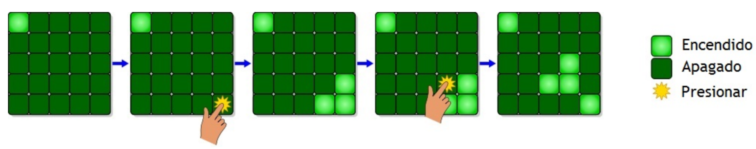
NUMBER OF SOLUTIONS TO THE LIGTHS OUT GAME

VICENTE MUÑOZ

Abstract. Using linear algebra over the field $\mathbb{F}_2$, we compute the number of solutions to the game Lights Out. This is given in terms of the irreducible polynomials over $\mathbb{F}_2$.

The present text is a (somehow trimmed) English version of the paper "Las matemáticas del juego Lights Out!" (in Spanish, La Gaceta de la RSME, 2015).

Lights Out is an electronic game, released by the Company Tiger Toys in 1995. The game consists of a 5 by 5 grid of lights. When the game starts, a random number or a stored pattern of these lights is switched on. Pressing any of the lights will toggle it and the four adjacent lights. The goal of the puzzle is to switch all the lights off.



A number of papers and webpages in Recreational Mathematics have appear since on the topic, mainly occupied in ways to solve the puzzle (see [9, 15] and the references therein). We are interested in the problem for a board of general size $n \times n$, specifically in the problem of starting with all lights on. By the work of Sutner, it is known that this game has always solutions. Here we shall study *how many solutions* there are.

In the case of a grid 5×5, this problem has been analysed mathematically in the papers [1, 8], by matrix algebra arguments over the field $\mathbb{F}_2$. We are going to extend this method to general grids $n \times n$ and use some (elementary) theory on finite fiels and irreducible polynomials (over $\mathbb{F}_2$) to help us computing the number of solutions. Similar results have appeared already in the literature [2, 3, 4, 7, 5, 6, 12, 14, 16].

Let us start with some notations. Consider an $n \times n$-grid. The position of a square is given by a bit in $\mathbb{F}_2 = \{0, 1\}$, where 0 means "off" and 1 means "on". Therefore the set of possible positions of the grid is given by the $\mathbb{F}_2$-vector space $V = (\mathbb{F}_2)^{n^2}$. Here each factor corresponds to a square and the order is going from left to right line by line, and then from top to bottom. Pressing a square an even number of times is like no pressing it at all, and pressing it an odd number of times is like just pressing it once. Hence the possible ways of pressing squares is given again by $V = (\mathbb{F}_2)^{n^2}$, where a 0 means "not pressing" and 1 means "pressing". The order of the factors corresponds to the squares in the same way as before. The effect of the possible ways of pressing squares is given by an $\mathbb{F}_2$-linear function

$$f_n : V \to V \tag{1}$$

Date: April 2014.
2010 *Mathematics Subject Classification.* 97A20, 11C20, 12Y05.
Key words and phrases. Mathematical games. Irreducible polynomials. Finite fields. Linear algebra.

whose matrix is

$$M_n = \begin{pmatrix} B_n & I_n & 0 & \dots & 0 & 0 \\ I_n & B_n & I_n & \dots & 0 & 0 \\ 0 & I_n & B_n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B_n & I_n & 0 \\ 0 & 0 & \dots & I_n & B_n & I_n \\ 0 & 0 & \dots & 0 & I_n & B_n \end{pmatrix}, \tag{2}$$

where I_n is the identity $(n \times n)$-matrix and

$$B_n = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & \dots & 1 & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 & 1 \end{pmatrix}. \tag{3}$$

That is, if $a = (a_1, \dots, a_{n^2})^t \in V$ is a way of pressing squares then $f(a) = M\,a$ is the resulting pattern of lights. The result of [13] means that $\mathbf{1} = (1, 1, \dots, 1)^t \in \operatorname{im}(f)$. Therefore the number of possible solutions to $f(a) = \mathbf{1}$ is $M(n) = 2^d_n$, where

$$d_n = \dim \ker(f_n).$$

Theorem 1. *Let $P_n(t) = \det(B_n - tI_n) \in \mathbb{F}_2[t]$ be the characteristic polynomial of B_n. Then d_n is the degree of* $\gcd(P_n(t), P_n(t+1))$.

Proof. The characteristic polynomial of (3) is a degree n polynomial $P_n \in \mathbb{F}_2[t]$. By the Cayley-Hamilton theorem, $P_n(B_n) = 0$. Now let us see that P_n is the minimal polynomial, that is, the minimum degree monic polynomial P satisfying $P(B_n) = 0$. If $v_1 = (1, 0, 0, \dots, 0)$, then $v_2 = B_n(v_1) = (*, 1, 0, \dots, 0)$, $v_3 = B_n(v_2) = (*, *, 1, 0, \dots, 0)$ and so on. So $v_1, \dots, v_n = B_n^{n-1}(v_1)$ are linearly independent. Therefore $I, B_n, \dots, B_n^{n-1}$ are linearly independent. This means that $P_n(t)$ is the minimal polynomial.

As a consequence, all repeated eigenvalues of B_n appear in Jordan blocks of maximum size. Let $\lambda_1, \dots, \lambda_r$ be the (distinct) eigenvalues of B_n in the algebraic closure $\overline{\mathbb{F}}_2$, and let d_i be the multiplicity of λ_i. There is a basis (over $\overline{\mathbb{F}}_2$) in which we can write

$$B_n \sim B'_n = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_r \end{pmatrix}, \text{ where } J_i = \begin{pmatrix} \lambda_i & 0 & \dots & 0 \\ 1 & \lambda_i & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & \lambda_i \end{pmatrix}, \ i = 1, \dots, r$$

Consider now the matrix (2), which is an endomorphism of $V = \mathbb{F}_2^{n^2} = \mathbb{F}_2^n \oplus \overset{(n)}{\cdots} \mathbb{F}_2^n$. Going to the algebraic closure $\overline{\mathbb{F}}_2$, and using the basis found above on each copy of $\mathbb{F}_2^n$, we have

$$M_n \sim M'_n = \begin{pmatrix} B'_n & I_n & 0 & \dots & 0 & 0 \\ I_n & B'_n & I_n & \dots & 0 & 0 \\ 0 & I_n & B'_n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & B'_n & I_n & 0 \\ 0 & 0 & \dots & I_n & B'_n & I_n \\ 0 & 0 & \dots & 0 & I_n & B'_n \end{pmatrix}.$$

Now we reorde the basis. Take the first vector of each of the factors $\mathbb{F}_2^n$, then continue by the second vector of each of the factors, and so successively. This gives a matrix as follows:

$$M_n \sim M_n'' = \begin{pmatrix} K_1 & 0 & \dots & 0 \\ 0 & K_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & K_r \end{pmatrix}, \text{ with } K_i = \begin{pmatrix} \Lambda_{\lambda_i} & 0 & 0 & \dots & 0 \\ I & \Lambda_{\lambda_i} & 0 & \dots & 0 \\ 0 & I & \Lambda_{\lambda_i} & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & I & \Lambda_{\lambda_i} \end{pmatrix},$$

where we have written

$$\Lambda_\lambda = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 1 & \lambda & 1 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}.$$

Note that $\Lambda_\lambda = B_n + (\lambda - 1)I_n$, so the basis that puts B_n in Jordan form, does also put Λ_λ into its Jordan form $\Lambda'_\lambda = B'_n + (\lambda - 1)I_n$. Hence

$$M_n \sim M_n''' = \begin{pmatrix} K'_1 & 0 & \dots & 0 \\ 0 & K'_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & K'_r \end{pmatrix}, \text{ with } K'_i = \begin{pmatrix} B'_n + (\lambda_i - 1)I_n & 0 & \dots & 0 \\ I & B'_n + (\lambda_i - 1)I_n & \dots & 0 \\ 0 & I & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B'_n + (\lambda_i - 1)I_n \end{pmatrix}.$$

where

$$B'_n + (\lambda_i - 1)I_n = \begin{pmatrix} J_{i1} & 0 & \dots & 0 \\ 0 & J_{i2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{ir} \end{pmatrix}, \text{ and } J_{ij} = \begin{pmatrix} \lambda_j + \lambda_i - 1 & 0 & \dots & 0 \\ 1 & \lambda_j + \lambda_i - 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & \lambda_j + \lambda_i - 1 \end{pmatrix}.$$

Rearranging the blocks, we see that $M_n \sim M_n'''$, which is formed by blocks, for each pair (i, j) of the form

$$T_{ij} = \begin{pmatrix} J_{ij} & 0 & \dots & 0 \\ I & J_{ij} & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & I & J_{ij} \end{pmatrix}. \tag{4}$$

The size of J_{ij} is the multiplicity of the eigenvalue λ_j in $P_n(t)$, and the number of J_{ij} in (4) is the multiplicity of the eigenvalue λ_i.

To compute $d_n = \dim \ker M_n$, we need to sum the dimensions of the kernels of each T_{ij}. Note that there is a contribution to the kernel only when $\lambda_i - \lambda_j = 1$. Suposse now that $\lambda_i - \lambda_j = 1$, and let v be a vector in the kernel of T_{ij}. Write it as $v = v_1 + \ldots + v_{d_i}$, according to the splitting in (4). Then, abbreviating $J = J_{ij}$, we have $T_{ij}(v) = 0 \implies Jv_1 = 0, Jv_2 = v_1, \ldots, Jv_{d_i} = v_{d_i - 1}$. If $d_i \le d_j$, the kernel is determined by $v = v_{d_i}$ subject to $J^{d_i} v = 0$, that is of dimension d_i. If $d_j < d_i$, can choose v_{d_i} freely, and the dimension is d_j. So $\dim \ker T_{ij} = \min\{d_i, d_j\}$. Finally

$$d_n = \dim \ker M_n = \sum_{\lambda_i = \lambda_j + 1} \dim \ker T_{ij} = \sum_{\lambda_i = \lambda_j + 1} \min\{d_i, d_j\} = \deg \gcd(P_n(t), P_n(t+1)).$$

□

Note that a trivial consequence to Theorem 1 is that

$$d_n \le n$$

(initially we only know $d_n \le n^2$). This of course follows by the Lights Chasing solving method explained in [1, 15]). Another consequence of the formula is $d_n = \sum_{\lambda_i = \lambda_j + 1} \min\{d_i, d_j\}$ is that d_n is even.

Now we want to compute the polynomial $P_n(t)$.

Proposition 2. *$P_n(t) = \sum_{b=0}^{[n/2]} \binom{n-b}{b}(1+t)^{n-2b}$. Moreover, P_n satisfy the recurrence $P_{n+1}(t) = (1+t)P_n(t) + P_{n-1}(t)$.*

Proof. The polynomial $P_n(t)$ is the determinant of

$$B_n - tI_n = \begin{pmatrix} 1-t & 1 & 0 & \dots & 0 & 0 \\ 1 & 1-t & 1 & \dots & 0 & 0 \\ 0 & 1 & 1-t & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1-t & 1 \\ 0 & 0 & \dots & 0 & 1 & 1-t \end{pmatrix}.$$

Consider the algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$, which is an infinite field. We shall calculate the above determinant for $t \in \overline{\mathbb{F}}_2$ generic. Then by Gauss elimination applied to $B_n - tI_n$, we get the matrix

$$\begin{pmatrix} c_1 & 0 & 0 & \dots & 0 & 0 \\ * & c_2 & 0 & \dots & 0 & 0 \\ * & * & c_3 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ * & * & \dots & * & c_{n-1} & 0 \\ * & * & \dots & * & * & c_n \end{pmatrix},$$

where

$$c_1 = 1-t$$
$$c_{k+1} = 1 - t - c_k^{-1}, \qquad k \geq 1.$$

Then the characteristic polynomial of M is

$$P_n(t) = \det(M - tI) = \prod_{k=1}^{n} c_k$$

Writing $d_s = \prod_{k=1}^{s} c_k$, we have that $d_{s+1} = c_{k+1}d_s = (1-t)d_s - d_s c_k^{-1} = (1-t)d_s - d_{s-1}$, and $P_n(t) = d_n$. The recurrence relation follows readily from this (noting that as we are in characteristic 2, signs are not relevant).

Consider the generating function $g(x) = \sum_{s\geq 0} d_s x^s$. We have the recurrence $g(x) = 1 + x(1-t)g(x) - x^2 g(x)$, hence

$$g(x) = \frac{1}{1 - x(1-t) + x^2}$$

and

$$P_n(t) = \mathrm{Coeff}_{x^n}\, g(x).$$

Expanding in power series,

$$g(x) = \sum_{a\geq 0}(x(1-t) - x^2)^a = \sum_{a\geq 0}\sum_{b=0}^{a}\binom{a}{b}(-1)^b(1-t)^{a-b}x^{a+b}.$$

Recalling that we are in characteristic 2, so $\pm 1 = 1$, we have

$$P_n(t) = \sum_{b=0}^{[n/2]}\binom{n-b}{b}(1+t)^{n-2b}.$$

□

Note that we can write

$$Q_n(t) = P_n(t+1) = \sum_{b=0}^{[n/2]}\binom{n-b}{b}t^{n-2b}, \tag{5}$$

and then $d_n = \deg \gcd(Q_n(t), Q_n(t+1))$. Moreover, the binomial coefficients $\binom{m}{k}$ are easily computed modulo 2. Certainly, $\binom{m}{k} = 1$ if, writing m and k in binary, every time we have a 1 at a position for k, then we also have a 1 at the same position for m. Otherwise $\binom{m}{k} = 0$.

Here it goes a list of the polynomialds $R_n(t) = \gcd(P_n(t), P_n(t+1))$ for $n \leq 57$

R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}	R_{13}	R_{14}
1	1	1	$(1+t+t^2)^2$	$t(1+t)$	1	1	1	$(1+t+t^2)^4$	1	$t^3(1+t)^3$	1	1	$(1+t+t^2)^2$

R_{15}	R_{16}	R_{17}	R_{18}	R_{19}	R_{20}	R_{21}	R_{22}	R_{23}	R_{24}	R_{25}	R_{26}	R_{27}	R_{28}
1	$(1+t+t^4)^2$	$t(1+t)$	1	$(1+t+t^2)^8$	1	1	1	$t^7(1+t)^7$	$(1+t+t^2)^2$	1	1	1	1

R_{29}	R_{30}	R_{31}	R_{32}
$t(1+t)(1+t+t^2)^4$	$(1+t^3+t^5)^2(1+t^2+t^3+t^4+t^5)^2$	1	$(1+t+t^2+t^3+t^5)^2(1+t+t^3+t^4+t^5)^2$

R_{33}	R_{34}	R_{35}	R_{36}	R_{37}	R_{38}	R_{39}	R_{40}	R_{41}	R_{42}	R_{43}	R_{44}
$(1+t+t^4)^4$	$(1+t+t^2)^2$	$t^3(1+t)^3$	1	1	1	$(1+t+t^2)^{16}$	1	$t(1+t)$	1	1	$(1+t+t^2)^2$

R_{45}	R_{46}	R_{47}	R_{48}	R_{49}	R_{50}	R_{51}	R_{52}	R_{53}	R_{54}	R_{55}	R_{56}	R_{57}
1	1	$t^{15}(1+t)^{15}$	1	$(1+t+t^2)^4$	$(1+t+t^4)^2$	1	1	$t(1+t)$	$(1+t+t^2)^2$	1	1	1

These polynomials are factored into irreducible polynomials in $\mathbb{F}_2[t]$. We see there are clear patterns for the repetition of each irreducible factor. Actually this is so, as we show next.

First, let us recall some basic facts on irreducible polynomials in $\mathbb{F}_2[t]$. If $F(t)$ is an irreducible polynomial of degree α, then $\mathbb{F}_2[t]/(F)$ is a field of order 2^α, hence isomorphic to $\mathbb{F}_{2^\alpha}$. In $\mathbb{F}_{2^\alpha}$, all elements satisfy $\xi^{2^\alpha} - \xi = 0$. Hence $F(t)|(t^{2^\alpha} - t)$. Therefore all irreducible polynomials of degree α appear as irreducible factors of

$$V_\alpha(t) = t^{2^\alpha} - t.$$

This gives an easy an effective way of finding them all recursively. Note that if $\beta|\alpha$ then $V_\beta | V_\alpha$. So $W_\alpha(t)$ for the product of all irreducible polynomials of degree α, then $V_\alpha = \prod_{\beta|\alpha} W_\beta$. Note that $W_1(t) = t(t-1) = t^2 - 1$. If $\varphi(\alpha)$ is the degree of W_α, the $\sum_{\beta|\alpha} \varphi(\beta) = 2^\alpha$. This can be solved with the Möbius inversion formula

$$\varphi(\alpha) = \sum_{d|\alpha} \mu(d) 2^{\alpha/d}$$

where $\mu(d) = 1$ if d is square-free and has an even number of prime factors, $\mu(d) = -1$ if d is square-free and has an odd number of prime factors and $\mu(d) = 0$ if d is divisible by a square. Note that the number of irreducible polynomials of degree α is $N_\alpha = \varphi(\alpha)/\alpha$. Here there is a short list of the first few irreducible polynomials

$$t, t+1, t^2+t+1, t^3+t+1, t^3+t^2+1, t^4+t+1, t^4+t^3+1, t^4+t^3+t^2+t+1, t^5+t^2+1,$$
$$t^5+t^3+1, t^5+t^3+t^2+t+1, t^5+t^4+t^2+t+1, t^5+t^4+t^3+t+1, t^5+t^4+t^3+t^2+1, \ldots$$

Consider the set of irreducible polynomials $\mathcal{I} = \bigcup \mathcal{I}_\alpha$, where $\mathcal{I}_\alpha = \{F_{\alpha,j} | 1 \leq j \leq N_\alpha\}$ are those of degree α.

If $F \in \mathcal{I}$ then there are two cases:

- If $F(t) \neq F(t+1)$, then both are irreducible polynomials. If $F(t)|R_n(t)$ then also $F(t+1)|R_n(t)$.
- If $F(t) = F(t+1)$, then $F(t)$ can appear alone as a factor of $R_n(t)$. But note that the roots of $F(t)$ come in pairs $(\lambda, \lambda+1)$. So $\deg F(t)$ is even.

Theorem 3.
- *The maximum power of $t(1+t)$ dividing R_{n-1} is $(t(1+t))^{2^l-1}$ for $n = 3\cdot 2^l \cdot (2k+1)$.*
- *Let $F = F_{\alpha,j} \in \mathcal{I}_\alpha$, $\alpha > 1$. There is an odd number $s = s_{\alpha,j} | 4^\alpha - 1$ such that $F|R_{n-1}$ if and only if $s|n$. Moreover, the maximum power of F dividing R_{n-1} is $F^{2^{l+1}}$ for $n = s \cdot 2^l \cdot (2k+1)$.*

Proof. We find easier to work with $Q_n(t)$ defined in (5). From Proposition 2, Q_n satisfy the recurrence $Q_{n+1} = tQ_n(t) + Q_{n-1}(t)$ and $Q_0(t) = 1$. From here it follows that

$$Q_{n+a} = Q_n Q_a + Q_{n-1} Q_{a-1},$$

for all $n, a \geq 1$. For $a = 1$ it is the initial recurrence. For $a+1$ it is checked as follows: $Q_{n+a+1} = Q_{n+1}Q_a + Q_nQ_{a-1} = (tQ_n + Q_{n-1})Q_a + Q_nQ_{a-1} = Q_n(tQ_a + Q_{a-1}) + Q_{n-1}Q_a = Q_nQ_{a+1} + Q_{n-1}Q_a$. As a consequence,

$$\begin{cases} Q_{2n} = Q_n^2 + Q_{n-1}^2 = (Q_n + Q_{n-1})^2 \\ Q_{2n+1} = Q_{n+1}Q_n + Q_nQ_{n-1} = tQ_n^2 \end{cases}$$

Now let us prove the statement of the theorem.

(1) First, an easy consequence is that Q_{2n} is not divisible by t and Q_{2n+1} is divisible by t.
(2) Q_n and Q_{n+1} are coprime for all $n \geq 0$.
(3) In the second place, an easy induction shows that for $2n = 2^l(2k+1)$, we have $Q_{2n-1} = t^{2^l-1}(1 + \ldots)$. Equivalently, $2^l || 2n \iff t^{2^l-1} || Q_{2n-1}$ (where $||$ means the maximum power dividing a polynomial). This is clear for $l = 1$, since in this case n is odd and $Q_{n-1} = 1 + \ldots$, so $Q_{2n-1} = tQ_{n-1}^2 = t(1 + \ldots)$. For $l \geq 2$, Then $2^l || 2n \iff 2^{l-1} || n$, and n is even, $n = 2t$ say. So $t^{2^{l-1}-1} || Q_{n-1}$ which is equivalent to $t(t^{2^{l-1}-1})^2 = t^{2^l-1} || tQ_{n-1}^2 = Q_{2n-1}$.
(4) Let $F(t)$ be an irreducible polynomial (not equal to t). Then $F | Q_{n-1} \iff F^2 | Q_{2n-1}$. As $F | R_{n-1} \iff F(t) | Q_{n-1}, F(t+1) | Q_{n-1}$, we have that $F | R_{n-1} \iff F^2 | R_{2n-1}$. Therefore if $F^p || R_{n-1}$ for n odd, then $F^{2^l p} || R_{2^l n-1}$ (later we shall see that $p = 2$).
(5) Suppose $F | Q_{a-1}$, $F | Q_{b-1}$. Then $F | Q_{a+b-1}$. This follows from the formula $Q_{a+b-1} = Q_{b-1}Q_a + Q_{b-2}Q_{a-1}$. Note that if $F | Q_{a+b-1}$ and $F | Q_{a-1}$ then $F | Q_{b-1}$, since $F \not| Q_a$ (by (2)). Therefore $\{a; F | Q_{a-1}\}$ is an ideal intersected by $\mathbb{Z}_{>0}$. Let s_F be its generator.
(6) By (4), s_F is odd. Let $p > 0$ be the integer such that $F^p || Q_{s_F-1}$. Then $F^p | Q_{ks_F-1}$, for any $k \geq 1$. Moreover $F^{2p} | Q_{2s_F-1}$, so $F^{2p} | Q_{2ks_F-1}$ for any $k \geq 1$. Using $Q_{(2k+1)s_F-1} = Q_{2ks_F-1}Q_{s_F} + Q_{2ks_F-2}Q_{s_F-1}$, we have that F^p is the maximum power dividing $Q_{(2k+1)s_F-1}$ for any $k \geq 0$. Therefore $F^{2^l p} || Q_{2^l(2k+1)s_F-1}$.
(7) Applying (6) to $F = 1+t$, note that $Q_2 = 1 + t^2 = (1+t)^2$. So $s_F = 3$. We know that Q_{n-1} is divisible by t only for even n, so $t(1+t) | Q_{n-1}$ for n multiple of 6. Let $n = 2^l 6(2k+1)$. Then $(1+t)^{2^{l+1}} || Q_{n-1}$ and $t^{2^{l+1}-1} || Q_{n-1}$. So $(t(1+t))^{2^{l+1}-1} || Q_{n-1}$.
(8) Now let $F\mathcal{I}_\alpha$ with $\alpha > 1$. It only remains to see that $p = 2$. By an explicit computation,

$$\begin{aligned} Q_{2^\alpha-2} &= 1 + t^{2^{\alpha-1}} + t^{2^{\alpha-1}+2^{\alpha-2}} + \ldots + t^{2^{\alpha-1}+\ldots+2} \\ Q_{2^\alpha-1} &= t^{2^\alpha-1} \\ Q_{2^\alpha} &= 1 + t^{2^{\alpha-1}} + t^{2^{\alpha-1}+2^{\alpha-2}} + \ldots + t^{2^{\alpha-1}+\ldots+2} + t^{2^\alpha} \end{aligned}$$

and $t^2 Q_{2^\alpha-2}Q_{2^\alpha} = t^{4^\alpha} + t^2 = (t^{2^\alpha} + t)^2$.

An irreducible polynomial F of degree α satisfies that $F^2 || (t^{2^\alpha} + t)^2$. Therefore $F^2 || Q_{2^\alpha-2}Q_{2^\alpha}$. But also Q_n and Q_{n-2} cannot share an irreducible factor different from t, so either $F^2 || Q_{2^\alpha-2}$ or $F^2 || Q_{2^\alpha}$. In the first case $s_F | 2^\alpha - 1$ and $p = 2$; in the second case $s_F | 2^\alpha + 1$ and $p = 2$.
(9) Finally, $F^2 || R_{n-1}$ for n odd, if and only if $F(t)^2 || Q_{n-1}(t)$ and $F(t+1)^2 || Q_{n-1}(t)$. Let $G(t) = F(t+1)$. If $G = F$ then the statement follows taking $s_{\alpha,j} = s_F$, $F = F_{\alpha,j}$. If $G \neq F$, then consider s_F, s_G. There are several possibilities: If $F^2, G^2 || Q_{2^\alpha-2}$, then $s_F, s_G | 2^\alpha - 1$; then $s_{\alpha,j} = \gcd(s_F, s_G)$. If $F^2, G^2 || Q_{2^\alpha}$, then $s_F, s_G | 2^\alpha + 1$; then $s_{\alpha,j} = \operatorname{lcm}(s_F, s_G)$. If $F^2 || Q_{2^\alpha-2}$ and $G^2 || Q_{2^\alpha}$, then $s_{\alpha,j} = s_F s_G$, since $s_F | 2^\alpha - 1$, $s_G | 2^\alpha + 1$, and $2^\alpha - 1$, $2^\alpha + 1$ are coprime. In all cases $s_{\alpha,j} | 4^\alpha - 1$.

□

We rewrite Theorem 3 as follows. Consider the generating function $D(x) = \sum_{n \geq 0} d_n x^n$. Define

$$S(x) = x + 2x^2 + x^3 + 4x^4 + x^5 + 2x^6 + x^7 + 8x^8 + x^9 + \ldots = \sum_{n \geq 0} \frac{2^n x^{2^n}}{1 - x^{2^{n+1}}}.$$

Then

$$D(x) = x \left(4S(x^6) - 2\frac{x^6}{1 - x^6} + \sum_{\alpha > 1, 1 \leq j \leq N_\alpha} 2\alpha S(x^{s_{\alpha,j}}) \right).$$

The remaining information is the numbers $s_{\alpha,j}$ associated to each irreducible polynomial $F_{\alpha,j}$ with $\alpha > 1$. These are odd numbers and we know that $s_{\alpha,j} | 4^\alpha - 1$. Therefore an easy way to find them is by looking at the first divisor n of $4^\alpha - 1$ such that $F(t), F(t+1)$ both divide $Q_{n-1}(t)$. There is even a more efficient method: consider the divisors of either $2^\alpha - 1$, $2^\alpha + 1$, and look for s_F, s_G independently. Then $s_{\alpha,j} = \mathrm{lcm}(s_F, s_G)$. A Mathematica notebook for doing this is provided here.

```
P[n_, t_]:=Factor[Sum[Binomial[n - k, k]t^(n - 2k), {k, 0, Floor[n/2]}], Modulus → 2]

Irreducibles = {t^2 + t + 1, t^3 + t + 1, t^3 + t^2 + 1, t^4 + t + 1, t^4 + t^3 + 1, t^4 + t^3 + t^2 + t + 1, t^5 + t^2 + 1,

t^5 + t^3 + 1, t^5 + t^3 + t^2 + t + 1, t^5 + t^4 + t^2 + t + 1, t^5 + t^4 + t^3 + t + 1, t^5 + t^4 + t^3 + t^2 + 1};

Irreducibles2 = PolynomialLCM[Irreducibles/.t → t + 1, 1, Modulus → 2];

NN = Length[Irreducibles];

F[n_]:=Extract[Irreducibles, {n}]

G[n_]:=Extract[Irreducibles2, {n}]

Div[n_]:=Flatten[{Divisors[2^Exponent[F[n], t] - 1], Divisors[2^Exponent[F[n], t] + 1]}]

EF[n_, k_]:=Exponent[PolynomialGCD[P[n, t], F[k], Modulus → 2], t]

EG[n_, k_]:=Exponent[PolynomialGCD[P[n, t], G[k], Modulus → 2], t]

k = 1; While[k < NN + 1, z = 2; While[EF[Extract[Div[k], z] - 1, k]==0, z++]; w = z; z = 2;

While[EG[Extract[Div[k], z] - 1, k] == 0, z++]; Print[F[k], “,”, LCM[Extract[Div[k], w], Extract[Div[k], z]]]; k++]
```

The behaviour of $s_{\alpha,j}$ is very erratic as this sample shows:

$F_{\alpha,j}(t)$	$s_{\alpha,j}$
$1+t+t^2$	5
$1+t+t^3$	63
$1+t^2+t^3$	63
$1+t+t^4$	17
$1+t^3+t^4$	255
$1+t^2+t^5$	341
$1+t^3+t^5$	31
$1+t+t^2+t^3+t^5$	33
$\vdots$	$\vdots$

$\vdots$	$\vdots$
$1+t^2+t^3+t^5+t^9$	262143
$1+t+t^4+t^5+t^9$	513
$1+t+t^3+t^6+t^9$	171
$1+t^3+t^4+t^6+t^9$	511
$1+t+t^2+t^3+t^4+t^6+t^9$	513
$1+t^2+t^5+t^6+t^9$	511
$1+t^3+t^5+t^6+t^9$	37449
$1+t+t^2+t^3+t^5+t^6+t^9$	29127
$\vdots$	$\vdots$

Remark 4. The $(n \times n)$-grid $V = \mathbb{F}_2^{n^2}$ has an action of the dihedral group D_8, and the map (1) is D_8-equivariant. If we can determine $\ker f_n$ as D_8-representation, then we could analyse the number of solutions of the Lights Out game up to rotation and symmetry, thereby recovering the sequence in [11].

Acknowledgements. I am very grateful to M. Alekseyev, J. Scherphuis, K. Sutner and G. Navarro for very useful comments, references and encouragement.

References

[1] M. Anderson y T. Fell, Turning Lights Out with Linear Algebra, *Mathematics Magazine* **71** (1998), 300–303.

[2] R. Barua y S. Ramakrishnan, σ-game, σ^+-game and two-dimensional automata additive cellular *Theor. Computer Sci.* **154** (1996), 349–366.

[3] H. Eriksson, K. Eriksson y J. Sjöstrand, Note on the Lamp Lighting Problem, *Advances Applied Math.* **27** (2001), 357–366.

[4] R. Fleischer y J. Yu, A Survey of the Game “Lights Out!”, *Lecture Notes in Computer Science* **8066** (2013), 176–198.

[5] J. Goldwasser, W. Klostermeyer y H. Ware, Fibonacci polynomials and parity domination in grid graphs, *Graphs and Combinatorics* **18** (2002), 271–283.

[6] J. Goldwasser, W. Klostermeyer y G. Trapp, Characterizing switch-setting problems, *Linear and Multilinear Algebra* **43** (1997), 121–136.
[7] M. Hunziker, A. Machiavelo y J. Park, Chebyshev polynomials over finite fields and reversibility of σ-automata on square grids, *Theor. Computer Sci.* **320** (2004), 465–483.
[8] O. Martín-Sánchez, Two reflected analyses of lights out, *Mathematics Magazine* **74** (2001), 295–304.
[9] Mathworld, `http://mathworld.wolfram.com/LightsOutPuzzle.html`
[10] N.J.A. Sloane, Sequence A075462, *The On-Line Encyclopedia of Integer Sequences*, `http://oeis.org/A075462`
[11] N.J.A. Sloane, Sequence A075463, *The On-Line Encyclopedia of Integer Sequences*, `http://oeis.org/A075463`
[12] J. Scherphuis, The Mathematics of Lights Out, `http://www.jaapsch.net/puzzles/lomath.htm`
[13] K. Sutner, Linear Cellular Automata and the Garden-of-Eden, *Math. Intelligencer* **11** (1989), 49–53.
[14] K. Sutner, σ-Automata and Chebyshev-polynomials, *Theor. Computer Sci.* **230** (2000) 49–73.
[15] Wikipedia, `http://en.wikipedia.org/wiki/Lights_Out_%28game%29`
[16] H. Ware, Divisibility properties of Fibonacci polynomials over $GF(2)$, MSc. Thesis, West Virginia University, 1997

Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, Plaza de Ciencias 3, 28040 Madrid, Spain

E-mail address: `vicente.munoz@mat.ucm.es`