AppliedMath

MDPI

Article

Rotating Binaries

Anant Gupta [1], Idriss J. Aberkane [2], Sourangshu Ghosh [3], Adrian Abold [4], Alexander Rahn [5] and Eldar Sultanow [6,7,*]

1 Georgia Institute of Technology, North Ave NW, Atlanta, GA 30332, USA; agupta886@gatech.edu
2 Unesco-Unitwin Complex Systems Digital Campus, ECCE e-Lab, CEDEX, 67081 Strasbourg, France; idriss.aberkane@polytechnique.edu
3 Department of Civil Engineering, Indian Institute of Technology Kharagpur, Kharagpur 721302, India; sourangshu@iitkgp.ac.in
4 Department of EEI, Friedrich-Alexander-Universität Erlangen-Nürnberg, Lange Gasse 20, 90403 Nuremberg, Germany; adrian.abold@fau.de
5 Faculty of Information Systems and Applied Computer Sciences (WIAI), University of Bamberg, Kapuzinerstraße 16, 96047 Bamberg, Germany; Alexander.Rahn@stud.uni-bamberg.de
6 Chair of Business Informatics, Processes and Systems, Potsdam University, Karl-Marx Straße 67, 14482 Potsdam, Germany
7 Capgemini, Bahnhofstraße 30, 90402 Nuremberg, Germany
* Correspondence: eldar.sultanow@wi.uni-potsdam.de or eldar.sultanow@capgemini.com; Tel.: +49-1514-025-1786

Abstract: This paper investigates the behavior of rotating binaries. A rotation by r digits to the left of a binary number B exhibits in particular cases the divisibility $l \mid N_1(B) \cdot r + 1$, where l is the bit-length of B and $N_1(B)$ is the Hamming weight of B, that is the number of ones in B. The integer r is called the *left-rotational distance*. We investigate the connection between this rotational distance, the length, and the Hamming weight of binary numbers. Moreover, we follow the question under which circumstances the above-mentioned divisibility is true. We have found out and will demonstrate that this divisibility occurs for $kn + c$ cycles.

Keywords: binary rotation; circular left shift; collatz cycle; randomness

Citation: Gupta, A.; Aberkane, I.J.; Ghosh, S.; Abold, A.; Rahn, A.; Sultanow, E. Rotating Binaries. *AppliedMath* **2022**, *2*, 104–117. https://doi.org/10.3390/appliedmath2010005

Received: 26 October 2021
Accepted: 10 January 2022
Published: 3 February 2022

1. Introduction

With this manuscript, we pursue the goal of exploring the connection between rotations of binary vectors and $3n + c$ cycles. Theorem 3 and its generalization in Section 9 mainly contribute to this exploration, since they narrow down the conditions for the sought divisibilities and for the cycle existences. The starting point of our research is a divisibility feature of rotated binary numbers, which has been discovered by Darrell Cox [1] and taken further, analyzed, and visualized for numerous cases using the Python programming language by Eldar Sultanow [2]. This investigation is motivated by the use case of information encryption and efficiency improvement of cryptographic algorithms, especially of those algorithms that are implemented by a linear feedback shifting register (LFSR) as demonstrated by Grosek and Hromada [3]. In the following we will develop a computational base for the binary rotation, its related cycles and generalize the divisibility feature. Definition 1 specifies the term "left-rotational distance" as follows:

Definition 1. *The left-rotational distance r of a binary number B is the number of rotations, which lead from* $B_{\min}$ *to* $B_{\max}$.

Let us take a binary number B of length l with $N_1(B)$ ones (and $N_0(B) = l - N_1(B)$ zeros), for example $l = 8$, $N_1(B) = 5$ and $B = 10110101 = 181$, the minimum that is obtainable by rotating B is $B_{\min} = 01011011 = 91$ and the maximum is $B_{\max} = 11011010 = 218$. The left-rotational distance is $r = 3$, since we obtain the maximum 11011010 by three left rotates of

the minimum 01011011. The maximum $218 = (91 \times 2^3) \bmod (255)$ can be obtained directly using Equation (1) as follows:

$$\begin{aligned} B_{\max} &= (B_{\min} \cdot 2^r) \bmod (2^l - 1) \\ B_{\min} &= (B_{\max} \cdot 2^{l-r}) \bmod (2^l - 1) \end{aligned} \tag{1}$$

Vice versa, we calculate the minimum directly as $91 = (218 \times 2^{8-3}) \bmod (255)$. Moreover, we can calculate the length l (See Sedgewick and Wayne [4], p. 185) and the Hamming weight $N_1(B)$ using $B_{\max}$ (see Weisstein [5] and Allouche and Shallit [6], p. 74) directly:

$$\begin{aligned} l &= \lfloor \log_2(B_{\max}) \rfloor + 1 \\ N_1(B) &= B_{\max} - \operatorname{gde}(B_{\max}!, 2) = B_{\max} - \textstyle\sum_{i=1}^{l-1} \lfloor B_{\max}/2^i \rfloor \end{aligned}$$

It is briefly mentioned that $\operatorname{gde}(n, 2)$ denotes the greatest dividing exponent of the base 2 with respect to a number n, which is the largest integer value of k such that $2^k \mid n$ with $2^k \leq n$, see [7].

By applying these formulas to our example, we obtain $l = \lfloor \log_2(218) \rfloor + 1 = 7 + 1 = 8$ and $N_1(B) = 218 - \operatorname{gde}(218!, 2) = 218 - (109 + 54 + 27 + 13 + 6 + 3 + 1) = 218 - 213 = 5$. The divisibility $l \mid N_1(B) \cdot r + 1$ can be written in our example as $8 \mid \left(218 - \sum_{i=1}^{7} \lfloor 218/2^i \rfloor\right) \cdot 3 + 1$. In our example the divisibility $l \mid N_1(B) \cdot r + 1$ holds, since $8 \mid 5 \times 3 + 1$ is true.

Our question is: Under which circumstances is this divisibility generally granted? The paper aims to describe the rotational behavior allowing us to unveil its connection to cycles and related concepts and to generalize the $3n + c$ cycles to $kn + c$ cycles. The approach to the question of divisibility behavior can be summarized as follows:

- Describing the rotational behavior: Starting point is the diophantine Equation (2). Showing that this diophantine equation always has solutions a, b would answer the question of whether the divisibility holds.
- Unveiling the connection between rotations, cycles, and related concepts: By introducing a boundary feature with Function (6), Halbeisen and Hungerbühler lay the foundation for this, which Cox et al. supplemented with another feature by Function (7). The cycle's existence depends on this divisibility as stated by Theorem 3.
- Generalizing from $3n + c$ to $kn + c$ cycles: With this generalization, we broaden the field to study the divisibility behavior. Section 9 makes the key contribution to this. We could generalize Theorem 3 for restricting the existence of cycles depending on the divisibility. A proof of this divisibility remains still open.

Theorems in the body of this paper, notably the referred work of Halbeisen and Hungerbühler [8] provide ways of describing the rotational behavior, but no proof of this divisibility. The diophantine Equation (2) is strongly related to this question: To prove that this divisibility holds, we need to show that there always exist integers a and b that solve the diophantine equation, which we deduce from Equation (1):

$$\left(\frac{(2^l - 1)b + B_{\max}}{B_{\min}} \right)^{N_1(B)} = 2^{a \cdot l - 1} = 2^{r \cdot N_1(B)} \tag{2}$$

In our example $a = b = 2$ provide a solution: to solve $218 = (91 \times 2^r) \bmod (2^8 - 1)$ we substitute $2^r = Y$ and solve the linear congruence $(91 \cdot Y) \equiv 218 \bmod (2^8 - 1)$, which is solvable if $\gcd(91, 2^8 - 1) \mid 218$ and there is a unique solution if 91 and the modulus $2^8 - 1$ are coprime $\gcd(91, 2^8 - 1) = 1$. This coprimality is given here. The solution is $Y \equiv 8 \bmod (255)$ and resubstitution of Y leads to $2^r \equiv 8 \bmod (255)$, which brings us to the solutions $r = 3, 11, 19, 27, \ldots$ and so on. All these r values enables us to find solutions $a = 2, 7, 12$ for $5 \cdot r = 8 \cdot a - 1$. In order that the divisibility $l \mid N_1(B) \cdot r + 1$ is given, we must show that $\gcd(B_{\min}, 2^L - 1) \mid B_{\max}$ and $2^l - 1 \mid 2^r B_{\min} - B_{\max}$.

Based on the fact that binary rotations lead to $3n + c$ cycles, Section 3 contributes as well to the question under which conditions the divisibility is granted. Although we

can illustrate and exemplify this divisibility behavior for many such cycles, we have not succeeded in providing a proof. At least we were able to identify and compile connections, limitations, and references to related/relevant concepts. The generalization of binary rotations to $kn + c$ cycles in Section 9 expands the field of the investigated divisibility behavior.

2. Fields of Application

In today's world, or rather in today's digital age, cryptographic methods have become increasingly important in order to ensure confidentiality, secrecy, and integrity of data in the presence of an adversary. Our results have the potential to contribute to existing approaches of encrypting information and moreover to provide new ways to perform encryption possibly more efficiently. Currently, LFSR is one of the main methods for cryptography (see Grosek and Hromada [3]) and they possess already an efficiency. Our idea consists in utilizing the findings given in the following sections to make LFSR's more efficient (due to lowering memory requirements) by abbreviating shifting algorithms with the Collatz method.

We reduce the amount of electrical calculation to the number of equivalence classes instead of the number of binaries 2^l, since we will see that the characteristics within such a class are constant (see in Section 7). Therefore we only have to calculate any equation once for an equivalence class and can simply shift it by an e.g., LFSR afterward. In Section 8 we will also calculate the amount of all equivalence classes for a given length l and therefore the ratio of computational power reduction.

Moreover we will generalize our given $3n + c$ cycles to $kn + c$ cycles for a more generic version of cycle representation (see in Section 9). This possesses a novelty value of our work too and provides the most practical application, such as for example the field of application for randomness. The importance of Collatz sequences for randomness has been elaborated extensively in the literature, which we want to take up briefly with the following digression. If we take any odd integer, let' say x_0 as an input for the repeatedly called function f_c (which is function (4)). We can assume that the function f is "sufficiently mixing", since $f(x)$ is called repeatedly an the output $f(x)$ becomes due to the additional variable k more and more obfuscated.

We clearly see the potential of those procedures and, furthermore, even Apple decided to submit for a patent [9] in order to use Collatz as a one-way hashing function, since the algorithms become increasingly important.

3. Binary Rotations Lead Us to $3n + c$ Cycles

Take a binary number B with a Hamming weight $N_1(B)$ as input for a function z, which Darrel Cox [1] defined as follows, where $0 \leq x_1 < x_2 < \ldots < x_{N_1(B)} \leq N_1(B) - 1$ are the positions (indexing is zero-based) in B occupied by 1:

$$z(B) = \sum_{i=1}^{N_1(B)} 3^{N_1(B)-i} 2^{x_i} \tag{3}$$

This function z is adapted from Halbeisen's and Hungerbühler's function φ, see [8]. In the introductory example $B_{\max} = 11011010$ we have $z(B_{\max}) = z(11011010) = 319$ and the five positions in our binary number $B_{\max}$ that are occupied by 1 are $(x_1, x_2, x_3, x_4, x_5) = (0, 1, 3, 4, 6)$:

$$\begin{aligned} 319 &= 3^{N_1(B)-1}2^{x_1} + 3^{N_1(B)-2}2^{x_2} + 3^{N_1(B)-3}2^{x_3} + 3^{N_1(B)-4}2^{x_4} + 3^{N_1(B)-5}2^{x_5} \\ &= 3^4 2^0 + 3^3 2^1 + 3^2 2^3 + 3^1 2^4 + 3^0 2^6 \end{aligned}$$

Similarly we can calculate $z(B_{\min}) = z(01011011) = 842$. Both integers, the 319 and the 864 belong to a $3n + 13$ cycle that is given by the following function whose parameter in this case is $c = 2^l - 3^{N_1(B)} = 13$:

$$f_c(x) = \begin{cases} {}^{3x+c}/_{2} & 2 \nmid x \\ {}^{x}/_{2} & \text{otherwise} \end{cases} \tag{4}$$

Note that 319 is the smallest member and 864 is the largest member of this sequence and the binary representation of $B_{\max} = 11011010$ reflects the course of this cycle starting with its smallest member 319, where the ones represent odd members and the zeros represent even members:

$$(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8) = (319, 485, 734, 367, 557, 842, 421, 638)$$

Table 1 shows the left-rotational distances of a binary number that we obtain from the integer x in the first column using the reverse function $z^{-1}(x)$ to another number located in the same row of v. For example the left-rotational distance of $557 = z(10101101)$ to $734 = z(01101011)$ is six, which we highlighted blue. Table 1 highlights our case of the rotational distance from $842 = z(01011011) = z(B_{\min})$ to $319 = z(11011010) = z(B_{\max})$ using the color green. The integer $r = 3$ is the only rotational distance value that provides a solution for the divisibility $8 \mid 5 \cdot r + 1$.

Table 1. Rotational distances of the $3x + 13$ cycle members.

	319	**485**	**734**	**367**	**557**	**842**	**421**	**638**
319	0	1	2	3	4	5	6	7
485	7	0	1	2	3	4	5	6
734	6	7	0	1	2	3	4	5
367	5	6	7	0	1	2	3	4
557	4	5	**6**	7	0	1	2	3
842	**3**	4	5	6	7	0	1	2
421	2	3	4	5	6	7	0	1
638	1	2	3	4	5	6	7	0

4. What We Know about Cycles

Starting point of our considerations is the function $f_c(x)$ given by Equation (4). Below we introduce a monoidal description of cycles. And as part of our own contribution, we develop a formula for calculating the smallest member in such a cycle.

Let S be a set containing two elements n_1 and n_0, which are bijective functions over $\mathbb{Q}$:

$$n_1(x) = {}^{3x+c}/_{2} \qquad n_0(x) = {}^{x}/_{2} \tag{5}$$

Let a binary operation be the left-to-right composition of functions $n_1 \circ n_0$, where $n_1 \circ n_0(x) = n_0(n_1(x))$. S^* is the composition monoid (transformation monoid), which is freely generated by S. The identity element is the identity function $id_{\mathbb{Q}} = e$. We call e an *empty string*. S^* consists of all expressions (strings) that can be concatenated from the generators n_1 and n_0. Every string can be written in precisely one way as product of factors n_1 and n_0 and natural exponents $k_i > 0$:

$$e, n_1^{k_1}, n_0^{k_1}, n_1^{k_1} n_0^{k_2}, n_0^{k_1} n_1^{k_2}, n_1^{k_1} n_0^{k_2} n_1^{k_3}, n_0^{k_1} n_1^{k_2} n_0^{k_3}, \ldots$$

These uniquely written products are called *reduced words* over S. Using exponents $k_i, h_i > 0$, we construct strings $s_i = n_1^{k_i} n_0^{h_i}$ and concatenate these to a larger string:

$$s_1 s_2 \cdots s_l = n_1^{k_1} n_0^{h_1} n_1^{k_2} n_0^{h_2} \cdots n_1^{k_l} n_0^{h_l}$$

Note that each string s_i is a reduced word, since $k_i, h_i > 0$. Let us evaluate this (large) string by inputting a natural number v_1. If the result is again v_1 then we obtain a cycle:

$$n_1^{k_1} n_0^{h_1} n_1^{k_2} n_0^{h_2} \cdots n_1^{k_l} n_0^{h_l}(v_1) = n_0^{h_l}(n_1^{k_l}(\cdots n_0^{h_2}(n_1^{k_2}(n_0^{h_1}(n_1^{k_1}(v_1)))))) = v_1$$

We write the sums briefly as $N_1 = k_1 + \cdots + k_l$ and $N_0 = h_1 + \cdots + h_l$. The cycle contains $N_1 + N_0$ elements. Example 2 illustrates, how bit rotations relate to compositions of the two functions n_0 and n_1. We summarize this fact to the following Definition 2:

Definition 2. *A cycle consists of $N_1 + N_0$ elements, where $N_1 = k_1 + \cdots + k_l$ is the number of its odd members and $N_0 = h_1 + \cdots + h_l$ the number of its even members.*

Moreover we define $A = a_1 + \cdots + a_l$ with

$$a_i = 2^{\sum_{j=1}^{i-1} k_j + h_j} \cdot \left(3^{k_i} - 2^{k_i}\right) \cdot 3^{\sum_{j=i+1}^{l} k_j}$$

We introduced this Definition 2 to prepare or allow us for the formulation of Theorem 1, which calculates the smallest member of the $3n + c$ cycle, which in line with Definition 2 consists of N_1 odd and N_0 even members:

Theorem 1. *The smallest number v_1 belonging to a cycle having N_1 odd and N_0 even members is:*

$$v_1 = \frac{c \cdot A}{2^{N_1+N_0} - 3^{N_1}}$$

This Theorem 1 corresponds to Theorem 5 provided and proved by Anant Gupta [10]. Note that we stick to our notation since it is aligned with Weisstein's (and Allouche's and Shallit's) established formalism.

Example 1. *We consider a $3n + 11$ cycle that has $N_1 + N_0 = 8 + 6 = 14$ elements and choose $(k_1, k_2, k_3, k_4) = (3, 1, 3, 1)$ and $(h_1, h_2, h_3, h_4) = (1, 1, 2, 2)$. Its smallest element is $v_1 = 13$ and we obtain all elements by evaluating the strings: $v_2 = n_1(v_1)$, $v_3 = n_1(v_2)$, $v_4 = n_1(v_3)$ and $v_5 = n_0(v_4)$ and so forth. It applies:*

$$\begin{aligned} & n_1 n_1 n_1 n_0 \circ n_1 n_0 \circ n_1 n_1 n_1 n_0 n_0 \circ n_1 n_0 n_0(v_1) \\ = \;& n_1^3 n_0 \circ n_1 n_0 \circ n_1^3 n_0^2 \circ n_1 n_0^2(v_1) \\ = \;& s_1 \circ s_2 \circ s_3 \circ s_4(v_1) = v_1 \end{aligned}$$

This cycle is $(v_1, v_2, v_3, \ldots, v_{14}) = (13, 25, 43, 70, 35, 58, 29, 49, 79, 124, 62, 31, 52, 26)$. We calculate v_1 directly as follows:

$$v_1 = \frac{11 \times 11609}{2^{8+6} - 3^8} = \frac{11 \times 11609}{9823} = 13$$

In this case $11609 = A = a_1 + a_2 + a_3 + a_4 = 4617 + 1296 + 3648 + 2048$*:*

$$\begin{array}{llll} a_1 = 2^0 & (3^3 - 2^3) & 3^{1+3+1} & = 4617 \\ a_2 = 2^{3+1} & (3^1 - 2^1) & 3^{3+1} & = 1296 \\ a_3 = 2^{3+1+1+1} & (3^3 - 2^3) & 3^1 & = 3648 \\ a_4 = 2^{3+1+1+1+3+2} & (3^1 - 2^1) & 3^0 & = 2048 \end{array}$$

Theorem 2. *The maximum odd element in a $3n + c$ cycle occurs immediately before the maximum even element.*

Proof. The maximum even element of the cycle cannot succeed an even element as the preceding element would be twice the element taken. The maximum odd element occurs before the maximum even element is equivalent to saying that the maximum even element follows the maximum odd element. Let v_1, v_2 be odd elements in the cycle with $v_1 > v_2$, then the elements after v_1, v_2 will be $w_1 = {}^{3v_1+c}/_2$ and $w_2 = {}^{3v_2+c}/_2$. Since $v_1 > v_2$ and $w_1 > w_2$, the element after the maximum odd element is greater than the element after

any other odd element. Therefore the maximum odd element of the cycle precedes the maximum even element of the cycle. □

In conformity with Definition 2, let us consider a $3n + c$ cycle $(v_1, v_2, \ldots, v_l)$ consisting of N_1 odd integers and N_0 even integers. Let us consider a binary parity vector (it is synonymous to a binary sequence or binary non-reduced word) consisting of $l = N_1 + N_0$ elements, which has a 1 at position i, if v_i is odd, and otherwise 0. Theorem 3 specifies several cycle restrictions:

Theorem 3. *For a $3n + c$ cycle with N_1 odd and N_0 even members applies:*

(a) *A cycle only exists if the inequality $2^{N_1+N_0} - 3^{N_1} > 0$ holds, see [11].*
(b) *The condition for a cycle's existence can be detailed as follows [11]: A non-inherited cycle only exists if $c \mid 2^{N_1+N_0} - 3^{N_1}$.*
(c) *Let $0 \leq x_1 < x_2 < \ldots < x_{N_1} \leq N_1 - 1$ be all positions (the indexing is zero-based) in the parity vector occupied by 1. A $3n + c$ cycle only exists if the divisibility $2^{N_1+N_0} - 3^{N_1} \mid c \cdot z(s)$ holds, where z is the function given by (3), see [11,12].*
(d) *The number of $3n + c$ cycles is always less than or equal to the number of $3n + a \cdot c$ cycles, where a is an odd number (this can be deduced from the work of Darrell Cox [11] as well).*

Example 2. *We refer to the $3n + 11$ cycle $(13, 25, 43, 70, 35, 58, 29, 49, 79, 124, 62, 31, 52, 26)$ again. The corresponding parity vector is $(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$ and the non-reduced word is $n_1n_1n_1n_0n_1n_0n_1n_1n_1n_0n_0n_1n_0n_0$.*

The indices are $(x_1, \ldots, x_8) = (0, 1, 2, 4, 6, 7, 8, 11)$ and therefore $z(8) = 3^7 2^0 + 3^6 2^1 + 3^5 2^2 + 3^4 2^4 + 3^3 2^6 + 3^2 2^7 + 3^1 2^8 + 3^0 2^{11} = 11609$.
Correctly it applies that $2^{8+6} - 3^8 \mid 11 \times 11609$, more specifically it is $9.823 \mid 127.699$ and $9.823 \times 13 = 127.699$.

Theorem 4. *Two different primitive cycles, $3n + c_1$ and $3n + c_2$, can never share a common parity vector.*

Proof. A $3n + c$ cycle with a given parity vector first appears at:

$$c = \frac{2^{N_1+N_0} - 3^{N_1}}{\gcd(A, 2^{N_1+N_0} - 3^{N_1})}$$

Let there exist cycles $3n + c_1$ and $3n + c_2$ with the same parity vector, this implies that the values of A and $2^{N_1+N_0} - 3^{N_1}$ as defined in Definition 2 are the same for both cycles. Therefore using the formula, a cycle can exist iff v_1 is an integer, i.e., $c \cdot A$ divides $2^{N_1+N_0} - 3^{N_1}$. The cycle will originate for the minimum such value of c. Therefore there can only be one value of c for which the parity vector produces a cycle that is not inherited. □

5. Boundary Features of Cycles

Halbeisen and Hungerbühler [8] introduced a boundary feature for cycles as a function $M(l, n)$, where l is the cycle length and n the number of its odd members. Let $S_{l,n}$ denote the set of all binary words of length l containing exactly n ones and otherwise only zeros. This set contains exactly $\binom{l}{n}$ words—exactly the number of ways in which we may select n elements out of l total where the order is irrelevant. In Halbeisen's and Hungerbühler's notation, the Hamming weight is denoted by n, which corresponds to our notation N_1 following Wolfram Math [5], that is $n = N_1$. In the example given by Table 2, the elements of the set $S_{5,2}$ are all listed in the first column.

The second column of Table 2 contains all binary words that result from left-rotating the binary word B in the first column up to l times:

$$\lambda_{\text{left}}(B, 5), \lambda_{\text{left}}(B, 1), \lambda_{\text{left}}(B, 2), \lambda_{\text{left}}(B, 3), \lambda_{\text{left}}(B, 4)$$

In generalized terms, this set is denoted as $\sigma(B) = \{\lambda_{\text{left}}(B,i) : 1 \leq i \leq l\}$. Remembering that z is the function (3), the third column of Table 2 contains the corresponding output of this function when inputting the rotated binary words:

$$z(\lambda_{\text{left}}(B,5)), z(\lambda_{\text{left}}(B,1)), z(\lambda_{\text{left}}(B,2)), z(\lambda_{\text{left}}(B,3)), z(\lambda_{\text{left}}(B,4))$$

The last column contains the minimum of these values. Finally, the largest of all these minima is $M(5,2)$ or generally, see [8]:

$$M(l,n) = \max_{B \in S_{l,n}} \{ \min_{t \in \sigma(B)} z(t) \} \tag{6}$$

Additionally to Halbeisen's and Hungerbühler's boundary feature $M(l,n)$ Darrell Cox et al. [1] introduced another boundary feature as a function $N(l,n)$. Let $g = \gcd(l,n)$, the function $N(l,n)$ is defined as follows:

$$N(l,n) = 2 \cdot M(l,n) - \sum_{i=0}^{g-1} 2^{i \cdot n/g} 3^{n-1-i \cdot n/g} \tag{7}$$

Example 3. *We choose a cycle given by $f_c(x)$ of length $l = 5$ having $n = 2$ odd members, where $c = 2^l - 3^n = 2^5 - 3^2 = 23$. Let us choose the binary words* 11000 *and* 10100 *and calculate the smallest member of the corresponding cycle in each case.*

In the first case, namely 11000 *synonymous with $n_1 n_1 n_0 n_0 n_0 = n_1^2 n_0^3 = n_1^{k_1} n_0^{h_1}$ we obtain $v_1 = {}^{c \cdot A}/_{2^{N_1+N_0} - 3^{N_1}} = {}^{23 \cdot 5}/_{2^{2+3} - 3^2} = 5$. The resulting cycle is $(5, 19, 40, 20, 10)$ which is given by the first row and third column in Table 2.*

In the second case, 10100 *that is synonymous with $n_1 n_0 n_1 n_0 n_0 = n_1^1 n_0^1 n_1^1 n_0^2 = n_1^{k_1} n_0^{h_1} n_1^{k_2} n_0^{h_2}$ we obtain $v_1 = {}^{23 \cdot 7}/_{2^{2+3} - 3^2} = 7$. The resulting cycle is $(7, 22, 11, 28, 14)$ which is given by the second row and third column in Table 2.*

Table 2 exhibits how $M(l,n)$ is calculated, which in our concrete case is $M(5,2) = 7$. Additionally we calculate $N(5,2) = 2 \cdot M(5,2) - 2^0 3^{2-1-0} = 14 - 3 = 11$.

Table 2. Calculation of $M(5,2)$.

	Word s	**Set $\sigma(s)$ of Left Rotated Words**	$\{z(t) : t \in \sigma(s)\}$	$\min_{t \in \sigma(s)} z(t)$
1	11000	11000, 10001, 00011, 00110, 01100	5, 19, 40, 20, 10	5
2	10100	10100, 01001, 10010, 00101, 01010	7, 22, 11, 28, 14	7
3	10010	10010, 00101, 01010, 10100, 01001	11, 28, 14, 7, 22	7
4	10001	10001, 00011, 00110, 01100, 11000	19, 40, 20, 10, 5	5
5	01100	01100, 11000, 10001, 00011, 00110	10, 5, 19, 40, 20	5
6	01010	01010, 10100, 01001, 10010, 00101	14, 7, 22, 11, 28	7
7	01001	01001, 10010, 00101, 01010, 10100	22, 11, 28, 14, 7	7
8	00110	00110, 01100, 11000, 10001, 00011	20, 10, 5, 19, 40	5
9	00101	00101, 01010, 10100, 01001, 10010	28, 14, 7, 22, 11	7
10	00011	00011, 00110, 01100, 11000, 10001	40, 20, 10, 5, 19	5
		The largest of all minimum z values is $M(l,n) = M(5,2) =$		7

6. Constructing One Cycle from Another

Cycles may interrelate, which means they have the same length and an equal amount of odd members. We refer to Example 3 and consider the $3n + 23$ cycle $(5, 19, 40, 20, 10)$. A cycle, which interrelates to this $3n + 23$ cycle is for example the $3n + 69$ cycle $(15, 57, 120, 60, 30)$. The latter is a non-primitive cycle (see definition in Appendix A).

If we go back to Example 1, then we can provide two interrelated cycles as well. For $l = N_1 + N_0 = 8 + 6 = 14$ we obtain $c = 2^l - 3^{N_1} = 2^{14} - 3^8 = 9823$ and the $3n + 9823$ cycle is (11609, 22325, 38399, 62510, 31255, 51794, 25897, 43757, 70547, 110732, 55366, 27683, 46436, 23218).

When we divide the parameter c and all cycle members by 893, then we obtain the reduced interrelated $3n + 11$ cycle $(13, 25, 43, 70, 35, 58, 29, 49, 79, 124, 62, 31, 52, 26)$.

Theorem 5. *Let a $3n + c$ cycle of length $l = N_1 + N_0$ has N_1 odd and N_0 even members, where $c = 2^l - 3^{N_1}$. It always applies that $M(l, n)$ is greater than the smallest member and $N(l, n)$ is less than the largest odd member of this cycle. Recall that we can take N_1 and n to be synonymous, since Halbeisen and Hungerbühler denote the Hamming weight by n.*

If c is divisible by an odd integer a, then for the (reduced) interrelated $3n + {}^{c}/_{a}$ cycle it applies that ${}^{M(l,n)}/_{a}$ is greater than the smallest member and ${}^{N(l,n)}/_{a}$ is less than the largest odd member of this reduced cycle.

The upper bound $M(l, n)$ has been unveiled and proved by Halbeisen and Hungerbühler [8] and the lower bound $N(l, n)$ was discovered and empirically verified by Cox et al. [1].

7. Constant Sums of $3n + c$ Cycle Members

For a compact visualization of our cycle member, we will collect all cycle elements $z(B)$ from all shifted versions of a given vector B in so-called equivalence classes. The reason why we declare those equivalence classes is that any member within such a class can be calculated also over the equivalence class representative. As we will see in this section, we can utilize this phenomenon due to the constancy within the equivalence classes.

Let us consider the set of all possible binary words of the length $l = 5$. This set contains $2^5 = 32$ elements. There exist 8 different periodic sequences, whereby we consider two sequences to be the *same*, if one of them can be obtained by left or right rotations from the other. Therefore different sequences do not share any sequence member. The members of these different sequences do not depend on the binary word's value, but from its length l and Hamming weight $N_1(B)$. A set of elements with the same sequence is called equivalence class.

Now, let us regard a set of the *same* (periodic) sequences and the number of its members is not equal to l. In this case the members of these sequences additionally depend from the left-rotational distance r of $B_{\min}$ to $B_{\max}$. In those cases the set may contain ${}^{l}/_{2}$, ${}^{l}/_{3}$ or $2l$ sequences.

Let B be a binary number of length l and with a Hamming weight $N_1(B)$. We use this binary number B to create a $3n + c$ sequence $(v_1, v_2, \ldots, v_l)$ by performing left-rotations and applying the function z as we did in Section 5:

$$v_1 = z(\lambda_{\text{left}}(B, 1)), v_2 = z(\lambda_{\text{left}}(B, 2)), \ldots, v_l = z(\lambda_{\text{left}}(B, l))$$

Moreover, we define a function Z that uses the binary number B as an input and yields the sum of all the members belonging to the periodic sequence $(v_1, v_2, \ldots, v_l)$ which we generated from B:

$$Z(B) = \sum_{i=1}^{l} v_i = \sum_{i=1}^{l} z(\lambda_{\text{left}}(B, i))$$

Example 4. *We choose $B = 00001$ and this results in $B_{\min} = 00001$ and $B_{\max} = 10000$. The length $l = 5$ and the Hamming weight $N_1(B) = 1$. This is a really trivial case of periodic sequence generation. Each row in Table 3 depicts the periodic sequence which we generated from B. This Table 3 illustrates that the generated cycles are not only reflected (horizontally) by rows, but also (vertically) by columns. That is because the digit 1 appears on every position within our rotated binary number B only once. Finally always $Z(B) = 2^l - 1 = 31$. Note that $B_{\min}$ and $B_{\max}$ are identical for the (rotated) B in each table row, since rotating a binary number generally does*

not affect the corresponding $B_{\min}$ *and* $B_{\max}$. *Halbeisen's and Hungerbühler's set* $S_{l,n}$ *which we introduced in Section 5 contains in the present case* l *words:* $S_{l,n} = S_{5,1} = \binom{5}{1} = 5$. *Therefore our equivalence class for* $l = 5$ *and the Hamming weight* $N_1(B) = 1$ *has the size of 5 elements. This behavior is exactly the same for* $N_1(B) = l - 1$, *since the binary number* 11110 *behaves in the same way as* 00001.

Table 3. Trivial Case for $l = 5$ and $N_1(B) = 1$.

B			v_1	v_2	v_3	v_4	v_5	$Z(B)$
00001	=	1	16	8	4	2	1	31
00010	=	2	8	4	2	1	16	31
00100	=	4	4	2	1	16	8	31
01000	=	8	2	1	16	8	4	31
10000	=	16	1	16	8	4	2	31
		$Z(B) =$	31	31	31	31	31	

Now let us consider less trivial cases. The number of possible Hamming weights is odd for a binary word having an even length. For instance, if the binary number's length $l = 4$ then this binary number can have a Hamming weight $N_1(B) \in \{0, 1, 2, 3, 4\}$. If the binary number's length $l = 6$ then this binary number can have a Hamming weight $N_1(B) \in \{0, 1, 2, 3, 4, 5, 6\}$.

Example 5. *We choose* $B = 001001$ *which results in* $B_{\min} = 001001$ *and* $B_{\max} = 100100$. *The length* $l = 6$ *is even and the Hamming weight is* $N_1(B) = 2$. *Table 4 shows that for* $N_1(B) = 2$ *the periodic sequence which we generated from B represents a concatenation of the cycle* $(44, 22, 11)$, *in which this cycle occurs exactly twice. In other words, this sequence has* $N_1(B) = 2$ *periods. We have* $l/N_1(B) = 6/2 = 3$ *distinct words and therefore* 3 *distinct equivalence class members in this periodic sequence which we generated from B.*

When we invert the binary number $B = 001001$ *by replacing* 0 *with* 1 *(and vice versa) we obtain the binary number* 110110. *This inverted binary number has the Hamming weight* $N_1(B) = l - 2 = 4$ *and exhibits the same behavior as* $B = 001001$. *Generally spoken, the cases for* $N_1(B) = l - 2$ *behave as same as* $N_1(B) = 2$.

Table 4. Non-trivial case for $l = 6$ and $N_1(B) = 2$.

B			v_1	v_2	v_3	v_4	v_5	v_6	$Z(B)$
001001	=	9	44	22	11	44	22	11	154
010010	=	18	22	11	44	22	11	44	154
100100	=	36	11	44	22	11	44	22	154
	$1/2 \cdot Z(B) =$		77	77	77	77	77	77	

Example 6. *We choose* $B = 010101$ *which results in* $B_{\min} = 010101$ *and* $B_{\max} = 101010$. *The length is again* $l = 6$ *and the Hamming weight is* $N_1(B) = 3$. *Table 5 shows that for* $N_1(B) = 3$ *the periodic sequence which we generated from B represents a concatenation of the cycle* $(74, 37)$, *in which this cycle occurs exactly three times. In other words, this sequence has* $N_1(B) = 3$ *periods. Here we have* $l/N_1(B) = 6/3 = 2$ *distinct words and therefore* 2 *distinct equivalence class members in this periodic sequence which we generated from B.*

Also here, inverting the binary number B leads to the same behavior, i.e., the cases for $N_1(B) = l - 3$ *behave the same as* $N_1(B) = 3$.

Table 5. Non-trivial case for $l = 6$ and $N_1(B) = 3$.

B			v_1	v_2	v_3	v_4	v_5	v_6	$Z(B)$
010101	=	21	74	37	74	37	74	37	333
101010	=	42	37	74	37	74	37	74	333
	$1/3 \cdot Z(B) =$		111	111	111	111	111	111	

It is important to note in conclusion that the amount of cycles that we can generate from a given binary number B is deterministic and not random. The Hamming weight $N_1(B)$ affects the binary combinatorics and it affects together with the length l the number of possible cycles that we are able to generate from B.

For a given binary number B of length l with a Hamming weight $N_1(B)$ the cases behave as same as for the inverted binary number (having the Hamming weight $l - N_1(B)$). For a given binary number B the possibilities for generating periodic sequences from B are limited as well.

8. Equivalence Classes for a Binary B of Length l

In the previous section, we took a look at the construct within one equivalence class. In this section we will analyze the construct from all different equivalence classes to each other for all possible binary input values B of a given length l.

It is important to understand how many equivalence classes there exist, or in other words, how many different constants $Z(B)$ we have for any given length l with all possible binaries B. Grosek and Hromada [3] provide us a formula to obtain the amount of equivalence classes for a given length l.

$$C(l, N_1(B), d) = \frac{1}{d} \cdot \left(\binom{d}{\frac{N_1(B) \cdot d}{l}} - \sum_{\substack{k \in D_{l,N_1(B)} \\ k|d \,,\, k<d}}^{k} k \cdot C(l, N_1(B), k) \right) \tag{8}$$

$C(l, N_1(B), d)$ returns how many equivalence classes we have for our input parameters l, the hamming weight $N_1(B)$ and the cardinality d of an equivalence class. In trivial cases the size and therefore the cardinality of any class is always $d = |B| = l$ and also for a Hamming weight of $N_1(B) = 0$ or $N_1(B) = l$ the cardinality is always $d = 1$ since we only have one sequence with only ones ore zeros. But due to the periodicity in non-trivial cases we also have different sizes for our classes and therefore also different cardinalities for each class. We collect different cardinalities for a given length l and hamming weight $N_1(B)$ in $D_{l,N_1(B)}$.

$$D_{l,N_1(B)} = \{d_1, d_2, ..., d_i\} \tag{9}$$

Example 7. *Now let us find out how many equivalence classes we have for a binary word of length $l = 6$. First we need all cardinalities for each possible Hamming weight $N_1(B)$ with $0 \leq N_1(B) \leq l$. The cardinalities are as followed $D_{6,0} = D_{6,6} = \{1\}$, $D_{6,1} = D_{6,5} = \{6\}$,since this counts for all trivial cases. $D_{6,2} = D_{6,4} = \{6, 3\}$ and $D_{6,3} = \{6, 2\}$ are non trivial cases and have therefor more than one equivalence class with different sizes. In Tables 4 and 5 we already saw the different sizes of the equivalence classes for those cardinalities.*

Now we can start applying our input parameters to formula (8). First let us look at the sum function in our equation. The sum has three conditions $k \in D_{l,N_1(B)}$, $k|d$ and $k < d$. Since k has to be less than d but also be an element out of $D_{l,N_1(B)}$ it is necessary to have at least two elements in $D_{l,N_1(B)}$ to hit the sum. In trivial cases it is otherwise always zero.

$$C(6,0,1) = \frac{1}{1} \times \binom{1}{0} = 1 \text{ case}$$
$$C(6,6,1) = \frac{1}{1} \times \binom{1}{1} = 1 \text{ case}$$
$$C(6,1,6) = \frac{1}{6} \times \binom{6}{1} = 1 \text{ case}$$
$$C(6,5,6) = \frac{1}{6} \times \binom{6}{5} = 1 \text{ case}$$

After calculating our trivial cases we clearly see that we end with only one specific equivalence class for those given input variables.

Now let us look at one non trivial case with the input parameter $l = 6$, $N_1(B) = 2$ *and* $D_{6,2} = 6, 3$.

$$C(6,2,3) = \frac{1}{3} \times \left[\binom{3}{1} - 0 \times 0\right] = 1 \text{ case}$$
$$C(6,2,6) = \frac{1}{6} \times \left[\binom{1}{1} - 3 \times 1\right] = 2 \text{ cases}$$

The first equation has again zero for the sum function, since $k = 3$ *is indeed an element of* $D_{l,N_1(B)}$ *but not smaller than the cardinality* $d_1 = 3$. *On the other hand for* $d_2 = 6$ *in* $D_{6,2} = \{3, 6\}$ *we do have a possible value for the sum index k. In fact* $k = 3$ *fulfills all three conditions and has therefore* $-3 \cdot C(6,2,3)$ *as an additional subtrahend in our equation.*

If we do the same for $D_{6,4} = \{6, 3\}$ *and* $D_{6,3} = \{6, 2\}$ *we end up with* $C(6,4,3) = 1$ *case,* $C(6,3,2) = 1$ *case,* $C(6,4,6) = 2$ *cases and* $C(6,3,6) = 3$ *cases. After counting the cases we end up with 14 different constants, like we already mentioned in the previous chapter.*

9. Generalizations to $kn + c$ Cycles

First we generalize the function (4) by introducing the following function:

$$f_{k,c}(x) = \begin{cases} {}^{kx+c}/_{2} & 2 \nmid x \\ {}^{x}/_{2} & \text{otherwise} \end{cases} \tag{10}$$

9.1. Generalization of Theorem 1

We can generalize Theorem 1 by replacing 3 by k. The smallest number v_1 belonging to a $kn + c$ cycle having N_1 odd and N_0 even members is:

$$v_1 = \frac{c \cdot A}{(k-2)(2^{N_1+N_0} - k^{N_1})}$$

9.2. Generalization of Theorem 2

Theorem 2 applies equally to $kn + c$ cycles as it does to $3n + c$ cycles. The proof provided for Theorem 2 is trivially generalizable to $kn + c$ cycles. This applies to the proof of the generalized Theorem 1 too.

9.3. Generalization of Theorem 3

Leaving the task of prove to the reader, we simply generalize Theorem 3 for $kn + c$ cycles having N_1 odd and N_0 even members:

(a) A cycle only exists if the inequality $2^{N_1+N_0} - k^{N_1} > 0$ holds.
(b) A cycle only exists if the integer c and the difference $2^{N_1+N_0} - k^{N_1}$ are not coprime: $\gcd(c, 2^{N_1+N_0} - k^{N_1}) > 1$.

(c) Let $0 \leq x_1 < x_2 < \ldots < x_{N_1} <\leq N_1 - 1$ be all positions (the indexing is zero-based) in the parity vector occupied by 1. A cycle only exists if the divisibility $2^{N_1+N_0} - k^{N_1} \mid c \cdot z(s)$ holds, where z is the function (3).
(d) The number of $kn + c$ cycles is always less than or equal to the number of $kn + a \cdot c$ cycles, where a is an odd number.

9.4. Generalization of Theorem 4

We generalize Theorem 4 by stating that two different primitive cycles, $kn + c_1$ and $kn + c_2$, can never share a common parity vector.

Proof. A $kn + c$ cycle with a given parity vector first appears at:

$$c = \frac{(k-2)(2^{N_1+N_0} - k^{N_0})}{\gcd(A, (k-2)(2^{N_1+N_0} - k^{N_0}))}$$

Let there exist cycles $kn + c_1$ and $kn + c_1$ with the same parity vector, this implies that the values of A and $(k-2)(2^{N_1+N_0} - k^{N_1})$ as defined in Definition 2 are same for both the cycles. Therefore using the formula, a cycle can exist if v_1 is an integer, i.e., $c \cdot A$ divides $(k-2)(2^{N_1+N_0} - k^{N_1})$. The cycle will originate for the minimum such value of c. Therefore there can only be one value of c for which the parity vector produces a cycle that is not inherited. □

9.5. Generalizing the Binary Rotations to kn + c Cycles

Let B be a binary number. The divisibility feature $l \mid N_1(B) \cdot r + 1$, demonstrated in Section 3 holds for the generalized $kn + c$ cycles. For this we set $c = (k-2)(2^l - k^{N_1(B)})$ and generalize function (3) as follows:

$$z_k(B) = \sum_{i=1}^{N_1} k^{N_1 - i} 2^{x_i} \tag{11}$$

Here again $0 \leq x_1 < x_2 < \ldots < x_{N_1} \leq N_1 - 1$ are the positions (indexing is zero-based) in B occupied by 1. It should be noted that this divisibility is an observation that remains to be proven. Possibly such a proof would contribute significantly to a proof of the Collatz conjecture.

9.6. More Theorems for kn + c Cycles

A positive integer k is called a *Crandall number*, if there exists a $kn + 1$ cycle. The following very fundamental Theorem 6 is well known, see [13,14]:

Theorem 6. *Every Wieferich number is a Crandall number. In other words, if k is a Wieferich number, then a cycle kn + 1 cycle exists.*

Franco and Pomerance provided a proof for Theorem 6 in their paper [14].

Theorem 7. *If c_1 and c_2 are coprime, then for a given k both functions f_{k,c_1} and f_{k,c_2} do not have any common non-trivial cycle (cycle with the same parity vector).*

A proof is given by Anant Gupta [10]. The idea can be sketched as follows: Let i be an integer. Since k^i does not divide $2^{N_1+N_0} - k^{N_1}$, all $kn + c$ cycles where $c = k^i$ will require $2^{N_1+N_0} - k^{N_1}$ to divide A (recall that A is specified by Definition 2), which is the same condition for $kx + 1$ cycles. This implies that all cycles of f_{k,k^i} are equal to the cycles of $f_{k,1}$. Similarly all cycles of $f_{k,c}$ are equal to the cycles of $f_{k,k^i \cdot c}$.

10. Conclusions

In this paper, we investigated the behavior of rotating binary numbers. We found out that a rotation by r digits to the left of a binary number B exhibits in particular cases the divisibility $l \mid N_1(B) \cdot r + 1$, where l is the bit-length of B and N_1 is the Hamming weight of B and r is the left-rotational distance as specified by Definition 1. We investigated the connection between this rotational distance, the bit length, and the Hamming weight. A core property is, that only under certain circumstances the above-mentioned divisibility becomes true – namely, this divisibility occurs for cycles.

Additionally, we reduce the amount of electrical calculation for the cycle calculations to the number of equivalence classes instead of the number of binaries 2^l. The cycle generation is exactly the same for any member within such a class and can therefore be resolved from the other members that have been already calculated.

Furthermore, we defined a more generic version of *sufficiently mixing* with more cryptography power, since we generalize $3x + c$ cycles to $kx + c$ cycles by introducing another variable k. Therefore, the range of all possible values becomes expanded and more obfuscated.

Author Contributions: A.G. introduced the formula for calculating the smallest cycle element and performed the formal proofs and verified the generalization to $kn + c$ cycles. I.J.A. directed the research and validated the results and findings of this article. He contributed important ideas to make the article submission-ready and guided the authors. S.G. performed the literature research and A.A. worked out the section on the practical application of this research. Moreover, A.A. elaborated the sections of constant sums and equivalence classes. A.R. verified the algorithms using python implementations and contributed to documenting editing and fixing. E.S. conceptualized this research, forms the basis of this article including the rotation formulas, diophantine equation, Tables 1 and 2 illustrating Halbeisen's and Hungerbühler's model, set up the nomenclature, and performed the formal analysis. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Fundamentals short and sweet

B	We denote B as a number in base-2 representation (a binary word) of bit-length $l = N_1(B) + N_0(B)$ consisting of $N_1(B)$ ones and $N_0(B)$ zeros.
bit-length	The bit-length l of an integer n specifies the number of bits used for the binary representation of this integer. It is given by $l = \lfloor \log_2(n) \rfloor + 1 = \lceil \log_2(n+1) \rceil$, see [15].
$\mathrm{gde}(n, 2)$	The greatest dividing exponent of base 2 with respect to a number n is the largest integer value of k such that $2^k \mid n$, where $2^k \leq n$, see [7].
digit count $N_d^2(B)$	The number $N_d^2(B) = N_d(B)$ of digits d in the base-2 representation of the number B is called the binary digit count for d. Thus $N_1(B)$ specifies the number of ones in B (also termed as *Hamming weight* of B) given by the difference $B - \mathrm{gde}(B!, 2)$. Analogously, $N_0(B)$ specified the number of zeros in B [5].
rotate a binary	The left rotation (left circular shift) of a binary B by r bits is the function $\lambda_{\text{left}}(B, r, l) = (B \cdot 2^r) \bmod (2^l - 1))$, where l is the bit-length of B. The right rotation is given by $\lambda_{right}(B, r, l) = \lambda_{\text{left}}(B, l - r, l)$. The bit-length is implicitly given and we can use shorter $\lambda_{\text{left}}(B, r)$.

rotational distance	The left-rotational distance of a binary B_2 from the binary B_1 is the required amount of rotating B_1 (bit by bit) until the rotated binary matches B_2. The right-rotational distance is defined analogously.
$3n + c$ cycle	We consider the function $f_c(x)$ given by Equation (4) and call a cycle the sequence of distinct positive integers $(v_1, v_2, \ldots, v_l)$ where $f_c(v_1) = v_2$ and $f_c(v_2) = v_3$ and so forth and finally $f_c(v_{l+1}) = v_1$.
$kn + c$ cycle	We generalize $3n + c$ cycles by replacing 3 with any positive integer k.
periodic sequence	Let $(v_1, v_2, \ldots, v_l)$ be a $3n + c$ cycle. We call a sequence that forms a repetition of this cycle $(v_1, v_2, \ldots, v_l, v_1, v_2, \ldots, v_l, \ldots)$ periodic.
Primitive cycle	If all members of a $3n + c$ cycle share a same common divisor greater than one, then this cycle is referred to as a *non-primitve* (inherited or interrelated) cycle, otherwise it is a *primitve* cycle, see [1].
Parity vector	The parity vector of a $3n + c$ cycle $(v_1, v_2, \ldots, v_l)$ is a binary vector having $l = N_1 + N_0$ entries – a 1 at position i, if v_i is odd, and otherwise 0.
Non-reduced word	Let us consider a $3n + c$ cycle with N_1 odd and N_0 even members. The non-reduced word describing this cycle is a word of length $N_1 + N_0$ over the alphabet $\{n_1, n_0\}$, which has a n_1 at those positions, where an odd member and a n_0 where an even member is located in the cycle. For instance, we treat the word $n_1n_0n_1n_1n_0n_1n_0n_1$ synonymous to the parity vector $(1, 0, 1, 1, 0, 1, 0, 1)$ or even simpler to the binary sequence (binary word) 10110101.

References

1. Cox, D.; Ghosh, S.; Sultanow, E. Generalizing Halbeisen's and Hungerbühler's optimal bounds for the length of Collatz cycles to 3n+c cycles. *J. Math. Comput. Sci.* **2021**, *24*, 330–337. [CrossRef]
2. Sultanow, E. Data Science for Number and Coding Theory: Divisibility, Periodic Sequences and Discrete Logarithm. Slides from the Talk "Data Science for Number and Coding Theory" at "Code Days 2021". 2021. Available online: https://www.slideshare.net/Sultanow/data-science-for-number-and-coding-theory-246114021 (accessed on 26 October 2021).
3. Grosek, O.; Hromada, V. Rotation-Equivalence classes of binary vectors. *Tatra Mt. Math. Publ.* **2016**, *70*, 93–98. [CrossRef]
4. Sedgewick, R.; Wayne, K. *Algorithms*, 4th ed.; Addison-Wesley: Upper Saddle River, NJ, USA, 2011.
5. Weisstein, E.W. "Digit Count." From MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/DigitCount.html (accessed on 26 October 2021).
6. Allouche, J.P.; Shallit, J. *Automatic Sequences*; Cambridge University Press: Cambridge, UK, 2003.
7. Weisstein, E.W. "Greatest Dividing Exponent." From MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/GreatestDividingExponent.html (accessed on 26 October 2021).
8. Halbeisen, L.; Hungerbühler, N. Optimal bounds for the length of rational Collatz cycles. *Acta Arith.* **1997**, *78*, 227–239. [CrossRef]
9. Ciet, M.; Farrugia, A.J.; Icart, T. System and Method for a Collatz Based Hash Function. U.S. Patent US 2013/0108038A1, 2 May 2013.
10. Gupta, A. On Cycles of Generalized Collatz Sequences. *arXiv* **2020**, arXiv:2008.11103.
11. Cox, D. The 3n+1 Problem: A Probabilistic Approach. *J. Integer. Seq.* **2012**, *15*. [CrossRef]
12. Böhm, C.; Sontacchi, G. On the existence of cycles of given length in integer sequences like $x_{n+1} = x_n/2$ if x_n even, and $x_{n+1} = 3x_n + 1$ otherwise. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Nat.* **1978**, *64*, 260–264.
13. Crandall, R.E. On the "3x+1" problem. *Math. Comput.* **1978**, *32*, 1281–1292. [CrossRef]
14. Franco, Z.; Pomerance, C. On a conjecture of Crandall concerning the "qx+1" problem. *Math. Comput.* **1995**, *64*, 1333–1336. [CrossRef]
15. Weisstein, E.W. "Bit Length." From MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/BitLength.html (accessed on 26 October 2021).