Broccoli

We will spend most of the course on a simpler random situation: that of passing Broccoli around a dinner table. Dinner guests labeled $0, 1, \dots, p-1$ are sitting at a round table. Guest 0 has a bowl of Broccoli they wish to pass either to their left or their right. They will decide by flipping a coin: heads to the right and tails to the left. The receiver will then repeat the procedure to again pass the Broccoli. We say that the Broccoli is performing a <u>random walk</u> around the table: at each step the Broccoli will either move to the left or the right according to a coin toss.

<u>Questions</u>

- Will every guest hold the plate at some point?
- How long before everyone has held the plate?

It is not guaranteed that everyone will hold the Broccoli at some moment (as one may see Heads, Tails, Heads, Tails repeated indefinitely) but it is highly likely that after p^2 steps everyone will have seen the Broccoli.

We formalize this situation as a random walk on the group $\mathbb{Z}/(p)$ (or $\mathbb{Z}_p$) and will use harmonic analysis to determine optimal mixing times. Lets start by reviewing the group $\mathbb{Z}_p$ and some probability.

$\mathbb{Z}_p$

As a set $\mathbb{Z}_p$ is $\{0, \dots, p-1\}$. The binary operation $\oplus$ on $\mathbb{Z}_p$ we are interested in addition modulo p or

$$t \oplus s = \begin{cases} t+s & \text{if } 0 \leq t+s \leq p-1 \\ t+s-p & \text{if } t+s \geqslant p \end{cases}$$

more explicitly. The set $\mathbb{Z}_p$ with the binary operation $\oplus$ is a group. This means the operation $\oplus$ satisfies

Closure	$a \oplus b \in \mathbb{Z}_p$ for all $a, b \in \mathbb{Z}_p$
Associativity	$(a \oplus b) \oplus c = a \oplus (b \oplus c)$ for all $a, b, c \in \mathbb{Z}_p$
Identity	there is $e \in \mathbb{Z}_p$ with $e \oplus a = a = a \oplus e$ for all $a \in \mathbb{Z}_p$
Inverses	for all $a \in \mathbb{Z}_p$ there is $b \in \mathbb{Z}_p$ with $a \oplus b = e = b \oplus a$

There is also the fact that $\mathbb{Z}_p$ is Abelian.

Abelian	$a \oplus b = b \oplus a$ for all $a, b \in \mathbb{Z}_p$

The subgroups of $\mathbb{Z}_p$ are all generated by a single element.

Subgroups	$\{0\}$, $\langle t \rangle$ for all $t \mid p$, $\mathbb{Z}_p$

Random Walks

In a random walk one moves at each iteration from one's current position to a new location by choosing a ~~destination~~ movement at random. We formalize the notion of "at random" using a probability distribution: a device that tells us the likelihood of each of the possible ~~destinations~~ movements at every iteration. A probability distribution does not describe a mechanism for producing random ~~destination~~ movement but only the outcome likelihoods.

Probability Distributions

A <u>probability distribution</u> on $\mathbb{Z}_p$ is any function $\mu : \mathbb{Z}_p \to [0,1]$ satisfying

$$\sum_{t=0}^{p-1} \mu(t) = 1$$

From the point of view of random walks one thinks of $\mu(t)$ as the likelihood that ones destination will be $t \oplus$ current position.

Note that $\mu(t)$ is NOT the likelihood one will be at position t following the iteration.

Example The uniform distribution or Lebesgue distribution on $\mathbb{Z}_p$ is the function $\lambda(t) = \frac{1}{p}$ for all $t \in \mathbb{Z}_p$. We can check it is a probability distribution

$$\sum_{t \in \mathbb{Z}_p} \lambda(t) = \sum_{t=0}^{p-1} \frac{1}{p} = p \times \frac{1}{p} = 1 .$$

Example Fix $s \in \mathbb{Z}_p$. The singular distribution or Dirac distribution on $\mathbb{Z}_p$ at s is the function $\delta_s(t) = \begin{cases} 1 & t = s \\ 0 & t \neq s \end{cases}$ for all $t \in \mathbb{Z}_p$.

We can check it is a probability distribution

$$\sum_{t=0}^{p-1} \delta_s(t) = \delta_s(s) + \sum_{\substack{t=0 \\ t \neq s}}^{p-1} \delta_s(t) = \delta_s(s) + 0 = 1 .$$

Example The pass the Broccoli distribution on $\mathbb{Z}_p$ is the function

$$\mu(t) = \begin{cases} \frac{1}{2} & t = 1 \\ -\frac{1}{2} & t = -1 \\ 0 & \text{otherwise} \end{cases}$$

for all $t \in \mathbb{Z}_p$. From

$$\sum_{t=0}^{p-1} \mu(t) = \mu(1) + \mu(-1) = \tfrac{1}{2} + \tfrac{1}{2} = 1$$

it is a probability distribution.

If we are at location $u \in \mathbb{Z}_p$ and move to position $u \oplus t$ with t chosen at random, where will we end up? It depends on the distribution that "random" refers to:

δ_s	$u \oplus s$ with certainty
λ	all positions equally likely
μ	$u \oplus 1$ or $u \oplus (-1)$ both equally likely.

END

Events An <u>event</u> is any subset of $\mathbb{Z}_p$. The <u>probability of an event</u> $A \subset \mathbb{Z}_p$ given a probability distribution $\mu : \mathbb{Z}_p \to [0,1]$ is

$$\mu(A) = \sum_{t \in A} \mu(t)$$

if $A \neq \emptyset$ and we put $\mu(\emptyset) = 0$.

Event probabilities have the following properties.

Monotonicity $\mu(A) \leq \mu(B)$ whenever $A \subset B$

Additivity if $A_1, \dots, A_k$ are pairwise disjoint (i.e. $A_i \cap A_j = \emptyset$ for all $1 \leq i \neq j \leq k$) then $\mu(A_1 \cup \dots \cup A_k) = \mu(A_1) + \dots + \mu(A_k)$

Totality $\mu(\mathbb{Z}_p) = 1$

Integration Given a function $f : \mathbb{Z}_p \to \mathbb{C}$ its <u>integral</u> with respect to a probability distribution μ on $\mathbb{Z}_p$ is

$$\mu(f) = \sum_{t=0}^{p-1} f(t)\mu(t)$$

and is sometimes written $\int f \, d\mu$ or $\mathbb{E}_\mu(f)$.