Probability distributions convoluted by quasigroups

Alexey Yashunsky

Keldysh Institute of Applied Mathematics, RAS
Moscow, Russia

Loops'11, July 25–27

Probabilities on quasigroups

Let Q be a *finite binary quasigroup* with multiplication $a \cdot b$, and $a \backslash b$, b/a — the corresponding left and right divisions.

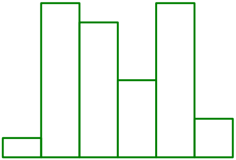
Probabilities on quasigroups

Let Q be a *finite binary quasigroup* with multiplication $a \cdot b$, and $a \backslash b$, b/a — the corresponding left and right divisions.

$$Q = \{1, \ldots, q\}$$

$$u = (u_1, u_2, \ldots, u_q), \quad u_i \geqslant 0$$

$$u_1 + u_2 + \ldots + u_q = 1$$



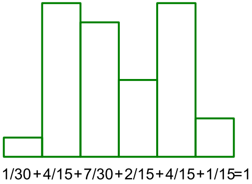
Probabilities on quasigroups

Let Q be a *finite binary quasigroup* with multiplication $a \cdot b$, and $a \backslash b$, b/a — the corresponding left and right divisions.

$$Q = \{1, \ldots, q\}$$

$$u = (u_1, u_2, \ldots, u_q), \quad u_i \geqslant 0$$

$$u_1 + u_2 + \ldots + u_q = 1$$



Distribution support: $N(u) = \{i \in Q : u_i > 0\}$.

Probability convolution $u * v$

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \setminus i} = \sum_{j=1}^{q} u_{i/j} v_j$$

Probability convolution $u * v$

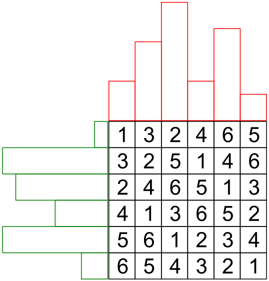
$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \backslash i} = \sum_{j=1}^{q} u_{i/j} v_j$$

If $x, y \in Q$ have distributions u and v, then $x \cdot y$ has a distribution $u * v$.

Probability convolution $u * v$

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \backslash i} = \sum_{j=1}^{q} u_{i/j} v_j$$

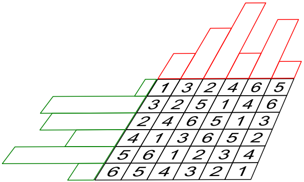
If $x, y \in Q$ have distributions u and v, then $x \cdot y$ has a distribution $u * v$.



Probability convolution $u * v$

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \backslash i} = \sum_{j=1}^{q} u_{i/j} v_j$$

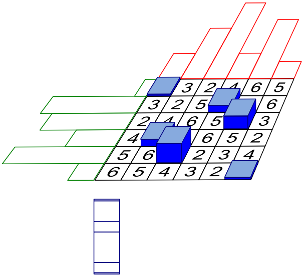
If $x, y \in Q$ have distributions u and v, then $x \cdot y$ has a distribution $u * v$.



Probability convolution $u * v$

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \backslash i} = \sum_{j=1}^{q} u_{i/j} v_j$$

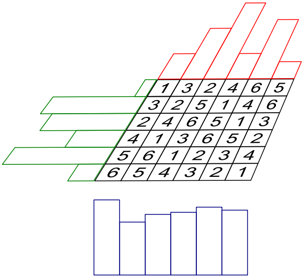
If $x, y \in Q$ have distributions u and v, then $x \cdot y$ has a distribution $u * v$.



Probability convolution $u * v$

$$(u * v)_i = \sum_{j=1}^{q} u_j v_{j \backslash i} = \sum_{j=1}^{q} u_{i/j} v_j$$

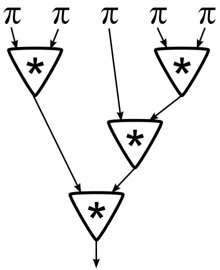
If $x, y \in Q$ have distributions u and v, then $x \cdot y$ has a distribution $u * v$.



Iterated convolutions

Let π be an initial distribution on Q.

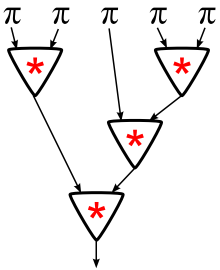
$$(\pi * \pi) * (\pi * (\pi * \pi))$$



Iterated convolutions

Let π be an initial distribution on Q.

$$(\pi * \pi) * (\pi * (\pi * \pi))$$

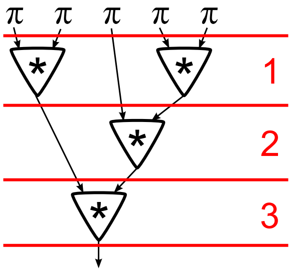


Length $L = 4$.

Iterated convolutions

Let π be an initial distribution on Q.

$$(\pi * \pi) * (\pi * (\pi * \pi))$$



Length $L = 4$. Depth $D = 3$.

Known results

• $(\ldots(\pi * \pi) * \pi)\ldots) * \pi)$	a Markov chain (quasigroup stream filters)

Known results

$(\ldots(\pi * \pi) * \pi)\ldots) * \pi)$	a Markov chain (quasigroup stream filters)
Group Q, arbitrary convolution	a Markov chain (random walks on finite groups)

Known results

$(\ldots(\pi * \pi) * \pi)\ldots) * \pi)$	a Markov chain (quasigroup stream filters)
Group Q, arbitrary convolution	a Markov chain (random walks on finite groups)

$N(\pi) = Q$: ergodic Markov chain is with a bistochastic matrix

$L \to \infty$: convolutions converge to the uniform distribution on Q.

Known results

$(\ldots(\pi * \pi) * \pi)\ldots) * \pi)$	a Markov chain (quasigroup stream filters)
Group Q, arbitrary convolution	a Markov chain (random walks on finite groups)

$N(\pi) = Q$: ergodic Markov chain is with a bistochastic matrix $L \to \infty$: convolutions converge to the uniform distribution on Q.

- $N(\pi) = Q$, *averages* of distributions with $L = m$, $m \to \infty$: converge to the uniform distribution.

Known results

$(\ldots(\pi * \pi) * \pi)\ldots) * \pi)$	a Markov chain (quasigroup stream filters)
Group Q, arbitrary convolution	a Markov chain (random walks on finite groups)

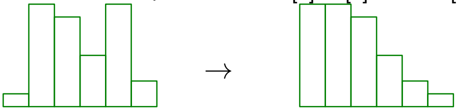
$N(\pi) = Q$: ergodic Markov chain is with a bistochastic matrix $L \to \infty$: convolutions converge to the uniform distribution on Q.

- $N(\pi) = Q$, *averages* of distributions with $L = m$, $m \to \infty$: converge to the uniform distribution.

When do quasigroup convolutions converge to the uniform distribution?

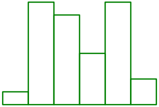
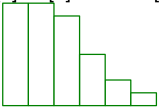
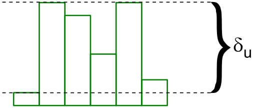
Convergence in depth

$$(u_1, u_2, \ldots, u_q) \quad \to \quad (u_{[1]}, u_{[2]}, \ldots, u_{[q]})$$

- 

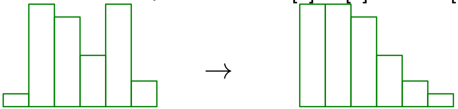
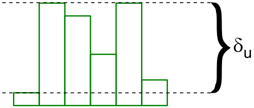
Convergence in depth

$$(u_1, u_2, \ldots, u_q) \quad \to \quad (u_{[1]}, u_{[2]}, \ldots, u_{[q]})$$

-  $\to$ 
- $\delta_u = u_{[1]} - u_{[q]}$ 

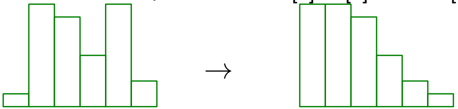
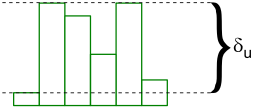
Convergence in depth

$$(u_1, u_2, \ldots, u_q) \quad \to \quad (u_{[1]}, u_{[2]}, \ldots, u_{[q]})$$

- 
- $\delta_u = u_{[1]} - u_{[q]}$ 

- $\delta_{u*v} \leqslant \min\{(1 - u_{[q]})\delta_v, (1 - v_{[q]})\delta_u\}$

Convergence in depth

- $$(u_1, u_2, \ldots, u_q) \quad \to \quad (u_{[1]}, u_{[2]}, \ldots, u_{[q]})$$
  
- $\delta_u = u_{[1]} - u_{[q]}$
  

- $\delta_{u*v} \leqslant \min\{(1 - u_{[q]})\delta_v, (1 - v_{[q]})\delta_u\}$

Theorem

Let w be an iterated convolution of depth k with initial distribution π. Then:

$$\delta_w \leqslant (1 - \pi_{[q]})^k.$$

Theorem (convergence in depth)

Let w be an iterated convolution of depth n with initial distribution π, $|N(\pi)| > \frac{|Q|}{2}$. Then there exists a $d \in (0, 1]$:

$$\delta_w \leqslant (1 - d)^n,$$

Theorem (convergence in depth)

Let w be an iterated convolution of depth n with initial distribution π, $|N(\pi)| > \frac{|Q|}{2}$. Then there exists a $d \in (0, 1]$:

$$\delta_w \leqslant (1-d)^n,$$

and consequently

$$\max \left| w_i - \frac{1}{|Q|} \right| \leqslant (1-d)^n.$$

Theorem (convergence in depth)

Let w be an iterated convolution of depth n with initial distribution π, $|N(\pi)| > \frac{|Q|}{2}$. Then there exists a $d \in (0, 1]$:

$$\delta_w \leqslant (1-d)^n,$$

and consequently

$$\max \left| w_i - \frac{1}{|Q|} \right| \leqslant (1-d)^n.$$

Theorem (convergence in length)

Let w be an iterated convolution of length m with initial distribution π, $|N(\pi)| > \frac{|Q|}{2}$. Then there exists an $\alpha > 0$:

$$\max \left| w_i - \frac{1}{|Q|} \right| \leqslant \frac{1}{m^\alpha}.$$

Generalization failure

	1	**2**	**3**	**4**	**5**	**6**
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

$$N(\pi) = \{1, 2\}$$

Generalization failure

	1	2	3	4	5	6
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

$$N(\pi) = \{1, 2\}$$

- $N(\pi * \pi) = \{1, 2, 3\}$

Generalization failure

	1	2	3	4	5	6
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

$$N(\pi) = \{1, 2\}$$

- $N(\pi * \pi) = \{1, 2, 3\}$
- $N((\pi * \pi) * (\pi * \pi)) = Q$

Generalization failure

	1	2	3	4	5	6
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

$$N(\pi) = \{1, 2\}$$

- $N(\pi * \pi) = \{1, 2, 3\}$
- $N((\pi * \pi) * (\pi * \pi)) = Q$
- $N((\ldots((\pi * \pi) * \pi)\ldots) * \pi) = \{1, 2, 3, 4\}$

Support properties

Let D_n be the set of all distributions with depth n (for some fixed π).

Support properties

Let D_n be the set of all distributions with depth n (for some fixed π).

$$N_n^D = \bigcup_{u \in D_n} N(u).$$

Support properties

Let D_n be the set of all distributions with depth n (for some fixed π).

$$N_n^D = \bigcup_{u \in D_n} N(u).$$

Theorem

There exists a subquasigroup $Q' \subseteq Q$ and a number n' such that for all $n > n'$:

$$N_n^D = Q'.$$

Q' is generated by elements of $N(\pi)$.

Support properties

Let D_n be the set of all distributions with depth n (for some fixed π).

$$N_n^D = \bigcup_{u \in D_n} N(u).$$

Theorem

There exists a subquasigroup $Q' \subseteq Q$ and a number n' such that for all $n > n'$:

$$N_n^D = Q'.$$

Q' is generated by elements of $N(\pi)$.

Without loss of generality: $Q' = Q$.

Convergence of averages

Define $d^{(n)}$ — the average of distributions with depth n:

$$d^{(n)} = \frac{1}{|D_n|} \sum_{u \in D_n} u.$$

Remark: $d^{(n)}$ is itself a probability distribution on Q.

Convergence of averages

Define $d^{(n)}$ — the average of distributions with depth n:

$$d^{(n)} = \frac{1}{|D_n|} \sum_{u \in D_n} u.$$

Remark: $d^{(n)}$ is itself a probability distribution on Q.

Theorem

There exist $d \in (0;1]$ and n' such that for every $n \geqslant n'$:

$$\delta_{d^{(n)}} \leqslant (1-d)^{n-n'},$$

and consequently

$$\max_{i \in Q} \left| d_i^{(n)} - \frac{1}{|Q|} \right| \leqslant (1-d)^{n-n'}.$$

Support periodicity in length

Let L_m be the set of all distributions with length m (for some fixed π).

Support periodicity in length

Let L_m be the set of all distributions with length m (for some fixed π).

$$N_m^L = \bigcup_{u \in L_m} N(u).$$

Support periodicity in length

Let L_m be the set of all distributions with length m (for some fixed π).

$$N_m^L = \bigcup_{u \in L_m} N(u).$$

Theorem

There exist r and m' such that for every $m \geqslant m'$ the sets

$$N_m^L, N_{m+1}^L, \dots, N_{m+r-1}^L$$

are pairwise disjoint, while $N_{m+r}^L = N_m^L$.
$N_m^L \cup N_{m+1}^L \cup \ldots \cup N_{m+r-1}^L$ is a subquasigroup $Q' \subseteq Q$, generated by $N(\pi)$.

Support periodicity in length

Let L_m be the set of all distributions with length m (for some fixed π).

$$N^L_m = \bigcup_{u \in L_m} N(u).$$

Theorem

There exist r and m' such that for every $m \geqslant m'$ the sets

$$N^L_m, N^L_{m+1}, \dots, N^L_{m+r-1}$$

are pairwise disjoint, while $N^L_{m+r} = N^L_m$.
$N^L_m \cup N^L_{m+1} \cup \ldots \cup N^L_{m+r-1}$ is a subquasigroup $Q' \subseteq Q$, generated by $N(\pi)$.

If $r > 1$ there is *periodicity* in the supports.

Support periodicity in length

Let L_m be the set of all distributions with length m (for some fixed π).

$$N_m^L = \bigcup_{u \in L_m} N(u).$$

Theorem

There exist r and m' such that for every $m \geqslant m'$ the sets

$$N_m^L, N_{m+1}^L, \dots, N_{m+r-1}^L$$

are pairwise disjoint, while $N_{m+r}^L = N_m^L$.
$N_m^L \cup N_{m+1}^L \cup \ldots \cup N_{m+r-1}^L$ is a subquasigroup $Q' \subseteq Q$, generated by $N(\pi)$.

If $r > 1$ there is *periodicity* in the supports.
Again, without loss of generality: $Q' = Q$.

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L

Example

	1	**2**	**3**	**4**	**5**	**6**
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1, 2\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1, 2\}$
1	$\pi * \pi$	$\{3, 4\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$

Example

	1	**2**	**3**	**4**	**5**	**6**
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1, 2\}$
1	$\pi * \pi$	$\{3, 4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5, 6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1, 2\}$

Example

	1	**2**	**3**	**4**	**5**	**6**
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Example

	1	**2**	**3**	**4**	**5**	**6**
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Supports are periodic ($r > 1$) iff there exists a homomorphism $\varphi : Q \to \mathbb{Z}_r$ such that $\varphi(N(\pi)) = 1 \in \mathbb{Z}_r$.

Example

	1	2	3	4	5	6
1	3	4	6	5	2	1
2	4	3	5	6	1	2
3	5	6	1	2	4	3
4	6	5	2	1	3	4
5	2	1	3	4	5	6
6	1	2	4	3	6	5

m	L_m	N_m^L
0	π	$\{1,2\}$
1	$\pi * \pi$	$\{3,4\}$
2	$(\pi * \pi) * \pi, \pi * (\pi * \pi)$	$\{5,6\}$
3	$((\pi * \pi) * \pi) * \pi, (\pi * (\pi * \pi)) * \pi,$ $\pi * ((\pi * \pi) * \pi), \pi * (\pi * (\pi * \pi)),$ $(\pi * \pi) * (\pi * \pi)$	$\{1,2\}$

Supports are periodic ($r > 1$) iff there exists a homomorphism $\varphi : Q \to \mathbb{Z}_r$ such that $\varphi(N(\pi)) = 1 \in \mathbb{Z}_r$.
The period r is the biggest value for which such a homomorphism exists.

Averages in length

Define $\ell^{(m)}$ — the average of distributions with length m:

$$\ell^{(m)} = \frac{1}{|L_m|} \sum_{u \in L_m} u.$$

Averages in length

Define $\ell^{(m)}$ — the average of distributions with length m:

$$\ell^{(m)} = \frac{1}{|L_m|} \sum_{u \in L_m} u.$$

Theorem

Suppose there exists an m' such that $N_m^L = Q$ for every $m \geqslant m'$. Then there exist $\alpha, \beta > 0$ and $m'' > m'$ such that for $m \geqslant m''$:

$$\max_{i \in Q} \left| \ell_i^{(m)} - \frac{1}{|Q|} \right| \leqslant \frac{\beta}{m^\alpha}.$$

The periodic case

$$\dots \quad N^L_m, \quad N^L_{m+1}, \quad \dots, \quad N^L_{m+r-1}, \quad N^L_{m+r}, \quad N^L_{m+r+1}, \quad \dots$$

The periodic case

$$\begin{array}{cccccccc} \dots & N_m^L, & N_{m+1}^L, & \dots, & N_{m+r-1}^L, & N_{m+r}^L, & N_{m+r+1}^L, & \dots \\ \dots & Q_0, & Q_1, & \dots, & Q_{r-1}, & Q_0, & Q_1, & \dots \end{array}$$

The periodic case

$$\begin{array}{ccccccc} \ldots & N^L_m, & N^L_{m+1}, & \ldots, & N^L_{m+r-1}, & N^L_{m+r}, & N^L_{m+r+1}, & \ldots \\ \ldots & Q_0, & Q_1, & \ldots, & Q_{r-1}, & Q_0, & Q_1, & \ldots \end{array}$$

$$Q_0 \cup Q_1 \cup \ldots \cup Q_{r-1} = Q$$

The periodic case

$$\begin{array}{ccccccc} \ldots & N^L_m, & N^L_{m+1}, & \ldots, & N^L_{m+r-1}, & N^L_{m+r}, & N^L_{m+r+1}, & \ldots \\ \ldots & Q_0, & Q_1, & \ldots, & Q_{r-1}, & Q_0, & Q_1, & \ldots \end{array}$$

$$Q_0 \cup Q_1 \cup \ldots \cup Q_{r-1} = Q$$

$$|Q_0| = |Q_1| = \ldots = |Q_{r-1}| = \frac{|Q|}{r}$$

The periodic case

$$\begin{array}{cccccccc} \dots & N^L_m, & N^L_{m+1}, & \dots, & N^L_{m+r-1}, & N^L_{m+r}, & N^L_{m+r+1}, & \dots \\ \dots & Q_0, & Q_1, & \dots, & Q_{r-1}, & Q_0, & Q_1, & \dots \end{array}$$

$$Q_0 \cup Q_1 \cup \ldots \cup Q_{r-1} = Q$$

$$|Q_0| = |Q_1| = \ldots = |Q_{r-1}| = \frac{|Q|}{r}$$

Theorem

Suppose there exists an m' and sets Q_b, $b = 0, \ldots, r-1$ such that $N^L_{rk+b} = Q_b$ for every $m \geqslant m'$. Then there exist $\alpha, \beta > 0$ and $m'' > m'$ such that for $rk + b \geqslant m''$:

$$\max_{i \in Q_b} \left| \ell_i^{(rk+b)} - \frac{1}{|Q_b|} \right| \leqslant \frac{\beta}{k^\alpha}.$$

Thank You for Your attention!