Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institute of Theoretical Computer Science
Mohsen Ghaffari, Angelika Steger, David Steurer, Emo Welzl, Peter Widmayer

Algorithms, Probability, and Computing **Solutions KW42** **HS17**

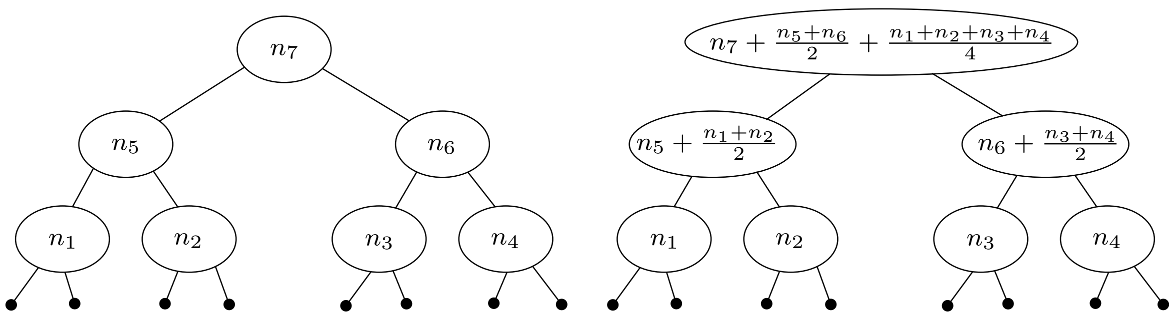
Solution of in-class exercise 1: Locating a Point in a Line Arrangement

The lemma contains a chain of two inequalities:

$$\sum_{v \text{ inner node}} |\bar{S}_v| \leq 2 \cdot \sum_{v \text{ inner node}} |S_v| \leq 2n^2.$$

The second inequality is easy to derive: The number $|S_v|$ of coordinates for level v can be bounded by the number of edges that belong to level v, and the total number of edges does not exceed n^2.

So it remains to look at the first inequality. Let us first look at an example, so that we may believe the statement. Below we have depicted a tree to store $n = 7$ levels: On the left-hand side, the tree for the original sets S_v, and on the right-hand side, the tree with the 'enhanced' sets $\bar{S}_v$. We have annotated the nodes with the number ($|S_v|$ and $|\bar{S}_v|$, respectively) of x-coordinates stored in that node.



Indeed our example has

$$\begin{aligned}\sum_{v \text{ inner node}} |\bar{S}_v| &= \left(1 + \frac{1}{2} + \frac{1}{4}\right)(n_1 + n_2 + n_3 + n_4) + \left(1 + \frac{1}{2}\right)(n_5 + n_6) + n_7 \\ &\leq 2\,(n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7) \\ &= 2 \cdot \sum_{v \text{ inner node}} |S_v|.\end{aligned}$$

The example suggests that we should group the nodes of the tree by their depth. (We refrain to speak of the 'levels' of the tree, because that will almost certainly cause confusion vis-à-vis the levels v of the line arrangement). Thus, let h denote the height of the tree and for $0 \le i \le h$ let

$$m_i := \sum_{\substack{v \text{ inner node} \\ \text{at depth } i}} |S_v|, \qquad \bar{m}_i := \sum_{\substack{v \text{ inner node} \\ \text{at depth } i}} |\bar{S}_v|.$$

Now

$$\sum_{v \text{ inner node}} |\bar{S}_v| = \sum_{k=0}^{h} \bar{m}_k \le m_h + \sum_{k=0}^{h-1} \left(m_k + \frac{\bar{m}_{k+1}}{2} \right) = \sum_{v \text{ inner node}} |S_v| + \frac{1}{2} \cdot \sum_{v \text{ inner node}} |\bar{S}_v| - \frac{\bar{m}_0}{2}$$

which yields the claim.

Solution of in-class exercise 2: Nearest Neighbor Changes

This is the classical use case for backward analysis. Instead of considering the points as being inserted one by one and counting the number of nearest neighbors occurring, we get the very same number if we start with the whole set $P_n := P$, and then for each $i = n-1, n-2, \dots, 1$, obtain P_i from P_{i+1} by removing a point $p \in P_i$ chosen uniformly at random.

Define X_i to be the nearest neighbor of q in P_i. We are interested in the random variable $X := |\{X_i | i \in \{1..n\}\}|$. To this end we just calculate the probability $x_i = \Pr[X_i \neq X_{i+1}]$ for $1 \le i \le n-1$. Clearly, then,

$$\mathbf{E}[X] = 1 + \sum_{i=1}^{n-1} x_i.$$

We now note that $X_i \neq X_{i+1}$ occurs if and only if $P_i = P_{i+1} \setminus \{X_{i+1}\}$. This yields that

$$x_i = \Pr[X_i \neq X_{i+1}] = \Pr[P_i = P_{i+1} \setminus \{X_{i+1}\}] = \frac{1}{i+1},$$

where the second equality follows from the fact that P_i is generated from P_{i+1} by removing a point uniformly at random. As a very important remark: please note that this simple argument only works because **no matter** what P_{i+1} is, P_i is always generated by removing one of its elements uniformly at random and the random variable X_i **is completely determined** by P_i (what the currently nearest point is does not depend on the insertion history). You have to verify this before you apply a backward analysis of this type.

Finally,

$$\mathbf{E}[X] = 1 + \sum_{i=1}^{n-1} x_i = H_n.$$

Solution of in-class exercise 3: Checking Matrix Multiplication

Assume that the matrix C is wrong in exactly the i-th row compared to the correct product AB. We define $D = AB - C$. This is a zero-matrix except in the i-th row, $D_{i,-} \neq (0, \ldots, 0)$. The probability of detecting an error equals $\Pr\left[(D_{i,-})^T x \equiv_2 1\right]$, where $x \in_{\text{u.a.r.}} \{0, 1\}^n$. We have seen in the lecture (not in the lecture notes) that this probability equals $\frac{1}{2}$. Here is a formal proof of the argument: Let j be such that $D_{ij} = 1$. We have

$$(Dx)_i = (D_{i,-})^T x = \sum_{k=1}^{n} D_{ik} x_k = \underbrace{\sum_{k=1, k \neq j}^{n} D_{ik} x_k}_{=: S} \quad + \quad \underbrace{D_{ij}}_{=1} x_j,$$

hence

$$\begin{aligned}
\Pr\left[(Dx)_i = 1\right] &= \Pr\left[S + x_j = 1\right] \\
&= \Pr\left[S + x_j = 1 \mid S = 0\right] \cdot \Pr\left[S = 0\right] + \Pr\left[S + x_j = 1 \mid S = 1\right] \cdot \Pr\left[S = 1\right] \\
&= \Pr\left[x_j = 1 \mid S = 0\right] \cdot \Pr\left[S = 0\right] + \Pr\left[x_j = 0 \mid S = 1\right] \cdot \Pr\left[S = 1\right] \\
&= \Pr\left[x_j = 1\right] \cdot \Pr\left[S = 0\right] + \Pr\left[x_j = 0\right] \cdot \Pr\left[S = 1\right] \\
&\qquad\qquad\qquad\qquad \text{because } S, x_j \text{ are independent} \\
&= \frac{1}{2} \cdot \Pr\left[S = 0\right] + \frac{1}{2} \cdot \Pr\left[S = 1\right] \\
&= \frac{1}{2}.
\end{aligned}$$

Solution of in-class exercise 4: The Schwartz-Zippel Theorem is Tight

Let $\{a_1, \ldots, a_d\} \subseteq S$ be a set of d elements. We define the polynomial $p(x_1, \ldots, x_n)$ as

$$p(x_1, \ldots, x_n) := (x_1 - a_1)(x_1 - a_2) \cdots (x_1 - a_d).$$

Note that the only variable occurring in this polynomial is x_1, and the degree of the polynomial is d.

This polynomial evaluates to zero if and only if $x_1 \in \{a_1, \ldots, a_d\}$. The other variables $x_2, \ldots, x_n$ can be set to arbitrary values in S. Therefore, the number of n-tuples $(r_1, \ldots, r_n) \in S^n$ with $p(r_1, \ldots, r_n) = 0$ is exactly

$$\underbrace{d}_{\text{choices for } r_1} \times \underbrace{|S|}_{\text{choices for } r_2} \times \cdots \times \underbrace{|S|}_{\text{choices for } r_n},$$

which is $d \cdot |S|^{n-1}$.

Solution of in-class exercise 5: The Permanent and the Determinant

(a) By the definition of the determinant and by linearity of expectation, we have

$$\mathbf{E}[\det(B)] = \sum_{\pi \in \mathcal{S}_n} \operatorname{sign}(\pi)\, \mathbf{E}\Big[b_{1,\pi(1)} b_{2,\pi(2)} \dots b_{n,\pi(n)}\Big].$$

Now let $Z \subseteq \mathcal{S}_n$ be defined as

$$Z := \{\pi \in \mathcal{S}_n | a_{1,\pi(1)} a_{2,\pi(2)} \dots a_{n,\pi(n)} = 1\},$$

that is the set of transversals that do not contain a zero element of A. We then have that

$$\mathbf{E}[\det(B)] = \sum_{\pi \in Z} \operatorname{sign}(\pi)\, \mathbf{E}\Big[\epsilon_{1,\pi(1)} \epsilon_{2,\pi(2)} \dots \epsilon_{n,\pi(n)}\Big],$$

and by independence of the $\epsilon_{i,j}$,

$$\mathbf{E}[\det(B)] = \sum_{\pi \in Z} \operatorname{sign}(\pi)\, \mathbf{E}\Big[\epsilon_{1,\pi(1)}\Big]\, \mathbf{E}\Big[\epsilon_{2,\pi(2)}\Big] \dots \mathbf{E}\Big[\epsilon_{n,\pi(n)}\Big] = 0,$$

as each expectation is zero.

(b) This calculation is more involved. We first note that by definition (and reusing the set Z from (a)),

$$\mathbf{E}\Big[(\det(B))^2\Big] = \mathbf{E}\left[\left(\sum_{\pi \in Z} \operatorname{sign}(\pi) \epsilon_{1,\pi(1)} \epsilon_{2,\pi(2)} \dots \epsilon_{n,\pi(n)}\right)^2\right].$$

Expanding the multiplication and applying linearity of expectation yields

$$\mathbf{E}\Big[(\det(B))^2\Big] = \sum_{\pi_1,\pi_2 \in Z} \operatorname{sign}(\pi_1) \cdot \operatorname{sign}(\pi_2) \cdot \mathbf{E}\Big[\epsilon_{1,\pi_1(1)} \epsilon_{1,\pi_2(1)} \epsilon_{2,\pi_1(2)} \epsilon_{2,\pi_2(1)} \dots \epsilon_{n,\pi_1(n)} \epsilon_{n,\pi_2(n)}\Big].$$

Now we start disentangling dependencies. First of all, since the $\epsilon_{i,j}$ are independent from one another, we can separate the expectation as

$$\mathbf{E}\Big[(\det(B))^2\Big] = \sum_{\pi_1,\pi_2 \in Z} \operatorname{sign}(\pi_1) \cdot \operatorname{sign}(\pi_2) \cdot \mathbf{E}\Big[\epsilon_{1,\pi_1(1)} \epsilon_{1,\pi_2(1)}\Big]\, \mathbf{E}\Big[\epsilon_{2,\pi_1(2)} \epsilon_{2,\pi_2(1)}\Big] \dots \mathbf{E}\Big[\epsilon_{n,\pi_1(n)} \epsilon_{n,\pi_2(n)}\Big].$$

Now we observe that

$$\mathbf{E}\Big[\epsilon_{i,j} \epsilon_{i,k}\Big] = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{otherwise.} \end{cases}$$

For that reason, all the summands with $\pi_1 \neq \pi_2$ have at least one zero factor in the product and thus vanish. Remaining are the summands where the permutations are equal and thus

$$\mathbf{E}\Big[(\det(B))^2\Big] = \sum_{\pi \in Z} \operatorname{sign}^2(\pi) \cdot \mathbf{E}\Big[\epsilon^2_{1,\pi(1)}\Big]\, \mathbf{E}\Big[\epsilon^2_{2,\pi(2)}\Big] \dots \mathbf{E}\Big[\epsilon^2_{n,\pi(n)}\Big] = |Z|.$$

On the other hand, obviously

$$\operatorname{per}(A) = \sum_{\pi \in Z} 1 = |Z|,$$

which establishes the claim.