Orientable sequences over nonbinary alphabets

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

September 2023

Notation

- 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 periodic sequence that includes every possible string of size n exactly once as a subsequence of consecutive symbols in one period of the sequence.
- 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.

Notation

- The order n de Bruijn digraph, $B_n(q)$, is a directed graph with $\mathbb{Z}_q^n$ as its vertex set and for any 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 every i $(1 \leqslant i < n)$.
- We then say that $\mathbf{x}$ 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 said to be conjugates if they have the same successors.
- 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 is known as Lempel's D-morphism since it was studied in [2].

Lempel D-morphism

- 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 if $gcd(\beta, q) = 1$.
- A cycle in $B_n(q)$ is primitive if it does not simultaneously contain a word and any of its translates.

Orientable sequences

- **Definition 1**
  We define an n-window sequence $S = (s_i)$ 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 $s_n(i) = (s_i, s_{i+1}, \ldots, s_{i+n-1})$.
- **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 , $s_n(i) \neq s_n(j)^R$, where $s_n(j)^R$ is the reverse of the word $s_n(j)$.
- **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, $s_n(i) \neq s'_n(j)^R$.

Orientable sequences

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 a disjoint set of q primitive orientable sequences of order $n+1$ and period m satisfying the condition $(*)$.

(b) If $gcd(w(S), q) = 1$ then $D_\beta^{-1}(S)$ is one sequence made of q shifts $T_0, T_1, \ldots, T_{q-1}$, where $T_i = T_{i-1} + c$.

An upper bound

- **Definition 4**
  An n-tuple $u = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leqslant i \leqslant n-1)$, is m-symmetric for some $m \leqslant n$ if and only if $u_i = u_{m-1-i}$ for every i $(0 \leqslant i \leqslant m-1)$.
- 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 $\mathrm{u} = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leqslant i \leqslant n-1)$, is *uniform* if and only if $u_i = c$ for every i $(0 \leqslant i \leqslant n-1)$ for some $c \in \mathbb{Z}_q$. An n-tuple $\mathrm{u} = (u_0, u_1, \ldots, u_{n-1})$, $u_i \in \mathbb{Z}_q$ $(0 \leqslant i \leqslant n-1)$, is *alternating* if and only if $u_0 = u_{2i}$ and $u_1 = u_{2i+1}$ for every i $(0 \leqslant i \leqslant \lfloor (n-1)/2 \rfloor)$, where $u_0 \neq u_1$.
- **Lemma 1**
  If $n \geqslant 2$ and $\mathrm{u} = (u_0, u_1, \ldots, u_{n-1})$ is a q-ary n-tuple that is both symmetric and $(n-1)$-symmetric, then u is uniform.

An upper bound

- **Lemma 2**
  If $n \geqslant 2$ and $\mathrm{u} = (u_0, u_1, \ldots, u_{n-1})$ is a q-ary n-tuple that is both symmetric and $(n-2)$-symmetric then either u is uniform or n is odd and u is alternating.
- **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 3** ([3])
  The period of an $\mathcal{OS}_q(n)$ is at most $(q^n - q^{\lceil n/2 \rceil})/2$.

An upper bound

- As a first step towards establishing our bound we need to define a special set of n-tuples, as follows.
- **Definition 7**
  Suppose $n \geqslant 2$, and that $\mathrm{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a q-ary $(n-r)$-tuple ($r \geqslant 1$). Then let $L_n(\mathrm{v})$ be the following set of q-ary n-tuples:

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

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

An upper bound

- **Lemma 4**
  Suppose v and w are symmetric tuples of lengths $n-1$ and $n-2$, respectively, and they are not both uniform. Then

$$L_n(\mathrm{v}) \cap L_n(\mathrm{w}) = \emptyset.$$

- We are particularly interested in how the sets $L_n(\mathrm{v})$ intersect with the sets of n-tuples occurring in either S or S^R, when S is an $\mathcal{OS}_q(n)$ and v is symmetric. To this end we make the following definition.
- **Definition 8**
  Suppose $n \geqslant 2$, $r \geqslant 1$, $S = (s_i)$ is an $\mathcal{OS}_q(n)$, and $\mathrm{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a k-ary $(n-r)$-tuple. Then let

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

An upper bound

- We can now state the first result towards deriving our bound.
- **Lemma 5**
  Suppose $n \geqslant 2$, $r \geqslant 1$, $S = (s_i)$ is an $\mathcal{OS}_q(n)$, and $\mathrm{v} = (v_0, v_1, \ldots, v_{n-r-1})$ is a q-ary symmetric $(n-r)$-tuple. Then $|L_S(\mathrm{v})|$ is even.
- That is, if $|L_n(\mathrm{v})|$ is odd, this shows that S and S^R combined must omit at least one of the n-tuples in $L_n(\mathrm{v})$. 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. [4], 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 $\mathcal{OS}_2(n)$.

An upper bound

- **Theorem 2** (Generalization of Theorem from [4])
  Suppose that $S = (s_i)$ is an $\mathcal{OS}_q(n)$ ($q \geqslant 2$, $n \geqslant 2$). Then the period of S is at most

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

- Table 1 provides the values of the bounds in the above theorem for small q and n.

Tabela 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

Bibliography

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