# A PASCAL-LIKE BOUND FOR THE NUMBER OF NECKLACES WITH FIXED DENSITY 

I. HECKENBERGER AND J. SAWADA


#### Abstract

A bound resembling Pascal's identity is presented for binary necklaces with fixed density using Lyndon words with fixed density. The result is generalized to $k$-ary necklaces and Lyndon words with fixed content. The bound arises in the study of Nichols algebras of diagonal type.


## 1. Introduction

A necklace is the lexicographically smallest word in an equivalence class of words under rotation ${ }^{1}$. A Lyndon word is a primitive necklace, which means that it is strictly smaller than any of its non-trivial rotations. The density of a binary word is the number of 1 s it contains. Let $\mathbf{N}(n, d)$ denote the set of all binary necklaces of length $n$ and density $d$. Similarly, let $\mathbf{L}(n, d)$ denote the set of all binary Lyndon words of length $n$ and density $d$. Let the cardinality of these two sets be denoted by $N(n, d)$ and $L(n, d)$, respectively. The following formulae are well-known for any $n \geq 1$ and $0 \leq d \leq n$ (see [4] and [10, Sect. 2]):

$$
N(n, d)=\frac{1}{n} \sum_{j \mid \operatorname{gcd}(n, d)} \phi(j)\binom{n / j}{d / j}, \quad L(n, d)=\frac{1}{n} \sum_{j \mid \operatorname{gcd}(n, d)} \mu(j)\binom{n / j}{d / j},
$$

where $\phi$ and $\mu$ denote Euler's totient function and the Möbius function, respectively. Note that $N(n, d)=N(n, n-d)$ and $L(n, d)=L(n, n-d)$. Our main result is to prove the following Pascal's identity-like bound on $N(n, d)$.

Theorem 1.1. For any $0<d<n$,

$$
N(n, d) \leq L(n-1, d)+L(n-1, d-1) .
$$

Bounds on necklaces and Lyndon words like the one presented in the above theorem are generally difficult to prove directly from their enumeration formulae. Previous bounds on these objects used in algorithm analysis [10] use a combinatorial-style proof, and that is the approach we follow in this paper. To prove this theorem, we actually show something stronger. Let $\Sigma_{k}=$

[^0]$\{0,1,2, \ldots, k-1\}$ denote an alphabet of size $k$. Let $\mathbf{W}_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$ denote the set of all words over $\Sigma_{k}$ where each symbol $i$ appears precisely $n_{i}$ times. Such a set is said to be a set with fixed content, as used by [1, Sect. 18.3.3]. In a similar manner let $\mathbf{N}_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$ denote the set of necklaces with the given fixed content and let $\mathbf{L}_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$ denote the set of Lyndon words with the given fixed content. Let the cardinality of these two sets be denoted by $N_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$ and $L_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$, respectively. In [4] and [10, Sect. 2], explicit formulas for the number of necklaces and Lyndon words with fixed content are given:
\[

$$
\begin{aligned}
& N_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)=\frac{1}{n} \sum_{j \mid \operatorname{gcd}\left(n_{0}, \ldots, n_{k-1}\right)} \phi(j) \frac{(n / j)!}{\left(n_{0} / j\right)!\cdots\left(n_{k-1} / j\right)!}, \\
& L_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)=\frac{1}{n} \sum_{j \mid \operatorname{gcd}\left(n_{0}, \ldots, n_{k-1}\right)} \mu(j) \frac{(n / j)!}{\left(n_{0} / j\right)!\cdots\left(n_{k-1} / j\right)!},
\end{aligned}
$$
\]

where $n=n_{0}+n_{1}+\cdots+n_{k-1}$. In Section 3, we prove the following more general result.

Theorem 1.2. Let $k \geq 2$ and $n_{0}, n_{1}, \ldots, n_{k-1} \geq 1$ be positive integers. Then

$$
N_{k}\left(n_{0}, \ldots, n_{k-1}\right) \leq \sum_{i=0}^{k-1} L_{k}\left(n_{0}, \ldots, n_{i-1}, n_{i}-1, n_{i+1}, \ldots, n_{k-1}\right) .
$$

Moreover, the inequality is strict if $k>2$.
Observe that when $k=2$, Theorem 1.2 simplifies to Theorem 1.1. After presenting some preliminary materials in Section 2, we prove the theorems in Section 3. For more background on Lyndon words see [6].
1.1. An Application. The inequalities in Theorems 1.1 and 1.2 seem to be new. They arised with the study of Nichols algebras of diagonal type in [5] in order to determine whether such a Nichols algebra is a free algebra. Roughly, the inequality implies that a certain rational function is in fact a polynomial, and freeness of the Nichols algebra holds if none of these polynomials vanish at the point of an affine space determined by the braiding of the Nichols algebra. The calculation of the zeros of such a polynomial simplifies significantly if the inequality is known to be strict. Strictness when $k=2$ is further discussed in Section 4.

## 2. Background

A word is called a prenecklace, if it is the prefix of some necklace. For any non-empty word $\alpha$ let $|\alpha|$ denote the length of $\alpha$ and let lyn $(\alpha)$ be the length of the longest prefix of $\alpha$ that is a Lyndon word. The following observation
is applied implicitly in many necklace algorithms including the ones from [2]. It is an extension of the classical property stated by Duval [3, P. 380] that every necklace has the form $\beta^{t}$ where $\beta$ is a Lyndon word and $t \geq 1$.

Lemma 2.1. Let $\alpha=a_{1} a_{2} \cdots a_{n}$ be a prenecklace with $p=\operatorname{lyn}(\alpha)$. Then $\alpha$ is a necklace if and only if $n \bmod p=0$.

Proof. Suppose $\alpha$ is a necklace. We know that $\alpha$ has the form $\beta^{t}$ for some Lyndon word $\beta$ and some $t \geq 1$. Since $p=\operatorname{lyn}(\alpha),|\beta| \leq p$. If $|\beta|=p$ then we are done. Otherwise $\beta=a_{1} a_{2} \cdots a_{q}$ for some $q<p$. Thus $a_{1} a_{2} \cdots a_{p}=$ $\left(a_{1} a_{2} \cdots a_{q}\right)^{j} a_{1} a_{2} \cdots a_{i}$ for some $j \geq 1$ and $1 \leq i<q$. However, since $\beta$ is a Lyndon word, $a_{1} a_{2} \cdots a_{q}<a_{i+1} \cdots a_{q} a_{1} a_{2} \cdots a_{i}$. But this implies that $a_{1} a_{2} \cdots a_{i}\left(a_{1} a_{2} \cdots a_{q}\right)^{j}<a_{1} a_{2} \cdots a_{p}$, which contradicts $a_{1} a_{2} \cdots a_{p}$ being a Lyndon word. Now suppose $n \bmod p=0$. Since $a_{1} a_{2} \cdots a_{p}$ is a Lyndon word, we clearly have that $\alpha$ is less than or equal to any of its rotations, and hence is a necklace.

The following theorem was named the Fundamental theorem of necklaces by Ruskey and a proof of the theorem is presented in [9] which builds on a foundation of results from Duval [3]. There is a similar statement by Reutenauer [8] on page 164.

Theorem 2.2. [2, Thm. 2.1] Let $\alpha=a_{1} \cdots a_{n-1}$ be a prenecklace over the alphabet $\Sigma_{k}$, where $n, k \geq 2$. Let $p=\operatorname{lyn}(\alpha)$ and let $b \in \Sigma_{k}$. Then $\alpha b$ is a prenecklace if and only if $a_{n-p} \leq b$. In this case,

$$
\operatorname{lyn}(\alpha b)= \begin{cases}p & \text { if } b=a_{n-p} \\ n & \text { if } b>a_{n-p}\end{cases}
$$

Corollary 2.3. If $\alpha=a_{1} a_{2} \cdots a_{n}$ is a prenecklace and $b>a_{n}$, then the word $a_{1} a_{2} \cdots a_{n-1} b$ is a Lyndon word.

Proof. Since $\alpha$ is a prenecklace, then so is $a_{1} a_{2} \cdots a_{n-1}$. From Theorem 2.2, we have $a_{n-p} \leq a_{n}$ since $\alpha$ is a prenecklace. Since $a_{n}<b$ then $a_{n-p}<b$ and thus Theorem 2.2 implies that $a_{1} a_{2} \cdots a_{n-1} b$ is a Lyndon word.

Corollary 2.4. If $\alpha=a_{1} a_{2} \cdots a_{n}$ is a necklace and $b>a_{1}$, then $\alpha b$ is a Lyndon word.

Proof. Let $p=\operatorname{lyn}(\alpha)$. By Lemma 2.1, $n \bmod p=0$. Since $\alpha$ is a prenecklace, Theorem 2.2 implies that $\alpha b$ is a Lyndon word since $b>a_{1}=$ $a_{n+1-p}$.

The following result follows from inductively applying Theorem 2.2 and corresponds to [2, Lem. 2.3].

Corollary 2.5. Let $\alpha=a_{1} a_{2} \cdots a_{n}$ be a prenecklace with $p=\operatorname{lyn}(\alpha)<n$, that is, $\alpha$ is not a Lyndon word. Then $\alpha=\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{i}$ for some $j \geq 1$ and $1 \leq i \leq p$.

The following remark follows directly from the definition of a necklace.
Remark 2.6. Every necklace over $\Sigma_{k}$ that contains a 0 and a non-0 element must begin with 0 and end with a non- 0 .

## 3. Proof of Main Theorems

A necklace $\alpha=a_{1} a_{2} \cdots a_{n}$ is said to be stable if $a_{1} a_{2} \cdots a_{n-1}$ is a Lyndon word; otherwise $\alpha$ is unstable. We prove Theorem 1.2, which generalizes Theorem 1.1, by partitioning $\mathbf{N}_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$ into two sets $\mathbf{S}$ and $\mathbf{U}$, which contain the stable and unstable necklaces of $\mathbf{N}_{k}\left(n_{0}, n_{1}, \ldots, n_{k-1}\right)$, respectively.

Lemma 3.1. Let $k \geq 2$ and $n_{0}, n_{1}, \ldots, n_{k-1} \geq 1$ be positive integers. Then

$$
|\mathbf{S}|=\sum_{i=1}^{k-1} L_{k}\left(n_{0}, \ldots, n_{i-1}, n_{i}-1, n_{i+1}, \ldots, n_{k-1}\right)
$$

Proof. Since each $n_{i}>0$, by Remark 2.6 every necklace in $\mathbf{S}$ must begin with 0 and end with a non- 0 . By partitioning $\mathbf{S}$ by its last symbol, the result follows from Corollary 2.4 and the definition of stable.

It remains to show that $|\mathbf{U}| \leq L_{k}\left(n_{0}-1, n_{1}, n_{2}, \ldots, n_{k-1}\right)$. We assume $k \geq 2$ and each $n_{i} \geq 1$. Let $\alpha=a_{1} a_{2} \cdots a_{n}$ be a necklace in U. From Remark 2.6, $a_{1}=0$ and $a_{n}>0$. Let $\alpha^{\prime}=a_{1} a_{2} \cdots a_{n-1}$ and let $x=a_{n}$. Since $\alpha$ is unstable, $\alpha^{\prime}$ is a prenecklace, but not a Lyndon word. Thus, applying Corollary 2.5, we can write $\alpha^{\prime}$ as $\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{i}$ where $j \geq 1$ and $1 \leq i \leq p$. For the upcoming function $f$, we define $z$, which we call the index of $\alpha$ associated with $f$, to be the largest index no more than $i$ such that $a_{z}=0$. Such an index exists since $a_{1}=0$. Thus

$$
\alpha=\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{z-1} a_{z} a_{z+1} a_{z+2} \cdots a_{i} x
$$

Consider the function $f: \mathbf{U} \rightarrow \mathbf{L}_{k}\left(n_{0}-1, n_{1}, n_{2}, \ldots, n_{k-1}\right)$ as follows:

$$
f(\alpha)= \begin{cases}\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{z-1} x & \text { if } z=i \\ \left(a_{1} a_{2} \cdots a_{p}\right)^{j} x a_{i} a_{i-1} \cdots a_{z+2} a_{1} a_{2} \cdots a_{z-1} a_{z+1} & \text { if } z<i\end{cases}
$$

Clearly $f(\alpha)$ has the required content. To see that $f(\alpha)$ is a Lyndon word, consider two cases depending on $z$. Suppose $z=i$. As stated earlier, $\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{z}=\alpha^{\prime}$ is a prenecklace. Thus since $x>a_{z}$, $\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{z-1} x$ is a Lyndon word by Corollary 2.3. Suppose $z<i$. Note that $\left(a_{1} a_{2} \cdots a_{p}\right)^{j}$ is a necklace and $a_{1}=0$. Since each symbol in $x a_{i} a_{i-1} \cdots a_{z+2}$ is non- $0, \beta=\left(a_{1} a_{2} \cdots a_{p}\right)^{j} x a_{i} a_{i-1} \cdots a_{z+2}$ is a Lyndon
word by Corollary 2.4. Observe that $\beta a_{1} a_{2} \cdots a_{z}$ is a prenecklace, since it is a prefix of the necklace $\beta^{2}$. Thus, since $a_{z+1}>0$ from the definition of $z$ and $a_{z}=0$, Corollary 2.3 implies $\beta a_{1} a_{2} \cdots a_{z-1} a_{z+1}$ is a Lyndon word. Hence $f(\alpha)$ is a Lyndon word.

Lemma 3.2. Let $k \geq 2$ and $n_{0}, n_{1}, \ldots, n_{k-1}$ be positive integers. Then

$$
|\mathbf{U}| \leq L_{k}\left(n_{0}-1, n_{1}, n_{2}, \ldots, n_{k-1}\right) .
$$

Proof. We prove that $f$ is one-to-one. Consider necklaces $\alpha$ and $\beta$ in $\mathbf{U}$. Set:

$$
\begin{aligned}
\alpha & =\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{z-1} a_{z} a_{z+1} a_{z+2} \cdots a_{i} x \\
\beta & =\left(b_{1} b_{2} \cdots b_{p^{\prime}}\right)^{j^{\prime}} b_{1} b_{2} \cdots b_{z^{\prime}-1} b_{z^{\prime}} b_{z^{\prime}+1} b_{z^{\prime}+2} \cdots b_{i^{\prime}} x^{\prime}
\end{aligned}
$$

where $z$ (resp. $z^{\prime}$ ) is the index of $\alpha$ (resp. of $\beta$ ) associated with $f$. Suppose $f(\alpha)=f(\beta)$. If $j p=j^{\prime} p^{\prime}$, then $p=p^{\prime}$ since both $a_{1} a_{2} \cdots a_{p}$ and $b_{1} b_{2} \cdots b_{p^{\prime}}$ are Lyndon words. If $p=p^{\prime}$ then clearly $\alpha=\beta$ by the definition of $f$. This means that $p \neq j^{\prime} p^{\prime}$ and $p^{\prime} \neq j p$. Thus, without loss of generality assume that $j p<j^{\prime} p^{\prime}$. Suppose $p<p^{\prime}<j p$, which implies $j>1$. But this implies there exists $1 \leq h<j$ and $0<t \leq p$ such that $b_{1} b_{2} \cdots b_{p^{\prime}}=$ $\left(a_{1} a_{2} \cdots a_{p}\right)^{h} a_{1} a_{2} \cdots a_{t}$ which contradicts $b_{1} b_{2} \cdots b_{p^{\prime}}$ being a Lyndon word. By a similar argument we cannot have $p^{\prime}<p<j^{\prime} p^{\prime}$. Thus $j p<p^{\prime}$, which by the definition of $f$, implies $j^{\prime}=1$ and $a_{1} a_{2} \cdots a_{p}=b_{1} b_{2} \cdots b_{p}$. Consider two cases based on $\ell=\left|a_{z+2} \cdots a_{i} x\right|$.
(i) Suppose $j p+\ell \geq p^{\prime}>j p$. This implies $\ell>0$. Let $\ell^{\prime}=\left|b_{z^{\prime}+2} \cdots b_{i^{\prime}} x^{\prime}\right|$. Recall $a_{1}=b_{1}=0$ and each letter of $a_{z+1} \cdots a_{i} x$ and $b_{z^{\prime}+1} \cdots b_{i^{\prime}} x^{\prime}$ is non- 0 . Thus, since $f(\alpha)=f(\beta)$, we must have $j p+\ell=p^{\prime}+\ell^{\prime}$, which means $z=z^{\prime}$. But this means $x^{\prime}=a_{i^{\prime}+1}=b_{i^{\prime}+1}$, which means that $\beta$ ends with $b_{1} b_{2} \cdots b_{i^{\prime}+1}$ which is a proper prefix of $b_{1} b_{2} \cdots b_{p^{\prime}}$. Since $i^{\prime}+1<p^{\prime}$ we have $n \bmod p^{\prime} \neq 0$ and thus Lemma 2.1 implies that $\beta$ is not a necklace, a contradiction.
(ii) Suppose $j p+\ell<p^{\prime}$. In this case, for $f(\alpha)=f(\beta)$, it must be that some suffix of $b_{1} b_{2} \cdots b_{p^{\prime}}$ is a prefix of $a_{1} a_{2} \cdots a_{z-1}=b_{1} b_{2} \cdots b_{z-1}$ which contradicts $b_{1} b_{2} \cdots b_{p^{\prime}}$ being a Lyndon word.

Together Lemma 3.1 and Lemma 3.2 prove Theorem 1.1. To complete the proof of Theorem 1.2, the following lemma proves that for $k>2$ the function $f$ is not a bijection.

Lemma 3.3. The function $f$ is not a surjection when $k>2$.
Proof. We consider two cases depending on the parity of $n_{0}$. For each case we demonstrate a word $\gamma$ in $\mathbf{L}_{k}\left(n_{0}-1, n_{1}, n_{2}, \ldots, n_{k-1}\right)$ that is not in the
range of $f$. Consider $\alpha \in \mathbf{U}$ and let $\gamma=f(\alpha)$. Observe that since $k>2$, the shortest prefix $u$ of $\gamma=u v$ containing two different symbols is also a prefix of $\alpha$. Moreover, if $v$ ends with $0^{j} t$, with $j \geq 0$ and $t \in\{1,2, \ldots, k-1\}$, then $0^{j+1} t$ is a subword of $\alpha$.

- Case 1: $n_{0}=2 j+1$ for $j \geq 0$. There is no necklace in $\mathbf{U}$ that maps to the Lyndon word $0^{j} 1^{n_{1}} 2^{n_{2}} \cdots(k-1)^{n_{k-1}-1} 0^{j}(k-1)$ because such a necklace would have to start with $0^{j} 1$ but have the subword $0^{j+1}$.
- Case 2: $n_{0}=2 j$ for $j \geq 1$. There is no necklace in $\mathbf{U}$ that maps to the Lyndon word $0^{j}(k-1)^{n_{k-1}} \cdots 3^{n_{3}} 2^{n_{2}} 1^{n_{1}-1} 0^{j-1} 1$ because such a necklace would have to start with $0^{j}(k-1)$ but have the subword $0^{j} 1$.


## 4. Special Cases When $N(n, d)=L(n-1, d)+L(n-1, d-1)$

In this section we discuss when the inequality given by Theorem 1.1 is equality. Recall that the density $d$ of a binary word is the number of 1 s it contains.

Lemma 4.1. If $d \in\{1,2, n-2, n-1\}$ and $0<d<n$ then $N(n, d)=$ $L(n-1, d)+L(n-1, d-1)$ except for $(n, d)=(2,1)$.

Proof. Recall that $N(n, d)=N(n, n-d)$ and $L(n, d)=L(n, n-d)$. Thus it suffices to prove the result for $d=1$ and $d=2$. For $d=1$ and $n>2$, $\mathbf{N}(n, 1)=\left\{0^{n-1} 1\right\}, \mathbf{L}(n-1,1)=\left\{0^{n-2} 1\right\}$, and $\mathbf{L}(n-1,0)=\emptyset$, and thus the result holds. For $d=2$, consider the parity of $n$. If $n$ is even, then $\mathbf{L}(n, 2)=\left\{0^{n-j-2} 10^{j} 1 \left\lvert\, j \in\left\{0,1, \ldots, \frac{n-2}{2}-1\right\}\right.\right\}$ and $\mathbf{N}(n, 2)=\mathbf{L}(n, 2) \cup$ $\left\{0^{(n-2) / 2} 10^{(n-2) / 2} 1\right\}$. If $n$ is odd, then $\mathbf{N}(n, d)=\mathbf{L}(n, 2)=\left\{0^{n-j-2} 10^{j} 1 \mid j \in\right.$ $\left.\left\{0,1, \ldots, \frac{n-3}{2}\right\}\right\}$. Thus, $N(n, 2)=\left\lfloor\frac{n}{2}\right\rfloor, L(n-1,2)=\left\lfloor\frac{n-2}{2}\right\rfloor$, and $L(n-1,1)=$ 1 , and therefore the result holds.

We now consider the other values of $d$.

Lemma 4.2. If $2<d<n-2$ then $N(n, d)=L(n-1, d)+L(n-1, d-1)$ if and only if $(n, d) \in\{(6,3),(7,3),(7,4),(8,4),(9,3),(9,6)\}$.

Proof. The claim can be verified directly from the enumeration formulae for $n \leq 10$. A table of relevant values for $N(n, d)($ resp. $L(n, d))$ are provided in the left (resp. right) table below.

| $n / d$ | 3 | 4 | 5 | 6 | 7 |
| ---: | ---: | ---: | ---: | ---: | ---: |
| 6 | $\mathbf{4}$ |  |  |  |  |
| 7 | $\mathbf{5}$ | $\mathbf{5}$ |  |  |  |
| 8 | 7 | $\mathbf{1 0}$ | 7 |  |  |
| 9 | $\mathbf{1 0}$ | 14 | 14 | $\mathbf{1 0}$ |  |
| 10 | 12 | 22 | 26 | 22 | 12 |


| $n / d$ | 2 | 3 | 4 | 5 | 6 | 7 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 5 | 2 | 2 |  |  |  |  |
| 6 | 2 | 3 | 2 |  |  |  |
| 7 | 3 | 5 | 5 | 3 |  |  |
| 8 | 3 | 7 | 8 | 7 | 3 |  |
| 9 | 4 | 9 | 14 | 14 | 9 | 4 |

For $n>10$, let $z=n-d$ (the number of $0 s$ ). Recall that $N(n, d)=$ $N(n, n-d)$ and $L(n, d)=L(n, n-d)$. Thus, if $N(n, d)=L(n-1, d)+$ $L(n-1, d-1)$ then $N(n, n-d)=L(n-1, n-d)+L(n-1, n-(d-1))$. Thus, we can assume $2<z \leq n / 2$. Consider three cases for $z=3, z=4$, and $z \geq 5$. Each result is proved by specifying a Lyndon word $\beta \in \mathbf{L}(n-1, d)=$ $\mathbf{L}_{2}(z-1, d)$ not in the range of $f$ when the domain is the set of unstable necklaces in $\mathbf{N}(n, d)=\mathbf{N}_{2}(z, d)$.

- Case: $z=3$. Depending on the parity of $n$ let $\beta$ be either $01^{t} 01^{t+1}$ or $01^{t} 01^{t+2}$. Since $n>10$, we have $t \geq 3$. Consider any necklace $\alpha$ in $\mathbf{N}_{2}(3, d)$ which can be written as $01^{t_{1}} 01^{t_{2}} 01^{t_{3}}$ for non-negative integers $t_{1}, t_{2}, t_{3}$. Note that if $t_{2}<t_{1}$ then the the rotation of $\alpha$ starting with $01^{t_{2}}$ is less than $\alpha$, a contradiction to $\alpha$ being a necklace. Similarly for $t_{3}$. Thus, $t_{2}, t_{3} \geq t_{1}$. But for any such (unstable) $\alpha, f(\alpha)=01^{t_{1}} 01^{t_{2}+t_{3}} \neq \beta$.
- Case: $z=4$. Depending on the value of $(n \bmod 3)$ let $\beta$ be one of the words $01^{t} 01^{t} 01^{t+1}, 01^{t} 01^{t+1} 01^{t+1}$, and $01^{t} 01^{t+1} 01^{t+2}$. Since $n>10$, we have $t \geq 2$. Consider any unstable necklace $\alpha=a_{1} a_{2} \cdots a_{n}$ in $\mathbf{N}_{2}(4, d)$ which can be written as $01^{t_{1}} 01^{t_{2}} 01^{t_{3}} 01^{t_{4}}$ for non-negative integers $t_{1}, t_{2}, t_{3}, t_{4}$. Again, observe that if $t_{2}<t_{1}$ then the rotation of $\alpha$ starting with $01^{t_{2}}$ is less than $\alpha$, a contradiction to $\alpha$ being a necklace. Similarly for $t_{3}, t_{4}$. Thus, $t_{2}, t_{3}, t_{4} \geq t_{1}$. Moreover, since $n>10$, if $t_{4}=1$ then at least one of $t_{1}$ or $t_{2}$ or $t_{3}$ is greater than one which similarly contradicts $\alpha$ being a necklace as the rotation starting with $01^{t_{4}}$ will be less than $\alpha$. Thus $t_{4}>1$. Recall we can write $\alpha$ as $\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{i} x$ where $x=1, j \geq 1$, and $1 \leq i \leq p$ where $p$ is the length of the longest Lyndon prefix of $a_{1} a_{2} \cdots a_{n-1}$. Since clearly $a_{1}=0$ and $a_{p}=1, p \in\left\{t_{1}+1, t_{1}+t_{2}+2, t_{1}+t_{2}+t_{3}+3\right\}$. If $p=t_{1}+1$ then $j=3$ and $t_{1}=t_{2}=t_{3}$ by the definition of $p$. However then $f(\alpha)=01^{t_{1}} 01^{t_{1}} 01^{t_{1}+t_{4}}$ which is not equal to any possible $\beta$. If $p=t_{1}+t_{2}+2$ then $t_{1}=t_{3}$ and $t_{2}>t_{1}$ by the definition of $p$, and thus $t_{2}>t_{3}$. However, then $f(\alpha)=01^{t_{1}} 01^{t_{2}+t_{4}-1} 01^{t_{3}+1}$ which is not equal to any possible $\beta$. Finally, if $p=t_{1}+t_{2}+t_{3}+3$ then $t_{3}>t_{1}$ by the definition of $p$. However, then $f(\alpha)=01^{t_{1}} 01^{t_{2}} 01^{t_{3}+t_{4}}$ which is also not equal to any possible $\beta$.
- Case: $z \geq 5$. Recall $n>10$ and $z \leq n / 2$. Consider the length $n-1$ word $\beta=0011^{s} 01(01)^{t}$ where $t=z-4$ and $s=n-2 t-6$. Since $z \geq 5$, we have $t \geq 1$ and since $z \leq n / 2$, we have $s>0$. Clearly $\beta$ is a Lyndon word and it has $z-10$ s. Now suppose there exists an unstable necklace $\alpha=a_{1} a_{2} \cdots a_{n}$ in $\mathbf{N}_{2}(z, d)$ such that $f(\alpha)=\beta$. Recall we can write $\alpha$ as $\left(a_{1} a_{2} \cdots a_{p}\right)^{j} a_{1} a_{2} \cdots a_{i} x$ where $x=1, j \geq 1$, and $1 \leq i \leq p$. As noted earlier, if $\beta$ begins with 001 , then so must $\alpha$. Thus $a_{1} a_{2} a_{3}=001$. Consider $z^{\prime}$, the index of $\alpha$ associated with $f$. If $z^{\prime}>2$, then $f(\alpha)$ must have two subwords of the form 001 and hence is not equal to $\beta$. Otherwise $z^{\prime}=2$. If $i=z^{\prime}$ then $\alpha$ ends with 001. In order for $f(\alpha)=\beta, \alpha$ must begin with 0011 . However this contradicts $\alpha$ being a necklace because the rotation starting with its suffix 001 will be less than $\alpha$. Thus $z^{\prime}=2<i$. This means that $a_{1}=0, a_{2}=0$, and each of $a_{3}, a_{4}, \ldots, a_{i}, x$ is 1 . Thus, from the definition of $f, f(\alpha)$ must end 1101 which contradicts $\beta$ ending with 0101.


## 5. Acknowledgements

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), RGPIN-2018-04211.

## References

[1] J. Arndt. Matters computational. Ideas, algorithms, source code. Springer, Berlin, Heidelberg, 2011.
[2] K. Cattell, F. Ruskey, J. Sawada, M. Serra, and C. R. Miers. Fast algorithms to generate necklaces, unlabeled necklaces, and irreducible polynomials over GF(2). J. Algorithms, 37(2):267-282, 2000.
[3] J. P. Duval. Factorizing words over an ordered alphabet. Journal of Algorithms, 4(4):363-381, 1983.
[4] E. N. Gilbert and J. Riordan. Symmetry types of periodic sequences. Illinois J. Math., 5:657-665, 1961.
[5] I. Heckenberger and Y. Zheng. A characterization of Nichols algebras of diagonal type which are free algebras. In preparation, 2018.
[6] M. Lothaire. Algebraic Combinatorics on Words. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2002.
[7] D. Perrin and A. Restivo. Words, Chapter 8 in Handbook of Enumerative Combinatorics. Discrete Mathematics and Its Applications Series, Champan and Hall/CRC, 2015.
[8] C. Reutenauer. Free Lie Algebras. London Mathematical Society Monographs 7, Oxford Science Publications, 1993.
[9] F. Ruskey. Combinatorial Generation. Working version (1j) edition, 2003.
[10] F. Ruskey and J. Sawada. An efficient algorithm for generating necklaces with fixed density. SIAM J. Comput., 29(2):671-684, 1999.

Philipps Universität Marburg, Fachbereich Mathematik und Informatik, Hans-Meerwein-Str., 35032 Marburg, GERMANY

Email address: heckenberger@mathematik.uni-marburg.de
School of Computer Science, University of Guelph, Canada
Email address: jsawada@uoguelph.ca


[^0]:    ${ }^{1} \mathrm{~A}$ necklace is often thought to be an equivalence class of words under rotation. Here we use the term to identify each such class with its minimal word $[7]$.

