Constructing orientable sequences

Chris J. Mitchell and Peter R. Wild
Information Security Group, Royal Holloway, University of London
me@chrismitchell.net;   peterrwild@gmail.com

2nd January 2022

Abstract

This paper describes new, simple, recursive methods of construction for *orientable sequences*, i.e. periodic binary sequences in which any n-tuple occurs at most once in a period in either direction. As has been previously described, such sequences have potential applications in automatic position-location systems, where the sequence is encoded onto a surface and a reader needs only examine n consecutive encoded bits to determine its location and orientation on the surface. The only previously described method of construction (due to Dai et al.) is somewhat complex, whereas the new techniques are simple to both describe and implement. The methods of construction cover both the standard 'infinite periodic' case, and also the aperiodic, finite sequence, case. Both the new methods build on the Lempel homomorphism, first introduced as a means of recursively generating de Bruijn sequences.

1   Introduction

In this paper we are concerned with binary sequences with the property that any n-tuple of consecutive bits occurs either just once in a period, in the case of a periodic infinite sequence, or just once in a finite sequence (the aperiodic case). One important special case of such sequences are the de Bruijn sequences — see, for example, [11]. These sequences, sometimes referred to as shift register sequences (see Golomb, [12]), have been very widely studied and have a range of applications in coding and cryptography. One application which is of particular relevance to this paper, is that of *position location*, i.e. use of an encoding of an n-window sequence onto a surface that allows the location of any point on the surface by examining just n consecutive entries of the sequence (see, for example, Burns and Mitchell [3, 4] and Petriu [17]).

We are particularly interested in the special case of *orientable sequences* i.e. where, for given order n, any n-tuple of consecutive values occurs just

once in a period *in either direction*, in the case of an infinite sequence, or just once in either direction in a finite sequence (the aperiodic case). These sequences have position-location applications in the case where the reader of such a sequence wishes to determine both its position and its direction of travel. Such sequences were introduced some 30 years ago — see Burns and Mitchell [4] and Dai et al. [8]. More recent work on the use of sequences for position location includes that of Szentandrási et al. [19], Bruckstein et al. [2], Berkowitz and Kopparty [1], and Chee et al. [5, 6]. However, none of this more recent work provides any methods for constructing orientable sequences. Observe that orientable sequences are a particular type of universal cycle — see Chung et al. [7] and Jackson et al. [14].

Observe that no periodic orientable sequence exists for $n < 5$. A simple example of a periodic orientable sequence of order 5 is provided by the sequence of period $m = 6$ with generating cycle [001101], which has optimally long period (see Table 1). Sawada [1] provides examples of orders 6 and 7 of periods 16 and 36 respectively,[00101011100000] and [001101111001101010100111010010], which were shown to be optimally long by exhaustive search.

As previously mentioned, Dai et al. [8] give a method of construction for orientable sequences for every $n \geq 5$; they also provide an upper bound on the period of such sequences. Whilst the method of construction is shown to generate sequences of asymptotically optimal periods, i.e. the ratio of the period of a generated sequence with the upper bound tends to 1 as $n \to \infty$, the method itself is somewhat complex. For a given order n, it involves working with the set of cycles of length n that are orientable. These cycles can be divided into pairs made up of a cycle and its reverse. Using a graph-theoretic argument that is existential rather than constructive, Dai et al. show how one of every pair of the cycles can be joined to give an orientable sequence of order n.

A key motivation for this paper is to work towards addressing the following problem posed by Dai et al. [8].

> It is an open problem as to whether a more practical procedure exists for the construction of orientable sequences that have this asymptotically optimal period.

It seems likely that the reference to 'practical' here means a direct method of construction rather than one based on an existence proof. We present below a recursive construction method that is much simpler, and can also generate sequences that are within a fixed factor of asymptotically optimal period. The fixed factor depends on the period of the 'starter sequence', but (using an example given at http://debruijnsequence.org/db/orientable)

---

[1]See http://debruijnsequence.org/db/orientable

sequences can be constructed with periods at least 63% of the maximum possible. Of course the sequences have period shorter than those due to Dai et al. [8], which as noted above are of asymptotically optimal period.

We also examine here the aperiodic case, i.e. where the sequence is of finite length. Whilst this case was briefly examined by Burns and Mitchell [4], the only previously known method of construction was a trivial derivation from the periodic case (see [4] Lemma 1, and also as outlined in Section 4 below). Analogously to the periodic case, we give below a simple, recursive method of constructing such sequences of close to asymptotically optimal length; 00010111 and 00001101001111 are examples of (optimally long) aperiodic orientable sequences of orders 4 and 5, respectively.

The remainder of this paper is structured as follows. In Section 2, the terminology used throughout the paper is introduced, together with a range of fundamental results. The Lempel homomorphism and its application are reviewed in Section 3. A method for constructing orientable sequences using the Lempel homomorphism is described in Section 4; this is followed in Section 5 by an approach to the construction of aperiodic orientable sequences. The paper concludes in Section 6.

2 Terminology and fundamental results

2.1 Periodic binary sequences with a tuple property

We are concerned here with periodic binary sequences $S = (s_i)$, where $s_i \in \mathbb{B} = \{0, 1\}$, and where the period m of such a sequence is the smallest positive m such that $s_{i+m} = s_i$ for all i. We are particularly interested in finite sub-strings of such sequences (n-tuples), and for $n > 0$ we write

$$\mathbf{s}_n(i) = (s_i, s_{i+1}, \ldots, s_{i+n-1})$$

for the n-tuple *appearing at position i* in S. We are also interested in the *weight* of (one period of) a periodic sequence $S = (s_i)$, and we write:

$$w(S) = \sum_{i=0}^{m-1} s_i$$

where m is the period of S.

To simplify certain discussions below, we also introduce the notion of a *generating cycle*. If $S = (s_i)$ is a periodic binary sequence of period m, then the sequence of m values $s_0, s_1, \ldots, s_{m-1}$ forms the generating cycle of S, and clearly the generating cycle defines the entire sequence. Following Lempel [15], we write $S = [s_0, s_1, \ldots, s_{m-1}]$.

We define an *n-window sequence* $S = (s_i)$ (see, for example, [16]) to be a periodic binary sequence of period m with the property that no n-tuple appears more than once in a period of the sequence, i.e. with the property that if $\mathbf{s}_n(i) = \mathbf{s}_n(j)$ for some i, j, then $i \equiv j \pmod{m}$.

A *de Bruijn sequence of order n* [9] is then simply an n-window sequence of period 2^n (i.e. of maximal period), and has the property that every possible n-tuple appears once in a period.

Since we are interested in tuples occurring either forwards or backwards in a sequence we also introduce the notion of a *reversed* tuple, so that if $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ is a binary n-tuple, i.e. if $\mathbf{u} \in \mathbb{B}^n$, then $\mathbf{u}^R = (u_{n-1}, u_{n-2}, \ldots, u_0)$ is its *reverse*. If a tuple $\mathbf{u}$ satisfies $\mathbf{u} = \mathbf{u}^R$ then we say it is *symmetric*.

The *complement* (or what Lempel [15] refers to as the *dual*) of a tuple involves switching every 0 to a 1 and vice versa, and if $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{B}^n$ we write $\bar{\mathbf{u}} = (u_0 \oplus 1, u_1 \oplus 1, \ldots, u_{n-1} \oplus 1)$, where here, as throughout, $\oplus$ denotes exclusive-or (or, equivalently, modulo 2 addition). In a similar way, we refer to sequences being complementary if one can be obtained from the other by switching every 1 to a 0 and vice versa.

Following Lempel [15], we define the *conjugate* of an n-tuple to be the tuple obtained by switching the first bit, i.e. if $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{B}^n$, then the conjugate $\hat{\mathbf{u}}$ of $\mathbf{u}$ is the n-tuple $(u_0 \oplus 1, u_1, \ldots, u_{n-1})$.

Two n-window sequences $S = (s_i)$ and $T = (t_i)$ are said to be *disjoint* if they do not share an n-tuple, i.e. if $\mathbf{s}_n(i) \neq \mathbf{t}_n(j)$ for every i, j. An n-window sequence is said to be *primitive* if it is disjoint from its complement.

We next give a well known result (closely related to Theorem 2 of Lempel [15]) showing how two disjoint n-window sequences can be 'joined' to create a single n-window sequence, if they contain conjugate n-tuples; see also Lemma 3 of Sawada et al. [18].

Theorem 2.1 *Suppose $S = (s_i)$ and $T = (t_i)$ are disjoint n-window sequences of orders ℓ and m respectively. Moreover suppose S and T contain the conjugate n-tuples $\mathbf{u}$ and $\mathbf{v}$ at positions i and j, respectively (i.e. $\mathbf{u} = \hat{\mathbf{v}}$). Then*

$$[s_o, s_1, \ldots, s_{i+n-1}, t_{j+n}, t_{j+n+1}, \ldots, t_{m-1}, t_0, \ldots, t_{j+n-1}, s_{i+n}, s_{i+n+1}, \ldots, s_{\ell-1}]$$

is a generating cycle for an n-window sequence of period $\ell + m$.

We also introduce a graph of fundamental importance to the study of n-window sequences.

Definition 2.2 *The de Bruijn-Good graph $\mathcal{G}_n$ [13] is a directed graph with vertex set $\mathbb{B}^n$, where for $\mathbf{u}, \mathbf{v} \in \mathbb{B}^n$ (where $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} =$*

$(v_0, v_1, \ldots, v_{n-1})$) *there is a directed edge* $\mathbf{u} \to \mathbf{v}$ *if and only if* $u_{i+1} = v_i$, $0 \leq i \leq n - 1$.

It should be clear that every vertex in $\mathcal{G}_n$ has two incoming edges and two outgoing edges. It should also be clear that an $(n + 1)$-window sequence defines a (directed) cycle in $\mathcal{G}_n$, (where every $(n + 1)$-tuple maps to an edge), and, using the same mapping, a de Bruijn sequence of order $n + 1$ is equivalent to an Eulerian cycle in $\mathcal{G}_n$. This latter remark immediately establishes the existence of de Bruijn sequences for every n (given every node has degree 2). It is also straightforward to see that a de Bruijn sequence of order n defines an Hamiltonian cycle in $\mathcal{G}_n$, this time using the rather more obvious mapping of n-tuples to nodes.

2.2 Orientable sequences

The main focus of this paper is on n-window sequences with the property that an n-tuple cannot occur twice within a period in either direction. To this end we give the following definitions, following Dai et al. [8].

Definition 2.3 *An n-window sequence $S = (s_i)$ of period m is said to be an orientable sequence of order n (an $\mathcal{OS}(n)$) if, for any i, j, $\mathbf{s}_n(i) \neq \mathbf{s}_n(j)^R$.*

We also need the following related concept.

Definition 2.4 *A pair of disjoint orientable sequences of order n, $S = (s_i)$ and $S' = (s_i')$, are said to be orientable-disjoint (or simply o-disjoint) if, for any i, j, $\mathbf{s}_n(i) \neq \mathbf{s'}_n(j)^R$.*

As noted in Section 1, Dai et al. [8] give an upper bound on the period of orientable sequences.

Theorem 2.5 (Dai et al. [8]) *Suppose S is an $\mathcal{OS}(n)$ ($n \geq 5$). Then the period of S is at most:*

$$\begin{array}{ll} 2^{n-1} - 41/9 \times 2^{n/2-1} + n/3 + 16/9 & if \quad n \equiv 0 \pmod 4 \\ 2^{n-1} - 31/9 \times 2^{(n-1)/2} + n/3 + 19/9 & if \quad n \equiv 1 \pmod 4 \\ 2^{n-1} - 41/9 \times 2^{n/2-1} + n/6 + 20/9 & if \quad n \equiv 2 \pmod 4 \\ 2^{n-1} - 31/9 \times 2^{(n-1)/2} + n/6 + 43/18 & if \quad n \equiv 3 \pmod 4 \end{array}$$

The values arising from Theorem 2.5 for $5 \leq n \leq 9$ are given in Table 1.

Observe that the bound of Theorem 2.5 does not appear to be sharp for $n > 5$; as noted in the introduction, Sawada (see `http://debruijnsequence.org/db/orientable`) has shown that the maximum periods of an OS(6) and OS(7) are 16 and 36 respectively.

Table 1: Bounding the period of an $\mathcal{OS}(n)$ (from Theorem 2.5)

Order (n)	Maximum period m for an $\mathcal{OS}(n)$
5	6
6	17
7	40
8	96
9	206

3 The Lempel homomorphism

3.1 The homomorphism

The construction method we introduce later in this paper is an application of the homomorphism D, due to Lempel, [15].

Definition 3.1 (Lempel [15]) *The mapping $D : \mathbb{B}^n \to \mathbb{B}^{n-1}$ is as follows. If $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{B}^n$ then*

$$D(\mathbf{u}) = (u_0 \oplus u_1, u_1 \oplus u_2, \ldots, u_{n-2} \oplus u_{n-1}) \in \mathbb{B}^{n-1}.$$

The Lempel homomorphism has the following properties [15].

- D is onto, i.e. $D(\mathbb{B}^n) = \mathbb{B}^{n-1}$ ([15], Lemma 1).

- If $\mathbf{u}, \mathbf{v} \in \mathbb{B}^n$ then $D(\mathbf{u}) = D(\mathbf{v})$ if and only if $\mathbf{u} = \mathbf{v}$ or $\mathbf{u} = \bar{\mathbf{v}}$ ([15], Lemma 2).

- D is a graph homomorphism of $\mathcal{G}_n$ onto $\mathcal{G}_{n-1}$ ([15], Theorem 4).

We extend the notation to allow D to be applied to periodic binary sequences in the natural way. That is, D is a map from the set of periodic binary sequences to itself; the image of a sequence of period m will clearly have period dividing m. (See also Etzion [10] for a discussion of other properties of D). In the natural way we can define D^{-1} to be the 'inverse' of D, i.e. if S is a periodic binary sequence than $D^{-1}(S)$ is the set of all binary sequences T with the property that $D(T) = S$.

3.2 Constructing de Bruijn sequences

We next observe how the Lempel homomorphism can be used to construct a de Bruijn sequence of order $n + 1$ from a de Bruijn sequence of order n.

Although these results are well-known, we briefly give them here using our terminology, since they are of key importance for the orientable sequence construction given below. We first need the following result.

Theorem 3.2 *Suppose $S = (s_i)$ is an n-window sequence of period m. Then:*

- *if $w(S)$ is even then $D^{-1}(S)$ consists of a disjoint pair of complementary primitive $(n + 1)$-window sequences of period m, and*

- *if $w(S)$ is odd then $D^{-1}(S)$ consists of two different shifts of a single $(n + 1)$-window sequence of period $2m$ and weight m.*

Proof Suppose $T = (t_i) \in D^{-1}(S)$. It follows from the definition of D that

$$ t_i = t_0 \oplus \bigoplus_{j=0}^{i-1} s_j. $$

We consider the two cases separately.

- Suppose $w(S)$ is even. Then it follows immediately that $t_{m+i} = t_i$ for all i, i.e. $D^{-1}(S)$ consists of a pair of sequences of period m. It also immediately follows that the two sequences are complementary. Next suppose that $\mathbf{t}_{n+1}(i) = \mathbf{t}_{n+1}(j)$ for some i,j. Hence $D(\mathbf{t}_{n+1}(i)) = D(\mathbf{t}_{n+1}(j))$, i.e., by definition of D we know that $\mathbf{s}_n(i) = \mathbf{s}_n(j)$. Since S is an n-window sequence of period m, it follows that $i \equiv j \pmod{m}$, and hence T is an $(n + 1)$-window sequence.

  To establish primitivity, suppose the opposite, i.e. suppose $\mathbf{t}_{n+1}(i) = \bar{\mathbf{t}}_{n+1}(j)$ for some i,j. Then $D(\mathbf{t}_{n+1}(i)) = D(\bar{\mathbf{t}}_{n+1}(j))$, i.e. $\mathbf{s}_n(i) = \mathbf{s}_n(j)$. As previously this implies $i \equiv j \pmod{m}$, but since we know T has period m this immediately gives a contradiction since we assumed $\mathbf{t}_{n+1}(i) \neq \mathbf{t}_{n+1}(j)$.

- Now suppose $w(S)$ is odd. Then it follows immediately that $t_{m+i} = t_i \oplus 1$ for all i, and hence $t_{2m+i} = t_i$ for all i, i.e. T has period $2m$. The fact that $D^{-1}(S)$ contains two possible shifts of the same sequence follows by considering that t_0 can be either 0 or 1. The fact that T is an $(n+1)$-window sequence follows by precisely the same argument as for the even weight case. Finally, it has weight precisely half the period since if $\mathbf{u}$ is an $(n+1)$-tuple occurring in T, then $\bar{\mathbf{u}}$ also occurs in T. ∎

We next give two simple examples of the operation of D^{-1}.

Example 3.3 *First suppose $S = [101]$ (of even weight); then $D^{-1}(S) = \{[011], [100]\}$. Alternatively suppose $S = [100]$ (of odd weight); then $D^{-1}(S) = \{[100011]\}$.*

Since the weight of a binary de Bruijn sequence of order $n > 1$ is always even, the above theorem immediately gives as a corollary the following result due to Lempel [15].

Corollary 3.4 *Suppose $S = (s_i)$ is a de Bruijn sequence of order $n > 1$. Then $D^{-1}(S)$ consists of a disjoint pair of complementary disjoint $(n + 1)$-window sequences of period 2^n.*

To complete the construction we need the following simple lemma (in essence given in a discussion in §IV.A of Lempel [15]).

Lemma 3.5 *Suppose $S = (s_i)$ is a de Bruijn sequence of order $n > 1$, and let $D^{-1}(S) = \{T, T'\}$, where (from Corollary 3.4) T and T' are a disjoint pair of complementary disjoint $(n+1)$-window sequences of period 2^n. Then T and T' contain conjugate $(n + 1)$-tuples.*

Proof Consider the two $(n + 1)$-tuples consisting of alternating bits, i.e. $\mathbf{u} = (1010\ldots)$ and $\mathbf{v} = (0101\ldots)$. They are clearly complementary and so one occurs in T and the other in T' — they must both occur in one or other of T and T' since by an obvious numerical argument T and T' between them contain all $(n + 1)$-tuples. Suppose, without loss of generality, $\mathbf{u}$ occurs at position i in $T = (t_i)$; then $t_{i-1} = 1$ since if $t_{i-1} = 1$ then $\mathbf{v}$ occurs at position $i - 1$ in T, contradicting the disjointness of T and T'. Hence the conjugate to $\mathbf{v}$ occurs at position $i - 1$ in T, giving the desired result. ∎

It follows immediately that, combining Corollary 3.4 with Theorem 2.1 and Lemma 3.5, it is simple to construct a de Bruijn sequence of order $n + 1$ from one of order n by applying the inverse Lempel homomorphism and then 'joining' the two resulting sequences.

4 Constructing orientable sequences

4.1 Applying the Lempel homomorphism

We next show that a similar approach to that described above can be used to construct orientable sequences of order $n + 1$ from one of order n.

Theorem 4.1 *Suppose $S = (s_i)$ is an orientable sequence of order n and period m. Then:*

- *if $w(S)$ is even then $D^{-1}(S)$ consists of an o-disjoint pair of primitive complementary orientable sequences of order $n+1$ and period m, and*

- *if $w(S)$ is odd then $D^{-1}(S)$ consists of two different shifts of a single orientable sequence of order $n+1$, period $2m$ and weight m.*

Proof As previously we consider two cases.

- If $w(S)$ is even then Theorem 3.2 shows that $D^{-1}(S)$ consists of an disjoint pair of primitive complementary $(n+1)$-window sequences of order $n+1$ and period m. It therefore remains to show that the two sequences are themselves orientable, and also that they are o-disjoint.

  First suppose that $T = (t_i) \in D^{-1}(S)$ is not orientable. i.e. $\mathbf{t}_{n+1}(i) = \mathbf{t}_{n+1}(j)^R$ for some i, j. Then $D(\mathbf{t}_{n+1}(i)) = D(\mathbf{t}_{n+1}(j)^R)$, i.e. $\mathbf{s}_n(i) = \mathbf{s}_n(j)^R$, contradicting the assumption that S is orientable.

  Next suppose that $T, T' \in D^{-1}(S)$ are not o-disjoint (where $T = (t_i)$ and $T' = (t'_i)$). We know they are disjoint (from Theorem 3.2), and hence it must hold that $\mathbf{t}_{n+1}(i) = \mathbf{t}'_{n+1}(j)^R$. Then $D(\mathbf{t}_{n+1}(i)) = D(\mathbf{t}'_{n+1}(j)^R)$, i.e. $\mathbf{s}_n(i) = \mathbf{s}_n(j)^R$, again contradicting the assumption that S is orientable.

- If $w(S)$ is odd then Theorem 3.2 again almost establishes the result. It remains to show that the $(n+1)$-window sequence of period $2m$ is orientable. However, this follows by precisely the same argument as used in the previous case. ∎

Clearly this result is not enough on its own to enable construction of 'long' orientable sequences, since, even if S has odd weight and period m, then $T \in D^{-1}(S)$ will have weight m, i.e. it will have odd weight if and only if m is odd. Moreover, even if S has odd weight and odd period, then $T \in D^{-1}(S)$ will have period $2m$, and hence $U \in D^{-1}(T)$ will have even weight. This is shown by the simple case in Example 4.2.

Example 4.2 *Let S be the $\mathcal{OS}(5)$ of period $m = 6$ with generating cycle [001101], mentioned in Section 2.2. S has weight 3 (odd) and hence Theorem 4.1 tells us that $D^{-1}(S)$ contains a single $\mathcal{OS}(6)$ of period 12, namely: [000100111011]. However, this has weight 6 (even) so that another application of D^{-1} will yield a complementary pair of $\mathcal{OS}(7)$s of period 12, namely [000011101001] and [111100010110].*

To achieve 'period doubling' for multiple iterations of the above construction, two 'obvious' possibilities present themselves:

- find a sequence S with the property that when applying the construction method iteratively, the output complementary pair of sequences contains a conjugate pair of tuples (thereby enabling the two sequences to be joined to create a single 'double length' sequence — see Theorem 2.1);

- find a sequence S (with odd weight) with the property that it is possible to modify the double length output sequence $T \in D^{-1}(S)$ to ensure that it too has odd weight.

In the next section we exhibit an approach of the second type.

4.2   An approach to maintaining odd weight

We first define a method of 'extending' orientable sequences of a special type.

Definition 4.3 *Suppose $S = (s_i)$ is an orientable sequence of order n and period m with the property that there is there is exactly one occurrence of 1^{n-4} in a period (and hence it contains no longer runs of $1s$); suppose the generating cycle of S is $[s_0, s_1, \ldots, s_{m-1}]$ where $s_r = s_{r+1} = \cdots = s_{r+n-5} = 1$ for some r. Define the function $\mathcal{E}$ (with domain and range the set of periodic binary sequences) as follows. If S has odd weight then set $\mathcal{E}(S) = S$, and if S has even weight then define $\mathcal{E}(S)$ to be the sequence with generating cycle*

$$[s_0, s_1, s_{r-1}, 1, s_r, s_{r+1}, \ldots s_{m-1}]$$

i.e. where the single occurrence of 1^{n-4} is replaced with 1^{n-3}.

Remark 4.4 *Note that, as discussed in Dai et al. [8], it is simple to see that any orientable sequence can contain at most one occurrence of 1^{n-3} in a period.*

We can now state a key result.

Lemma 4.5 *Suppose $S = (s_i)$ is an orientable sequence of order n and period m with the property that there is exactly one occurrence of 1^{n-4} in a period. Then $\mathcal{E}(S)$ is an orientable sequence of order n, period m or $m+1$ (depending on whether $w(S)$ is odd or even) and odd weight.*

Proof The result clearly holds if S has odd weight, and we thus suppose S has even weight. The fact that $\mathcal{E}(S)$ has odd weight follows immediately from the definition. Again by definition the period of $\mathcal{E}(S)$ divides $m+1$, and

is precisely $m+1$ because $[s_0, s_1, s_{r-1}, 1, s_r, s_{r+1}, ... s_{m-1}]$ contains exactly one occurrence of 1^{n-3}.

It remains to show that $\mathcal{E}(S)$ is an $\mathcal{OS}(n)$. We only need to examine the n-tuples which include the inserted 1. Inserting this single 1 means that the following three n-tuples that occur in S (where the subscripts are computed modulo $m+1$):

$$
\begin{aligned}
u_0 &= (s_{r-3}, s_{r-2}, s_{r-1}, 1^{n-4}, s_{r+n-4}), \\
u_1 &= (s_{r-2}, s_{r-1}, 1^{n-4}, s_{r+n-4}, s_{r+n-3}), \\
u_2 &= (s_{r-1}, 1^{n-4}, s_{r+n-4}, s_{r+n-3}, s_{r+n-2})
\end{aligned}
$$

are replaced in $\mathcal{E}(S)$ by the following four n-tuples:

$$
\begin{aligned}
v_0 &= (s_{r-3}, s_{r-2}, s_{r-1}, 1^{n-3}), \\
v_1 &= (s_{r-2}, s_{r-1}, 1^{n-3}, s_{r+n+4}), \\
v_2 &= (s_{r-1}, 1^{n-3}, s_{r+n-4}, s_{r+n-3}), \\
v_3 &= (1^{n-3}, s_{r+n-4}, s_{r+n-3}, s_{r+n-2}).
\end{aligned}
$$

Now all four of the v_i tuples contain 1^{n-3}, and hence they are all distinct and cannot occur in S (or S^R). The only remaining task is to show that $v_0 \neq v_3^R$ and $v_1 \neq v_2^R$. However, if $v_0 = v_3^R$ or $v_1 = v_2^R$ then it immediately follows that u_1 is symmetric, which contradicts the assumption that S is orientable. ∎

This then enables us to give a means to recursively generate 'long' orientable sequences. We first define a special class of sequence.

Definition 4.6 *An $\mathcal{OS}(n)$ with the property that there is exactly one occurrence of 0^{n-4} in a period is said to be* good.

Theorem 4.7 *Suppose $S = (s_i)$ is a good $\mathcal{OS}(n)$ of odd weight and period m. If $T \in D^{-1}(S)$ then $\mathcal{E}(T)$ is a good $\mathcal{OS}(n+1)$ of odd weight, and period either $2m$ (if m is odd) or $2m+1$ (if m is even).*

Proof The fact that T is an $\mathcal{OS}(n+1)$ of period $2m$ follows immediately from Theorem 4.1; we also know the weight of T is m. Since 0^{n-4} occurs exactly once in S, both 0^{n-3} and 1^{n-3} occur exactly once in T, as $D^{-1}(0^{n-4}) = \{0^{n-3}, 1^{n-3}\}$. This means that T is good and also the conditions of Lemma 4.5 apply. This in turn means that $\mathcal{E}(T)$ is an orientable sequence of order $n+1$ and odd weight. The fact that $\mathcal{E}(T)$ is good follows from observing that applying $\mathcal{E}$ cannot affect the number of occurrences of 0^{n-3}. Finally, $\mathcal{E}(T)$ has period either $2m$ (if m is odd) or $2m+1$ (if m is even), since T has weight m. ∎

This immediately gives the following result.

Corollary 4.8 *Suppose S_n is a good $\mathcal{OS}(n)$ of period m_n. Recursively define the sequences $S_{i+1} = \mathcal{E}(D^{-1}(S_i))$ for $i \geq n$, and suppose S_i has period m_i $(i > n)$. Then, S_i is a good $\mathcal{OS}(i)$ for every i, and for every $j \geq 0$:*

- *if m_n is odd, $m_{n+2j+1} = 2m_{n+2j}$ and $m_{n+2j+2} = 2m_{n+2j+1} + 1$;*

- *if m_n is even, $m_{n+2j+1} = 2m_{n+2j} + 1$ and $m_{n+2j+2} = 2m_{n+2j+1}$.*

Proof If m_i is odd for any $i \geq m$, then $D^{-1}(S_i)$ will have odd weight and hence $S_{i+1} = D^{-1}(S_i)$; that is, S_{i+1} will have even period $(2m_i)$. By similar reasoning, S_{i+2} will have odd period $(2m_{i+1} + 1 = 4m_i + 1)$. This immediately yields the result. ∎

Simple numerical calculations give the following.

Corollary 4.9 *Suppose the sequences (S_i) are defined as in Corollary 4.8. Then*

- *if m_n is odd, $m_{n+2j} = 2^{2j}m_n + (2^{2j} - 1)/3$ and $m_{n+2j+1} = 2^{2j+1}m_n + (2^{2j+1} - 2)/3$;*

- *if m_n is even, $m_{n+2j} = 2^{2j}m_n + (2^{2j+1} - 2)/3$ and $m_{n+2j+1} = 2^{2j+1}m_n + (2^{2j+2} - 1)/3$.*

We conclude by giving a simple example of how the above process can be used to generate an infinite family of orientable sequences.

Example 4.10 *[001010111] is the generating cycle of an $\mathcal{OS}(6)$ of period 9, which is good since it contains exactly one instance of 0^2. It also has odd weight. So it can be used as S_6 for the first application of D^{-1}. This results in a good $\mathcal{OS}(7)$ of period 18 with generating cycle: [000110010111001101]. This has weight 9 (which is odd), i.e. $\mathcal{E}(D^{-1}(S_6)) = D^{-1}(S_6)$, and so $S_7 = $ [000110010111001101]. We next have*

$$D^{-1}(S_7) = [000010001101000100111101110010111011]$$

which has even weight and hence we need to insert an extra 1 after the unique sequence of four 1s, i.e.

$$S_8 = [0000100011010001001111101110010111011].$$

Continuing in this way we obtain sequences with the periods listed in Table 2.

Table 2: A family of orientable sequences

Order (n)	Period (m_n)	Remarks
6	9	
7	18	No need to insert an extra 1 as the weight
		is odd since [001010111] has odd period
8	37	After adding the extra 1
9	74	No need to insert an extra 1
10	149	
$\cdots$	$\cdots$	
$6 + 2j$	$9(2^{2j}) + (2^{2j} - 1)/3$	
$6 + 2j + 1$	$9(2^{2j+1}) + (2^{2j+1} - 2)/3$	

For the sequences in Example 4.10 we thus have $m_n > 9 \times 2^{n-6}$ and from Dai et al. [8] we know that $m_n < 2^{n-1}$ for any orientable sequence of order n. That is, even for this simple example, the sequences obtained have periods at least 9/32 of the optimal values. Clearly sequences with periods closer to the optimal values can be obtained if the 'starter sequence' has period larger than the value given in the table[2], although the generated sequences will never by asymptotically optimal in length (unlike the sequences of Dai et al. [8]). The sequence of period 9 was found by hand, and in the absence of a systematic search it is not clear whether a good $\mathcal{OS}(6)$ of period greater than 9 exists.

5 The aperiodic case

5.1 Introduction and definitions

Up to this point we have only considered *periodic* sequences, i.e. infinite binary sequences which repeat after a finite period. However, many of the ideas we have thus far discussed also apply to the *aperiodic* case, i.e. where we are dealing with a single finite sequence. If $S = (s_0, s_1, \ldots, s_{\ell-1})$ is a binary sequence of length ℓ, i.e. $s_i \in \mathbb{B}$ for $0 \leq i < \ell$, then S is an aperiodic orientable sequence of order n (an $\mathcal{AOS}(n)$) if and only if the collection of $2\ell - 2n + 2$ n-tuples $\mathbf{s}_n(i)$ and $\mathbf{s}_n(i)^R$ ($0 \leq i \leq \ell - n$) are all distinct.

As noted in Section 1, sequences of both periodic and aperiodic type have potential applications in position-location applications where the sequence is

---

[2]An example of a good $\mathcal{OS}(8)$ of period 80 has been found by Sawada — see `http://debruijnsequence.org/db/orientable` — yielding sequences of length at least 63% of the longest possible such sequence.

encoded onto a surface which may be read in either direction, and reading n digits reveals the location of the reader and the direction of travel. Whether the periodic or aperiodic sequences are more appropriate depends on whether the surface on which the sequence is encoded forms a closed loop, e.g. when the surface is a cylinder, or not.

This case was briefly considered by Burns and Mitchell [4], who give some simple results on the lengths of the longest such sequences, obtained from computer searches — see Table 3, where it is claimed that the for $4 \leq n \leq 7$ the length given is the length of the longest such sequence. Note that such sequences are referred to there as binary aperiodic 2-orientable window sequences.

Table 3: Existence of aperiodic orientable sequences

Order (n)	Sequence length (ℓ)
4	8
5	14
6	26
7	48
8	108
9	210
10	440
11	872
12	1860
13	3710
14	7400
15	15467
16	31766

It follows immediately from the definitions that if $S = (s_i)$ is an $\mathcal{OS}(n)$ of period m, then $(s_0, s_1 \ldots, s_{n+m-2})$ is an $\mathcal{AOS}(n)$ of length $m + n - 1$ (see also [4]).

Finally, analogously to the periodic case, we define:

- a pair of $\mathcal{AOS}(n)$s to be *disjoint* if they do not share an n-tuple;

- a pair of $\mathcal{AOS}(n)$s to be *o-disjoint* if they do not share an n-tuple in either direction; and

- an aperiodic sequence to be *primitive* if it is disjoint from its complement.

5.2 Applying the Lempel homomorphism

The Lempel homomorphism applies equally in the aperiodic case, and the following result analogous to Theorem 4.1 holds. As the operator D acts in the same way on $(n+1)$-windows in the aperiodic case as the periodic case the proof follows using precisely the same arguments as in Theorems 3.2 and 4.1.

Theorem 5.1 *Suppose $S = (s_i)$ is an $\mathcal{AOS}(n)$ of length ℓ. Then $D^{-1}(S)$ consists of an o-disjoint pair of primitive complementary $\mathcal{AOS}(n+1)s$ of length $\ell + 1$.*

Of course, this result does not enable us to generate long aperiodic orientable sequences. As in the periodic case, we need to find a way to combine the pair of sequences output from the inverse Lempel homomorphism. Fortunately, as we show below, if you start the iterative process with a sequence with very special properties then this can be achieved.

5.3 A special case

We start by considering a very special type of $\mathcal{AOS}(n)$. We first need the following.

Definition 5.2 *If $S = (s_i)$ is an $\mathcal{AOS}(n)$, $n > 1$, of length ℓ with the property that the first $n-1$ bits are 0s and the last $n-1$ bits are 1s, i.e. $S = 0^{n-1} \cdots 1^{n-1}$, then we say S is* ideal.

We can now state the following simple result, which follows immediately from Theorem 5.1 and the definition of D.

Lemma 5.3 *Suppose $S = (s_i)$ is an ideal $\mathcal{AOS}(n)$. Then:*

$$D^{-1}(S) = \{(0^n \cdots a_n), (1^n \cdots \bar{a}_n)\}$$

where a_n is a subsequence consisting of n alternating bits (whether it starts with a 0 or a 1 is immaterial).

This then leads to the following main result.

Theorem 5.4 *Suppose $S = (s_i)$ is an ideal $\mathcal{AOS}(n)$ of length ℓ, and let $D^{-1}(S) = \{T, \bar{T}\}$ where $T = (0^n \cdots a_n)$ as in Lemma 5.3. Let $U = \bar{T}^R$.*

- *If n is even, let V be the sequence of length $2\ell - n + 2$ consisting of the $\ell + 1$ bits of T followed by the final $\ell - n + 1$ bits of U (i.e. U with the first n bits omitted).*

- *If n is odd, let V be the sequence of length $2\ell - n + 3$ consisting of the $\ell + 1$ bits of T followed by the final $\ell - n + 2$ bits of U (i.e. U with the first $n - 1$ bits omitted).*

In both cases V is an ideal $\mathcal{AOS}(n + 1)$.

Proof Without loss of generality we suppose throughout that a_n starts with a 0 (and hence ends with a 0/1 if n is odd/even).

First suppose that n is even. Then, since $\bar{T} = 1^n \cdots \bar{a}_n$, $U = \bar{a}_n \cdots 1^n$, the first n bits of U match the final n bits of T. It follows that the merging of the two sequences to create V does not introduce any additional 'new' $(n + 1)$-tuples, i.e. the set of $(n + 1)$-tuples in V is equal to those appearing in T and U. Hence, since $U = \bar{T}^R$, and T and $\bar{T}$ are an o-disjoint pair of primitive complementary $\mathcal{AOS}(n + 1)$s (from Theorem 5.1), it follows that V is an $\mathcal{AOS}(n + 1)$. The fact that it is ideal follows immediately from its method of construction, and its length is equal to the sum of the lengths of T and U minus n, the number of 'overlapped' bits, i.e. $2(\ell + 1) - n = 2\ell - n + 2$.

Now suppose that n is odd. In this case $U = \bar{a}_n \cdots 1^n$, and so the final $n - 1$ bits of U match the first $n - 1$ bits of T. The 'merging' of T and U to create V introduces a single additional 'new' $(n + 1)$-tuple in V, namely the $(n + 1)$-bit alternating tuple starting with a 0 — all other tuples occur in T or U; similarly, the only additional 'new' $(n + 1)$-tuple in V^R is the $(n + 1)$-bit alternating tuple starting with a 1 (since $n + 1$ is even). Neither of these tuples could appear in T or U (or their reverses) since the image under D of these $(n + 1)$-tuples is 1^n, which cannot appear in S since it is symmetric. It thus again follows that V is an ideal $\mathcal{AOS}(n + 1)$, in this case of length equal to the sum of the lengths of T and U minus $n - 1$, the number of 'overlapped' bits, i.e. $2(\ell + 1) - (n - 1) = 2\ell - n + 3$. ∎

The above construction clearly gives an iterative method of computing an $\mathcal{AOS}(n)$ for arbitrary n, given an ideal $\mathcal{AOS}$ to act as a 'starter' in the construction. The length of the sequences obtained is given by the following lemma.

Lemma 5.5 *Suppose S_n is an ideal $\mathcal{AOS}(n)$ of length ℓ_n, and moreover suppose that S_{m+n} is an ideal $\mathcal{AOS}(m + n)$ of length ℓ_{m+n} obtained from S_n using m iterations of the approach given in Theorem 5.4. Then*

$$\ell_{m+n} = 2^m(\ell_n - n + 1) + x_m/3 + m + n - 1.$$

where x_m is one of $2^m - 1$ (n even, m even), $2^m - 2$ (n even, m odd), $2^{m+1} - 2$ (n odd, m even), or $2^{m+1} - 1$ (n odd, m odd).

Proof For any sequence S_r ($r \geq n$) we consider the value ν_r, i.e. the number of r-tuples appearing in S_r. Clearly $\nu_r = \ell_r - r + 1$. From Theorem 5.4, we immediately have that $\nu_{n+1} = 2\nu_n$ if n is even, and $\nu_{n+1} = 2\nu_n + 1$ if n is odd. The result then follows from some simple calculations. ∎

We now give a simple example of the use of the above iterative construction, yielding an infinite family of aperiodic orientable sequences.

Example 5.6 *We start by observing that $S_2 = 01$ is an ideal $\mathcal{AOS}(2)$ of length 2. This is clearly optimally long. Now $D^{-1}(S) = \{001, 110\}$, i.e. $T = 001$ and $U = 011$. Since 2 is even, we overlap the sequences by $n = 2$ positions to obtain $S_3 = 0011$. Note that S_3 is also of optimal length since there are only four asymmetric 3-tuples, two of which appear.*

Repeating the construction, applying D^{-1} to 0011 gives $T = 00010$ and $U = 10111$. Overlapping them by $2(= n - 3)$ bit-positions we get $S_4 = 00010111$ of length 8. This involves adding the extra 4-tuple 0101, which could not appear in either T or U as its image under D is 111, which is symmetric. S_4 is also optimally long according to Table 3.

We next obtain $S_5 = 00001101001111$ of length 14. Continuing this process gives sequences of the lengths in Table 4.

Table 4: A family of aperiodic orientable sequences

Order (n)	Sequence length (ℓ)
2	2
3	4
4	8
5	14
6	26
7	48
8	92
9	178
10	350
...	...
$2r$	$2^{2r-2} + (2^{2r-2} - 1)/3 + 2r - 1$
$2r + 1$	$2^{2r-1} + (2^{2r-1} - 2)/3 + 2r$

Inspection of Table 4 reveals that for $n \leq 7$ the sequences are optimally long (according to Table 3), but for larger values of n they are not. However,

they are very simple to construct, and from Lemma 5.5 (see also Table 4) the length of the sequence S_n is greater than $2^n/3$. A simple upper bound (see Lemma 15 of [4]) means that the length of any $\mathcal{AOS}(n)$ is at most $2^{n-1} - 2^{\lfloor (n-1)/2 \rfloor} + n - 1$; that is, the sequences generated by this approach have lengths at least $2/3$ of the optimal values.

6   Conclusions and possible future work

We have described how the Lempel homomorphism can be applied to recursively generate infinite families of both periodic and aperiodic orientable sequences. We have given examples of infinite families of orientable sequences, both periodic and aperiodic, generated using the construction methods and having, in both cases, close to optimal period/length — the periodic sequences have period at least 63% of the optimal value, and the aperiodic sequences have length at least $2/3$ of optimal. Moreover, sequences with greater period/length can be obtained should longer 'starter' sequences for the recursions be chosen. The method of construction in both cases is direct very simple, partially answering the question posed by Dai et al. [8] and quoted in Section 1. They only *partially* answer the question since the periods/lengths of the sequences produced are not asymptotically optimal. The methods are also of low complexity in terms of time — they are trivially linear in the sequence length; however, the storage complexity is high since the entire sequence needs to be available to perform the recursion operation.

Since in both cases the sequences are generated using a simple recursive approach, it may well be possible to devise simple encoding and decoding methods, i.e. algorithms that, for an $\mathcal{OS}(n)$ or an $\mathcal{AOS}(n)$, enable a position value to be converted into the n-tuple that occurs in that position in the sequence or its reverse (encoding) or vice versa (decoding). Such algorithms are clearly of value in potential position-location applications of orientable sequences — see, for example, [4, 16].

Devising such algorithms is left for future work. Other possible directions for future research include generalising the construction methods given in this paper, both to arbitrary size alphabets and to the multi-dimensional case.

Acknowledgements

References

[1] R. Berkowitz and S. Kopparty, *Robust positioning patterns*, Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10–12, 2016 (R. Krauthgamer, ed.), SIAM, 2016, pp. 1937–1951.

[2] A. M. Bruckstein, T. Etzion, R. Giryes, N. Gordon, R. J. Holt, and D. Shuldiner, *Simple and robust binary self-location patterns*, IEEE Trans. Inf. Theory **58** (2012), no. 7, 4884–4889.

[3] J. Burns and C. J. Mitchell, *Coding schemes for two-dimensional position sensing*, Tech. Report HPL–92–19, January 1992, `https://hplabs.itcs.hp.com/techreports/92/HPL-92-19.html`.

[4] _____, *Coding schemes for two-dimensional position sensing*, Cryptography and Coding III (M. J. Ganley, ed.), Oxford University Press, 1993, pp. 31–66.

[5] Y. M. Chee, D. T. Dao, H. M. Kiah, S. Ling, and H. Wei, *Binary robust positioning patterns with low redundancy and efficient locating algorithms*, Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6–9, 2019 (T. M. Chan, ed.), SIAM, 2019, pp. 2171–2184.

[6] _____, *Robust positioning patterns with low redundancy*, SIAM J. Comput. **49** (2020), no. 2, 284–317.

[7] F. Chung, P. Diaconis, and R. Graham, *Universal cycles for combinatorial structures*, Discrete Mathematics **110** (1992), 43–59.

[8] Z.-D. Dai, K. M. Martin, M. J. B. Robshaw, and P. R. Wild, *Orientable sequences*, Cryptography and Coding III (M. J. Ganley, ed.), Oxford University Press, Oxford, 1993, pp. 97–115.

[9] N. G. de Bruijn, *A combinatorial problem*, Proceedings Nederlandse Akademie van Wetenschappen **49** (1946), 758–764.

[10] T. Etzion, *The depth distribution — A new characterization for linear codes*, IEEE Transactions on Information Theory **43** (1997), 1361–1363.

[11] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Review **24** (1982), 195–221.

[12] S. W. Golomb, *Shift register sequences*, Holden-Day, San Francisco, 1967.

[13] I. J. Good, *Normally recurring decimals*, Journal of the London Mathematical Society **21** (1946), 167–169.

[14] B. Jackson, B. Stevens, and G. Hurlbert, *Research problems on Gray codes and universal cycles*, Discret. Math. **309** (2009), no. 17, 5341–5348.

[15] A. Lempel, *On a homomorphism of the de Bruijn graph and its application to the design of feedback shift registers*, IEEE Transactions on Computers **C-19** (1970), 1204–1209.

[16] C. J. Mitchell, T. Etzion, and K. G. Paterson, *A method for constructing decodable de Bruijn sequences*, IEEE Transactions on Information Theory **42** (1996), 1472–1478.

[17] E. M. Petriu, *Absolute-type position transducers using a pseudorandom encoding*, IEEE Transactions on Instrumentation and Measurement **IM-36** (1987), 950–955.

[18] J. Sawada, A. Williams, and D. C.-H. Wong, *Universal cycles for weight-range binary strings*, Combinatorial Algorithms — 24th International Workshop, IWOCA 2013, Rouen, France, July 10–12, 2013, Revised Selected Papers (T. Lecroq and L. Mouchard, eds.), Lecture Notes in Computer Science, vol. 8288, Springer, 2013, pp. 388–401.

[19] I. Szentandrási, M. Zachariás, J. Havel, A. Herout, M. Dubská, and R. Kajan, *Uniform marker fields: Camera localization by orientable De Bruijn tori*, 11th IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2012, Atlanta, GA, USA, November 5–8, 2012, IEEE Computer Society, 2012, pp. 319–320.