SORTING WITH UNRELIABLE COMPARISONS: A PROBABILISTIC ANALYSIS

LAURENT ALONSO, PHILIPPE CHASSAING, FLORENT GILLET, SVANTE JANSON, EDWARD M. REINGOLD, AND RENÉ SCHOTT

Abstract. We provide a probabilistic analysis of the output of Quicksort when comparisons can err.

1. Introduction

Suppose that a sorting algorithm unknowingly uses element comparisons that can err; that is, considering sorting algorithms based solely on binary comparisons of the elements to be sorted (algorithms such as insertion sort, selection sort, quicksort, and so on), what problems do we face when those comparisons are unreliable? For example, [3] gives a clever $\mathcal{O}\left(\epsilon^{-1}\log n\right)$ algorithm to assure, with probability $1-\epsilon$, that a putatively sorted sequence of length n is truly sorted. But knowing the structure of the ill-sorted output would likely make error checking easier. As a first step in order to understand this structure, we propose to analyze the number of inversions in the output of a sorting algorithm (we choose Quicksort [6]) subject to errors.

We assume throughout this paper that the elements of the sequence

$$x = (x_1, x_2, \ldots, x_n)$$

to be sorted are distinct. We assume further that the only comparisons subject to err are those made between elements being sorted; that is, comparisons among indices, and so on are always correct. Errors in element comparisons are random events, spontaneous and independent of each other, of position, and of value, with a common probability p, n being the length of the list to be sorted. The number of inversions in the output sequence $y = (y_1, y_2, \ldots, y_n)$ is denoted

$$I(y) = \#\left\{(i,j), 1 \le i < j \le n \mid y_i > y_j\right\}.$$

We assume that the input list is sorted in random order, each of the $n!$ random orders being equiprobable. Finally we denote by $I(n,p)$ the random number of inversions in the output sequence of Quicksort subject to errors.

Our result is, roughly speaking,

$$I(n,p) = \mathcal{O}\left(n^2 p\right),$$

in the sense that $\frac{I(n,p)}{n^2 p}$ converges in distribution to some nondegenerate random variable X which is characterized by a functional equation. The "surprise", not so unexpected afterwards, is that there are phase changes in the limit law, depending on the asymptotic behaviour of p. Here and later we regard n and p as independent variables. In the limit results we always assume $n \to \infty$ and $p \to c \in [0,1]$, often with further conditions added.

The organization of this paper is as follows: The results are stated in Section 2. In Section 3, we establish a general functional equation for $I(n,p)$. In the remaining sections, we prove convergence results for $I(n,p)$ when:

- $p \to c$, $0 < c \leq 1$,
- p vanishes slower than $1/n$,
- $p \simeq \lambda/n$ where λ is a positive constant.

The case $np \to 0$ is different and not treated in detail, see Remark 2.8. In Section 4, we establish a general result of convergence using contraction methods (cf. [10, 11]), and we use it in Section 5 , for the first two cases. These methods do not apply for Case 3, which requires poissonization (see Section 6, where we use an embedding of Quicksort in a Poisson point process).

2. Results

Set

$$X_{n,p} = \frac{I(n,p)}{n^2 p}.$$

We will always let U denote a random variable that is uniformly distributed on $[0,1]$. Also, $\mathbb{N}^*$ shall denote the set of positive integers, and $\mathbb{N}$ the set of nonnegative integers.

Case 1: $\lim p = c > 0$.

Theorem 2.1. *If $\lim p = c$, $c \in]0,1]$, $X_{n,p}$ converges in distribution to a random variable X_c whose distribution is characterized as the unique solution with finite mean of the equation*

$$X_c \stackrel{law}{=} [(1-2c)U + c]^2 X_c + [(2c-1)U + 1 - c]^2 \widetilde{X}_c + T(c,U), \tag{1}$$

in which $\widetilde{X}_c$ denotes an independent copy of X_c, both are independent of U, and

$$T(c,U) = \frac{1-c}{2}(U^2 + (1-U)^2) + cU(1-U).$$

Furthermore,

$$\mathbb{E}\left[X_c\right] = \frac{2-c}{2(1+2c-2c^2)},$$

and

$$\operatorname{Var}(X_c) = \frac{(1-c)^2(1-2c)^2}{4(1+2c-2c^2)^2(3+6c-8c^2+4c^3-2c^4)}.$$

As usual with laws related to Quicksort, see e.g. [10, 11], Un is approximately the position of the pivot of the first step of the algorithm. As in standard Quicksort recurrences, the coefficients of X_c and of its independent copy $\tilde{X}_c$ are related to the sizes of the two sublists on the left and right of the pivot, sizes respectively asymptotic to $((1-2c)U + c)\,n$ and $((2c-1)U + 1 - c)\,n$. The toll function $T(c,U)$ is approximately $(n^2p)^{-1} \approx (n^2c)^{-1}$ times the number of inversions created in the first step: $c(1-c)U^2n^2/2$ is approximately the number of inversions of the cUn elements, smaller than the pivot but misplaced on the right of it, with the elements smaller than the pivot, that are placed, as they should be, on the left, and $c^2U(1-U)n^2$ is the number of inversions between misplaced elements from the two sides of the pivot. The toll function $T(c,U)$ depends on only one of the two sources of randomness (the randomly sorted input list, and the places of the errors), viz. the first one, through U. The second source of randomness is killed by the law of large numbers: in the average, each of the $cUn + o(n)$ misplaced numbers from the right of the pivot produces inversions with one half of the $(1 - c)Un + o(n)$ elements smaller than the pivot, that are placed, as they should be, on the left. As opposed to the other values of c, the choices $c = 0.5$ and $c = 1$ lead to deterministic $X_c = 1/2$, without any surprise : for $p = 0.5$ the output sequence is a random uniform permutation, with a number of inversions concentrated around $n^2/4$; for $p = 1$ the output sequence is decreasing, and has $n(n - 1)/2$ inversions.

Case 2: p vanishes slower than $\frac{1}{n}$.

Theorem 2.2. *If* $\lim p = 0$ *and* $\lim np = +\infty$, $X_{n,p}$ *converges in distribution to a random variable* X *whose distribution is characterized as the unique solution with finite mean of the equation*

$$X \overset{law}{=} U^2 X + (1 - U)^2 \widetilde{X} + \frac{U^2 + (1 - U)^2}{2}. \tag{2}$$

In (2), $\widetilde{X}$ *denotes an independent copy of* X *and both are independent of* U. *Furthermore,*

$$\mathbb{E}[X] = 1 \qquad \textit{and} \qquad \mathrm{Var}(X) = \frac{1}{12}.$$

Note that equation (2) is just (1) specialized to $c = 0$. The phase transition between (1) and (2) is due to the fact that for $p \ll 1$ the errors do not change anymore the sizes of buckets (and the runtime) in a significant way. The solution X equals half the sum of the squares of the widths of the random intervals $[Y_{k,j}, Y_{k,j+1}]$ defined by (3) below. Also, $2X$ equals the area $\int_0^1 Z(t)\,dt$ under the FIND limit process Z [4], see Remark 2.5.

Case 3: $\lim np = \lambda$.

Assume that

- Π is a Poisson point process of intensity λ on $\mathbb{N}^* \times [0, 1]$ (we regard a Poisson process as a random set of points, see [5] for details);
- $\{U_{k,j} : k \geq 0, 1 \leq i \leq 2^k\}$ is an array of independent uniform random variables on $[0, 1]$, independent of Π;
- the random variables $Y_{k,j}$ are defined recursively by

$$\begin{aligned} Y_{0,0} = 0, \qquad Y_{0,1} = 1, \qquad Y_{k+1,2j} &= Y_{k,j} && \text{for } 0 \leq j \leq 2^k, \\ Y_{k+1,2j-1} &= (1 - U_{k,j})Y_{k,j-1} + U_{k,j}Y_{k,j} && \text{for } 1 \leq j \leq 2^k; \end{aligned} \tag{3}$$

- for $x \in [0, 1]$, $J_k(x) = 2j - 1$ if $Y_{k-1,j-1} \leq x < Y_{k-1,j}$,

and define, for $\lambda > 0$, (the sum is a.s. finite by Lemma 6.4)

$$X(\lambda) = \frac{1}{\lambda} \sum_{(k,x)\in\Pi} \left|x - Y_{k,J_k(x)}\right|. \tag{4}$$

The variables $Y_{k,j}$ describe a fragmentation process (see also [4] for historical references): we start with $[0, 1)$ and recursively break each interval into two at a random point (uniformly chosen). In the k-th generation we thus have a partition of $[0, 1)$ into 2^k intervals $I_{k,j}$, $1 \leq j \leq 2^k$, with $I_{k,j} = [Y_{k,j-1}, Y_{k,j})$. The interval of generation $k - 1$ that contains x is cut at step k at the point $Y_{k,J_k(x)}$. Hence $\left|x - Y_{k,J_k(x)}\right|$ in (4) is the distance from x to this cut point.

Theorem 2.3. *If* $\lim p = 0$ *and* $\lim np = \lambda > 0$, *then* $X_{n,p}$ *converges in distribution to* $X(\lambda)$. *The family* $\{X(\lambda)\}_{\lambda>0}$ *of random variables satisfy the functional equation:*

$$X(\lambda) \overset{law}{=} U^2 X(\lambda U) + (1-U)^2 \widetilde{X}(\lambda(1-U)) + \Theta(\lambda, U), \tag{5}$$

in which, conditionally, given that $U = u$, $X(\lambda U)$, $\widetilde{X}(\lambda(1-U))$ *and* $\Theta(\lambda, U)$ *are independent,* $X(\lambda U)$ *and* $\widetilde{X}(\lambda(1-U))$ *are distributed as* $X(\lambda u)$ *and* $X(\lambda(1-u))$, *respectively, and*

$$\Theta(\lambda, u) \overset{law}{=} \frac{1}{\lambda} \sum_{i=1}^{N_\lambda} |u - V_i|\,,$$

in which N_λ *is a Poisson random variable with mean* λ, *the random variables* V_i *are uniformly distributed on* $[0,1]$, *and* N_λ, *and the* V_i*'s are independent.*

Moreover, $\{X(\lambda)\}_{\lambda>0}$ *is (up to equivalence in laws) the only family of random variables satisfying* (5) *such that,* $X(\lambda) \geq 0$ *a.s.,* $\mathbb{E}[X(\lambda)^n] < \infty$ *for each* $n \geq 0$, *and* $\lambda^{2n-1}\mathbb{E}[X(\lambda)^n] \to 0$ *as* $\lambda \to 0$ *for each* $n \geq 1$.

Furthermore,

$$\mathbb{E}[X(\lambda)] = 1, \qquad \mathrm{Var}(X(\lambda)) = \frac{1}{12} + \frac{1}{3\lambda}. \tag{6}$$

Remark 2.4. Note that the functional equations (1), (2) and (5) really are equations for distributions, but it is more convenient to state them for random variables as done here. For (5) to make sense, it is implicitly assumed that the distributions $\mathcal{L}(X(\lambda))$ depend measurably on λ, i.e. that $\lambda \mapsto \mathbb{P}(X(\lambda) \in A)$ is measurable for every Borel set A. (For our $X(\lambda)$, measurability, and indeed continuity, in λ follows from (8) below.) We do not know whether the extra assumptions in Theorem 2.3 for uniqueness of the solution of (5) are necessary.

Let us comment further on equation (4). Writing $\Pi_k = \{x : (k,x) \in \Pi\}$ and $\Pi_{k,j} = \Pi_k \cap I_{k,j}$, we can thus rewrite (4) as

$$X(\lambda) = \frac{1}{\lambda} \sum_{k=1}^{\infty} \sum_{j=1}^{2^k} \sum_{x \in \Pi_{k,j}} |x - x_{k,j}|, \tag{7}$$

where $x_{k,j}$ is either the left or right endpoint of $I_{k,j}$ (depending on whether j is even or odd).

Note that, conditioned on the partitions $\{I_{k,j}\}$, i.e. on $\{Y_{k,j}\}_{k,j}$, each $\Pi_{k,j}$ is a Poisson process on $I_{k,j}$ with intensity λ, with the processes $\Pi_{k,j}$ independent. Since only the distribution of $X(\lambda)$ matters, we can by this conditioning and an obvious symmetry of the Poisson processes $\Pi_{k,j}$ just as well let $x_{k,j}$ in (7) be the left endpoint of $I_{k,j}$ for every k and j.

Let Π' be a Poisson process on $(0,1] \times (0,\infty)$ with intensity 1, and let $\xi(t) = \sum_{(x,y)\in\Pi',\, y \leq t} x$, $t \geq 0$. (This is a pure jump Lévy process with Lévy measure $\mathbb{1}_{(0,1]}dt$.) Let $\xi^{(k,j)}(t)$ be independent copies of this process, independent of $\{Y_{k,j}\}$. A scaling argument shows that (7) can be written

$$X(\lambda) = \frac{1}{\lambda} \sum_{k=1}^{\infty} \sum_{j=1}^{2^k} |I_{k,j}| \xi^{(k,j)}(\lambda |I_{k,j}|). \tag{8}$$

Remark 2.5. Let $X = \frac{1}{2}\sum_{k=1}^{\infty}\sum_{j=1}^{2^k}|I_{k,j}|^2$. Then X satisfies (2), so this is the limit variable X in Theorem 2.2. (X is a.s. finite and has finite mean by Lemma 6.1.) Moreover, the FIND limit process Z in [4] is defined by $Z(t) = \sum_{k=1}^{\infty}\sum_{j=1}^{2^k}|I_{k,j}|\mathbb{1}_{t\in I_{k,j}}$; hence $\int_0^1 Z(t)\,dt = \sum_{k=1}^{\infty}\sum_{j=1}^{2^k}|I_{k,j}|^2 = 2X$. This justifies the claims made after Theorem 2.2.

Moreover, by the law of large numbers, $\mathbb{E}|\lambda^{-1}\xi(\lambda) - 1/2| \to 0$ as $\lambda \to \infty$. It follows from (8) (by dominated convergence using Lemma 6.1) that $\mathbb{E}|X(\lambda)-X| \to 0$ and hence $X(\lambda)$ converges to X in distribution as $\lambda \to \infty$.

In this third case, we have a system of equations involving an infinite family of laws, and we could not adapt the contraction method: we rather use a poissonization. The phase transition from (2) to (5) is explained easily: instead of a number of errors $\gg 1$, we have now $\mathcal{O}(1)$ errors at each step, and the law of large numbers does not hold anymore for the number of inversions produced by step 1. Actually the number N_λ of errors at the first step is asymptotically Poisson distributed, and the N_λ errors are at positions nV_i, approximately uniformly distributed on $[0,1]$. Thus, the number of inversions caused by this first step is approximately

$$n\sum_{i=1}^{N_\lambda}|U - V_i| \approx n^2 p\Theta(\lambda, U).$$

Remark 2.6. Actually we prove a stronger theorem in each of the three cases, as we prove convergence of laws for the Wasserstein d_1 metric [9]. It entails convergence of the first moment. The convergence of higher moments is an open problem.

Remark 2.7. As we shall see in Section 6, the distribution tail $\mathbb{P}(X(\lambda) \geq x)$ decreases exponentially fast (Theorem 6.5).

Remark 2.8. When $np \to 0$ very slowly, that is $(np)^{-1} \ll \log n$, we conjecture that $2np\log(I(n,p)/n)$ converges in distribution to $\log U$, with the consequence that $n^{1-\varepsilon} \ll I(n,p) \ll n$, for any positive ε. Actually, the main contribution to $I(n,p)$ comes from the "first" error, in some sense. When $(np)^{-1} \simeq \log n$, the probability that no error occurs has a positive limit, and conditionally, given the occurence of at least one error, the situation is similar to the previous case, that is, $\log(I(n,p))/\log n$ converges in distribution to a random variable with values in $(0,1)$. When $(np)^{-1} \gg \log n$, $\mathbb{P}(I(n,p) = 0) \to 1$.

3. Functional equation for the number of inversions

At the first step Quicksort compares all elements of the input list with the first element of the list (usually called *pivot*). All items less (resp. larger) than the pivot are stored in a sublist on the left (resp. right) of the pivot. Comparisons are not reliable, therefore s_ℓ items that should belong to the left sublist are wrongly stored in the right sublist, and s_r items larger than the pivot are misplaced in the left sublist.

Since its items are chosen randomly, the input list is a random permutation and the rank of the pivot can be written $\lceil nU\rceil$, where U is uniformly distributed on $[0,1]$ and $\lceil x\rceil$ is the ceiling of x. Also, s_ℓ (resp. s_r) is a binomial random variable with parameters $(\lceil nU\rceil - 1,\ p)$ (resp. $(n - \lceil nU\rceil,\ p)$). Quicksort is then independently applied on the left sublist ℓ and on the right sublist r and new errors occur, producing two new sublists $\tilde{\ell}$ and $\tilde{r}$. Set

$$Z_{n,p} = \lceil Un \rceil - s_\ell + s_r,$$

so that $Z_{n,p} - 1$ (resp. $n - Z_{n,p}$) is the size of ℓ and $\tilde{\ell}$ (resp. r and $\tilde{r}$).

In order to enumerate the inversions of the output list, we introduce a *purely fictitious* error-correcting algorithm that parallels the implementation of Quicksort: This fictitious error-correcting algorithm has two recursive steps,

- First, the error-correcting algorithm corrects the sublists $\tilde{\ell}$ (resp. $\tilde{r}$) at costs $L = I(\tilde{\ell})$ (resp. $R = I(\tilde{r})$, producing two increasing sublists $\hat{\ell}$ and $\hat{r}$. Note that L and R are conditionally independent, given $Z_{n,p}$. Furthermore, the two sublists ℓ and r obtained at the end of Step 1 are in uniform random order before the second step of Quicksort, so that, conditionally given $Z_{n,p}$, cost L (resp. R) is distributed as $I(Z_{n,p} - 1, p)$ (resp. $I(n - Z_{n,p}, p)$).
- Then the error-correcting algorithm corrects the errors of Step 1, at a cost $t(n,p) = I(\hat{\ell} - \text{pivot} - \hat{r})$. Here $\hat{\ell} - \text{pivot} - \hat{r}$ stands for the list obtained when one puts $\hat{\ell}$, the pivot and $\hat{r}$ side by side. The number of inversions $t(n,p)$ in the list $\hat{\ell} - \text{pivot} - \hat{r}$ is analyzed in detail at the end of this section.

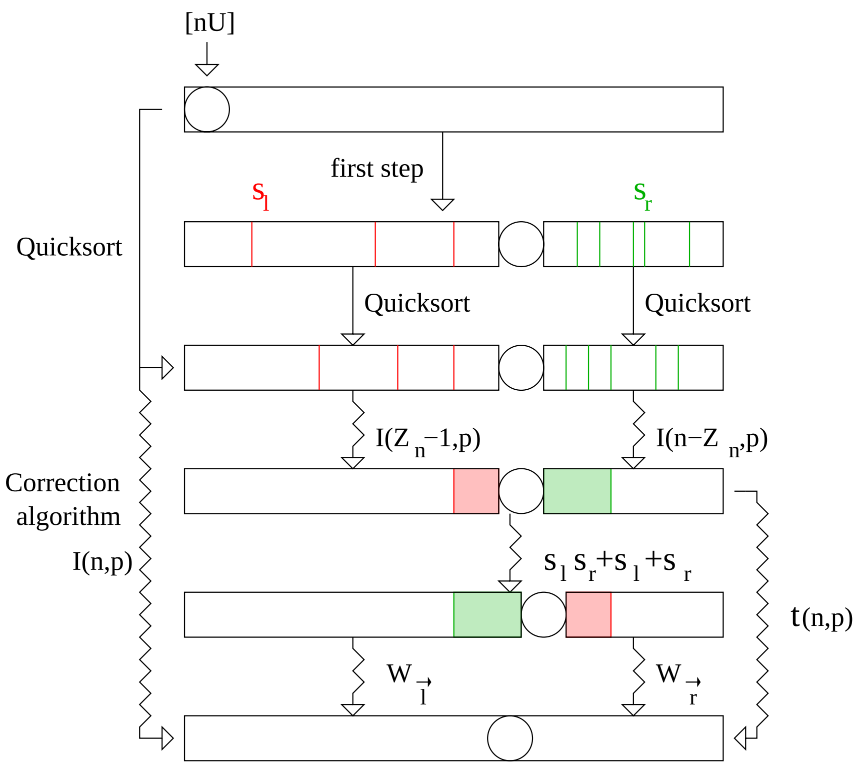

FIGURE 1. The error-correcting algorithm.

These two steps lead to the following equation for $I(n, p)$:

$$I(n, p) \stackrel{law}{=} I(Z_{n,p} - 1, p) + I'(n - Z_{n,p}, p) + t(n, p) \tag{9}$$

where $Z_{n,p} = \lceil Un \rceil - s_\ell + s_r$. We shall obtain the asymptotic distribution of $t(n, p)$, and as a consequence (9) will translate, after renormalisation, in a functional equation satisfied by the limit law of $I(n, p)/n^2 p$. The limit law appears on both sides of the functional equation, as expected, due to the recursive structure of Quicksort, and is thus characterized as the fixed point of some transformation.

Description of $t(n, p)$. At the end of the first step of the error-correcting algorithm, we obtain two subarrays $\hat{\ell}$ and $\hat{r}$, left and right of the pivot (cf. Figure 3). They are sorted in increasing order but there are s_r (red) elements larger than the pivot just to its left and s_ℓ (green) elements smaller than the pivot element just to its right. Thus, the only misplaced elements that the proofreader must correct in step 2 are clustered around the pivot.

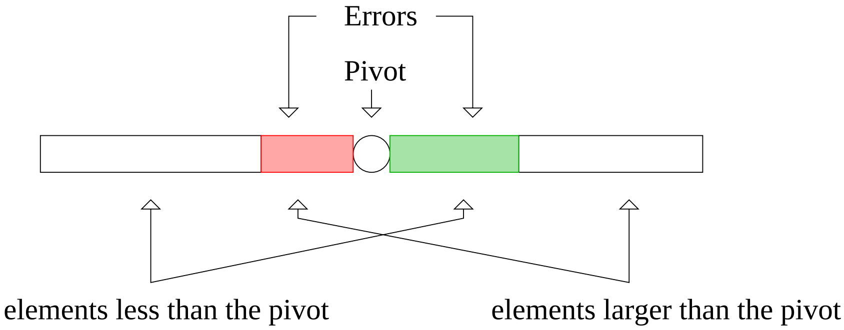

FIGURE 2. The two sublists $\hat{\ell}$ and $\hat{r}$.

In order to sort the list, the red and green sublists must be exchanged. This requires $s_\ell s_r + s_\ell + s_r$ inversions. We get therefore two unsorted lists $\vec{\ell}$ and $\vec{r}$ each composed of two sorted sublists. All items of $\vec{\ell}$ (resp. of $\vec{r}$) are now smaller (resp. larger) than the pivot, so that the length of $\vec{\ell}$ (resp. of $\vec{r}$) is $\lceil nU \rceil - 1$ (resp. $n - \lceil nU \rceil$). It remains to sort $\vec{\ell}$ and $\vec{r}$, at respective costs $W_{\vec{\ell}}$ and $W_{\vec{r}}$ that are conditionally independent given U, leading to:

$$t(n, p) = s_\ell s_r + s_\ell + s_r + W_{\vec{\ell}} + W_{\vec{r}}. \tag{10}$$

A model for $\left(W_{\vec{\ell}}, W_{\vec{r}}\right)$. Let W_m be the number of inversions in a list of m elements sorted as follows: each element is painted black or white with probability p (resp. $1 - p$). Then the black and white sublists are separately sorted in increasing order and the two sorted sublists are placed side by side, producing a new list h with m elements. We have

Proposition 3.1. *Let $Y_1, \dots, Y_m$ be m independent Bernoulli random variables with the same parameter p, and let $S_m = Y_1 + \cdots + Y_m$. Then*

$$W_m \stackrel{law}{=} \left(\sum_{i=1}^{m} iY_i \right) - \frac{S_m(S_m + 1)}{2}.$$

Proof. Let us abbreviate S_m to S. Among the Y_i's, let $Y_{i_1}, \dots, Y_{i_S}$ denote the S random variables equal to 1, $Y_{i_{S+1}}, \cdots, Y_{i_m}$ those equal to 0, with $i_1 < \cdots < i_S$ and $i_{S+1} < \cdots < i_m$. Now W_m can be seen as the number of inversions of the list $\left(i_j\right)_{1 \le j \le m}$. In order to move the numbers i_j ($j \le S$) to the correct position, the proofreader corrects inversions with each of the $i_j - j$ elements of $\{1, \cdots, m\}$ that are smaller than i_j and do not belong to $\{i_1, \cdots, i_S\}$. Thus

$$W_m = \sum_{j=1}^{S} (i_j - j), \tag{11}$$

leading to the result. □

With the help of Proposition 3.1, we can give a useful description of the distribution of $(s_\ell, W_{\vec{\ell}})$ and $(s_r, W_{\vec{r}})$:

Proposition 3.2. *Conditionally, given that the length of* $\vec{\ell}$ *is* $m-1$, $(s_\ell, W_{\vec{\ell}})$ *and* $(s_r, W_{\vec{r}})$ *are independent and distributed as* (S_{m-1}, W_{m-1}) *and* (S_{n-m}, W_{n-m}), *respectively.*

To sum up the results of this section, renormalizing (9), one obtains a functional equation satisfied by $X_{n,p}$:

$$X_{n,p} \overset{law}{=} A_{n,p} X_{Z_{n,p}-1,p} + B_{n,p} \widetilde{X}_{n-Z_{n,p},p} + T_{n,p} \tag{12}$$

in which

$$Z_{n,p} = \lceil Un \rceil - s_\ell + s_r, \tag{13}$$

$$A_{n,p} = \left(\frac{Z_{n,p} - 1}{n} \right)^2, \tag{14}$$

$$B_{n,p} = \left(\frac{n - Z_{n,p}}{n} \right)^2, \tag{15}$$

$$t(n,p) = s_\ell s_r + s_\ell + s_r + W_{\vec{\ell}} + W_{\vec{r}}, \tag{16}$$

$$T_{n,p} = \frac{t(n,p)}{n^2 p}, \tag{17}$$

and

- U is a uniform random variable on $[0,1]$, and $\lceil nU \rceil$ is the position of the pivot,
- conditionally, given $\lceil nU \rceil = m$, $(s_\ell, W_{\vec{\ell}})$ and $(s_r, W_{\vec{r}})$ are distributed as in Proposition 3.2,
- $X = (X_m)_{m \ge 0}$, $\widetilde{X} = \left(\widetilde{X}_m\right)_{m \ge 0}$ are two independent sequences with the same unknown distribution, independent of $(U, s_\ell, W_{\vec{\ell}}, s_r, W_{\vec{r}})$, or, equivalently, of $(A_{n,p}, B_{n,p}, Z_{n,p}, T_{n,p})$.

The errors having a balancing effect, $Z_{n,p} = \lceil Un \rceil - s_\ell + s_r$ has the same mean, $(n+1)/2$, and a smaller variation than $\lceil Un \rceil$; we prove this in the following form.

Lemma 3.3.

$$\mathbb{E}\left[(Z_{n,p}-1)^2 + (n - Z_{n,p})^2\right] \le \mathbb{E}\left[(\lceil Un \rceil - 1)^2 + (n - \lceil Un \rceil)^2\right] = \frac{(n-1)(2n-1)}{3} \le \frac{2}{3} n^2.$$

Proof. The left hand side is the expected number of pairs i and j that end up on the same side of the pivot. This happens if i and j originally are on the same side of the pivot and we either compare both correctly or make errors for both of them, or if they are on each side of the pivot and we make an error for exactly one of them. Hence

$$\begin{aligned}\mathbb{E}\left[(Z_{n,p}-1)^2+(n-Z_{n,p})^2\right] &= \left(p^2+(1-p)^2\right)\mathbb{E}\left[(\lceil Un\rceil-1)^2+(n-\lceil Un\rceil)^2\right] \\ &\quad + 2p(1-p)2\mathbb{E}\left[(\lceil Un\rceil-1)(n-\lceil Un\rceil)\right] \\ = \mathbb{E}\left[(\lceil Un\rceil-1)^2+(n-\lceil Un\rceil)^2\right] &- 2p(1-p)\mathbb{E}\left[(\lceil Un\rceil-1-(n-\lceil Un\rceil))^2\right]\end{aligned}$$

which proves the first inequality. The rest is a simple calculation. □

Let $I^{(k)}(n,p)$ be the number of inversions created at step k. We shall need the following bound:

Lemma 3.4. *For every $k \geq 1$,*

$$\mathbb{E}\left[I^{(k)}(n,p)\right] \leq \frac{1}{2}\left(\frac{2}{3}\right)^k n^2 p.$$

Proof. For $k=1$, $I^{(1)}(n,p)=t(n,p)$, and a simple calculation yields

$$\mathbb{E}\left[t(n,p)\right] = p\frac{(n-1)(n+1)}{3} - p^2\frac{(n-1)(n-2)}{6} \leq \frac{1}{3}n^2 p.$$

For $k>1$ we find by induction, conditioning on the partition in the first step,

$$\mathbb{E}\left[I^{(k)}(n,p)\right] \leq \mathbb{E}\left[\frac{1}{2}\left(\frac{2}{3}\right)^{k-1}(Z_{n,p}-1)^2 p + \frac{1}{2}\left(\frac{2}{3}\right)^{k-1}(n-Z_{n,p})^2 p\right]$$

and the result follows by Lemma 3.3. □

Proposition 3.5. *Set $a_{n,p}=\mathbb{E}\left[X_{n,p}\right]$. Then*

$$a_{n,p} \leq 1.$$

Proof. By Lemma 3.4, $a_{n,p} \leq \sum_1^\infty \frac{1}{2}\left(\frac{2}{3}\right)^k$. □

4. Fixed point theorems

The proofs of the first two cases are examples of the contraction method [10, 11]: on one hand we have more or less explicitly defined random variables $A^{(i)}_{n,p}$, $1 \leq i \leq I$, and $T_{n,p}$, and we know how to prove directly that they converge to $A^{(i)}$, T. On the other hand, we have a family $X_{n,p}$ of random variables defined by induction:

$$X_{n,p} \overset{\text{law}}{=} \sum_{i=1}^{I} A^{(i)}_{n,p} X^{(i)}_{Z^{(i)}_{n,p},p} + T_{n,p}, \tag{18}$$

and a random variable X implicitly defined by the following functional equation

$$X \overset{\text{law}}{=} \sum_{i=1}^{I} A^{(i)} X^{(i)} + T, \tag{19}$$

in which, in some sense, $\lim Z^{(i)}_{n,p} = +\infty$. Then, under additional technical conditions, the convergence of the "coefficients" $A^{(i)}_{n,p}$, $T_{n,p}$, entails the convergence of the "solution" $X_{n,p}$. One has to prove existence and unicity of the solutions, usually as fixed points of contracting transformations in a subspace of the space of probability measures, with a suitable metric. In the case we are interested in, (18) holds and:

- I is a fixed positive integer;
- $C_{n,p} = (A^{(1)}_{n,p}, Z^{(1)}_{n,p}, \dots, A^{(I)}_{n,p}, Z^{(I)}_{n,p}, T_{n,p})$ is a given random vector for each n, p;
- $Z^{(i)}_{n,p} \in [0, \dots, n-1]$;
- The families $(X^{(i)}_{n,p})_{n,p}$, $i = 1, 2, \dots, I$, are i.i.d. and independent of $C_{n,p}$, and and $X^{(i)}_{n,p} \overset{law}{=} X_{n,p}$.

Given such $C_{n,p}$ we thus define, for any distributions $G_{0,p}, \dots, G_{n-1,p}$,

$$\Phi(G_{0,p}, \dots, G_{n-1,p}) = \mathcal{L}\left(\sum_{i=1}^{I} A^{(i)}_{n,p} X^{(i)}_{Z^{(i)}_{n,p},p} + T_{n,p}\right),$$

when, as above, the families $(X^{(i)}_{k,p})_{k,p}$, $i = 1, 2, \dots, I$, are i.i.d. and independent of $C_{n,p}$, and further $X^{(i)}_{k,p}$ has the distribution $G_{k,p}$. Thus (18) can be written

$$G_{n,p} = \Phi(G_{0,p}, \dots, G_{n-1,p}).$$

For (19) we similarly assume

- $C = (A^{(1)}, \dots, A^{(I)}, T)$ is a given random vector;
- the variables $X^{(i)}$, $i = 1, 2, \dots, I$ are i.i.d. and independent of C, and $X^{(i)} \overset{law}{=} X$.

Given such C we define

$$\Psi(F) = \mathcal{L}\left(\sum_{i=1}^{I} A^{(i)} X^{(i)} + T\right),$$

when the variables $X^{(i)}$, $i = 1, 2, \dots, I$ are i.i.d. with distribution F and independent of C. Then (19) can be written

$$\Psi(F) = F.$$

Let D be the space of probability measures μ on $\mathbb{R}$, such that $\int_{\mathbb{R}} |x| \ d\mu(x) < +\infty$. The space D is endowed with the Wasserstein metric

$$\begin{aligned} d_1(\mu, \nu) &= \inf_{\substack{\mathcal{L}(X)=\mu \\ \mathcal{L}(Y)=\nu}} \|X - Y\|_1 \\ &= \left\|F^{-1}(U) - G^{-1}(U)\right\|_1 . \end{aligned} \tag{20}$$

in which F and G denote the distribution functions of μ and ν, F^{-1} (resp. G^{-1}) denote the generalized inverses of F and G and, as in previous sections, U is a uniform random variable. Since $F^{-1}(U)$ (resp. $G^{-1}(U)$) has distribution μ (resp. ν), the infimum is attained in relation (20).

The metric d_1 makes D a complete metric space. Convergence of $\mathcal{L}(X_n)$ to $\mathcal{L}(X)$ in D is equivalent to convergence of X_n to X in distribution *and*

$$\lim \mathbb{E}\left[|X_n|\right] = \mathbb{E}\left[|X|\right];$$

also, convergence in D entails

$$\lim \mathbb{E}\left[X_n\right] = \mathbb{E}\left[X\right].$$

We refer to [9] for an extensive treatment of Wasserstein metrics. In what follows, we shall improperly refer to the convergence of X_n to X in D, meaning the convergence of their distributions. Let us take care first of relation (19):

Theorem 4.1. *If* $\sum_{i=1}^{I} \mathbb{E}\left[\left|A^{(i)}\right|\right] < 1$, *then* Ψ *is a strict contraction and (19) has a unique solution in* D.

Proof. Let (X, Y) be a couple of random variables, with laws μ and ν, respectively, such that

$$\mathbb{E}\left[|X - Y|\right] = d_1(\mu, \nu).$$

Let $\left(\left(X^{(i)}, Y^{(i)}\right)\right)_{1\le i\le I}$ be I independent copies of (X, Y). Furthermore, assume that C and $\left(\left(X^{(i)}, Y^{(i)}\right)\right)_{1\le i\le I}$ are independent. Then the probability distribution of

$$\sum_{i=1}^{I} A^{(i)} X^{(i)} + T, \quad \text{resp.} \ \sum_{i=1}^{I} A^{(i)} Y^{(i)} + T$$

is $\Psi(\mu)$ (resp. $\Psi(\nu)$) and

$$\begin{aligned} d_1(\Psi(\mu), \Psi(\nu)) &\le \sum_{i=1}^{I} \mathbb{E}\left[\left|A^{(i)}\right| \left|X^{(i)} - Y^{(i)}\right|\right] \\ &\le d_1(\mu, \nu) \sum_{i=1}^{I} \mathbb{E}\left[\left|A^{(i)}\right|\right]. \end{aligned}$$

Thus Ψ is a contraction with contraction constant smaller than 1. Since D is a complete metric space, this implies that Ψ has a unique fixed point in D, by Banach's fixed point theorem. □

We prove now a theorem which is a variant of those used by the precited authors: the difference is not deep, but here we deal with family of laws, not sequences, as we have two parameters, n and p. As a consequence, to cover Theorems 2.1 and 2.2, it will be convenient in their proofs to consider convergence with respect to a *filter* $\mathcal{F}$ on $\mathbb{N} \times [0, 1]$. The filter $\mathcal{F}_1$ corresponding to Theorem 2.1 has basis

$$V_{N,\varepsilon} = \{n \ge N\} \times [c - \varepsilon, c + \varepsilon],$$

while the filter $\mathcal{F}_2$ corresponding to Theorem 2.2 has basis

$$\widetilde{V}_{N,\varepsilon} = \left\{(n, p) \,\middle|\, 0 < p \le \varepsilon,\, n \ge N/p\right\}.$$

Theorem 4.2. *Suppose that* (18) *holds for* $n \ge 1$ *and* $X_{0,p} = 0$*; i.e.* $G_{n,p} = \Phi(G_{0,p}, \ldots, G_{n-1,p})$ *for* $n \ge 1$ *and* $G_{0,p} = \delta_0$*, where* $G_{n,p} = \mathcal{L}(X_{n,p})$*. If*

i) $\left(\mathbb{E}\left[X_{n,p}\right]\right)_{n,p}$ *is bounded,*

ii) $\sum_{i=1}^{I} \mathbb{E}\left[\left|A^{(i)}\right|\right] < 1$,

iii) $T_{n,p} \xrightarrow[\mathcal{F}]{L^1} T$, $A^{(i)}_{n,p} \xrightarrow[\mathcal{F}]{L^1} A^{(i)}$,

iv) $\lim_{\mathcal{F}} \ \mathbb{E}\left[\left|A^{(i)}_{n,p}\right| \ ; \ (Z^{(i)}_{n,p}, p) \notin V\right] = 0, \qquad \forall V \in \mathcal{F}$,

then

– Ψ *is a contraction for* d_1 *and the equation* $\Psi(F) = F$ *has a unique solution* F *in* D.
– $X_{n,p}$ *converges in distribution to* F. *More precisely,* $d_1(G_{n,p}, F) \to 0$ *along* $\mathcal{F}$.

We need a lemma.

Lemma 4.3. *Assume that three families of nonnegative numbers* $(a_{n,p}, b_{n,p})_{0\leq n, 0<p<1}$, *and* $(\gamma_{i,n,p})_{0\leq n, 0\leq i\leq n, 0<p<1}$ *satisfy the inequalities:*

$$a_{n,p} \leq b_{n,p} + \sum_{i=0}^{n-1} \gamma_{i,n,p} a_{i,p},$$

Let $\mathcal{F}$ *be a filter. Under the following assumptions:*

– $a_{n,p}$ *is nonnegative and bounded,*
– *for some* $\Gamma < 1$ *and some* $V_0 \in \mathcal{F}$, $\forall (n,p) \in V_0$, $\sum_{k=0}^{n-1} \gamma_{k,n,p} < \Gamma$,
– $\lim_{\mathcal{F}} b_{n,p} = 0$,
– $\forall V \in \mathcal{F}$, $\lim_{\mathcal{F}} \sum_{k \ s.t. \ (k,p)\notin V} \gamma_{k,n,p} = 0$,

we have

$$\lim_{\mathcal{F}} \ a_{n,p} = 0.$$

Proof of Lemma 4.3. The proof is also a variant of the proof of [10, Proposition 3.3]. Let M be a bound for $a_{n,p}$, and let

$$a = \limsup_{\mathcal{F}} \ a_{n,p}.$$

For any $\epsilon > 0$, let $V_\epsilon \in \mathcal{F}$ be such that for $(n,p) \in V_\epsilon$,

$$a_{n,p} \leq a + \epsilon.$$

Then for $(n,p) \in V_\epsilon \cap V_0$ we have

$$\begin{aligned} a_{n,p} &\leq \sum_{k \text{ s.t. } (k,p)\notin V_\epsilon} \gamma_{k,n,p} a_{k,p} + \sum_{k \text{ s.t. } (k,p)\in V_\epsilon} \gamma_{k,n,p} a_{k,p} + b_{n,p} \\ &\leq M \sum_{k \text{ s.t. } (k,p)\notin V_\epsilon} \gamma_{k,n,p} + (a+\epsilon)\Gamma + b_{n,p}. \end{aligned}$$

Going to the limit, we obtain that for any $\epsilon > 0$,

$$a \leq (a+\epsilon)\Gamma.$$

□

Proof of Theorem 4.2. We can choose $X^{(i)}$ and the family $\left(X_{k,p}^{(i)}\right)_{k\geq 0}$ in such a way that

$$\mathbb{E}\left[\left|X_{k,p}^{(i)} - X^{(i)}\right|\right] = d_1(G_{k,p}, F),$$

and we can also choose the families $\left(X^{(i)},(X^{(i)}_{k,p})_{k\geq 0}\right)_{0\leq i\leq I}$ to be i.i.d. Then

$$\begin{aligned}
d_1(G_{n,p},F) &\leq \mathbb{E}\left[\Big|\sum_{i=1}^{I} A^{(i)}_{n,p} X^{(i)}_{Z^{(i)}_{n,p},p} + T_{n,p} - \sum_{i=1}^{I} A^{(i)} X^{(i)} - T\Big|\right] \\
&\leq \sum_{k=0}^{n-1} \mathbb{E}\left[\sum_{i=1}^{I} \big|A^{(i)}_{n,p} \mathbb{1}_{Z^{(i)}_{n,p}=k}\big|\right] \mathbb{E}\left[\big|X^{(i)}_{k,p} - X^{(i)}\big|\right] + b_{n,p} \\
&\leq \sum_{k=0}^{n-1} \gamma_{k,n,p}\, d_1(G_{k,p},F) + b_{n,p}
\end{aligned}$$

with

$$\begin{aligned}
b_{n,p} &= \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p} - A^{(i)}\big| X^{(i)}\right] + \mathbb{E}\left[|T_{n,p} - T|\right], \\
\gamma_{k,n,p} &= \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p}\big| \mathbb{1}_{Z^{(i)}_{n,p}=k}\right].
\end{aligned}$$

Set

$$a_{n,p} = d_1(G_{n,p},F),$$

and let us check the assumptions of Lemma 4.3:

$$0 \leq a_{n,p} \leq \mathbb{E}\left[X_{n,p}\right] + \mathbb{E}\left[X\right] \leq 1 + \mathbb{E}\left[X\right] \;;$$

for the second assumption,

$$\limsup_{\mathcal{F}} \sum_{k=0}^{n-1} \gamma_{k,n,p} = \limsup_{\mathcal{F}} \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p}\big|\right] = \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}\big|\right] < 1 \;;$$

$\lim_{\mathcal{F}} b_{n,p} = 0$ by assumption iii), as

$$\sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p} - A^{(i)}\big| X^{(i)}\right] = \mathbb{E}\left[X\right] \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p} - A^{(i)}\big|\right] \;;$$

finally

$$\sum_{k \text{ s.t. } (k,p)\notin V} \gamma_{k,n,p} = \sum_{i=1}^{I} \mathbb{E}\left[\big|A^{(i)}_{n,p}\big| \;;\; (Z^{(i)}_{n,p},p) \notin V\right].$$

Therefore $d_1(G_{n,p},F)$ vanishes along $\mathcal{F}$ and the proof of the theorem is now complete. □

The following Theorem is folklore. It gives the means and variances in Theorems 2.1 and 2.2, after some computations.

Theorem 4.4. *Suppose that* (19) *holds, where* $\sum_i \mathbb{E}\left[|A^{(i)}|\right] < 1$ *and* $\mathbb{E}\left[|X|\right] < \infty$*; in other words,* $\mathcal{L}(X) = F$*, where* F *is the unique solution in* D *to* $\Psi(F) = F$*. Then*

$$\mathbb{E}\left[X\right] = \frac{\mathbb{E}\left[T\right]}{1 - \sum_i \mathbb{E}\left[A^{(i)}\right]}. \tag{21}$$

Moreover, if further $\sum_i \mathbb{E}\left[|A^{(i)}|^2\right] < 1$ *and* $\mathbb{E}\left[T^2\right] < \infty$*, then* $\mathbb{E}\left[X^2\right] < \infty$ *and*

$$\operatorname{Var}(X) = \frac{\mathbb{E}\left[T^2\right] + 2\,\mathbb{E}[X]\,\mathbb{E}\left[T\sum_i A^{(i)}\right] + \mathbb{E}\left[\left(\sum_i A^{(i)}\right)^2 - 1\right](\mathbb{E}[X])^2}{1 - \sum_i \mathbb{E}\left[A^{(i)\,2}\right]}. \tag{22}$$

Proof. Taking expectations in (19) we obtain $\mathbb{E}[X] = \sum_i \mathbb{E}\left[A^{(i)}\right]\mathbb{E}[X] + \mathbb{E}[T]$, which yields (21).

For the second part, let $D_2 = \{\mu \in D : \int x\,d\mu(x) = \mathbb{E}[X],\ \int x^2\,d\mu(x) < \infty\}$. It is easy to see that now Ψ is a strict contraction in D_2 with the d_2 metric; hence Ψ has a unique fixed point in D_2. Since $D_2 \subset D$, this fixed point must be F, which shows that $\mathbb{E}\left[X^2\right] < \infty$. If we square (19) and take the expectation, we obtain

$$\mathbb{E}\left[X^2\right] = \mathbb{E}\left[\sum_{i=1}^{I} A^{(i)\,2}\right]\mathbb{E}\left[X^2\right] + \sum_{i,j=1,\,i\neq j}^{I} \mathbb{E}\left[A^{(i)}A^{(j)}\right](\mathbb{E}[X])^2 + 2\sum_{i=1}^{I}\mathbb{E}\left[A^{(i)}T\right]\mathbb{E}[X] + \mathbb{E}\left[T^2\right],$$

which yields (22). ☐

5. Proofs of Theorems 2.1 and 2.2

We apply Theorem 4.2 to the functional equation (12), with $I = 2$,

$$\left(A^{(1)}_{n,p}, Z^{(1)}_{n,p}\right) = (A_{n,p}, Z_{n,p} - 1),$$
$$\left(A^{(2)}_{n,p}, Z^{(2)}_{n,p}\right) = (B_{n,p}, n - Z_{n,p}).$$

Here the distribution of $\left(A^{(i)}_{n,p}, Z^{(i)}_{n,p}\right)$ does not depend on i. We verify the assumptions i)–iv) of Theorem 4.2 for Theorems 2.1 and 2.2 together; for the second theorem take $c = 0$. The first assumption holds true by Proposition 3.5.

Verification of the second point. We have

$$A^{(1)} = A = [(1-2c)U + c]^2,$$
$$A^{(2)} = B = [(2c-1)U + 1 - c]^2,$$

and $c \in [0,1]$. Easy computations give

$$\mathbb{E}\left[[(1-2c)U + c]^2\right] + \mathbb{E}\left[[(2c-1)U + 1 - c]^2\right] = \frac{2}{3}(1 - c + c^2) \le \frac{2}{3}.$$

Verification of the third point. We must prove the convergence of $A_{n,p}$, $B_{n,p}$ and $T_{n,p}$ to A, B and $T(c,U)$, in L^1. Recall (13)–(17).

Note first that, conditioned on U, $s_\ell \sim \operatorname{Bi}(\lceil nU\rceil - 1, p)$ and thus

$$\mathbb{E}\big((s_\ell - (\lceil nU\rceil - 1)p)^2 \mid U\big) = (\lceil nU\rceil - 1)p(1-p) \le np.$$

Hence, taking the expectation,

$$\mathbb{E}\big(s_\ell - (\lceil nU\rceil - 1)p\big)^2 \le np$$

and thus

$$\|s_\ell - nUp\|_2 \le \|s_\ell - (\lceil nU\rceil - 1)p\|_2 + p \le (np)^{1/2} + p \le 2(np)^{1/2}.$$

Consequently,

$$\left\|\frac{s_\ell}{n} - Uc\right\|_2 \le \left\|\frac{s_\ell}{n} - Up\right\|_2 + |p-c| \to 0, \tag{23}$$

and, similarly but sharper,

$$\left\|\frac{s_\ell}{n\sqrt{p}} - U\sqrt{c}\right\|_2 \le \frac{2}{\sqrt{n}} + \frac{|p-c|}{\sqrt{p}} \to 0. \tag{24}$$

Similarly,

$$\left\|\frac{s_r}{n} - (1-U)c\right\|_2 \to 0 \tag{25}$$

and

$$\left\|\frac{s_r}{n\sqrt{p}} - (1-U)\sqrt{c}\right\|_2 \to 0. \tag{26}$$

From (13), (23) and (25) follows

$$\left\|\frac{Z_{n,p}-1}{n} - \big(U - Uc + (1-U)c\big)\right\|_2 \to 0. \tag{27}$$

It follows easily from Hölder's inequality that multiplication is a continuous bilinear map $L^2 \times L^2 \to L^1$. Hence (27) yields

$$\|A_{n,p} - A\|_1 = \left\|\left(\frac{Z_{n,p}-1}{n}\right)^2 - \big(U - Uc + (1-U)c\big)^2\right\|_1 \to 0,$$

verifying the first assertion. (27) similarly implies $\|B_{n,p} - B\|_1 \to 0$ too.

For $T_{n,p}$ we first observe that, similarly, from (24) and (26),

$$\left\|\frac{s_\ell s_r}{n^2 p} - U(1-U)c\right\|_1 \to 0.$$

Moreover, since $np \to \infty$, (23) and (25) imply $\left\|s_\ell/n^2p\right\|_1 \le \left\|s_\ell/n^2p\right\|_2 \to 0$ and $\left\|s_r/n^2p\right\|_1 \to 0$.

For the terms $W_{\vec{\ell}}$ and $W_{\vec{r}}$ we use Proposition 3.1. We have $\|S_m - mp\|_2 = \sqrt{mp(1-p)}$ and thus, uniformly for $0 \le m \le n$,

$$\left\|\frac{S_m}{n\sqrt{p}} - \frac{m}{n}\sqrt{c}\right\|_2 \le \frac{1}{\sqrt{n}} + |\sqrt{p} - \sqrt{c}| \to 0,$$

which, using Hölder again, yields

$$\left\|\frac{S_m(S_m+1)}{2n^2p} - \frac{c}{2}\left(\frac{m}{n}\right)^2\right\|_1 \le \frac{3}{\sqrt{n}} + \frac{1}{n\sqrt{p}} + 3|\sqrt{p} - \sqrt{c}| \to 0. \tag{28}$$

Moreover, let $W'_m = \sum_{i=1}^m iY_i$. Then $\mathbb{E}W'_m = \frac{m(m+1)p}{2}$ and

$$\|W'_m - \mathbb{E}W'_m\|_2^2 = \operatorname{Var}(W'_m) = \sum_{i=1}^m i^2 p(1-p) \le m^3 p,$$

and thus

$$\left\|\frac{W'_m}{n^2p} - \frac{1}{2}\left(\frac{m}{n}\right)^2\right\|_2 \le \frac{1}{\sqrt{np}} + \frac{1}{2n} \to 0. \tag{29}$$

Proposition 3.1 now yields, by (28) and (29), uniformly for $m \leq n$,

$$\left\| \frac{W_m}{n^2 p} - \frac{1-c}{2} \left(\frac{m}{n}\right)^2 \right\|_1 \to 0.$$

Consequently, using Proposition 3.2,

$$\left\| \frac{W_{\vec{\ell}}}{n^2 p} - \frac{1-c}{2} U^2 \right\|_1 \to 0,$$

$$\left\| \frac{W_{\vec{r}}}{n^2 p} - \frac{1-c}{2} (1-U)^2 \right\|_1 \to 0.$$

Collecting the various terms above, we find $\|T_{n,p} - T\|_1 \to 0$.

Verification of the fourth point. We have to check that

$$\lim_{\mathcal{F}_i} \mathbb{E}\left[\left|A_{n,p}\right| \; ; \; (Z_{n,p}, p) \notin V\right] = 0, \qquad \forall V \in \mathcal{F}_i.$$

But for $(n,p) \in V_{N,\varepsilon}$ (resp. for $(n,p) \in \widetilde{V}_{N,\varepsilon}$),

$$\mathbb{E}\left[\left|A_{n,p}\right| \; ; \; (Z_{n,p}, p) \notin V_{N,\varepsilon}\right] \leq \left(\frac{N-1}{n}\right)^2,$$

$$\mathbb{E}\left[\left|A_{n,p}\right| \; ; \; (Z_{n,p}, p) \notin \widetilde{V}_{N,\varepsilon}\right] \leq \left(\frac{N}{np}\right)^2.$$

6. Proof of Theorem 2.3.

The proof of this theorem is done in three steps:

(i) We prove that $X(\lambda)$ is almost surely finite, and has exponentially decreasing distribution tail. Thus it has moments of all orders.

(ii) With the help of a Poisson point process representation of Quicksort, we prove the convergence of certain copies of $X_{n,p}$ to a copy of $X(\lambda)$ *for the norm* $\|.\|_1$. This entails the weak convergence.

(iii) We prove that $X(\lambda)$ satisfies the functional equation (5), and that (5) has a unique solution under the extra assumptions in the theorem.

Some properties of $X(\lambda)$. Recall that the increasing sequence $(Y_{k,j})_{0 \leq j \leq 2^k}$, defined by the recurrence relation (3), splits $[0,1]$ in 2^k intervals, obtained recursively by breaking each of the 2^{k-1} intervals of the previous step in two random pieces. For $k \geq 0$ and $1 \leq i \leq 2^k$, let

$$\begin{aligned}
w_{k,i} &= Y_{k,i} - Y_{k,i-1}, \\
M_k &= \max\left\{w_{k,i}; 1 \leq i \leq 2^k\right\}, \\
F_{k,\alpha} &= \left(\frac{1+\alpha}{2}\right)^k \sum_{1 \leq i \leq 2^k} w_{k,i}^\alpha \\
\mathcal{F}_k &= \sigma\left(Y_{i,j}, i \leq k, 1 \leq j \leq 2^i - 1\right) \\
\mathcal{F} &= \left(\mathcal{F}_k\right)_{k \geq 0}.
\end{aligned}$$

We begin with a simple estimate (see also [4]):

Lemma 6.1. $\mathbb{E}\left[w_{k,j}^2\right] = 3^{-k}$.

Proof. The length $w_{k,j} = |I_{k,j}|$ is the product of k independent random variables, each uniform on $[0,1]$. Hence $\mathbb{E}\left[w_{k,j}^2\right] = \left(\mathbb{E}\left[U^2\right]\right)^k = 3^{-k}$. □

Lemma 6.2. *For $\alpha > 0$, $(F_{k,\alpha})_{k\geq 0}$ is a $\mathcal{F}$-martingale, and $\mathbb{E}\left[F_{k,\alpha}\right] = 1$.*

Proof. Clearly $\mathbb{E}\left[F_{0,\alpha}\right] = 1$. Also:

$$\begin{aligned}
\mathbb{E}\left[F_{k+1,\alpha}|\mathcal{F}_k\right] &= \left(\frac{1+\alpha}{2}\right)^{k+1} \sum_{i=1}^{2^k} \mathbb{E}\left[w_{k+1,2i-1}^\alpha + w_{k+1,2i}^\alpha|\mathcal{F}_k\right] \\
&= \left(\frac{1+\alpha}{2}\right)^{k+1} \sum_{i=1}^{2^k} w_{k,i}^\alpha \mathbb{E}\left[V_{k,i-1}^\alpha + (1-V_{k,i-1})^\alpha\right] \\
&= \left(\frac{1+\alpha}{2}\right)^{k} \sum_{i=1}^{2^k} w_{k,i}^\alpha.
\end{aligned}$$

□

Let $\rho = 0.792977\ldots$ denote the largest solution of the equation $\rho = -2e\ln\rho$. Lemma 6.2 entails that

Lemma 6.3. $\mathbb{E}\left[M_k\right] \leq \rho^k$.

Proof. Clearly,

$$M_k^\alpha \leq \left(\frac{2}{1+\alpha}\right)^k F_{k,\alpha},$$

thus, for $\alpha \geq 1$,

$$\mathbb{E}\left[M_k\right] \leq \mathbb{E}\left[M_k^\alpha\right]^{1/\alpha} \leq \left(\frac{2}{1+\alpha}\right)^{k/\alpha} \mathbb{E}\left[F_{k,\alpha}\right]^{1/\alpha} = \left(\frac{2}{1+\alpha}\right)^{k/\alpha}.$$

The rate $\left(\frac{2}{1+\alpha}\right)^{1/\alpha}$ reaches its minimum for $1+\alpha = 4.311\ldots$, a constant that is an old friend of Quicksort and binary search trees. This leads to the desired value for ρ. □

A weaker form of this inequality (for $\alpha = 2$), actually sufficient for our purposes, is given in [4]. The sequence $(F_{k,\alpha})_{k\geq 0}$ is a specialization of martingales that are of a great use for the study of general branching random walks, see for instance [1], of which binary search trees are a special case [7, 8].

Lemma 6.4. $\mathbb{E}\left[X(\lambda)\right] = 1$.

Proof. Set $\mathcal{F}_\infty = \sigma\left(Y_{k,j}, k \geq 0, 1 \leq j \leq 2^k - 1\right)$. Inspecting (7), we see that

$$\mathbb{E}\left[X(\lambda)\,|\,\mathcal{F}_\infty\right] = \frac{1}{2}\sum_{k\geq 1}\left(\frac{2}{3}\right)^k F_{k,2},$$

because, conditionally given $\mathcal{F}_\infty$, the expected number of points of $\Pi_{k,j}$ is $\lambda w_{k,j}$ and each of them has an expected contribution $w_{k,j}/(2\lambda)$ to $X(\lambda)$. □

As a consequence of Lemma 6.3, we have

Theorem 6.5. *The distribution tail $\mathbb{P}\left(X(\lambda) \geq x\right)$ decreases exponentially fast.*

Proof. Equivalently, we prove the first result for $\Xi(\lambda) = \lambda X(\lambda)$. Since

$$\left|x - Y_{k,J_k(x)}\right| \le M_k,$$

we have

$$\Xi(\lambda) \le \sum_{(k,x)\in\Pi} M_k = \sum_{k\ge 1} N_k M_k,$$

where $N_k = |\Pi_k|$ is a Poisson random variable with mean λ. We split its tail as follows:

$$\begin{aligned}\mathbb{P}\left(\Xi(\lambda) \ge x\right) &\le \mathbb{P}\left(\sum_{k\ge 1} N_k M_k \ge x\right)\\ &\le p_1 + p_2,\end{aligned}$$

in which

$$\begin{aligned}p_1 &= \mathbb{P}\left(\sum_{1\le k\le n} N_k M_k \ge x/2\right),\\ p_2 &= \mathbb{P}\left(\sum_{k>n} N_k M_k \ge x/2\right).\end{aligned}$$

We have, by the standard Chernoff bound for the Poisson distribution,

$$p_1 \le \mathbb{P}\left(\sum_{1\le k\le n} N_k \ge x/2\right) \le \exp\left(\frac{x}{2}\left(1 - \ln(x/2n\lambda)\right) - n\lambda\right),$$

the last inequality holding only for $n \le \frac{x}{2\lambda}$. Also

$$\begin{aligned}p_2 &\le \mathbb{P}\left(\sum_{0\le k\le n} N_k \rho^{k/2} \ge x/2\right) + \mathbb{P}\left(\exists k > n,\ M_k > \rho^{k/2}\right)\\ &\le \left(1 + \frac{2\lambda}{x}\right)\frac{\rho^{(n+1)/2}}{1-\sqrt{\rho}},\end{aligned}$$

using a Markov first moment inequality to bound both terms. For any α in $(0,1)$, the choice $n \simeq \frac{\alpha x}{2\lambda}$ leads to an exponential decrease of the tail. □

Convergence of $X_{n,p}$ to $X(\lambda)$. We assume that the input list for Quicksort contains the integers $\{1, 2, \ldots, n\}$ in random order. We model our erratic Quicksort as follows using the variables $U_{k,j}$ and Π in Section 2, but with the intensity λ of Π replaced by $\lambda(n,p) = -n\ln(1-p)$:

In the first step, we use the pivot $p_{1,1} = \lceil nU_{0,1}\rceil$ and let for each i (except the pivot) there be an error in the comparison of i and the pivot if $\Pi_1 \cap (\frac{i-1}{n}, \frac{i}{n}] \ne \emptyset$. (Recall that $\Pi_k = \{x : (k,x) \in \Pi\}$.) Note that our choice of $\lambda(n,p)$ yields the right error probability p.

Let $p'_{1,1}$ be the position of the pivot after the first step. (This position was earlier denoted $Z_{n,p}$; it may differ from $p_{1,1}$ because of errors.) The items of the left sublist will thus be placed on positions $1, \ldots, p'_{1,1} - 1$ and those in the right sublist on positions $p'_{1,1} + 1, \ldots, n$. Let $p'_{1,0} = 0$ and $p'_{1,2} = 1 + n$.

When the k-th step begins, we have a set of 2^{k-1} sublists $(\ell_{k-1,j})_{j=1,\dots,2^{k-1}}$, the elements of $\ell_{k-1,j}$ being on positions $p'_{k-1,j-1}+1,\dots,p'_{k-1,j}-1$, $j=1,\dots,2^{k-1}$ (with the convention that the sublist is empty when $p'_{k-1,j}-p'_{k-1,j-1}\le 1$). In each nonempty such sublist we choose as pivot the item with rank $\lceil U_{k-1,j}(p'_{k-1,j}-p'_{k-1,j-1}-1)\rceil$, in this sublist, so that its position in the final output will be exactly

$$p_{k,2j-1}=p'_{k-1,j-1}+\lceil U_{k-1,j}(p'_{k-1,j}-p'_{k-1,j-1}-1)\rceil, \tag{30}$$

in case no errors occurs while proceeding the sublist. We assume an error is made when comparing the element at position i with the pivot $p_{k,2j-1}$ if $\Pi_k\cap(\frac{i-1}{n},\frac{i}{n}]\neq\emptyset$. Let $p'_{k,2j}=p'_{k-1,j}$. Let $p'_{k,2j-1}$ be the position of the pivot $p_{k,2j-1}$ after the comparisons (as in the first step, $p'_{k,2j-1}$ may differ from $p_{k,2j-1}$ because of errors); let $p'_{k,2j-1}=p'_{k-1,j}$ if the sublist was empty. Set

$$y_{k,j}=p_{k,j}/n \quad\text{and}\quad y'_{k,j}=p'_{k,j}/n.$$

We expect $y_{k,j}$ and $y'_{k,j}$ to converge to $Y_{k,j}$ as $n\to+\infty$.

This procedure (stopped when there are no more nonempty sublists) is an exact simulation of the erratic Quicksort, so we may assume that $I(n,p)$ is the number of inversions created by it. As in Section 3, let $I^{(k)}(n,p)$ be the number of inversions created at step k, so

$$I(n,p)=\sum_{k=1}^{\infty}I^{(k)}(n,p).$$

We will prove that, using the notation of (7),

$$\delta_k=\left\|\frac{1}{n^2p}I^{(k)}(n,p)-\frac{1}{\lambda(n,p)}\sum_{j=1}^{2^k}\sum_{x\in\Pi_{k,j}}|x-x_{k,j}|\right\|_1\to 0 \tag{31}$$

for each k. Since also, by Lemmas 3.4 and 6.1,

$$\begin{aligned}\delta_k&\le\frac{1}{n^2p}\mathbb{E}\left[I^{(k)}(n,p)\right]+\frac{1}{\lambda(n,p)}\mathbb{E}\left[\sum_{j=1}^{2^k}\sum_{x\in\Pi_{k,j}}|x-x_{k,j}|\right]\\&=\frac{1}{n^2p}\mathbb{E}\left[I^{(k)}(n,p)\right]+\mathbb{E}\left[\frac12\sum_{j=1}^{2^k}w_{k,j}^2\right]\le\left(\frac23\right)^k,\end{aligned}$$

it follows by dominated convergence that, using (7),

$$\left\|X_{n,p}-X\big(\lambda(n,p)\big)\right\|_1\le\sum_{k=1}^{\infty}\delta_k\to 0.$$

Moreover, $\lambda(n,p)\to\lambda$, and it follows easily from (8) that $\left\|X\big(\lambda(n,p)\big)-X(\lambda)\right\|_1\to 0$. Hence we have $\mathbb{E}\,|X_{n,p}-X(\lambda)|\to 0$, which proves the convergence.

It remains to verify (31). Set

$$X^{(k)}=\sum_{j=1}^{2^k}\sum_{x\in\Pi_{k,j}}|x-x_{k,j}|.$$

Relation (31) is equivalent to

$$\mathbb{E}\left|\frac{1}{n}I^{(k)}(n,p) - X^{(k)}\right| \to 0. \tag{32}$$

For simplicity, we write in the sequel λ instead of $\lambda(n,p)$. We begin with a lemma.

Lemma 6.6. *For each k and j,*

$$\max\left\{\left\|Y_{k,j} - y'_{k,j}\right\|_1, \left\|Y_{k,j} - y_{k,j}\right\|_1\right\} \le \frac{k(1+\lambda)}{n}.$$

Proof. Recall that $p'_{k,j} = ny'_{k,j}$, so (30) translates to

$$p_{k,2j-1} = ny'_{k-1,j-1} + \lceil U_{k-1,j}(ny'_{k-1,j} - ny'_{k-1,j-1} - 1)\rceil,$$

We use induction on k. Comparing the definitions of $Y_{k,j}$ and $y'_{k,j}$, we see that it suffices to consider an odd $j = 2l-1$, and in that case there are three sources of a difference:

(i) The differences between $y'_{k-1,l-1}$ and $Y_{k-1,l-1}$ and between $y'_{k-1,l}$ and $Y_{k-1,l}$. By the induction hypothesis, this contributes at most $(k-1)(1+\lambda)/n$.

(ii) The -1 inside (and the rounding by) the ceiling function. This contributes at most $1/n$.

(iii) The shift of the pivot, from $p_{k,2j-1}$ to $p'_{k,2j-1}$, caused by the erroneous comparisons. The shift is bounded by the total number of errors at step k, so its mean is less than λ, and the contribution is less than λ/n.

□

We return to (32). For $k = 1$, $I^{(1)}(n,p)$ is just $t(n,p)$ studied in Section 3, and (10) yields

$$I^{(1)}(n,p) = s_\ell s_r + s_\ell + s_r + W_{\vec{\ell}} + W_{\vec{r}}.$$

Let E_1 be the set of items i such that an error was made in the comparison with $p_{1,1}$. Relation (11) entails that

$$\sum_{i\in E_1} |i - p_{1,1}| = W_{\vec{\ell}} + W_{\vec{r}} + \tfrac{1}{2}s_\ell(s_\ell+1) + \tfrac{1}{2}s_r(s_r+1).$$

We shall denote this last sum $\tilde{I}^{(1)}(n,p)$. Thus, we have

$$\left|I^{(1)}(n,p) - \tilde{I}^{(1)}(n,p)\right| = \left|s_\ell s_r + s_\ell + s_r - \tfrac{1}{2}s_\ell(s_\ell+1) - \tfrac{1}{2}s_r(s_r+1)\right| \le s_\ell^2 + s_r^2.$$

Furthermore

$$\mathbb{E}\left[s_\ell^2 \mid \lceil nU_{1,1} = k\rceil\right] = (k-1)p(1-p) + ((k-1)p)^2 \le np + n^2p^2. \tag{33}$$

Hence,

$$\left\|I^{(1)}(n,p) - \tilde{I}^{(1)}(n,p)\right\|_1 = \mathcal{O}(1).$$

Moreover, $\frac{1}{n}\tilde{I}^{(1)}(n,p) = \sum_{i\in E_1}|\frac{i}{n} - y_{1,1}|$ differs from $X^{(1)} = \sum_{j=1}^{2}\sum_{x\in\Pi_{1,j}}|x - x_{1,j}|$ in (32) in four ways only (recall that $x_{1,1} = x_{1,2} = Y_{1,1}$):

(i) i/n differs from x by at most $1/n$. Since the expected number of terms is not larger than λ, this gives a contribution $\mathcal{O}(1/n)$.

(ii) $|y_{1,1} - x_{1,j}| = |y_{1,1} - Y_{1,1}|$, which by Lemma 6.6 has expectation $\mathcal{O}(1/n)$. Thus this too gives a contribution $\mathcal{O}(1/n)$.

(iii) If there are two or more points in $\Pi_1 \cap (\frac{i-1}{n}, \frac{i}{n}]$ for some i, $X^{(1)}$ contains more terms than $\frac{1}{n}\tilde{I}^{(1)}(n,p)$. It is easily seen that the expected number of such extra points in each interval $(\frac{i-1}{n}, \frac{i}{n}]$ is less than $(\lambda/n)^2$, and each point contributes for at most 1 to $X^{(1)}$.

(iv) Each point in $\Pi_1 \cap (\frac{p_{1,1}-1}{n}, \frac{p_{1,1}}{n}]$ contributes for an extra term in $X^{(1)}$ again. The expected number of such extra points is λ/n and each of these terms contributes for at most 1 to $X^{(1)}$.

This verifies (32) for $k = 1$.

For $k \geq 2$ we argue similarly. We can approximate $I^{(k)}(n,p)$ by the sum of the distances between the errors and the respective pivots,

$$\tilde{I}^{(k)}(n,p) = \sum_{j \leq 2^{k-1}} \sum_{i \in E_{k-1,j}} |i - p_{k,2j-1}|,$$

as follows: Let $E_{k,j}$ be the set of items $i \in \ell_{k,j}$ subject to error when compared with $p_{k+1,2j-1}$, and let $\mathcal{G}_k$ be the σ-algebra generated by $(U_{\ell,j})_{\ell \leq k, j \leq 2^\ell}$ and $\Pi_1 \cup \Pi_2 \cup \cdots \cup \Pi_{k-1}$. As for $k = 1$, using relation (11), we obtain the following bound:

$$\begin{aligned}\mathbb{E}\left[\left|I^{(k)}(n,p) - \tilde{I}^{(k)}(n,p)\right| \;\middle|\; \mathcal{G}_k\right] &\leq \sum_{j \leq 2^{k-1}} \left(p^2 \left(\#\ell_{k-1,j}\right)^2 + p\#\ell_{k-1,j}\right) \\ &\leq 2^{k-1}(n^2p^2 + np) = \mathcal{O}\left(1\right),\end{aligned}$$

and as a consequence,

$$\left\|I^{(k)}(n,p) - \tilde{I}^{(k)}(n,p)\right\|_1 = \mathcal{O}\left(1\right).$$

Now,

$$\frac{1}{n}\tilde{I}^{(k)}(n,p) = \sum_{j \leq 2^{k-1}} \sum_{i \in E_{k-1,j}} \left|\frac{i}{n} - y_{k,2j-1}\right|$$

differs from $X^{(k)} = \sum_{j=1}^{2^k} \sum_{x \in \Pi_{k,j}} |x - x_{k,j}|$ in (32) in the same four ways as for $k = 1$, plus an extra fifth way:

(i) See the case $k = 1$.

(ii) $|y_{k,2j-1} - x_{k,2j-1}| = |y_{k,2j-1} - x_{k,2j}| = |y_{k,2j-1} - Y_{k,2j-1}|$, which by Lemma 6.6 has expectation $\mathcal{O}\left(1/n\right)$. Thus this too gives a contribution $\mathcal{O}\left(1/n\right)$.

(iii) Two or more points in $\Pi_k \cap (\frac{i-1}{n}, \frac{i}{n}]$ for some i, see the case $k = 1$.

(iv) Each point in $\Pi_k \cap (-1/n + y_{k,2j-1}, y_{k,2j-1}]$ contributes for an extra term in $X^{(k)}$. The expected number of such extra points is $\lambda 2^{k-1}/n$ and each of these terms contributes for at most 1 to $X^{(k)}$.

(v) There is a new source of error in this approximation, because some points x in Π_k and the corresponding positions $i = \lceil nx \rceil$ belong to subintervals that do not correspond to each other, because the endpoints $y'_{k-1,j}$ differ somewhat from $Y_{k-1,j}$. By Lemma 6.6, the expected number of such cases is $\mathcal{O}\left(1/n\right)$, so again we get a contribution of order $\mathcal{O}\left(1/n\right)$ only.

This verifies (32) and thus the convergence of $X_{n,p}$ to $X(\lambda)$.

The functional equation for $X(\lambda)$. We first check that $X(\lambda)$ satisfies the functional equation and our side conditions.

Proposition 6.7. *$(X(\lambda))_{\lambda>0}$ is a solution of (5). Moreover, $\mathbb{E}\left[X(\lambda)^n\right] < \infty$ and $\lambda^n \mathbb{E}\left[X(\lambda)^n\right] \to 0$ as $\lambda \to 0$, for $n \geq 1$.*

Proof. All moments are finite by Theorem 6.5. Moreover, $\mathbb{E}\left[(\lambda X(\lambda))^n\right] \to 0$ as $\lambda \to 0$ by (8) and dominated convergence.

For $a < b$, let $\Pi(a,b)$ is a Poisson point process of intensity λ on $\mathbb{N}^* \times [a,b]$, and let $\{U_{k,j} : k \geq 0, 1 \leq i \leq 2^k\}$ be independent uniform random variables as in Section 2, and further independent of $\Pi(a,b)$. Define $\{Y_{k,j} : k \geq 0, 1 \leq i \leq 2^k\}$ and $J_k(x)$ as in Section 2, with the slight modification

$$Y_{0,0} = a \qquad \text{and} \qquad Y_{0,1} = b$$

and set

$$X(\lambda, a, b) = \frac{1}{\lambda} \sum_{(k,x)\in\Pi(a,b)} \left|x - Y_{k,J_k(x)}\right|.$$

Note that $X(\lambda, 0, 1) = X(\lambda)$. Shifting and rescaling $\Pi(a,b)$, we obtain

$$X(\lambda, a, b) \overset{law}{=} X(\lambda, 0, b-a) \overset{law}{=} (b-a)^2 X(\lambda(b-a)).$$

Let us split $X(\lambda)$: we have

$$\begin{aligned}
X(\lambda) &= X_0(\lambda) + X_1(\lambda) + X_2(\lambda) \\
\lambda X_0(\lambda) &= \sum_{(x,1)\in\Pi(a,b)} \left|x - Y_{1,1}\right| \\
\lambda X_1(\lambda) &= \sum_{\substack{(k,x)\in\Pi(a,b)\\ k\geq 2, x \leq Y_{1,1}}} \left|x - Y_{k,J_k(x)}\right|, \\
\lambda X_2(\lambda) &= \sum_{\substack{(k,x)\in\Pi(a,b)\\ k\geq 2, x \geq Y_{1,1}}} \left|x - Y_{k,J_k(x)}\right|.
\end{aligned}$$

We see, using general properties of Poisson point processes and the recursive construction of $\{Y_{k,j} : k \geq 0, 1 \leq i \leq 2^k\}$, that

$$\begin{aligned}
(X_0(\lambda), X_1(\lambda), X_2(\lambda)) &\overset{law}{=} (\Theta(\lambda, Y_{1,1}), X(\lambda, 0, Y_{1,1}), \widetilde{X}(\lambda, Y_{1,1}, 1)) \\
&\overset{law}{=} (\Theta(\lambda, Y_{1,1}), Y_{1,1}^2 X(\lambda Y_{1,1}), (1-Y_{1,1})^2 \widetilde{X}(\lambda(1-Y_{1,1}))),
\end{aligned}$$

in the sense that, conditionally given that $Y_{1,1} = u$, $X_0(\lambda)$, $X_1(\lambda)$ and $X_2(\lambda)$ are independent and distributed as $\Theta(\lambda, u)$, $u^2 X(\lambda u)$, $(1-u)^2 X(\lambda(1-u))$, respectively. Also $Y_{1,1} = U_{0,1}$ is uniformly distributed on $[0,1]$. ☐

Uniqueness of solutions of (5)**.** The idea of the proof is that (5) uniquely determines the moments of its solutions. However, using (5), computations of moments by induction are hardly tractable because all three terms on the right of (5) depend on U. To circumvent this problem, we consider a new functional equation

$$Y(\lambda) \overset{law}{=} \xi(\lambda) + UY(\lambda U) + (1-U)\widetilde{Y}(\lambda(1-U)), \tag{34}$$

in which

- $\xi(\lambda)$ is as in Section 2; equivalently, $\xi(\lambda) = \sum_{x\in\Pi_1} x$;
- $\xi(\lambda)$ and $\left(U, Y(\lambda U), \widetilde{Y}(\lambda(1-U))\right)$ are independent;
- conditionally, given $U = u$, $Y(\lambda U)$ and $\widetilde{Y}(\lambda(1-U))$ are independent and distributed as $Y(\lambda u)$ and $Y(\lambda(1-u))$, respectively.

We say that a family of nonnegative random variables $(Y(\lambda))_{\lambda>0}$ (with laws depending measurably on λ) is an *admissible* solution of (34) if it satisfies furthermore, for any $n \geq 1$,

(i) $\mathbb{E}[Y(\lambda)^n] < \infty$;
(ii) $\lambda^{n-1}\mathbb{E}[Y(\lambda)^n] \to 0$ as $\lambda \to 0$.

Similarly, we say that a solution $(Z(\lambda))_{\lambda>0}$ of (5) is admissible if it satifies the conditions $\mathbb{E}[Z(\lambda)^n] < \infty$ and $\lambda^{2n-1}\mathbb{E}[Z(\lambda)^n] \to 0$ as $\lambda \to 0$ in Theorem 2.3.

To conclude the proof of the theorem, we prove the following two propositions.

Proposition 6.8. *If $(Z(\lambda))_{\lambda>0}$ is an admissible solution of* (5)*, then the family $(\xi(\lambda) + \lambda Z(\lambda))_{\lambda>0}$, in which $\xi(\lambda)$ and $Z(\lambda)$ are assumed independent, is an admissible solution of* (34).

Proposition 6.9. *All admissible solutions of* (34) *have the same moments $f_n(\lambda)$, $n \geq 1$.*

Let $(Z(\lambda))_{\lambda>0}$ be an admissible solution of (5). As the moments of $\xi(\lambda)+\lambda Z(\lambda)$ uniquely determine the moments of $Z(\lambda)$, it follows from Propositions 6.7, 6.8 and 6.9 that $X(\lambda)$ and $Z(\lambda)$ have the same moments. Since $X(\lambda)$ has an exponentially decreasing tail by Lemma 6.5 , its moments satisfy the Carleman condition [2, Chap. 7], and determine uniquely its distribution. Hence $Z(\lambda) \stackrel{law}{=} X(\lambda)$, concluding the proof of uniqueness for admissible solutions of (5).

Before proving Propositions 6.8 and 6.9, we need a lemma.

Lemma 6.10. *The n-th moment $g_n(\lambda) = \mathbb{E}[\xi(\lambda)^n]$ is a polynomial of degree n with $g_n(0) = 0$.*

Proof. Owing to Campbell's Theorem [5, p.28], we have

$$\mathbb{E}\left[e^{s\xi(\lambda)}\right] = \exp\left(\lambda\left(\mathbb{E}\left[e^{sU}\right] - 1\right)\right) = \exp\left(\lambda\left(\frac{s}{2!} + \frac{s^2}{3!} + \dots\right)\right).$$

Expanding the last expression gives the lemma. □

Proof of Proposition 6.8. Lemma 6.10 shows that $\mathbb{E}[\xi(\lambda)^n]$ is finite for every λ and converges to 0 as $\lambda \to 0$. Hence, by Minkowski's inequality for the norm $\|\cdot\|_n = \mathbb{E}[|\cdot|^n]^{1/n}$, the conditions on the moments of $Y(\lambda) = \xi(\lambda) + \lambda Z(\lambda)$ follow from (and are equivalent to) the corresponding conditions on the moments of $Z(\lambda)$.

To show (34), it is enough to show

$$\begin{aligned}\lambda Z(\lambda) &\stackrel{law}{=} UY(\lambda U) + (1-U)\widetilde{Y}(\lambda(1-U)) \\ &= U\xi(\lambda U) + \lambda U^2 Z(\lambda U) + (1-U)\widetilde{\xi}(\lambda(1-U)) + \lambda(1-U)^2\widetilde{Z}(\lambda(1-U)),\end{aligned}$$

where, as usual, conditioned on $U = u$, the terms on the right hand side are independent with the right distributions. This follows immediately from (5), since

$$\lambda\Theta(\lambda, u) \stackrel{law}{=} u\xi(\lambda u) + (1-u)\widetilde{\xi}(\lambda(1-u)).$$

□

Proof of Proposition 6.9. Consider the sequence of integral equations

$$P_0(\lambda) = 1, \qquad P_n(\lambda) = 2\int_0^1 u^n P_n(\lambda u)du + \psi_n(\lambda), \quad n \geq 1, \tag{35}$$

in which

$$\psi_n(\lambda) = \sum_{\substack{r+k+\ell=n\\ k<n,\ell<n}} \binom{n}{r,k,\ell} g_r(\lambda) \int_0^1 u^k (1-u)^\ell P_k(\lambda u) P_\ell(\lambda(1-u))\, du. \tag{36}$$

Proposition 6.9 is a consequence of the next lemma. □

Lemma 6.11. *The induction formula* (35) *and the initial condition* $P_1(0) = 0$ *defines a unique sequence of polynomials,* $(P_n(\lambda))_{n\geq 0}$. *Furthermore,* P_n *has degree* n*, and vanishes at* 0. *If* $(Y(\lambda))_\lambda$ *is an admissible solution of (34), then, for* $n \geq 1$*, its* n*-th moment* $\mathbb{E}\left[Y(\lambda)^n\right]$ *is equal to* $P_n(\lambda)$.

Proof. Consider $n \geq 1$ and assume that the properties in the lemma hold for $1 \leq m \leq n-1$. Then, for k and ℓ smaller than n, and $r+k+\ell = n$, the expression

$$g_r(\lambda) \int_0^1 u^k (1-u)^\ell P_k(\lambda u) P_\ell(\lambda(1-u))\, du$$

is a polynomial with degree n and, due to Lemma 6.10, vanishes at 0. Thus, in this case, $\psi_n(\lambda)$ is a polynomial with degree n, vanishing at 0. It is now easy to check that a polynomial $P_n(\lambda)$ satisfies (35) if and only if, for $(n,k) \neq (1,0)$,

$$\left[\lambda^k\right] P_n = \frac{n+k+1}{n+k-1} \left[\lambda^k\right] \psi_n. \tag{37}$$

Also, by the induction assumptions,

$$\begin{aligned}
\mathbb{E}\left[Y(\lambda)^n\right] &= \mathbb{E}\left[\left(\xi(\lambda) + UY(U\lambda) + (1-U)\widetilde{Y}((1-U)\lambda)\right)^n\right] \\
&= \sum_{r+k+\ell=n} \binom{n}{r,k,\ell} g_r(\lambda) \mathbb{E}\left[U^k (1-U)^\ell Y(U\lambda)^k \widetilde{Y}((1-U)\lambda)^\ell\right] \\
&= 2\mathbb{E}\left[U^n Y(\lambda U)^n\right] + \psi_n(\lambda).
\end{aligned}$$

Note that $\psi_n(\lambda) \geq 0$ for $\lambda \geq 0$. Since Y is admissible, $\lambda \to f_n(\lambda) = \mathbb{E}\left[Y(\lambda)^n\right]$ is nonnegative and measurable. Thus, for $\lambda > 0$, we can rewrite the previous equation:

$$\begin{aligned}
f_n(\lambda) &= 2\int_0^1 u^n f_n(\lambda u) du + \psi_n(\lambda) \\
&= 2\lambda^{-n-1} \int_0^\lambda v^n f_n(v) dv + \psi_n(\lambda).
\end{aligned}$$

Since $f_n(\lambda)$ is assumed to be finite and $\psi_n(\lambda) \geq 0$, the integral on the right hand side is convergent, and thus it is a continuous function of λ. As a consequence f_n belongs to $C^\infty(0,+\infty)$, and is solution, on $(0,+\infty)$, of the following differential equation:

$$\lambda f_n'(\lambda) + (n-1) f_n(\lambda) = (n+1)\psi_n(\lambda) + \lambda \psi_n'(\lambda).$$

As Y is admissible, $\lambda^{n-1} f_n(\lambda) \to 0$ as $\lambda \to 0$, but the general solution of the differential equation is $P_n(\lambda) + C\,\lambda^{-n+1}$. Thus $f_n = P_n$ on $(0,+\infty)$. □

Computation of the first moments. The moments of $Y(\lambda)$, and thus of $X(\lambda)$, can be computed up to arbitrary order with the help of (35). For the first two moments, the calculations run as follows. Expanding

$$\exp\left(\lambda\left(\frac{s}{2!}+\frac{s^2}{3!}+\dots\right)\right),$$

in the proof of Lemma 6.10 we obtain

Lemma 6.12.

$$g_1(\lambda)=\mathbb{E}\left[\xi(\lambda)\right]=\frac{1}{2}\lambda \qquad \textit{and} \qquad g_2(\lambda)=\mathbb{E}\left[\xi(\lambda)^2\right]=\frac{1}{4}\lambda^2+\frac{1}{3}\lambda.$$

Proposition 6.13.

$$\lambda\mathbb{E}\left[X(\lambda)\right]=\mathbb{E}\left[\Xi(\lambda)\right]=\lambda \qquad \textit{and} \qquad \lambda^2\mathrm{Var}\left(X(\lambda)\right)=\mathrm{Var}\left(\Xi(\lambda)\right)=\frac{1}{3}\lambda+\frac{1}{12}\lambda^2.$$

Proof. Taking $n=1$ in (36) and (37), we find, using Lemma 6.12,

$$\psi_1(\lambda)=g_1(\lambda)=\tfrac{1}{2}\lambda,$$
$$P_1(\lambda)=\tfrac{3}{1}\cdot\tfrac{1}{2}\lambda=\tfrac{3}{2}\lambda.$$

Taking $n=2$, we similarly find

$$\begin{aligned}\psi_2(\lambda)&=g_2(\lambda)+2\cdot 2g_1(\lambda)\int_0^1 uP_1(u)\,du+2\int_0^1 u(1-u)P_1(\lambda u)P_1(\lambda(1-u))\,du\\&=\tfrac{1}{3}\lambda+\tfrac{7}{5}\lambda^2,\\P_2(\lambda)&=\tfrac{4}{2}\cdot\tfrac{1}{3}\lambda+\tfrac{5}{3}\cdot\tfrac{7}{5}\lambda^2=\tfrac{2}{3}\lambda+\tfrac{7}{3}\lambda^2.\end{aligned}$$

Since $Y(\lambda)=\xi(\lambda)+\lambda X(\lambda)$, with independent summands,

$$P_1(\lambda)=\mathbb{E}\left[Y(\lambda)\right]=\mathbb{E}\left[\xi(\lambda)\right]+\lambda\mathbb{E}\left[X(\lambda)\right],$$

which by Lemma 6.12 yields $\lambda\mathbb{E}\left[X(\lambda)\right]=\lambda$. Similarly,

$$\lambda^2\mathbb{E}\left[X(\lambda)^2\right]=P_2(\lambda)-\mathbb{E}\left[\xi(\lambda)^2\right]-2\mathbb{E}\left[\xi(\lambda)\right]\mathbb{E}\left[\lambda X(\lambda)\right]=\tfrac{1}{3}\lambda+\tfrac{13}{12}\lambda^2,$$

which yields the variance formula. □

The formulas for mean and variance of $X(\lambda)$ can also be obtained directly from (8) and Lemma 6.12; we leave this as an exercise.

7. Concluding remarks

We have presented a probabilistic analysis of Quicksort when some comparisons can err. Analysing other sorting algorithms such as merge sort, insertion sort or selection is even more intricate. They do not fit into the model presented in this paper and further more involved probabilistic models/arguments are required. We conjecture that the same normalization holds for the number of inversions in the *output of merge sort* for $n=2^m\to+\infty$, $p=\lambda/n$, and that the limit law $\hat{Y}(\lambda)$ satisfies

$$\mathbb{E}\left[\hat{Y}(\lambda)\right]=\sum_{k\geq 0}\frac{2^k}{(2^k+2)(2^k+3)}=0.454674373\dots<\mathbb{E}\left[X(\lambda)\right].$$

References

[1] J.D. Biggins. Uniform convergence of martingales in the branching random walk, *Ann. Probab.*, 20(1):137–151, 1992.
[2] W. Feller. *An introduction to probability theory and its applications, Vol. II,* 2nd ed., John Wiley & Sons, 1971.
[3] F. Ergün, S. Kannan, S.R. Kummar, R. Rubinfeld & M. Vishanathan. Spot-Checkers, *J. Comput. Sys. Sci.*, 60(3):717–751, 2000.
[4] R. Grüber & U. Rösler. Asymptotic distribution theory for Hoare's selection algorithm, *Adv. Appl. Prob.*, 28:252–269, 1996.
[5] J.F.C. Kingman. *Poisson processes,* Oxford University Press, New York, 1993.
[6] D.E. Knuth. *The Art of Computer Programming. Vol. 3 : Sorting and Searching,* 2nd ed., John Wiley & Sons, 1986.
[7] H.M. Mahmoud. *Evolution of random search trees,* John Wiley & Sons, 1992.
[8] B. Pittel. On growing random binary trees, *J.Math.Anal.Appl.*, 103:461–480, 1984.
[9] S.T. Rachev. *Probability Metrics and the Stability of Stochastic Models*, Wiley, Chichester, U.K., 1991.
[10] U. Rösler. A limit theorem for "Quicksort", *Theor. Inf. Appl.*, 25:85–100, 1991.
[11] U. Rösler & L. Rüschendorf. The contraction method for recursive algorithms, *Algorithmica*, 29:3-33, 2001.

INRIA-Lorraine and LORIA, Université Henri Poincaré-Nancy I, BP 239, 54506, Vandœuvre-lès-Nancy, France
E-mail address: Laurent.Alonso@loria.fr

Institut Élie Cartan, Université Henri Poincaré-Nancy I, BP 239, 54506, Vandœuvre-lès-Nancy, France
E-mail address: Philippe.Chassaing@antares.iecn.u-nancy.fr
URL: http://www.iecn.u-nancy.fr/~chassain/

Institut Élie Cartan, Université Henri Poincaré-Nancy I, BP 239, 54506, Vandœuvre-lès-Nancy, France
E-mail address: Florent.Gillet@antares.iecn.u-nancy.fr

Department of Mathematics, Uppsala University, PO Box 480, S-751 06 Uppsala, Sweden
E-mail address: svante.janson@math.uu.se
URL: http://www.math.uu.se/~svante/

Department of Computer Science, Illinois Institute of Technology, Stuart Building, 10 West 31st Street, Suite 236, Chicago, IL 60616-3729 U.S.A.
E-mail address: reingold@iit.edu

Institut Élie Cartan and LORIA, Université Henri Poincaré-Nancy I, BP 239, 54506, Vandœuvre-lès-Nancy, France
E-mail address: schott@loria.fr