Fix a probability distibution μ on $\mathbb{Z}_p$. If we use μ to drive a random walk on $\mathbb{Z}_p$ then the distibution after n steps is given by the n-fold convolution μ^{*n} of μ where

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

and $\mu^{*n} = \mu^{*n-1} * \mu$. What can we say about the long-term behaviour of the random walk i.e. the limit as $n \to \infty$ of μ^{*n}?

Limits

Let $n \mapsto \mu_n$ be a sequence of probability distributions on $\mathbb{Z}_p$. A probability distibution μ_∞ on $\mathbb{Z}_p$ is a limit of the sequence $\mu_1, \mu_2, \dots$ if

$$\lim_{n\to\infty} \mu_n(t) = \mu_\infty(t)$$

for all $t \in \mathbb{Z}_p$. The limit $\lim_{n\to\infty} \mu_n(t)$ is a limit of a sequence of numbers so makes sense in the usual way.

Theorem Let $\mu_1, \mu_2, \dots$ be a sequence of probability distibutions on $\mathbb{Z}_p$. A probability distibution μ_∞ is their limit if and only if $\lim_{n\to\infty} d(\mu_n, \mu_\infty) = 0$.

(Recall that

$$d(\mu,\nu) = \max\{|\mu(A) - \nu(A)| : A \subset \mathbb{Z}_p\} = \frac{1}{2}\sum_{t=0}^{p-1} |\mu(t) - \nu(t)|$$

for all distibutions μ, ν on $\mathbb{Z}_p$.)

Ergodicity

Roughly speaking, a distibution μ is ergodic if after many steps there is a fair chance that the current location is anywhere. Specifically, a distibution μ is ergodic if the sequence μ^{*n} converges to λ.

Our goal for the moment is a criterion for ergodicity in terms of μ alone.

<u>Eg</u> If $p=6$ and $\mu = \frac{1}{2}\delta_{-2} + \frac{1}{2}\delta_2$ is μ ergodic?

Solution: In $\mathbb{Z}_6$ we have $-2=4$. After one step the biccoli is either at location 2 or location 4. After two steps it is in one of locations 0, 2, 4. Since 6 is even and we take steps of even size, the biccoli can never be at positions 1, 3, 5. $\square$

<u>Eg</u> If $p=6$ and $\mu = \delta_1$ is μ ergodic?

Solution: At each step the biccoli is in a specific location (with guest n mod p at step n) so there is never a time at which everyone has a positive probability of having biccoli. $\square$

<u>Eg</u> If $p=6$ and $\mu = \frac{1}{2}\delta_1 + \frac{1}{2}\delta_3$ is μ ergodic?

Solution: After two steps the biccoli can be with guests $\{0,2,4\}$ only. After three steps it will be with guests $\{1,3,5\}$ only, and this pattern repeats. $\square$

Support

The <u>support</u> of a distribution $\mu : \mathbb{Z}_p \to [0,1]$ is the set

$$\mathrm{spt}(\mu) = \{ t \in \mathbb{Z}_p : \mu(t) > 0 \}$$

of outcomes that μ does not consider impossible. In particular, the support of μ^{*n} is the set of guests who have a non-zero probability of being the biccoli holder after n passes. If $\mu^{*n} \longrightarrow \lambda$ then there must in particular be some $n \in \mathbb{N}$ with ~~supp~~ $\mathrm{spt}(\mu^{*n}) = \mathbb{Z}_p$. What is the support of μ^{*n} and when does μ have the property that $\mathrm{spt}(\mu^{*n}) = \mathbb{Z}_p$ for some $n \in \mathbb{N}$?

<u>Theorem</u> Let μ, ν be probability distributions on $\mathbb{Z}_p$. Then $t \in spt(\mu * \nu)$ if and only if

Proof:
$$
\begin{gathered}
t \in spt(\mu * \nu) \\
\Updownarrow \\
(\mu * \nu)(t) > 0 \\
\Updownarrow \\
\sum_{s=0}^{p-1} \mu(t \ominus s)\nu(s) > 0 \\
\Updownarrow \\
\exists s \in \mathbb{Z}_p : \mu(t \ominus s) > 0 \text{ and } \nu(s) > 0 \\
\Updownarrow \\
\exists s \in \mathbb{Z}_p : t \ominus s \in spt(\mu) \text{ and } s \in spt(\nu) \\
\Updownarrow \\
t \in spt(\mu) \oplus spt(\nu)
\end{gathered}
$$
$\square$

Here $spt(\mu) \oplus spt(\nu) = \{a+b : a \in spt(\mu) \text{ and } b \in spt(\nu)\}$. Thus $spt(\mu) \oplus spt(\nu)$ is the support of $\mu * \nu$. Define, for any $A \subset \mathbb{Z}_p$ the set $A^{\oplus n} = A^{\oplus n-1} \oplus A$ so that $A^{\oplus 2} = A \oplus A$, $A^{\oplus 3} = A \oplus A \oplus A$ etc. By induction the support of μ^{*n} is $spt(\mu)^{\oplus n}$. If μ is to be ergodic then $spt(\mu)^{\oplus n} = \mathbb{Z}_p$ must hold for some (and therefore all subsequent) $n \in \mathbb{N}$.

<u>Lemma</u> If $spt(\mu) \subset \Gamma \oplus \alpha$ for some $\Gamma < \mathbb{Z}_p$ proper and some $\alpha \in \mathbb{Z}_p$ then $spt(\mu)^{\oplus n}$ is never $\mathbb{Z}_p$.

Proof: $(\Gamma \oplus \alpha) \oplus (\Gamma \oplus \beta) = \Gamma \oplus (\alpha \oplus \beta)$. $\square$

This explains all of the earlier examples succinctly.

It turns out that the converse is true as well!

<u>Lemma</u> If $A \subset \mathbb{Z}_p$ is not contained in a coset of a proper subgroup of $\mathbb{Z}_p$ then there is $n \in \mathbb{N}$ with $A^{\oplus n} = \mathbb{Z}_p$.

Proof: The idea is to deduce that $|A^{\oplus n}|$ is strictly increasing, so that at some point $A^{\oplus n}$ must have cardinality p and equal $\mathbb{Z}_p$.

We begin with the following fact.

Fact: If $A, B \subset \mathbb{Z}_p$ are both non-empty and $|A| = |A \oplus B| = |B|$ then A, B are both cosets of the same subgroup $\Gamma < \mathbb{Z}_p$.

Proof: Fix $t \in A$ and $s \in B$. Put $A' = A \ominus t$ and $B' = B \ominus s$. (If A and B are cosets of some Γ then A' and B' would have to be Γ.) Lets prove A' and B' are the same subgroup. Since $0 \in A'$ and $0 \in B'$ we have $A' \subset A' \oplus B'$ and $B' \subset A' \oplus B'$. But our cardinality assumption then gives $|A'| = |A' \oplus B'| = |B'|$ so that $A' = A' \oplus B' = B'$. Thus

$$A' \oplus A' = A' \oplus B' = A' \qquad B' \oplus B' = A' \oplus B' = B'$$

so A', B' are both subgroups, and equal. Certainly A and B are both cosets of that subgroup. $\square$

Now suppose A is not contained in a ~~proper~~ coset of a proper subgroup of $\mathbb{Z}_p$. Then $|A| < |A \oplus A|$. We cannot have $A \oplus A$ contained in a coset of a proper subgroup of $\mathbb{Z}_p$ as otherwise A would be too. If $A \oplus A = \mathbb{Z}_p$ we are done. Otherwise the Fact gives $|A \oplus A \oplus A| > |A \oplus A|$. Repeating at most p times, eventually $A^{\oplus n} = \mathbb{Z}_p$. $\square$

The two lemmas together prove the following theorem.

<u>Theorem</u> Fix a distribution μ on $\mathbb{Z}_p$. The support $\mathrm{spt}(\mu)$ is not contained in a ~~proper subgr~~ coset of a proper subgroup of $\mathbb{Z}_p$ if and only if there is $n \in \mathbb{N}$ with $\mathrm{spt}(\mu^{*n}) = \mathbb{Z}_p$.