# On the speed of convergence of Heisenberg random walks 

Joint work with Daniel Bump, Persi Diaconis, Angela Hicks and Harold Widom

Laurent Miclo Institut de Mathématiques de Toulouse

Plan of the talk
(1) Motivations and main result
(2) Representation theory
(3) Eigenvalues bounds
4. Further results

For $n \in \mathbb{N} \backslash\{1,2\}$, let

$$
H(n):=\left\{\left(\begin{array}{lll}
1 & x & z \\
0 & 1 & y \\
0 & 0 & 1
\end{array}\right): x, y, z \in \mathbb{Z}_{n}\right\}
$$

Denoting $(x, y, z)$ the above matrix, the matrix multiplication can be written

$$
(x, y, z)\left(x^{\prime}, y^{\prime}, z^{\prime}\right)=\left(x+x^{\prime}, y+y^{\prime}, z+z^{\prime}+x y^{\prime}\right)
$$

Consider the symmetric generating set

$$
S:=\{(1,0,0),(-1,0,0),(0,1,0),(0,-1,0)\}
$$

and $Q$ the uniform distribution on $S$.

## Random walk

The random walk associated consists in sampling independent elements according to $Q$ and in multiplying them. At any time $k \in \mathbb{Z}_{+}$, the resulting distribution is $Q^{* k}$ and if $n$ is odd, it converges for $k$ large to the uniform distribution $U$ on $H(n)$. Quantitatively order $n^{2}$ steps are necessary for convergence:

## Theorem

There exists constants $A<B$ such that

$$
A \exp \left(-2 \pi^{2} k / n^{2}\right) \leqslant\left\|Q^{* k}-U\right\|_{\mathrm{tv}} \leqslant B \exp \left(-2 \pi^{2} k / n^{2}\right)
$$

These estimates were first proved by Diaconis and Saloff-Coste [94-96], using geometric analysis on nilpotent groups (Nash inequalities, moderate growth conditions, ...). Related results can be found in Stong [94-95], Alexopoulos [02], Breuillard [04-05], Diaconis [10] or Peres and Sly [13].

## An interesting matrix

The goal of the talk is to present an alternative approach based on Fourier analysis (representation theory). In particular to quantify the fact that the convergence of the $z$-coordinate should be faster (order $n \ln (n)$, but it should be $n$ ) than that of the $x$ - and $y$-coordinates (order $n^{2}$ ).
Everything boils down to bounding the spectrum of the matrix $M(c):=(P+D(c)) / 2$, with $c \in \mathbb{Z}_{n}$, where $P$ is the transition kernel of the random walk on $\mathbb{Z}_{n}$ and $D(c)$ is the diagonal matrix with entries

$$
\forall j \in \mathbb{Z}_{n}, \quad D_{j, j}(c):=\cos (2 \pi c j / n)
$$

Surprisingly, these simple matrices come up in a variety of solid state physics and ergodic theory problems, such as Harper's Operators, Hofstader's Butterfly or the Ten Martinis Problem of Simon. They are also connected to the fast Fourier transform and to the Lévy's area of Brownian motions.

## Basic formulas (1)

Let $G$ be a finite group with $\widehat{G}$ the irreducible unitary representations. For $Q$ a probability on $G$ and $\rho \in \widehat{G}$, define the Fourier transform

$$
\widehat{Q}(\rho):=\sum_{g \in G} Q(g) \rho(g)
$$

The Fourier Inversion Theorem enables to reconstruct $Q$ from these matrices:

$$
\forall g \in G, \quad Q(g)=\frac{1}{|G|} \sum_{\rho \in \hat{G}} d_{\rho} \operatorname{tr}\left(\widehat{Q}(\rho) \rho(g)^{*}\right)
$$

where $d_{\rho}$ is the dimension of the representation $\rho$.

## Basic formulas (2)

The Fourier transform takes convolutions into products, thus $\widehat{Q * Q}(\rho)=(\widehat{Q}(\rho))^{2}$. It can also be shown (Schur's lemma) that if $U$ is the uniform distribution on $G$, then $\widehat{U}(\rho)=0$, except for the trivial representation $\mathbb{1}$ of $\hat{G}$.
Diaconis [88] has deduced the following upper bound: for any $k \in \mathbb{N}$,

$$
\left\|Q^{* k}-U\right\|_{\mathrm{tv}}^{2} \leqslant \frac{1}{4} \sum_{\rho \in \hat{G} \backslash\{\mathbb{1}\}} d_{\rho}\left\|\hat{Q}^{k}(\rho)\right\|^{2}
$$

where the norm of a matrix $M$ is given by $\|M\|^{2}:=\operatorname{tr}\left(M M^{*}\right)$.

Fix an integer $m$ dividing $n$ and let $V:=\left\{f: \mathbb{Z}_{m} \rightarrow \mathbb{C}\right\}$. Consider $a, b \in \mathbb{Z}_{n / m}$ and $c \in \mathbb{Z}_{m}$ which is prime with $m$. Denote $q_{m}=e^{2 \pi i / m}, q_{n}=e^{2 \pi i / n}$ and define $\rho_{a, b, c} \in G L(V)$ via

$$
\forall f \in V, \forall j \in \mathbb{Z}_{m},
$$

$$
\rho_{a, b, c}(x, y, z) f(j):=q_{n}^{a x+b y} q_{m}^{c(y j+z)} f(j+x)
$$

It can be checked that such $\rho_{a, b, c}$ are distinct irreducible representations of $H(n)$. For fixed $m$ their number is $\left(\frac{n}{m}\right)^{2} \phi(m)$ where $\phi$ is the Euler phi function. Since

$$
\sum_{m \mid n}\left(\frac{n}{m}\right)^{2} \phi(m) m^{2}=n^{3}=|H(n)|
$$

they form a complete set of irreducible representations of $H(n)$.

- When $m=1$, this gives $n^{2} 1$-dimensional representations (or characters):

$$
\rho_{a, b, 1}(x, y, z):=q_{n}^{a x+b y}
$$

- Consider the uniform probability $Q$ on $S$ and let us compute $\hat{Q}(a, b, c)$. When $m=1$, we get

$$
\hat{Q}(a, b, 1)=\frac{1}{2} \cos \left(\frac{2 \pi a}{n}\right)+\frac{1}{2} \cos \left(\frac{2 \pi b}{n}\right)
$$

When $m=2$ (so $n$ is even), we get

$$
\hat{Q}(a, b, 1)=\frac{1}{2}\left(\begin{array}{cc}
\cos \left(\frac{2 \pi b}{n}\right) & \cos \left(\frac{2 \pi a}{n}\right) \\
\cos \left(\frac{2 \pi a}{n}\right) & -\cos \left(\frac{2 \pi b}{n}\right)
\end{array}\right)
$$

More generally, for $m \geqslant 3$,

$$
\forall I, k \in \mathbb{Z}_{m}, \quad \hat{Q}(a, b, c)_{I, k}=\frac{1}{4} \begin{cases}2 \Re\left(q_{n}^{b} q_{m}^{\prime c}\right) & , \text { if } I=k \\ q_{n}^{a} & , \text { if } k=I+1 \\ q_{n}^{-a} & , \text { if } k=I-1 \\ 0 & , \text { otherwise }\end{cases}
$$

Conjugating with the diagonal matrix $\left(1, q_{n}^{a}, q_{n}^{2 a}, \ldots, q_{n}^{(m-1) a}\right)$ produces a matrix with 1 on the super and sub diagonals (and $q_{n}^{-m a}$ and $q_{n}^{m a}$ in the "special corners").

- When $n$ is prime, there are $n^{2}$ one-dimensional 1-dimensional representations and $n-1 n$-dimensional representations, with $\widehat{Q}(0,0, c)$ conjugate to $M(c)$.

When $n$ is prime, one thus gets, for any $k \in \mathbb{N}$,

$$
\begin{aligned}
4\left\|Q^{* k}-U\right\|_{\mathrm{tv}}^{2} \leqslant & \sum_{(a, b) \neq(0,0)}\left(\frac{1}{2} \cos \left(\frac{2 \pi a}{n}\right)+\frac{1}{2} \cos \left(\frac{2 \pi b}{n}\right)\right)^{2 k} \\
& +\sum_{c=1}^{n-1} n\left\|M(c)^{k}\right\|^{2}
\end{aligned}
$$

For the first sum, consider for instance the case $a=0$ and $b=1$. If $k$ is of order $n^{2}$, say $k=\eta n^{2}$, it appears the

$$
\begin{aligned}
\left(\frac{1}{2}+\frac{1}{2} \cos \left(\frac{2 \pi}{n}\right)\right)^{2 k} & =\left(1-\frac{\pi^{2}}{n^{2}}+O\left(\frac{1}{n^{4}}\right)\right)^{2 \eta n^{2}} \\
& \sim \exp \left(-2 \pi^{2} \eta\right)
\end{aligned}
$$

The other terms can be similarly bounded so that in the end, the whole first sum is of order $\exp \left(-2 \pi^{2} \eta\right)$ up to an universal factor.

## Proof of the theorem when $n$ is prime (2)

For the second sum, consider the eigenvalues of $M(c)$ :

$$
1>\beta_{1}(c) \geqslant \beta_{2}(c) \geqslant \cdots \geqslant \beta_{n}(c)>-1
$$

and denote $\beta^{*}(c):=\max \left(\beta_{1}(c),-\beta_{n}(c)\right)$. The following bounds enable to end the proof of the theorem, taking into account that $\beta^{*}(c)=\beta^{*}(n-c)$.

## Proposition

There exists an universal constant $\theta>0$ such that: for $0<c<n / \ln (n)$,

$$
\beta^{*}(c) \leqslant 1-\frac{\theta}{n^{4 / 3}}
$$

for $n / \ln (n) \leqslant c<n / 2$,

$$
\beta^{*}(c) \leqslant 1-\frac{3}{4}\left(\frac{c}{n}\right)^{2}
$$

More generally, consider for $n, c \in \mathbb{N}$ and $\alpha \in \mathbb{R}$, the diagonal matrix $D(n, c, \alpha)$ with entries

$$
\cos \left(\frac{2 \pi c}{n}(j+\alpha)\right), \quad 0 \leqslant j \leqslant n-1
$$

and the matrix $M(n, c, \alpha):=(P+D(n, c, \alpha)) / 2$. Let $S(n, c, \alpha)$ be the spectrum of $M(n, c, \alpha)$.
We have the following properties:
(a) $\forall k \in \mathbb{N}, \quad S(n, c, \alpha) \subset S(k n, k c, \alpha)$
(b) If $n$ is even, $S(n, c, \alpha)=-S\left(n, c, \alpha+\frac{n}{2 c}\right)$
(c) If $n$ is odd, $S(n, c, \alpha) \subset-S\left(2 n, 2 c, \alpha+\frac{n}{2 c}\right)$
(a) comes from a juxtaposition of the eigenvectors, (b) from the multiplication of an eigenvector by $\left((-1)^{j}\right)_{0 \leqslant i \leqslant n-1}$ and (c) from (b) and (a) with $k=2$.

Consider on $K$ a transition kernel on $\bar{S}=S \sqcup\{\infty\}$ where

- $K$ is irreducible on the finite set $S$ and reversible with respect to a positive measure $\mu$.
- $\infty$ is an absorbing point which is reachable from $S$.

Let be given for any $x \in S$ a path

$$
\gamma_{x}:=\left(x_{0}=x, x_{1}, x_{2}, \ldots, x_{\left|\gamma_{x}\right|}=\infty\right)
$$

going from $x$ to $\infty$ with $K\left(x_{I}, x_{I+1}\right)>0$ for $0 \leqslant I \leqslant\left|\gamma_{x}\right|-1$. Then the largest eigenvalue of $K$ is bounded above by $1-1 / A$ where

$$
A:=\max _{x \in S, y \in \bar{S}} \frac{2}{\mu(x) K(x, y)} \sum_{z \in S:(x, y) \in \gamma_{z}}\left|\gamma_{z}\right| \mu(z)
$$

## Path arguments (1)

The matrix $M(c)$ can be transformed into a subMarkov kernel by considering

$$
K_{c}:=(I+2 M(c)) / 3
$$

We come back to the previous situation by taking $S:=\mathbb{Z}_{n}$ and completing $K_{c}$ into an absorbed kernel (with $\left.K_{c}(x, \infty):=(1-\cos (2 \pi c x / n)) / 3\right)$. Thus it remains to find convenient paths in order to prove:

## Lemma

There exists an universal constant $\theta>0$ such that for all positive integer $n$ and $1 \leqslant c \leqslant n / \ln (n)$, we have

$$
\beta_{1}(c) \leqslant 1-\theta\left(\frac{c}{n}\right)^{4 / 3}
$$

The idea is to use paths exiting $\mathbb{Z}_{n}$ where the probability to go in one step to $\infty$ is no longer negligible (it is the weakest at 0 mod $(n / c)$ ). So to get out of the "bad positions" (where the chain is not sufficiently killed!), we use paths of length $(n / c)^{2 / 3}$ to join the nearest "good positions". From the latter ones, just go directly to $\infty$. For a good $x$, we have

$$
\begin{aligned}
K_{c}(x, \infty) & \geqslant \frac{1}{3}\left(\frac{1}{2}\left(\frac{2 \pi c}{n}\left(\frac{n}{c}\right)^{2 / 3}\right)^{2}+O\left(\frac{2 \pi c}{n}\left(\frac{n}{c}\right)^{2 / 3}\right)^{4}\right) \\
& \sim \frac{2 \pi^{2}}{3}\left(\frac{c}{n}\right)^{2 / 3}
\end{aligned}
$$

The wanted bound follows easily (after an appropriate optimization which led to the exponent $2 / 3$ ).

For $\frac{n}{\log (n)} \leqslant c \leqslant \frac{n}{2}$, we get a similar bound:

$$
\beta_{1}(c) \leqslant 1-\frac{3}{4}\left(\frac{c}{n}\right)^{2}
$$

The proof is the same, except that to join good positions from bad ones, use paths of length $\lceil\lfloor n / c\rfloor / 4\rceil$.

Note that these path arguments are quite robust, e.g. by real shift of the diagonal, namely if $(\cos (2 \pi c j / n))_{j \in \mathbb{Z}_{n}}$ is replaced by $(\cos (2 \pi c(\alpha+j) / n))_{j \in \mathbb{Z}_{n}}$ where $\alpha \in \mathbb{R}$. With the inclusion $S(n, c, 0) \subset-S\left(2 n, 2 c, \frac{n}{2 c}\right)$, this the key for the minoration of the lowest eigenvalue:

## Lowest eigenvalue

## Lemma

There exists an universal constant $\theta>0$ such that for all positive integer $n$ and $1 \leqslant c \leqslant n / \ln (n)$, we have

$$
\beta_{n}(c) \geqslant-1+\theta\left(\frac{c}{n}\right)^{4 / 3}
$$

and for $\frac{n}{\log (n)} \leqslant c<\frac{n}{2}$,

$$
\beta_{n}(c) \geqslant-1+\frac{3}{4}\left(\frac{c}{n}\right)^{2}(1+o(1))
$$

It ends the proof of the announced proposition.

## More precise asymptotics (1)

So we got an order $n^{-4 / 3}$ for the spectral gap of the matrix $M:=M(1)$. In fact the right order is $n^{-1}$ and one can go further:

## Theorem

For $n$ large, the $k$-th largest eigenvalue $\beta_{k}$ of $M, k \in \mathbb{N}$, behaves like

$$
\beta_{k}=1-\frac{\mu_{k}}{n}+o\left(\frac{1}{n}\right)
$$

where $\mu_{k}=(2 k-1) \pi$ is the $k$-th smallest eigenvalue of the (harmonic oscillator) Schrödinger operator on $\mathbb{R}$ :

$$
-\frac{1}{4} \frac{d^{2}}{d x^{2}}+\pi^{2} x^{2}
$$

## More precise asymptotics (2)

This is proven by showing the convergence of the corresponding eigenfunctions, appropriately renormalized (via classical Fourier transform analysis).
There is a similar result for the lowest eigenvalues: for $n$ large, the $k$-th smallest eigenvalue $\beta_{n-k+1}$ of $M, k \in \mathbb{N}$, behaves like

$$
\beta_{n-k+1}=-1+\frac{\mu_{k}}{n}+o\left(\frac{1}{n}\right)
$$

In the previous examples the diagonal was quite regular, what does happen if one shuffles it by replacing $(\cos (2 \pi c j / n))_{j \in \mathbb{Z}_{n}}$ by $(\cos (2 \pi c \sigma(j) / n))_{j \in \mathbb{Z}_{n}}$, where $\sigma$ belongs to the permutation group $\mathcal{S}_{n}$ ?
Consider the case $c=1$. Heuristically the non-scrambled diagonal should be the worst case, because it is constructing the safer place for the particle not to be killed. We have not been able to prove that, but here is a result in this direction: there exists a universal constant $c>0$ such that for all $n \in \mathbb{N} \backslash\{1,2\}$, whatever $\sigma \in \mathcal{S}_{n}$, the corresponding largest eigenvalue is bounded above by $1-c / n$.

## Quality of a niche (1)

The proof is based on a probabilistic estimate of the quality of a niche. Consider $\left(X_{t}\right)_{t \geqslant 0}$ the continuous-time random walk on $\mathbb{Z}$, with jump rates 1 between neighbors. Make it starts from 0. Fix $n \in \mathbb{Z}_{+}$and denote

$$
\tau_{n}:=\inf \left\{t \geqslant 0:\left|X_{t}\right|=n+1\right\}
$$

Let $\left(u_{x}\right)_{x \in \llbracket-n, n \rrbracket}$ be some killing rates and $\mathcal{E}$ be an independent exponential variable of parameter 1 . An associated absorption time $\bar{\tau} \in[0,+\infty]$ is defined by

$$
\bar{\tau}:=\inf \left\{t \geqslant 0: \int_{0}^{t} u_{X_{s}} d s \geqslant \mathcal{E}\right\}
$$

Using Ray-Knight type ideas in a discrete context, we get:

## Quality of a niche (2)

## Proposition

We have for $n \geqslant 1$,
$\mathbb{P}\left[\bar{\tau}>\tau_{n}\right] \leqslant G_{n}(v):=\left(\prod_{y \in \llbracket 0, n-1 \rrbracket} \frac{1}{1+(n+1)(n+1-y) v_{y}}\right)^{1 /(n+1)}$
where $v:=\left(v_{y}\right)_{y \in \llbracket 0, n \rrbracket}:=\min \left(u_{-y}, u_{y}\right)$
The functional $G_{n}$ has nice monotonicity properties:

$$
\begin{aligned}
v \leqslant v^{\prime} & \Rightarrow G_{n}(v) \geqslant G_{n}\left(v^{\prime}\right) \\
G_{n}(v) & \leqslant G_{n}(\bar{v})
\end{aligned}
$$

where $\bar{v}$ is the non-decreasing ordering of the entries of $v$. It enables to compare niches and to prove the announced result on the scrambled diagonals.

## Convergence of the center (1)

The previous improved bounds are the key to good estimates on the speed of convergence of the center of $H(n)$, which is $\left\{(0,0, z): z \in \mathbb{Z}_{n}\right\}$. Let us consider the case where $n$ is prime. the Fourier inversion theorem implies that for any $k \in \mathbb{Z}_{+}$and $z \in \mathbb{Z}_{n}$,

$$
\mathbb{P}\left[Z_{k}=z\right]=\frac{1}{n}+\frac{1}{n} \sum_{c=1}^{n-1} e^{\frac{-2 \pi i c z}{n}} \sum_{l=1}^{n}\left(\hat{Q}(0,0, c)^{k}\right)_{1, l}
$$

where $\left(X_{k}, Y_{k}, Z_{k}\right)_{k \in \mathbb{Z}_{+}}$is the underlying random walk. Indeed, a priori we have for any $k \in \mathbb{Z}_{+}$and $(x, y, z) \in H(n)$,
$\left.\mathbb{P}\left[X_{k}=x, Y_{k}=y, Z_{k}=z\right]=\frac{1}{n^{3}} \sum_{\rho \in \hat{H}(n)} d_{\rho} \operatorname{tr}(\hat{Q}(\rho))^{k} \rho\left((x, y, z)^{-1}\right)\right)$
Using the explicit description of $\hat{H}(n)$, we get that

$$
\sum_{x, y \in \mathbb{Z}_{n}} \rho\left((x, y, z)^{-1}\right)=0
$$

if $\rho$ is one of the non-trivial representations of dimensicn 1 and

## Convergence of the center (2)

$$
\left.\sum_{x, y \in \mathbb{Z}_{n}} \rho\left((x, y, z)^{-1}\right)\right)=n e^{\frac{-2 \pi i c z}{n}}\left(\begin{array}{cccc}
1 & 0 & \ldots & 0 \\
\vdots & \vdots & & \vdots \\
1 & 0 & \ldots & 0
\end{array}\right)
$$

for the $n$-dimensional representations $(0,0, c)$, with $c \in \mathbb{Z}_{n} \backslash\{0\}$.

## Corollary

There exists a universal constant $\theta>0$ such that for any prime $n$ and any time $k \in \mathbb{Z}_{+}$,

$$
\left\|\mathcal{L}\left(Z_{k}\right)-U\right\|_{\mathrm{tv}} \leqslant n e^{-\theta k / n}
$$

It is an immediate consequence of the previous results, using for any $k \in \mathbb{Z}_{+}, c \in \mathbb{Z}_{n} \backslash\{0\}$ and $I \in \llbracket 1, n \rrbracket$, the rough bound

$$
\left|\left(\hat{Q}(0,0, c)^{k}\right)_{1, l}\right| \leqslant \beta^{*}(c)^{k} \leqslant(1-\theta / n)^{k}
$$

