# A Number Theoretic View on Binary Shift Registers

George Petrides*

Department of Informatics
University of Bergen
Bergen, Norway

firstname.lastname@uib.no

**Abstract**

In this paper we describe a number theoretic view on binary shift register sequences. We illustrate this approach by revisiting some known results on the pure and circulating registers which we reprove using tools from modular arithmetic.

## 1 Introduction

The motivation for this paper was the simple observation that the cycles produced by shift registers are denoted by a representative member, which very often instead of as a binary sequence, it is given by its integer value. Starting from this, we take on an alternative view on the theory of shift registers by moving away from the traditional approach of binary sequences and working entirely with the corresponding integers. After providing basic information on the necessary theory using the new approach in Sect. 2, we apply it to two well studied registers, the Pure (Sect. 3) and Complementary (Sect. 4) circulating registers, and re-obtain known results [2, 4, 6, 7, 3] using tools from modular arithmetic.

Our aim is not to pronounce the similarities and differences, or make any claims on possible advantages and disadvantages between existing approaches and the one we describe here. It is rather to provide a unified description of this number theoretic approach so it can serve as an additional tool for further studies in the domain of shift registers.

## 2 From Binary Sequences to Modular Arithmetic

Any non-singular binary shift register of order $n$ can be defined in terms of a bijective map $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ given by

$$g(s_0, \ldots, s_{n-1}) = (s_1, \ldots, s_{n-1}, s_0 \oplus F(s_1, \ldots, s_{n-1})) \ , \tag{1}$$

for some Boolean function $F : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ [2].

*This work was supported by The Research Council of Norway under project 247742/O70.

We can shift from binary tuples to modular arithmetic by considering each $k$-tuple $(s_0, \ldots, s_{k-1}) \in \mathbb{F}_2^k$ as the binary representation of the integer $\sum_{i=0}^{k-1} s_i 2^{k-1-i} \in \mathbb{Z}_{2^k}$. The corresponding functions will be $F : \mathbb{Z}_{2^{n-1}} \to \mathbb{Z}_2$ and $g : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ given by

$$g(x) = \begin{cases} 2x + F(x) \mod 2^n & \text{if } x < 2^{n-1} \\ 2x + 1 - F(x - 2^{n-1}) \mod 2^n & \text{if } x \geq 2^{n-1} \end{cases} . \tag{2}$$

Rewriting (2) in terms of the *support* of $F$, namely the set $\mathcal{D} \subseteq \mathbb{Z}_{2^{n-1}}$ such that $x \in \mathcal{D}$ if and only if $F(x) = 1$, we obtain

$$g_{n,\mathcal{D}}(x) = \begin{cases} 2x + 1 \mod 2^n & \text{if } x \in \mathcal{D} \text{ or if } x \geq 2^{n-1} \text{ and } x - 2^{n-1} \notin \mathcal{D} \\ 2x \mod 2^n & \text{otherwise} \end{cases} . \tag{3}$$

We can also define the *complemetary* map of $g_{n,\mathcal{D}}$ as $\overline{g}_{n,\mathcal{D}} = g_{n,\mathbb{Z}_{2^{n-1}} \setminus \mathcal{D}}$.

**Example 1.** Two basic, yet important maps are $g_{n,\emptyset}$, called the *Pure Circulating Register* of order $n$ ($PCR_n$), and its complementary map $g_{n,\mathbb{Z}_{2^{n-1}}}$, called the *Complementary Circulating Register* of order $n$ ($CCR_n$). For brevity we will be respectively denoting them by $g_{p_n}$and $g_{c_n}$. They are given by

$$g_{p_n}(x) = \begin{cases} 2x \mod 2^n & \text{if } x < 2^{n-1} \\ 2x + 1 \mod 2^n & \text{if } x \geq 2^{n-1} \end{cases} = \overline{g}_{c_n}(x) \tag{4}$$

and

$$g_{c_n}(x) = \begin{cases} 2x + 1 \mod 2^n & \text{if } x < 2^{n-1} \\ 2x \mod 2^n & \text{if } x \geq 2^{n-1} \end{cases} = \overline{g}_{p_n}(x) . \tag{5}$$

The *weight* of $x \in \mathbb{Z}_{2^n}$, denoted by $wt(x)$, is the number of ones in its binary representation. By Eqn. (1) we can deduce that $wt(x) - 1 \leq wt(g_{n,\mathcal{D}}(x)) \leq wt(x) + 1$.

**Example 2.** For any $x \in \mathbb{Z}_{2^n}$, $PCR_n$ simply cyclically shifts the binary representation of $x$ and therefore $wt(g_{p_n}(x)) = wt(x)$. $CCR_n$, however, also complements the last bit after the cyclic shift, hence the weights differ by one: $wt(g_{c_n}(x)) = wt(x) + 1$ if $x < 2^{n-1}$ and $wt(g_{c_n}(x)) = wt(x) - 1$ otherwise.

For each $x \in \mathbb{Z}_{2^n}$, the smallest $i \in \mathbb{Z}$ such that $x = g_{n,\mathcal{D}}^i(x)$ is called its *period with respect to* $g_{n,\mathcal{D}}$ and denoted by $p_{g_{n,\mathcal{D}}}(x)$, where $g_{n,\mathcal{D}}^i$ denotes the composition of $g_{n,\mathcal{D}}$ with itself $i$ times. Each map $g_{n,\mathcal{D}}$ partitions $\mathbb{Z}_{2^n}$ into *cycles*. We say $x_1, x_2 \in \mathbb{Z}_{2^n}$ belong to the same cycle if and only if $x_2 = g_{n,\mathcal{D}}^i(x_1)$ for some $i$ such that $1 \leq i < p_{g_{n,\mathcal{D}}}(x_1)$. We shall denote each cycle by $C_t$ where $t$ is its member with the smallest integer value. The number of elements in a cycle is called its *length* and is equal to the period of each of them. In case there is a single cycle we call it a *maximal length* or *full* or *de Bruijn* cycle. Mykkeltveit [5] proved the conjecture of Golomb [2] that no more than $Z(n) = \frac{1}{n} \sum_{d|n} \phi(d) 2^{n/d}$ cycles can be obtained from any map $g_{n,\mathcal{D}}$, where $\phi$ is Euler's Totient function.

**Example 3.** The 8 cycles from $PCR_5$ are $C_0 = \{0\}$, $C_1 = \{1,2,4,8,16\}$, $C_3 = \{3,6,12,24,17\}$, $C_5 = \{5,10,20,9,18\}$, $C_7 = \{7,14,28,25,19\}$, $C_{11} = \{11,22,13,26,21\}$, $C_{15} = \{15,30,29,27,23\}$, and $C_{31} = \{31\}$. The 4 cycles from $CCR_5$ are $C_0 = \{0,1,3,7,15,31,30,28,24,16\}$, $C_2 = \{2,5,11,23,14,29,26,20,8,17\}$, $C_4 = \{4,9,19,6,13,27,22,12,25,18\}$, and $C_{10} = \{10,21\}$.

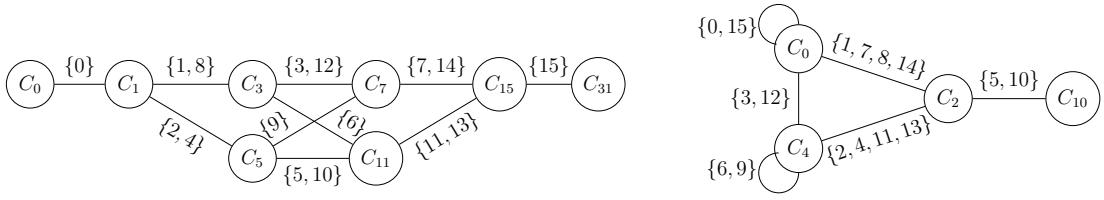


Figure 1: The adjacency graph for $PCR_5$ (left) and $CCR_5$ (right).

The adjacency graph of a map $g_{n,\mathcal{D}}$ is the undirected connected graph with vertices the map's cycles, and for each $x \in \mathbb{Z}_{2^{n-1}}$ an edge labelled $x$ between the cycle containing $x$ and the cycle containing $\overline{g}_{n,\mathcal{D}}(x)$. An edge from a cycle to itself is called *intracyclic*, and *extracyclic* otherwise. For brevity, we represent multiple edges between two cycles by a single edge labelled by the set of the corresponding labels that we call the *adjacency set*.

**Example 4.** The adjacency graphs for $PCR_5$ and $CCR_5$ are given in Fig. 1.

Two distinct $x_1, x_2 \in \mathbb{Z}_{2^{n-1}}$ belong to the same adjacency set of a map $g_{n,\mathcal{D}}$ if either

A. $x_1$ and $x_2$ belong to the same cycle and $\overline{g}_{n,\mathcal{D}}(x_1)$ and $\overline{g}_{n,\mathcal{D}}(x_2)$ belong to the same cycle, in which case we shall call $x_1$ and $x_2$ an *intracyclic pair*, or

B. $x_1$ and $\overline{g}_{n,\mathcal{D}}(x_2)$ belong to the same cycle and $x_2$ and $\overline{g}_{n,\mathcal{D}}(x_1)$ belong to the same cycle, in which case we shall cal $x_1$ and $x_2$ an *extracyclic pair*.

**Example 5.** An intracyclic pair in $PCR_5$ are 2 and 4 which are on $C_1$ while $g_{c_n}(2) = 5$ and $g_{c_n}(4) = 9$ are on $C_5$. An extracyclic pair in $CCR_5$ are 5 and 10 since 5 and $g_{p_n}(10) = 20$ are on $C_2$, and $g_{p_n}(5) = 10$.

The two conditions for intracyclic pairs can be expressed formally as ($a_1$) $x_2 = g^i_{n,\mathcal{D}}(x_1)$ and ($a_2$) $\overline{g}_{n,\mathcal{D}}(x_1) = g^j_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(x_2))$, for some $i, j$ such that $1 \le i < p_1$ and $1 \le j < p_2$, where $p_1 = p_{g_{n,\mathcal{D}}}(x_1)$ and $p_2 = p_{g_{n,\mathcal{D}}}(\overline{g}_{n,\mathcal{D}}(x_1))$. Together they imply

$$\overline{g}_{n,\mathcal{D}}(x_1) = g^j_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(g^i_{n,\mathcal{D}}(x_1))) \ . \tag{6}$$

*Remark* 6. Conditions ($a_1$) and ($a_2$) are equivalent to $x_1 = g^{p_1-i}_{n,\mathcal{D}}(x_2)$ and $\overline{g}_{n,\mathcal{D}}(x_2) = g^{p_2-j}_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(x_1))$. Hence, if one member of an intracyclic pair satisfies (6) with the pair of exponents $(i, j)$, the other member satisfies it with the pair of exponents $(p_1 - i, p_2 - j)$.

Similarly, the extracyclic pair conditions can be expressed as ($b_1$) $x_1 = g^i_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(x_2))$ and ($b_2$) $x_2 = g^j_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(x_1))$, for some $i, j$ such that $1 \le i < p_1$ and $1 \le j < p_2$, where $p_1$ and $p_2$ are as above. Together they imply

$$x_1 = g^i_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(g^j_{n,\mathcal{D}}(\overline{g}_{n,\mathcal{D}}(x_1)))) \ . \tag{7}$$

The study of adjacency sets provides guidelines for joining and splitting cycles from a map $g_{n,\mathcal{D}}$. Adding an element of an adjacency set to $\mathcal{D}$ if it does not exist, or removing it if it does, affects the cycles connected by the edge it labels. If the edge is extracyclic then the two cycles sharing it merge into a single cycle, otherwise the corresponding cycle splits into two cycles. By joining all cycles, we obtain a de Bruijn cycle.

# 3 PCR

## 3.1 Cycle Structure

Since $g_{p_n}(2^n-1) = 2^n-1$, cycle $C_{2^n-1}$ is of length 1. For any $x \in \mathbb{Z}_{2^n} \setminus \{2^n-1\}$, (4) can be expressed as

$$g_{p_n}(x) = 2x \mod 2^n - 1 \ . \tag{8}$$

The length of the cycle containing $x \in \mathbb{Z}_{2^n} \setminus \{2^n-1\}$ is equal to the period $p_{g_{p_n}}(x)$, the smallest positive exponent $i$ such that $2^i x \equiv x \mod 2^n-1$, or equivalently

$$2^i \equiv 1 \mod \frac{2^n-1}{\gcd(x, 2^n-1)} \ . \tag{9}$$

It follows that when $x$ is coprime to $2^n-1$, the length of the cycle containing it is equal to $n$, the maximum possible. Therefore, there are at least $\frac{\phi(2^n-1)}{n}$ cycles of length $n$.

**Proposition 7.** *The length of any cycle in $PCR_n$ divides $n$.*

*Proof.* Suppose a cycle in $PCR_n$ has length $k$ not dividing $n$, in which case $n = ak+b$ for positive integers $a$ and $b < k$. For every element $x$ in the cycle we have $g^n_{p_n}(x) = 2^n x \equiv x \mod 2^n-1$, where $2^n x = 2^{ak+b}x = 2^b 2^{ak} x \equiv 2^b x \mod 2^n-1$ since $2^k x \equiv x \mod 2^n-1$. Thus $2^b x \equiv x \mod 2^n-1$, a contradiction on the minimality of $k$. □

Let $\zeta(k,n)$ denote the number of cycles of length $k$ in $PCR_n$. Clearly, $\sum_{k=1}^{n} k\,\zeta(k,n) = |\mathbb{Z}_{2^n}| = 2^n$. This number is in fact equal to the number of binary Lyndon words and irreducible polynomials of degree $k$ over $\mathbb{Z}_2$ [1, 8].

**Proposition 8.**

$$\zeta(k,n) \ = \ \begin{cases} \dfrac{1}{k}\displaystyle\sum_{d|k} \mu(d) 2^{k/d} & \text{if } k \mid n \\ 0 & \text{otherwise} \end{cases} \ ,$$

*where $\mu$ is the Möbius function.*

*Proof.* By Prop. 7, $k$ must divide $n$. It follows that $\sum_{d|n} d\,\zeta(d,n) = 2^n$ and by Möbius inversion we obtain $\zeta(k,n) = \frac{1}{k}\sum_{d|k}\mu(d)2^{k/d}$ for any divisor $k$ of $n$, as required. □

Golomb [2] proved that $PCR_n$ partitions $\mathbb{Z}_{2^n}$ into exactly $Z(n)$ cycles. Summing $\zeta(k,n)$ over all divisors of $n$, an alternative formula can be obtained.

**Corollary 9** ([8])**.** *The number of cycles in $PCR_n$ is*

$$Z(n) = \sum_{d|n} \frac{1}{d} \sum_{d'|d} \mu(d') 2^{d/d'} \ .$$

### 3.2 Adjacency Sets

We begin with the fact that no intracyclic edge exists in $PCR_n$ as it would require an $x \in \mathbb{Z}^{n-1}$ to be on the same cycle as $g_{c_n}(x)$, which as seen in Example 2 is impossible due to unequal weights [3].

A similar contradiction with respect to weights asserts that no extracyclic pairs exist either: On one hand, since $x_2 < 2^{n-1}$, $g_{c_n}(x_2)$ being on the same cycle as $x_1$ implies $wt(x_1) = wt(g_{c_n}(x_2)) = wt(x_2) + 1$. On the other hand, since $x_1 < 2^{n-1}$, $g_{c_n}(x_1)$ being on the same cycle as $x_2$ implies $wt(x_2) = wt(g_{c_n}(x_1)) = wt(x_1) + 1$.

Regarding intracyclic pairs, 0 and $2^n - 1$ which have period 1, and $2^{n-1} - 1$ for which $g_{c_n}(2^{n-1}-1) = 2^n - 1 \in C_{2^n-1}$, need not be considered. For any $x \in \mathbb{Z}_{2^{n-1}} \setminus \{2^{n-1}-1\}$, (5) can be expressed as

$$g_{c_n}(x) = 2x + 1 \mod 2^n - 1 \ . \tag{10}$$

Using (8) and (10), and rearranging, (6) for $PCR_n$ becomes

$$-2(2^{i+j} - 1)x_1 \equiv 2^j - 1 \mod 2^n - 1 \ , \tag{11}$$

for some $i, j$ such that $1 \leq i < p_{g_{p_n}}(x_1)$ and $1 \leq j < p_{g_{p_n}}(2x_1 + 1)$. In fact, Lemma 10 below asserts that $1 \leq i, j \leq n - 1$.

We note that we must have $i + j \neq n$, otherwise the LHS of (11) would be congruent to 0, leading to a contradiction as the RHS can never be congruent to 0. Then, the congruence is solvable if and only if $\gcd(2^{i+j} - 1, 2^n - 1) = 2^{\gcd(n,i+j)} - 1$ divides $2^j - 1$, which implies $\gcd(n, i + j)$ divides $j$.

**Lemma 10.** *In $PCR_n$, intracyclic pairs label edges between cycles of length $n$ only.*

*Proof.* Let $x_1$ and $x_2$ be an intracyclic pair in $PCR_n$, and denote the length of the cycle containing them by $p_1$, and that of the cycle containing $2x_1 + 1$ and $2x_2 + 1$ by $p_2$. To prove the lemma it suffices to show the equality of periods $p_1 = p_2 = n$.

First, multiplying both sides of (11) by $2^{p_1}$, using that $2^{p_1}x_1 = x_1$ and applying (11) on the LHS, and rearranging, we obtain

$$2^{p_1} + 2^j \equiv 2^{p_1+j} + 1 \mod 2^n - 1 \ . \tag{12}$$

We must have that each of the summands on the LHS is congruent to a distinct summand on the RHS modulo $2^n - 1$. Such pairwise congruences are equivalent to pairwise congruences in the exponents modulo $n$. The range of $j$ implies $j \not\equiv 0 \mod n$, hence the only possibility left is $p_1 \equiv 0 \mod n$ giving $p_1 = n$ as required.

Next, we multiply both sides of (11) by $2^{p_2}$. On the LHS we have

$$\begin{aligned} -(2^{i+j} - 1)2^{p_2}(2x_1 + 1 - 1) &\equiv -(2^{i+j} - 1)(2x_1 + 1 - 2^{p_2}) \\ &\equiv 2^j - 1 + (2^{i+j} - 1)(2^{p_2} - 1) \mod 2^n - 1 \ , \end{aligned}$$

where in the second step we used $2^{p_2}(2x_1+1) = (2x_1+1)$, and in the third we applied (11). Combining this with the RHS and rearranging, we obtain

$$2^{p_2+i+j} + 2^j \equiv 2^{p_2+j} + 2^{i+j} \mod 2^n - 1 \ . \tag{13}$$

Working as above, and since $i \not\equiv 0 \mod n$, we are left with $p_2 = n$ as required. □

Magleby [4] and Fredricksen (as acknowledged in [3]) proved in different ways that the adjacency sets in $PCR_n$ have size at most 2. The number of adjacency sets of this maximal size was determined in [6, 7] and later on in [3], each using a different method. We provide an alternative proof for both of these results.

**Lemma 11.** *All intracyclic pairs in $PCR_n$ are disjoint.*

*Proof.* Suppose on the contrary that there exist two non-disjoint intracyclic pairs in $PCR_n$, say $x_1$ with $x_2$ and $x_1$ with $x_3$. Apart from the exponent pair $(i, j)$ that connects $x_1$ and $x_2$ as above and yields (11), there exists an exponent pair $(i', j')$, $1 \leq i', j' \leq n-1$, connecting $x_1$ and $x_3$ and yielding

$$-2(2^{i'+j'}-1)x_1 \equiv 2^{j'}-1 \mod 2^n-1 \ . \tag{14}$$

Multiplying both sides of (14) by $2^{i+j}-1$, applying (11) on the LHS and rearranging yields

$$2^{i+j+j'}+2^j+2^{i'+j'} \equiv 2^{i'+j'+j}+2^{j'}+2^{i+j} \mod 2^n-1 \ . \tag{15}$$

Considering pairwise congruences as in the proof of Lemma 10, there are three cases:

First, $i+j+j' \equiv i'+j'+j \mod n$ which implies $i \equiv i' \mod n$. Then, as $j \not\equiv i+j \mod n$, we are left with $j \equiv j' \mod n$. Given that $1 \leq i, j, i', j' \leq n-1$, we must have $i = i'$ and $j = j'$, yielding $x_2 = x_3$ and contraditicting that they are distinct.

Second, $i+j+j' \equiv j' \mod n$, implying $i+j \equiv 0 \mod n$, which is impossible as we have seen that $i+j \neq n$.

Third, $i+j+j' \equiv i+j \mod n$ implies $j' \equiv 0 \mod n$ and contradicts the range of $j'$. Since all cases lead to a contradiction, all intracyclic pairs in $PCR_n$ must be disjoint. □

**Corollary 12** ([4])**.** *The maximum size any adjacency set can have in $PCR_n$ is* 2*.*

*Proof.* Suppose on the contrary that there exists an adjacency set in $PCR_n$ containing more than two distinct elements, and consider three of them. Since no extracyclic pairs exist in $PCR_n$, pairwise these three elements form non-disjoint intracyclic pairs, in contradiction to Lemma 11. □

**Corollary 13** ([6, 7])**.** *In $PCR_n$, adjacency sets of size* 2 *label edges between cycles of length $n$ only.*

*Proof.* This is a direct consequence of Lemma 10 and Cor. 12. □

**Theorem 14** ([6, 7])**.** *In $PCR_n$, the number of adjacency sets of size* 2 *is given by*

$$p(n) = \frac{1}{2}\sum_{\substack{d|n \\ d\neq n}} \phi\left(\frac{n}{d}\right)\left(\frac{n}{d}-2\right)2^{d-1} \ .$$

*Proof.* Adjacency sets of size 2 in $PCR_n$ correspond to intracyclic pairs. Therefore, we begin by counting the number of suitable pairs of exponents $(i, j)$ that render (11) solvable. As we have seen, we must have $i+j \neq n$ and $\gcd(n, i+j)$ divides $j$. Any proper

divisor $d$ of $n$ is a possible gcd, and the possibilities for $i+j$ are integers in the interval $1 \leq i+j \leq n-1$ (due to reduction modulo $n$ in the exponents) such that $\gcd(n, i+j) = d$. There are $\phi(n/d)$ of them. The possibilities for $j$ are the multiples of $d$ excluding $i+j$ (since $i \neq 0$) in the interval $1 \leq j \leq n-1$. There are $n/d-2$ of them.

Next, for each suitable $d$, $i$ and $j$ there are $2^d-1$ possible solutions to (11) given by $x_1 = x_0 + \frac{2^n-1}{2^d-1}k$, where $k$ is an integer such that $0 \leq k \leq 2^d-2$ and

$$x_0 = -2^{-1}\left(\frac{2^{i+j}-1}{2^d-1}\right)^{-1}\left(\frac{2^j-1}{2^d-1}\right) \bmod \frac{2^n-1}{2^d-1} \ .$$

We are only interested in those solutions such that $x_1 < 2^{n-1}$. When $d=1$, there is a single solution. It is straightforward to verify that $(2^{i+j}-1)^{-1} \equiv \sum_{l=1}^{(i+j)^{-1} \bmod n} 2^{-l(i+j)} \bmod 2^n-1$. It can then be shown (details will be given in the full paper) that $x_1 \equiv \sum_{l=1}^{n-j(i+j)^{-1}} 2^{-1-l(i+j)}$. If $x_1 > 2^{n-1}$ then $2^{n-1}$ must appear as one of the summands, and we would have $-1-l(1+j) \equiv n-1 \mod n$ which is only possible if either 0 or $n$ were in the range of the sum. This however does not happen as $j(i+j)^{-1} \not\equiv 0 \mod n$.

For $d > 1$, we have $x_0 < \frac{2^n-1}{2^d-1} < 2^{n-1}$ due to the modulus, hence $k=0$ is suitable. Since $x_0$ is between 0 and the modulus, the maximum suitable value of $k$ is $k_m$ such that $k_m\left(\frac{2^n-1}{2^d-1}\right) < 2^{n-1}$ and $(k_m+1)\left(\frac{2^n-1}{2^d-1}\right) > 2^{n-1}$. After simple operations, this becomes $2^{d-1}-1-\frac{2^{n-1}-2^{d-1}}{2^n-1} \leq k_m < 2^{d-1}-\frac{2^{n-1}-2^{d-1}}{2^n-1}$. Since the fraction is less than one, $k_m = 2^{d-1}-1$. Hence, the suitable solutions are for $0 \leq k \leq 2^{d-1}-1$, which means that only $2^{d-1}$ out of the $2^d-1$ possible solutions are suitable.

Finally, putting everything together gives us the number of suitable solutions to (11). The required number of distinct intracyclic pairs is half this number, something that follows from Remark 6 and the fact that if the congruence is solvable for the pair of exponents $(i,j)$ then it is also solvable for the pair $(n-i, n-j)$. □

# 4 CCR

For any $x \in \mathbb{Z}_{2^n}$, (5) can be expresed as

$$g_{c_n}(x) = 2x+1 \mod 2^n+1 \ . \tag{16}$$

It is easy to check that for any exponent $k \in \mathbb{Z}^+$ we have

$$g_{c_n}^k(x) = 2^k(x+1)-1 \mod 2^n+1 \ . \tag{17}$$

Throughout this section we will refer to the *dyadic valuation* of positive integer $n$ which is the highest power of 2 that divides $n$. For brevity, we will denote it by $\nu(n)$ instead of the conventional $\nu_2(n)$.

## 4.1 Cycle Structure

The length of the cycle containing $x \in \mathbb{Z}_{2^n}$ is equal to the period $p_{g_{c_n}}(x)$, the smallest positive exponent $i$ such that $g_{c_n}^i(x) = x$. Using (17) this is equivalent to $2^i(x+1) \equiv x+1$

mod $2^n+1$, or

$$2^i \equiv 1 \mod \frac{2^n+1}{\gcd(x+1, 2^n+1)} \ . \tag{18}$$

It follows that when $x+1$ is coprime to $2^n+1$, the length of the cycle containing it is equal to $2n$, the maximum possible. Hence, there are at least $\frac{\phi(2^n+1)}{2n}$ cycles of length $2n$.

Hauge [3] proved that the length of each cycle is even and divides $2n$ with an odd quotient. We reformulate this as follows.

**Proposition 15.** *The length of each cycle in $CCR_n$ is even and divides $2n$ but not $n$.*

*Proof.* From Eqn. (17) we can see that $g_{c_n}^n(x) \not\equiv x \mod 2^n+1$ and $g_{c_n}^{2n}(x) \equiv x \mod 2^n+1$ for all $x \in \mathbb{Z}_{2^n}$. If a cycle had length $k$ dividing $n$, that would contradict the inequality, and if it did not divide $2n$ then we would reach a contradiction as in the proof of Prop. 7. Consequently, $k$ is even. □

Let $\zeta^*(k,n)$ denote the number of cycles of length $2k$ in $CCR_n$. Clearly, $\sum_{k=1}^{n} k\,\zeta^*(k,n) = |\mathbb{Z}_{2^n}| = 2^n$.

**Proposition 16.**

$$\zeta^*(k,n) \ = \ \begin{cases} \dfrac{1}{2^{\nu(2n)}k} \displaystyle\sum_{d|k} \mu(d) 2^{\frac{2^{\nu(n)}k}{d}} & \text{if } k \mid \frac{n}{2^{\nu(n)}} \\ 0 & \text{otherwise} \end{cases} \ .$$

*Proof.* By Prop. 15, $2k$ must divide $2n$ but not $n$. It is not difficult to check that for any integer $n$, the divisors of $2n$ that are not divisors of $n$ are of the form $2^{\nu(2n)}d$ where $d \mid \frac{n}{2^{\nu(n)}}$. It follows that $\sum_{d|\frac{n}{2^{\nu(n)}}} 2^{\nu(2n)} d\,\zeta^*(d,n) = 2^n$. Using the substitution $n' = n/2^{\nu(n)}$ in the range of the sum and the RHS, and applying Möbius inversion we obtain $\zeta^*(k,n) = \frac{1}{2^{\nu(2n)}k} \sum_{d|k} \mu(d) 2^{\frac{2^{\nu(n)}k}{d}}$ for any divisor $k$ of $n/2^{\nu(n)}$, as required. □

Golomb [2] states that in $CCR_n$ there are $Z^*(n) = \frac{1}{2}Z(n) - \frac{1}{2n}\sum_{2d|n} \phi(2d) 2^{n/2d}$ cycles. We can provide an alternative formula by summing $\zeta^*(k,n)$ over all divisors of $n/2^{\nu(n)}$.

**Corollary 17.** *The number of cycles in $CCR_n$ is*

$$Z^*(n) = \frac{1}{2^{\nu(2n)}} \sum_{d|\frac{n}{2^{\nu(n)}}} \frac{1}{d} \sum_{d'|d} \mu(d') 2^{\frac{2^{\nu(n)}d}{d'}} \ .$$

### 4.2 Adjacency Sets

Both intra- and extracyclic pairs exist in $CCR_n$. Before we begin with intracyclic ones, note that for any $x \in \mathbb{Z}_{2^n-1}$, (4) can be expressed as

$$g_{p_n}(x) = 2x \mod 2^n+1 \ . \tag{19}$$

Using (16), (17) and (19), and rearranging, (6) for $CCR_n$ becomes

$$2(2^{i+j}-1)(x_1+1) \equiv 2^j - 1 \mod 2^n+1 \ , \tag{20}$$

for some $i, j$ such that $1 \leq i < p_{g_{c_n}}(x_1)$ and $1 \leq j < p_{g_{c_n}}(2x_1+1)$. In fact, Lemma 18 below asserts that $1 \leq i, j \leq 2n-1$.

We note that we must have $i+j \neq 2n$, otherwise the LHS of the congruence would be congruent to 0, leading to a contradiction as the RHS can never be congruent to 0. Then, the congruence is solvable if and only if $\gcd(2^{i+j}-1, 2^n+1)$ divides $2^j-1$. We have

$$\gcd(2^{i+j}-1, 2^n+1) = \begin{cases} 2^{\gcd(i+j,n)}+1 & \text{if } \nu(i+j) > \nu(n) \\ 1 & \text{otherwise} \end{cases} .$$

Thus, when $\nu(i+j) \leq \nu(n)$ the congruence is always solvable. It turns out (details to follow in the full paper) that to have $x_1, x_2 < 2^{n-1}$ as required, we must have that both $i$ and $j$ are odd and $\gcd(i+j, n) = 2$.

Next consider $\nu(i+j) > \nu(n)$, in which case $\nu(\gcd(i+j,n)) = \nu(n)$. We must have that $2^{\gcd(i+j,n)}+1$ divides $2^j-1$ which implies

$$2^{\gcd(i+j,n)}+1 \ = \gcd(2^j-1, 2^{\gcd(i+j,n)}+1) = \begin{cases} 2^{\gcd(j,\gcd(i+j,n))}+1 & \text{if } \nu(j) > \nu(n) \\ 1 & \text{otherwise} \end{cases} .$$

Since $2^{\gcd(i+j,n)}+1$ cannot be equal to 1, the only possibility is to have $\nu(j) > \nu(n)$ in which case $\gcd(i+j, n) = \gcd(j, \gcd(i+j, n))$ implying that $\gcd(i+j, n)$ divides $j$.

**Lemma 18.** *In $CCR_n$, intracyclic pairs label edges between cycles of length $2n$ only.*

*Proof.* The proof is very similar to that of Lemma 10, the equivalent result for $PCR_n$. The result for $p_1$ we obtain following the same steps as in the case for $PCR_n$, only this time we have $2^{p_1}(x_1+1) = x_1+1$, and we need to work modulo $2n$ in the exponents.

For $p_2$, the LHS of (20) after multiplication by $2^{p_2}$ becomes

$$\begin{aligned} -(2^{i+j}-1)2^{p_2}(2x_1+1+1) &\equiv -(2^{i+j}-1)(2x_1+1+2^{p_2}+1-1) \\ &\equiv 2^j - 1 + (2^{i+j}-1)(2^{p_2}-1) \mod 2^n+1 \ , \end{aligned}$$

where in the second step we used $2^{p_2}(2x_1+1) = (2x_1+1)$, and in the third we applied (20). The rest is also identical to the $PCR_n$ case, again working modulo $2n$ in the exponents instead of $n$. □

**Lemma 19.** *All intracyclic pairs in $CCR_n$ are disjoint.*

*Proof.* The proof is almost identical to that of Lemma 11, the equivalent result for $PCR_n$. The only difference is that due to the modulus being $2^n+1$ instead of $2^n-1$, here we need to work modulo $2n$ instead of $n$ in the exponents. All other arguments are the same. □

**Corollary 20** ([3])**.** *The maximum size any adjacency set can have in $CCR_n$ is 4.*

*Proof.* Suppose on the contrary that there exists an adjacency set in $CCR_n$ containing more than four distinct elements, and consider five of them. Since extracyclic pairs exist in $CCR_n$, these five elements can belong to two different cycles, one of which must contain at least three of them. But then, these three elements will pairwise form non-disjoint intracyclic pairs, in contradiction to Lemma 19. □

**Corollary 21** ([3])**.** *In $CCR_n$, adjacency sets of size 4 label edges between cycles of length $2n$ only.*

*Proof.* This is a direct consequence of Lemma 18 and Cor. 20. □

Next, we consider extracyclic pairs. Using (16), (17) and (19), and rearranging, (7) for $CCR_n$ becomes

$$(2^{i+j+2}-1)(x_1+1) \equiv 2^i(2^{j+1}+1) \mod 2^n+1 \ . \tag{21}$$

First, we note that when $i=j=n-1$, both sides of the congruence become 0, meaning that any $x_1 \in \mathbb{Z}_{2^{n-1}}$ is a solution. Using $i=n-1$ and once again (16), (17) and (19), Condition ($b_1$) for $CCR_n$ yields

$$x_1+x_2 \equiv 2^{n-1}-1 \mod 2^n+1 \ . \tag{22}$$

This means that for each $x$ in an adjacency set, $2^{n-1}-1-x$, which is always distinct, also belongs to the same adjacency set. In other words, every adjacency set has even cardinality, as first noticed by Hauge [3]. Let intracyclic pairs $x_1, x_2$ and $x_3, x_4$ belong to the same adjacency set. Suppose $x_3 = 2^{n-1}-1-x_1$ satisfies (20) for some exponent pair $(i', j')$. Straightforward simplifications yield

$$-2(2^{i'+j'}-1)(x_1+1) \equiv 2^{j'}-2^{i'+j'} \mod 2^n+1 \ . \tag{23}$$

Multiplying both sides of this congruence by $2^{i+j}-1$, applying (20) on the LHS, and rearranging we obtain

$$2^{i+j+i'+j'}+2^j+2^{j'} \equiv 2^{i+j+j'}+2^{i'+j'+j}+1 \mod 2^n+1 \ . \tag{24}$$

Working as we have done earlier, such as in the proof of Lemma 10, we obtain $j'=2n-i$ and $i'=2n-j$. Combining this with Remark 6 we obtain that adjacency sets of size 4 are characterised by the pairs of exponents $(i,j)$, $(2n-i,2n-j)$, $(j,i)$ and $(2n-j,2n-i)$. The first two coincide with the other two when $i=j$ (since $2n-j \neq i$).

**Theorem 22** ([3])**.** *The number of adjacency sets of size 4 in $CCR_n$ is given by*

$$c(n) = \frac{1}{4}h(n)\phi(n) + \frac{1}{4}\sum_{\substack{d \mid \frac{n}{2^{\nu(n)}} \\ d \neq \frac{n}{2^{\nu(n)}}}} \phi\left(\frac{n}{2^{\nu(n)}d}\right)\left(\frac{n}{2^{\nu(n)}d}-2\right)2^{2^{\nu(n)}d-1} \ ,$$

*where $h(n)=-1$ if $n$ is odd and $h(n)=(n-2)$ if $n$ is even.*

*Proof.* We have seen that adjacency sets of size 4 in $CCR_n$ correspond to pairs of intracyclic pairs, or equivalently quadruples of the form $(x_1, x_2, 2^{n-1} - x_1 - 1, 2^{n-1} - x_2 - 1)$. We begin by counting the number of suitable pairs of exponents $(i, j)$ that render (20) solvable and the corresponding suitable solutions. Recall that there are two cases for this.

The first is when $\nu(i+j) \leq \nu(n)$, both $i$ and $j$ are odd and $\gcd(i+j, n) = 2$. Recall that the last two conditions ensure that $x_1, x_2 < 2^{n-1}$, and consequently the entire quadruple is suitable. The last condition also implies that $n$ must be even, and $\nu(i + j) = 1$. By the latter, the possibilities for $i + j$ are even integers in the interval $1 \leq i + j \leq 2n - 1$ (due to reduction modulo $2n$ in the exponents) such that $\gcd(\frac{i+j}{2}, n) = 1$. In other words, $i + j = 2k_{ij}$ for $k_{ij}$ in the interval $1 \leq k_{ij} \leq n - 1$ such that $\gcd(n, k_{ij}) = 1$. There are $\phi(n)$ of them. For each possible $i + j$, the possibilities for $i$ (and consequently $j$) are the odd integers in the interval $1 \leq i \leq 2n - 1$. There are $n$ of them.

For each suitable $i$ and $j$ there is a single solution $x_1$ to (20) given by

$$x_1 + 1 = 2^{-1} \left(2^{i+j} - 1\right)^{-1} \left(2^j - 1\right) \bmod 2^n + 1 \ .$$

Since there is a single solution and by what we have seen earlier, when $i = j$ the quadruple reduces to the pair $(x_1, x_2)$. Therefore, for each possible $i + j$ we need to exclude $\frac{i+j}{2}$ and $n + \frac{i+j}{2}$ from the possibilities for $i$. Hence the total number of solutions from this case is $(n - 2)\phi(n)$.

The second case is when $\nu(i+j) > \nu(n)$, $\nu(j) > \nu(n)$ and $\gcd(i + j, n)$ divides $j$. Since $\gcd(i + j, n) = 2^{\nu(n)} \gcd\left(\frac{i+j}{2^{\nu(i+j)}}, \frac{n}{2^{\nu(n)}}\right)$, for any divisor $d$ of $\frac{n}{2^{\nu(n)}}$, $2^{\nu(n)}d$ is a possible gcd. The possibilities for $i + j$ are integers in the interval $1 \leq i + j \leq 2n - 1$ (due to reduction modulo $2n$ in the exponents) such that $\nu(i + j) > \nu(n)$ and $\gcd\left(\frac{i+j}{2^{\nu(i+j)}}, \frac{n}{2^{\nu(n)}}\right) = d$. In other words, $i + j = 2^{\nu(n)+1}dk_{ij}$ for $k_{ij}$ in the interval $1 \leq k_{ij} \leq \frac{n}{2^{\nu(n)}d} - 1$ such that $\gcd\left(\frac{n}{2^{\nu(n)}d}, k_{ij}\right) = 1$. There are $\phi\left(\frac{n}{2^{\nu(n)}d}\right)$ of them.

The possibilities for $j$ are multiples of $2^{\nu(n)}d$ excluding $i + j$ (as $i \neq 0$) in the interval $1 \leq j \leq 2n-1$ such that $\nu(j) > \nu(n)$. In other words, $j = 2^{\nu(n)+1}dk_j$ for $k_j$ in the interval $1 \leq k_j \leq \frac{n}{2^{\nu(n)}d} - 1$ excluding $\frac{i+j}{2^{\nu(n)+1}d}$. There are $\frac{n}{2^{\nu(n)}d} - 2$ of them.

For each suitable $d$, $i$ and $j$ there are $2^d + 1$ solutions to (20) given by $x_1 = x_0 - 1 + \frac{2^n+1}{2^{\nu(n)d}+1}k$, where $k$ is an integer such that $0 \leq k \leq 2^{\nu(n)d}$ and

$$x_0 = 2^{-1} \left(\frac{2^{i+j} - 1}{2^{\nu(n)d} + 1}\right)^{-1} \left(\frac{2^j - 1}{2^{\nu(n)d} + 1}\right) \bmod \frac{2^n + 1}{2^{\nu(n)d} + 1} \ .$$

We are only interested in those solutions such that $x_1, x_2 < 2^{n-1}$. Full details on this part of the proof will be provided in the full paper.

Finally, putting everything together gives us the number of suitable solutions to (20). The number of pairs of intracyclic pairs is one fourth of this number, something that follows from our discussion just before this Theorem and the fact that if the congruence is solvable for the pair of exponents $(i, j)$ then it is also solvable for the pair $(2n - i, 2n - j)$. □

**Acknowledgements**

The author would like to thank Prof. Tor Helleseth for valuable discussions and encouragement.

## References

[1] Bernard Elspas. The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, pages 45–60, 1959.

[2] Solomon W Golomb. *Shift Register Sequences*. Aegean Park Press, 1981.

[3] Erik R Hauge. On the cycles and adjacencies in the complementary circulating register. *Discrete Mathematics*, 145:105–132, 1995.

[4] Kay B Magleby. The synthesis of nonlinear feedback shift registers. Technical Report 6207-1, Stanford Electronics Laboratory, 1963.

[5] Johannes Mykkeltveit. A proof of golomb's conjecture for the de bruijn graph. *Journal of Combinatorial Theory*, 13(1):40–45, 1972.

[6] Johannes Mykkeltveit. Generating and counting the double adjacencies in a pure circulating shift register. *IEEE Transactions on Computers*, C–24(3):299–304, 1975.

[7] Eric J Van Lantschoot. Double adjacencies between cycles of a circulating shift register. *IEEE Transactions on Computers*, C–22(10):244–955, 1973.

[8] Elbert A Walker. Non-linear recursive sequences. *Canadian Journal of Math*, 11:370–378, 1959.