Resolution to Sutner's Conjecture

William Boyles*

February 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 Electronic 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 [2]. He also found that when $d(G) = \dim(\ker(A + I))$ over the field $GF(2)$, 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 [2]. 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 [2].

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 $\mathbb{Z}_2[x]$ [3]. We then apply identities from Hunziker, Machiavelo, and Park that relate the polynomials $(2n + 1) \times (2n + 1)$ grids and $n \times n$ grids [1]. Finally, we use a result from Ore about the GCD of two products [4]. Together, these results allow us to prove Sutner's conjecture and describe exactly when 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 $\mathbb{Z}_2[x]$ [3].

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

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

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

$$d_n = \deg \gcd(f_n(x), f_n(x + 1)).$$

*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 can make calculating certain $f_n(x)$ easier [1].

Theorem 2 (Hunziker, Machiavelo, and Park)**.** *Let $n = b \cdot 2^{k-1} - 1$ where $b, k \in \mathbb{N}$. Then*

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

In particular, we will use this result to relate $f_{2n+1}(x)$ and $f_{4n+3}(x)$ to $f_n(x)$.

Corollary 1. *The following identities hold*

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

Proof. Notice that $2n+1 = (n+1)2^{2-1} - 1$ and $4n+3 = (n+1)2^{3-1} - 1$. Thus, our desired identities follow from Theorem 2. ■

Now that we have a way to express $f_{2n+1}(x)$ and $f_{4n+3}(x)$ as a product of $f_n(x)$ and a power of x, we simply need a way to express the GCD of products so we can calculate d_n. This is where a number-theoretic result from Ore comes in handy [4].

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 [2].

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,

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

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

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

Thus, we see that these two remaining GCD terms are either both 1 nor not 1 simultaneously. This means we can further simplify to

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

So, we see that

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

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

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

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

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. ■

4 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 $n \in \mathbb{N}$, $d_{2^n-1} = 0$ [2]. 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 $k \in \mathbb{N}$, $d_{3\cdot 2^k-1} = 2$.*

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 $k \in \mathbb{N}$,*

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

References

[1] 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.

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

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

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