

Hidden Words Statistics for Large Patterns

Svante Janson*

Department of Mathematics
Uppsala University, PO Box 480
SE-751 06 Uppsala, Sweden

svante.janson@math.uu.se

Wojciech Szpankowski†

Department of Computer Science
Purdue University
West Lafayette, IN, U.S.A.

szpan@purdue.edu

Submitted: Mar 20, 2020; Accepted: Apr 15, 2021; Published: TBD

© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

We study here the so called *subsequence pattern matching* also known as *hidden pattern matching* in which one searches for a given pattern w of length m as a *subsequence* in a random text of length n . The quantity of interest is the number of occurrences of w as a subsequence (i.e., occurring in *not* necessarily consecutive text locations). This problem finds many applications from intrusion detection, to trace reconstruction, to deletion channel, and to DNA-based storage systems. In all of these applications, the pattern w is of variable length. To the best of our knowledge this problem was only tackled for a fixed length $m = O(1)$. In our main result we prove that for $m = o(n^{1/3})$ the number of subsequence occurrences is normally distributed. In addition, we show that under some constraints on the structure of w the asymptotic normality can be extended to $m = o(\sqrt{n})$. For a special pattern w consisting of the same symbol, we indicate that for $m = o(n)$ the distribution of number of subsequences is either asymptotically normal or asymptotically log normal. After studying some special patterns (e.g., alternating) we conjecture that this dichotomy is true for all patterns. We use Hoeffding's projection method for U -statistics to prove our findings.

Mathematics Subject Classifications: 60C05, 68W40, 68R05, 68R15

1 Introduction and Motivation

One of the most interesting and least studied problem in pattern matching is known as the *subsequence string matching* or the *hidden pattern matching* [12]. In this case, we search for a pattern $w = w_1w_2 \cdots w_m$ of length m in the text $\Xi^n = \xi_1 \dots \xi_n$ of length

*This work was partly supported by the Knut and Alice Wallenberg Foundation

†This work was partially supported by the NSF Center for Science of Information (CSoI) Grant CCF-0939370, and in addition by NSF Grants CCF-1524312, CCF-2006440, and CCF-2007238.

n as *subsequence*, that is, we are looking for indices $1 \leq i_1 < i_2 < \dots < i_m \leq n$ such that $\xi_{i_1} = w_1, \xi_{i_2} = w_2, \dots, \xi_{i_m} = w_m$. We say that w is *hidden* in the text Ξ^n . We do not put any constraints on the gaps $i_{j+1} - i_j$, so in language of [8] this is known as the *unconstrained* hidden pattern matching. The most interesting quantity of such a problem is the number of subsequence occurrences in the text generated by a random source. In this paper, we study the limiting distribution of this quantity when m , the length of the pattern, grows with n .

Hereafter, we assume that a memoryless source generates the text Ξ , that is, all symbols are generated independently with probability p_a for symbol $a \in \mathcal{A}$, where the alphabet \mathcal{A} is assumed to be finite. We denote by $p_w = \prod_j p_{w_j}$ the probability of the pattern w . Our goal is to understand the probabilistic behavior, in particular, the limiting distribution of the number of subsequence occurrences that we denote by $Z := Z_\Xi(w)$. It is known that the behavior of Z depends on the order of magnitude of the pattern length m . For example, for the *exact pattern matching* (i.e., the pattern w must occur as a *string* in consecutive positions of the text), the limiting distribution is normal for $m = O(1)$ (more precisely, when $np_w \rightarrow \infty$, hence up to $m = O(\log n)$), but it becomes a Pólya–Aeppli distribution when $np_w \rightarrow \lambda > 0$ for some constant λ , and finally (conditioned on being non-zero) it turns into a geometric distribution when $np_w \rightarrow 0$ [12] (see also [2]). We might expect a similar behaviour for the subsequence pattern matching. In [8] it was proved by analytic combinatoric methods that the number of subsequence occurrences, $Z_\Xi(w)$, is asymptotically normal when $m = O(1)$, and not much is known beyond this regime. (See also [3]). Asymptotic normality for fixed m follows also by general results for U -statistics [10]. However, in many applications – as discussed below – we need to consider patterns w whose lengths grow with n .

In this paper, we prove two main results. In Theorem 6 we establish that for $m = o(n^{1/3})$ the number of subsequence occurrences is normally distributed. Furthermore, in Theorem 7 we show that under some constraints on the structure of w , the asymptotic normality can be extended to $m = o(\sqrt{n})$. Moreover, for the special pattern $w = a^m$ consisting of the same symbol repeated, we show in Theorem 4 that for $m = o(\sqrt{n})$, the distribution of number of occurrences is asymptotically normal, while for larger m (up to cn for some $c > 0$) it is asymptotically log-normal. We study more special patterns in Section 4 and conjecture that this dichotomy is true for a large class of patterns. Finally, for typical random w we establish in Corollary 20 that Z is asymptotically normal for $m = o(n^{2/5})$.

Regarding methodology, unlike [8] we use here probabilistic tools. We first observe that Z can be represented as a U -statistic (see (2.3) and Section 3.2). This suggests to apply the Hoeffding projection method [10] to prove asymptotic normality of Z for some large patterns. Indeed, we first decompose Z into a sum of orthogonal random variables with variances of decreasing order in n (for m not too large), and show that the variable of the largest variance converges to a normal distribution, proving our main results Theorems 6 and 7.

The hidden pattern matching problem, especially for large patterns, finds many applications from intrusion detection, to trace reconstruction, to deletion channel, to DNA-

based storage systems [1, 4, 5, 6, 12, 17]. Here we discuss below in some detail two of them, namely the deletion channel and the trace reconstruction problem.

A deletion channel [5, 6, 7, 14, 17, 20] with parameter d takes a binary sequence $\Xi^n = \xi_1 \cdots \xi_n$ where $\xi_i \in \mathcal{A}$ as input and deletes each symbol in the sequence independently with probability d . The output of such a channel is then a *subsequence* $\zeta = \zeta(x) = \xi_{i_1} \cdots \xi_{i_M}$ of Ξ , where M follows the binomial distribution $\text{Binom}(n, (1-d))$, and the indices i_1, \dots, i_M correspond to the bits that are *not* deleted. Despite significant effort [6, 14, 15, 17, 20] the mutual information between the input and output of the deletion channel and its capacity are still unknown. However, it turns out that the mutual information $I(\Xi^n; \zeta(\Xi^n))$ can be exactly formulated as the problem of the subsequence pattern matching. In [5] it was proved that

$$I(\Xi^n; \zeta(\Xi^n)) = \sum_w d^{n-|w|} (1-d)^{|w|} (\mathbb{E}[Z_{\Xi^n}(w) \log Z_{\Xi^n}(w)] - \mathbb{E}[Z_{\Xi^n}(w)] \log \mathbb{E}[Z_{\Xi^n}(w)]), \quad (1.1)$$

where the sum is over all binary sequences of length smaller than n and $Z_{\Xi^n}(w)$ is the number of subsequence occurrences of w in the text Ξ^n . As one can see, to find precise asymptotics of the mutual information we need to understand the probabilistic behavior of Z for $m \leq n$ and typical w . The trace reconstruction problem [4, 11, 16, 18] is related to the deletion channel problem since we are asking how many copies of the output deletion channel we need to see until we can reconstruct the input sequence with high probability.

The rest of the paper is structured as follows. Section 2 contains detailed definitions and some other preliminaries, followed by first (Theorem 4) detailed results for the simple example of a pattern $w = a^m$, which can be treated by elementary methods. Then we present our main results (Theorems 6 and 7). The proofs of the main results are given in Section 3. Section 4 discusses some special cases; in particular, we consider a random pattern w (Theorem 19 and Corollary 20). In the concluding section we comment on the sharpness of our results and conditions, and state a conjecture for a possible extension to larger m .

2 Main Results

In this section we formulate precisely our problem and present our main results. Proofs are delayed till the next section.

2.1 Problem formulation and notation

We consider a random string $\Xi^n = \xi_1 \dots \xi_n$ of length n . We assume that ξ_1, ξ_2, \dots are i.i.d. random letters from a finite alphabet \mathcal{A} ; each letter ξ_i has the distribution

$$\mathbb{P}(\xi_i = a) = p_a, \quad a \in \mathcal{A}, \quad (2.1)$$

for some given vector $\mathbf{p} = (p_a)_{a \in \mathcal{A}}$; we assume $p_a > 0$ for each a . We may also use ξ for a random letter with this distribution.

Let $w = w_1 \cdots w_m$ be a fixed string of length m over the same alphabet \mathcal{A} . We assume $n \geq m$. Let

$$p_w := \prod_{j=1}^m p_{w_j}, \quad (2.2)$$

which is the probability that $\xi_1 \cdots \xi_m$ equals w .

Let $Z = Z_{n,w}(\xi_1 \cdots \xi_n)$ be the number of occurrences of w as a subsequence of $\xi_1 \cdots \xi_n$. For a set \mathcal{S} (in our case $[n]$ or $[m]$) and $k \geq 0$, let $\binom{\mathcal{S}}{k}$ be the collection of sets $\alpha \subseteq \mathcal{S}$ with $|\alpha| = k$. Thus, $|\binom{\mathcal{S}}{k}| = \binom{|\mathcal{S}|}{k}$. For $k = 0$, $\binom{\mathcal{S}}{0}$ contains just the empty set \emptyset . For $k = 1$, we identify $\binom{\mathcal{S}}{1}$ and \mathcal{S} in the obvious way. We write $\alpha \in \binom{[n]}{k}$ as $\{\alpha_1, \dots, \alpha_k\}$, where we assume that $\alpha_1 < \cdots < \alpha_k$. Then

$$Z = \sum_{\alpha \in \binom{[n]}{m}} I_\alpha, \quad (2.3)$$

where

$$I_\alpha = \prod_{j=1}^m \mathbf{1}\{\xi_{\alpha_j} = w_j\}. \quad (2.4)$$

Remark 1. In the limit theorems, we are studying the asymptotic distribution of Z . We then assume that $n \rightarrow \infty$ and (usually) $m \rightarrow \infty$; we thus implicitly consider a sequence of words $w^{(n)}$ of lengths $m_n = |w^{(n)}|$. But for simplicity we do not show this in the notation.

We have $\mathbb{E} I_\alpha = p_w$ for every α . Hence,

$$\mathbb{E} Z = \sum_{\alpha \in \binom{[n]}{m}} \mathbb{E} I_\alpha = \binom{n}{m} p_w. \quad (2.5)$$

Further, let

$$Y_\alpha := p_w^{-1} I_\alpha, \quad (2.6)$$

so $\mathbb{E} Y_\alpha = 1$, and

$$Z^* := p_w^{-1} Z = \sum_{\alpha \in \binom{[n]}{m}} Y_\alpha, \quad (2.7)$$

so $\mathbb{E} Z^* = \binom{n}{m}$ and

$$Z^* - \mathbb{E} Z^* = p_w^{-1} Z - \binom{n}{m} = \sum_{\alpha \in \binom{[n]}{m}} (Y_\alpha - 1). \quad (2.8)$$

We also write $\|Y\|_p := (\mathbb{E} |Y|^p)^{1/p}$ for the L^p norm of a random variable Y , while $\|\mathbf{x}\|$ is the usual Euclidean norm of a vector \mathbf{x} in some \mathbb{R}^m . Also, \xrightarrow{d} and \xrightarrow{p} mean convergence in distribution and probability, respectively. Finally, C denotes constants that may be different at different occurrences; they may depend on the alphabet \mathcal{A} and $(p_a)_{a \in \mathcal{A}}$, but not on n , m or w .

We are now ready to present our main results regarding the limiting distribution of Z , the number of subsequence $w = a_1, \dots, a_m$ occurrences when $m \rightarrow \infty$. We start with a simple example, namely, $w = a^m = a \cdots a$ for some $a \in \mathcal{A}$, and show that depending on whether $m = o(\sqrt{n})$ or not the number of subsequences will follow asymptotically either the normal distribution or the log-normal distribution.

Before we present our results we consider asymptotically normal and log-normal distributions in general, and discuss their relation.

2.2 Asymptotic normality and log-normality

If X_n is a sequence of random variables and a_n and b_n are sequences of real numbers, with $b_n > 0$, then

$$X_n \sim \text{AsN}(a_n, b_n) \tag{2.9}$$

means that

$$\frac{X_n - a_n}{\sqrt{b_n}} \xrightarrow{d} N(0, 1). \tag{2.10}$$

We say that X_n is *asymptotically normal* if $X_n \sim \text{AsN}(a_n, b_n)$ for some a_n and b_n , and *asymptotically log-normal* if $\ln X_n \sim \text{AsN}(a_n, b_n)$ for some a_n and b_n (this assumes $X_n \geq 0$). Note that these notions are equivalent when the asymptotic variance b_n is small, as made precise by the following lemma.

Lemma 2. *If $b_n \rightarrow 0$, and a_n are arbitrary, then*

$$\ln X_n \sim \text{AsN}(a_n, b_n) \iff X_n \sim \text{AsN}(e^{a_n}, b_n e^{2a_n}). \tag{2.11}$$

Proof. By replacing X_n by X_n/e^{a_n} , we may assume that $a_n = 0$. If $\ln X_n \sim \text{AsN}(0, b_n)$ with $b_n \rightarrow 0$, then $\ln X_n \xrightarrow{p} 0$, and thus $X_n \xrightarrow{p} 1$. It follows that $\ln X_n/(X_n - 1) \xrightarrow{p} 1$ (with $0/0 := 1$), and thus

$$\frac{X_n - 1}{b_n^{1/2}} = \frac{X_n - 1}{\ln X_n} \frac{\ln X_n}{b_n^{1/2}} \xrightarrow{d} N(0, 1), \tag{2.12}$$

and thus $X_n \sim \text{AsN}(1, b_n)$.

The converse is proved by the same argument. □

Remark 3. Lemma 2 is best possible. Suppose that $\ln X_n \sim \text{AsN}(a_n, b_n)$. If $b_n \rightarrow b > 0$, then $\ln(X_n/e^{a_n}) = \ln X_n - a_n \xrightarrow{d} N(0, b)$, and thus

$$X_n/e^{a_n} \xrightarrow{d} e^{\zeta_b}, \quad \zeta_b \sim N(0, b). \tag{2.13}$$

In this case (and only in this case), X_n thus converges in distribution, after scaling, to a log-normal distribution. If $b_n \rightarrow \infty$, then no linear scaling of X_n can converge in distribution to a non-degenerate limit, as is easily seen.

2.3 A simple example

We consider first a simple example where the asymptotic distribution can be found easily by explicit calculations. Fix $a \in \mathcal{A}$ and let $w = a^m = a \cdots a$, a string with m identical letters. Then, if $N = N_a$ is the number of occurrences of a in $\xi_1 \cdots \xi_n$, then

$$Z = \binom{N_a}{m}. \quad (2.14)$$

We will show that Z is asymptotically normal if m is small, and log-normal for larger m .

Theorem 4. *Let $w = a^m$. Suppose that $m < np_a$, with $np_a - m \gg n^{1/2}$.*

(i) *Then*

$$\ln Z \sim \text{AsN}\left(\ln \binom{np_a}{m}, n \left| \ln \left(1 - \frac{m}{np_a}\right) \right|^2 p_a(1 - p_a)\right). \quad (2.15)$$

(ii) *In particular, if $m = o(n)$, then*

$$\ln Z \sim \text{AsN}\left(\ln \binom{np_a}{m}, (p_a^{-1} - 1) \frac{m^2}{n}\right). \quad (2.16)$$

(iii) *If $m = o(n^{1/2})$, then this implies*

$$Z / \mathbb{E} Z \sim \text{AsN}\left(1, (p_a^{-1} - 1) \frac{m^2}{n}\right), \quad (2.17)$$

and thus

$$Z \sim \text{AsN}\left(\mathbb{E} Z, (p_a^{-1} - 1) \frac{m^2}{n} (\mathbb{E} Z)^2\right). \quad (2.18)$$

Proof. (i): We have $N_a \sim \text{Bin}(n, p_a)$. Define $Y := N_a - np_a$. Then, by the Central Limit Theorem,

$$Y \sim \text{AsN}(0, np_a(1 - p_a)). \quad (2.19)$$

By (2.14), we have

$$\begin{aligned} \ln Z - \ln \binom{np_a}{m} &= \ln \binom{np_a + Y}{m} - \ln \binom{np_a}{m} \\ &= \ln \Gamma(np_a + Y + 1) - \ln \Gamma(np_a + Y - m + 1) - \ln m! \\ &\quad - (\ln \Gamma(np_a + 1) - \ln \Gamma(np_a - m + 1) - \ln m!) \\ &= \int_{y=0}^Y \int_{x=-m}^0 (\ln \Gamma)''(np_a + x + y + 1) dx dy \end{aligned} \quad (2.20)$$

where $\Gamma(x)$ is the Euler gamma function. We fix a sequence $\omega_n \rightarrow \infty$ such that $np_a - m \gg \omega_n \gg n^{1/2}$; this is possible by the assumption. Note that (2.19) implies that $Y/\omega_n \xrightarrow{P} 0$, and thus $\mathbb{P}(|Y| \leq \omega_n) \rightarrow 1$. We may thus in the sequel assume $|Y| \leq \omega_n$. We assume also that n is so large that $np_a - m \geq 2\omega_n > 0$.

Stirling's formula implies, by taking the logarithm and differentiating twice (in the complex half-plane $\operatorname{Re} z > \frac{1}{2}$, say)

$$(\ln \Gamma)''(x) = \frac{1}{x} + O\left(\frac{1}{x^2}\right) = \frac{1}{x} \left(1 + O\left(\frac{1}{x}\right)\right), \quad x \geq 1. \quad (2.21)$$

Consequently, (2.20) yields, noting the assumptions just made imply $|Y| \leq \omega_n \leq \frac{1}{2}(np_a - m)$,

$$\begin{aligned} \ln Z - \ln \binom{np_a}{m} &= \int_{y=0}^Y \int_{x=-m}^0 \frac{1}{np_a + x + y + 1} \left(1 + O\left(\frac{1}{np_a - m}\right)\right) dx dy \\ &= \int_{y=0}^Y \int_{x=-m}^0 \frac{1}{np_a + x} \left(1 + O\left(\frac{\omega_n}{np_a - m}\right)\right) dx dy \\ &= \left(1 + O\left(\frac{\omega_n}{np_a - m}\right)\right) Y \int_{x=-m}^0 \frac{1}{np_a + x} dx \\ &= (1 + o(1)) Y \ln \frac{np_a}{np_a - m}. \end{aligned} \quad (2.22)$$

Consequently, using also (2.19), we obtain

$$\frac{\ln Z - \ln \binom{np_a}{m}}{n^{1/2} \left| \ln \left(1 - \frac{m}{np_a}\right) \right|} = (1 + o_P(1)) \frac{Y}{n^{1/2}} \xrightarrow{d} N(0, p_a(1 - p_a)), \quad (2.23)$$

which is equivalent to (2.15).

(ii): If $m = o(n)$, then $\left| \ln \left(1 - \frac{m}{np_a}\right) \right| \sim \frac{m}{np_a}$, and (2.16) follows.

(iii): If $m = o(n^{1/2})$, then (ii) applies, so (2.16) holds; hence Lemma 2 implies

$$Z / \binom{np_a}{m} \sim \operatorname{AsN}\left(1, (p_a^{-1} - 1) \frac{m^2}{n}\right). \quad (2.24)$$

Furthermore,

$$\mathbb{E} Z = \binom{n}{m} p_a^m = \frac{n^m e^{O(m^2/n)}}{m!} p_a^m \sim \frac{n^m}{m!} p_a^m \quad (2.25)$$

and, similarly, $\binom{np_a}{m} \sim \frac{n^m p_a^m}{m!}$. Hence, $\mathbb{E} Z \sim \binom{np_a}{m}$ and (2.17) follows from (2.24); (2.18) is an immediate consequence. \square

Example 5. Let $w = a^m$ as in Theorem 4, and let $m \sim c\sqrt{n}$ for some $c > 0$. Then, as $n \rightarrow \infty$, by Theorem 4(ii), with $Z = Z_n$, $z_n := \binom{np_a}{m}$ and $\sigma^2 := c^2(p_a - 1)$,

$$\ln Z_n \sim \operatorname{AsN}(\ln z_n, \sigma^2) \quad (2.26)$$

and thus

$$\ln \frac{Z_n}{z_n} \xrightarrow{d} N(0, \sigma^2). \quad (2.27)$$

Hence, Z_n/z_n converges in distribution to a log-normal distribution, so Z_n is asymptotically log-normal but not asymptotically normal. See also Remark 3.

2.4 General results

We now present our main results. However, first we discuss the road map of our approach. First, we observe that the representation (2.3) shows that Z can be viewed as a U -statistic. For convenience, we consider Z^* in (2.7), which differs from Z by a constant factor only, and show in (3.18) that $Z^* - \mathbb{E} Z^*$ can be decomposed into a sum $\sum_{\ell=1}^m V_\ell$ of orthogonal random variables V_ℓ such that, when m is not too large, $\text{Var}(\sum_{\ell=2}^m V_\ell) = o(\text{Var} V_1)$. Next, in Lemma 14 we prove that V_1 appropriately normalized converges to the standard normal distribution. This will allow us to conclude the asymptotic normality of Z .

Here, we only consider the region $m = o(n^{1/2})$. First, for $m = o(n^{1/3})$ we claim that the number of subsequence occurrences always is asymptotically normal.

Theorem 6. *If $m = o(n^{1/3})$, then*

$$Z \sim \text{AsN}\left(\binom{n}{m} p_w, \sigma_1^2 p_w^2\right), \quad (2.28)$$

where

$$\sigma_1^2 = \sum_{i=1}^n \sum_{a \in \mathcal{A}} p_a^{-1} \left(\sum_{j: w_j=a} \binom{i-1}{j-1} \binom{n-i}{m-j} \right)^2 - n \binom{n-1}{m-1}^2. \quad (2.29)$$

Furthermore, $\mathbb{E} Z = \binom{n}{m} p_w$ and $\text{Var} Z \sim p_w^2 \sigma_1^2$.

In the second main result, we restrict the patterns w to such that are not typical for the random text; however, we will allow $m = o(n^{1/2})$.

Theorem 7. *Let $\mathbf{q} = (q_a)_{a \in \mathcal{A}}$ be the proportions of the letters in w , i.e., $q_a := \frac{1}{m} \sum_{j=1}^m \mathbf{1}\{w_j = a\}$. Suppose that $\liminf_{n \rightarrow \infty} \|\mathbf{q} - \mathbf{p}\| > 0$. If further $m = o(n^{1/2})$, then we have the asymptotic normality*

$$Z \sim \text{AsN}\left(\binom{n}{m} p_w, \sigma_1^2 p_w^2\right), \quad (2.30)$$

where σ_1^2 is given by (2.29). Furthermore, $\mathbb{E} Z = \binom{n}{m} p_w$ and $\text{Var} Z \sim p_w^2 \sigma_1^2$.

We prove both theorems in Section 3.5 after some preliminary results as presented in the next section.

3 Analysis and Proofs

In this section we will prove our main results. We start with some preliminaries.

3.1 Preliminaries and more notation

Let, for $a \in \mathcal{A}$,

$$\varphi_a(x) := p_a^{-1} \mathbf{1}\{x = a\} - 1. \quad (3.1)$$

Thus, letting ξ be any random variable with the distribution of ξ_i ,

$$\mathbb{E} \varphi_a(\xi) = 0, \quad a \in \mathcal{A}. \quad (3.2)$$

Let $p_* := \min_a p_a$ and

$$B := p_*^{-1} - 1. \quad (3.3)$$

Lemma 8. *Let φ_a and B be as above.*

(i) *For every $a \in \mathcal{A}$,*

$$\mathbb{E}[\varphi_a(\xi)^2] = p_a^{-1} - 1 \leq B. \quad (3.4)$$

(ii) *For some $c_1 > 0$ and every $a \in \mathcal{A}$,*

$$\|\varphi_a(\xi)\|_2 = (p_a^{-1} - 1)^{1/2} \geq c_1. \quad (3.5)$$

(iii) *For any vector $\mathbf{r} = (r_a)_{a \in \mathcal{A}}$ with $\sum_a r_a = 1$,*

$$\left\| \sum_{a \in \mathcal{A}} r_a \varphi_a(\xi) \right\|_2 \geq \|\mathbf{r} - \mathbf{p}\| := \left(\sum_{a \in \mathcal{A}} |r_a - p_a|^2 \right)^{1/2}. \quad (3.6)$$

Proof. The definition (3.1) yields

$$\mathbb{E}[\varphi_a(\xi)^2] = p_a^{-2} \text{Var}[\mathbf{1}\{\xi = a\}] = p_a^{-2} p_a(1 - p_a) = p_a^{-1} - 1. \quad (3.7)$$

Hence, (3.4) and (3.5) follow, with B given by (3.3).

Finally, for every $x \in \mathcal{A}$, by (3.1) again,

$$\sum_{a \in \mathcal{A}} r_a \varphi_a(x) = r_x p_x^{-1} - \sum_{a \in \mathcal{A}} r_a = r_x/p_x - 1 \quad (3.8)$$

and thus

$$\mathbb{E} \left(\sum_{a \in \mathcal{A}} r_a \varphi_a(\xi) \right)^2 = \sum_{a \in \mathcal{A}} p_a (r_a/p_a - 1)^2 = \sum_{a \in \mathcal{A}} p_a^{-1} (r_a - p_a)^2 \quad (3.9)$$

and (3.6) follows. □

3.2 A decomposition

The representation (2.3) shows that Z is a special case of a U -statistic. (Recall that, in general, a U -statistic is a sum over subsets α as in (2.3) of $f(\xi_{\alpha_1}, \dots, \xi_{\alpha_k})$ for some function f .) For fixed m , the general theory of [10] applies and yields asymptotic normality. (Cf. [13, Section 4] for a related problem.) For $m \rightarrow \infty$ (our main interest), we can still use the orthogonal decomposition of [10], which in our case takes the following form.

By the definitions in Section 2.1 and (3.1),

$$Y_\alpha = \prod_{j=1}^m (p_{w_j}^{-1} \mathbf{1}\{\xi_{\alpha_j} = w_j\}) = \prod_{j=1}^m (\varphi_{w_j}(\xi_{\alpha_j}) + 1). \quad (3.10)$$

By multiplying out this product, we obtain

$$Y_\alpha = \sum_{\gamma \subseteq [m]} \prod_{j \in \gamma} \varphi_{w_j}(\xi_{\alpha_j}). \quad (3.11)$$

Hence,

$$Z^* = \sum_{\alpha \in \binom{[n]}{m}} Y_\alpha = \sum_{\alpha \in \binom{[n]}{m}} \sum_{\gamma \subseteq [m]} \prod_{j \in \gamma} \varphi_{w_j}(\xi_{\alpha_j}) = \sum_{\alpha \in \binom{[n]}{m}} \sum_{\gamma \subseteq [m]} \prod_{k=1}^{|\gamma|} \varphi_{w_{\gamma_k}}(\xi_{\alpha_{\gamma_k}}). \quad (3.12)$$

We rearrange this sum. First, let $\ell := |\gamma| \in [m]$, and consider all terms with a given ℓ . For each α and γ , with $|\gamma| = \ell$, let

$$\alpha_\gamma := \{\alpha_{\gamma_1}, \dots, \alpha_{\gamma_\ell}\} \in \binom{[n]}{\ell}. \quad (3.13)$$

For given $\gamma \in \binom{[m]}{\ell}$ and $\beta \in \binom{[n]}{\ell}$, the number of $\alpha \in \binom{[n]}{m}$ such that $\alpha_\gamma = \beta$ equals the number of ways to choose, for each $k \in [\ell + 1]$, $\gamma_k - \gamma_{k-1} - 1$ elements of α in a gap of length $\beta_k - \beta_{k-1} - 1$, where we define $\beta_0 = \gamma_0 = 0$ and $\beta_{\ell+1} = n + 1$, $\gamma_{\ell+1} = m + 1$; this number is

$$c(\beta, \gamma) := \prod_{k=1}^{\ell+1} \binom{\beta_k - \beta_{k-1} - 1}{\gamma_k - \gamma_{k-1} - 1}. \quad (3.14)$$

Consequently, combining the terms in (3.12) with the same α_γ ,

$$Z^* = \sum_{\ell=0}^m \sum_{\gamma \in \binom{[m]}{\ell}} \sum_{\beta \in \binom{[n]}{\ell}} c(\beta, \gamma) \prod_{k=1}^{\ell} \varphi_{w_{\gamma_k}}(\xi_{\beta_k}). \quad (3.15)$$

We define, for $0 \leq \ell \leq m$ and $\beta \in \binom{[n]}{\ell}$,

$$V_{\ell, \beta} := \sum_{\gamma \in \binom{[m]}{\ell}} c(\beta, \gamma) \prod_{k=1}^{\ell} \varphi_{w_{\gamma_k}}(\xi_{\beta_k}) \quad (3.16)$$

and

$$V_\ell := \sum_{\beta \in \binom{[n]}{\ell}} V_{\ell, \beta}. \quad (3.17)$$

Thus (3.15) yields the decomposition

$$Z^* = \sum_{\ell=0}^m V_\ell. \quad (3.18)$$

For $\ell = 0$, $\binom{[n]}{0}$ contains only the empty set \emptyset , and

$$V_0 = V_{0, \emptyset} = \binom{n}{m} = \mathbb{E} Z^*. \quad (3.19)$$

Furthermore, note that two summands in (3.15) with different β are orthogonal, as a consequence of (3.2) and independence of different ξ_i . Consequently, the variables $V_{\ell, \beta}$ ($\ell \in [m]$, $\beta \in \binom{[n]}{\ell}$) are orthogonal, and hence the variables V_ℓ ($\ell = 0, \dots, m$) are orthogonal.

Let

$$\sigma_\ell^2 := \text{Var}(V_\ell) = \mathbb{E} V_\ell^2 = \sum_{\beta \in \binom{[n]}{\ell}} \mathbb{E} V_{\ell, \beta}^2, \quad 1 \leq \ell \leq m. \quad (3.20)$$

Note also that by the combinatorial definition of $c(\beta, \gamma)$ given before (3.14), we see that

$$\sum_{\beta \in \binom{[n]}{\ell}} c(\beta, \gamma) = \binom{n}{m}, \quad (3.21)$$

since this is just the number of $\alpha \in \binom{[n]}{m}$, and

$$\sum_{\gamma \in \binom{[m]}{\ell}} c(\beta, \gamma) = \binom{n - \ell}{m - \ell}, \quad (3.22)$$

since this sum is the total number of ways to choose $m - \ell$ elements of the $n - \ell$ elements of α in the gaps.

3.3 The projection method

We use the projection method used by [10] to prove asymptotic normality for U -statistics. Translated to the present setting, the idea of the projection method is to approximate $Z^* - \mathbb{E} Z^* = Z^* - V_0$ by V_1 , thus ignoring all terms with $\ell \geq 2$ in the sum in (3.18). In order to do this, we estimate variances.

First, by (3.4) and the independence of the ξ_i ,

$$\left\| \prod_{k=1}^{\ell} \varphi_{w_{\gamma_k}}(\xi_{\beta_k}) \right\|_2 = \left(\prod_{k=1}^{\ell} \mathbb{E} |\varphi_{w_{\gamma_k}}(\xi_{\beta_k})|^2 \right)^{1/2} \leq B^{\ell/2}. \quad (3.23)$$

By Minkowski's inequality, (3.16), (3.23) and (3.22),

$$\|V_{\ell,\beta}\|_2 \leq \sum_{\gamma \in \binom{[m]}{\ell}} c(\beta, \gamma) B^{\ell/2} = B^{\ell/2} \binom{n-\ell}{m-\ell} \quad (3.24)$$

or, equivalently,

$$\mathbb{E} V_{\ell,\beta}^2 \leq B^\ell \binom{n-\ell}{m-\ell}^2. \quad (3.25)$$

This leads to the following estimates.

Lemma 9. For $1 \leq \ell \leq m$,

$$\sigma_\ell^2 := \mathbb{E} V_\ell^2 \leq \widehat{\sigma}_\ell^2 := B^\ell \binom{n}{\ell} \binom{n-\ell}{m-\ell}^2. \quad (3.26)$$

Proof. The definition of V_ℓ in (3.17) and (3.25) yield, since the summands $V_{\ell,\beta}$ are orthogonal,

$$\sigma_\ell^2 := \mathbb{E} V_\ell^2 = \sum_{\beta \in \binom{[m]}{\ell}} \mathbb{E} V_{\ell,\beta}^2 \leq \binom{n}{\ell} B^\ell \binom{n-\ell}{m-\ell}^2, \quad (3.27)$$

as needed. □

Note that, for $1 \leq \ell < m$,

$$\frac{\widehat{\sigma}_{\ell+1}^2}{\widehat{\sigma}_\ell^2} = B \frac{\binom{n}{\ell+1} \binom{n-\ell-1}{m-\ell-1}^2}{\binom{n}{\ell} \binom{n-\ell}{m-\ell}^2} = B \frac{n-\ell}{\ell+1} \left(\frac{m-\ell}{n-\ell} \right)^2 \leq B \frac{m^2}{(\ell+1)n}. \quad (3.28)$$

Lemma 10. If $m \leq B^{-1/2} n^{1/2}$, then

$$\text{Var}(Z^* - V_1) \leq B^2 m^2 \binom{n-1}{m-1}^2. \quad (3.29)$$

Proof. By (3.28) and the assumption, for $1 \leq \ell < m$,

$$\frac{\widehat{\sigma}_{\ell+1}^2}{\widehat{\sigma}_\ell^2} \leq \frac{1}{\ell+1} \leq \frac{1}{2}, \quad (3.30)$$

and thus, summing a geometric series,

$$\begin{aligned} \text{Var}(Z^* - V_1) &= \sum_{\ell=2}^m \text{Var}(V_\ell) \leq \sum_{\ell=2}^m \widehat{\sigma}_\ell^2 \leq \sum_{\ell=2}^m 2^{2-\ell} \widehat{\sigma}_2^2 \leq 2 \widehat{\sigma}_2^2 \\ &= B^2 n(n-1) \binom{n-2}{m-2}^2 \leq B^2 m^2 \binom{n-1}{m-1}^2. \end{aligned} \quad (3.31)$$

□

3.4 The first term V_1

For $\ell = 1$, we identify $\binom{[n]}{\ell}$ and $[n]$, and we write $V_{1,i} := V_{1,\{i\}}$. Note that, by (3.14),

$$c(i, j) := c(\{i\}, \{j\}) = \binom{i-1}{j-1} \binom{n-i}{m-j}. \quad (3.32)$$

Remark 11. For later use, we define also

$$\pi(i, j) := \frac{c(i, j)}{c(1, 1)} = \frac{c(i, j)}{\binom{n-1}{m-1}}. \quad (3.33)$$

Then, for fixed i , $(\pi(i, j))_j$ is a (shifted) hypergeometric distribution denoted as HGe:

$$\pi(i, j) = \mathbb{P}(X = j - 1) = \frac{\binom{i-1}{j-1} \binom{n-i}{m-j}}{\binom{n-1}{m-1}} \quad (3.34)$$

which we write as

$$X \sim \text{HGe}(n - 1, m - 1, i - 1). \quad (3.35)$$

For $\ell = 1$, (3.17) and (3.16) become

$$V_1 = \sum_{i=1}^n V_{1,i} \quad (3.36)$$

with, using (3.32),

$$V_{1,i} = \sum_{j=1}^m c(i, j) \varphi_{w_j}(\xi_i) = \sum_{j=1}^m \binom{i-1}{j-1} \binom{n-i}{m-j} \varphi_{w_j}(\xi_i). \quad (3.37)$$

Note that $V_{1,i}$ is a function of ξ_i , and thus the random variables $V_{1,i}$ are independent. Furthermore, (3.2) implies $\mathbb{E} V_{1,i} = 0$. Let

$$\tau_i^2 := \text{Var } V_{1,i} = \mathbb{E} V_{1,i}^2. \quad (3.38)$$

Then, see (3.20),

$$\sigma_1^2 = \text{Var } V_1 = \sum_{i=1}^n \text{Var } V_{1,i} = \sum_{i=1}^n \tau_i^2. \quad (3.39)$$

Observe that it follows from (3.37) and (3.1) that

$$\tau_i^2 = \sum_{a \in \mathcal{A}} p_a^{-1} \left(\sum_{j: w_j=a} \binom{i-1}{j-1} \binom{n-i}{m-j} \right)^2 - \binom{n-1}{m-1}^2. \quad (3.40)$$

Taking $\ell = 1$ in (3.25) yields the upper bound

$$\tau_i^2 = \mathbb{E} V_{1,i}^2 \leq B \binom{n-1}{m-1}^2, \quad i \in [n]. \quad (3.41)$$

Summing over i , or using (3.26), we obtain

$$\sigma_1^2 := \mathbb{E} V_1^2 \leq \widehat{\sigma}_1^2 := Bn \binom{n-1}{m-1}^2. \quad (3.42)$$

Remark 12. The upper bound (3.42), which is the case $\ell = 1$ of Lemma 9, is achievable. Indeed, for $w = a \cdots a$, by (3.40),

$$\tau_i^2 = (p_a^{-1} - 1) \binom{n-1}{m-1}^2, \quad (3.43)$$

and thus by (3.39),

$$\sigma_1^2 = n(p_a^{-1} - 1) \binom{n-1}{m-1}^2. \quad (3.44)$$

Now choose a to minimize p_a and recall (3.3).

We will see in Lemma 16 that the bound (3.42) is sharp within a constant factor much more generally.

We show also a general lower bound. This too is sharp, see Section 4.1.

Lemma 13. *There exists $c, c' > 0$ such that*

$$\sigma_1^2 \geq \frac{c}{m} \widehat{\sigma}_1^2 = c' \frac{n}{m} \binom{n-1}{m-1}^2. \quad (3.45)$$

Proof. We consider the first term in the sum in (3.37) separately, and write

$$V_{1,i} = c(i, 1) \varphi_{w_1}(\xi_i) + V'_{1,i}, \quad (3.46)$$

where

$$V'_{1,i} := \sum_{j=2}^m c(i, j) \varphi_{w_j}(\xi_i). \quad (3.47)$$

We have, by (3.32), $c(i, 1) = \binom{n-i}{m-1}$. Consequently, for any $i \in [n]$,

$$\frac{c(i, 1)}{c(1, 1)} = \frac{\binom{n-i}{m-1}}{\binom{n-1}{m-1}} = \frac{\prod_{k=0}^{m-2} (n-i-k)}{\prod_{k=0}^{m-2} (n-1-k)} = \prod_{k=0}^{m-2} \left(1 - \frac{i-1}{n-1-k}\right)$$

$$\geq 1 - \sum_{k=0}^{m-2} \frac{i-1}{n-1-k} \geq 1 - \frac{m(i-1)}{n-m+1}. \quad (3.48)$$

Let $\delta \leq 1/4$ be a fixed small positive number, chosen later. Assume that $i \leq 1 + \delta n/m$. In particular, either $i = 1$ or $m \leq m(i-1) \leq \delta n < n/2$, and thus (3.48) implies

$$\frac{c(i,1)}{c(1,1)} \geq 1 - \frac{m(i-1)}{n-m} \geq 1 - \frac{\delta n}{n/2} = 1 - 2\delta. \quad (3.49)$$

By (3.22), (3.49) implies

$$\sum_{j=2}^m c(i,j) = \binom{n-1}{m-1} - c(i,1) = c(1,1) - c(i,1) \leq 2\delta c(1,1). \quad (3.50)$$

Hence, by (3.47), Minkowski's inequality and (3.4), cf. (3.24),

$$\|V'_{1,i}\|_2 \leq \sum_{j=2}^m c(i,j) \|\varphi_{w_j}(\xi_i)\|_2 \leq \sum_{j=2}^m c(i,j) B^{1/2} \leq 2\delta B^{1/2} c(1,1). \quad (3.51)$$

Furthermore, (3.5) and (3.49) yield

$$\|c(i,1)\varphi_{w_1}(\xi_i)\|_2 \geq c(i,1)c_1 \geq c_1(1-2\delta)c(1,1) \geq \frac{1}{2}c_1c(1,1). \quad (3.52)$$

Finally, (3.46) and the triangle inequality yield, using (3.52) and (3.51),

$$\|V_{1,i}\|_2 \geq \|c(i,1)\varphi_{w_1}(\xi_i)\|_2 - \|V'_{1,i}\|_2 \geq (\frac{1}{2}c_1 - 2\delta B^{1/2})c(1,1). \quad (3.53)$$

We now choose $\delta := c_1/(8B^{1/2})$, and find that for some $c_2 > 0$,

$$\tau_i^2 := \|V_{1,i}\|_2^2 \geq c_2 c(1,1)^2, \quad i \leq 1 + \delta n/m. \quad (3.54)$$

Consequently, by (3.39),

$$\sigma_1^2 = \sum_{i=1}^n \tau_i^2 \geq \frac{\delta n}{m} c_2 c(1,1)^2 = c_3 \frac{n}{m} \binom{n-1}{m-1}^2. \quad (3.55)$$

This proves (3.45), with $c' := c_3$ and $c = c'/B$. \square

Lemma 14. *Suppose that $m = o(n)$. Then V_1 is asymptotically normal:*

$$V_1/\sigma_1 \xrightarrow{d} N(0,1). \quad (3.56)$$

Proof. We show that the central limit theorem applies to the sum $V_1 = \sum_i V_{1,i}$ in (3.36). The terms $V_{1,i}$ are independent and have means $\mathbb{E} V_{1,i} = 0$. We verify Lyapunov's condition.

The random variable ξ is defined on some probability space (Ω, \mathcal{F}, P) and takes values in the finite set \mathcal{A} . Thus the linear space \mathcal{V} of functions $\Omega \rightarrow \mathbb{R}$ of the form $f(\xi)$ has finite dimension $|\mathcal{A}|$. Moreover, every function in \mathcal{V} is bounded. The L^2 and L^3 norms $\|\cdot\|_2$ and $\|\cdot\|_3$ are thus finite on \mathcal{V} , and are thus both norms on the finite-dimensional vector space \mathcal{V} ; hence there exists a constant C such that for any function f ,

$$\|f(\xi)\|_3 \leq C\|f(\xi)\|_2. \quad (3.57)$$

In particular, since the definition (3.37) shows that $V_{1,i}$ is a function of $\xi_i \stackrel{d}{=} \xi$,

$$\|V_{1,i}\|_3 \leq C\|V_{1,i}\|_2 = C\tau_i, \quad 1 \leq i \leq n. \quad (3.58)$$

Furthermore, by (3.41) and (3.45),

$$\frac{\max_i \tau_i^2}{\sigma_1^2} \leq \frac{B \binom{n-1}{m-1}^2}{c' \frac{n}{m} \binom{n-1}{m-1}^2} = C \frac{m}{n} = o(1). \quad (3.59)$$

Consequently, using (3.58), (3.39) and (3.59),

$$\begin{aligned} \frac{\sum_{i=1}^n \mathbb{E} |V_{1,i}|^3}{\sigma_1^3} &= \frac{\sum_{i=1}^n \|V_{1,i}\|_3^3}{\sigma_1^3} \leq \frac{C \sum_{i=1}^n \tau_i^3}{\sigma_1^3} \leq C \frac{\max_i \tau_i \sum_{i=1}^n \tau_i^2}{\sigma_1^3} \\ &= C \frac{\max_i \tau_i}{\sigma_1} = o(1). \end{aligned} \quad (3.60)$$

This shows the Lyapunov condition, and thus a standard form of the central limit theorem, [9, Theorem 7.2.4 or 7.6.2], yields (3.56). \square

3.5 Proofs of Theorem 6 and 7

We next prove a general theorem showing asymptotic normality under some conditions.

Theorem 15. *Suppose that $n \rightarrow \infty$ and that*

$$m^2 \binom{n-1}{m-1}^2 = o(\sigma_1^2). \quad (3.61)$$

Then

$$\text{Var } Z = p_w^2 \text{Var } Z^* \sim p_w^2 \sigma_1^2 \quad (3.62)$$

and

$$\frac{Z^* - \mathbb{E} Z^*}{\sigma_1} \xrightarrow{d} N(0, 1), \quad (3.63)$$

$$\frac{Z - \mathbb{E} Z}{(\text{Var } Z)^{1/2}} = \frac{Z^* - \mathbb{E} Z^*}{(\text{Var } Z^*)^{1/2}} \xrightarrow{d} N(0, 1). \quad (3.64)$$

Proof. By Lemma 10 and (3.61),

$$\text{Var}\left(\frac{Z^* - V_1}{\sigma_1}\right) = \frac{\text{Var}(Z^* - V_1)}{\sigma_1^2} \leq B^2 \frac{m^2 \binom{n-1}{m-1}^2}{\sigma_1^2} = o(1). \quad (3.65)$$

Hence, recalling $\mathbb{E} V_1 = 0$,

$$\frac{Z^* - \mathbb{E} Z^* - V_1}{\sigma_1} \xrightarrow{\mathbb{P}} 0. \quad (3.66)$$

Combining (3.56) and (3.66), we obtain (3.63).

Furthermore, by (3.65), and since the terms in (3.18) are orthogonal,

$$\text{Var} Z^* = \text{Var} V_1 + \text{Var}(Z^* - V_1) = \sigma_1^2 + o(\sigma_1^2) \sim \sigma_1^2, \quad (3.67)$$

which yields (3.62), and also shows that we may replace σ_1 by $(\text{Var} Z^*)^{1/2}$ in (3.63), which yields (3.64); the equality in (3.64) is a trivial consequence of (2.7). \square

Now we are ready to prove our main results.

Proof of Theorem 6. By Lemma 13,

$$\frac{m^2 \binom{n-1}{m-1}^2}{\sigma_1^2} \leq C \frac{m^3}{n} = o(1). \quad (3.68)$$

Thus (3.61) holds, and the result follows by Theorem 15 together with (2.5) and (2.7). \square

Recall that in Theorem 7, the range of m is improved, assuming that w is *not* typical for the random source with probabilities $\mathbf{p} = (p_a)_{a \in \mathcal{A}}$ that we consider.

Proof of Theorem 7. By Theorem 15, with (3.61) verified by Lemma 16 below. \square

Lemma 16. *Let $\mathbf{q} = (q_a)_{a \in \mathcal{A}}$ be the proportions of the letters in w . Then*

$$\sigma_1^2 \geq \frac{m^2}{n} \binom{n}{m}^2 \|\mathbf{q} - \mathbf{p}\|^2 = n \binom{n-1}{m-1}^2 \|\mathbf{q} - \mathbf{p}\|^2. \quad (3.69)$$

Proof. Let

$$\psi_i(x) := \sum_{j=1}^m c(i, j) \varphi_{w_j}(x). \quad (3.70)$$

Thus (3.37) is $V_{1,i} = \psi_i(\xi_i)$, and (3.39) is, since $\mathbb{E} \psi_i(\xi) = 0$,

$$\sigma_1^2 = \text{Var} V_1 = \sum_{i=1}^n \mathbb{E} [\psi_i(\xi_i)^2] = \mathbb{E} \sum_{i=1}^n \psi_i(\xi)^2. \quad (3.71)$$

Hence, by the Cauchy–Schwarz inequality,

$$n\sigma_1^2 = n \mathbb{E} \sum_{i=1}^n \psi_i(\xi)^2 \geq \mathbb{E} \left(\sum_{i=1}^n \psi_i(\xi) \right)^2. \quad (3.72)$$

Furthermore, by (3.70) and (3.21)

$$\sum_{i=1}^n \psi_i(x) = \sum_{i=1}^n \sum_{j=1}^m c(i, j) \varphi_{w_j}(x) = \sum_{j=1}^m \binom{n}{m} \varphi_{w_j}(x) = \binom{n}{m} \sum_{a \in \mathcal{A}} m q_a \varphi_a(x). \quad (3.73)$$

Hence, (3.6) yields

$$\left\| \sum_{i=1}^n \psi_i(\xi) \right\|_2 = m \binom{n}{m} \left\| \sum_{a \in \mathcal{A}} q_a \varphi_a(\xi) \right\|_2 \geq m \binom{n}{m} \|\mathbf{q} - \mathbf{p}\|. \quad (3.74)$$

Combining (3.72) and (3.74) yields (3.69). \square

4 Some Special Cases

In this section we consider two interesting cases. In the first we assume that the pattern w is alternating and in the second case we consider random w .

4.1 Alternating w

As an extreme example, we consider alternating w , that is, $w = 010101 \dots$ for $\mathcal{A} = \{0, 1\}$. We prove that this case matches the general lower bound (3.45) in Lemma 13.

Theorem 17. *Consider the unbiased binary case $\mathcal{A} = \{0, 1\}$ and $p_0 = p_1 = \frac{1}{2}$, and let w be an alternating string $010101 \dots$. Then, for any $m \leq n/2$,*

$$\sigma_1^2 \leq 10 \frac{n}{m} \binom{n-1}{m-1}^2. \quad (4.1)$$

Proof. It is slightly more convenient to let $\mathcal{A} = \{\pm 1\}$; thus we consider $w = w_1 \cdots w_m$ with

$$w_j = (-1)^j \quad (4.2)$$

in the unbiased case $p_1 = p_{-1} = \frac{1}{2}$. Then, by (3.1), for $x \in \mathcal{A}$,

$$\varphi_1(x) = 2 \cdot \mathbf{1}\{x = 1\} - 1 = x \quad (4.3)$$

$$\varphi_{-1}(x) = 2 \cdot \mathbf{1}\{x = -1\} - 1 = -x, \quad (4.4)$$

and thus, for $a, x \in \mathcal{A}$,

$$\varphi_a(x) = ax. \quad (4.5)$$

By (3.37), (4.5) and (4.2),

$$V_{1,i} = \sum_{j=1}^m c(i,j)w_j\xi_i = \sum_{j=1}^m (-1)^j c(i,j)\xi_i =: \tau_i \xi_i, \quad (4.6)$$

where we thus define

$$\tau_i := \sum_{j=1}^m (-1)^j c(i,j) = \sum_{j=1}^m (-1)^j \binom{i-1}{j-1} \binom{n-i}{m-j}. \quad (4.7)$$

Note that (4.6) gives $\mathbb{E} V_{1,i}^2 = \tau_i^2$, so (4.7) is consistent with our earlier definition (3.38). (The sign of τ_i is irrelevant for our purposes.) By (4.7) and (3.33)–(3.34), we have, with $\pi(i,j)$ and $X \sim \text{HGe}(n-1, m-1, i-1)$, as defined in Remark 11,

$$\frac{-\tau_i}{\binom{n-1}{m-1}} = \sum_{j=1}^m (-1)^{j-1} \pi(i,j) = \sum_{j=1}^m (-1)^{j-1} \mathbb{P}(X = j-1) = \mathbb{E}(-1)^X. \quad (4.8)$$

By Lemma 18 below, this implies, for $2 \leq m \leq n/2$ and $1 \leq i \leq (n+1)/2$,

$$\frac{|\tau_i|}{\binom{n-1}{m-1}} \leq \exp\left(-\frac{(i-1)(n-i)(m-1)(n-m)}{(n-1)^2(n-2)}\right) \leq \exp\left(-\frac{(i-1)m}{8n}\right). \quad (4.9)$$

This enables us to conclude, using the symmetry $|\tau_i| = |\tau_{n+1-i}|$ and still assuming $2 \leq m \leq n/2$, that

$$\begin{aligned} \sigma_1^2 &= \sum_{i=1}^n \tau_i^2 \leq 2 \sum_{i=1}^{\lfloor n/2 \rfloor} \tau_i^2 \leq 2 \binom{n-1}{m-1}^2 \sum_{i=1}^{\infty} e^{-(i-1)m/4n} \\ &= \frac{2}{1 - e^{-m/4n}} \binom{n-1}{m-1}^2 \leq \frac{10n}{m} \binom{n-1}{m-1}^2, \end{aligned} \quad (4.10)$$

as claimed in (4.1). The case $m = 1$ is trivial by (3.42), with $B = 1$ by (3.3). \square

Lemma 18. *Suppose that X is a hypergeometric random variable $X \sim \text{HGe}(n, k, \ell)$. Then*

$$|\mathbb{E}(-1)^X| \leq \exp(-2 \text{Var } X) = \exp\left(-2 \frac{k(n-k)\ell(n-\ell)}{n^2(n-1)}\right). \quad (4.11)$$

Note that the expectation in (4.11) is the difference of the probabilities that X is even or odd.

Proof. By (a special case of) a theorem by [19], the probability generating function of X has only negative real zeroes, and thus there exist probabilities $r_i \in [0, 1]$, $i = 1, \dots, k$,

such that if $I_i \sim \text{Be}(r_i)$ are independent indicator variables, then $\sum_i I_i$ has the same distribution as X , i.e.,

$$X \stackrel{d}{=} \sum_i I_i. \quad (4.12)$$

Hence, with $s_i := 1 - r_i$,

$$\mathbb{E}(-1)^X = \mathbb{E}(-1)^{\sum_i I_i} = \prod_i \mathbb{E}(-1)^{I_i} = \prod_i (s_i - r_i) \quad (4.13)$$

and thus, using also $\text{Var } X = \sum_i \text{Var } I_i$ by (4.12),

$$\begin{aligned} |\mathbb{E}(-1)^X| &= \prod_i |s_i - r_i| = \prod_i (1 - 2 \min\{r_i, s_i\}) \leq \prod_i (1 - 2r_i s_i) \\ &\leq \exp\left(-2 \sum_i r_i s_i\right) = \exp\left(-2 \sum_i \text{Var } I_i\right) \\ &= \exp(-2 \text{Var } X). \end{aligned} \quad (4.14)$$

This yields (4.11) by the standard formula

$$\text{Var } X = \frac{k(n-k)\ell(n-\ell)}{n^2(n-1)}. \quad (4.15)$$

This completes the proof. \square

4.2 A random w

Theorem 7 applies when w is far from a typical string Ξ_m from our random source. In this subsection we consider the opposite case, i.e., when w is like Ξ_m . More precisely, we consider the case when $w = W$ is a random string, of a given length m , drawn from the same source; thus $W \stackrel{d}{=} \Xi_m$, but W is independent of Ξ_n . (We use capital W to emphasize that the string is random.) We think of this as a two-stage random experiment. First we sample W ; then we sample Ξ . Conditioned on $W = w$, we thus have the same situation as before.

We write, for example, $\sigma_1^2(w)$ to indicate the dependence on w ; thus $\sigma_1^2(W)$ is a random variable. The next theorem shows that $\sigma_1^2(W)$ is concentrated about a value that is roughly the geometric mean of the upper and lower bounds in (3.42) and (3.45).

Theorem 19. *Let $W \stackrel{d}{=} \Xi_m$. Then, for $n \geq 1$ and $1 \leq m \leq n/2$,*

$$\mathbb{E}[\sigma_1^2(W)] = \Theta\left(\frac{n}{\sqrt{m}} \binom{n-1}{m-1}\right). \quad (4.16)$$

Furthermore, if also $m, n \rightarrow \infty$, then

$$\frac{\sigma_1^2(W)}{\mathbb{E}[\sigma_1^2(W)]} \rightarrow 1 \quad (4.17)$$

in probability.

Corollary 20. For random $w = W \stackrel{d}{=} \Xi_m$, (3.61) holds for $m = o(n^{2/5})$ with high probability, and hence for a typical pattern w the number of w occurrences Z is asymptotically normal as long as $m = o(n^{2/5})$. More precisely, in this case

$$Z/\mathbb{E}Z \sim \text{AsN}\left(1, \frac{\mathbb{E}[\sigma_1^2(W)]}{\mathbb{E}^2[Z]}\right) \quad (4.18)$$

with $\mathbb{E}[Z] = \binom{n}{m} 2^{-mh+O_p(m^{1/2})}$ where $h = -\sum_{a \in \mathcal{A}} p_a \log p_a$ is the source entropy.

Proof of Theorem 19. Define the covariance matrix

$$\rho(a, b) := \text{Cov}(\varphi_a(\xi), \varphi_b(\xi)), \quad a, b \in \mathcal{A}. \quad (4.19)$$

We have already computed $\rho(a, a) = p_a^{-1} - 1$ in (3.7). Similarly, in general, recalling (3.1),

$$\rho(a, b) = p_a^{-1} p_b^{-1} \text{Cov}(\mathbf{1}\{\xi = a\}, \mathbf{1}\{\xi = b\}) = p_a^{-1} \mathbf{1}\{a = b\} - 1. \quad (4.20)$$

By (3.37), for a given string w ,

$$\begin{aligned} \tau_i^2(w) &= \text{Var} V_{1,i} = \sum_{j=1}^m \sum_{k=1}^m c(i, j)c(i, k) \text{Cov}(\varphi_{w_j}(\xi_i), \varphi_{w_k}(\xi_i)) \\ &= \sum_{j=1}^m \sum_{k=1}^m c(i, j)c(i, k) \rho(w_j, w_k), \end{aligned} \quad (4.21)$$

where $\rho(w_j, w_k) = \text{Cov}(\varphi_{w_j}(\xi_i), \varphi_{w_k}(\xi_i))$. Thus, by (3.39),

$$\sigma_1^2(w) = \sum_{i=1}^n \tau_i^2(w) = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^m c(i, j)c(i, k) \rho(w_j, w_k). \quad (4.22)$$

Now let $w = W$ be random, with $W \stackrel{d}{=} \Xi_m$. Then, the letters W_j are i.i.d. with $W_j \stackrel{d}{=} \xi$. In particular, it follows from (4.20) that for any fixed a ,

$$\mathbb{E} \rho(W_j, a) = \mathbb{E} \rho(a, W_j) = 0, \quad (4.23)$$

and thus $\mathbb{E} \rho(W_j, W_k) = 0$ when $j \neq k$, while

$$\mathbb{E} \rho(W_j, W_j) = \sum_{a \in \mathcal{A}} p_a (p_a^{-1} - 1) = |\mathcal{A}| - 1 =: A_1. \quad (4.24)$$

Consequently, taking the expectation in (4.22) and recalling (3.33),

$$\mathbb{E}[\sigma_1^2(W)] = \sum_{i=1}^n \sum_{j=1}^m \sum_{k=1}^m c(i, j)c(i, k) \mathbb{E} \rho(W_j, W_k) = A_1 \sum_{i=1}^n \sum_{j=1}^m c(i, j)^2$$

$$= A_1 \binom{n-1}{m-1}^2 \sum_{i=1}^n \sum_{j=1}^m \pi(i, j)^2. \quad (4.25)$$

where $\pi(i, j)$ is defined in Remark 11. We thus want to estimate the final double sum.

First, fix i and recall from (3.34) that $(\pi(i, j))_j$ is the probability distribution of $X + 1$ with $X \sim \text{HGe}(n-1, m-1, i-1)$. Let $\mu := \mathbb{E} X + 1$ and $\gamma^2 := \text{Var} X$. By Chebyshev's inequality,

$$\sum_{|j-\mu|>2\gamma} \pi(i, j) = \mathbb{P}(|X + 1 - \mu| > 2\gamma) \leq \frac{1}{4}, \quad (4.26)$$

and thus by the Cauchy–Schwarz inequality,

$$\frac{9}{16} \leq \left(\sum_{|j-\mu|\leq 2\gamma} \pi(i, j) \right)^2 \leq (4\gamma + 1) \sum_{|j-\mu|\leq 2\gamma} \pi(i, j)^2. \quad (4.27)$$

Furthermore, see (4.15), $\gamma^2 = \text{Var} X \leq im/n$. Hence,

$$\sum_{j=1}^m \pi(i, j)^2 \geq \frac{C}{\gamma + 1} \geq C \min(\gamma^{-1}, 1) \geq C \min\left(\left(\frac{n}{mi}\right)^{1/2}, 1\right). \quad (4.28)$$

Summing over $n/2 \leq i \leq n$, say, yields

$$\sum_{i=1}^n \sum_{j=1}^m \pi(i, j)^2 \geq C \frac{n}{m^{1/2}}. \quad (4.29)$$

In the opposite direction, we again fix i and note that

$$\sum_{j=1}^m \pi(i, j)^2 \leq \max_j \pi(i, j) \sum_{j=1}^m \pi(i, j) = \max_j \pi(i, j). \quad (4.30)$$

It follows from (3.32) that

$$\frac{\pi(i, j+1)}{\pi(i, j)} = \frac{c(i, j+1)}{c(i, j)} = \frac{(i-j)(m-j)}{j(n-i-m+j+1)}, \quad (4.31)$$

and it follows easily that the maximum in (4.30) is attained at

$$j = j_0 := \left\lceil \frac{im}{n+1} \right\rceil = \frac{im}{n} + O(1). \quad (4.32)$$

It is then easy to see, by Stirling's formula and some calculations, that for $i \leq \lceil n/2 \rceil$,

$$\max_j \pi(i, j) \leq C \left(\frac{n}{mi}\right)^{1/2}. \quad (4.33)$$

Hence, by (4.30) and (4.33),

$$\sum_{i=1}^n \sum_{j=1}^m \pi(i, j)^2 \leq 2 \sum_{i=1}^{\lceil n/2 \rceil} \max_j \pi(i, j) \leq C \sum_{i=1}^n \frac{n^{1/2}}{m^{1/2} i^{1/2}} \leq C \frac{n}{m^{1/2}}. \quad (4.34)$$

The result (4.16) for the expectation follows by (4.25), (4.29) and (4.34).

Next, we estimate the variance of $\sigma_1^2(W)$. Let

$$Y := \sigma_1^2(W) / \binom{n-1}{m-1}^2 = \sum_{j=1}^m \sum_{k=1}^n \sum_{i=1}^n \pi(i, j) \pi(i, k) \rho(W_j, W_k) \quad (4.35)$$

and note that, by (4.16),

$$\mathbb{E} Y = \Theta\left(\frac{n}{m^{1/2}}\right). \quad (4.36)$$

Since the random letters W_j are independent, it follows from (4.23) that the random variables $\rho(W_j, W_k)$, $j \leq k$, have covariances 0; furthermore, these variables are bounded. Hence, (4.35) implies

$$\text{Var } Y \leq C \sum_{j=1}^m \sum_{k=1}^m \left(\sum_{i=1}^n \pi(i, j) \pi(i, k) \right)^2. \quad (4.37)$$

To estimate (4.37), we split the inner sum into the ranges $i \leq \lceil n/2 \rceil$ and $i > \lceil n/2 \rceil$, using $(x + y)^2 \leq 2(x^2 + y^2)$; by symmetry it suffices to consider the case $i \leq \lceil n/2 \rceil$. It follows from (4.31) after some calculations that then

$$\begin{aligned} \pi(i, j) &\leq C e^{-C(j-j_0)^2/(j+j_0)} \pi(i, j_0) \leq C j_0^{-1/2} e^{-C(j-j_0)^2/(j+j_0)} \\ &\leq C j^{-1/2} e^{-C(j-j_0)^2/(j+j_0)} \end{aligned} \quad (4.38)$$

where j_0 is defined in (4.32). It follows, omitting the details, that for $1 \leq j \leq k \leq m$,

$$\sum_{i=1}^{\lceil n/2 \rceil} \pi(i, j) \pi(i, k) \leq C \frac{n}{m k^{1/2}} e^{-C(j-k)^2/m} \quad (4.39)$$

and thus (4.37) yields, using (4.36),

$$\begin{aligned} \text{Var } Y &\leq C \sum_{k=1}^m \sum_{j=1}^m \frac{n^2}{m^2 k} e^{-C(j-k)^2/m} \leq C \sum_{k=1}^m \frac{n^2}{m^{3/2} k} \leq C \frac{n^2}{m^{3/2}} \log m \\ &\leq C \frac{\log m}{m^{1/2}} (\mathbb{E} Y)^2. \end{aligned} \quad (4.40)$$

Consequently, as $m \rightarrow \infty$,

$$\text{Var} \left(\frac{\sigma_1^2(W)}{\mathbb{E}[\sigma_1^2(W)]} \right) = \text{Var} \left(\frac{Y}{\mathbb{E} Y} \right) \leq C \frac{\log m}{m^{1/2}} \rightarrow 0, \quad (4.41)$$

and (4.17) follows. \square

5 Concluding Remarks

Finally, we collect here some further comments, examples and conjectures, in the hope of stimulating further research.

Example 21. Consider again the case when $w = a^m = a \cdots a$ is a constant string, treated by a direct method in Section 2.3 and Theorem 4. Let us see what Theorem 15 yields. In this case, by (3.44), with $c_a := p_a^{-1} - 1 > 0$,

$$\sigma_1^2 = \sum_{i=1}^n \tau_i^2 = n c_a \binom{n-1}{m-1}^2, \quad (5.1)$$

and thus (3.61) reduces to $m^2 = o(n)$. (This also follows by Lemma 16.)

Consequently, Theorem 15 applies and shows asymptotic normality when $m = o(n^{1/2})$, which we already knew, see Theorems 4(iii) and 7. This example shows that Theorems 15 and 7 are sharp, in the sense that the range of m for which they yield asymptotic normality cannot be extended; see Example 5.

Remark 22. The argument in the proof of Theorem 7 applies also in other cases where σ_1^2 is of the same order as the upper bound in (3.42). Then Theorem 15 applies and shows asymptotic normality for $m = o(n^{1/2})$. A simple example is when $w = 0 \cdots 01 \cdots 1$, or more generally, when, say, the first and second half of w have different distributions of the letters, even if the average proportions in the entire string $\mathbf{q} = \mathbf{p}$. (This can be seen by a modification of the argument in the proof of Lemma 16.)

Based on these examples we conjecture the following.

Conjecture 23. *If $\sigma_1^2 = o\left(\binom{n}{m}^2\right)$, or equivalently $\sigma_1^2 = o\left(\frac{n^2}{m^2} \binom{n-1}{m-1}^2\right)$, then*

$$Z / \mathbb{E} Z \sim \text{AsN}\left(1, \frac{\sigma_1^2}{\binom{n}{m}^2}\right). \quad (5.2)$$

Moreover, at least as long as $m = o(n)$,

$$\ln Z \sim \text{AsN}\left(a_n, \frac{\sigma_1^2}{\binom{n}{m}^2}\right) \quad (5.3)$$

for some sequence a_n .

In particular, by (4.1), if Conjecture 23 holds, then for an alternating string $w = 0101 \cdots$, Z is asymptotically normal for any $m = o(n)$. Moreover, for random w as discussed in Section 4.2, by Theorem 19, Conjecture 23 suggests that asymptotic normality holds for $m = o(n^{2/3})$, and log-normality beyond that.

Note that this conjecture implies that if σ_1^2 is of a smaller order than the upper bound in (3.42) (for $n^{1/3} \leq m \leq n$, say), then asymptotic normality holds for a larger range of m than $o(n^{1/2})$, while our proof above, on the contrary, verifies this only in a range smaller than $m = o(n^{1/2})$.

References

- [1] M. Atallah, R. Gwadera and W. Szpankowski, Reliable detection of episodes in event sequences. *Third IEEE International Conference on Data Mining (ICDM-03)*, 67–74, Melbourne, Florida, November 2003.
- [2] E. A. Bender and F. Kochman, The distribution of subword counts is usually normal. *European Journal of Combinatorics* **14** (1993), 265–275.
- [3] J. Bourdon and B. Vallée, Generalized pattern matching statistics. In *Mathematics and Computer Science (Colloquium Proceedings, Versailles, 2002)*, B. Chauvin et al. eds., Birkhäuser Verlag, 2002, pp. 229–245.
- [4] M. Cheraghchi, R. Gabrys, O. Milenkovic and J. Ribeiro, Coded trace reconstruction. *IEEE Trans. Inform. Theory* **66** (2020), no. 10, 6084–6103.
- [5] M. Drmota, K. Viswanathan and W. Szpankowski, Mutual Information for a Deletion Channel, *ISIT 2012*, Boston, 2012.
- [6] S. Diggavi and M. Grossglauser, Information transmission over finite buffer channels, *IEEE Trans. Info. Th.*, **52** (2006), 1226–1237.
- [7] R. L. Dobrushin, Shannon’s theorem for channels with synchronization errors. *Problems Inform. Transmission* **3** (1967), no. 4, 11–26 (1969).
- [8] P. Flajolet, W. Szpankowski and B. Vallée, Hidden word statistics. *Journal of the ACM* **53** (2006), 1–37.
- [9] A. Gut, *Probability: A Graduate Course*, 2nd ed. Springer, New York, 2013.
- [10] W. Hoeffding, A class of statistics with asymptotically normal distribution. *Ann. Math. Statistics* **19** (1948), 293–325.
- [11] N. Holden and R. Lyons, Lower bounds for trace reconstruction. *Ann. Appl. Probab.* **30** (2020), no. 2, 503–525.
- [12] P. Jacquet and W. Szpankowski, *Analytic Pattern Matching: From DNA to Twitter*. Cambridge University Press, 2015.
- [13] S. Janson, B. Nakamura and D. Zeilberger. On the asymptotic statistics of the number of occurrences of multiple permutation patterns. *J. Comb.* **6** (2015), no. 1-2, 117–143.
- [14] A. Kalai, M. Mitzenmacher and M. Sudan, Tight asymptotic bounds for the deletion channel with small deletion probabilities. *ISIT*, Austin, 2010.
- [15] Y. Kanoria and A. Montanari, On the deletion channel with small deletion probability. *ISIT*, Austin, 2010; see [arXiv:1104.5546](https://arxiv.org/abs/1104.5546) for an extension.
- [16] A. McGregor, E. Price and S. Vorotnikova, Trace reconstruction revisited. *European Symposium on Algorithms* (2014), 689–700.
- [17] M. Mitzenmacher, A survey of results for deletion channels and related synchronization channels. *Probab. Surveys* **6** (2009), 1–33.
- [18] Y. Peres and A. Zhai, Average-case reconstruction for the deletion channel: subpolynomially many traces suffice. *FOCS*, 2017.

- [19] V. A. Vatutin and V. G. Mikhaïlov, Limit theorems for the number of empty cells in an equiprobable scheme for group allocation of particles. (Russian) *Teor. Veroyatnost. i Primenen.* **27** (1982), no. 4, 684–692. English transl.: *Theory Probab. Appl.* **27** (1983), no. 4, 734–743.
- [20] R. Venkataramanan, S. Tatikonda and K. Ramchandran, Achievable rates for channels with deletions and insertions. *ISIT*, St. Petersburg, Russia, 2011.