On the Dimension of the Space of Harmonic Functions on a Discrete Torus

Masato Goshima and Masakazu Yamagishi

CONTENTS

Let $d(n)$ denote the corank of $I + A$ over the field with two elements, where A is the adjacency matrix of the discrete torus $C_n \times C_n$, and I is the identity matrix. We shall prove that $d(2n) = 2d(n)$ and $d(2^r + 1) = d(2^r - 1) + 4$. For the proof of the latter result, we use an elliptic curve. Our motivation for this study is the "lights out" puzzle.

1. INTRODUCTION

Let Γ be a finite undirected graph, $V(\Gamma)$ the vertex set of Γ, and $\mathcal{F}(\Gamma)$ the set of maps from $V(\Gamma)$ to $\mathbb{F}_2$, the finite field with two elements. Then $\mathcal{F}(\Gamma)$ is a vector space of dimension $|V(\Gamma)|$ over $\mathbb{F}_2$. We call an element of $\mathcal{F}(\Gamma)$ a *configuration* of Γ, which we often identify with a column vector in $\mathbb{F}_2^{|V(\Gamma)|}$, fixing an order in $V(\Gamma)$.

Let $A(\Gamma)$ be the adjacency matrix of Γ, I the identity matrix of degree $|V(\Gamma)|$, and $\Delta(\Gamma)$ the linear transformation on $\mathcal{F}(\Gamma)$ defined by

$$(\Delta(\Gamma)f)(v) = f(v) + \sum_{u\sim v} f(u),$$

where $u \sim v$ means that vertices u, v are adjacent. In case Γ has loops or multiple edges, we explicitly write the definition of $\Delta(\Gamma)$ as

$$(\Delta(\Gamma)f)(v) = f(v) + \sum_{u\in V(\Gamma)} A_{uv} f(u),$$

where A_{uv} is (mod 2 of) the (u, v)-component of $A(\Gamma)$. We may consider that

$$\Delta(\Gamma)f = (I + A(\Gamma))f$$

under the identification $\mathcal{F}(V) = \mathbb{F}_2^{|V(\Gamma)|}$.

Define $\mathcal{H}(\Gamma) = \ker \Delta(\Gamma)$ and

$$d(\Gamma) = \dim_{\mathbb{F}_2} \mathcal{H}(\Gamma) = \operatorname{corank}_{\mathbb{F}_2}(I + A(\Gamma)).$$

As is well known, $\Delta(\Gamma)$ is an analogue of the Laplacian (see, for example, [Cartier 72, Cartier 73]), and so $\mathcal{H}(\Gamma)$ is the space of "harmonic" functions on Γ.

2000 AMS Subject Classification: 11B39, 11T06, 11T99, 14H52, 31C05

Keywords: Lights out puzzle, graph Laplacian, discrete torus, elliptic curve, Chebyshev–Dickson polynomials

n	$d(n)$	n	$d(n)$	n	$d(n)$	n	$d(n)$	n	$d(n)$	n	$d(n)$
1	0	51	20	101	0	151	0	201	4	251	0
2	0	52	0	102	40	152	0	202	0	252	208
3	4	53	0	103	0	153	20	203	0	253	0
4	0	54	8	104	0	154	0	204	80	254	224
5	8	55	8	105	12	155	48	205	48	255	284
6	8	56	0	106	0	156	16	206	0	256	0
7	0	57	4	107	0	157	0	207	4	257	288
8	0	58	0	108	16	158	0	208	0	258	232
9	4	59	0	109	0	159	4	209	0	259	0
10	16	60	48	110	16	160	256	210	24	260	224
11	0	61	0	111	4	161	0	211	0	261	4
12	16	62	80	112	0	162	8	212	0	262	0
13	0	63	52	113	0	163	0	213	4	263	0
14	0	64	0	114	8	164	0	214	0	264	352
15	12	65	56	115	8	165	52	215	8	265	8
16	0	66	88	116	0	166	0	216	32	266	0
17	16	67	0	117	4	167	0	217	40	267	4
18	8	68	64	118	0	168	32	218	0	268	0
19	0	69	4	119	16	169	0	219	4	269	0
20	32	70	16	120	96	170	48	220	32	270	24
21	4	71	0	121	0	171	76	221	16	271	0
22	0	72	32	122	0	172	0	222	8	272	256
23	0	73	0	123	4	173	0	223	0	273	4
24	32	74	0	124	160	174	8	224	0	274	0
25	8	75	12	125	8	175	8	225	12	275	8
26	0	76	0	126	104	176	0	226	0	276	16
27	4	77	0	127	112	177	4	227	0	277	0
28	0	78	8	128	0	178	0	228	16	278	0
29	0	79	0	129	116	179	0	229	0	279	44
30	24	80	128	130	112	180	48	230	16	280	64
31	40	81	4	131	0	181	0	231	44	281	0
32	0	82	0	132	176	182	0	232	0	282	8
33	44	83	0	133	0	183	4	233	0	283	0
34	32	84	16	134	0	184	0	234	8	284	0
35	8	85	24	135	12	185	8	235	8	285	12
36	16	86	0	136	128	186	88	236	0	286	0
37	0	87	4	137	0	187	16	237	4	287	0
38	0	88	0	138	8	188	0	238	32	288	128
39	4	89	0	139	0	189	52	239	0	289	16
40	64	90	24	140	32	190	16	240	192	290	16
41	0	91	0	141	4	191	0	241	0	291	4
42	8	92	0	142	0	192	256	242	0	292	0
43	0	93	44	143	0	193	0	243	4	293	0
44	0	94	0	144	64	194	0	244	0	294	8
45	12	95	8	145	8	195	60	245	8	295	8
46	0	96	128	146	0	196	0	246	8	296	0
47	0	97	0	147	4	197	0	247	0	297	44
48	64	98	0	148	0	198	88	248	320	298	0
49	0	99	44	149	0	199	0	249	4	299	0
50	16	100	32	150	24	200	64	250	16	300	48

TABLE 1. Values of $d(n) = d(C_{n,n})$.

We make this situation into a puzzle as follows. (This is called the σ^+-game in [Sutner 89, Sutner 90].) Each vertex corresponds to a lighted button. A configuration $f \in \mathcal{F}(\Gamma)$ represents the on/off state of the buttons: a button corresponding to $v \in V(\Gamma)$ is thought to be "on" if $f(v) = 1$, "off" if $f(v) = 0$. Pushing a set of buttons corresponding to a subset $S \subset V(\Gamma)$ changes f to $f + \Delta(\Gamma)\chi_S$, where $\chi_S \in \mathcal{F}(\Gamma)$ is the characteristic function of S:

$$\chi_S(v) = \begin{cases} 1 & \text{if } v \in S, \\ 0 & \text{if } v \notin S. \end{cases}$$

By the definition of $\Delta(\Gamma)$, pushing a single button v reverses its state as well as that of the buttons that are adjacent to v. A subset $S \subset V(\Gamma)$ is said to be a *solution* to f if $f + \Delta(\Gamma)\chi_S = O$, where O is the zero configuration. A configuration is said to be *solvable* if it has a solution. Since a configuration is solvable if and only if it belongs to the image of $\Delta(\Gamma)$, we see that exactly $1/2^{d(\Gamma)}$ of the configurations of Γ are solvable. The purpose of this puzzle is to determine whether a given configuration is solvable and to find a solution if it is solvable.

Let P_n be the path with n vertices and $P_{m,n} = P_m \times P_n$ the Cartesian product. In the case $\Gamma = P_{m,n}$, we call this puzzle the $m \times n$ *lights out* puzzle. The case $P_{5,5}$ is the original lights out puzzle and $d(P_{5,5}) = 2$. See [Joyner 02, Chapter 6].

Similarly, in the case $\Gamma = C_{m,n} = C_m \times C_n$, where C_n denotes the cycle graph with n vertices, we call this puzzle the $m \times n$ *torus lights out* puzzle. The subject of this paper is the sequence $d(n) = d(C_{n,n})$. No general explicit formula for $d(n)$ is known, and the behavior of $d(n)$ seems mysterious; see Table 1.

The dimension $d(n)$ itself as well as the characterization of n such that $d(n) > 0$ has been investigated by several authors from various viewpoints: automata theory, graph theory, harmonic analysis, and so on. See, for example, [Barua and Ramakrishnan 96, Goldwasser et al. 02, Hunziker et al. 04, Zaidenberg 08a, Zaidenberg 08b, Zaidenberg 09].

Our results are the following.

Theorem 1.1. *We have $d(C_{2m,2n}) = 2d(C_{m,n})$ for $m \geq 1$, $n \geq 1$. In particular, we have $d(2n) = 2d(n)$.*[1]

Theorem 1.2. *We have $d(2^r+1) = d(2^r-1)+4$ for $r \geq 1$.*

Combining Theorem 1.2 with Corollary 3.6 below, we obtain the following.

Corollary 1.3. *The statement $d(n) > 0$ holds for positive integers of the form $n = 2^r \pm 1$, $n \neq 1, 7$.*

This gives an alternative proof of [Goldwasser et al. 02, Theorem 14], via a known relation between lights out and torus lights out (see Section 4).

The characterization of n with nonzero $d(n)$ is certainly an interesting problem, but the dimension $d(n)$ itself is a much more interesting subject, as our theorems show.

The content of this paper is as follows. We prove Theorem 1.1 in Section 2, by constructing an explicit isomorphism

$$\mathcal{H}(C_{m,n}) \oplus \mathcal{H}(C_{m,n}) \cong \mathcal{H}(C_{2m,2n}).$$

We prove Theorem 1.2 in Section 3, using the multiplication-by-2 map on the elliptic curve

$$(x + y + z)(xy + z^2) + z^3 = 0.$$

In Section 4 we present a conjecture, motivated by a known relation between lights out and torus lights out. Assuming this conjecture, we give alternative proofs of Theorems 1.1 and 1.2. In Section 5 we make three further observations on the sequence $d(n)$. Table 1 gives some values of $d(n)$.

2. DOUBLING

Let $\mathbb{Z}$ denote the ring of rational integers. We identify the vertex set $V(C_{m,n})$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, adjacency relations being

$$(i, j) \sim (i \pm 1, j), \quad (i, j) \sim (i, j \pm 1).$$

We also identify a configuration $f \in \mathcal{F}(C_{m,n})$ with an $m \times n$ matrix (a_{ij}) such that $a_{ij} = f((i, j))$. In the rest of this section, we always assume that

$$i \in \mathbb{Z}/m\mathbb{Z}, \ \ j \in \mathbb{Z}/n\mathbb{Z}, \ \ k \in \mathbb{Z}/2m\mathbb{Z}, \ \ l \in \mathbb{Z}/2n\mathbb{Z}.$$

Let us write $\mathcal{F}_{m,n} = \mathcal{F}(C_{m,n})$, $\Delta_{m,n} = \Delta(C_{m,n})$, and $\mathcal{H}_{m,n} = \mathcal{H}(C_{m,n})$. We introduce $\mathbb{F}_2$-linear maps

$$\iota^{\pm}_{m,n} : \mathcal{F}_{m,n} \to \mathcal{F}_{2m,2n},$$
$$\pi^{\pm}_{m,n} : \mathcal{F}_{2m,2n} \to \mathcal{F}_{m,n},$$

as follows:

$$\iota^{+}_{m,n} : (a_{ij}) \mapsto (b_{kl}),$$

where

$$b_{kl} = \begin{cases} a_{k/2,l/2}, & k \equiv l \equiv 0 \pmod 2, \\ 0, & \text{otherwise,} \end{cases}$$

[1] This is stated without proof in [Brouwer 08].

and

$$\iota^-_{m,n} : (a_{ij}) \mapsto (b_{kl}),$$

where

$$b_{kl} = \begin{cases} a_{(k-1)/2,(l-1)/2}, & k \equiv l \equiv 1 \pmod 2 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\begin{aligned} \pi^+_{m,n} &: (b_{kl}) \mapsto (a_{ij}), \quad a_{ij} = b_{2i,2j}, \\ \pi^-_{m,n} &: (b_{kl}) \mapsto (a_{ij}), \quad a_{ij} = b_{2i+1,2j+1}. \end{aligned}$$

Note that $2i \in \mathbb{Z}/2m\mathbb{Z}$ and so on are well defined.

We also define

$$\mathcal{D}^\pm_{m,n} = \Delta_{2m,2n} \circ \iota^\pm_{m,n}.$$

For example, $\mathcal{D}^+_{m,n}$ sends (a_{ij}) to

$$\begin{pmatrix} a_{00} & a_{00}+a_{01} & a_{01} & a_{01}+a_{02} & \cdots \\ a_{00}+a_{10} & 0 & a_{01}+a_{11} & 0 & \cdots \\ a_{10} & a_{10}+a_{11} & a_{11} & a_{11}+a_{12} & \cdots \\ a_{10}+a_{20} & 0 & a_{11}+a_{21} & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

This map is essentially the same as the "doubling" map in [Zaidenberg 08b, 2.35].

Lemma 2.1.

(i) $\iota^\pm_{m,n}$, $\mathcal{D}^\pm_{m,n}$ *are injective.*

(ii) $\mathrm{image}(\iota^+_{m,n}) \cap \mathrm{image}(\iota^-_{m,n}) = \{O\}$.

(iii) $\mathrm{image}(\mathcal{D}^+_{m,n}) \cap \mathrm{image}(\mathcal{D}^-_{m,n}) = \{O\}$.

(iv) $\Delta_{2m,2n} \circ \mathcal{D}^\pm_{m,n} = \iota^\pm_{m,n} \circ \Delta_{m,n}$.

(v) *The restriction of* $\mathcal{D}^+_{m,n} \circ \pi^+_{m,n} + \mathcal{D}^-_{m,n} \circ \pi^-_{m,n}$ *to* $\mathcal{H}_{2m,2n}$ *is the identity map.*

(vi) $\pi^\pm_{m,n}(\mathcal{H}_{2m,2n}) \subset \mathcal{H}_{m,n}$.

Proof: Statements (i) through (iii) are clear. For statement (iv), let $f = (a_{ij}) \in \mathcal{F}_{m,n}$, $(b_{kl}) = \Delta_{2m,2n}(\mathcal{D}^+_{m,n}(f))$ and $(c_{kl}) = \iota^+_{m,n}(\Delta_{m,n}(f))$. By the description of $\mathcal{D}^+_{m,n}$ above, we see that $b_{kl} = 0$ unless $(k,l) = (2i,2j)$ for some (i,j), in which case

$$b_{kl} = a_{ij} + a_{i-1,j} + a_{i+1,j} + a_{i,j-1} + a_{i,j+1}.$$

By the definition of $\iota^+_{m,n}$, we see that $c_{kl} = 0$ unless $(k,l) = (2i,2j)$ for some (i,j), in which case c_{kl} is equal to the (i,j)-entry of $\Delta_{m,n}(f)$, namely

$$c_{kl} = a_{ij} + a_{i-1,j} + a_{i+1,j} + a_{i,j-1} + a_{i,j+1}.$$

Thus we have $b_{kl} = c_{kl}$ for any (k,l). Similarly for the "minus" case.

For (v), note that $\mathcal{D}^+_{m,n} \circ \pi^+_{m,n} + \mathcal{D}^-_{m,n} \circ \pi^-_{m,n} = \Delta_{2m,2n} \circ (\iota^+_{m,n} \circ \pi^+_{m,n} + \iota^-_{m,n} \circ \pi^-_{m,n})$. For $f = (b_{kl}) \in \mathcal{F}_{2m,2n}$, we have

$$\begin{aligned} &(\iota^+_{m,n} \circ \pi^+_{m,n} + \iota^-_{m,n} \circ \pi^-_{m,n})(f) \\ &= \begin{pmatrix} b_{00} & 0 & b_{02} & 0 & \cdots \\ 0 & b_{11} & 0 & b_{13} & \cdots \\ b_{20} & 0 & b_{22} & 0 & \cdots \\ 0 & b_{31} & 0 & b_{33} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \end{aligned}$$

If $f \in \mathcal{H}_{2m,2n}$, i.e., $\Delta_{2m,2n}(f) = O$, then

$$b_{kl} = b_{k-1,l} + b_{k+1,l} + b_{k,l-1} + b_{k,l+1},$$

and hence

$$\left(\Delta_{2m,2n} \circ (\iota^+_{m,n} \circ \pi^+_{m,n} + \iota^-_{m,n} \circ \pi^-_{m,n})\right)(f) = f.$$

To prove (vi), let $f \in \mathcal{H}_{2m,2n}$. We have

$$\begin{aligned} O &= \Delta_{2m,2n}(f) \\ &= \Delta_{2m,2n}\left(\mathcal{D}^+_{m,n}(\pi^+_n(f)) + \mathcal{D}^-_{m,n}(\pi^-_n(f))\right) \\ &= \iota^+_{m,n}(\Delta_{m,n}(\pi^+_{m,n}(f))) + \iota^-_{m,n}(\Delta_{m,n}(\pi^-_{m,n}(f))), \end{aligned}$$

by (iv), (v). Hence by (ii), we have

$$\Delta_{m,n}(\pi^+_{m,n}(f)) = \Delta_{m,n}(\pi^-_{m,n}(f)) = O,$$

which completes the proof. □

Proof of Theorem 1.1: We shall show that

$$\mathcal{D}^+_{m,n}(\mathcal{H}_{m,n}) \oplus \mathcal{D}^-_{m,n}(\mathcal{H}_{m,n}) = \mathcal{H}_{2m,2n}.$$

First, we claim that for $f \in \mathcal{F}_{m,n}$,

$$\begin{aligned} f \in \mathcal{H}_{m,n} &\iff \mathcal{D}^+_{m,n}(f) \in \mathcal{H}_{2m,2n} \\ &\iff \mathcal{D}^-_{m,n}(f) \in \mathcal{H}_{2m,2n}. \end{aligned}$$

Indeed, we have

$$\begin{aligned} f \in \mathcal{H}_{m,n} &\iff \Delta_{m,n}(f) = O \\ &\iff \iota^\pm_{m,n}(\Delta_{m,n}(f)) = O \\ &\iff \Delta_{2m,2n}(\mathcal{D}^\pm_{m,n}(f)) = O \\ &\iff \mathcal{D}^\pm_{m,n}(f) \in \mathcal{H}_{2m,2n} \end{aligned}$$

by Lemma 2.1(i), (iv). In particular, we have

$$\mathcal{D}^+_{m,n}(\mathcal{H}_{m,n}) + \mathcal{D}^-_{m,n}(\mathcal{H}_{m,n}) \subset \mathcal{H}_{2m,2n}.$$

Second, we have

$$\mathcal{D}^+_{m,n}(\mathcal{H}_{m,n}) \cap \mathcal{D}^-_{m,n}(\mathcal{H}_{m,n}) = \{O\}$$

by Lemma 2.1(iii). Finally, it follows from Lemma 2.1(v), (vi) that

$$\mathcal{H}_{2m,2n} \subset \mathcal{D}^+_{m,n}(\mathcal{H}_{m,n}) + \mathcal{D}^-_{m,n}(\mathcal{H}_{m,n}).$$

This completes the proof. □

3. AN ELLIPTIC CURVE

The spectrum of $\Delta(C_{m,n})$ is well known when mn is prime to the characteristic.

Lemma 3.1. *Let K be an algebraically closed field whose characteristic is prime to mn, and ζ_m (respectively ζ_n) a primitive mth (respectively nth) root of unity in K. The adjacency matrix $A(C_{m,n})$ is diagonalizable over K, and the eigenvalues are, multiplicity taken into account,*

$$\zeta_n^i + \zeta_n^{-i} + \zeta_m^j + \zeta_m^{-j}, \quad 0 \le i \le n-1,\ 0 \le j \le m-1.$$

Let $\overline{\mathbb{F}}_2$ be the algebraic closure of $\mathbb{F}_2$. Since

$$\begin{aligned} d(C_{m,n}) &= \operatorname{corank}_{\mathbb{F}_2}(I + A(C_{m,n})) \\ &= \operatorname{corank}_{\overline{\mathbb{F}}_2}(I + A(C_{m,n})), \end{aligned}$$

we have the following.

Corollary 3.2. *For m, n odd, we have $d(C_{m,n}) = |S(m,n)|$, where*

$$\begin{aligned} &S(m,n) \\ &\quad = \big\{(x,y) \in \overline{\mathbb{F}}_2^\times \times \overline{\mathbb{F}}_2^\times \mid x + x^{-1} + y + y^{-1} + 1 = 0, \\ &\qquad\quad x^m = y^n = 1\big\}. \end{aligned}$$

See [Hunziker et al. 04, Zaidenberg 08b] for the proof of Lemma 3.1 and Corollary 3.2.

Corollary 3.3. *Suppose m, n are odd.*

$$\text{(i)}\ \ d(C_{m,n}) \equiv \begin{cases} 0 \pmod 4, & mn \not\equiv 0 \pmod 3 \\ & \text{or } m \equiv n \equiv 0 \pmod 3, \\ 2 \pmod 4, & \text{otherwise.} \end{cases}$$

$$\text{(ii)}\ \ d(n) \equiv \begin{cases} 0 \pmod 8, & n \not\equiv 0 \pmod 3, \\ 4 \pmod 8, & n \equiv 0 \pmod 3. \end{cases}$$

Proof: Put

$$S_0(m,n) = \{(x,y) \in S(m,n) \mid x \neq 1,\ y \neq 1\}.$$

If $(x,y) \in S_0(m,n)$, then the four pairs

$$(x,y),\ \ (x^{-1},y),\ \ (x,y^{-1}),\ \ (x^{-1},y^{-1}) \in S_0(m,n)$$

are distinct. Hence $|S_0(m,n)| \equiv 0 \pmod 4$. Furthermore, if $(x,y) \in S_0(n,n)$, then the eight pairs

$$(x^\pm, y^\pm),\ \ (y^\pm, x^\pm) \in S_0(n,n)$$

are distinct. Hence $|S_0(n,n)| \equiv 0 \pmod 8$. Let $\omega \in \overline{\mathbb{F}}_2$ be a third root of unity. Noting that in $\overline{\mathbb{F}}_2$, $x + x^{-1} = 0$ (respectively $x + x^{-1} = 1$) if and only if $x = 1$ (respectively $x = \omega, \omega^2$), we have

$$S(m,n) = \begin{cases} S_0(m,n), \\ \qquad \text{if } mn \not\equiv 0 \pmod 3, \\ S_0(m,n) \cup \{(1,\omega),(1,\omega^2),(\omega,1),(\omega^2,1)\}, \\ \qquad \text{if } m \equiv n \equiv 0 \pmod 3, \\ S_0(m,n) \cup \{(1,\omega),(1,\omega^2)\}, \\ \qquad \text{if } m \not\equiv 0 \equiv n \pmod 3, \\ S_0(m,n) \cup \{(\omega,1),(\omega^2,1)\}, \\ \qquad \text{if } m \equiv 0 \not\equiv n \pmod 3. \end{cases}$$

The claim follows easily. □

Let us now consider the equation

$$x + x^{-1} + y + y^{-1} + 1 = 0$$

over $\overline{\mathbb{F}}_2$. Clearing denominators and homogenizing, we obtain a projective curve

$$E : (x + y + z)(xy + z^2) + z^3 = 0$$

defined over $\mathbb{F}_2$. It turns out that E is an elliptic curve. We list basic properties of E. Some of them are known and used in [Zaidenberg 08b, Section 3.3]. We follow the notation of [Silverman 86]; in particular, $E[n]$ denotes the set of n-torsion points. We write $S(n) = S(n,n)$.

Lemma 3.4.

(i) *E is an elliptic curve with identity element $O = [1,1,0]$.*

(ii) *$E[2] = \{O, P_2\}$, where $P_2 = [0,0,1]$.*

(iii) *E is ordinary; i.e., $E[2^r]$ is a cyclic group of order 2^r for each $r \ge 1$.*

(iv) $E(\mathbb{F}_2) = E[4] = E[2] \cup \{[1,0,0],[0,1,0]\}$, *and there is no point of E at infinity.*

(v) *The congruent zeta function of $E/\mathbb{F}_2$ is*

$$Z(E/\mathbb{F}_2, T) = \frac{(1-\alpha T)(1-\bar{\alpha} T)}{(1-T)(1-2T)},$$

where $\alpha + \bar{\alpha} = -1$ and $\alpha\bar{\alpha} = 2$. Consequently, $|E(\mathbb{F}_{2^r})| = 2^r + 1 - \alpha^r - \bar{\alpha}^r$.

(vi) *For n odd, we can consider $S(n)$ as a subset of $E(\overline{\mathbb{F}}_2)$ by $(x,y) \mapsto [x,y,1]$. Under this identification, $S(2^r-1) = E(\mathbb{F}_{2^r}) \setminus E[4]$.*

(vii) *Let $[a,b,1] \in E(\overline{\mathbb{F}}_2) \setminus E[4]$.*

(a) $-[a,b,1] = [b,a,1]$.

(b) $ab \neq 0$ *and* $[a,b,1] + P_2 = [a^{-1}, b^{-1}, 1]$.

Proof: The verification is straightforward. (iii) E is ordinary because $|E[2]| = 2$.

(v) $\alpha + \bar{\alpha} = -1$, since $|E(\mathbb{F}_2)| = 4$.

(vii)(a) The line through $[a,b,1]$ and O is $-x + y + (a-b)z = 0$. The third intersection point of this line with E is $[b,a,1]$.

(vii)(b) The line through $[a,b,1]$ and P_2 is $bx - ay = 0$. The third intersection point is $[b^{-1}, a^{-1}, 1]$. Therefore, $[a,b,1] + P_2 = -[b^{-1}, a^{-1}, 1] = [a^{-1}, b^{-1}, 1]$ by (a). □

Remark 3.5. The curve E is isomorphic to 15A8 in Cremona's database [Cremona 97].

Corollary 3.6. (Cf. [Zaidenberg 08b], Lemma 3.5.) *$d(2^r - 1) = 2^r - 3 - \alpha^r - \bar{\alpha}^r$, where $\alpha, \bar{\alpha}$ are the roots of $t^2 + t + 2$.*

Proof: This follows from Corollary 3.2 and Lemma 3.4(iv), (v), (vi). □

Proof of Theorem 1.2: Consider the multiplication-by-2 map

$$[2] : E \to E.$$

This is a 2-isogeny, since E is ordinary. The image of $E(\overline{\mathbb{F}}_2) \setminus E[4]$ under this map is $E(\overline{\mathbb{F}}_2) \setminus E[2]$. We claim that

$$[2]^{-1}\left(E(\mathbb{F}_{2^r}) \setminus E[2]\right) = S(2^r - 1) \cup S(2^r + 1).$$

Let $P = [x,y,1] \in E(\overline{\mathbb{F}}_2) \setminus E[4]$ and suppose that $[2]P \in E(\mathbb{F}_{2^r}) \setminus E[2]$. Let ϕ be the 2^r-power Frobenius automorphism of $\overline{\mathbb{F}}_2$, which also acts on $E(\overline{\mathbb{F}}_2)$ as an endomorphism. From

$$[2]P = ([2]P)^{\phi} = [2]P^{\phi},$$

it follows that

$$P^{\phi} - P \in E[2] = \{O, P_2\},$$

i.e., $[x^{2^r}, y^{2^r}, 1] = [x,y,1]$ or $[x^{2^r}, y^{2^r}, 1] = [x,y,1] + P_2 = [x^{-1}, y^{-1}, 1]$. We have $(x,y) \in S(2^r - 1)$ in the former case, and $(x,y) \in S(2^r + 1)$ in the latter case. This proves the claim.

Since $S(2^r - 1)$ and $S(2^r + 1)$ are disjoint and $\deg[2] = 2$, we have

$$|S(2^r - 1)| + |S(2^r + 1)| = 2|E(\mathbb{F}_{2^r}) \setminus E[2]|,$$

i.e.,

$$d(2^r - 1) + d(2^r + 1) = 2(d(2^r - 1) + 2),$$

from which the theorem follows. □

4. LIGHTS OUT AND TORUS LIGHTS OUT

It is known that

$$d(C_{m,n}) > 0 \iff mn \equiv 0 \pmod 3 \text{ or } d(P_{m-1,n-1}) > 0$$

(cf. [Zaidenberg 08b, Corollary 2.12]). We sought a quantitative version of this fact, but could not find any in the literature. Here we present the following conjecture.

Conjecture 4.1. *For a positive integer k, let $\nu_2(k)$ denote the largest integer ν such that 2^ν divides k. We have*

$$d(C_{m,n}) = 2d(P_{m-1,n-1}) + 2\delta_{m,n},$$

where $\delta_{m,n} = \delta_{n,m}$ and

- *if $mn \not\equiv 0 \pmod 3$, then $\delta_{m,n} = 0$;*
- *if $m \not\equiv 0 \pmod 3$, $n \equiv 0 \pmod 3$, then*

$$\delta_{m,n} = \begin{cases} 0, & \nu_2(m) > \nu_2(n) + 1, \\ 1, & \nu_2(m) \leq \nu_2(n) + 1; \end{cases}$$

- *if $m \equiv n \equiv 0 \pmod 3$, then*

$$\delta_{m,n} = \begin{cases} 1, & |\nu_2(m) - \nu_2(n)| > 1, \\ 2, & |\nu_2(m) - \nu_2(n)| \leq 1. \end{cases}$$

In particular, we have

$$d(n) = \begin{cases} 2d(P_{n-1,n-1}), & n \not\equiv 0 \pmod 3, \\ 2d(P_{n-1,n-1}) + 4, & n \equiv 0 \pmod 3. \end{cases}$$

We have checked the validity of this conjecture for $2 \le m \le n \le 65$ and for $m = n \le 345$. If this conjecture is true, then most of our observations on $d(n)$ will have counterparts for $d(P_{n-1,n-1})$. For example, Theorem 1.1 and Corollary 3.3 would settle Sutner's conjecture [Sutner 89, p. 52]. See also [Hunziker et al. 04, p. 475].

We have another formulation of this conjecture in terms of Chebyshev–Dickson polynomials (cf. [Zaidenberg 08b, Appendix B]). In the rest of this section, we always work in the polynomial ring $\mathbb{F}_2[x]$. Let $T_n, E_n \in \mathbb{F}_2[x]$ be the Chebyshev–Dickson polynomials of respectively the first and second kinds:

$$T_{n+1}(x) = xT_n(x) + T_{n-1}(x), \quad T_0(x) = 0,\, T_1(x) = x,$$
$$E_{n+1}(x) = xE_n(x) + E_{n-1}(x), \quad E_0(x) = 1,\, E_1(x) = x.$$

Here are some basic properties of Chebyshev–Dickson polynomials. See [Zaidenberg 08b, Appendix B] or [Hunziker et al. 04] for reference.

Lemma 4.2.

(i) $\deg T_n = \deg E_n = n$.

(ii) $T_n(x) = xE_{n-1}(x)$.

(iii) $E_n(0) = 0 \iff n \equiv 1 \pmod 2$.

(iv) $E_n(1) = 0 \iff n + 1 \equiv 0 \pmod 3$.

(v) $E_{2^k m-1}(x) = x^{2^k-1} E_{m-1}(x)^{2^k}$.

(vi) $E_{2^k-2}(x)E_{2^k}(x) = (x^{2^k-1} - 1)^2$.

The following two results explain the importance of Chebyshev–Dickson polynomials for our subject.

Theorem 4.3. [Sutner 00]

$$d(P_{m,n}) = \deg \gcd(E_m(x), E_n(x+1)).$$

Theorem 4.4. [Barua and Ramakrishnan 96] $d(C_{m,n}) > 0$ *holds if and only if* $\deg \gcd(T_m(x), T_n(x+1)) > 0$.

Our conjecture is a quantitative version of the latter theorem.

Conjecture 4.5. $d(C_{m,n}) = 2 \deg \gcd(T_m(x), T_n(x+1))$.

Proposition 4.6. *Conjectures 4.1 and 4.5 are equivalent.*

Proof: Put

$$\varepsilon_{m,n} = \deg \gcd(T_m(x), T_n(x+1)) - \deg \gcd(E_{m-1}(x), E_{n-1}(x+1)).$$

By Theorem 4.3, we have to verify $\varepsilon_{m,n} = \delta_{m,n}$. For $f, g \in \mathbb{F}_2[x]$, let $\nu_f(g)$ denote the largest integer ν such that f^ν divides g, and let

$$a = \nu_x(E_{m-1}(x)), \quad b = \nu_x(E_{n-1}(x+1))$$

and

$$c = \nu_{x+1}(E_{m-1}(x)), \quad d = \nu_{x+1}(E_{n-1}(x+1)).$$

By Lemma 4.2(ii), we have

$$\begin{aligned} \varepsilon_{m,n} &= \min\{a+1, b\} - \min\{a, b\} + \min\{c, d+1\} \\ &\quad - \min\{c, d\} \\ &= \begin{cases} 0, & a \ge b,\, c \le d, \\ 2, & a < b,\, c > d, \\ 1, & \text{otherwise.} \end{cases} \end{aligned}$$

By Lemma 4.2(iii), (iv), (v), we have

$$\begin{aligned} a &= 2^{\nu_2(m)} - 1, \\ b &= \begin{cases} 2^{\nu_2(n)+1}, & n \equiv 0 \pmod 3, \\ 0, & \text{otherwise,} \end{cases} \\ c &= \begin{cases} 2^{\nu_2(m)+1}, & m \equiv 0 \pmod 3, \\ 0, & \text{otherwise,} \end{cases} \\ d &= 2^{\nu_2(n)} - 1. \end{aligned}$$

Putting these together, we obtain $\varepsilon_{m,n} = \delta_{m,n}$. □

We give alternative proofs of Theorems 1.1 and 1.2, assuming Conjecture 4.5.

Theorem 1.1 follows from $T_{2k}(x) = T_k(x)^2$, which is a consequence of Lemma 4.2(ii), (v).

By Lemma 4.2(ii), (vi) and noting that $(x+1)^{2^r} - (x+1) = x^{2^r} - x$, we have

$$T_{2^r+1}(x)T_{2^r-1}(x)T_{2^r-1}(x+1) = (x^{2^r} - x)^2 T_{2^r-1}(x+1),$$

and

$$T_{2^r+1}(x+1)T_{2^r-1}(x)T_{2^r-1}(x+1) = (x^{2^r} - x)^2 T_{2^r-1}(x).$$

By taking "$2 \deg \gcd$" of both sides, we obtain Theorem 1.2.

5. FURTHER OBSERVATIONS

We make three observations on $d(n)$.

5.1 Prime Powers

Conjecture 5.1. *$d(p^k) = d(p)$ if p is a prime.*

We have checked the validity of this conjecture directly for $p^k \leq 5^4$, and also for $p^k \leq 2^{16}$ assuming Conjecture 4.5. In [Goshima and Yamagishi 09], assuming Conjecture 5.1 for $p = 5$, we gave a nice criterion for the solvability of the $5^k \times 5^k$ torus lights out puzzle.

5.2 Additivity

Additivity in the naive sense

$$\gcd(m, n) = 1 \Longrightarrow d(mn) = d(m) + d(n)$$

sometimes holds but does not hold in general. For example, $d(15) = d(3) + d(5)$, but $d(63) > d(7) + d(9)$. The "partnership graph" by Zagier seems to give the most precise formulation; see [Zaidenberg 08b, Section 3.4]. Note that we have

$$\gcd(m, n) = 1 \Longrightarrow d(mn) \geq d(m) + d(n),$$

by Corollary 3.2 and Theorem 1.1. Alternatively, we can see this as follows. There is a natural graph covering map $C_{mn,mn} \to C_{m,m}$, which induces an injection $i_1 : \mathcal{H}_{m,m} \hookrightarrow \mathcal{H}_{mn,mn}$. Similarly, we have $i_2 : \mathcal{H}_{n,n} \hookrightarrow \mathcal{H}_{mn,mn}$. If $\gcd(m, n) = 1$, then we can show that $i_1(\mathcal{H}_{m,m})$, $i_2(\mathcal{H}_{n,n})$ are linearly independent, and hence we have

$$\mathcal{H}_{m,m} \oplus \mathcal{H}_{n,n} \cong i_1(\mathcal{H}_{m,m}) \oplus i_2(\mathcal{H}_{n,n}) \subset \mathcal{H}_{mn,mn}.$$

5.3 Primes p with $d(p) > 0$

As we have just seen, if $d(n) > 0$ then $d(kn) > 0$ for all $k \geq 1$. What is interesting therefore is the case that $d(n) > 0$ but $d(n') = 0$ for all proper divisors n' of n. Such an n is called MAD in [Brouwer 08]. For example, a prime p with $d(p) > 0$ is MAD. By Corollary 1.3, Mersenne primes except for 7 and Fermat primes have this property. A natural question arises: do there exist other primes with $d(p) > 0$? Some examples are given in [Brouwer 08]:

$$\begin{aligned}
683 &= \frac{2^{11}+1}{3}, & 2731 &= \frac{2^{13}+1}{3}, \\
43691 &= \frac{2^{17}+1}{3}, & 61681 &= \frac{2^{20}+1}{17}, \\
174763 &= \frac{2^{19}+1}{3}, & 178481 &= \frac{2^{23}-1}{47}, \\
2796203 &= \frac{2^{23}+1}{3}, & 3033169 &= \frac{2^{29}+1}{177}, \\
6700417 &= \frac{2^{32}+1}{641}, & 15790321 &= \frac{2^{28}+1}{17}.
\end{aligned}$$

See also [Hunziker et al. 04] for the first four. It would be interesting to be able to characterize such primes.

ACKNOWLEDGMENTS

The authors express their deep gratitude to Professors Toshiaki Adachi, Yasushi Mizusawa, and Yoshihiro Nakamura for stimulating discussions and useful comments. The authors also thank the referee for suggestions that resulted in an improved presentation of this paper.

REFERENCES

[Barua and Ramakrishnan 96] Rana Barua and S. Ramakrishnan. "σ-Game, σ^+-Game and Two-Dimensional Additive Cellular Automata." *Theoret. Comput. Sci.* 154:2 (1996), 349–366.

[Brouwer 08] Andries E. Brouwer. "Button Madness and Lights Out on Rectangles." Available online (http://www.win.tue.nl/~aeb/ca/madness/madrect.html), 2008.

[Cartier 72] P. Cartier. "Fonctions harmoniques sur un arbre." In *Symposia Mathematica, Vol. IX (Convegno di Calcolo delle Probabilità, INDAM, Rome, 1971)*, pp. 203–270. London: Academic Press, 1972.

[Cartier 73] Pierre Cartier. "Géométrie et analyse sur les arbres." In *Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 407*, Lecture Notes in Math. 317, pp. 123–140. Berlin: Springer, 1973.

[Cremona 97] J. E. Cremona. *Algorithms for Modular Elliptic Curves*, second edition. Cambridge, UK: Cambridge University Press, 1997.

[Goldwasser et al. 02] John Goldwasser, William Klostermeyer, and Henry Ware. "Fibonacci Polynomials and Parity Domination in Grid Graphs." *Graphs Combin.* 18:2 (2002), 271–283.

[Goshima and Yamagishi 09] Masato Goshima and Masakazu Yamagishi. "Two Remarks on Torus Lights Out Puzzle." *Adv. Appl. Discrete Math.* 4:2 (2009), 115–126.

[Hunziker et al. 04] Markus Hunziker, António Machiavelo, and Jihun Park. "Chebyshev Polynomials over Finite Fields and Reversibility of σ-Automata on Square Grids." *Theoret. Comput. Sci.* 320:2–3 (2004), 465–483.

[Joyner 02] David Joyner. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine and Other Mathematical Toys.* Baltimore: Johns Hopkins University Press, 2002.

[Silverman 86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106. New York: Springer, 1986.

[Sutner 89] Klaus Sutner. "Linear Cellular Automata and the Garden-of-Eden." *Math. Intelligencer* 11:2 (1989), 49–53.

[Sutner 90] Klaus Sutner. "The σ-Game and Cellular Automata." *Amer. Math. Monthly* 97:1 (1990), 24–34.

[Sutner 00] Klaus Sutner. "σ-Automata and Chebyshev Polynomials." *Theoret. Comput. Sci.* 230:1–2 (2000), 49–73.

[Zaidenberg 08a] Mikhail Zaidenberg. "Convolution Equations on Lattices: Periodic Solutions with Values in a Prime Characteristic Field." In *Geometry and Dynamics of Groups and Spaces*, Progr. Math. 265, pp. 721–742. Basel: Birkhäuser, 2008.

[Zaidenberg 08b] Mikhail Zaidenberg. "Periodic Binary Harmonic Functions on Lattices." *Adv. in Appl. Math.* 40:2 (2008), 225–265.

[Zaidenberg 09] Mikhail Zaidenberg. "Periodic Harmonic Functions on Lattices and Points Count in Positive Characteristic." *Cent. Eur. J. Math.* 7:3 (2009), 365–381.

Masato Goshima, Division of Mathematics and Mathematical Science, Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan (astralslidejp@yahoo.co.jp)

Masakazu Yamagishi, Department of Mathematics, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan. (yamagishi.masakazu@nitech.ac.jp)

Received January 29, 2010; accepted February 3, 2010.