We are now ready to be a bit more formal about random walks on $\mathbb{Z}_p$. Broadly speaking, in a random walk on $\mathbb{Z}_p$ one has a sequence $\mu_1, \mu_2, \mu_3, \ldots$ of probability distributions on $\mathbb{Z}_p$ and at each stage chooses a random element t_i of $\mathbb{Z}_p$ according to the distribution μ_i. One's location after n steps is $t_1 \oplus t_2 \oplus \cdots \oplus t_n$. This is a random location in $\mathbb{Z}_p$ and therefore corresponds to some distribution ν_n with $\nu_n(s)$ the probability that $t_1 \oplus t_2 \oplus \cdots \oplus t_n = s$.

Eg If $\mu_1 = \mu_2 = \frac{1}{2}(\delta_{-1} + \delta_1)$ what is ν_2?

Both t_1 and t_2 are either 1 or -1, so $t_1 \oplus t_2$ can be $-2, 0$ or 2.

Thus $\nu_2 = \frac{1}{4}\delta_{-2} \oplus \frac{1}{2}\delta_0 \oplus \frac{1}{4}\delta_2$. □

(Usually we will in this course have $\mu_1 = \mu_2 = \cdots = \mu_n$ choosing each step with the same distribution. In this case some things will be easier.) There is a particular way of calculating the distribution of ν_n using convolutions.

Convolutions

The convolution of probability distributions μ, ν on $\mathbb{Z}_p$ is the map $\mu * \nu : \mathbb{Z}_p \to \mathbb{R}$ defined by

$$(\mu * \nu)(t) = \sum_{s=0}^{p-1} \mu(t \ominus s)\nu(s)$$

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

Eg If $\mu = \frac{1}{2}\delta_{-1} + \frac{1}{2}\delta_1$ then what is $\mu * \mu$?

$$(\mu * \mu)(t) = \sum_{s=0}^{p-1} \mu(t \ominus s)\mu(s) = \frac{1}{2}\mu(t \ominus (-1)) + \frac{1}{2}\mu(t \ominus 1)$$

$$= \frac{1}{2}\left(\frac{1}{2}\delta_{-1}(t \ominus (-1)) + \frac{1}{2}\delta_{+1}(t \ominus (-1))\right)$$

$$+ \frac{1}{2}\left(\frac{1}{2}\delta_{-1}(t \ominus 1) + \frac{1}{2}\delta_1(t \ominus 1)\right)$$

$$= \frac{1}{4}\delta_{-2}(t) + \frac{1}{4}\delta_0(t) + \frac{1}{4}\delta_0(t) + \frac{1}{4}\delta_2(t)$$

so we get $\mu * \mu = \frac{1}{4}\delta_{-2} + \frac{1}{2}\delta_0 + \frac{1}{4}\delta_2$. □

At least in the example, it appears $\mu_1 * \mu_2$ is the distribution of $t_1 \oplus t_2$ when t_1 chosen randomly according to μ_1 and t_2 chosen randomly according to μ_2. This is no coincidence.

Probability of being at location t after two steps

$=$ Sum over probabilities of distinct paths $r \oplus s = t$

$=$ Sum over probabilities first step is $t \ominus s$ and second step is s

$=$ Sum over $0 \le s \le p-1$ that first step is $t-s$ and second is s

$= \sum_{s=0}^{p-1}$ Probability first step is $t \ominus s$ and second is s

$= \sum_{s=0}^{p-1} \mu_1(t \ominus s)\, \mu_2(s)$

$= (\mu_1 * \mu_2)(t)$

In the blue equality we have used <u>independence</u>: the fact that the first step does not affect the distribution of the second step.

Facts Here are some facts about convolutions.

Commutative	$\mu * \nu = \nu * \mu$
Associative	$(\mu * \nu) * \eta = \mu * (\nu * \eta)$
Linearity	$\mu * (\alpha\nu + \beta\eta) = \alpha\, \mu * \nu + \beta\, \mu * \nu$
Entropy	$\max\{H(\mu), H(\nu)\} \le H(\mu * \nu) \le H(\mu) + H(\nu)$
Identity	$\mu * \lambda = \lambda$
Shift	$(\delta_s * \mu)(t) = \mu(t \ominus s)$

The first three properties are algebraic. The first tells us about the uncertainty of a convolution: it is at least as uncertain as μ and ν

but cannot be of greater entropy than the sum of the entropies. We think of convolution as "smoothing out" the distributions involved: the result of the convolution of μ and ν will be smoother. One cannot make λ smoother by convolution because it is already as smooth as possible/maximises uncertainty.

Random Walks

Fix a distribution μ on $\mathbb{Z}_p$. If our steps are all randomly and independently chosen with distribution μ, what is the distibution of our location after n steps? By induction it is the n-fold convolution of μ. Define $\mu^{*n} = \mu^{*(n-1)} * \mu$ inductively. Thus

$$\mu^{*0} = \delta_0 \qquad \mu^{*1} = \mu \qquad \mu^{*2} = \mu * \mu \qquad \mu^{*3} = \mu * \mu * \mu$$

and so on, $\mu^{*0} = \delta_0$ being taken by convention because $\delta_0 * \eta = \eta$.

Eg If $\mu = \frac{1}{2}(\delta_{-1} + \delta_1)$ and the broccoli starts at position 0 then μ^{*n} is the distibution of the broccoli after n passes. □

Notation

In the notation and language of probability theory we write X_n for the position (random as it is) of the broccoli after n steps. The probability that $X_n = t$ (that the broccoli is with guest t after n steps) is then $\mu^{*n}(t)$. This is written $\mathbb{P}(X_n = t)$. For instance $\mathbb{P}(X_1 = t) = \mu(t)$ and $\mathbb{P}(X_2 = s) = (\mu * \mu)(s)$.

Return Probabilities

What is the probability that $X_1 = s$ and $X_n = t$?