Resolution to Sutner's Conjecture

William Boyles*

June 20, 2022

1 Introduction

Consider a game played on a simple graph $G = (V, E)$ where each vertex consists of a clickable light. Clicking any vertex v toggles on on/off state of v and its neighbors. One wins the game by finding a sequence of clicks that turns off all the lights. When G is a 5×5 grid, this game was commercially available from Tiger Electronics as *Lights Out*.

Sutner was one of the first to study these games mathematically. He showed that for any G the initial configuration of all lights on is solvable [3]. He also found that when $d(G) = \dim(\ker(A + I))$ over the field $\mathbb{Z}_2$, where A is the adjacency matrix of G, is 0 all initial configurations are solvable. In particular, 1 out of every $2^{d(G)}$ initial configurations are solvable, while each solvable configuration has $2^{d(G)}$ distinct solutions [3]. When investigating $n \times n$ grid graphs, Sutner conjectured the following relationship:

$$\begin{aligned} d_{2n+1} &= 2d_n + \delta_n,\ \delta_n \in \{0, 2\} \\ \delta_{2n+1} &= \delta_n, \end{aligned}$$

where $d_n = d(G)$ for G an $n \times n$ grid graph [3].

We resolve this conjecture in the affirmative. We use results from Sutner that give the nullity of a $n \times n$ board as the GCD of two polynomials in the ring $\mathbb{Z}_2[x]$ [4]. We then apply identities from Hunziker, Machiavelo, and Park that relate the polynomials $(2n + 1) \times (2n + 1)$ grids and $n \times n$ grids [2]. We then apply a result from Ore about the GCD of two products [6]. Together, these results allow us to prove Sutner's conjecture. We then go further and show for exactly which values of n δ_n is 0 or 2.

2 Preliminary Results

Sutner showed how to calculate d_n as the degree of the GCD of two polynomials in $\mathbb{Z}_2[x]$ [4].

Theorem 1 (Sutner). *Let $f_n(x)$ be the polynomial in the ring $\mathbb{Z}_2[x]$ defined recursively by*

$$f_n(x) = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ x f_{n-1}(x) + f_{n-2}(x) & \textit{otherwise} \end{cases}.$$

Then for all $n \in \mathbb{N}$.

$$d_n = \deg \gcd(f_{n+1}(x), f_{n+1}(x + 1)).$$

*Department of Mathematics, North Carolina State University, Raleigh, NC 27695 (wmboyle2@ncsu.edu)

This recursive definition gives a brute force approach to calculate $f_n(x)$. However, Hunziker, Machiavelo, and Park show the following identity that makes calculating $f_n(x)$ easier when n is divisible by powers of 2 [2].

Theorem 2 (Hunziker, Machiavelo, and Park)**.** *Let $n = b \cdot 2^k$ where b and k are non-negative integers. Then*

$$f_n(x) = x^{2^k - 1} f_b^{2^k}(x).$$

In particular, we will use this result to relate $f_{2n+2}(x)$ and $f_{4n+4}(x)$ to $f_{n+1}(x)$.

Corollary 1. *The following identities hold*

$$\begin{aligned} f_{2n+2}(x) &= x f_{n+1}^2(x) \\ f_{4n+4}(x) &= x^3 f_{n+1}^4(x). \end{aligned}$$

Proof. Notice that $2n+2 = (n+1)2^1$ and $4n+4 = (n+1)2^2$. Thus, our desired identities follow from Theorem 2. ■

Now that we have a way to express $f_{2n+2}(x)$ and $f_{4n+4}(x)$ as a product of $f_{n+1}(x)$ and a power of x, we simply need a way to express the GCD of products so we can relate d_{2n+1} and d_n. This is where a number-theoretic result from Ore comes in handy [6].

Theorem 3 (Ore)**.** *Let a, b, c, and d be integers. Let (a, b) denote* $\gcd(a, b)$*. Then*

$$(ab, cd) = (a, c)(b, d) \left(\frac{a}{(a, c)}, \frac{d}{(b, d)} \right) \left(\frac{c}{(a, c)}, \frac{b}{(b, d)} \right).$$

Ore's result deals specifically with integers. However, because both the integers and $\mathbb{Z}_2[x]$ are Euclidean domains, the result will still hold.

3 Proof of Sutner's Conjecture

Finally, we are ready to prove Sutner's conjecture [3].

Theorem 4. *For all $n \in \mathbb{N}$,*

$$d_{2n+1} = 2d_n + \delta_n,$$

where $\delta_n \in \{0, 2\}$, and $\delta_{2n+1} = \delta_n$.

Proof. Let (a, b) denote $\gcd(a, b)$. Applying the results from Theorems 1, 2, and 3,

$$\begin{aligned} d_{2n+1} &= \deg\left(f_{2n+2}(x), f_{2n+2}(x+1)\right) \\ &= \deg\left(x f_{n+1}^2(x), (x+1) f_{n+1}^2(x+1)\right) \\ &= \deg(x, x+1)\left(f_{n+1}^2(x), f_{n+1}^2(x+1)\right) \left(\frac{x+1}{(x, x+1)}, \frac{f_{n+1}^2(x)}{(f_{n+1}^2(x), f_{n+1}^2(x+1))} \right) \left(\frac{x}{(x, x+1)}, \frac{f_{n+1}^2(x+1)}{(f_{n+1}^2(x), f_{n+1}^2(x+1))} \right) \\ &= \deg\left(f_{n+1}(x), f_{n+1}(x+1)\right)^2 \left(x+1, \frac{f_{n+1}^2(x)}{(f_{n+1}(x), f_{n+1}(x+1))^2} \right) \left(x, \frac{f_{n+1}^2(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))^2} \right) \\ &= \deg\left(f_{n+1}(x), f_{n+1}(x+1)\right)^2 \left(x+1, \frac{f_{n+1}(x)}{(f_{n+1}(x), f_{n+1}(x+1))} \right) \left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))} \right) \\ &= 2d_n + \deg \left(x+1, \frac{f_{n+1}(x)}{(f_{n+1}(x), f_{n+1}(x+1))} \right) \left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))} \right). \end{aligned}$$

Notice that if we substitute $x+1$ for x,

$$\left(x+1, \frac{f_{n+1}(x)}{(f_{n+1}(x+1), f_{n+1}(x))}\right) \text{ becomes } \left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))}\right).$$

Thus, we see that these two remaining GCD terms in our expression for d_{2n+1} are either both 1 or not 1 simultaneously. This means we can further simplify to

$$d_{2n+1} = 2d_n + 2\deg\left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))}\right).$$

So, we see that

$$d_{2n+1} = 2d_n + \delta_n, \text{ where } \delta_n = 2\deg\left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))}\right).$$

Thus, $\delta_n \in \{0, 2\}$ as desired.

What remains is to show that $\delta_n = \delta_{2n+1}$. Applying Corollary 1,

$$\begin{aligned}
d_{4n+3} &= \deg\left(x^3 f_{n+1}^4(x), (x+1)^3 f_{n+1}^4(x+1)\right) \\
&= \deg\left(x^3, (x+1)^3\right)\left(f_{n+1}^4(x), f_{n+1}^4(x+1)\right)\left(x^3, \frac{f_{n+1}^4(x+1)}{(f_{n+1}^4(x), f_{n+1}^4(x+1))}\right)\left((x+1)^3, \frac{f_{n+1}^4(x)}{(f_{n+1}^4(x), f_{n+1}^4(x+1))}\right) \\
&= \deg\left(f_{n+1}(x), f_{n+1}(x+1)\right)^4\left(x^3, \frac{f_{n+1}^4(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))^4}\right)\left((x+1)^3, \frac{f_{n+1}^4(x)}{(f_{n+1}(x), f_{n+1}(x+1))^4}\right) \\
&= \deg\left(f_{n+1}(x), f_{n+1}(x+1)\right)^4\left(x^3, \frac{f_{n+1}^3(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))^3}\right)\left((x+1)^3, \frac{f_{n+1}^3(x)}{(f_{n+1}(x), f_{n+1}(x+1))^3}\right) \\
&= \deg\left(f_{n+1}(x), f_{n+1}(x+1)\right)^4\left(x, \frac{f_{n+1}(x+1)}{(f_{n+1}(x), f_{n+1}(x+1))}\right)^3\left((x+1), \frac{f_{n+1}(x)}{(f_{n+1}(x), f_{n+1}(x+1))}\right)^3 \\
&= 4d_n + 3\delta_n.
\end{aligned}$$

Also, from our work previously in this proof,

$$\begin{aligned}
d_{4n+3} &= d_{2(2n+1)+1} \\
&= 2d_{2n+1} + \delta_{2n+1} \\
&= 2\left(2d_n + \delta_n\right) + \delta_{2n+1} \\
&= 4d_n + 2\delta_n + \delta_{2n+1}.
\end{aligned}$$

For these two expressions for d_{4n+3} to be equal, we must have $\delta_{2n+1} = \delta_n$, as desired. ■

This result seems to have been proven prior by Yamagishi [5]. However, Yamagishi does not mention the connection to Sutner's conjecture, and the proof provided is not as direct as the one we provide.

4 Extended Results

Theorem 4 proves Sutner's conjecture as stated and even gives a formula for finding δ_n. However, this formula is somewhat messy, containing one polynomial division and two polynomial GCDs. We can improve this formula to just a modulo operation on n. First, we'll need a few lemmas establishing divisibility properties on $f_n(x)$.

Lemma 1. *The polynomial $f_n(x)$ is divisible by x if and only if n is even.*

Proof. First, we'll prove that if n is even, then $f_n(x)$ is divisible by x. We will proceed by induction. Notice that x divides $f_0(x) = 0$. Assume for some integer $k \geq 0$ that x divides $f_{2k}(x)$. Then

$$f_{2k}(x) = xg(x),$$

for some $g(x) \in \mathbb{Z}_2[x]$. Applying the recursive definition of $f_n(x)$ provided in Theorem 1,

$$\begin{aligned} f_{2k+2}(x) &= xf_{2k+1}(x) + f_{2k}(x) \\ &= x\left(f_{2k+1}(x) + g(x)\right). \end{aligned}$$

So, $f_{2k+2}(x)$ is also divisible by x.

Second, we'll prove that if n is odd, then $f_n(x)$ is not divisible by x. We will proceed by induction. Notice that x does not divide $f_1(x) = 1$. Assume for some natural number k that x does not divide $f_{2k-1}(x)$. Then

$$f_{2k-1}(x) = xg(x) + 1,$$

for some $g(x) \in \mathbb{Z}_2[x]$. Applying the recursive definition of $f_n(x)$ provided in Theorem 1,

$$\begin{aligned} f_{2k+1}(x) &= xf_{2k}(x) + f_{2k-1}(x) \\ &= x\left(f_{2k}(x) + g(x)\right) + 1. \end{aligned}$$

So, $f_{2k+1}(x)$ is also not divisible by x. ■

Corollary 2. *The polynomial $f_n(x+1)$ is divisible by $x+1$ if and only if n is even.*

Proof. Substitute $x+1$ for x in Lemma 1 to obtain the desired result. ■

Lemma 2. *The polynomial $f_n(x)$ is divisible by $x+1$ if and only if n is divisible by 3.*

Proof. First, we'll prove that if n is divisible by 3, then $x+1$ divides $f_n(x)$. We will proceed by induction. Notice that $x+1$ divides $f_0(x) = 0$. Assume for some integer $k \geq 0$ that $x+1$ divides $f_{3k}(x)$. Then

$$f_{3k}(x) = (x+1)g(x),$$

for some $g(x) \in \mathbb{Z}_2[x]$. Applying the recursive definition of $f_n(x)$ provided in Theorem 1,

$$\begin{aligned} f_{3k+3}(x) &= xf_{3k+2}(x) + f_{3k+1}(x) \\ &= x\left(xf_{3k+1}(x) + f_{3k}(x)\right) + f_{3k+1}(x) \\ &= (x^2+1)f_{3k+1}(x) + xf_{3k}(x) \\ &= (x+1)^2 f_{3k+1}(x) + x(x+1)g(x) \\ &= (x+1)\left((x+1)f_{3k+1} + xg(x)\right). \end{aligned}$$

So, $f_{3k+3}(x)$ is also divisible by $x+1$.

Next, we'll prove that if n is not divisible by 3, then $x+1$ does not divide $f_n(x)$. We will proceed by induction. Notice that $x+1$ neither divides $f_1(x) = 1$ nor $f_2(x) = x$. Assume for some integer $k \geq 0$ that $x+1$ does not divide $f_{3k+1}(x)$. Then

$$f_{3k+1}(x) = (x+1)g_1(x) + 1,$$

for some $g_1(x) \in \mathbb{Z}_2[x]$. Applying the recursive definition of $f_n(x)$ provided in Theorem 1,

$$f_{3k+2}(x) = xf_{3k+1}(x) + f_{3k}(x).$$

By our work earlier in this proof, we know that $x+1$ divides $f_{3k}(x)$. Thus,

$$f_{3k}(x) = (x+1)g_2(x),$$

for some $g_1(x) \in \mathbb{Z}_2[x]$. So,

$$\begin{aligned} f_{3k+2}(x) &= x\left((x+1)g_1(x)+1\right) + (x+1)g_2(x) \\ &= x(x+1)g_1(x) + x + (x+1)g_2(x) \\ &= (x+1)\left(xg_1(x) + g_2(x) + 1\right) + 1. \end{aligned}$$

So, f_{3k+2} is also not divisible by $x+1$.

Now assume that for some integer $k \geq 1$ that $x+1$ does not divide $f_{3k-1}(x)$. Thus,

$$f_{3k-1}(x) = (x+1)g_3(x) + 1,$$

for some $g_3(x) \in \mathbb{Z}_2[x]$. Applying the recursive definition of $f_n(x)$ provided in Theorem 1 and our work previously in this proof,

$$\begin{aligned} f_{3k+1}(x) &= xf_{3k}(x) + f_{3k-1}(x) \\ &= x(x+1)g_2(x) + (x+1)g_3(x) + 1 \\ &= (x+1)\left(xg_2(x) + g_3(x)\right) + 1. \end{aligned}$$

So, $f_{3k+1}(x)$ is also not divisible by $x+1$. ■

Corollary 3. *The polynomial $f_n(x+1)$ is divisible by x if and only if n is divisible by 3.*

Proof. Substitute x for $x+1$ in Lemma 2 to obtain the desired result. ■

Now with these divisibility properties about $f_n(x)$, we can state and prove a much simpler way to find when δ_n is 0 or 2.

Theorem 5. *The value of δ_n is 2 if and only if $n+1$ is divisible by 3.*

Proof. From our work in Theorem 4, we know that

$$\delta_n = 2\deg\left(x+1, \frac{f_{n+1}(x)}{(f_{n+1}(x), f_{n+1}(x+1))}\right).$$

So we see that δ_n is 2 exactly when $f_{n+1}(x)$ can be divided without remainder by $x+1$ more times than $f_{n+1}(x+1)$.

For $n+1$ is not divisible by 3, Lemma 2 tells us that $f_{n+1}(x)$ is not divisible by $x+1$. So in this case, $\delta_n = 0$, as desired.

For $n+1$ divisible by 3, let $n+1 = b \cdot 2^k$ for some integers $b, k \geq 0$ where b is odd. Notice that since $n+1$ is divisible by 3, b must also be divisible by 3. Applying Corollary 1,

$$f_{n+1}(x) = x^{2^k-1}f_b^{2^k}(x) \text{ and } f_{n+1}(x+1) = (x+1)^{2^k-1}f_b^{2^k}(x+1).$$

Since b is an odd multiple of 3, Lemma 2 and Corollary 2 tell us that $x+1$ divides $f_b(x)$, but $x+1$ does not divide $f_b(x+1)$. So,

$$f_{n+1}(x) = x^{2^k-1}(x+1)^{2^k}g^{2^k}(x) \text{ and } f_{n+1}(x+1) = (x+1)^{2^k-1}x^{2^k}g^{2^k}(x+1),$$

for some $g(x) \in \mathbb{Z}_2[x]$, where $g(x)$ and $g(x+1)$ are both divisible by neither x nor $x+1$. So, we see that $f_{n+1}(x)$ can be divided without remainder by $x+1$ one more time than $f_{n+1}(x+1)$. So, $\delta_n = 2$, as desired. ■

5 Future Work

There are many other relationships with d_n, some of which are yet to be proven. For example, Sutner mentions that for all $k \in \mathbb{N}$, $d_{2^k-1} = 0$ [3]. We believe that the following relationships hold, but are unaware of a proof.

Conjecture 1. *There are infinitely many n such that $d_n = 2$. In particular, for all $k \in \mathbb{N}$, $d_{2\cdot 3^k-1} = 2$.*

This conjecture is similar to Sutner's result that shows there are infinitely many n such that $d_n = 0$.

Conjecture 2. *Let a be an odd natural number. If a is not divisible by 21, then for all $k \in \mathbb{N}$,*

$$d_{a^k-1} = d_{a-1}.$$

Goshima and Yamagishi conjectured a similar statement on tori instead of grids and for a prime [1].

Theorem 6. *The case of $a = 3$ for Conjecture 2 and 1 are equivalent.*

Proof. For $a = 3$, Conjecture 2 says that for all $k \in \mathbb{N}$,

$$d_{3^k-1} = d_{3-1} = 0.$$

Since 3^k is divisible by 3, Theorem 5 tells us that $\delta_{3^k-1} = 2$. So, applying Theorem 4,

$$d_{2\cdot 3^k-1} = 2d_{3^k-1} + \delta_{3^k-1} = 2,$$

exactly what Conjecture 1 states. Apply all the same results in reverse to shows that Conjecture 2 implies 1. ■

References

[1] Masato Goshima and Masakazu Yamagishi, *On the dimension of the space of harmonic functions on a discrete torus*, Experimental Mathematics **19** (2010), no. 4, 421–429.

[2] Markus Hunziker, António Machiavelo, and Jihun Park, *Chebyshev polynomials over finite fields and reversibility of σ-automata on square grids*, Theoretical Computer Science **320** (2004), no. 2, 465–483.

[3] Klaus Sutner, *Linear cellular automata and the Garden-of-Eden*, The Mathematical Intelligencer **11** (1989), no. 2, 49–53.

[4] ———, *sigma-automata and chebyshev-polynomials*, Theoretical Computer Science **230** (1996), 49–73.

[5] Masakazu Yamagishi, *Periodic harmonic functions on lattices and chebyshev polynomials*, Linear Algebra and its Applications **476** (2015), 1–15.

[6] Øystein Ore, *Number theory and its history*, p. 109, McGraw-Hill, 1948, Section 5-4, Problem 2.