THE LARGE SIEVE, PROPERTY (T) AND THE HOMOLOGY OF DUNFIELD-THURSTON RANDOM 3-MANIFOLDS

E. KOWALSKI

In their paper [DT1], N. Dunfield and W. Thurston define a notion of "random 3-manifold" and study some properties of those manifolds with respect (among other things) to the existence of finite covers with certain covering groups, especially with regard to their homological properties (in particular, which ones have positive first Betti number). In this note, we show that some applications of the large sieve to random walks on groups with Property (T) (or Property (τ)) may be used to refine some of their results.

To state our results, let $g \geqslant 1$ be an integer. Let G denote the mapping class group of a closed surface Σ_g of genus g, and let S be a fixed finite set of generators, such that $S = S^{-1}$ (i.e., a symmetric generating set). For $g = 1$, assume that $1 \in S$ (this is to avoid periodicity issues with the random walk; it can also be assumed for simplicity if $g \geqslant 2$, but there it is not necessary). Associated to this is a simple random walk (X_k) on G defined by

$$X_0 = 1, \qquad X_{k+1} = X_k \xi_{k+1} \text{ for } k \geqslant 0,$$

where (ξ_k) is a sequence of independent S-valued random variables with uniform distribution

$$\boldsymbol{P}(\xi_k = s) = \frac{1}{|S|}, \qquad \text{for all } s \in S.$$

Let (M_k) denote the corresponding sequence of random 3-manifolds: M_k is obtained from two copies of a handlebody H_g of genus g with boundary $\partial H_g = \Sigma_g$ by identifying their common boundary Σ_g using the mapping class $X_k \in G$.

Dunfield and Thurston have shown that, given a prime number ℓ, the probability that $H_1(M_k, \mathbf{F}_\ell)$ is zero tends to 1 as $k \to +\infty$ and $\ell \to +\infty$, and hence the probability that $H_1(M_k, \mathbf{Q}) \neq 0$ tends to 0, but that the expected value of the order of $H_1(M_k, \mathbf{Z})$ tends to infinity as $k \to +\infty$ (see Corollary 8.5 in [DT1]). We will give quantitative formulations of those results.

Proposition 1. *Let $g \geqslant 1$ be given and let (M_k) be the Dunfield-Thurston sequence of random 3-manifolds. Then*

(1) *There exists $C \geqslant 0$ and $\delta > 0$, depending only on g and S, such that*

$$\boldsymbol{P}(H_1(M_k, \mathbf{Q}) \neq 0) \leqslant C \exp(-\delta k) \tag{1}$$

for all $k \geqslant 1$. In particular, by the easy Borel-Cantelli lemma, almost surely, there are at most finitely many k for which $H_1(M_k, \mathbf{Q})$ is non-zero.

(2) *There exists $b > 0$, $\alpha > 0$ and $C' \geqslant 0$ such that*

$$\boldsymbol{P}\Big(H_1(M_k, \mathbf{F}_\ell) \neq 0 \textit{ for at least } \log bk \textit{ primes}\Big) \geqslant 1 - \frac{C'}{\log k}, \tag{2}$$

$$\boldsymbol{P}\Big(\textit{The order of } H_1(M_k, \mathbf{Z}) \textit{ is } < k^{\alpha \log\log k}\Big) \leqslant \frac{C'}{\log k}, \tag{3}$$

and in particular we have

$$\boldsymbol{E}\Big(\textit{Order of } H_1(M_k, \mathbf{Z})_{tors}\Big) \geqslant c k^{\alpha \log\log k}$$

for some constant $c > 0$, where $H_1(M_k, \mathbf{Z})_{tors}$ is the torsion subgroup of $H_1(M_k, \mathbf{Z})$.

This shows that with probability going to 1, $H_1(M_k,\mathbf{Z})$ is a finite abelian group with "superpolynomial" growth in terms of k. Since (3) is deduced rather wastefully from (2), it is even possible that the size of $H_1(M_k,\mathbf{Z})$ could be growing quite a bit faster. On the other hand, it's not clear how to trade a faster convergence of the probability in (2) for a slower growth of $H_1(M_k,\mathbf{Z})$.

The proof will proceed by combining the analysis of $H_1(M_k,\mathbf{Z})$ in [DT1] with an application of the following sieve result (a special case of a general abstract form of the large sieve principle), which is obtained by combining [K1, Pr. 2.13, Th. 7.3] (or the older version currently available online [K2, Pr. 3.1, Cor. 9.7]). This is based, in turn, on generalizations of fairly classical ideas of analytic number theory and on their implementation in the case of random walks on discrete finitely generated groups for which Property (T) of Kazhdan, or Property (τ) of Lubotzky, holds. It is likely that other combinations of those ideas exist with interesting consequences.

Theorem 2. *With notation as above, let $V = H_1(\Sigma_g,\mathbf{Z}) \simeq \mathbf{Z}^2g$ be the first homology group of Σ_g, $\langle\cdot,\cdot\rangle$ the symplectic intersection pairing on V and let*

$$\rho\,:\,G\rightarrow Sp(V,\langle\cdot,\cdot,\rangle)\simeq Sp(2g,\mathbf{Z})$$

be the surjective homomorphism defined by means of the action of a mapping class on V. For any prime ℓ, denote by $\rho_\ell(g)$ the image of $\rho(g)$ by the reduction map $Sp(2g,\mathbf{Z})\rightarrow Sp(2g,\mathbf{F}_\ell)$, where $\mathbf{F}_\ell=\mathbf{Z}/\ell\mathbf{Z}$.

There exists $\eta>0$ and $A\geqslant 0$, depending only on g and S with the following properties: for any $L\geqslant 2$, for any choice of subsets $\Omega_\ell\subset Sp(2g,\mathbf{F}_\ell)$ for all primes ℓ, we have

$$\boldsymbol{E}\Big(\Big(Q(X_k,L)-P(L)\Big)^2\Big)\leqslant(1+L^A\exp(-k\eta))P(L), \tag{4}$$

where

$$Q(X_k,L)=|\{\ell\leqslant L\ \mid\ \rho_\ell(X_k)\in\Omega_\ell\}|, \tag{5}$$

$$P(L)=\sum_{\ell\leqslant L}\frac{|\Omega_\ell|}{|Sp(2g,\mathbf{F}_\ell)|}, \tag{6}$$

and the sums over ℓ run over primes only. In particular, we have

$$\boldsymbol{P}(\rho_\ell(X_k)\notin\Omega_\ell \textit{ for all } \ell\leqslant L)\leqslant(1+L^A\exp(-k\eta))P(L)^{-1}. \tag{7}$$

Both parts of Proposition 1 will be consequences of Theorem 2 for well-chosen sets Ω_ℓ, coming from the description of $H_1(M_k,\mathbf{Z})$ and $H_1(M_k,\mathbf{F}_\ell)$ found in [DT1, §8], which we recall in a lemma.

Lemma 3. *Let $\varphi\in G$ be a mapping class and let M_φ be the 3-manifold obtained by gluing two copies of H_g along their common boundary Σ_g using the mapping class φ.*

(1) *Let $J=\ker(H_1(\Sigma_g,\mathbf{Z})\rightarrow H_1(H_g,\mathbf{Z})$. Then*

$$H_1(M_\varphi,\mathbf{Z})\simeq H_1(\Sigma_g,\mathbf{Z})/\langle J,\rho(\varphi)(J)\rangle,$$

and moreover $J\simeq\mathbf{Z}^g$ is a lagrangian sublattice in $H_1(\Sigma_g,\mathbf{Z})$ with respect to the intersection pairing.

(2) *For any prime ℓ, we have similarly*

$$H_1(M_\varphi,\mathbf{F}_\ell)\simeq H_1(\Sigma_g,\mathbf{F}_\ell)/\langle J_\ell,\rho_\ell(\varphi)(J_\ell)\rangle$$

where $J_\ell=J/\ell J$ is the image of J in $H_1(\Sigma_g,\mathbf{F}_\ell)\simeq\mathbf{F}_\ell^{2g}$.

Proof of Proposition 1. Since the handlebody H_g and the boundary surface Σ_g are fixed throughout the argument, the lagrangian lattice J is likewise fixed, and so are its reductions J_ℓ. Now let

$$\Omega_\ell=\{g\in Sp(V/\ell V)\ \mid\ \langle J_\ell,g(J_\ell)\rangle=\mathbf{F}_\ell^{2g}\}$$

(the set of symplectic matrics over $\mathbf{F}_\ell$ for which J_ℓ and $g(J_\ell)$ are "transverse").

Then the lemma applied to $\varphi = X_k$ implies the basic criterion

$$H_1(M_k, \mathbf{F}_\ell) \neq 0 \text{ if and only if } \rho_\ell(X_k) \notin \Omega_\ell \tag{8}$$

which allows us to reduce the statements of Proposition 1 to sieve conditions.

We start with part (1). We have the basic upper bound

$$\dim_{\mathbf{Q}} H_1(M_k, \mathbf{Q}) \leqslant \dim_{\mathbf{F}_\ell} H_1(M_k, \mathbf{F}_\ell)$$

and hence, if $H_1(M_k, \mathbf{Q}) \geqslant 1$, it follows from the criterion that

$$\rho_\ell(X_k) \notin \Omega_\ell, \qquad \text{for any prime } \ell.$$

According to (7), it follows that for any $L \geqslant 2$ we have

$$\boldsymbol{P}(H_1(M_k, \mathbf{Q}) \neq 0) \leqslant \boldsymbol{P}(\rho_\ell(X_k) \notin \Omega_\ell \text{ for } \ell \leqslant L) \leqslant (1 + L^A \exp(-k\eta))P(L)^{-1}$$

where the constants A, η are given by Theorem 2 and $P(L)$ is given by (6). We choose $L = \exp(\frac{k\eta}{A})$ (if this is $\geqslant 2$; otherwise, the bound (1) is trivial anyway, by increasing the constant C if need be). From the computation in [DT1, 8.3], we know that

$$\frac{|\Omega_\ell|}{|Sp(2g, \mathbf{F}_\ell)|} = \prod_{j=1}^{g} \frac{1}{1 + \ell^{-j}}. \tag{9}$$

It follows easily that for some constant $a > 0$ we have

$$\frac{|\Omega_\ell|}{|Sp(2g, \mathbf{F}_\ell)|} \geqslant a$$

for any $\ell \geqslant 2$. Hence $P(L) \geqslant a\pi(L)$ where $\pi(L)$ is the number of primes $\ell \leqslant L$. By Chebychev's estimate $\pi(L) \geqslant bL(\log L)^{-1}$ for some (explicit) constant $b > 0$, we deduce that

$$\boldsymbol{P}(H_1(M_k, \mathbf{Q}) \neq 0) \leqslant \frac{2}{ab} \frac{\log L}{L} \leqslant C \exp(-\delta k)$$

for some constant C, δ being any positive real number $< \frac{\eta}{A}$.

To deal with part (2) we must change the choice of Ω_ℓ. In fact we now define

$$\tilde{\Omega}_\ell = \{g \in Sp(V/\ell V) \mid \langle J_\ell, g(J_\ell)\rangle \neq \mathbf{F}_\ell^{2g}\} = Sp(2g, \mathbf{F}_\ell) - \Omega_\ell,$$

so the criterion (8) takes the form

$$H_1(M_k, \mathbf{F}_\ell) = 0 \text{ if and only if } \rho_\ell(X_k) \notin \tilde{\Omega}_\ell. \tag{10}$$

The density of $\tilde{\Omega}_\ell$ is now

$$\frac{|\tilde{\Omega}_\ell|}{|Sp(2g, \mathbf{F}_\ell)|} = 1 - \prod_{j=1}^{g} \frac{1}{1 + \ell^{-j}} = \frac{1}{\ell} + O\Big(\frac{1}{\ell^2}\Big)$$

for $\ell \geqslant 2$ (and fixed g), by Taylor expansion at 0 of

$$x \mapsto \frac{1}{1+x} \cdots \frac{1}{1+x^g}.$$

Hence the well-known asymptotic formula for the sum of inverses of primes $\ell \leqslant L$ gives

$$P(L) = \log\log L + O(1)$$

for $L \geqslant 2$, where $P(L)$ is computed for $\tilde{\Omega}_\ell$ now. By (4), we have

$$\boldsymbol{E}\Big((Q(X_k, L) - P(L))^2\Big) \leqslant (1 + L^A \exp(-k\eta))P(L)$$

where $Q(X_k, L)$ defined by (5) is equal to the number of primes $\ell \leqslant L$ for which $H_1(M_k, \mathbf{F}_\ell) \neq 0$, by (10). This means that if L is small enough, $Q(X_k, L)$ will be close to $P(L)$.

Precisely, we have

$$\boldsymbol{E}\Big((Q(X_k,L)-P(L))^2\Big) \geqslant \frac{1}{4}P(L)^2\boldsymbol{P}\Big(Q(X_k,L)<\tfrac{1}{2}P(L)\Big)$$

by positivity. Let L_0 be large enough that we have $P(L)\geqslant \frac{1}{2}\log\log L$ for all $L\geqslant L_0$ (L_0 exists and depends only on g). Then for $L\geqslant L_0$, we obtain

$$\boldsymbol{P}(Q(X_k,L)<\tfrac{1}{4}\log\log L)\leqslant (1+L^A\exp(-k\eta))P(L)^{-1}\leqslant 2\frac{1+L^A\exp(-k\eta)}{\log\log L}.$$

We select again $L=\exp(\frac{k\eta}{A})$, if this is $\geqslant L_0$ (otherwise the estimate (2) is trivial after increasing the constant C'), and obtain that

$$\boldsymbol{P}(Q(X_k,L)<\tfrac{1}{4}\log bk)\leqslant \frac{4}{\log bk}.$$

with $b=\frac{\eta}{A}$. In other words, with probability at least $1-4(\log bk)^{-1}$, $H_1(M_k,\mathbf{F}_\ell)\neq 0$ for at least $\frac{1}{4}\log bk$ distinct primes, which implies (2).

Now to go from this to the lower bound (3) for the size of $H_1(M_k,\mathbf{Z})$, we argue as follows: if $H_1(M_k,\mathbf{Z})$ is finite, and if $Q(X_k,L)\geqslant \frac{1}{4}\log bk$, then $H_1(M_k,\mathbf{Z})$ has non-zero ℓ-primary parts for at least that many primes, and its size is at least the product of those primes. We don't know how the primes which occur are distributed, but the product involved is at least as large as the product of the first $[\frac{1}{4}\log bk]$ primes. Thus with probability at least $1-\frac{4}{\log bk}$, we have

$$|H_1(M_k,\mathbf{Z})|\geqslant \prod_{\ell\leqslant X}\ell$$

where X is the $[\frac{1}{4}\log bk]$-th prime. Using Chebychev-type bounds again, the k-th prime is at least $fk\log k$ (for $k\geqslant 2$) and the sum of logarithms of primes $\leqslant X$ is at least $f'X$ for $X\geqslant 2$ (for some explicit constants f, $f'>0$), so we have

$$X\geqslant f(\log bk)(\log\log bk),$$

and

$$\prod_{\ell\leqslant X}\ell=\exp\Big(\sum_{\ell\leqslant X}\log\ell\Big)\geqslant \exp(f'X)\geqslant \exp(ff'(\log bk)(\log\log bk))\geqslant k^{\alpha\log\log k}$$

for some $\alpha>0$. Therefore, we have shown that

$$\boldsymbol{P}(\text{Order of } H_1(M_k,\mathbf{Z})<k^{\alpha\log\log k})\leqslant \frac{4}{\log bk},$$

hence (3). □

From the point of view of sieve, the arguments are amusing because two deductions are made from the same sieve by "exchanging" the inclusion/exclusion point of view.

The proof of part (2) is very similar to the standard argument of Turan to prove the result of Hardy and Ramanujan according to which "almost all" integers $n\leqslant X$ have about $\log\log X$ prime divisors (counted without multiplicity). There, however, one can use obvious upper bounds on the size (and number) of prime divisors to ensure that the number is really the truth, not just a lower bound. If the order of $H_1(M_k,\mathbf{Z})$ (or of its torsion part rather) behaves like a "random" integer, we would expect that the fact that there are roughly $\log k$ prime divisors (at least) implies that this integer is of size exponential in k. The author lacks geometric and topological experience to have any idea if this "randomness" is a reasonable expectation.

In the database used in [DT2], containing 10986 distinct hyperbolic 3-manifolds, the maximal size of the torsion subgroup of $H_1(M,\mathbf{Z})$ is 423, and the histogram of the values looks roughly like that of an exponential distribution (with mean approximately 62.92791); however, the number of prime factors doesn't exceed 5, and because it is so small, it's unclear how meaningful a comparison between the experimental data and the number of prime factors of integers sampled according to an approximation to this exponential distribution can be.

References

[DT1] N. Dunfield and W. Thurston: *Finite covers of random 3-manifolds*, Invent. math. 166 (2006) 457–521.

[DT2] N. Dunfield and W. Thurston: *The virtual Haken conjecture: Experiments and examples*, Geometry & Topology 7 (2003), 399–441.

[K1] E. Kowalski: *The large sieve and its applications*, in preparation.

[K2] E. Kowalski: *The principle of the large sieve*, preprint (2006), see `arXiv:math.NT/0610021` or `www.math.u-bordeaux1.fr/~kowalski/principle-large-sieve.pdf`.

Université Bordeaux I - IMB, 351, cours de la Libération, 33405 Talence Cedex, France

E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`