The Kaimanovich – Vershik Lemma

The Kaimanovich - Vershik Lemma plays the equivalent role of the Plünnecke - Ruzsa inequality in the proof of Freiman's thm

Plünnecke - Ruzsa

If $A, B \subset \mathbb{Z}$, $\#(A+B) \leq C \cdot \#A$
then $\exists A_0 \subset A$ s.t. $\#A_0 \geq \#A$ s.t.

$$|A_0 + B^{\oplus k}| \leq C^k \cdot \#A$$

Lemma: Let Γ be a countable abelian group, and let $\mu, \nu \in \mathcal{P}(\Gamma)$ be probability measures w/ $H(\mu), H(\nu) < \infty$.
Let

$$\delta_k = H(\mu * (\nu^{*(k+1)})) - H(\mu * (\nu^{*k})).$$

Then δ_k is nonincreasing in k. In particular,

$$H(\mu * (\nu^{*k})) \leq H(\mu) + k(H(\mu * \nu) - H(\mu))$$

Def:

Let X_0 be a random variable distributed according to μ.

Let $\{ Z_j \mid j = 1, \dots, n \}$ be a set of pairwise independent and X_0-independent random variables with distribution ν.

Let $X_n := X_0 + Z_1 + Z_2 + \cdots + Z_n$.

X_n is distributed according to $\mu * (\nu^{*n})$

$$H(X_n \mid Z_1) = \sum_{p \in \Gamma} \nu(Z_1 = p)\, H(X_{n-1} + p)$$

Since Γ is abelian, $H(X_{n-1} + p) = H(X_{n-1})$

$$\Rightarrow \quad H(X_n \mid Z_1) = H(X_{n-1})$$

Now

$$H(Z_1 \mid X_n) = H(Z_1, X_n) - H(X_n)$$

$$= H(Z_1) + H(X_n \mid Z_1) - H(X_n)$$

$$= H(\nu) + H(\mu * \nu^{*(n-1)}) - H(\mu * \nu^{*n})$$

Note test

$$H(Z_1 \mid X_n, X_{n+1})$$

$$= \sum_{p_1, p_2} \mathbb{P}(X_n = p_1, X_{n+1} = p_2)\, H(Z_1 \mid X_n = p_1, Z_{n+1} = p_2 - p_1)$$

$$= \sum_{p_1, p_2} \mu(Z_{n+1} = p_2)\, \mathbb{P}(X_n = p_1)\, H(Z_1 \mid X_n = p_1, Z_{n+1} = p_2)$$

$$= \sum_{p_1} \mathbb{P}(X_n = p_1) \sum_{p_2} \mu(Z_{n+1} = p_2)\, H((Z_1 \mid X_n = p_1) \mid Z_{n+1} = p_2)$$

$$= \sum_{p_1} \mathbb{P}(X_n = p_1)\, H((Z_1 \mid X_n = p_1) \mid Z_{n+1})$$

$$= \sum_{p_1} \mathbb{P}(X_n = p_1) \Big(H((Z_1 \mid X_n = p_1), Z_{n+1}) - H(Z_{n+1}) \Big)$$

independence

$$= \sum_{p_1} \mathbb{P}(X_n = p_1) \Big(H(Z_1 \mid X_n = p_1) + H(Z_{n+1}) - H(Z_{n+1}) \Big)$$

$$= \sum_{p_1} \mathbb{P}(X_n = p_1)\, H(Z_1 \mid X_n = p_1)$$

$$= H(Z_1 \mid X_n)$$

On the other hand, for any X, Y, Z, $H(X|Y,Z) \leq H(X|Y)$.

thus,

$$H(Z_1 | X_n, X_{n+1}) \leq H(Z_1 | X_{n+1}).$$

Therefore,

$$H(Z_2 | X_n) \leq H(Z_2 | X_{n+1})$$

$\Rightarrow$

$$H(\nu) + H(\mu * \nu^{*(n-1)}) - H(\mu * \nu^{*n})$$

$$\leq H(\nu) + H(\mu * \nu^{*n}) - H(\mu * \nu^{*(n+1)})$$

$\Leftrightarrow$ $H(\nu) - \delta_{n-1} \leq H(\nu) - \delta_n$

and $\delta_n \leq \delta_{n-1}$

$\square$.

By discretizing, we get

Prop: Let $\mu, \nu \in \mathcal{P}(\mathbb{R})$, $H_n(\mu), H_n(\nu) < \infty$.

Then

$$H_n(\mu * (\nu^{*k})) \leq H_n(\mu) + k \cdot \left(H_n(\mu * \nu) - H_n(\mu)\right) + O\left(\frac{k}{n}\right).$$

Simple Observation

Let $\mu, \nu \in \mathcal{P}([0,1])$, $H_m(\mu) < \infty$, $H_m(\nu) < \infty$

then

$$H_m(\mu * \nu)$$

$$= H_m\left(\int \mu * \delta_y \, d\nu(y)\right)$$

$$\geq \int H_m(\mu * \delta_y) \, d\nu(y)$$

$$|H_m(\mu * \delta_y) - H_m(\mu)| \leq 1$$

Thus

$$H(\mu * \nu) \geq \int H_m(\mu) \, d\nu(y) - O\left(\tfrac{1}{m}\right)$$

$$\Rightarrow H(\mu * \nu) \geq H_m(\mu) - O\left(\tfrac{1}{m}\right)$$

The Proof of The Inverse Theorem.

Recall the statement (simplified)

$\forall \varepsilon > 0,\ m \geq 2 \quad \exists\ \delta = \delta(\varepsilon, m)$ s.t.

$\forall n \geq n_0(\varepsilon, m, \delta)$

IF $\quad \nu, \mu \in \mathcal{P}([0,1])$

then either

1. $H_n(\mu * \nu) > H_n(\mu) + \delta$

or 2. $\exists\ I, J \subset \{0, \dots, n\}$, $\#(I \cup J) \geq (1-\varepsilon)n$

s.t.

$\mathbb{P}_{i=k}\left(\mu^{x,i} \text{ is } (\varepsilon, m)\text{-uniform}\right) > 1-\varepsilon \quad \forall k \in I$

$\mathbb{P}_{i=k}\left(\nu^{x,i} \text{ is } (\varepsilon, m)\text{-uniform}\right) > 1-\varepsilon \quad \forall k \in J.$

Now let $\quad \mu, \nu \in \mathcal{P}([0,1])$,

and let $\quad k = k(m, \varepsilon)$ be large enough so that our previous repeated convolution theorem concludes that if $\tau = \nu^{*k}$

then for n large enough, $\exists I, J \subset \{0, \dots, n\}$

s.t. $\#(I \cup J) > (1-\varepsilon/2)n$.

$$\mathbb{P}_{i=k}\left(\tau^{x,i} \text{ is } (\tfrac{\varepsilon}{2}, m)\text{-uniform}\right) > 1 - \varepsilon/2 \quad , k \in I$$

and

$$\mathbb{P}_{i=k}\left(\nu^{x,i} \text{ is } (\varepsilon, m)\text{-atomic}\right) > 1 - \varepsilon/2 \quad , k \in J.$$

Let $I_0 \subset I$ denote the set of $k \in I$

such that

$$\mathbb{P}_{i=k}\left(\mu^{x,i} \text{ is } (\varepsilon, m)\text{-uniform}\right) > 1 - \varepsilon$$

IF $\# I_0 > \# I - \frac{\varepsilon}{2} n$

then we are done: For almost every index, $k \in \{0, \dots, n\}$, either $\nu^{x,i}$ is atomic or $\mu^{x,i}$ is uniform.

We proceed by showing that the

condition $\#(I_0) < \# I - \frac{\varepsilon}{2} n$

violates the inverse along with

$H_n(\mu * \nu) < H_n(\mu) + \delta$ contradicts

the Kaĭmanovich - Vershik Lemma.

Suppose $\# I_0 < \# I - \varepsilon/2\, n$, let $I_1 = I \setminus I_0$

$\Rightarrow \quad \# I_1 > \frac{\varepsilon}{2} n$

Now, by definition, $k \in I_1$ implies

$\mathbb{P}_{i=k}(\tau^{x,i}$ is $(\varepsilon/2, m)$-uniform$) > 1 - \varepsilon/2$

and

$\mathbb{P}_{i=k}(\mu^{x,i}$ is (ε, m)-uniform$) \leq 1 - \varepsilon$.

$\Rightarrow \quad k \in I_1$ implies

$\mathbb{P}_{i=k}(\mu^{x,i}$ is not (ε, m)-uniform$) \geq \varepsilon$

Let x, y be such that

$\mu^{x,i}$ is not (ε, m)-uniform and

$\tau^{y,i}$ is $(\varepsilon/2, m)$-uniform.

then

$$H_m(\tau^{y,i}) > 1 - \varepsilon/2 \geq H_m(\mu^{x,i}) + \varepsilon/2$$

__Note:__

$$\mathbb{P}_{i=j}\left(\tau^{y,i}\in A,\ \mu^{x,i}\in B\right)=\mathbb{P}_{i=j}\left(\tau^{x,i}\in A\right)\mathbb{P}_{i=j}\left(\mu^{x,i}\in B\right)$$

The note implies

$$\mathbb{P}_{i=j}\left(H_m(\tau^{y,i})>1-\varepsilon/2 \text{ and } H_m(\mu^{x,i})<1-\varepsilon\right)>\varepsilon/2.$$

Now for x,y satisfying this condition,

$$H_m(\mu^{x,i}*\nu^{y,i})$$
$$\geq H_m(\mu^{x,i})+\frac{\varepsilon}{2}-O\left(\frac{1}{m}\right)$$

Now we use local-global entropy to conclude:

$$H_n(\mu*\tau)=\mathbb{E}_{0\leq i\leq n}\left(H_m(\mu^{x,i}*\nu^{y,i})\right)+O\left(\frac{m}{n}\right)$$

$$=\frac{\# I_2}{n+1}\mathbb{E}_{i\in I_2}\left(H_m(\mu^{x,i}*\tau^{y,i})\right)$$
$$+\frac{n+1-\# I_2}{n+1}\mathbb{E}_{i\in I_2^c}\left(H_m(\mu^{x,i}*\tau^{y,i})\right)$$
$$+O\left(\frac{1}{m}+\frac{m}{n}\right)$$

$$> \frac{\# I_2}{n+1} \left(\mathbb{E}_{i \in I_2}\left(H_m(\mu^{x,i})\right) + \left(\frac{\varepsilon}{2}\right)^2 \right)$$

$> \varepsilon/2\, n$

$$+ \frac{n+1 - \# I_2}{n+1} \mathbb{E}_{i \in I_2^c}\left(H_m(\mu^{x,i})\right) + O\left(\tfrac{1}{m} + \tfrac{m}{n}\right)$$

$$> \mathbb{E}_{0 \le i \le n}\left[H_m(\mu^{x,i})\right] + \left(\frac{\varepsilon}{2}\right)^3 + O\left(\tfrac{1}{m} + \tfrac{m}{n}\right).$$

$$= H_n(\mu) + \left(\frac{\varepsilon}{2}\right)^3 + O\left(\tfrac{1}{m} + \tfrac{m}{n}\right)$$

$\ast$ for n and m large enough,

$$H_n(\mu * \tau) > H_n(\mu) + \frac{\varepsilon^3}{10}$$

By Kaimanovich–Vershik,

$$H_n(\mu * \tau) \le H_n(\mu) + K\left(H_n(\mu * \nu) - H_n(\mu)\right) + O\left(\tfrac{K}{n}\right).$$

$$\Rightarrow \quad H_n(\mu * \nu) - H_n(\mu) > \frac{\varepsilon^3}{10K}.$$

If $\delta = \varepsilon^3/100K$ we are done modulo some extra conditions on m that one could remove B.

Important Corollary

Cor A: For every $\varepsilon > 0$ and $m \in \mathbb{Z}_+$, $\exists\, \delta = \delta(\varepsilon, m)$ s.t. $\forall n > n_0(\varepsilon, \delta, m)$ and every $\mu \in \mathcal{P}([0,1])$, if

$$\mathbb{P}_{0 \le i \le n}\left(H_m(\mu^{x,i}) < 1 - \varepsilon \right) > 1 - \varepsilon$$

then for every $\nu \in \mathcal{P}([0,1])$,

$$H_n(\nu) > \varepsilon \implies H_n(\mu * \nu) \ge H_n(\mu) + \delta.$$

An Interesting Corollary

Cor: For every measure $\mu \in \mathcal{P}(\mathbb{R})$ with uniform entropy dimension $0 < \alpha < 1$, and for every $\varepsilon > 0$, there is a $\delta > 0$ and such that for all large enough n and every $\nu \in \mathcal{P}([0,1])$

$$H_n(\nu) > \varepsilon \implies H_n(\mu * \nu) \ge H_n(\mu) + \delta.$$