Chapter 4. Probabilistic Arguments

A. Introduction — Strong uniform times.

There are a number of other arguments available for bounding the rate of convergence to the uniform distribution. This chapter discusses the method of strong uniform times and coupling. Let's begin with a simple example, drawn from Aldous and Diaconis (1986).

Example 1. Top in at random. Consider mixing a deck of n cards by repeatedly removing the top card and inserting it at a random position. This corresponds to choosing a random cycle:

$$(1) \qquad P(\mathrm{id}) = P(21) = P(321) = P(4321) = \ldots = P(n\, n-1 \ldots 1) = \frac{1}{n}.$$

The following argument will be used to show that $n \log n$ shuffles suffice to mix up the cards. Consider the bottom card of the deck. This card stays at the bottom until the first time a card is inserted below it. This is a geometric waiting time with mean n. As the shuffles continue, eventually a second card is inserted below the original bottom card (this takes about $n/2$ further shuffles). The two cards under the original bottom card are equally likely to be in relative order low-high or high-low.

Similarly, the first time a third card is inserted below the original bottom card, each of the six possible orders of the three bottom cards is equally likely. Now consider the first time T that the original bottom card comes to the top. By an inductive argument, all $(n-1)!$ arrangements of the lower cards are equally likely. When the original bottom card is inserted at random, all $n!$ possible arrangements of the deck are equally likely.

When the original bottom card is at position k from the bottom, the waiting time for a new card to be inserted is geometric with mean n/k. Thus the waiting time T has mean $n + \frac{n}{2} + \frac{n}{3} + \ldots + \frac{n}{n} \doteq n \log n$.

To make this argument rigorous, introduce strong uniform times. Let G be a finite group. Intuitively, a stopping time is a rule which looks at a sequence of elements in G and says "stop at the jth one." The rule is allowed to depend on what appears up to time j, but not to look in the future. Formally, *a stopping time* is a function $T\colon G^\infty \to \{1, 2, \ldots, \infty\}$ such that if $T(\underset{\sim}{s}) = j$ then $T(\underset{\sim}{s}') = j$ for all $\underset{\sim}{s}'$ with $s_i' = s_i$ for $1 \le i \le j$. Let Q be a probability on G, X_k the associated random walk, P the associated probability on G^∞. A *strong uniform time* T is a stopping time T such that for each $k < \infty$,

$$(2) \qquad P\{T = k,\ X_k = s\} \quad \text{is constant in } s.$$

Note that (2) is equivalent to independence of the stopping time and the stopped process:

(3)
$$P\{X_k = s | T = k\} = 1/|G|$$

or to

(4)
$$P\{X_k = s | T \le k\} = 1/|G|.$$

In Example 1, the time T that the first card takes to reach the top and has been inserted into the deck is certainly a stopping time. The inductive argument given shows that, given $T = k$, all arrangements of the deck are equally likely, so T is a strong uniform time. Many other examples will be given in the remainder of this chapter. The following lemma relates strong uniform times to the distance between Q^{*k} and the uniform distribution U.

LEMMA 1. *Let Q be a probability on the finite group G. Let T be a strong uniform time for Q. Then for all $k \ge 0$*

$$||Q^{*k} - U|| \le P\{T > k\}.$$

Proof. For any $A \subset G$,

$$\begin{aligned} Q^{*k}(A) &= P\{X_k \in A\} \\ &= \sum_{j \le k} P\{X_k \in A, T = j\} + P\{X_k \in A, T > k\} \\ &= \sum_{j \le k} U(A) P(T = j) + P\{X_k \in A | T > k\}\ P\{T > k\} \\ &= U(A) + [P\{X_k \in A | T > k\} - U(A)]\ P\{T > k\}. \end{aligned}$$

Thus,

$$|Q^{*k}(A) - U(A)| \le P\{T > k\}.$$

□

Using this result we can deduce a sharp bound for the first example: $n \log n$ steps are both necessary and sufficient to drive the variation distance to zero.

Theorem 1. *For the top in at random shuffle defined in (1), let $k = n \log n + cn$. Then,*

(5)
$$||P^{*k} - U|| \le e^{-c} \text{ for } c \ge 0,\ n \ge 2,$$

(6)
$$||P^{*k} - U|| \to 1 \text{ as } n \to \infty,\ \textit{for } c = c(n) \to -\infty.$$