Resolution to Sutner's Conjecture

William Boyles*

June 23, 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 Fibonacci Polynomials

Sutner showed how to calculate d_n as the degree of the GCD of two polynomials in $\mathbb{Z}_2[x]$ [4]. In this section, we will establish some divisibility properties of these polynomials.

Theorem 2.1 (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)

These polynomials f are often referred to as Fibonacci polynomial because when defined over the reals, evaluating $f_n(x)$ at $x = 1$ gives the nth Fibonacci number.

The recursive definition given in Theorem 2.1 provides 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 2.2 (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 2.2.1. *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 2.2. ∎

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

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

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

Hunziker, Machiavelo, and Park also showed the following identity [2].

Theorem 2.4 (Hunziker, Machiavelo, and Park)**.** *A polynomial $\tau(x)$ in $\mathbb{Z}_2[x]$ divides both $f_n(x)$ and $f_m(x)$ if and only if it divides $f_{\gcd(m,n)}$. In particular,*

$$\gcd(f_m(x), f_n(x)) = f_{\gcd(m,n)}(x).$$

We specifically will use the following corollary:

Corollary 2.4.1. *For some polynomial $\tau(x)$ in $\mathbb{Z}_2[x]$, let $n \geq 0$ be the smallest integer such that $\tau(x)$ divides $f_n(x)$. Then for all $m \geq 0$, $tau(x)$ divides $f_m(x)$ if and only if n divides m.*

Proof. Let $\tau(x)$ be some polynomial in $\mathbb{Z}_2[x]$. Let $f_n(x)$ be the smallest Fibonacci polynomial such that $\tau(x)$ divides $f_n(x)$.

Assume that $\tau(x)$ divides $f_m(x)$ for some number m. Then $\tau(x)$ is a common factor of $f_m(x)$ and $f_n(x)$, so Theorem 2.4 tells us that $\tau(x)$ divides $f_{\gcd(m,n)}(x)$. Since $f_n(x)$ is the smallest Fibonacci polynomial that is divisible by $\tau(x)$,

$$\gcd(m, n) \geq n.$$

This inequality only holds if $\gcd(m, n) = n$. Thus, m must be a multiple of n as desired.

Now assume that m is a multiple of n. Then $\gcd(m,n)=n$. Theorem 2.4 tells us

$$\gcd(f_m(x), f_n(x)) = f_{\gcd(m,n)}(x) = f_n(x).$$

Since $\tau(x)$ divides $f_n(x)$, and $f_n(x)$ is the GCD of $f_m(x)$ and $f_n(x)$, $\tau(x)$ must also divide $f_m(x)$, as desired. ■

In particular, we will use the following instances of Corollary 2.4.1 to determine when δ_n is 0 or 2.

Corollary 2.4.2. *The following are true:*

(i) x *divides* $f_n(x)$ *if and only if* $n \equiv 0 \mod 2$.

(ii) $x+1$ *divides* $f_n(x+1)$ *if and only if* $n \equiv 0 \mod 2$.

(iii) $x+1$ *divides* $f_n(x)$ *if and only if* $n \equiv 0 \mod 3$.

(iv) x *divides* $f_n(x+1)$ *if and only if* $n \equiv 0 \mod 3$.

Proof. Notice,

(i) We find that $f_2(x) = x$ is the smallest Fibonacci polynomial divisible by x, so we apply Corollary 2.4.1 to get the desired result.

(ii) Follows from (i) by substituting $x+1$ for x.

(iii) We find that $f_3(x) = (x+1)^2$ is the smallest Fibonacci polynomial divisible by $x+1$, so we apply Corollary 2.4.1 to get the desired result.

(iv) Follows from (iii) by substituting $x+1$ for x.

■

3 Proof of Sutner's Conjecture

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

Theorem 3.1. *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 2.1, 2.2, and 2.3,

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

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 2.2.1,

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

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 3.1 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. We'll do so by using the divisibility properties established in Corollary 2.4.2.

Theorem 4.1. *The value of δ_n is 2 if and only if $n+1$ is divisible by 3.*

Proof. From our work in Theorem 3.1, 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, Corollary 2.4.2 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 2.2.1,

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

Since b is an odd multiple of 3, Corollary 2.4.2 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 5.1. *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 5.2. *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 5.1. *The case of $a = 3$ for Conjecture 5.2 and 5.1 are equivalent.*

Proof. For $a = 3$, Conjecture 5.2 says that for all $k \in \mathbb{N}$,

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

Since 3^k is divisible by 3, Theorem 4.1 tells us that $\delta_{3^k-1} = 2$. So, applying Theorem 3.1,

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

exactly what Conjecture 5.1 states. One can apply all same steps in reverse to shows that Conjecture 5.1 implies the $a = 3$ case of Conjecture 5.2. ∎

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.