Quantum Bernoulli Factory

Suzie Brown

June 25, 2018

Problem statement

Suppose we have access to a black box producing coin flips where the probability of observing heads is p. Roughly speaking, a Bernoulli factory is an algorithm that uses queries of this black box to produce a coin flip where the probability of observing heads is $f(p)$, for some specified function f.

Let us now make this notion more precise.

Definition 1. Let $f : S \to [0,1]$ be a function with domain $S \subseteq [0,1]$, and suppose we have a sequence of Bernoulli random variables $X_1, X_2, \ldots \overset{iid}{\sim} \text{Bernoulli}(p)$ with unknown parameter $p \in [0,1]$. Let $U \in \mathcal{U}$ denote a set of auxiliary random variables with known distributions, independent of p. Let τ_U be a stopping time with respect to the natural filtration. A *Bernoulli factory* is a function $\mathcal{A} : \mathcal{U} \times \{0,1\}^T \to \{0,1\}$ such that $\mathcal{A}(U, X_1, \ldots, X_T) \sim \text{Bernoulli}(f(p))$ for all $p \in [0,1]$. For brevity, we also denote $Y := \mathcal{A}(U, X_1, \ldots, X_T)$.

Example 1. $f(p) \equiv 1/2$.
The following solution to this problem is described in Von Neumann (1951). We flip the coin twice and, if the two outcomes are different, take the second one as the result. If the outcomes are the same, we start again. In this case no auxiliary random variable U is required.

$$\tau = \min\{t \in \{2, 4, \ldots\} : X_{t-1} \neq X_t\}$$
$$\mathcal{A}(X_1, \ldots, X_T) = X_\tau$$

It is easy to show that this procedure produces heads with probability 1/2:

$$\mathbb{P}(X_\tau = 1) = \mathbb{P}(X_2 = 1 \mid X_2 \neq X_1) = \frac{\mathbb{P}(X_1 = 0, X_2 = 1)}{\mathbb{P}(X_1 = 0, X_2 = 1) + \mathbb{P}(X_1 = 1, X_2 = 0)} = \frac{(1-p)p}{(1-p)p + p(1-p)} = \frac{1}{2}$$

The running time τ of this Bernoulli factory is random and unbounded. In particular, $\tau \overset{d}{=} 2 \times \text{Geom}(2p(1-p))$. The running time is minimised when $p = 1/2$ (i.e. we already have a fair coin), in which case the expected running time is $\mathbb{E}(\tau) = 4$. This is why Von Neumann (1951) claims "the amended process is at most 25 percent as efficient as ordinary coin-tossing". He motivates this as a technique to ensure perfectly unbiased coin flips, but the more biased the original coin flipping procedure, the less efficient this correction will be, as illustrated in Figure 1.

Example 2. $f(p) = p^k, k \in \{1, 2, \ldots\}$.
This problem is solved easily by flipping the coin k times and outputting heads only if all k flips return heads. Again no auxiliary random variable is required.

$$\tau = k$$
$$\mathcal{A}(X_1, \ldots, X_T) = \mathbb{I}\{X_1 = 1, X_2 = 1, \ldots, X_\tau = 1\}$$

In this case the running time is deterministically equal to k. The procedure can be sped up if we allow a random running time, still bounded above by k, by stopping the process early if tails comes up. In this case we have

$$\tau = k \wedge \min\{t \in \{1, 2, \ldots\} : X_t = 0\}$$

and $\tau \overset{d}{=} \min\{k, \text{Geom}(1-p)\}$. Figure 2 shows the expected running time of this procedure for $k = 2$.

References

Von Neumann, J. (1951), '13. various techniques used in connection with random digits', *Appl. Math Ser* **12**(36-38), 3.

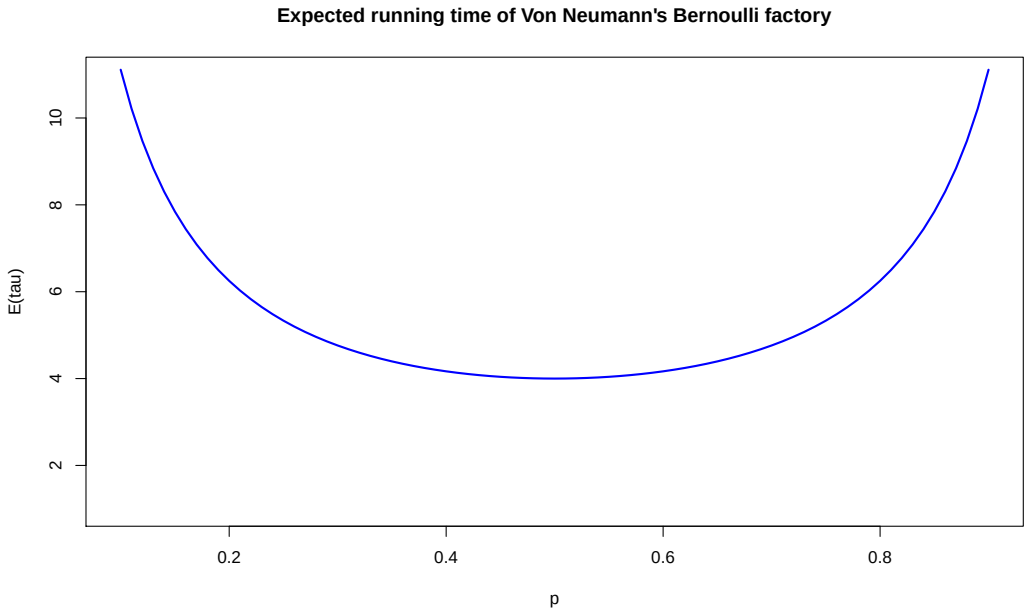

Figure 1: •

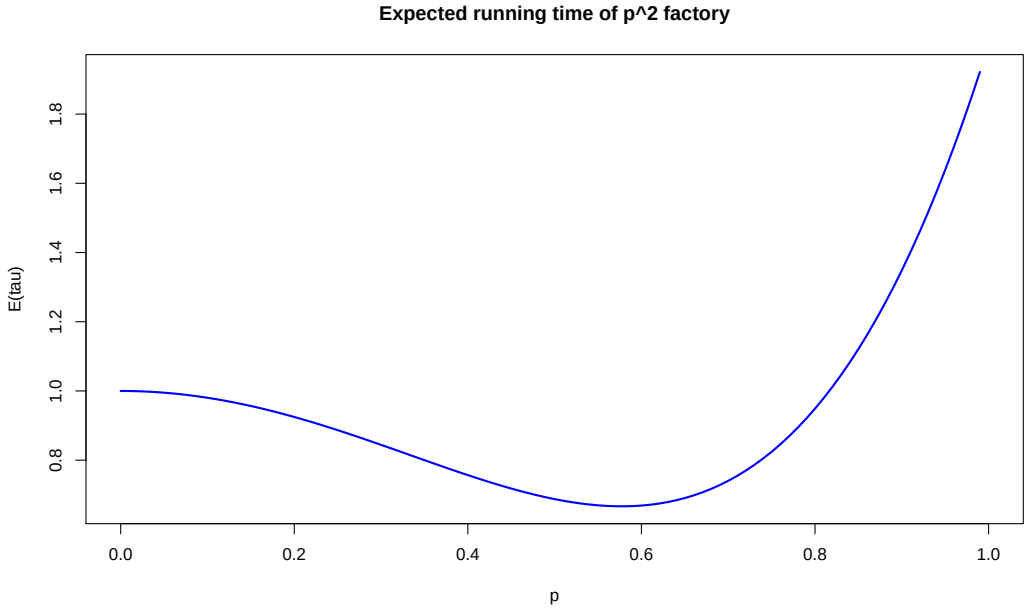

Figure 2: •