Analysis, Random Walks and Groups

Exercise sheet 2: solutions

January 30, 2023

These model solutions are the same models used by Tuomas in Manchester, but some exercises are omitted, attached into another exercises or separeted into separate exercises. I (Kai) might have commented somewhere with red color if I think it is in place. Corrections and improvements are welcome.

Homework exercises: Return these for marking to Kai Hippi in the tutorial on Week 3. Contact Kai by email if you cannot return these in-person, and you can arrange an alternative way to return your solutions. Remember to be clear in your solutions, if the solution is unclear and difficult to read, you can lose marks. Also, if you do not know how to solve the exercise, attempt something, you can get awarded partial marks.

1. (5pts)

Let $\mu_\alpha = \alpha\delta_0 + (1-\alpha)\delta_1$ on $\mathbb{Z}_5$ for some $0 < \alpha \leq 1$. For which α is μ_α ergodic? Explain your answer. Compute $d(\mu_\alpha * \mu_\alpha, \lambda)$ as a function of α.

Solution 1.

If $\alpha = 1$, the support of μ_α is $\{0\}$, which is a trivial subgroup of $\mathbb{Z}_p$, in particular by the subgroup characterisation of ergodicity $\mu_\alpha = \delta_0$ cannot be ergodic.

If $\alpha < 1$, the support of μ_α is $\{0,1\}$. Since 5 is a prime number, the only subgroups of $\mathbb{Z}_5$ are $\{0\}$ and $\mathbb{Z}_5$ and so $\{0,1\}$ cannot be a coset of any of these subgroups. Hence by the subgroup characterisation μ_α is ergodic.

The convolution

$$\mu_\alpha * \mu_\alpha(t) = \sum_{s \in \mathbb{Z}_p} \mu_\alpha(t \ominus s)\mu_\alpha(s) = \alpha\mu_\alpha(t) + (1-\alpha)\mu_\alpha(t \ominus 1).$$

We have $t \ominus 1 = 0$ when $t = 1$ and $t \ominus 1 = 1$ when $t = 2$. Thus we have

$$\mu_\alpha(t \ominus 1) = \alpha\delta_0(t \ominus 1) + (1-\alpha)\delta_1(t \ominus 1) = \alpha\delta_1(t) + (1-\alpha)\delta_2(t).$$

Hence the convolution

$$\mu_\alpha * \mu_\alpha(t) = \alpha[\alpha\delta_0(t) + (1-\alpha)\delta_1(t)] + (1-\alpha)[\alpha\delta_1(t) + (1-\alpha)\delta_2(t)],$$

which equals to

$$\alpha^2\delta_0(t) + 2\alpha(1-\alpha)\delta_1(t) + (1-\alpha)^2\delta_2(t).$$

By the L^1 identity for the total variation distance we have

$$d(\mu_\alpha * \mu_\alpha, \lambda) = \frac{1}{2}\sum_{t\in\mathbb{Z}_p} |\mu_\alpha * \mu_\alpha(t) - \lambda(t)|,$$

which, since $\mu_\alpha * \mu_\alpha(t) = 0$ when $t \neq 0$ and when $t = 1$ we have

$$\frac{|\alpha^2 - 1/5| + |2\alpha(1-\alpha) - 1/5| + |(1-\alpha)^2 - 1/5| + 2/5}{2},$$

which is our function of α.

2. (5pts)

Prove that if $\mu, \nu : \mathbb{Z}_p \to [0,1]$ are probability distributions, then the entropy

$$H(\mu * \nu) \leq H(\mu) + H(\nu).$$

Hint: Use the convexity of $\varphi(x) = -x\,log(x)$ (you do not need to prove the convexity).

Solution 2.

Convexity (Here should be concavity, you may just without a proof here that it gives subadditivity) of $\varphi(x) = -x\log x$ gives the **subadditivity** of φ:

$$\varphi(\sum_j x_j) \leq \sum_j \varphi(x_j)$$

for all finite sums of $x_j \geq 0$. We have by the definition of entropy and convolution that

$$\begin{aligned}
H(\mu * \nu) &= -\sum_{t\in\mathbb{Z}_p} \mu * \nu(t)\log \mu * \nu(t)\\
&= \sum_{t\in\mathbb{Z}_p} -\Big[\sum_{r\in\mathbb{Z}_p} \mu(t \ominus r)\nu(r)\Big]\log\Big[\sum_{s\in\mathbb{Z}_p} \mu(t\ominus s)\nu(s)\Big]\\
&= \sum_{t\in\mathbb{Z}_p} \varphi\Big(\sum_{r\in\mathbb{Z}_p} \mu(t\ominus r)\nu(r)\Big)\\
&\leq \sum_{t\in\mathbb{Z}_p}\sum_{r\in\mathbb{Z}_p} \varphi(\mu(t\ominus r)\nu(r))\\
&= \sum_{t,r\in\mathbb{Z}_p} -\mu(t\ominus r)\nu(r)\log(\mu(t\ominus r)\nu(r)).
\end{aligned}$$

Here

$$-\mu(t\ominus r)\nu(r)\log(\mu(t\ominus r)\nu(r)) = -\mu(t\ominus r)\nu(r)\log\mu(t\ominus r) - \mu(t\ominus r)\nu(r)\log\nu(r).$$

Thus

$$\sum_{t,r\in\mathbb{Z}_p} -\mu(t\ominus r)\nu(r)\log(\mu(t\ominus r)\nu(r)) = -\sum_{t,r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\mu(t\ominus r) - \sum_{t,r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\nu(r).$$

In the first sum on the right hand side, for any fixed $t \in \mathbb{Z}_p$, use change of variable $r \mapsto t \ominus r$, that is, set $u = t \ominus r$, which makes $r = t \ominus u$. Thus

$$\begin{aligned} -\sum_{t\in\mathbb{Z}_p}\sum_{r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\mu(t\ominus r) &= -\sum_{t\in\mathbb{Z}_p}\sum_{u\in\mathbb{Z}_p}\mu(u)\nu(t\ominus u)\log\mu(u) \\ &= -\sum_{u\in\mathbb{Z}_p}\mu(u)\log\mu(u)\sum_{t\in\mathbb{Z}_p}\nu(t\ominus u) \end{aligned}$$

Moreover, as ν is a probability distribution, we have, for every $t \in \mathbb{Z}_p$, that $\sum_{t\in\mathbb{Z}_p}\nu(t\ominus u) = 1$. Hence

$$-\sum_{u\in\mathbb{Z}_p}\mu(u)\log\mu(u)\sum_{t\in\mathbb{Z}_p}\nu(t\ominus u) = -\sum_{u\in\mathbb{Z}_p}\mu(u)\log\mu(u) = H(\mu).$$

Similarly

$$-\sum_{t,r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\nu(r) = -\sum_{r\in\mathbb{Z}_p}\nu(r)\log\nu(r)\sum_{t\in\mathbb{Z}_p}\mu(t\ominus r) = H(\nu).$$

Hence we have

$$-\sum_{t,r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\mu(t\ominus r) - \sum_{t,r\in\mathbb{Z}_p}\mu(t\ominus r)\nu(r)\log\nu(r) = H(\mu) + H(\nu),$$

which gives the claim.

Further exercises: Attempt these before the tutorial, they are not marked and will be discussed in the tutorial. If you cannot attend the tutorial, but want to do the attendance marks, you can return your attempts to these before the tutorial to Kai. Here Kai will not mark the further exercises, but will look if an attempt has been made and awards the attendance mark for that week's tutorial.

3.

Prove the following identities for the convolution: for all $f, g, h : \mathbb{Z}_p \to \mathbb{C}$ we have:

(a) **Commutativity:** $f * g = g * f$

(b) **Associativity:** $f * (g * h) = (f * g) * h$

(c) **Linearity:** if $\alpha, \beta \in \mathbb{C}$, then $f * (\alpha g + \beta h) = \alpha f * g + \beta f * h$

Solution 3.a

For every $t \in \mathbb{Z}_p$, the map $s \mapsto t \ominus s$ is a bijection $\mathbb{Z}_p \to \mathbb{Z}_p$. Thus

$$f*g(t) = \sum_{s\in\mathbb{Z}_p} f(t\ominus s)g(s) = \sum_{s\in\mathbb{Z}_p} f(t\ominus(t\ominus s))g(t\ominus s) = \sum_{s\in\mathbb{Z}_p} f(s)g(t\ominus s) = g*f(t).$$

Solution 3.b

We have

$$\begin{aligned}
[f*(g*h)](t) &= \sum_{s\in\mathbb{Z}_p} f(t\ominus s)(g*h)(s) \\
&= \sum_{s\in\mathbb{Z}_p} f(t\ominus s) \sum_{r\in\mathbb{Z}_p} g(s\ominus r)h(r) \\
&= \sum_{r\in\mathbb{Z}_p} h(r) \sum_{s\in\mathbb{Z}_p} f(t\ominus s)g(s\ominus r)
\end{aligned}$$

Given $r \in \mathbb{Z}_p$, by the change of variable $v = s \ominus r$, we have

$$t \ominus s = (t\ominus r)\ominus(s\ominus r) = (t\ominus r)\ominus v$$

so

$$\sum_{s\in\mathbb{Z}_p} f(t\ominus s)g(s\ominus r) = \sum_{v\in\mathbb{Z}_p} f((t\ominus r)\ominus v)g(v) = f*g(t\ominus r).$$

Thus

$$\sum_{r\in\mathbb{Z}_p} h(r) \sum_{s\in\mathbb{Z}_p} f(t\ominus s)g(s\ominus r) = \sum_{r\in\mathbb{Z}_p} f*g(t\ominus r)h(r) = [(f*g)*h](t).$$

Solution 3.c

We have

$$\begin{aligned}
[f*(\alpha g+\beta h)](t) &= \sum_{s\in\mathbb{Z}_p} f(t\ominus s)(\alpha g+\beta h)(s) \\
&= \alpha \sum_{s\in\mathbb{Z}_p} f(t\ominus s)g(s) + \beta \sum_{s\in\mathbb{Z}_p} f(t\ominus s)h(s) \\
&= \alpha f*g(t) + \beta f*h(t) \\
&= [\alpha f*g+\beta f*h](t).
\end{aligned}$$

4.

Let μ be a probability distribution on $\mathbb{Z}_4$, which is not a Dirac mass, and assume that the support

$$spt(\mu) = \{t \in \mathbb{Z}_4 \, : \, \mu(t) > 0\}$$

is a coset of a proper non-trivial subgroup of $\mathbb{Z}_4$. Is there a limit

$$\mu_\infty = \lim_{n \to \infty} \mu^{*n}?$$

What is it? No proofs necessary, just have a think how to maybe prove this.

Solution 4.

The only proper subgroup of $\mathbb{Z}_4$ is $\Gamma = \{0, 2\}$. The only coset of this is $\Gamma \oplus 1 = \{1, 3\}$. If we consider first the case μ is concentrated on Γ, as μ is not a Dirac mass, then μ^{*n} can only have a limit

$$\nu = \frac{1}{2}\delta_0 + \frac{1}{2}\delta_2$$

that is, ν is the uniform measure on the subgroup Γ

Formal proof: If μ is concentrated on Γ, then we could identify Γ with $\mathbb{Z}_2$ as follows. First of all, group theoretically Γ is **isomorphic** to $\mathbb{Z}_2$, that is there exists a bijection $\varphi : \mathbb{Z}_2 \to \Gamma$ such that $\varphi(a \oplus b) = \varphi(a) \oplus \varphi(b)$, $a, b, \in \mathbb{Z}_2$. Then

$$\nu = \varphi_* \lambda,$$

where λ is the uniform measure on $\mathbb{Z}_2$ and $\varphi_* \lambda$ is the **push forward distribution** (recall earlier exercises on Wasserstein distance), which is defined by

$$\varphi_* \lambda(A) = \lambda(\varphi^{-1} A), \quad A \subset \Gamma.$$

Since the push forward under inverse φ^{-1} of μ, that is, $\varphi_*^{-1}\mu$ is ergodic (it is not concentrated on any proper subgroup of $\mathbb{Z}_2$ as it is not a Dirac mass), the iterated convolutions

$$(\varphi_*^{-1}\mu)^{*n} \to \lambda$$

as $n \to \infty$ in $\mathbb{Z}_2$ by the subgroup characterisation of ergodicity. Since $\lambda = \varphi_*^{-1}\nu$, this gives that $\mu^{*n} \to \nu$ in Γ so the limit $\mu_\infty = \nu$.

As for the coset $\Gamma \oplus 1$ we have an issue: if μ is supported on $\Gamma \oplus 1 = \{1, 3\}$ the support

$$\mathrm{spt}(\mu * \mu) = \mathrm{spt}(\mu) \oplus \mathrm{spt}(\mu) = \{1, 3\} \oplus \{1, 3\} = \{0, 2\}$$

On on the other hand

$$\mathrm{spt}(\mu * \mu * \mu) = \mathrm{spt}(\mu) \oplus \mathrm{spt}(\mu) \oplus \mathrm{spt}(\mu) = \{1, 3\} \oplus \{1, 3\} \oplus \{1, 3\} = \{0, 2\} \oplus \{1, 3\} = \{1, 3\}$$

and again

$$\mathrm{spt}(\mu * \mu * \mu * \mu) = \{1, 3\} \oplus \{1, 3\} = \{0, 2\}$$

so the support of μ^{*n} alternates between $\{0,2\}$ and $\{1,3\}$, which are disjoint. In particular for even n and odd n we get measures μ^{*n} that have never the same support. Thus it is impossible for μ^{*n} to have a limit as $n \to \infty$.

5.

(a) Prove that for all $A, B \subset \mathbb{Z}_p$ the cardinalities

$$\max\{|A|,|B|\} \leq |A \oplus B| \leq |A||B|.$$

(b) Give examples of sets $A, B \subset \mathbb{Z}_p$ such that

$$|A \oplus B| = \max\{|A|,|B|\}.$$

(c) Give examples of sets $A, B \subset \mathbb{Z}_p$ which are not $\mathbb{Z}_p$ such that

$$|A \oplus B| = |A||B|.$$

Solution 5.a

Define a function $P : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$,

$$P(t,s) = t \oplus s.$$

Then

$$A \oplus B = P(A \times B)$$

so as P is a function we have

$$|P(A \times B)| \leq |A \times B| = |A||B|.$$

To the other direction, if $t \in A$, then the map $s \mapsto t \oplus s$, $s \in B$, is an injection $B \mapsto A \oplus B$. Hence

$$|B| \leq |A \oplus B|.$$

Similarly

$$|A| \leq |A \oplus B|$$

so the claim follows.

Solution 5.b

We can set $A = \{0\}$ and $B = \{1\}$. Then $A \oplus B = \{1\}$ so $|A \oplus B| = 1 = |B| = |A|$. A harder example could be if $p = 4$ and

$$A = \{0,2\} = B.$$

Then

$$A \oplus B = \{0,2\} = A = B$$

so

$$|A \oplus B| = |A| = |B|.$$

Solution 5.c

We can set $A = \{0\}$ and $B = \{1\}$. Then $A \oplus B = \{1\}$ so $|A \oplus B| = 1 = 1 \times 1 = |A||B|$.