\mathrm{P}) \cap \mathcal{C}(\mathbb{F}_q)\right).$$

In most cases, $\pi^{-1}(\mathrm{P})$ consists of two points $\{(x, y), (y, x)\}$. We have six cases to examine.

(i) $\nu_1 = \nu((1:0)) = \left(\dfrac{-2}{q}\right) + 1$, as

$$\pi^{-1}((1:0)) = \{\pm(-1+\sqrt{-2}, -1-\sqrt{-2})\}.$$

(ii) It is readily verified that $\nu((-1:1)) = 0$.

Now we suppose that $\mathrm{P} = (t:1), t \neq -1$. If $(x:y:1) \in \pi^{-1}(\mathrm{P})$, then a little computation shows

$$(t^2+t+1)x^2 + 2t^2x + 3t^2 + 3t + 1 = 0. \tag{4}$$

(iii) If $t^2+t+1 = 0$, then (4) reduces to $x = t$. If follows from $\pi((x:y:1)) = (t:1)$ that $t = -1$, which is impossible. We have thus $\nu((t:1)) = 0$ in this case. The number of such t is

$$\nu_3 = \left(\frac{-3}{q}\right) + 1.$$

If $t^2+t+1 \neq 0$, then (4) yields

$$x = \frac{-t^2 \pm (t+1)\sqrt{D}}{t^2+t+1},$$

where

$$D = -(2t^2+2t+1).$$

(iv) If $\sqrt{D} \notin \mathbb{F}_q$, then $\nu(\mathrm{P}) = 0$. We shall show below that the number of such $t \in \mathbb{F}_q, t \neq -1$ is

$$\nu_4 = \frac{1}{2}\left(q + \left(\frac{-2}{q}\right) - 2\right).$$

There is no overlap between cases (iii) and (iv), for if $t^2+t+1 = 0$, then $\sqrt{D} = 1 \in \mathbb{F}_q$.

(v) $\nu((t:1)) = 1$ if and only if $D = 0$ if and only if $t = \dfrac{-1 \pm \sqrt{-1}}{2}$. The number of such t is

$$\nu_5 = \left(\frac{-1}{q}\right) + 1.$$

(vi) In the remaining cases, we have $\nu((t:1)) = 2$. The number of such t is

$$\nu_6 = (q-1) - \nu_3 - \nu_4 - \nu_5.$$

Putting all together, we have

$$\#\mathcal{C}(\mathbb{F}_q) = \nu_0 + \nu_1 + \nu_5 + 2\nu_6 = q - \left(\frac{-1}{q}\right) - 2\left(\frac{-3}{q}\right) + 1.$$

It remains to prove the formula for ν_4. Since $t = -1$ satisfies $\sqrt{D} \in \mathbb{F}_q$ if and only if $\left(\frac{-1}{q}\right) = 1$, it suffices to show that the number of $t \in \mathbb{F}_q$ (including $t = -1$) such that $\sqrt{D} \in \mathbb{F}_q$ is

$$\frac{1}{2}\left(q + \left(\frac{-1}{q}\right) - \left(\frac{-2}{q}\right) + 1\right).$$

D is a square in $\mathbb{F}_q$ if and only if

$$(2t+1)^2 + 2u^2 + 1 = 0$$

holds for some $u \in \mathbb{F}_q$. There is a one-to-one correspondence between such t and $X \in \mathbb{F}_q$ such that $(X : Y : 1) \in \mathcal{C}_0(\mathbb{F}_q)$, where

$$\mathcal{C}_0 : X^2 + 2Y^2 + Z^2 = 0.$$

By looking at the Hilbert symbol $(-1, -2)_p = 1$, we see that $\mathcal{C}_0(\mathbb{F}_p)$ is non-empty, and hence $\#\mathcal{C}_0(\mathbb{F}_q) = q + 1$. The correspondence between X and $(X : Y : 1)$ is one-to-one if $Y = 0$, one-to-two otherwise. The number of affine $\mathbb{F}_q$-rational points with $Y = 0$ is

$$\mu_0 = \left(\frac{-1}{q}\right) + 1,$$

and that of $\mathbb{F}_q$-rational points at infinity is

$$\mu_\infty = \left(\frac{-2}{q}\right) + 1,$$

so that the number in question is

$$\mu_0 + \frac{1}{2}(q + 1 - \mu_0 - \mu_\infty) = \frac{1}{2}\left(q + \left(\frac{-1}{q}\right) - \left(\frac{-2}{q}\right) + 1\right).$$

□

The congruence zeta function of $\mathcal{C}$ over $\mathbb{F}_q$ is defined by

$$Z(\mathcal{C}/\mathbb{F}_q, t) = \exp \sum_{n=1}^{\infty} \frac{\#\mathcal{C}(\mathbb{F}_{q^n})}{n} t^n.$$

Corollary 21. *For $q = 2^f$, we have*

$$Z(\mathcal{C}/\mathbb{F}_q, t) = \begin{cases} \dfrac{(1+t)^2}{(1-t)(1-(qt)^2)} & \text{if } f \text{ is odd}, \\ \dfrac{1-t}{(1-qt)^2} & \text{if } f \text{ is even}. \end{cases}$$

For $q = p^f, p \geq 3$, we have

$$Z(\mathcal{C}/\mathbb{F}_q, t) = \frac{\left(1 - \left(\dfrac{-1}{q}\right)t\right)\left(1 - \left(\dfrac{-3}{q}\right)t\right)^2}{(1-t)(1-qt)}.$$

3.5 Proof of Theorem 6

Put $q = p^f, p \geq 3$. By Lemma 15, $d(C_{q-1} \boxtimes C_{q-1}; p)$ is equal to the number of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}$ except for the following two types of points.

(i) Points at infinity; there are two such points.

(ii) Points $(x : y : 1)$ with $xy = 0$; $(1 : 0 : 1), (0 : 1 : 1)$ if $p = 3$, $(\zeta_3^{\pm 1} : 0 : 1), (0 : \zeta_3^{\pm 1} : 1)$ if $\sqrt{-3} \in \mathbb{F}_q$. The number of such points is $2 + 2\left(\dfrac{-3}{q}\right)$.

By Proposition 20 we obtain Theorem 6(iii). By Corollary 16 and Remark 17, the assertions (i) and (ii) then follow from (iii). □

3.6 Proof of Theorem 4

Put $q = 2^f$. The proof of (iii) is similar to that of Theorem 6(iii); $d(C_{q-1} \boxtimes C_{q-1}; 2)$ is equal to the cardinality of $\mathcal{C}(\mathbb{F}_q)$ minus the number of points at infinity minus the number of points $(x : y : 1)$ with $xy = 0$. By Corollary 16, the assertions (i) and (ii) follow from (iii) and (iv), respectively.

It remains to prove (iv). By Lemma 15, we need to count the number of $(x : y : 1) \in \mathcal{C}(\bar{\mathbb{F}}_2)$ such that $x^{q+1} = y^{q+1} = 1$, i.e.,

$$(x : y : 1)^{\mathrm{Frob}_q} = (x^{-1} : y^{-1} : 1). \tag{5}$$

Recall that $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ over $\bar{\mathbb{F}}_2$. If f is odd, then there is no point satisfying (5) other than $(1 : 1 : 1)$ by Lemma 18, so that we have

$$d(C_{q+1} \boxtimes C_{q+1}; 2) = 1.$$

Suppose f is even and define a rational map $\varphi : \mathcal{C}_1 \to \mathcal{C}_1$ by

$$\varphi((x : y : z)) = (\zeta_3 y(x^2 + z^2) + xyz : \zeta_3 x(y^2 + z^2) + xyz : xyz),$$

which is defined outside $\{(1 : 0 : 0), (0 : 1 : 0)\}$. It is readily verified that

$$\varphi^{-1}((1 : 0 : 0)) = (0 : \zeta_3^2 : 1),$$

$$\varphi^{-1}((0 : 1 : 0)) = (\zeta_3^2 : 0 : 1),$$

$$\varphi^{-1}((1 : 1 : 1)) = (1 : 1 : 1).$$

Let $\mathrm{P} \in \mathcal{C}_1(\mathbb{F}_q)$ be a non-singular point. We have

$$\varphi^{-1}(\mathrm{P}) = \{(x : y : 1), (x^{-1}y^{-1} : 1)\}$$

for some $(x : y : 1) \in \mathcal{C}_1(\mathbb{F}_{q^2})$ with $xy \neq 0$. This is the reason that we defined the map φ. Since φ commutes with the action of the Galois group $\mathcal{G} = \mathrm{Gal}(\bar{\mathbb{F}}_2/\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle$ and P is invariant under $\mathcal{G}$, the set $\varphi^{-1}(\mathrm{P})$ is also invariant under $\mathcal{G}$. This means that either $(x : y : 1) \in \mathcal{C}_1(\mathbb{F}_q)$ or (5) holds. Conversely, any such point $(x : y : 1)$ appears in this way. Since $\#\mathcal{C}_1(\mathbb{F}_q) = q + 1$ and since the three singular points and $(0 : \zeta_3^2 : 1), (\zeta_3^2 : 0 : 1)$ are excluded, the number of points $(x : y : 1) \in \mathcal{C}_1(\bar{\mathbb{F}}_2) \setminus \{(1 : 1 : 1)\}$ satisfying (5) is

$$2(q + 1 - 3) - (q + 1 - 5) = q.$$

Likewise, the number of points $(x : y : 1) \in \mathcal{C}_2(\bar{\mathbb{F}}_2) \setminus \{(1 : 1 : 1)\}$ satisfying (5) is q. Together with $(1 : 1 : 1)$, the number of points $(x : y : 1) \in \mathcal{C}(\bar{\mathbb{F}}_2)$ satisfying (5) is $2q + 1$. This completes the proof. □

3.7 Proof of Theorem 7

By definition, $d^+(G; p)$ is the dimension over $\mathbb{F}_p$ of the eigenspace of $\mathrm{Adj}(G) + I$ for the eigenvalue zero. Let G, H be graphs with m, n vertices respectively. We have

$$\begin{aligned} d^+(G \boxtimes H; p) &= mn - \mathrm{rank}((\mathrm{Adj}(G) + I) \otimes (\mathrm{Adj}(H) + I)) \\ &= mn - \mathrm{rank}(\mathrm{Adj}(G) + I)\,\mathrm{rank}(\mathrm{Adj}(H) + I) \\ &= mn - (m - d^+(G; p))(n - d^+(H; p)). \end{aligned}$$

Theorem 7 then follows from the following Lemma. □

Lemma 22. *(i)* $d^+(P_n; p) = \begin{cases} 1 & \text{if } n + 1 \equiv 0 \pmod 3, \\ 0 & \text{if } n + 1 \not\equiv 0 \pmod 3. \end{cases}$

(ii) $d^+(C_n;p) = \begin{cases} 2 & \text{if } n \equiv 0 \pmod 3, \\ 1 & \text{if } p = 3, n \not\equiv 0 \pmod 3, \\ 0 & \text{if } p \neq 3, n \not\equiv 0 \pmod 3. \end{cases}$

Proof. (i) This is proved in [5, Corollary 5]. See also [14, Proposition 2.1]. We give an alternative proof using Chebyshev polynomials. By Lemma 9, we have $|\operatorname{Adj}(P_n) + I| = (-1)^n S_n(-1) = S_n(1)$. If $n+1 \not\equiv 0 \pmod 3$, then $S_n(1) \not\equiv 0 \pmod p$, so that $d^+(P_n;p) = 0$. Suppose $n+1 \equiv 0 \pmod 3$. We have $d^+(P_n;p) > 0$ since $S_n(1) = 0$. Any principal minor of degree $(n-1)$ of $\operatorname{Adj}(P_n) + I$ is

$$S_{n-1}(1) = (-1)^n \not\equiv 0 \pmod p.$$

Thus we have $\operatorname{rank}_{\mathbb{F}_p}(\operatorname{Adj}(P_n) + I) = n-1$, so that $d^+(P_n;p) = 1$. Explicitly,

$${}^t\begin{pmatrix} -1 & 1 & 0 & -1 & 1 & 0 & \dots & -1 & 1 & \end{pmatrix}$$

is a basis for the kernel.

(ii) We have similarly

$$|\operatorname{Adj}(C_n) + I| = C_n(1) - (-1)^n 2 = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 3, \\ (-1)^{n-1}3 & \text{otherwise,} \end{cases}$$

so that $d^+(C_n;p) = 0$ if $p \neq 3, n \not\equiv 0 \pmod 3$. If $p = 3, n \not\equiv 0 \pmod 3$, then $d^+(C_n;p) > 0$, and any principal minor of degree $(n-1)$ of $\operatorname{Adj}(C_n) + I$ is $S_{n-1}(1) \not\equiv 0 \pmod 3$. Thus we have $d^+(C_n;3) = 1$. Explicitly,

$${}^t\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

is a basis for the kernel. Finally, if $n \equiv 0 \pmod 3$, then any principal minor of degree $(n-2)$ of $\operatorname{Adj}(C_n) + I$ is $S_{n-2}(1) \not\equiv 0 \pmod 3$, so that $d^+(C_n;p) \leq 2$. Since $\operatorname{Adj}(C_n) + I$ has linearly independent eigenvectors

$${}^t\begin{pmatrix} -1 & 1 & 0 & -1 & 1 & 0 & \dots & -1 & 1 & 0 \end{pmatrix},$$

$${}^t\begin{pmatrix} -1 & 0 & 1 & -1 & 0 & 1 & \dots & -1 & 0 & 1 \end{pmatrix}$$

for the eigenvalue 0, we have $d^+(C_n;p) = 2$.

□

References

[1] Rana Barua, S. Ramakrishnan, σ-game, σ^+-game and two-dimensional additive cellular automata, Theoret. Comput. Sci. 154 (1996), no. 2, 349–366.

[2] Achim Clausing, Das Trisentis-Spiel, Math. Semesterber. 48 (2001), no. 1, 49–66.

[3] Masato Goshima and Masakazu Yamagishi, Two remarks on torus lights out puzzle, Adv. Appl. Discrete Math. 4 (2009), no. 2, 115–126.

[4] Masato Goshima and Masakazu Yamagishi, On the dimension of the space of harmonic functions on a discrete torus, to appear in Experiment. Math.

[5] Sylvain Gravier, Mehdi Mhalla, Eric Tannier, On a modular domination game, Theoret. Comput. Sci. 306 (2003), no. 1-3, 291–303.

[6] Markus Hunziker, António Machiavelo, Jihun Park, Chebyshev polynomials over finite fields and reversibility of σ-automata on square grids, Theoret. Comput. Sci. 320 (2004), no. 2-3, 465–483.

[7] David Joyner, Adventures in group theory. Rubik's cube, Merlin's machine and other mathematical toys, Johns Hopkins University Press, Baltimore, MD, 2002.

[8] Theodore J. Rivlin, Chebyshev polynomials. From approximation theory to algebra and number theory. Second edition. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1990.

[9] Palash Sarkar, Rana Barua, Multidimensional σ-automata, π-polynomials and generalised S-matrices, Theoret. Comput. Sci. 197 (1998), no. 1-2, 111–138.

[10] Klaus Sutner, The σ-game and cellular automata, Amer. Math. Monthly 97 (1990), no. 1, 24–34.

[11] Klaus Sutner, σ-automata and Chebyshev-polynomials, Theoret. Comput. Sci. 230 (2000), no. 1-2, 49–73.

[12] Mikhail Zaidenberg, Periodic binary harmonic functions on lattices, Adv. in Appl. Math. 40 (2008), no. 2, 225–265.

[13] Mikhail Zaidenberg, Convolution equations on lattices: periodic solutions with values in a prime characteristic field, Geometry and dynamics of groups and spaces, 721–742, Progr. Math., 265, Birkhäuser, Basel, 2008.

[14] Mikhail Zaidenberg, Periodic harmonic functions on lattices and points count in positive characteristic, Cent. Eur. J. Math. 7 (2009), no. 3, 365–381.