

The Rank Deficiency of Certain Sized *Lights Out* Boards

William Boyles

October 10, 2021

1 Intro Lemmas

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 $g : \mathbb{N} \rightarrow \mathbb{N}$ where $g(k) = 2^{k+1} + 2^{k-1} - 1$.

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

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

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 $S = 2(K - n)$. Finally, we find that the i th coefficient is 1 if and only if $\binom{2i+S}{S+i}$ is odd. Equivalently, it's 1 if and only if $i \& S + i$ is zero. $K = 2^{k+2} - 1$ for $g(k) = 2^{k+1} + 2^{k-1} - 1$. So,

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

In binary this is $S = 11\underbrace{0 \dots 0}_k$.

Let's think about what happens when we do $i \& S + i$ 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 $i = 1 \dots 2^k - 1$, 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 $i = 2^k$, $S + i = 100\underbrace{0 \dots 0}_k$. So, the $\&$ will result in a 0, meaning we get a coefficient of 1, as desired.
- In $i = 2^k + 1 \dots 2^{k+1} - 1$, 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, $S + 2^k = 100\underbrace{0 \dots 0}_k$ 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 $i = 2^{k+1}$, $S + i = 101\underbrace{0\dots 0}_k$. 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 $i = 2^{k+1} + 1\dots 2^{k+1} + 2^{k-1} - 1$, 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, $S + 2^{k+1} = 101\underbrace{0\dots 0}_k$. 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 flowed by $2^{k-1} - 1$ 0 coefficients, as desired.

□

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

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

Proof. In lemma 1, we showed that

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

Substituting $x+1$ for x and using mod 2 arithmetic (i.e. $(a+b)^c = a^c + b^c$ where c is a power of 2; $1 = -1$),

$$\begin{aligned} f(g(x), x+1) &= \left((x+1)^{2^{k-1}-1}\right) \left((x+1)^{2^{k+1}} + (x+1)^{2^k} + 1\right) \\ &= \left(x^{2^{k-1}} + 1\right) \frac{1}{x+1} \left(x^{2^{k+1}} + 1 + x^{2^k} + 1 + 1\right) \\ &= \left(x^{2^{k+1}} + x^{2^k} + 1\right) \frac{x^{2^{k-1}} - 1}{x - 1} \\ &= \left(x^{2^{k+1}} + x^{2^k} + 1\right) \left(x^{2^{k-1}-1} + x^{2^{k-1}-2} + \dots + 1\right). \end{aligned}$$

□

2 Main Result

Now that we have lemmas 1 and 2, we can prove our main result.

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

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

Proof. We can see from lemmas 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.

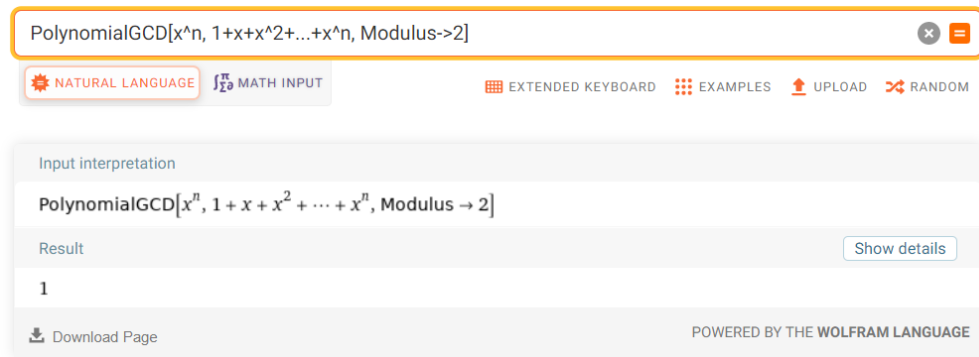


Figure 1: Wolfram|Alpha: $\text{PolynomialGCD}[x^n, 1 + x + x^2 + \dots + x^n, \text{Modulus} \rightarrow 2]$

□

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