# Closeness to the diagonal for longest common subsequences in random words 

Christian Houdré* Heinrich Matzinger ${ }^{\dagger}$


#### Abstract

The nature of the alignment with gaps corresponding to a longest common subsequence (LCS) of two independent iid random sequences drawn from a finite alphabet is investigated. It is shown that such an optimal alignment typically matches pieces of similar short-length. This is of importance in understanding the structure of optimal alignments of two sequences. Moreover, it is also shown that any property, common to two subsequences, typically holds in most parts of the optimal alignment whenever this same property holds, with high probability, for strings of similar short-length. Our results should, in particular, prove useful for simulations since they imply that the re-scaled two dimensional representation of a LCS gets uniformly close to the diagonal as the length of the sequences grows without bound.


Keywords: longest common subsequences; optimal alignments; last passage percolation; edit/Levensthein distance.
AMS MSC 2010: 05A05; 60C05; 60F10.
Submitted to ECP on December 29, 2014, final version accepted on April 20, 2016.

## 1 Introduction

Let $x$ and $y$ be two finite strings. A common subsequence of $x$ and $y$ is a subsequence of both $x$ and $y$, while a longest common subsequence (LCS) of $x$ and $y$ is a common subsequence of maximal length.

It is well known that common subsequences can be represented via alignments with gaps as illustrated, next, on some examples: First take the binary strings $x=0010$ and $y=0110$. A common subsequence is 01 , which can be represented as an alignment with gaps as follows: The common letters are aligned together, while each letter not appearing in the common subsequence is aligned with a gap. Several alignments can thus represent the same common subsequence and in this first example, an alignment corresponding to the common subsequence 01 is given by

| $x$ |  | 0 | 0 | 1 | 0 |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $y$ |  |  | 0 | 1 |  | 1 | 0 |

[^0]while another one is given by
\[

$$
\begin{array}{l|l|l|l|l|l|l|l|l}
x & & 0 & 0 & 1 & 0 & & &  \tag{1.2}\\
\hline y & & 0 & & 1 & & 1 & 0 &
\end{array}
$$
\]

Above, the LCS is not 01 but rather 010. An alignment corresponding to a LCS is called an optimal alignment (OA) or is said to be optimal. Neither (1.1) nor (1.2) represent optimal alignments, but an optimal alignment is given by:

$$
\begin{array}{l|l|l|l|l|l|l}
x & & 0 & 0 & 1 & & 0 \\
\hline y & & & 0 & 1 & 1 & 0
\end{array}
$$

which, again, is clearly not unique. Here the LCS of $x$ and $y$ is $\operatorname{LCS}(x ; y)=010$, which has length three, a fact denoted by $|L C S(x ; y)|=3$. Here is another example: let $x=$ christian and $y=$ krystyaan. Then, $\operatorname{LCS}(x ; y)=$ rstan and an alignment with gaps representing the LCS is:

$$
\left.\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|}
c & & h & r & i & & s & t & i & & a & & n  \tag{1.3}\\
\hline & & k & & r & & y & s & t & & y & a & a
\end{array} \right\rvert\,
$$

Again, all the letters which are part of the LCS are aligned with one another, while the other letters are aligned with gaps. In the above alignment of $x$ and $y, x_{5} x_{6} x_{7} x_{8} x_{9}=$ stian is aligned (with gaps) with $y_{4} y_{5} y_{6} y_{7} y_{8} y_{9}=s t y a a n$, and we say that the integer interval $[5,9]_{\mathrm{N}}$ is aligned with $[4,9]_{\mathbb{N}}$. Alternatively, we say that $[5,9]_{\mathrm{N}}$ gets mapped to $[4,9]_{\mathrm{N}}$ by the alignment we consider, meaning that the following two conditions are satisfied:
i) The letters $x_{5} x_{6} x_{7} x_{8} x_{9}$ are all aligned exclusively with gaps or with letters from the string $y_{4} y_{5} y_{6} y_{7} y_{8} y_{9}$.
ii) The letters from $y_{4} y_{5} y_{6} y_{7} y_{8} y_{9}$ are all aligned with gaps or with letters from the substring $x_{5} x_{6} x_{7} x_{8} x_{9}$.
To emphasize our terminology, we see that in the alignment (1.3), $[1,4]_{\mathbb{N}}$ is aligned with $[1,2]_{\mathbb{N}}\left([1,4]_{\mathbb{N}}\right.$ is also aligned with $\left.[1,3]_{\mathbb{N}}\right)$. In other words, in an alignment a piece of $x$ gets aligned with a piece of $y$ if and only if the letters from the piece of $x$ which get aligned to letters get only aligned with letters from the piece of $y$ and vice versa. Longest common subsequences and optimal alignments are important tools used in Computational Biology and Computational Linguistics for strings matching, e.g., see [6], [20], [21], and [25].

Throughout this paper, $X=X_{1} \cdots X_{n}$ and $Y=Y_{1} \cdots Y_{n}$ are two random strings/words where $\left(X_{i}\right)_{i \geq 1}$ and $\left(Y_{i}\right)_{i \geq 1}$ are two independent sequences of iid random variables with values in a finite alphabet $\mathcal{A}$ and having the same law. (No other assumption, besides its non triviality, is made on this common law.) Further, and again throughout, $L C_{n}$ denotes the length of the LCSs of $X$ and $Y$, i.e., $L C_{n}:=\left|L C S\left(X_{1} X_{2} \cdots X_{n} ; Y_{1} Y_{2} \cdots Y_{n}\right)\right|$.

To further put our framework in context, also note that $2\left(n-L C_{n}\right)$ is a version of the edit/Levenshtein distance used, e.g., in computer science. It is equal to the minimal number of insertions and deletions to change either string/word into the other.

A well known result of Chvátal and Sankoff [7] asserts that, when scaled by $n, \mathbb{E} L C_{n}$ converges to a constant $\gamma^{*} \in(0,1)$ (which depends on the size of the alphabet and on the law of $X_{1}$ ) given, via superadditivity, by $\gamma^{*}=\sup _{n \geq 1} \mathbb{E} L C_{n} / n$. However, to this day, even in the uniform binary case, the exact value of $\gamma^{*}$ is unknown. Moreover, Alexander [1] determined the rate of convergence to $\gamma^{*}$ showing that there exists an absolute constant $K_{A}$, independent of $n$, of the size of the finite alphabet $\mathcal{A}$, (and of the law of $X_{1}$ ), such that for all $n \geq 1$,

$$
\begin{equation*}
\gamma^{*} n-K_{A} \sqrt{n \log n} \leq \mathbb{E} L C_{n} \leq \gamma^{*} n \tag{1.4}
\end{equation*}
$$

This law of large numbers (with rate) gives the first order behavior of $L C_{n}$, and the next problem of interest is to study the order of the variance (or more generally, of the centered absolute moments) of $L C_{n}$. This order has been found to be linear in the length of the sequences in various instances (e.g., [10], [14], [18], [13]). This is, in particular, the case for iid binary sequences with zeros and ones having very different probabilities or for some classes of models "as close as one wants" to the uniform iid one [2]. In all the known instances, it turns out that the order of the variance of $L C_{n}$ is thus linear in $n$ which is the order conjectured by Waterman [24], for which Steele [23] had previously obtained a generic linear upper bound. However, the most important equiprobable iid (say, binary) case remains open.

In the present paper our purpose is different and we study optimal alignments at a macroscopic level. We present a general methodology showing that a property of optimal alignments holds true, provided this property typically holds true for shortstrings alignments. To prove these results, we partition $X$ into pieces of fixed length $k$ and, as $n$ goes to infinity, show that typically, and further with probability exponentially close to one, in any optimal alignment most of these pieces get aligned with pieces of $Y$ of similar length $k$. In other words, with high probability, there are no macroscopic gaps in the optimal alignments.

Let us explain, on a further example, how alignments have to stay close to the diagonal. Take the two related, English and German, words: $X=$ mother and $Y=$ mutter. The longest common subsequence is mter, hence $L C_{6}=4$ and the common subsequence mter corresponds to the following two alignments:

$$
\begin{array}{l|l|l|l|l|l|l|l}
m & o & & t & & h & e & r  \tag{1.5}\\
\hline m & & u & t & t & & e & r
\end{array}
$$

and

$$
\begin{array}{l|l|l|l|l|l|l|l}
m & o & & & t & h & e & r  \tag{1.6}\\
\hline m & & u & t & t & & e & r
\end{array}
$$

Next, view alignments as subsets of $\mathbb{R}^{2}$ as follows: If the $i$-th letter of $X$ gets aligned with the $j$-th letter of $Y$, then the set representing the alignment is to contain $(i, j)$. For example, the alignment (1.5) can be represented as: $(1,1),(3,3),(5,5),(6,6)$ with the corresponding plot

| $r$ |  |  |  |  |  | $\bullet$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $e$ |  |  |  |  | $\bullet$ |  |
| $t$ |  |  |  |  |  |  |
| $t$ |  |  | $\bullet$ |  |  |  |
| $u$ |  |  |  |  |  |  |
| $m$ | $\bullet$ |  |  |  |  |  |
|  | $m$ | $o$ | $t$ | $h$ | $e$ | $r$ |

while the alignment (1.6) can be represented as: $(1,1),(3,4),(5,5),(6,6)$ with the corresponding plot


Above, the symbol - indicates the aligned letter-pairs, and these points are said to represent the optimal alignment. An optimal alignment can then be viewed as the graph
of a function $f$ defined as follows: Let $f(0)=0$ and for $i, j=1, \ldots, n$, let $f(i)=j$ if the $i t h$ letter of the first sequence is aligned with the $j t h$ letter of the second sequence, while between these values and till $(n, n)$ let $f$ be defined via a linear interpolation. Then as shown in Section 4, with its notation, the function $f=f_{p_{1}, p_{2}}:[0, n] \rightarrow[0, n]$ stays between the two lines with respective slope $p_{1}$ and $p_{2}$. Moreover, under a strict concavity assumption on the limiting shape $\tilde{\gamma}$ (see the next section), $f_{p_{1}, p_{2}}$ becomes uniformly close to the identity as $n$ tends to infinity. More precisely, let $g_{n}:[0,1] \rightarrow[0,1]$ be defined via $g_{n}(x)=f(n x) / n$, then $\lim _{n \rightarrow+\infty} \sup _{0 \leq x \leq 1}\left|g_{n}(x)-x\right|=0$. In other words, there are no macroscopic gaps in any optimal alignment and any such alignment must remain close to the main diagonal.

This closeness to the diagonal property has proved crucial in obtaining the first result on the limiting law of $L C_{n}$, under a lower bound on the order of the variance, see [9]. Broadly speaking, when not close to the diagonal, many terms contribute to our CLT estimation but the corresponding set of random alignments has exponentially small probability; while when alignments are close to the diagonal, the estimation comes from only a few terms. The balance between these two cases leads to a central limit theorem. This CLT contrasts with the case of two independent uniform random permutations of $\{1,2, \cdots, n\}$, where the limiting distribution of the length of the longest common subsequences is the Tracy-Widom distribution, see [9]. The other, more pathological, instances, we are aware of and where a CLT holds true in a related problem, is for the length of the longest increasing subsequences of a single random word, potentially Markovian, where only one letter is attained with maximal probability, see [15], [16], [11], [12]. (However, for two or more random words the limiting law is no longer Gaussian [5].) This one word result contrasts, once more, with the single word permutation result of Baik, Deift and Johnansson [4] where the limiting law is the Tracy-Widom one.

Note that the LCS problem can be represented as a directed last passage percolation (LPP) problem with dependent weights. Indeed, let the set of vertices be

$$
V:=\{0,1,2, \ldots, n\} \times\{0,1,2, \ldots, n\}
$$

and let the set of oriented edges $\mathcal{E} \subset V \times V$ contain horizontal, vertical and diagonal edges. The horizontal edges are oriented to the right, while the vertical edges are oriented upwards, both having unit length. The diagonal edges point up-right at a 45 -degree angle and have length $\sqrt{2}$. Hence,

$$
\mathcal{E}:=\left\{\left(v, v+e_{1}\right),\left(v, v+e_{2}\right),\left(v, v+e_{3}\right): v \in V\right\}
$$

where $e_{1}:=(1,0), e_{2}:=(0,1)$ and $e_{3}:=(1,1)$. With the horizontal and vertical edges, we associate a weight of 0 . With the diagonal edge from $(i, j)$ to $(i+1, j+1)$ we associate the weight 1 if $X_{i+1}=Y_{j+1}$ and 0 (or $-\infty$ ) otherwise. In this manner, we obtain that $L C_{n}$ is equal to the total weight of the heaviest paths going from $(0,0)$ to $(n, n)$. (Another directed LPP representation can be obtained via $L C_{n}=\max _{\pi \in S I} \sum_{(i, j) \in \pi} \mathbf{1}_{\left\{X_{i}=Y_{j}\right\}}$, where $S I$ refers to the set of all paths with strictly increasing steps, i.e., paths with both coordinates strictly increasing from a step to another, from $(0,0)$ to the East, $x=n$, or North, $y=n$, boundary. A third representation would be as above but where now the paths going from $(0,0)$ to $(n, n)$ have either strictly increasing steps or North or East unit steps. Again to the strictly increasing steps the associated weight is $\mathbf{1}_{\left\{X_{i}=Y_{j}\right\}}$ while to the North as well as to the East unit steps is associated a weight value of 0 . As a final representation one could still proceed with strictly increasing paths but with the requirement that one ends the paths with a 1.)

Note that the weights in our percolation representations are not "truly 2-dimensional" and, in our opinion, this is the reason for the order of magnitude of the mean, variance
as well as the limiting law in the LCS problem to be different from other first/last passage-related models. To return to our specific results, they are the first studying the transversal fluctuations of the maximal paths of LCSs. Such questions have been of much interest in other percolation models. Let us only mention that Johansson [17] showed that for a Poisson points model in the plane, typical deviations of a maximal path from the diagonal is of order $n^{2 / 3}$, and $n^{2 / 3}$ is also the order of the transversal fluctuations in the directed polymer model studied in Seppäläinen [22]. (We refer to the respective bibliography of [17] and [22] for a much more complete and detailed picture on transversal fluctuations. We finally also note that in view of the results of [9], the transversal fluctuations of the LCSs of two independent random permutations of $\{1,2, \ldots, n\}$, one uniform and one arbitrary, are exactly the same as those of the longest increasing subsequences of a single uniform random permutation of $\{1,2, \ldots, n\}$.)

To finish this introductory section, let us briefly describe the rest of the paper. The next section presents some preliminary results, examples, and states the main result of the paper which is, in turn, proved in Section 3. Section 4 settles the closeness to the diagonal result and shows that each maximal path corresponding to the LCSs stays close to the diagonal. The last section explores the generic nature of short-strings alignments and some of its computational consequences.

## 2 Preliminaries

Throughout, let $n=k m$ and let the integers

$$
\begin{equation*}
r_{0}=0<r_{1}<r_{2}<r_{3}<\cdots<r_{m-1}<r_{m}=n, \tag{2.1}
\end{equation*}
$$

be such that

$$
\begin{equation*}
L C_{n}=\sum_{i=1}^{m}\left|L C S\left(X_{k(i-1)+1} X_{k(i-1)+2} \cdots X_{k i} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right| \tag{2.2}
\end{equation*}
$$

where $|L C S(\cdot ; \cdot)|$ is the length of the corresponding longest common substrings. In words, (2.2) asserts that there exists an optimal alignment aligning $[k(i-1)+1, k i]_{\mathbb{N}}$ with $\left[r_{i-1}+1, r_{i}\right]_{\mathbb{N}}$, for all $i=1,2, \ldots, m$.

The first goal of the present paper is to show that for $k$ large but fixed, and $n$ large enough, any such generic optimal alignment is such that the vast majority of the intervals $\left[r_{i-1}+1, r_{i}\right]_{\mathbb{N}}$ have length close to $k$. Building on this, a second goal is to show (see Section 5) that if a property $\mathcal{P}$ holds, with high probability, for string-pairs of (short) length order $k$, then typically a large proportion of aligned string-pairs satisfy the property $\mathcal{P}$.

Let us deal with our first goal and show that with high probability the optimal alignments satisfying (2.2), are such that most of their lengths $r_{i}-r_{i-1}$ are close to $k$. Of course, we need to quantify what is meant by "close to $k$ ". To do so, we first provide a definition. For $p>0$, let

$$
\begin{equation*}
\tilde{\gamma}(p):=\lim _{n \rightarrow \infty} \frac{\mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{n} ; Y_{1} Y_{2} \cdots Y_{n p}\right)\right|}{n(1+p) / 2} \tag{2.3}
\end{equation*}
$$

where, when not integers, the indices $n p$ are understood to be rounded-up to the nearest positive integers. This function $\tilde{\gamma}$ is just a re-parametrization of "the usual function"

$$
\gamma(q)=\lim _{n \rightarrow \infty} \frac{\mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{n-n q} ; Y_{1} Y_{2} \cdots Y_{n+n q}\right)\right|}{n},
$$

$q \in(-1,1)$, i.e.,

$$
\begin{equation*}
\tilde{\gamma}(p)=\gamma(q(p)), \tag{2.4}
\end{equation*}
$$

with $q(p)=(p-1) /(p+1)$.
A superadditivity argument, as in Chvátal and Sankoff [7], shows that the above limits do exist (and depend, for example, on the size of the alphabet but this is of no importance for our purposes). For $X$ and $Y$ identically distributed, the function $\gamma$ is symmetric about the origin, while a further superadditivity argument shows that it is concave there and so it reaches its maximum at $q=0$ (see [3] for details). It is not known whether or not the function $\gamma$ is strictly concave around $q=0$. From simulations this appears to be the case but, at present, a proof is elusive. (Again, the LCS problem is a last passage percolation problem, and for first/last passage percolation proving that the shape of the wet region is strictly concave seems difficult and in many cases has not been done.) Since $q(p)=(p-1) /(p+1)=1-2 /(p+1)$ is strictly increasing in $p$, with $q(1)=0$, if $\gamma$ were strictly concave around $q=0$, then it would reach a strict maximum there. Thus, $\tilde{\gamma}$ would also reach a strict maximum at $p=1$ but, without the strict concavity of $\gamma, p=1$ might not be the unique point of maximal value.

However, strict concavity is not needed, concavity is enough, for our results to hold. Indeed, (see Lemma 3.1) $\tilde{\gamma}$ is non-decreasing on $[0,1]$ and non-increasing on $[1, \infty)$ and thus ad hoc methods will show that $\tilde{\gamma}(p)$ is strictly smaller than $\tilde{\gamma}(1)=\gamma^{*}$, as soon as $p$ is farther away from 1 than a small given quantity. (If the unproven strict concavity is valid then, below, $p_{1}$ and $p_{2}$ could be chosen as close to 1 as one wishes to.)

Before coming to the proof of the main theorem, it is thus important to show the existence of, and provide estimates on, the aforementioned $p_{1}$ and $p_{2}$ chosen as close to 1 as possible. Let us first explore this question in the binary equiprobable case. Let $\gamma_{\ell}$ be any strict lower bound on $\gamma^{*}=\lim _{n \rightarrow \infty} \mathbb{E}\left|L C S\left(X_{1} \cdots X_{n} ; Y_{1} \cdots Y_{n}\right)\right| / n$. Then, if $x>0$ is such that

$$
\begin{align*}
& (1-x)\left(H_{2}\left(1-\frac{\gamma_{\ell}(2-x)}{2(1-x)}\right)-1\right)+H_{2}\left(x+(1-x)\left(1-\frac{\gamma_{\ell}(2-x)}{2(1-x)}\right)\right) \\
& \quad=(1-x)\left(H_{2}\left(1-\frac{\gamma_{\ell}}{2}\left(1+\frac{1}{1-x}\right)\right)-1\right)+H_{2}\left(1-\frac{\gamma_{\ell}}{2}(1+(1-x))\right)<0 \tag{2.5}
\end{align*}
$$

where $H_{2}(x)=-x \log _{2} x-(1-x) \log _{2}(1-x), 0<x<1$, is the binary entropy function, we claim that $p_{1}:=1-x$ and $p_{2}:=1 /(1-x)$ are such that

$$
\begin{equation*}
\tilde{\gamma}\left(p_{1}\right)<\tilde{\gamma}(1)=\gamma^{*}, \quad \tilde{\gamma}\left(p_{2}\right)<\tilde{\gamma}(1)=\gamma^{*} . \tag{2.6}
\end{equation*}
$$

Indeed, an easy upper bound on the probability that the length of the LCSs of $X_{1} \cdots X_{n}$ and $Y_{1} \cdots Y_{n(1-x)}$ is larger than $n(1-\eta)(1-x), 0<\eta<1$ is found as follows: First, take a non-random string $s$ of length $n(1-\eta)(1-x)$. The probability that $s$ is a subsequence of $Y_{1} \cdots Y_{(1-x) n}$ does not depend on $s$ (but only on the length of $s$ ), and so this probability would be the same if $s$ would consist only of ones. Therefore, the probability that $s$ is a subsequence of $Y_{1} \cdots Y_{n(1-x)}$ is the same as the probability that there are at least $n(1-x)(1-\eta)$ ones in $Y_{1} \cdots Y_{n(1-x)}$, which, in turn, is nothing but the probability for a binomial random variable, with parameters $(1-x) n$ and $1 / 2$, to be greater or equal to $n(1-x)(1-\eta)$. But, via classical exponential inequalities, this last probability is bounded above by

$$
\begin{equation*}
2^{n(1-x)\left(H_{2}(\eta)-1\right)} . \tag{2.7}
\end{equation*}
$$

Now, the number of subsequences of $X_{1} \cdots X_{n}$ of length $n(1-\eta)(1-x)$ is given by:

$$
\binom{n}{n(\eta+x-\eta x)} \leq 2^{n H_{2}(\eta+x-x \eta)} .
$$

Combining this last inequality with (2.7) leads to

$$
\begin{equation*}
\mathbb{P}\left(\left|L C S\left(X_{1} \cdots X_{n} ; Y_{1} \cdots Y_{n(1-x)}\right)\right| \geq(1-x)(1-\eta) n\right) \leq 2^{n\left((1-x)\left(H_{2}(\eta)-1\right)+H_{2}(\eta+x-\eta x)\right)} \tag{2.8}
\end{equation*}
$$

Therefore, from (2.8), as soon as

$$
\begin{equation*}
(1-x)\left(H_{2}(\eta)-1\right)+H_{2}(\eta+x-\eta x)<0 \tag{2.9}
\end{equation*}
$$

then, the probability that $\left|L C S\left(X_{1} \cdots X_{n} ; Y_{1} \cdots Y_{n(1-x)}\right)\right|$ is at least $(1-x)(1-\eta) n$ is exponentially small in $n$. In other words, the probability that the rescaled (by the average length of the two strings) LCS is at least:

$$
\begin{equation*}
\frac{2(1-x)(1-\eta)}{2-x}, \tag{2.10}
\end{equation*}
$$

is exponentially small in $n$. Now, to require the rescaled LCS value to be equal to $\gamma_{\ell}$, choose $\gamma_{\ell}$ equal to the quantity in (2.10), i.e., let

$$
\begin{equation*}
\eta=1-\frac{\gamma_{\ell}(2-x)}{2(1-x)} \tag{2.11}
\end{equation*}
$$

So, for $x$ given, (2.11) gives the value of $\eta$ corresponding to $\gamma_{\ell}$. We next find values of $x$ for which the probability, that the rescaled LCS of $X_{1} \cdots X_{n}$ and $Y_{1} \cdots Y_{n(1-x)}$ is at least $\gamma_{\ell}$, is exponentially small in $n$. Indeed, in (2.9) it is enough to replace $\eta$ by the value given in (2.11). This leads to the condition (2.5), and when (2.5) is satisfied, the probability that the LCS of $X_{1} \cdots X_{n}$ and $Y_{1} \cdots Y_{n(1-x)}$ has a rescaled value of at least $\gamma_{\ell}$ is exponentially small in $n$. Therefore, in this case, the rescaled limit, that is

$$
\tilde{\gamma}(1-x)=\lim _{n \rightarrow \infty} \frac{\mathbb{E}\left|L C S\left(X_{1} \cdots X_{n} ; Y_{1} \cdots Y_{n(1-x)}\right)\right|}{n}
$$

has to be at most $\gamma_{\ell}$. Thus, in this case, if $\gamma_{\ell}$ is a lower bound on $\tilde{\gamma}(1)$, then

$$
\tilde{\gamma}(1-x) \leq \gamma_{\ell}<\tilde{\gamma}(1)=\gamma^{*}
$$

so that $p_{1}=1-x$ and $p_{2}=1 /(1-x)$ satisfy (2.6).
Using $\gamma_{\ell}=0.7880$, which is a lower bound on $\gamma^{*}$ obtained, in the binary case, by Lueker [19], it is easily seen that (2.5) is negative for $x=0.28$. So $p_{1}=0.72$ and $p_{2}=1.39$ satisfy the needed conditions. Using these values as well as the upper bound 0.8263 (see [19]) provide an estimate for the fixed length $k$ for the pieces one would divide the strings into (see, below, the statement of our first theorem).

The entropic method, on obtaining bound on $p_{1}$ and $p_{2}$, presented above carries over, beyond the binary case, to arbitrary-size alphabets. However, in the non-uniform case such bounds might be far from optimal and require the knowledge of the probability associated with each letter. To further address this question, let us present a lemma, with a somehow easier approach, to deal with the generic case.
Lemma 2.1. Let $0<p_{1}=\gamma^{*} /\left(2-\gamma^{*}\right)<1$ and let $1<p_{2}=\left(2-\gamma^{*}\right) / \gamma^{*}$, then

$$
\begin{equation*}
\tilde{\gamma}\left(p_{1}\right)<\tilde{\gamma}(1)=\gamma^{*}, \quad \tilde{\gamma}\left(p_{2}\right)<\tilde{\gamma}(1)=\gamma^{*} \tag{2.12}
\end{equation*}
$$

Moreover, (2.12) continue to hold by taking $p_{1}=\gamma_{\ell} /\left(2-\gamma_{\ell}\right)$ and $p_{2}=\left(2-\gamma_{\ell}\right) / \gamma_{\ell}$ where $\gamma_{\ell}$ is any positive lower bound, such as $\sum_{\alpha \in \mathcal{A}}\left(\mathbb{P}\left(X_{1}=\alpha\right)\right)^{2}$, on $\gamma^{*}$.

Proof. First, note that when one sequence has length 0 , then the LCS also has length 0 , and thus

$$
\gamma(-1)=\gamma(1)=0
$$

Recall that the function $\gamma$ is concave and symmetric about 0 . Next, consider the LCS of the string $X=X_{1} X_{2} \cdots X_{2 n}$ and the empty string $Y$. Then, take $\epsilon n$ letters away from $X_{1} \cdots X_{2 n}$ and add that many letters to the $Y$ string, so as to now have, instead of the empty string, the string $Y_{1} Y_{2} \cdots Y_{\epsilon n}$. Then, provided $0<\epsilon<1$ is a small enough constant, it follows that with very high (in $n$ ) probability, the string $Y_{1} Y_{2} \cdots Y_{\epsilon n}$ is a substring of $X_{1} \cdots X_{2 n-\epsilon n}$. Indeed, let $T_{1}=\inf \left\{k \geq 0: X_{1}=Y_{k}\right\}, T_{2}=\inf \left\{k \geq T_{1}: X_{2}=Y_{k}\right\}$, $T_{3}=\inf \left\{k \geq T_{2}: X_{3}=Y_{k}\right\}, \ldots$ Then, conditionally on $X=x, T_{1}, T_{2}-T_{1}, T_{3}-T_{2}, \ldots$ are independent geometric random variables with individual parameter depending on the probabilities associated to the letters. But,

$$
\left|L C S\left(X_{1} \cdots X_{2 n-\epsilon n} ; Y_{1} \cdots Y_{\epsilon n}\right)\right|=\epsilon n
$$

if and only if $T_{\epsilon n} \leq 2 n-\epsilon n$. Thus, since the geometric property holds for any $x \in \mathcal{A}^{n}$,

$$
\begin{equation*}
\mathbb{P}\left(\mid L C S\left(X_{1} \cdots X_{2 n-\epsilon n} ; Y_{1} \cdots Y_{\epsilon n} \mid\right)=\epsilon n\right) \geq 1-\exp (-c n) \tag{2.13}
\end{equation*}
$$

where $c>0$ is a constant depending neither on $n$ nor on $\epsilon>0$ (provided $\epsilon>0$ is small enough) but depending on the minimal parameter of the geometric random variables (hence on the probabilities associated to the letters). Therefore, from the above, at $q=-1$, the slope is 1 , i.e., $\gamma^{\prime}\left((-1)^{+}\right)=1$ and similarly $\gamma^{\prime}\left(1^{-}\right)=-1$. By concavity and symmetry, for any $q_{1}$ with

$$
\begin{equation*}
q_{1}<-(1-\gamma(0)) \tag{2.14}
\end{equation*}
$$

it therefore follows that

$$
\gamma\left(q_{1}\right)<\gamma(0)
$$

and similarly for any $q_{2}$ with

$$
\begin{equation*}
q_{2}>1-\gamma(0) \tag{2.15}
\end{equation*}
$$

it follows that

$$
\gamma\left(q_{2}\right)<\gamma(0)
$$

The bounds obtained above rely on the value of $\gamma(0)=\gamma^{*}$ which is unknown, but for which upper and lower bounds (which depend on the distributions of the letters) do exist (and are rather accurate for uniform distributions). In our case, a lower bound on $\gamma^{*}$ is what is needed. The most trivial lower bound is obtained when aligning the two strings, without gaps, and just counting the number of correctly aligned letter pairs, more precisely, $L C_{n} \geq \sum_{i=1}^{n} \mathbf{1}_{\left\{X_{i}=Y_{i}\right\}}$. Hence, by the iid and independence assumptions,

$$
\begin{equation*}
\mathbb{E} L C_{n} \geq \sum_{i=1}^{n} \mathbb{P}\left(X_{i}=Y_{i}\right)=n \mathbb{P}\left(X_{1}=Y_{1}\right)=n \sum_{\alpha \in \mathcal{A}} \mathbb{P}\left(\left(X_{1}=\alpha\right)\right)^{2} \tag{2.16}
\end{equation*}
$$

Now, converting to $\tilde{\gamma}$, and recalling that $p(q)=(1+q) /(1-q)$, (2.14) becomes

$$
\begin{equation*}
p_{1}<\frac{\gamma(0)}{2-\gamma(0)} \tag{2.17}
\end{equation*}
$$

and in such a case, $\tilde{\gamma}\left(p_{1}\right)<\tilde{\gamma}(1)$. Similarly, (2.15) becomes

$$
\begin{equation*}
p_{2}>\frac{2-\gamma(0)}{\gamma(0)} \tag{2.18}
\end{equation*}
$$

and then $\tilde{\gamma}\left(p_{2}\right)<\tilde{\gamma}(1)$. Finally, in both (2.17) and (2.18), one can replace $\gamma(0)$ by any of its positive lower bound, for example the lower bound resulting from (2.16).

So let us now assume that $0<p_{1}<1<p_{2}$ are such that

$$
\begin{equation*}
\tilde{\gamma}\left(p_{1}\right)<\tilde{\gamma}(1)=\gamma^{*}, \quad \tilde{\gamma}\left(p_{2}\right)<\tilde{\gamma}(1)=\gamma^{*} \tag{2.19}
\end{equation*}
$$

The first result we next set to state, asserts that for $k$ fixed and $n$ large enough then typically in any optimal alignment (2.2) most of the intervals $\left[r_{i-1}+1, r_{i}\right]_{\mathrm{N}}$ (for $i=$ $1,2, \ldots, m$ ) have their length, $r_{i}-r_{i-1}$, between $k p_{1}$ and $k p_{2}$. By most, it is meant that by
taking $k$ large, but fixed, and $n$ large enough, the proportion of such intervals gets as close to 1 as one wishes to.

To do so, let us introduce some notation. Let $\epsilon>0, p_{1}>0$ and $p_{2}>0$ be constants. Let $A_{\epsilon, p_{1}, p_{2}}^{n}$ be the (random) set of optimal alignments of $X_{1} \cdots X_{n}$ and $Y_{1} \cdots Y_{n}$ satisfying (2.2), for which a proportion of at least $1-\epsilon$ of the intervals $\left[r_{i-1}+1, r_{i}\right]_{\mathbb{N}}, i=1,2, \ldots, m$, have their length between $k p_{1}$ and $k p_{2}$. More precisely, $A_{\epsilon, p_{1}, p_{2}}^{n}$ is the event that for all integer vectors $\left(r_{0}, r_{1}, \ldots, r_{m}\right)$ satisfying (2.1) and for which (2.2) holds,

$$
\begin{equation*}
\operatorname{Card}\left(\left\{i \in 1,2, \ldots, m: k p_{1} \leq r_{i}-r_{i-1} \leq k p_{2}\right\}\right) \geq(1-\epsilon) m \tag{2.20}
\end{equation*}
$$

As stated next, $A_{\epsilon, p_{1}, p_{2}}^{n}$ holds with high probability.
Theorem 2.2. Let $\epsilon>0$. Let $0<p_{1}<1<p_{2}$ be such that $\tilde{\gamma}\left(p_{1}\right)<\tilde{\gamma}(1)=\gamma^{*}$ and $\tilde{\gamma}\left(p_{2}\right)<\tilde{\gamma}(1)=\gamma^{*}$, and let $\delta \in\left(0, \min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)\right)$. Fix the integer $k$ to be such that $(1+\ln k) / k \leq \delta^{2} \epsilon^{2} / 16$, then

$$
\begin{equation*}
\mathbb{P}\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right) \geq 1-\exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{16}\right)\right) \tag{2.21}
\end{equation*}
$$

for all $n=n(\epsilon, \delta)$ large enough.
In words, and broadly, Theorem 2.2 asserts that for any $\epsilon>0$, there exists $k$ large enough, but fixed, such that if $X$ is divided into segments of length $k$ then, typically (at least a fraction $1-\epsilon$ of segments), and with high probability, the LCSs match these segments to segments of similar length in $Y$.

## 3 Proof of the main theorem

The proof of Theorem 2.2 requires the introduction of a few more definitions. So far we have looked at the integer intervals which are mapped by optimal alignments to the integer intervals $[k(i-1)+1, k i]_{\mathbb{N}}$. The opposite stand is now taken: given (nonrandom) integers $r_{0}=0<r_{1}<r_{2}<\cdots<r_{m}=n$, we request that the alignment aligns $[k(i-1)+1, k i]_{\mathbb{N}}$ with $\left[r_{i-1}+1, r_{i}\right]_{\mathbb{N}}$, for every $i=1,2, \ldots, m$. In general, such an alignment is not optimal and, the best score an alignment can attain under the above constraint is:

$$
\begin{aligned}
L_{n}(\vec{r}) & :=L_{n}\left(r_{0}, r_{1}, \ldots, r_{m}\right) \\
& :=\sum_{i=1}^{m}\left|L C S\left(X_{k(i-1)+1} X_{k(i-1)+2} \cdots X_{k i} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right| .
\end{aligned}
$$

Therefore, $L_{n}(\vec{r})$ represents the maximum number of aligned identical letter pairs under the constraint that $X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k}$ gets aligned with $Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}$, for all $i=1,2, \ldots, m$. Note moreover that for a non-random $\left(r_{0}, r_{1}, \ldots, r_{m}\right)$, the partial scores

$$
\left|\operatorname{LCS}\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|
$$

are independent of each other and, in this context, concentration inequalities will prove useful when dealing with $L_{n}(\vec{r})$. Next, let $\mathcal{R}_{\epsilon, p_{1}, p_{2}}$, be the (non-random) set of all integer vectors $\left(r_{0}, r_{1}, \ldots, r_{m}\right)$ satisfying (2.1) and (2.20), while $\overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$, denotes the (non-random) set of all integer vectors $\vec{r}=\left(r_{0}, r_{1}, \ldots, r_{m}\right)$ satisfying (2.1) but not (2.20).

Let us begin with a lemma.
Lemma 3.1. Let $\epsilon>0$. Let $0<p_{1}<1<p_{2}$ be such that $\tilde{\gamma}\left(p_{1}\right)<\gamma^{*}$ and $\tilde{\gamma}\left(p_{2}\right)<\gamma^{*}$, and let $\delta>0$ be such that $\delta<\min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)$. Let $\vec{r}=\left(r_{0}, \ldots, r_{m}\right) \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$, then

$$
\begin{equation*}
\mathbb{E}\left(L_{n}(\vec{r})-L C_{n}\right) \leq-\frac{\delta \epsilon n}{2} \tag{3.1}
\end{equation*}
$$

for all $n=n(\epsilon, \delta)$ large enough.

Longest common subsequences in random words

Proof. Let $p>0$, and let

$$
\tilde{\gamma}(p):=\lim _{n \rightarrow \infty} \frac{\mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{n} ; Y_{1} Y_{2} \cdots Y_{n p}\right)\right|}{n(1+p) / 2}
$$

where, by superadditivity, this limit exists with, moreover,

$$
\begin{equation*}
\frac{2 \mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{n} ; Y_{1} Y_{2} \cdots Y_{n p}\right)\right|}{n(1+p)} \leq \tilde{\gamma}(p) \tag{3.2}
\end{equation*}
$$

for any $n \geq 1$. Now, $\gamma: q \in(-1,1) \rightarrow \gamma(q) \in(0, \infty)$, defined via

$$
\gamma(q):=\lim _{n \rightarrow \infty} \frac{\mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{n-n q} ; Y_{1} Y_{2} \cdots Y_{n+n q}\right)\right|}{n}
$$

is symmetric about $q=0$ and, as already mentioned, is also concave (see [3]). Hence,

$$
\tilde{\gamma}(p)=\gamma\left(\frac{p-1}{p+1}\right)
$$

is non-decreasing up to $p=1$ and non-increasing afterwards. Thus, choosing the interval [ $p_{1}, p_{2}$ ] to contain $p=1$, it follows that for $p \notin\left[p_{1}, p_{2}\right]$,

$$
\begin{equation*}
\tilde{\gamma}(p) \leq \max \left(\tilde{\gamma}\left(p_{1}\right), \tilde{\gamma}\left(p_{2}\right)\right) \tag{3.3}
\end{equation*}
$$

Hence, for any $p \notin\left[p_{1}, p_{2}\right]$, combining (3.2) and (3.3) leads to:

$$
\begin{equation*}
\frac{2 \mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{k} ; Y_{1} Y_{2} \cdots Y_{k p}\right)\right|}{k(1+p)} \leq \max \left(\tilde{\gamma}\left(p_{1}\right), \tilde{\gamma}\left(p_{2}\right)\right) \tag{3.4}
\end{equation*}
$$

and therefore,

$$
\begin{equation*}
\frac{2 \mathbb{E}\left|L C S\left(X_{1} X_{2} \cdots X_{k} ; Y_{1} Y_{2} \cdots Y_{k p}\right)\right|}{k(1+p)} \leq \tilde{\gamma}(1)-\delta^{*}=\gamma^{*}-\delta^{*} \tag{3.5}
\end{equation*}
$$

where $\delta^{*}:=\min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)$.
Since the sequences $\left(X_{i}\right)_{i \geq 1}$ and $\left(Y_{i}\right)_{i \geq 1}$ are stationary, and assuming that $r_{i}-r_{i-1}=$ $k p$, the left-hand side of (3.5) becomes

$$
\frac{2 \mathbb{E}\left|L C S\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|}{k+r_{i}-r_{i-1}} .
$$

Thus, from (3.5), when $\left(r_{i}-r_{i-1}\right) / k \notin\left[p_{1}, p_{2}\right]$, then

$$
\begin{equation*}
\gamma^{*}-\frac{2 \mathbb{E}\left|L C S\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|}{k+r_{i}-r_{i-1}} \geq \delta^{*} . \tag{3.6}
\end{equation*}
$$

Hence, from (3.6),

$$
\begin{gathered}
\gamma^{*}\left(\frac{k+r_{i}-r_{i-1}}{2}\right)-\mathbb{E}\left|L C S\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right| \\
\geq \delta^{*}\left(\frac{k+r_{i}-r_{i-1}}{2}\right) \geq \delta^{*} \frac{k}{2}
\end{gathered}
$$

Letting $\mathcal{M}:=\left\{i:[k(i-1)+1, k i]\right.$ gets matched with strings of length not in $\left.\left[k p_{1}, k p_{2}\right]\right\}$, we then have

$$
\begin{align*}
\sum_{i \in \mathcal{M}}\left(\gamma^{*}\left(\frac{k+r_{i}-r_{i-1}}{2}\right)\right. & \left.-\mathbb{E}\left|\operatorname{LCS}\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|\right) \\
& \geq \sum_{i \in \mathcal{M}} \delta^{*} \frac{k}{2} \geq \delta^{*} \frac{k}{2} \epsilon m=\frac{n \delta^{*} \epsilon}{2} \tag{3.7}
\end{align*}
$$

On the other hand,

$$
\begin{align*}
& \sum_{i \in \mathcal{M}}\left(\gamma^{*}\left(\frac{k+r_{i}-r_{i-1}}{2}\right)-\mathbb{E}\left|\operatorname{LCS}\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|\right) \\
& \leq \sum_{i=1}^{m}\left(\gamma^{*}\left(\frac{k+r_{i}-r_{i-1}}{2}\right)-\mathbb{E}\left|\operatorname{LCS}\left(X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k} ; Y_{r_{i-1}+1} Y_{r_{i-1}+2} \cdots Y_{r_{i}}\right)\right|\right) \\
& =\gamma^{*} n-\mathbb{E} L_{n}(\vec{r}) \tag{3.8}
\end{align*}
$$

Therefore, combining (3.7) and (3.8) leads to

$$
\begin{equation*}
\gamma^{*} n-\mathbb{E} L_{n}(\vec{r}) \geq \frac{n \delta^{*} \epsilon}{2} \tag{3.9}
\end{equation*}
$$

as soon as $\left(r_{0}, r_{1}, \ldots, r_{m}\right) \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$. Now $\lim _{n \rightarrow+\infty} \mathbb{E} L C_{n} / n=\gamma^{*}$, while by hypothesis $\delta^{*}-\delta>0$,

$$
\begin{equation*}
0 \leq \gamma^{*}-\frac{\mathbb{E} L C_{n}}{n} \leq \frac{\left(\delta^{*}-\delta\right) \epsilon}{2} \tag{3.10}
\end{equation*}
$$

for all $n$ large enough. (At this last stage, a more quantitative bound, depending on $n$, could also be obtained using (1.4).) Combining (3.9) and (3.10) yields that for any $\vec{r} \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$,

$$
\mathbb{E}\left(L C_{n}-L_{n}(\vec{r})\right) \geq \frac{n \delta \epsilon}{2}
$$

for all $n$ large enough. The proof of the lemma is now complete.
Proof of Theorem 2.2. Clearly,

$$
\begin{equation*}
\operatorname{Card}\left(\overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}\right) \leq\binom{ n}{m} \leq \frac{n^{m}}{m!} \leq\left(\frac{e n}{m}\right)^{m}=(e k)^{m} \tag{3.11}
\end{equation*}
$$

by a well known and simple bound on the binomial coefficients.
Now, let $\delta<\delta^{*}:=\min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)$. By definition $L C_{n} \geq L_{n}(\vec{r})$, and so for $\vec{r}$ to define an optimal alignment requires:

$$
\begin{equation*}
L_{n}(\vec{r}) \geq L C_{n} \tag{3.12}
\end{equation*}
$$

Hence, for the event $A_{\epsilon, p_{1}, p_{2}}^{n}$ not to hold (see (2.20)), there needs to exist at least one $\vec{r} \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$ for which (3.12) is satisfied. Thus,

$$
\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}=\bigcup_{\vec{r} \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}}\left\{L_{n}(\vec{r})-L C_{n} \geq 0\right\}
$$

and

$$
\begin{equation*}
\mathbb{P}\left(\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq \sum_{\vec{r} \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}} \mathbb{P}\left(L_{n}(\vec{r})-L C_{n} \geq 0\right) \tag{3.13}
\end{equation*}
$$

When $\vec{r} \in \overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}$, it follows from Lemma 3.1 that:

$$
\mathbb{E}\left(L_{n}(\vec{r})-L C_{n}\right) \leq-\frac{\delta \epsilon n}{2}
$$

and so

$$
\begin{equation*}
\mathbb{P}\left(L_{n}(\vec{r})-L C_{n} \geq 0\right) \leq \mathbb{P}\left(L_{n}(\vec{r})-L C_{n}-\mathbb{E}\left(L_{n}(\vec{r})-L C_{n}\right) \geq \frac{\delta \epsilon n}{2}\right) \tag{3.14}
\end{equation*}
$$

for all $n$ large enough. Now, the difference $L_{n}(\vec{r})-L C_{n}$ changes by at most plus or minus two, when any one of the iid entries $X_{1}, X_{2}, \ldots, X_{n}, Y_{1}, Y_{2}, \ldots, Y_{n}$ is changed. Therefore, Hoeffding's martingale inequality, applied to the right-hand side of (3.14), gives

$$
\mathbb{P}\left(L_{n}(\vec{r})-L C_{n} \geq 0\right) \leq \mathbb{P}\left(L_{n}(\vec{r})-L C_{n}-\mathbb{E}\left(L_{n}(\vec{r})-L C_{n}\right) \geq \frac{\delta \epsilon n}{2}\right) \leq \exp \left(-\frac{\delta^{2} \epsilon^{2}}{16} n\right)
$$

(Recall that Hoeffding's martingale inequality asserts that if $f$ is a function of $j$ variables, such that changing any single of its entries changes $f$ by at most $\pm \Delta, \Delta>0$, and if $Z_{1}, Z_{2}, \ldots, Z_{j}$ are independent random variables, then

$$
\mathbb{P}\left(f\left(Z_{1}, Z_{2}, \ldots, Z_{j}\right)-\mathbb{E} f\left(Z_{1}, Z_{2}, \ldots, Z_{j}\right) \geq z\right) \leq \exp \left(-\frac{2 z^{2}}{j \Delta^{2}}\right)
$$

provided the expectation exists.) Combining this last inequality with (3.13), one obtains:

$$
\begin{equation*}
\mathbb{P}\left(\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq \operatorname{Card}\left(\overline{\mathcal{R}}_{\epsilon, p_{1}, p_{2}}\right) \exp \left(-\frac{\delta^{2} \epsilon^{2}}{16} n\right) \tag{3.15}
\end{equation*}
$$

But, from (3.11),

$$
\begin{equation*}
\mathbb{P}\left(\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq(e k)^{m} \exp \left(-\frac{\delta^{2} \epsilon^{2}}{16} n\right)=\exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{16}\right)\right) \tag{3.16}
\end{equation*}
$$

Therefore, the proof of Theorem 2.2 is complete.

## 4 Closeness to the diagonal

Let us begin with a definition. Let $D_{\epsilon, p_{1}, p_{2}}^{n}$ be the event that all the points representing any optimal alignment of $X_{1} X_{2} \cdots X_{n}$ with $Y_{1} Y_{2} \cdots Y_{n}$ are above the line $y=p_{1} x-p_{1} n \epsilon-$ $p_{1} k$, and below the line $y=p_{2} x+p_{2} n \epsilon+p_{2} k$.
Theorem 4.1. Let $\epsilon>0$. Let $0<p_{1}<1<p_{2}$ be such that $\tilde{\gamma}\left(p_{1}\right)<\gamma^{*}$ and $\tilde{\gamma}\left(p_{2}\right)<\gamma^{*}$, and let $0<\delta<\min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)$. Fix the integer $k$ to be such that $(1+\ln k) / k \leq$ $\delta^{2} \epsilon^{2} / 16$, then

$$
\begin{equation*}
\mathbb{P}\left(D_{\epsilon, p_{1}, p_{2}}^{n}\right) \geq 1-2 \exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{16}\right)\right), \tag{4.1}
\end{equation*}
$$

for all $n=n(\epsilon, \delta)$ large enough.
Proof. Let $D_{a}^{n}$ be the event that any optimal alignment of $X_{1} X_{2} \cdots X_{n}$ with $Y_{1} Y_{2} \cdots Y_{n}$ is above the line $y_{1}:=y_{1}(x)=p_{1} x-p_{1} n \epsilon-p_{1} k$; and let $D_{b}^{n}$ be the event that any optimal alignment of $X_{1} X_{2} \cdots X_{n}$ with $Y_{1} Y_{2} \cdots Y_{n}$ is below the line $y_{2}:=y_{2}(x)=p_{2} x+p_{2} n \epsilon+p_{2} k$. Clearly, $D_{a}^{n} \cap D_{b}^{n}=D_{\epsilon, p_{1}, p_{2}}^{n}$, hence

$$
\begin{equation*}
\mathbb{P}\left(\left(D_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq \mathbb{P}\left(\left(D_{a}^{n}\right)^{c}\right)+\mathbb{P}\left(\left(D_{b}^{n}\right)^{c}\right) \tag{4.2}
\end{equation*}
$$

and the result will be a consequence of the following two inclusions:

$$
\begin{equation*}
A_{\epsilon, p_{1}, p_{2}}^{n} \subset D_{a}^{n}, \quad A_{\epsilon, p_{1}, p_{2}}^{n} \subset D_{b}^{n} \tag{4.3}
\end{equation*}
$$

where $A_{\epsilon, p_{1}, p_{2}}^{n}$ is as in Theorem 2.2. Let us prove the first inclusion in (4.3). To start, assume that $x$ is an integer multiple of $k$, i.e., let $x=u k, u \in \mathbb{N}$. Next, and at first, let us consider the case where $x \leq n \epsilon$, i.e., that $p_{1} x-p_{1} n \epsilon \leq 0$. Any alignment (and, in particular, any optimal alignment) we consider, aligns any $x \in[0, n]_{\mathbb{N}}$ with $[0, n]_{\mathbb{N}}$. Hence, for every $x \leq n \epsilon$, the condition is always verified, that is any optimal alignment aligns $x$ with a $y$ which is at least equal to $p_{1} x-p_{1} n \epsilon$. Let us now consider the case where $x \geq n \epsilon$.

When the event $A_{\epsilon, p_{1}, p_{2}}^{n}$ holds, then any optimal alignment aligns all but a proportion $\epsilon$ of the interval $[(i-1) k+1, i k]_{\mathbb{N}}, i \in\{1, \ldots, m\}$ to integer intervals of length greater or equal to $k p_{1}$. The maximum number of integer intervals which could be matched with integer intervals of length less than $k p_{1}$ is thus $\epsilon m$. In the interval $[0, x]_{\mathbb{N}}$ there are $u$ intervals from the partition $[(i-1) k+1, i k]_{\mathbb{N}}, i \in\{1, \ldots, m\}$. Therefore, at least $u-\epsilon m$ of these intervals are matched to intervals of length no less than $k p_{1}$, implying that, when the event $A_{\epsilon, p_{1}, p_{2}}^{n}$ holds, $x$ gets matched by the optimal alignment with a value no less than $(u-\epsilon m) k p_{1}=p_{1} x-p_{1} \epsilon n$, since $x=u k$ and $n=m k$. This finishes the case where $x$ is an integer multiple of $k$. If $x$ is not an integer multiple of $k$, let $x_{1}$ denote the largest integer multiple of $k$ which is smaller than $x$. By definition,

$$
\begin{equation*}
x-x_{1}<k \tag{4.4}
\end{equation*}
$$

But, the two-dimensional alignment curve cannot go down, hence $x$ gets aligned with a point which cannot be below the point where $x_{1}$ gets aligned to. But, since $x_{1}$ is an integer multiple of $k$, it gets aligned with a point which is greater or equal to $p_{1} x_{1}-p_{1} \epsilon n$. Using (4.4), it follows that

$$
p_{1} x_{1}-p_{1} \epsilon n \geq p_{1} x-p_{1} \epsilon n-p_{1} k
$$

and this shows that when the event $A_{\epsilon, p_{1}, p_{2}}^{n}$ holds, then $x$ gets aligned above or on $p_{1} x-p_{1} \epsilon n-p_{1} k$. This finishes proving that the event $A_{\epsilon, p_{1}, p_{2}}^{n}$ is a sub-event of $D_{a}^{n}$. Therefore, by (2.21),

$$
\mathbb{P}\left(\left(D_{a}^{n}\right)^{c}\right) \leq \mathbb{P}\left(\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq \exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{16}\right)\right)
$$

Similarly, and symmetrizing the above arguments,

$$
\mathbb{P}\left(\left(D_{b}^{n}\right)^{c}\right) \leq \mathbb{P}\left(\left(A_{\epsilon, p_{1}, p_{2}}^{n}\right)^{c}\right) \leq \exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{16}\right)\right)
$$

finishing, via (4.2), the proof of the theorem.
Theorem 4.1 should prove useful in reducing the time to compute the LCS of two random sequences. Indeed, first by (4.1), when rescaled by $n$, the two-dimensional representation of an optimal alignment is, with high probability and up to a distance of order $\epsilon>0$, above the line $x \rightarrow p_{1} x$ and below the line $x \rightarrow p_{2} x$. Moreover, $\epsilon>0$ can be taken as small as we want, leaving it fixed though when $n$ goes to infinity. Next, simulations seem to indicate that the mean curve $\tilde{\gamma}$ is strictly concave at $p=1$. If strict concavity indeed hold, then $p_{1}$ and, say, $p_{2}=1 / p_{1}$, can be taken as close to 1 as we want, and still satisfy the conditions of the theorem. That is, taking $\epsilon$ as close to 0 as we want and $p_{1}$ as close to 1 as we want, the re-scaled two-dimensional representation of the optimal alignments would get uniformly as close to the diagonal as we want, as $n$ grows without bound.

Figure 1 is the graph of a simulation with two iid binary sequences of length $n=1000$. All the optimal alignments are contained between the two graphs below and are thus seen to all stay extremely close to the diagonal. The maximal vertical distance between two optimal paths is 26 and, for this vertical distance, the maximal horizontal stretch between which the two optimal paths split and then meet again is 112 .

## 5 Short string-lengths properties are generic

Often, a desirable property we want string-pairs to verify, e.g., a similar number of a given symbol or pattern, the presence of dominant matches, only holds with high

Longest common subsequences in random words


Figure 1: $n=1000$, uniform Bernoulli sequences
probability and if the two strings have their lengths not too far away from each other. Moreover, short strings are also often used as "seeds" to find longer or more global similarities and homologous properties ([21] contains many examples of such instances in applied problems). It is our purpose now to attempt to quantify such a generic phenomenon.

To to so, let $\mathcal{P}$ be a relation assigning to every pair of strings $(x, y)$ the value 1 if the pair $(x, y)$ has a certain property, and 0 otherwise. Hence, if $\mathcal{A}$ is the alphabet we consider,

$$
\mathcal{P}:\left(\cup_{k} \mathcal{A}^{k}\right) \times\left(\cup_{k} \mathcal{A}^{k}\right) \rightarrow\{0,1\}
$$

and if $\mathcal{P}(x, y)=1$, the string pair $(x, y)$ is said to have the property $\mathcal{P}$.
Let now $\epsilon>0$, be fixed, and let $\vec{r}=\left(r_{0}, r_{1}, \ldots, r_{m}\right)$ satisfy the condition (2.1). Let also $B_{\mathcal{P}}^{n}(\vec{r}, \epsilon)$ be the event that there is a proportion of at least $1-\epsilon$ of the string pairs

$$
\begin{equation*}
\left(X_{(i-1) k+1} \cdots X_{i k} ; Y_{r_{i-1}+1} \cdots Y_{r_{i}}\right) \tag{5.1}
\end{equation*}
$$

satisfying the property $\mathcal{P}$, i.e.,

$$
\begin{equation*}
B_{\mathcal{P}}^{n}(\vec{r}, \epsilon)=\left\{\sum_{i=1}^{m} \mathcal{P}\left(X_{(i-1) k+1} \cdots X_{i k} ; Y_{r_{i-1}+1} \cdots Y_{r_{i}}\right) \geq(1-\epsilon) m\right\} \tag{5.2}
\end{equation*}
$$

Next, let $B_{\mathcal{P}}^{n}(\epsilon)$ be the event that for every optimal alignment the proportion of aligned string pairs (5.1) satisfying the property $\mathcal{P}$ is at least $1-\epsilon$, i.e., $B_{\mathcal{P}}^{n}(\epsilon)$ holds if and only if for every $\vec{r}=\left(r_{0}, r_{1}, \ldots, r_{m}\right)$ satisfying (2.1) and such that $L C_{n}=L_{n}(\vec{r})$, the event $B_{\mathcal{P}}^{n}(\vec{r}, \epsilon)$ holds. Finally, assume that as soon as $r_{i}-r_{i-1} \in\left[k p_{1}, k p_{2}\right]$, the probability that
the string-pairs (5.1) have the required property is at least $1-q, q \in[0,1]$. Hence, assume that for every integer $\ell \in\left[k p_{1}, k p_{2}\right]$ :

$$
\mathbb{P}\left(\mathcal{P}\left(X_{1} \cdots X_{k} ; Y_{1} Y_{2} \cdots Y_{\ell}\right)=1\right) \geq 1-q
$$

We investigate, now, how small $q=q(k)$ needs to be in order to ensure that a large proportion of the aligned string pairs (5.1) has the property $\mathcal{P}$ (for every optimal alignment). Recall that $A_{\epsilon, p_{1}, p_{2}}^{n}$ is the event that every optimal alignment aligns a proportion of at least $1-\epsilon$ of the sub-strings $X_{(i-1) k+1} \cdots X_{i k}$ with sub-strings of $Y$ with length in $\left[k p_{1}, k p_{2}\right]$. Recall also that $\mathcal{R}_{\epsilon, p_{1}, p_{2}}$ is the set of integer vectors $\vec{r}=\left(r_{0}, r_{1}, \ldots, r_{m}\right)$, satisfying (2.1) and such that there is at least $(1-\epsilon) m$ of the differences $r_{i}-r_{i-1}$ in [ $k p_{1}, k p_{2}$ ].

Below, we deal with a small modification of the event $B_{\mathcal{P}}^{n}(\vec{r}, \epsilon)$. For this, let $\tilde{B}_{\mathcal{P}}^{n}(\vec{r}, \epsilon)$ be the event that among the aligned string pieces (5.1) there are no more than $m \epsilon$ which do not satisfy the property $\mathcal{P}$ and have their length $r_{i}-r_{i-1}$ in $\left[k p_{1}, k p_{2}\right]$. Clearly, for $\epsilon_{1}>0, \epsilon_{2}>0$,

$$
A_{\epsilon_{1}, p_{1}, p_{2}}^{n} \cap\left(\bigcap_{\vec{r} \in \mathcal{R}_{\epsilon_{1}, p_{1}, p_{2}}} \tilde{B}_{\mathcal{P}}^{n}\left(\vec{r}, \epsilon_{2}\right)\right) \subset B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right),
$$

and so

$$
\begin{equation*}
\mathbb{P}\left(\left(B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right)\right)^{c}\right) \leq \mathbb{P}\left(\left(A_{\epsilon_{1}, p_{1}, p_{2}}^{n}\right)^{c}\right)+\sum_{\vec{r} \in \mathcal{R}_{\epsilon_{1}, p_{1}, p_{2}}} \mathbb{P}\left(\left(\tilde{B}_{\mathcal{P}}^{n}\left(\vec{r}, \epsilon_{2}\right)\right)^{c}\right) \tag{5.3}
\end{equation*}
$$

Next,

$$
\mathbb{P}\left(\left(\tilde{B}_{\mathcal{P}}^{n}\left(\vec{r}, \epsilon_{2}\right)\right)^{c}\right) \leq\binom{ m}{\epsilon_{2} m} q^{\epsilon_{2} m} \leq \exp \left(H_{e}\left(\epsilon_{2}\right) m\right) q^{\epsilon_{2} m}
$$

where $H_{e}$ is the base $e$ entropy function, given by $H_{e}(x)=-x \ln x-(1-x) \ln (1-x), 0<$ $x<1$. Hence,

$$
\begin{equation*}
\mathbb{P}\left(\left(\tilde{B}_{\mathcal{P}}^{n}\left(\vec{r}, \epsilon_{2}\right)\right)^{c}\right) \leq q^{\epsilon_{2} m} \exp \left(H_{e}\left(\epsilon_{2}\right) m\right) \tag{5.4}
\end{equation*}
$$

Using (5.4) into (5.3) and, proceeding as in (3.11), noting that $\mathcal{R}_{\epsilon, p_{1}, p_{2}}$ has at most $(e k)^{m}$ elements, lead to

$$
\begin{equation*}
\mathbb{P}\left(\left(B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right)\right)^{c}\right) \leq \mathbb{P}\left(\left(A_{\epsilon_{1}, p_{1}, p_{2}}^{n}\right)^{c}\right)+(e k)^{m} q^{\epsilon_{2} m} \exp \left(H_{e}\left(\epsilon_{2}\right) m\right) \tag{5.5}
\end{equation*}
$$

Taking $q(k)=1 /(2 e k)^{1 / \epsilon_{2}}$, finally yields

$$
\begin{equation*}
\mathbb{P}\left(\left(B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right)\right)^{c}\right) \leq \mathbb{P}\left(\left(A_{\epsilon_{1}, p_{1}, p_{2}}^{n}\right)^{c}\right)+\exp \left(\left(H_{e}\left(\epsilon_{2}\right)-\ln 2\right) m\right) \tag{5.6}
\end{equation*}
$$

But, for $\epsilon_{2}<1 / 2, H_{e}\left(\epsilon_{2}\right)<\ln 2$, and then $\exp \left(\left(H_{e}\left(\epsilon_{2}\right)-\ln 2\right) m\right)$ is exponentially small in $m$. Now, our main theorem provides an exponentially small lower bound on $\mathbb{P}\left(\left(A_{\epsilon_{1}, p_{1}, p_{2}}^{n}\right)^{c}\right)$. Therefore, (5.6) asserts that a high proportion of the aligned string pairs (5.1) has property $\mathcal{P}$, in any optimal alignment, as soon as for pairs (5.1) with similar length, $q(k) \leq 1 /(2 e k)^{1 / \epsilon_{2}}$, where

$$
q(k):=\max _{\ell \in\left[k p_{1}, k p_{2}\right]} \mathbb{P}\left(\text { the pair }\left(X_{1} \cdots X_{k} ; Y_{1} \cdots Y_{\ell}\right) \text { does not satisfy property } \mathcal{P}\right)
$$

These assertions are summarized in the next theorem, which is obtained by letting, above, $\epsilon_{1}=\epsilon_{2}=\epsilon / 2$, using also Theorem 2.2.
Theorem 5.1. Let $0<\epsilon<1$. Let $0<p_{1}<1<p_{2}$ be such that $\tilde{\gamma}\left(p_{1}\right)<\gamma^{*}$ and $\tilde{\gamma}\left(p_{2}\right)<\gamma^{*}$, and let $0<\delta<\min \left(\gamma^{*}-\tilde{\gamma}\left(p_{1}\right), \gamma^{*}-\tilde{\gamma}\left(p_{2}\right)\right)$. Finally, let the integer $k \geq 1$ be such that

$$
\max _{\ell \in\left[k p_{1}, k p_{2}\right]} \mathbb{P}\left(\left(X_{1} \cdots X_{k} ; Y_{1} \cdots Y_{\ell}\right) \text { does not satisfy property } \mathcal{P}\right) \leq \frac{1}{(2 e k)^{2 / \epsilon}}
$$

Then, for any optimal alignment $\vec{r}$ (i.e., such that $L C_{n}=L_{n}(\vec{r})$ ), the proportion of string pairs $\left(X_{(i-1) k+1} \cdots X_{i k} ; Y_{r_{i-1}+1} \cdots Y_{r_{i}}\right)$ satisfying property $\mathcal{P}$ is at least $1-\epsilon$ with probability at least equal to:

$$
1-\mathbb{P}\left(\left(A_{\epsilon / 2, p_{1}, p_{2}}^{n}\right)^{c}\right)-\exp \left(\left(H_{e}\left(\frac{\epsilon}{2}\right)-\ln 2\right) m\right)
$$

and thus at least equal to:

$$
1-\exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon^{2}}{64}\right)\right)-\exp \left(\frac{n}{k}\left(H_{e}\left(\frac{\epsilon}{2}\right)-\ln 2\right)\right),
$$

for all $n=n(\epsilon, \delta)$ large enough.
Hence, from the above statement, the probability that less than a proportion $1-\epsilon$ of string pairs (5.1) have property $\mathcal{P}$ in every optimal alignment is exponentially small in $n$ (while holding $k, \epsilon$ and $\delta$ fixed) as soon as

$$
\begin{equation*}
k>\frac{64(1+\ln k)}{\epsilon^{2} \delta^{2}} \tag{5.7}
\end{equation*}
$$

and

$$
\begin{equation*}
\max _{\ell \in\left[k p_{1}, k p_{2}\right]} \mathbb{P}\left(\left(X_{1} \cdots X_{k} ; Y_{1} \cdots Y_{\ell}\right) \text { does not satisfy property } \mathcal{P}\right) \leq \frac{1}{(2 e k)^{2 / \epsilon}} \tag{5.8}
\end{equation*}
$$

The above theorem is very useful for showing that when a property holds for aligned string pairs with similar lengths, say of order $k$, then the property typically holds in most parts of the optimal alignment. From our experience, for most properties one is interested in, such as the study of dominant matches in optimal alignments, when $p_{1}$ and $p_{2}$ are close to 1 , but fixed, then the probability that

$$
\left(X_{1} \cdots X_{k} ; Y_{1} Y_{2} \cdots Y_{\ell}\right)
$$

does not satisfy this property is approximately the same for all $\ell \in\left[k p_{1}, k p_{2}\right]$. In other words, the behavior of the alignment of $X_{1} \cdots X_{k}$ with $Y_{1} \cdots Y_{\ell}$, does not depend much on $\ell$ as soon as $\ell$ is close to $k$ and $k$ is fixed. From (5.8), what is needed there is a bound, on the left hand-side probability, smaller than any inverse polynomial-order in $k$. (At least to be able to take $\epsilon$ as close to 0 as one wants to.) If instead $\epsilon>0$ is chosen small but fixed, then an inverse polynomial bound with a very large exponent will do). So, if this probability is, for example, of order $k^{-\ln k}$ or $e^{-k^{\alpha}}$ for some constant $\alpha>0$, the condition (5.8) is satisfied by taking $k$ large enough. Similarly, condition (5.7) is always satisfied for $k$ large enough.

We could also envision using Monte Carlo simulation to find a bound for the probability on the left of (5.8). For that purpose, assume that $\epsilon=0.2$ and take $\delta=0.1$. Then, by (5.7), $k$ must be at least 2518253 . The probability that strings of length approximately $k$ do not satisfy property $\mathcal{P}$ must be at most $(2 e k)^{-10} \approx(13690642)^{-10}$, so a probability smaller than $10^{-70}$. However, this is hardly feasible, indeed, to show that a probability is as small as $10^{-70}$, one would need to run an order of $10^{70}$ simulations.

## Further Improvements

There are several ways to improve our various bounds. First, we took $\binom{n}{m}$ as an upper bound for the cardinality of $\mathcal{R}_{\epsilon, p_{1}, p_{2}}$ and this can be improved. Indeed, note that if $\vec{r}=\left(r_{0}, r_{1}, \ldots, r_{m}\right) \in \mathcal{R}_{\epsilon, p_{1}, p_{2}}$, then at least $(1-\epsilon) m$ of the lengths $r_{i+1}-r_{i}$ are in the interval $\left[k p_{1}, k p_{2}\right]$. To determine these lengths we have at most

$$
\begin{equation*}
\left(\left(p_{2}-p_{1}\right) k\right)^{m} \tag{5.9}
\end{equation*}
$$

choices. Then, there can be as many as $\epsilon m$ of the lengths $r_{i+1}-r_{i}$, which are not in [ $k p_{1}, k p_{2}$ ]. Choosing those lengths is like choosing at most $\epsilon m$ points from a set of at most $n$ elements. Hence, we get as upper bound $\binom{n}{\epsilon m}$ which, in turn, can be upper bounded by, say,

$$
\begin{equation*}
\left(\frac{e k}{\epsilon}\right)^{\epsilon m} \tag{5.10}
\end{equation*}
$$

or via the entropy bound $\exp \left(n H_{e}(\epsilon / k)\right)$. Finally, we have to decide which among the $m$ lengths $r_{i}-r_{i-1}$ have their length in $\left[k p_{1}, k p_{2}\right]$ and which have not. That choice is further bounded via:

$$
\begin{equation*}
\binom{m}{\epsilon m} \leq \exp \left(H_{e}(\epsilon) m\right) \tag{5.11}
\end{equation*}
$$

Combining the bounds (5.9), (5.10) and (5.10), yields

$$
\begin{equation*}
\operatorname{Card}\left(\mathcal{R}_{\epsilon, p_{1}, p_{2}}\right) \leq\left(\left(p_{2}-p_{1}\right) k\left(\frac{e k}{\epsilon}\right)^{\epsilon} \exp \left(H_{e}(\epsilon)\right)\right)^{m} \tag{5.12}
\end{equation*}
$$

With this better bounding of the cardinality of $\mathcal{R}_{\epsilon, p_{1}, p_{2}}$, the inequality (5.5) becomes:

$$
\begin{align*}
\mathbb{P}\left(\left(B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right)\right)^{c}\right) \leq & \mathbb{P}\left(\left(A_{\epsilon_{1}, p_{1}, p_{2}}^{n}\right)^{c}\right) \\
& +\left(\left(p_{2}-p_{1}\right) k\left(\frac{e k}{\epsilon_{1}}\right)^{\epsilon_{1}} \exp \left(H_{e}\left(\epsilon_{1}\right)\right)\right)^{m} q^{\epsilon_{2} m} \exp \left(H_{e}\left(\epsilon_{2}\right) m\right), \tag{5.13}
\end{align*}
$$

which when combined with Theorem 2.2 yields that

$$
\begin{align*}
\mathbb{P}\left(\left(B_{\mathcal{P}}^{n}\left(\epsilon_{1}+\epsilon_{2}\right)\right)^{c}\right) \leq & \exp \left(-n\left(-\frac{1+\ln k}{k}+\frac{\delta^{2} \epsilon_{1}^{2}}{16}\right)\right) \\
& +\left(\left(p_{2}-p_{1}\right) k\left(\frac{e k}{\epsilon_{1}}\right)^{\epsilon_{1}} \exp \left(H_{e}\left(\epsilon_{1}\right)\right) q^{\epsilon_{2}} \exp \left(H_{e}\left(\epsilon_{2}\right)\right)\right)^{m} \tag{5.14}
\end{align*}
$$

Again, this last expression is exponentially small in $n$ (assuming $k$ fixed) if the following two conditions are satisfied:
(i)

$$
\begin{equation*}
k>\frac{16(1+\ln k)}{\epsilon_{1}^{2} \delta^{2}} \tag{5.15}
\end{equation*}
$$

(the smallest integer $k$ satisfying (5.15) with $\epsilon_{1}=0.2$ and $\delta=0.1$ is now 570146 ) and (ii)

$$
\begin{equation*}
q(k)<\frac{1}{\left(\left(p_{2}-p_{1}\right) k\left(\frac{e k}{\epsilon_{1}}\right)^{\epsilon_{1}} \exp \left(H_{e}\left(\epsilon_{1}\right)+H_{e}\left(\epsilon_{2}\right)\right)\right)^{1 / \epsilon_{2}}} ; \tag{5.16}
\end{equation*}
$$

and combining these last two conditions yields:

$$
\begin{equation*}
q(k)<\left(\frac{\epsilon_{1}^{2} \delta^{2}}{\left(p_{2}-p_{1}\right) 16(1+\ln k)\left(\frac{e k}{\epsilon_{1}}\right)^{\epsilon_{1}} \exp \left(H_{e}\left(\epsilon_{1}\right)+H_{e}\left(\epsilon_{2}\right)\right)}\right)^{1 / \epsilon_{2}} \tag{5.17}
\end{equation*}
$$

Typically $\epsilon_{1}+\epsilon_{2}$ should be of a given order. So, let us maximize the right-hand side of (5.17) under the constraint $\epsilon=\epsilon_{1}+\epsilon_{2}$. To do so, note that the power $1 / \epsilon_{2}$ has a much more minimizing influence than the expression $\epsilon_{1}^{2}$ in the numerator, while $1 \leq \exp \left(H_{e}\left(\epsilon_{1}\right)+H_{e}\left(\epsilon_{2}\right)\right) \leq 2$ and so this last quantity does not have much of an influence. Also, note $\left(e k / \epsilon_{1}\right)^{\epsilon_{1}}$ is somewhat negligible compared to $e k$. So, at first, let us disregard the quantities $\left(e k / \epsilon_{1}\right)^{\epsilon_{1}}$ and $\left.\exp \left(H_{e}\left(\epsilon_{1}\right)\right)+H_{e}\left(\epsilon_{2}\right)\right)$, and let

$$
g\left(k, \epsilon_{1}, \epsilon_{2}\right):=\left(\frac{\epsilon_{1}^{2} \delta^{2}}{\left(p_{2}-p_{1}\right) 16(1+\ln k)}\right)^{1 / \epsilon_{2}}
$$

Clearly, $g\left(k, \epsilon_{1}, \epsilon_{2}\right)$ is larger than the bound on the right-hand side of (5.17) and when all the parameters $p_{1}, p_{2}$ and $\delta$ are held fixed, $g\left(k, \epsilon_{1}, \epsilon_{2}\right)$ is decreasing in both $\epsilon_{1}$ and $\epsilon_{2}$. However, $\epsilon_{2}$ "has more decreasing influence" than $\epsilon_{1}$. Therefore, given $\epsilon$ and given that all the parameters are fixed (including $k$ ), maximizing $g\left(k, \epsilon_{1}, \epsilon_{2}\right)$ under the constraint $\epsilon_{1}+\epsilon_{2}=\epsilon, \epsilon_{1}, \epsilon_{2}>0$ lead to a quantity where $\epsilon_{2}$ is quite a bit larger than $\epsilon_{1}$.

Could Monte Carlo simulations be realistic with $\epsilon=0.1$ and the bounds which we have? The answer is no. Indeed, at first, $\delta /\left(p_{2}-p_{1}\right)$ gets better when $\left|p_{2}-p_{1}\right|$ increases since the derivative of $\tilde{\gamma}$ at $p=1$ is zero. When the interval $\left[k p_{1}, k p_{2}\right]$ becomes too large however, then the property might no longer hold with high probability for all pairs $\left(X_{1} \cdots X_{k}, Y_{1} \cdots Y_{\ell}\right)$, with $\ell \in\left[k p_{1}, k p_{2}\right]$. So, we will take $\left[p_{1}, p_{2}\right]$, as large as possible, so this property still holds with high probability for all the string pairs mentioned before. With such a choice, $\delta /\left(p_{2}-p_{1}\right)$ can be treated as a constant. Somewhat, optimistically, say that the constant is less than $1 / 3$. Now if $\epsilon=0.1$, then $\epsilon_{1}, \epsilon_{2} \leq 0.1$. In that case,

$$
g\left(k, \epsilon_{1}, \epsilon_{2}\right) \leq g(k, 0.1,0.1) \leq\left(\frac{0.01 \delta}{3 \times 16(1+\ln k)}\right)^{10} .
$$

Returning to (5.15) and taking $\delta=0.2$, we find that $k$ must be larger than $10^{10}$, so that $\ln k$ is bigger than 20. With this in mind, and in the present case where $\epsilon_{1}+\epsilon_{2}=0.1$, we find that $g\left(k, \epsilon_{1}, \epsilon_{2}\right)$ is smaller $10^{-56}$, so there is still little hope to perform Monte Carlo simulation here.

Monte Carlo simulation with $\epsilon_{1}=0.1$ and $\epsilon_{2}=0.2$ : Take also $\delta=0.2$ and $\delta /\left(p_{2}-\right.$ $\left.p_{1}\right)=1 / 2$. With these values, and using (5.15), then $k$ must be somewhat larger than $10^{2} \cdot 10 \cdot 8 \ln (24000) \approx 10^{5}$. Then, by (5.16), $q(k)$ should also be less than

$$
\left(10^{2} \cdot 10 \cdot 11 \cdot 8\right)^{-5} \approx 10^{-25}
$$

This is still a difficult order for Monte Carlo simulation and if we had $\epsilon_{2}=0.3$ instead, then we would get a bound $10^{-15}$ which remains a difficult order.

When only dealing with the inequality (5.16), things look somewhat better. Take $k=1000$ and $\left(p_{1}-p_{1}\right) k=100$, then the bound on $q(k)$ is of order about $10^{-5}$ which is feasible with Monte Carlo. So, if we could find another method than the one described here to make sure that most of the pieces of strings $X_{(i-1) k+1} X_{(i-1) k+2} \cdots X_{i k}$ are aligned with pieces of similar length we would end up in a favorable setting.

Acknowledgments: Many thanks to the referee for a thoughtful and detailed reading of this manuscript.

## References

[1] Alexander, K. S. The rate of convergence of the mean length of the longest common subsequence, Annals of Applied Probability 4, (1994), 1074-1082. MR-1304773
[2] Amsalu, S., Houdré, C. and Matzinger, H., Sparse long blocks and the variance of the length of the longest common subsequences in random words, arXiv:1204.1009 [math.PR], (2012).
[3] Amsalu, S., Houdré, C. and Matzinger, H., Sparse long blocks and the micro-structure of the longest common subsequences in random words, J. Stat. Phys., 154, 6, (2014), 1516-1549.
[4] Baik, J., Deift, P. and Johansson, K. On the distribution of the length of the longest increasing subsequence of random permutations. J. Amer. Math. Soc., 12(4):1119-1178, 1999. MR1682248
[5] Breton, J.-C. and Houdré, C., On the limiting law of the length of the longest common and increasing subsequences in random words. arXiv:1505.06164 [Math.PR], (2015).
[6] Capocelli, R.M., Sequences: Combinatorics, Compression, Security, and Transmission, Springer-Verlag New York, (1989). MR-1040295
[7] Chvátal, V. and Sankoff, D., Longest common subsequences of two random sequences, J. Appl. Probability, 12, (1975), 306-315. MR-0405531
[8] R. Durbin, S.R. Eddy, A. Krogh, and G. Mitchison. Biological Sequence Analysis: Probabilistic Models of Proteins and Nucleic Acids, Cambridge University Press, 1998.
[9] Houdré, C. and Işlak, Ü., A central limit theorem for the length of the longest common subsequences in random words, arXiv:1408.1559v3 [math.PR], (2015).
[10] Houdré, C., Lember, J. and Matzinger, H., On the longest common increasing binary subsequence, C.R. Acad. Sci. Paris Ser. I 343, (2006), 589-594. MR-2269870
[11] Houdré, C. and Litherland, T. L. On the longest increasing subsequence for finite and countable alphabets. HDPV: The Luminy Volume, IMS Collection, 5:185-212, 2009. MR2797948
[12] Houdré, C. and Litherland, T. L. On the limiting shape of Young diagrams associated with Markovian random words. arXiv:1110.4570 [math.PR], (2011). MR-2797948
[13] Houdré, C. and Ma, J., On the order of the central moments of the length of the longest common subsequences in random words, To appear: Progress in Probability: Birkhauser (2016).
[14] Houdré, C. and Matzinger, H., On the variance of the optimal alignments score for binary random words and an asymmetric scoring function, Under Revision: J. Stat. Phys (2016).
[15] Its, A. R., Tracy, C. and Widom, H. Random words, Toeplitz determinants, and integrable systems. I. Random matrix models and their applications. Math. Sci. Res. Inst. Publ., 40, 2001. MR-1842789
[16] Its, A. R., Tracy, C. and Widom, H. Random words, Toeplitz determinants, and integrable systems. II. Advances in nonlinear mathematics and science. Phys. D, 152-153:199-224, 2001. MR-1837910
[17] Johansson, K. Transversal fluctuations for increasing subsequences on the plane, Probab. Theory Related Fields 116, (2000) 445-456. MR-1757595
[18] Lember, J. and Matzinger, H., Standard deviation of the LCS when zero and one have different probabilities, Annals of Probability 37, (2009), 1192-1235. MR-2537552
[19] Lueker, G. S., Improved bounds on the average length of longest common subsequences Journal of the ACM, 56, Art. 17, (2009). MR-2536132
[20] Robin, S., Rodolphe, F., and Schbath, S., ADN, mots et modèles, Belin, Paris, 2003.
[21] Sankoff, D., and Kruskal, J., Time warps, string edits and macromolecules: The theory and practice of sequence comparison Center for the Study of Language and Information, 1999.
[22] Seppäläinen, T., Scaling for a one-dimensional directed polymer with boundary conditions, Ann. Probab. 40, (2012) 19-73. MR-2917766
[23] Steele, J. M., Long common subsequences and the proximity of two random strings, SIAM J. Appl. Math. 42 (1982), 731-737. MR-0665382
[24] Waterman, M. S., Estimating statistical significance of sequence alignments Phil. Trans. R. Soc. Lond. B. (1994), 383-390.
[25] Waterman, M. S., Introduction to Computational Biology: Maps, Sequences and Genomes (Interdisciplinary Statistics), CRC Press (2000).

# Electronic Journal of Probability Electronic Communications in Probability 

## Advantages of publishing in EJP-ECP

- Very high standards
- Free for authors, free for readers
- Quick publication (no backlog)
- Secure publication (LOCKSS ${ }^{1}$ )
- Easy interface (EJMS²)


## Economical model of EJP-ECP

- Non profit, sponsored by $\mathrm{IMS}^{3}, \mathrm{BS}^{4}$, ProjectEuclid ${ }^{5}$
- Purely electronic


## Help keep the journal free and vigorous

- Donate to the IMS open access fund ${ }^{6}$ (click here to donate!)
- Submit your best articles to EJP-ECP
- Choose EJP-ECP over for-profit journals

[^1]
[^0]:    *Georgia Institute of Technology, School of Mathematics, Atlanta, GA, 30332-0160. E-mail: houdre@math. gatech. edu. Research partially supported by the grant \# 246283 from the Simons Foundation and by a Simons Fellowship grant \# 267336.
    ${ }^{\dagger}$ Georgia Institute of Technology, School of Mathematics, Atlanta, GA, 30332-0160. E-mail: matzi@math. gatech.edu

[^1]:    ${ }^{1}$ LOCKSS: Lots of Copies Keep Stuff Safe http://www.lockss.org/
    ${ }^{2}$ EJMS: Electronic Journal Management System http://www.vtex.lt/en/ejms.html
    ${ }^{3}$ IMS: Institute of Mathematical Statistics http://www.imstat.org/
    ${ }^{4}$ BS: Bernoulli Society http://www.bernoulli-society .org/
    ${ }^{5}$ Project Euclid: https://projecteuclid.org/
    ${ }^{6}$ IMS Open Access Fund: http://www.imstat.org/publications/open.htm

