EasyChair Preprint

№ 9997

Orientable Sequences over Non Binary Alphabet

Abbas Alhakim, Chris Mitchell, Janusz Szmidt and Peter Wild

May 2, 2023

Orientable sequences over nonbinary alphabet

Abbas Alhakim, Chris J. Mitchell, Janusz Szmidt, Peter R. Wild

April 15, 2023

Abstract

We consider orientable sequences over residue group $\mathbb{Z}_q$. We prove properties of a generalized Lempel homomorphism and give an upper bound on periods of orientable sequences. We generalize the results of [6].

1 Introduction

For positive integers n and q greater than one let $\mathbb{Z}_q^n$ be the set of all q^n vectors of length n with entries in the group $\mathbb{Z}_q$ of residues modulo q. An order n de Bruijn sequence with alphabet in $\mathbb{Z}_q$ is a sequence that includes only once every possible string of size n as a subsequence of consecutive symbols. An order n de Bruijn digraph, $B_n(q)$, is a directed graph with $\mathbb{Z}_q^n$ as its vertex set and for two vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, $(\mathbf{x}; \mathbf{y})$ is an edge if and only if $y_i = x_{i+1}$ for all $i = 1$ to $n - 1$. We then say $\mathbf{x}$ is a predecessor of $\mathbf{y}$ and $\mathbf{y}$ is a successor of $\mathbf{x}$. Evidently, every vertex has exactly q successors and q predecessors. Furthermore, two vertices are conjugates if they have the same successors. A cycle in $B_n(q)$ is a path that starts and ends at the same vertex. It is called vertex disjoint if it does not visit any vertex more than once. Two cycles or two paths in the digraph are vertex disjoint if they do not have a common vertex. A cycle is primitive in $B_n(q)$ if it does not simultaneously contain a word and any of its translates. A function $d : \mathbb{Z}_q^n \to Z_q$ is said to be translation invariant if $d(w + \lambda) = d(w)$ for all $w \in \mathbb{Z}_q^n$ and all $\lambda \in \mathbb{Z}_q$. The weight $w(s)$ of a word or sequence s is the sum of all elements in s (not taken modulo q). Similarly, the weight of a cycle is the weight of the ring sequence that represents it. Obviously a de Bruijn sequence of order n defines a Hamiltonian cycle in $B_n(q)$, i.e., a cycle that visits each vertex exactly once and which we denote as a de Bruijn cycle.

For an integer $n > 1$ define a map $D : B_n(2) \to B_{n-1}(2)$ by

$$D(a_1, \ldots, a_n) = (a_1 + a_2, a_2 + a_3, \ldots, a_{n-1} + a_n)$$

where addition is modulo 2. This function defines a graph homomorphism and it is known as Lempel's D-morphism due to the fact that it was studied in [4].

We present a generalization to nonbinary alphabets [1]. For a nonzero $\beta \in \mathbb{Z}_q$, we define a function D_β from $B_n(q)$ to $B_{n-1}(q)$ as follows. For $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_{n-1})$, $D_\beta(a) = b$ if and only if $b_i = d_\beta(a_i, a_{i+1})$ for $i = 1$ to $n-1$, where $d_\beta(a_i, a_{i+1}) = \beta(a_{i+1} - a_i) \mod q$. Clearly D_β is translation invariant. It is also onto under a simple condition that $gcd(\beta, q) = 1$.

2 Orientable sequences

Definition 1
We define an n-window sequence $S = (s_i)$ (see, for example, [5]) to be a periodic 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 $s_n(i) = s_n(j)$ for some i, j, then $i = j \mod m$, where $s_n(i) = (s_i, s_{i+1}, \ldots, s_{i+n-1})$.

A de Bruijn sequence of order n over alphabet $\mathbb{Z}_q$ is then simply an n-window sequence of period q^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 $u = (u_0, u_1, \ldots, u_{n-1})$ is a q-ary n-tuple, i.e. if $u \in B_n(q)$, then $u^R = (u_{n-1}, u_{n-2}, \ldots, u_0)$ is its reverse. If a tuple u satisfies $u = u^R$ then we say it is symmetric. A translate of a tuple involves switching $u = (u_0, u_1, \ldots, u_{n-1}) \in B_n(q)$ to $\overline{u} = (u_0 + \lambda, u_1 + \lambda, \ldots, u_{n-1} + \lambda)$, where $\lambda \in \mathbb{Z}_q$. In a similar way, we refer to sequences being translates if one can be obtained from the other by an addition of a nonzero constant λ. We define the conjugate of an n-tuple to be the tuple obtained by switching the first bit, i.e. if $u = (u_0, u_1, \ldots, u_{n-1}) \in B_n(q)$, then the conjugate $\widehat{u}$ of u is the n-tuple $(u_0 + \lambda, u_1, \ldots, u_{n-1})$, where $\lambda \in \mathbb{Z}_q$.

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 $s_n(i) \neq t_n(j)$ 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 showing how two disjoint n-window sequences can be *joined* to create a single n-window sequence, if they contain conjugate n-tuples.

Lemma 1
Suppose $S = (s_i)$ and $T = (t_i)$ are disjoint n-window sequences of periods l and m respectively. Moreover suppose S and T contain the conjugate n-tuples u and v at positions i and j, respectively. Then

$$[s_0, s_1, \ldots, s_{i+n-1}, t_{j+n}, t_{j+n+1}, \ldots, t_{m-1}, t_0, \ldots, t_{j+n-1}, s_{i+n}, s_{i+n+1}, \ldots, s_{l-1}]$$

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

Definition 2
An n-window sequence $S = (s_i)$ of period m is said to be an q-orientable sequence of order n (an $\mathcal{OS}_q(n)$) if, for any i, j , $s_n(i) \neq s_n(j)^R$.

Definition 3
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, $s_n(i) \neq s'_n(j)^R$.

We extend the notation to allow the Lempel morphism D_β to be applied to periodic sequences in the natural way. That is, D_β is a map from the set of periodic sequences to itself; the image of a sequence of period m will clearly have period dividing m. In the natural way we can define D_β^{-1} to be the *inverse* of D_β, i.e. if S is a periodic sequence than $D_\beta^{-1}(S)$ is the set of all sequences T with the property that $D_\beta(T) = S$.

Theorem 1
Suppose $S = (s_i)$ is an orientable sequence of order n and period m with the property that

if $s_1, \ldots, s_n$ is a word in S then $-s_n, -s_{n-1}, \ldots, -s_1$ is not a word of S. $(*)$

Then
(a) If $w(S) = 0 \mod q$ then $D_\beta^{-1}(S)$ consists of an disjoin set of q primitive orientable sequences of order $n+1$ and period m satisfying the condition $(*)$.
(b) If $gcd(w(S), q) = 1$ than $D_\beta^{-1}(S)$ is one sequence made of q shifts $T_0, T_1, \ldots, T_{q-1}$, where $T_i = T_{i-1} + c$.

3 An upper bound

We present here the results from the paper [7]. We first introduce a special type of symmetry for q-ary n-tuples.

Definition 4
An n-tuple $u = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leq i \leq n-1)$, is m-symmetric for some $m \leq n$ if and only if $u_i = u_{m-1-i}$ for every i $(0 \leq i \leq m-1)$.

An n-tuple is simply said to be symmetric if it is n-symmetric. We also need the notions of uniformity and alternating.

Definition 5
An n-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leq i \leq n-1)$, is *uniform* if and only if $u_i = c$ for every i $(0 \leq i \leq n-1)$ for some $c \in \mathbb{Z}_q$. An n-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leq i \leq n-1)$, is *alternating* if and only if $u_0 = u_{2i}$ and $u_1 = u_{2i+1}$ for every i $(0 \leq i \leq \lfloor (n-1)/2 \rfloor)$, where $u_0 \neq u_1$.

We can then state the following elementary results.

Lemma 2
If $n \geq 2$ and $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ is a q-ary n-tuple that is both symmetric and $(n-1)$-symmetric, then $\mathbf{u}$ is uniform.

Lemma 3
If $n \geq 2$ and $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ is a q-ary n-tuple that is both symmetric and $(n-2)$-symmetric then either $\mathbf{u}$ is uniform or n is odd and $\mathbf{u}$ is alternating.

The following definition leads to a simple upper bound on the period of an $\mathcal{OS}_q(n)$.

Definition 6
Let $N_q(n)$ be the set of all non-symmetric q-ary n-tuples.

Clearly, if an n-tuple occurs in an $\mathcal{OS}_q(n)$ then it must belong to $N_q(n)$; moreover it is also immediate that $|N_q(n)| = q^n - q^{\lceil n/2 \rceil}$. Observing that all

the tuples in $\mathcal{OS}_q(n)$ and its reverse must be distinct, this immediately give the following well-known result.

Lemma 4 ([2])
The period of an $\mathcal{OS}_q(n)$ is at most $(q^n - q^{\lceil n/2 \rceil})/2$.

As a first step towards establishing our bound we need to define a special set of n-tuples, as follows.

Definition 7
Suppose $n \geq 2$, and that $\mathbf{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a q-ary $(n-r)$-tuple ($r \geq 1$). Then let $L_n(\mathbf{v})$ be the following set of q-ary n-tuples:

$$L_n(\mathbf{v}) = \{\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}) : \ u_i = v_i, \quad 0 \leq i \leq n-r-1\}.$$

That is $L_n(\mathbf{v})$ is simply the set of n-tuples whose first $n-r-1$ entries equal $\mathbf{v}$. Clearly, for fixed r, the sets $L_n(\mathbf{v})$ for all $(n-r)$-tuples $\mathbf{v}$ are disjoint. We have the following simple result.

Lemma 5
Suppose $\mathbf{v}$ and $\mathbf{w}$ are symmetric tuples of lengths $n-1$ and $n-2$, respectively, and they are not both uniform. Then

$$L_n(\mathbf{v}) \cup L_n(\mathbf{w}) = \emptyset.$$

We are particularly interested in how the sets $L_n(\mathbf{v})$ intersect with the sets of n-tuples occurring in either S or S^R, when S is an $\mathcal{OS}_q(n)$ and $\mathbf{v}$ is symmetric. To this end we make the following definition.

Definition 8
Suppose $n \geq 2$, $r \geq 1$, $S = (s_i)$ is an $\mathcal{OS}_q(n)$, and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a k-ary $(n-r)$-tuple. Then let

$$L_S(\mathbf{v}) = \{\mathbf{u} \in L_n(\mathbf{v}) : \ \mathbf{u} \text{ appears in } S \text{ or } S^R\}.$$

We can now state the first result towards deriving our bound.

Lemma 6
Suppose $n \geq 2$, $r \geq 1$, $S = (s_i)$ is an $\mathcal{OS}_q(n)$, and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a q-ary symmetric $(n-r)$-tuple. Then $|L_S(\mathbf{v})|$ is even.

That is, if $|L_n(\mathbf{v})|$ is odd, this shows that S and S^R combined must omit at least one of the n-tuples in $L_n(\mathbf{v})$. We can now state our main result.

Observe that, although the theorem below applies in the case $q = 2$, the bound is much weaker than the bound of Dai et al. [3] which is specific to the binary case. This latter bound uses arguments that only apply for $q = 2$. The fact that $q = 2$ is a special case can be seen by observing that, unlike the case for larger q, no string of $n-2$ consecutive zeros or ones can occur in an $\mathcal{OS}_d(n)$.

Theorem 2 (Generalization of Theorem from [3])
Suppose that $S = (s_i)$ is an $\mathcal{OS}_q(n)$ ($q \geq 2$, $n \geq 2$). Then the period of S is at most

$$\begin{array}{rl} (q^n - q^{\lceil n/2 \rceil} - q^{\lceil (n-1)/2 \rceil} + q)/2 & \text{if } q \text{ is odd,} \\ (q^n - q^{\lceil n/2 \rceil} - q)/2 & \text{if } q \text{ is even.} \end{array}$$

Table 1: Bounds on the period of an $\mathcal{OS}_q(n)$ (from Theorem 2)

Order	$q=2$	$q=3$	$q=4$	$q=5$
$n=2$	0	3	4	10
$n=3$	1	9	22	50
$n=4$	5	33	118	290
$n=5$	11	105	478	1490

We conclude by tabulating the values of the bounds of the above Theorem for small q and n.

We give an example of the sequence in $\mathcal{OS}_3(4)$: $S = 0001112$. Then in the notation of Theorem 1 (b):
$T_0 = \underline{0}\ 0\ 0\ 0\ 1\ 2\ 3\ \not{0}$
$T_1 = 1\ 1\ 1\ 1\ 2\ 3\ 4\ \not{1}$
$T_2 = 2\ 2\ 2\ 2\ 3\ 4\ 0\ \not{2}$
$T_3 = 3\ 3\ 3\ 3\ 4\ 0\ 1\ \not{3}$
$T_4 = 4\ 4\ 4\ 4\ 0\ 1\ 2\ \not{4}$

References

[1] A. Alhakim and M. Akinwande. A recursive construction of nonbinary de Bruijn sequences. Design, Codes and Cryptography. 60:155–169, (2011).

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

[3] 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, pp. 97–115, 1993.

[4] A. Lempel. On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers. IEEE Trans. Comput. C 19, 1204–1209 (1970).

[5] 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.

[6] C. J. Mitchell. and P. R. Wild. Constructing Orientable Sequences. IEEE Transations on Information Theory, Vol. 68, no. 7, July 2022.

[7] C. J. Mitchell. and P. R. Wild. Bounds on the period of k-ary orientable sequences. Preprint, January 2022.