The Rank Deficiency of Certain Sized *Lights Out* Boards

William Boyles

August 22, 2021

1 Intro Conjectures

Let $f(n,x)$ be the Chebyshev polynomial over $GF(2)$ that we defined previously. Recall that the rank deficiency of an $n \times n$ *Lights Out* board, $d(n)$, is the degree of $\gcd(f(n,x), f(n,x+1))$. Let $g : \mathbb{N} \to \mathbb{N}$ where $g(k) = 2^{k+1} + 2^{k-1} - 1$.

Conjecture 1. *Let $k \in \mathbb{N}$. Then*

$$f(g(k),x) = x^{2^{k-1}-1}\left(x^{2^{k+1}} + x^{2^k} + 1\right).$$

Proof. Recall how we determine the coefficients of $f(n,x)$ using the parity of binomial coefficients. First, we need to find a value $K = 2^k - 1$ where k is the smallest integer $K \geq n$. Second, we find $S = (K - n)$. Finally, we find that the ith coefficient is 1 if and only if $\binom{2i+S}{S+i}$ is odd. Equivalently, it's 1 if and only if $i \;\texttt{\&}\; S+i$ is zero.
$K = 2^{k+2} - 1$ for $g(k) = 2^{k+1} + 2^{k-1} - 1$. So,

$$\begin{aligned} S &= 2(K - g(k)) \\ &= 2\left((2^{k+2} - 1) - (2^{k+1} + 2^{k-1} - 1)\right) \\ &= 2\left(2^{k+2} - 2^{k+1} - 2^{k-1}\right) \\ &= 2\left(8 \cdot 2^{k-1} - 4 \cdot 2^{k-1} - 2^{k-1}\right) \\ &= 2\left(3 \cdot 2^{k-1}\right) \\ &= 3 \cdot 2^k. \end{aligned}$$

In binary this is $S = 11\underbrace{0\ldots0}_{k}$.

Let's think about what happens when we do $i \;\texttt{\&}\; S+i$ for various values of i.

- In $i = 0$, we see that the left side of the `&` is 0, so the entire result is 0. Therefore, the leading coefficient is a 1, as desired.
- In $i = 1 \ldots 2^k - 1$, the trailing k 0's in S will match whatever is in i's binary representation in $S+i$. So, the result of the `&` will be nonzero. Therefore, there will be $2^k - 1$ 0 coefficients following the leading 1, as desired.
- In $i = 2^k$, $S + i = 100\underbrace{0\ldots0}_{k}$. So, the `&` will result in a 0, meaning we get a coefficient of 1, as desired.
- In $i = 2^k + 1 \ldots 2^{k+1} - 1$, we see a combination of the previous two cases. We can write $i = 2^k + j$, where $1 \leq j \leq 2^k - 1$. As we saw in the previous case, $S + 2^k = 100\underbrace{0\ldots0}_{k}$ in binary. As in two cases

ago, the trailing k 0's in $S + 2^k$ will match whatever is in j's binary representation in $S + 2^k + j$. So, the result of the `&` operation will be nonzero. Therefore, the second 1 coefficient will be followed by $2^k - 1$ 0 coefficients, as desired.

- In $i = 2^{k+1}$, $S + i = 101\underbrace{0\ldots0}_{k}$. Since i does not have a 2^k or a 2^{k+2} in its binary representation, i `&` $S+i$ `==` 0. So, we get a coefficient of 1, as desired.
- In $i = 2^{k+1} + 1 \ldots 2^{k+1} + 2^{k-1} - 1$, we again see a combination of previous cases. We can write $i = 2^{k+1} + j$, where $1 \leq j \leq 2^{k-1} - 1$. As we saw in the previous case, $S + 2^{k+1} = 101\underbrace{0\ldots0}_{k}$. As in two cases ago, the trailing k 0's in $S + 2^{k+1}$ will match whatever is in j's binary representation in $S + 2^{k+1} + j$. So, the result of the `&` operation will be nonzero. Therefore, the third 1 coefficient will be floowed by $2^{k-1} - 1$ 0 coefficients, as desired.

$\square$

Conjecture 2. *Let $k \in \mathbb{N}$. Then*

$$f(g(k), x+1) = \left(x^{2^{k+1}} + x^{2^k} + 1\right)\left(x^{2^{k-1}-1} + \cdots + 1\right).$$

2 Main Result

The following relies on conjecture 1 and conjecture 2 being true.

Theorem 1. *Let $k \in \mathbb{N}$. Then*

$$\gcd\left(f(g(k), x), f(g(k), x+1)\right) = x^{2^{k+1}} + x^{2^k} + 1.$$

Proof. We can see from conjectures 1 and 2 that the desired gcd is a common factor of both polynomials. So, we just need to show that over $GF(2)$ that the remaining factors of both polynomials have no common factors. This result is easily verified by a computer.

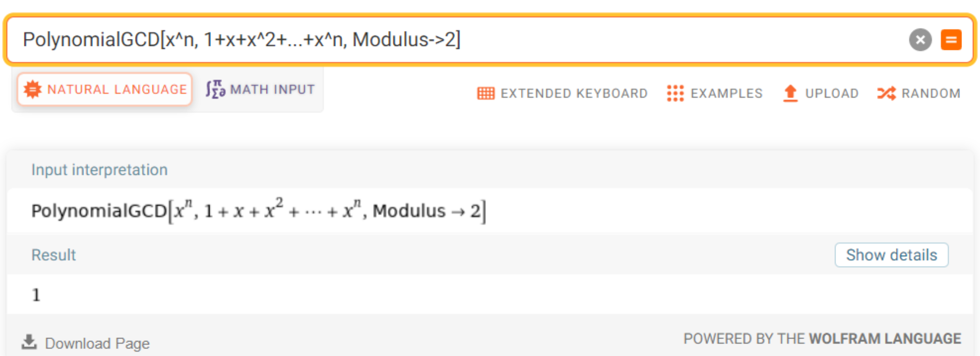

Figure 1: Wolfram|Alpha: PolynomialGCD[$x^n, 1 + x + x^2 + ... + x^n$, Modulus→2]

$\square$

Corollary 1. *A Lights Out board of size $g(k) \times g(k)$ will have nullity 2^{k+1}.*

3 Concluding Conjectures

Conjecture 3. *Let* $h : \mathbb{N} \to \mathbb{N}$ *where*

$$h(n) = \max\{g(m) \mid m \in \mathbb{N}, g(m) \leq n\}.$$

Then for all $n \in \mathbb{N}$*,*

$$\max\{d(m) \mid 1 \leq m \leq n\} = d(h(n)).$$

Corollary 2. $d(n) = n$ *only for* $n = 4$*. Otherwise,* $d(n) < n$*.*

Proof. Observe that $d(1) = d(2) = d(3) = 0$, and $d(g(1)) = d(4) = 4$.

Assume for contradiction that there exists some $n > 4$ such that $d(n) \geq n$.
Notice that for $k > 1$,

$$d(g(k)) = 2^{k+1} < g(k) = 2^{k+1} + 2^{k-1} - 1.$$

So,

$$d(h(n)) < h(n) \leq n = d(n).$$

However,

$$\max\{d(m) \mid 1 \leq m \leq n\} = d(n) > d(h(n)),$$

which contradicts conjecture 3. $\square$