Resolution to Sutner's Conjecture

William Boyles

February 6, 2022

1 Introduction

We resolve a conjecture first stated by Sutner in 1989 about the relationship between the nullity of *Lights Out* boards of size n and $2n+1$ in the affirmative [2]. We use results from Sutner that give the nullity of a $n \times n$ board as the GCD of two polynomials in $\mathbb{Z}_2[x]$ [3]. We then apply identities from Hunziker, Machiavelo, and Park that relate these polynomials for $(2n+1) \times (2n+1)$ boards to those for $n \times n$ boards [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 provide conditions under which each case occurs.

2 Preliminary Results

Let $d(n)$ be the nullity of an $n \times n$ *Lights Out* board. Sutner showed how to calculate $d(n)$ as the degree of the GCD of two polynomials [3].

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

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

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

$$d(n) = \deg \gcd \left(f_n(x), f_n(x+1)\right).$$

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*

$$f_{2n+1}(x) = xf_n^2(x)$$
$$f_{4n+3}(x) = x^3 f_n^4(x).$$

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 state and prove Sutner's conjecture [2].

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

$$d(2n+1) = 2d(n) + \delta_n,$$

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

Next, we'll calculate δ_{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, 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 $\delta_{2n+1} = \delta_n$. ■

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), 200–0.

[4] Øystein Ore, *Number theory and its history*, McGraw-Hill, 1948.