# The Discrepancy of the Lex-Least De Bruijn Sequence 

Joshua Cooper ${ }^{1}$<br>University of South Carolina<br>Christine Heitsch ${ }^{2}$.<br>Georgia Institute of Technology


#### Abstract

We answer the following question of R. L. Graham: What is the discrepancy of the lexicographically-least binary de Bruijn sequence? Here, "discrepancy" refers to the maximum (absolute) difference between the number of ones and the number of zeros in any initial segment of the sequence. We show that the answer is $\Theta\left(2^{n} \log n / n\right)$.


Key words: De Bruijn sequence, Ford sequence, discrepancy, greedy algorithm 2000 MSC: 05A16

## 1. Introduction

A binary de Bruijn sequence of order $k$ is a word $a_{1} \cdots a_{2^{k}}$ over the alphabet $\{0,1\}$ that contains every $k$-word exactly once as a subword when the indices are interpreted cyclically. It is well known (see, e.g., [7]) that the number of de Bruijn cycles of order $k$ is given by

$$
2^{2^{k-1}-k}
$$

Among these is the "Ford sequence" ${ }^{3}$, the remarkable cyclic binary word which is

1. the lexicographic least de Bruijn sequence,
2. the result of applying the least-first greedy algorithm to constructing a de Bruijn sequence (starting with $1^{k}$ ),

[^0]3. the result of concatenating all "Lyndon" words (lexicographically minimal representatives of free conjugacy classes) of each length dividing $k$ in lexicographic order, and
4. the de Bruijn sequence generated by a shift register whose truth table has minimum weight.

Since the greedy algorithm uses 0's before 1's whenever possible, it is natural to suspect that this special sequence has an excess of 0's early on, i.e, the difference between the number of 0's and 1's in initial segments is large. Indeed, Huang comments in [5] that

The "prefer one" algorithm proposed by Fredricksen joins the pure cycles of [a] circulating register (CR) in order according to the weights of the $n$-tuples... so some part of the sequence may contain many heavily weighted $n$-tuples and it leads to a bad local 0-1 balance.
R. L. Graham therefore asks for the maximum "discrepancy." In the present note, we show that it has order $2^{n} \log n / n$.

Define the equivalence relation $\sim$ ("conjugacy") on binary words by setting $x y \sim y x$ for any $x, y \in\{0,1\}^{*}$. For a word $w \in\{0,1\}^{*}$, define $w^{\circ}$ to be the lexicographic least element of the $\sim$-equivalence class $\llbracket w \rrbracket$ of $w$. If $w$ is aperiodic (i.e., if $w=x y$ with $x, y \neq \epsilon$, then $w \neq y x$ ), then $w^{\circ}$ is called a "Lyndon word." Then the lexicographically least binary order-n de Bruijn sequence $\mathcal{L}_{n}$ consists of the concatenation of all Lyndon words of length dividing $n$, in lexicographic order.

For a word $w \in\{0,1\}^{*}$, write $w_{k}$ for its $k^{\text {th }}$ symbol from left to right, starting with zero. Then we define the discrepancy of $w$ to be

$$
\operatorname{disc}(w)=\max _{M}\left|\sum_{k=0}^{M}(-1)^{w_{k}}\right| .
$$

Theorem 1. $\operatorname{disc}\left(\mathcal{L}_{n}\right)=\Theta\left(2^{n} \log n / n\right)$.
We conjecture a slightly stronger statement:
Conjecture 1. There is some $C$ so that $\lim _{n \rightarrow \infty} \frac{n \operatorname{disc}\left(\mathcal{L}_{n}\right)}{2^{n} \log n}=C$.
Our argument will estimate the discrepancy of $\mathcal{L}_{n}$ by considering substrings consisting of Lyndon words $w^{\circ}$ grouped by the length $k$ of their $0^{k} 1$ prefix. For $0<k<n$, let $S_{k}$ be the set of binary words of length $n$ containing the subword $0^{k}$ but not the subword $0^{k+1}$. Then the elements of $S_{k}$ are precisely those $w$ so that $w^{\circ}$ begins with $0^{k}$. Define $S_{k}^{\circ}=\left\{w^{\circ}: w \in S_{k}\right\}$, and let $\ell_{k}$ be the concatenation of the elements of $S_{k}^{\circ}$ in lexicographic order. Since the elements of $S_{k}^{\circ}$ precede those of $S_{k-1}^{\circ}$ in the lexicographic order, this means that

$$
\mathcal{L}_{n}=0 \cdot\left(\prod_{k=1}^{n-1} \ell_{n-k}\right) \cdot 1
$$

as long as $n$ is prime.
For a binary string $w$ of length $n$, we define the skew of $w$ to be

$$
\operatorname{sk}(w)=\sum_{i=0}^{n-1}(-1)^{w_{i}}
$$

so that

$$
\operatorname{disc}\left(\mathcal{L}_{n}\right)=\max _{1 \leq t \leq n-2}\left(1+\sum_{k=1}^{t} \operatorname{sk}\left(\ell_{n-k}\right)+\operatorname{disc}\left(\ell_{n-t-1}\right)\right)
$$

when $n$ is prime. This will allow us to bound the discrepancy of $\mathcal{L}_{n}$.

## 2. Preliminaries

Define $\alpha_{k}(n)$ to be the number of elements of $\{0,1\}^{n}$ containing no subword $0^{k}$, and let $\beta_{k}(n)$ be defined by

$$
\beta_{k}(n)=\sum_{\substack{w \in\{0,1\}^{n} \\ 0^{k} \notin w}} \operatorname{sk}(w) .
$$

For the remainder of this section, we fix a $k \geq 2$.
Lemma 2. The sequences $a_{n}=\alpha_{k}(n)$ and $b_{n}=\beta_{k}(n)$ satisfy:

1. $a_{n}=\sum_{j=1}^{k} a_{n-j}$ for $n \geq k$, and
2. $b_{n}=\sum_{j=1}^{k}\left[(j-2) a_{n-j}+b_{n-j}\right]$ for $n \geq k$.

Furthermore, $a_{j}=2^{j}$ for $0 \leq j<k$ and $b_{j}=0$ for $0 \leq j<k$.
Proof. Both recurrences follow from the following consideration: any string of length at least $k$ not containing a subword $0^{k}$ has a left-most 1 . Therefore, we may partition the $0^{k}$-free sequences into those which begin with a string of the form $0^{j} 1$ for $0 \leq j<k$. The "base case" formulas trivially follow from the fact that every string of length less than $k$ is $0^{k}$-free.

Lemma 3. For $n-1 \geq k \geq 3$,

$$
a_{n-1}=k+\sum_{j=3}^{k}(j-2) a_{n-j}+(k-1) \sum_{j=0}^{n-k-1} a_{j} .
$$

Proof. We proceed by induction. First, we verify that $a_{k}=k+\sum_{j=3}^{k}(j-$ 2) $a_{k+1-j}+(k-1) a_{0}$. Note that, by the "base case" part of Lemma $2, a_{j}=2^{j}$ in the relevant range, except that $a_{k}=2^{k}-1$. Therefore,

$$
k+\sum_{j=3}^{k}(j-2) a_{k+1-j}+(k-1) a_{0}=k+\sum_{j=3}^{k}(j-2) 2^{k+1-j}+k-1
$$

$$
\begin{aligned}
& =\sum_{j=1}^{k-2} j 2^{k-j-1}+2 k-1 \\
& =2^{k-2} \sum_{j=1}^{k-2} j 2^{-(j-1)}+2 k-1 \\
& =2^{k-2}\left(4-k 2^{-k+3}\right)+2 k-1 \\
& =2^{k}-2 k+2 k-1 \\
& =2^{k}-1=a_{k}
\end{aligned}
$$

Now, suppose the statement holds for $n$. Applying the first recurrence in Lemma 2,

$$
\begin{aligned}
a_{n} & =\sum_{j=1}^{k} a_{n-j} \\
& =a_{n-1}+\sum_{j=2}^{k} a_{n-j} \\
& =k+\sum_{j=3}^{k}(j-2) a_{n-j}+(k-1) \sum_{j=0}^{n-k-1} a_{j}+\sum_{j=2}^{k} a_{n-j} \\
& =k+\sum_{j=2}^{k}(j-1) a_{n-j}+(k-1) \sum_{j=0}^{n-k-1} a_{j} \\
& =k+\sum_{j=3}^{k}(j-2) a_{n+1-j}+(k-1) a_{n-k}+(k-1) \sum_{j=0}^{n-k-1} a_{j} \\
& =k+\sum_{j=3}^{k}(j-2) a_{n+1-j}+(k-1) \sum_{j=0}^{n-k} a_{j} .
\end{aligned}
$$

Corollary 4. $b_{n}<0$ for all $n-1 \geq k \geq 3$.
Proof. If we combine the recurrence for $b_{n}$ from Lemma 2 with the above Lemma 3,

$$
\begin{align*}
b_{n} & =\sum_{j=1}^{k}\left[(j-2) a_{n-j}+b_{n-j}\right] \\
& =-a_{n-1}+\sum_{j=3}^{k}(j-2) a_{n-j}+\sum_{j=1}^{k} b_{n-j} \\
& =-k-(k-1) \sum_{j=0}^{n-k-1} a_{j}+\sum_{j=1}^{k} b_{n-j}<0 \tag{1}
\end{align*}
$$

by induction.
Let $\rho_{k}$ be the largest (in absolute value) root of the polynomial $g(z)=$ $z^{k+1}-2 z^{k}+1$. It is proven in [9] that $\rho_{k}$ is real, lies between $5 / 3$ and 2 , and is unique in these respects. It is also shown in [9] that $\rho_{k} \rightarrow 2$ as $k \rightarrow \infty$. Note that

$$
z^{k}-\sum_{j=0}^{k-1} z^{j}=\frac{z^{k+1}-2 z^{k}+1}{z-1}
$$

so that $\rho_{k}$ is a root of the left-hand polynomial $f(z)$ here as well. Since $f(z)$ is the characteristic polynomial for the recurrence that the $a_{n}$ satisfy, $\rho_{k}$ is the growth rate of the $a_{n}$, i.e., $\lim _{n \rightarrow \infty} \log a_{n} / n=\rho_{k}$.

Lemma 5. For all $n \geq 1, a_{n} \geq \rho_{k} a_{n-1}$.
Proof. Since $\rho_{k}<2$, and $a_{n}=2^{n}$ for $0 \leq n<k$, the claimed bound holds for $n$ in this range. Suppose it holds for all $n<N$. Then by Lemma 2,

$$
\begin{aligned}
a_{n} & =\sum_{j=1}^{k} a_{n-j} \\
& \geq \sum_{j=1}^{k} \rho_{k} a_{n-j-1} \\
& =\rho_{k} a_{n-1} .
\end{aligned}
$$

Lemma 6. For $k \geq 4$ and all $n \geq k, b_{n} \geq-2 k a_{n} / 3$.
Proof. By (1),

$$
b_{n}=-k-(k-1) \sum_{j=0}^{n-k-1} a_{j}+\sum_{j=1}^{k} b_{n-j}
$$

If we suppose that $b_{j} \geq-\gamma k a_{j}$ for all $j<n$, then

$$
\begin{aligned}
b_{n} & \geq-k-k \sum_{j=0}^{n-k-1} a_{j}-\gamma k \sum_{j=1}^{k} a_{n-j} \\
& =-k-k \sum_{j=0}^{n-k-1} a_{j}-\gamma k a_{n}
\end{aligned}
$$

By iterating Lemma 5, we have

$$
b_{n} \geq-k-k \sum_{j=0}^{n-k-1} \rho_{k}^{j-n} a_{n}-\gamma k a_{n}
$$

$$
\begin{aligned}
& \geq-a_{n} k\left(\frac{1}{a_{n}}+\sum_{j=0}^{\infty} \rho_{k}^{j-n}+\gamma\right) \\
& =-a_{n} k\left(\frac{1}{a_{n}}+\frac{\rho_{k}^{-n}}{1-\rho_{k}^{-1}}+\gamma\right) \\
& \geq-a_{n} k\left(\frac{1}{a_{n}}+\frac{5}{2} \rho_{k}^{-n}+\gamma\right)
\end{aligned}
$$

We may begin by taking $\gamma=\frac{2 k-1}{k\left(2^{k+1}-3\right)} \leq \frac{7}{116}$ by considering $a_{k+1}=2^{k+1}-3$ and $b_{k+1}=1-2 k$. Then, $\gamma$ increases by at most

$$
\begin{aligned}
\sum_{n=k+1}^{\infty}\left(\frac{1}{a_{n}}+\frac{5}{2} \rho_{k}^{-n}\right) & \leq \sum_{n=k+1}^{\infty} \frac{1}{\rho_{k}^{n-k} a_{k}}+\frac{5}{2} \sum_{n=k+1}^{\infty} \rho_{k}^{-n} \\
& =\frac{\rho_{k}^{k}}{2^{k}-1} \sum_{n=k+1}^{\infty} \rho_{k}^{-n}+\frac{5}{2} \sum_{n=k+1}^{\infty} \rho_{k}^{-n} \\
& =\left(\frac{\rho_{k}^{k}}{2^{k}-1}+\frac{5}{2}\right) \rho_{k}^{-k-1} \sum_{n=0}^{\infty} \rho_{k}^{-n} \\
& =\left(\frac{\rho_{k}^{-1}}{2^{k}-1}+\frac{5}{2 \rho_{k}^{k+1}}\right) \cdot \frac{1}{1-\rho_{k}^{-1}} \\
& \leq\left(\frac{3}{5 \cdot 15}+\frac{5}{2(5 / 3)^{5}}\right) \cdot \frac{5}{2}=\frac{293}{500}
\end{aligned}
$$

The conclusion follows for all $n \geq k+1$, since $\frac{293}{500}+\frac{7}{116}=\frac{2343}{3625} \leq \frac{2}{3}$. It is also easy to verify that $b_{k} \geq-2 k a_{k} / 3$.

## 3. Main Result

Here we prove Theorem 1 stated in the introduction.
Proposition 7. For $4 \leq k<n$ and $n$ prime,

$$
\frac{k}{3}-2 \leq \frac{\operatorname{sk}\left(\ell_{k}\right)}{\alpha_{k+1}(n-k-2)} \leq 2 k-3
$$

Proof. The set $S_{k}$ contains each sequence of the form $0^{k} 1 w$ where $w$ is a $0^{k}$-free word of length $n-k-1$. However, the quantity $\operatorname{sk}\left(S_{k}\right)$ is not quite the sum of the skews of all $0^{k}$-free sequences of length $n-k-1$ prefixed by $0^{k} 1$ : it must include all elements of $S_{k}^{\circ}$, not just those that have prefix $0^{k}$ and contain no other runs $0^{k}$. For each word $w$ of length $n$ which contains more than one run of the form $0^{k}$, but no runs of the form $0^{k+1}$, only one of its conjugates (namely, $w^{\circ}$ ) appears in $S_{k}^{\circ}$. Define run $(w)$ to be the maximum $k$ so that $0^{k} \in w$, and let $\rho_{k}(w)$ be the number of subwords of the form $0^{k}$ in $w$, where $\operatorname{run}(w)=k$.
(Set $\rho_{k}(w)=0$ otherwise.) Since we may assume that each $w$ is aperiodic, this means that

$$
\begin{aligned}
\operatorname{sk}\left(\ell_{k}\right) & =\sum_{w \in S_{k}^{\circ}} \operatorname{sk}(w) \\
& =\sum_{\substack{w \in\{0,1\}^{n} \\
\operatorname{run}(w)=k}} \mathbb{1}\left(w=w^{\circ}\right) \operatorname{sk}(w) \\
& =\sum_{t \geq 0} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}} \frac{\operatorname{sk}\left(0^{k} 1 w 1\right)}{t+1} \\
& =\sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2+\operatorname{sk}(w)) .
\end{aligned}
$$

Define the "run-print" $\operatorname{rp}(w)$ of a word $w \in\{0,1\}$ with $\operatorname{run}(w)=k$ to be the set of indices $j \in[n]$ so that $w$ has a run $0^{k}$ starting at index $j$. Then we may write

$$
\begin{aligned}
\operatorname{sk}\left(\ell_{k}\right)= & \sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2+\operatorname{sk}(w)) \\
= & \sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2) \\
& +\sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{\left[n \in\left(\begin{array}{c}
{[n-k-2] \\
t}
\end{array}\right)\right.}} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\operatorname{rp}(w)=S}} \operatorname{sk}(w) .
\end{aligned}
$$

Now, for a given $S$ of cardinality $t$ and $w$ with $\operatorname{rp}(w)=S$, there is a $0^{k}$ run starting at location $s$ for each $s \in S$. Each such run is bounded on both sides by a 1. In between the runs are intervals, the sum over whose skews is nonpositive, by Corollary 4. Therefore,

$$
\sum_{\substack{w \in\{0,1\}^{n-k-2} \\ \operatorname{rp}(w)=S}} \operatorname{sk}(w) \leq \sum_{\substack{w \in\{0,1\}^{n-k-2} \\ \operatorname{rp}(w)=S}} t(k-1)
$$

so we have

$$
\begin{aligned}
\operatorname{sk}\left(\ell_{k}\right) \leq & \sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2) \\
& +\sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{S \in\left(\sum_{t-k-2]}^{[n-1}\right)}} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\operatorname{rp}(w)=S}} t(k-1)
\end{aligned}
$$

$$
\begin{aligned}
& <\sum_{t \geq 0} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2)+(k-1) \sum_{t \geq 0} \sum_{\substack{\left[n \in\left(\begin{array}{c}
{[n-k-2] \\
t}
\end{array}\right)\right.}} 1 \\
& =(k-2) \alpha_{k+1}(n-k-2)+(k-1) \alpha_{k+1}(n-k-2) \\
& =(2 k-3) \alpha_{k+1}(n-k-2) .
\end{aligned}
$$

On the other hand, by Lemma 6,

$$
\begin{aligned}
\operatorname{sk}\left(\ell_{k}\right) & =\sum_{t \geq 0} \frac{1}{t+1} \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}}(k-2+\operatorname{sk}(w)) \\
& \geq \sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=0}}(k-2)+\sum_{\substack{w \in\{0,1\}^{n-k-2} \\
\rho_{k}(w)=t}} \operatorname{sk}(w) \\
& =(k-2) \alpha_{k+1}(n-k-2)+\beta_{k+1}(n-k-2) \\
& \geq(k / 3-2) \alpha_{k+1}(n-k-2) .
\end{aligned}
$$

In the proof of Theorem 1 below, we use the following useful inequality of Janson (see, for example, [6]). The lower bound is standard; the upper bound is an easy modification of the one presented in [1]. Let $X$ be a finite set and let $P$ be a random subset of $X$, with elements $x \in X$ chosen independently with probability $p_{x}$. Let $\left\{Z_{i}: i \in \mathcal{I}\right\}$ be a system of subsets of $X$, and let $A_{i}$ denote the event that $Z_{i} \subset P$. If $Z_{i} \cap Z_{j}=\emptyset$, then $A_{i}$ and $A_{j}$ are independent. Let

$$
\Delta=\sum P\left(A_{i} \wedge A_{j}\right)
$$

where the sum is taken over all ordered pairs $i \neq j$ with $Z_{i} \cap Z_{j} \neq \emptyset$. Finally, define $\mu=\sum_{i} P\left(A_{i}\right)$.

Lemma 8. With $\mu, \Delta$ as above, if $\Delta \geq \mu / 2$, then

$$
e^{-\mu} \leq \bigwedge_{i \in I} \overline{A_{i}} \leq e^{-\mu^{2} / 3 \Delta}
$$

Proof of Theorem 1. Suppose for the moment that $n$ is prime and $k \geq 4$. We know that

$$
\operatorname{disc}\left(\mathcal{L}_{n}\right)=\max _{k}\left(1+\sum_{j=1}^{k-1} \operatorname{sk}\left(\ell_{n-j}\right)+\operatorname{disc}\left(\ell_{n-k}\right)\right)
$$

From Proposition 7, we have that

$$
\sum_{k=\log n+1}^{n} \operatorname{sk}\left(\ell_{k}\right) \geq \sum_{k=\log n+1}^{n}(k / 3-2) \cdot \alpha_{k+1}(n-k-2)
$$

$$
\begin{aligned}
& \geq \sum_{k=\log n+1}^{n}(k / 3-2) \cdot 2^{n-k-1}\left(1-n 2^{-k}\right) \\
& =\Omega\left(\frac{2^{n} \log n}{n}\right)
\end{aligned}
$$

On the other hand, for any $t$,

$$
\begin{aligned}
\sum_{k=t}^{n-1} \operatorname{sk}\left(\ell_{k}\right) & \leq \sum_{k=0}^{n-2}(2 k-3) \cdot \alpha_{k+1}(n-k-2) \\
& \leq \sum_{k=1}^{n-1} 2 k \cdot \alpha_{k}(n-k-1)
\end{aligned}
$$

We estimate this quantity using the inequality of Janson stated above. In this case, we take $X=[n], P$ is the set of indices where a 0 appears, $p_{x}=1 / 2$ for every $x, \mathcal{I}=[n-k+1], Z_{i}=[i, i+k-1]$ (i.e., the $i^{\text {th }}$ length $k$ interval of $[n]$ ), and $A_{i}$ is the event that a length $n$ word has a subsequence of the form $0^{k}$ on some $Z_{i}$. Then

$$
\mu=(n-k+1) 2^{-k}
$$

and

$$
\begin{aligned}
\Delta & =\sum_{\substack{1 \leq i, j \leq n-k+1 \\
0<|i-j|<k}} 2^{-k-|i-j|} \\
& <2^{-k+1}(n-k+1) \sum_{s=1}^{\infty} 2^{-s}=2^{-k+1}(n-k+1)=2 \mu .
\end{aligned}
$$

Furthermore,

$$
\Delta \geq 2^{-k}(n-k+1) \sum_{s=1}^{k-1} 2^{-s}>2^{-k-1}(n-k+1)=\mu / 2
$$

so the hypotheses hold. Therefore, for a uniform random choice of $w \in\{0,1\}^{n}$,

$$
P\left(0^{k} \notin w\right) \leq e^{-\mu / 12}=e^{-(n-k+1) /\left(12 \cdot 2^{k}\right)}
$$

Applying this bound to the above computations,

$$
k \alpha_{k}(n-k-1) \leq k \cdot 2^{n-k} e^{-(n-2 k) /\left(12 \cdot 2^{k}\right)}
$$

Let $T=\lfloor\log n\rfloor$. Then

$$
\sum_{k=1}^{n-1} k \alpha_{k}(n-k-1) \leq \sum_{k=1}^{n-1} k \cdot 2^{n-k} e^{-(n-2 k) /\left(12 \cdot 2^{k}\right)}
$$

$$
\begin{aligned}
&= 2^{n} \sum_{k=1}^{2 \log n} k \cdot 2^{-k} e^{-(n-2 k) /\left(12 \cdot 2^{k}\right)} \\
&+2^{n} \sum_{k=2 \log n+1}^{n-1} k \cdot 2^{-k} e^{-(n-2 k) /\left(12 \cdot 2^{k}\right)} \\
& \leq 2^{n} \sum_{k=-\infty}^{\infty} k \cdot 2^{-k} e^{-n /\left(24 \cdot 2^{k}\right)}+o\left(\frac{2^{n} \log n}{n}\right) \\
& \leq 2^{n} \sum_{k=-\infty}^{\infty}(T-k) \cdot 2^{k-T} e^{-n /\left(24 \cdot 2^{T-k}\right)}+o\left(\frac{2^{n} \log n}{n}\right) \\
& \leq 2^{n} \sum_{k=-\infty}^{\infty} \frac{2 \log n}{n} \cdot 2^{k} e^{-2^{k} / 48}+o\left(\frac{2^{n} \log n}{n}\right) \\
&=O\left(\frac{2^{n} \log n}{n}\right) \cdot \sum_{k=-\infty}^{\infty} 2^{k} e^{-2^{k} / 48}=O\left(\frac{2^{n} \log n}{n}\right) .
\end{aligned}
$$

Therefore, the total discrepancy is $\Theta\left(2^{n} \log n / n\right)$.
There are two more terms to consider: $\operatorname{sk}\left(\ell_{k}\right)$ with $k \leq 3$, and $\max _{k} \operatorname{disc}\left(\ell_{n-k}\right)$. The former terms are bounded by $O\left(\rho_{4}^{k}\right)=O\left(1.93^{k}\right)$, and therefore make an insignificant contribution. As for the latter, the length of $\ell_{n-k}$ is bounded above by $\alpha_{k+1}(n-k-2)$, and the above analysis shows that this quantity is $o\left(2^{n} \log n / n\right)$. Since the length of $\ell_{n-k}$ is an upper bound for $\operatorname{disc}\left(\ell_{n-k}\right)$, this term also does not affect the order of $\operatorname{disc}\left(\mathcal{L}_{n}\right)$.

Finally, we may drop the assumption that $n$ is prime. If not, then the above analysis is wrong: some words of length $n$, which would be part of the concatenation that gives rise to an $\ell_{k}$, are in fact periodic, and therefore only appear as their minimal roots in $\mathcal{L}_{n}$. (All Lyndon words of length dividing $n$ arise in this way.) However, the total number of symbols they contribute is at most

$$
\sum_{d \mid n, d<n} d 2^{d}<n^{2} 2^{n / 2}=o\left(\frac{2^{n} \log n}{n}\right)
$$

Hence, the asymptotic bound holds.

## 4. Acknowledgements

Thanks to Aaron Dutle for his careful reading of an earlier draft of this paper, and to Ron Graham for suggesting the problem.

## References

[1] N. Alon, J. Spencer, The probabilistic method. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley \& Sons, Inc., Hoboken, NJ, 2008.
[2] S. R. Blackburn, I. E. Shparlinski, Character sums and nonlinear recurrence sequences, Discrete Math. 306 (2006), no. 12, 1126-1131.
[3] L. R. Ford, A cyclic arrangement of $m$-tuples, Report P-1071, Rand Corp., Santa Monica, CA, 1957.
[4] H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, SIAM Rev. 24 (1982), no. 2, 195-221.
[5] Y. J. Huang, A new algorithm for the generation of binary de Bruijn sequences, J. Algorithms 11 (1990), no. 1, 44-51.
[6] S. Janson, Poisson approximation for large deviations, Random Struct. Alg. 1, 221-229 (1990).
[7] J. H. van Lint, R. M. Wilson, A course in combinatorics. Second edition. Cambridge University Press, Cambridge, 2001.
[8] M. H. Martin, A problem in arrangements, Bull. Amer. Math. Soc. 40 (1934), 859-864.
[9] A. M. Odlyzko, Asymptotic enumeration methods. Handbook of combinatorics, Vol. 2, 1063-1229, Elsevier, Amsterdam, 1995.


[^0]:    ${ }^{1}$ Corresponding Author: Department of Mathematics, University of South Carolina, 1523 Greene St., Columbia, SC 29208 USA, cooper@math.sc.edu, 803-777-3180, fax 803-777-3783.
    ${ }^{2}$ School of Mathematics, 686 Cherry Street, Georgia Institute of Technology, Atlanta, GA 30332 USA, heitsch@math.gatech.edu
    ${ }^{3}$ See the excellent survey [4] for a history of this and related sequences. The eponym, due to Fredricksen, refers to a 1957 unpublished manuscript of Ford ([3]). However, subsequent research has revealed earlier references. In [4], the author proposes that a 1934 paper of Martin ([8]) is the earliest appearance.

