Analysis, Random Walks and Groups
Spring 2019

Week 5 tutorial

1. Let $p \geq 7$. For $0 < \alpha < 1$ define

$$\mu = \alpha\delta_1 + (1-\alpha)\delta_{-1}.$$

Compute the convolutions $\mu * \mu$ and $\mu * \mu * \mu$.

Solution. We have

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

and we have

$$\mu(t \oplus 1) = \alpha\delta_0(t) + (1-\alpha)\delta_{-2}(t)$$
$$\mu(t \ominus 1) = \alpha\delta_2(t) + (1-\alpha)\delta_0(t)$$

so

$$\begin{aligned}\mu * \mu(t) &= \alpha(\alpha\delta_0(t) + (1-\alpha)\delta_{-2}(t)) + (1-\alpha)\alpha\delta_2(t) + (1-\alpha)\delta_0(t),\\ &= \alpha(1-\alpha)\delta_{-2}(t) + (\alpha^2 + (1-\alpha)^2)\delta_0(t) + \alpha(1-\alpha)\delta_2(t).\end{aligned}$$

Moreover,

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

Here

$$\mu * \mu(t \ominus 1) = \alpha(1-\alpha)\delta_{-1}(t) + (\alpha^2 + (1-\alpha)^2)\delta_1(t) + \alpha(1-\alpha)\delta_3(t)$$

and

$$\mu * \mu(t \oplus 1) = \alpha(1-\alpha)\delta_{-3}(t) + (\alpha^2 + (1-\alpha)^2)\delta_{-1}(t) + \alpha(1-\alpha)\delta_1(t),$$

which gives

$$\begin{aligned}\mu * \mu * \mu = \quad &\alpha(1-\alpha)^2\delta_{-3} + [\alpha^2(1-\alpha) + (1-\alpha)(\alpha^2 + (1-\alpha)^2)]\delta_{-1}\\ &+ [\alpha(\alpha^2 + (1-\alpha)^2) + \alpha(1-\alpha)^2]\delta_1 + \alpha^2(1-\alpha)\delta_3.\end{aligned}$$

2. 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. (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

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

(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

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

(c) We have

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

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

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

(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. (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

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

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

$$|B|\le |A\oplus B|.$$

Similarly

$$|A|\le |A\oplus B|$$

so the claim follows.

(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

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

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

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

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

Hint: Use the convexity of $\varphi(x) = -x\log x$.

Solution. Convexity of $\varphi(x) = -x\log x$ gives the **subadditivity** of φ:

$$\varphi(\sum_j x_j)\le \sum_j \varphi(x_j)$$

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.