Correctness Proof for Fisher-Yates Shuffle

Peter J. Haas

February 25, 2020

We can assume without loss of generality that we start out with array $x = [1, 2, \ldots, N]$. Now consider an arbitrary permutation $x' = [b_1, b_2, \ldots, b_N]$ where $b_1, \ldots, b_N$ are distinct integers between 1 and n. What is the probability that the F-Y algorithm produces x' from x? From the definition of conditional probability, we have

$$\begin{aligned}
&P(x'[i] = b_i \text{ for } 1 \le i \le N) \\
&\quad = P(x'[N] = b_N) \\
&\qquad \times P(x'[N-1] = b_{N-1} \mid x'[N] = b_N) \\
&\qquad \times P(x'[N-2] = b_{N-2} \mid x'[N] = b_n, x'[N-1] = b_{N-1}) \\
&\qquad \times \cdots \times P(x'[1] = b_1 \mid x'[N] = b_N, x'[N-1] = b_{N-1}, \ldots, x'[2] = b_2)
\end{aligned} \tag{1}$$

For the first random swap, it is clear that $P(x'[N] = b_N) = \frac{1}{N}$ since each item in the array is equally likely to be selected. For the second random swap, given that b_N is in position N, the probability that b_{N-1} (rather than one of the $N-2$ other remaining items) will end up in position $N-1$ is $\frac{1}{N-1}$, i.e.,

$$P(x'[N-1] = b_{N-1} \mid x'[N] = b_N) = \frac{1}{N-1}.$$

Continuing in this manner, we find that

$$P(x'[i] = b_i \mid x'[N] = b_N, x'[N-1] = b_{N-1}, \ldots, x'[i+1] = b_{i+1}) = \frac{1}{i}$$

for all i. Substituting into (1), we obtain

$$P(x'[i] = b_i \text{ for } 1 \le i \le N) = \frac{1}{N!}.$$

Since the permutation x' was arbitrary, this implies that each of the $N!$ possible permutations of x is produced with equal probability, as asserted.

Note: Recall that a "simpler" algorithm goes as follows: For $i = 1, 2, \ldots, n$, choose a random number $J \in \{1, 2, \ldots, n\}$ and swap $x[i]$ with $x[J]$. This simpler algorithm does not work. (Try running the algorithm many times and see how many times each possible permutation comes up. If the algorithm worked, the frequencies of the different permutations should be roughly equal.) A nice discussion of what goes wrong can be found at `https://blog.codinghorror.com/the-danger-of-naivete/`.