

THE UBIQUITY OF SURJECTIVE REDUCTION IN RANDOM GROUPS

E. KOWALSKI

A famous result of Matthews, Vaserstein and Weisfeiler [MVW] states that, given an almost simple simply-connected algebraic group G/\mathbf{Z} (e.g., $G = SL(n)$ or $G = Sp(2g)$, the symplectic group of size $2g$) and a Zariski-dense subgroup $\Gamma \subset G(\mathbf{Z})$, the induced reduction map

$$\Gamma \rightarrow G(\mathbf{F}_p)$$

is onto for all sufficiently large primes p , the bound depending of course on Γ . This applies in particular to $G(\mathbf{Z})$ itself and to congruence subgroups (matrices congruent to identity modulo some integer, for instance), and even this special case is not particularly easy to prove directly.

A natural question which is not answered by the proof of Matthews, Vaserstein and Weisfeiler (which uses the classification of finite simple groups) nor by the alternate argument of Hrushovsky and Pillay [HP] (based on ultrafilters and methods of model theory) is to quantify this result, i.e., to specify a $p_0(\Gamma)$ such that the reduction map is onto for all $p > p_0(\Gamma)$. This question seems quite subtle: it is not even clear what “simpler” invariants of Γ could be used to express an hypothetical bound for $p_0(\Gamma)$. (C. Hall has observed that $p_0(\Gamma)$ could probably be estimated using the related bound $p_1(\Gamma)$ defined as the smallest prime for which Γ acts irreducibly or semisimply modulo p for primes $p \geq p_1(\Gamma)$, after choosing a faithful irreducible representation $G \rightarrow GL(V)$).

In this simple note, we show that the sieve results developed in [K] together with results of Kantor and Lubotzky easily give some results that suggest that $p_0(\Gamma)$ should be usually pretty small.

More precisely, consider for simplicity the following setting: $n \geq 2$ is fixed, S is a fixed finite symmetric generating set of $SL(n, \mathbf{Z})$, and X_k (resp. Y_k) is a random walk on $SL(n, \mathbf{Z})$ defined by $X_0 = 1$, $X_{k+1} = X_k \xi_{k+1}$ (resp. $Y_0 = 1$, $Y_{k+1} = Y_k \xi'_{k+1}$), where the ξ_k and ξ'_k are uniformly distributed in S . Assume that the double vector $(\xi_k, \xi'_k)_{k \geq 1}$ is jointly independent, so that (X_k) and (Y_k) are independent random walks. For each $k \geq 1$, we consider the subgroup $\Gamma_k = \langle X_k, Y_k \rangle \subset SL(n, \mathbf{Z})$ generated by X_k and Y_k . It is not necessarily the case that Γ_k is Zariski-dense, but failing to do so should only increase the probability that the image of Γ_k by reduction modulo p is a proper subgroup.

However, defining

$$p_2(\Gamma) = \min\{p \geq 2 \mid \Gamma \rightarrow PSL(n, \mathbf{F}_p) \text{ is onto}\}$$

for an arbitrary $\Gamma \subset SL(n, \mathbf{Z})$, we prove:

Proposition 1. *Let n , S and (X_k, Y_k) be as above, and assume that $1 \in S$ in the case $n = 2$. For an arbitrary increasing function $\psi(k)$ defined for $k \geq 1$ such that*

$$\lim_{k \rightarrow +\infty} \psi(k) = +\infty,$$

we have

$$\lim_{k \rightarrow +\infty} \mathbf{P}(p_2(\Gamma_k) > \psi(k)) = 0.$$

Note that we obviously have

$$p_0(\Gamma) \geq p_2(\Gamma), \quad p_0(\Gamma) \geq p_1(\Gamma).$$

On the other hand, the discrepancy between $SL(n, \mathbf{F}_p)$ and $PSL(n, \mathbf{F}_p)$ is not significant and the latter is used merely to simplify the arguments.

Proof. Let $G = SL(n)$. We are going to apply the sieve for random walks in discrete groups developed in [K] with the following data: the sieve setting is

$$(G \times G, \{\text{primes}\}, G \times G \rightarrow G(\mathbf{F}_p) \times G(\mathbf{F}_p)),$$

the siftable set is the probability space Ω underlying (X_k, Y_k) and the map $F : \Omega \rightarrow G \times G$ is simply (X_k, Y_k) . It is easily checked that Property (τ) holds for the requisite subgroups of $G \times G$ with the same (τ) -constant as for G itself: there exists $\varepsilon > 0$ such that for any finite-dimensional unitary representation

$$G \times G \xrightarrow{\rho} GL(V)$$

such that ρ is trivial on $G(\mathbf{Z}/q\mathbf{Z})^2$ for some integer $q \geq 1$, and ρ has no non-zero invariant vector, we have

$$(1) \quad \max_{(s,t) \in S \times S} \|\pi(s,t)v - v\| \geq \varepsilon \|v\|$$

for any non-zero $v \in V$ (this in fact holds with maximum over the smaller generating set $S^{(2)} = (S \times \{1\}) \cup (\{1\} \times S)$ of $G(\mathbf{Z}) \times G(\mathbf{Z})$).

Now let $L \geq 2$ fix any choice of proper subsets $\Omega_\ell \subset G(\mathbf{F}_\ell) \times G(\mathbf{F}_\ell)$ for primes $\ell \leq L$; define

$$H = \sum_{\ell \leq L} \frac{|\Omega_\ell|}{|G(\mathbf{F}_\ell)|^2 - |\Omega_\ell|},$$

the sum over ℓ ranging over primes. The outcome of the group sieve procedure of [K, 3.2] in this context, with the sieve support consisting of primes $\ell \leq L$, is that

$$\mathbf{P}((X_k, Y_k) \pmod{\ell} \notin \Omega_\ell, \text{ for } \ell \leq L) \leq (1 + L^{2n^2} \exp(-ck))H^{-1}$$

for any $L \geq 2$ for some constant $c > 0$ depending essentially on n and the constant ε in (1) (see the proofs of [K, Th. 7.4] and [K, Prop. 7.2]).¹ Note that for $n = 2$, the condition $1 \in S$ is used to avoid parity problems (see [K, Prop. 7.8]).

We select Ω_ℓ to be the set of those $(x, y) \in G(\mathbf{F}_\ell)^2$ such that the images of x and y in $PSL(n, \mathbf{F}_\ell)$ generate $PSL(n, \mathbf{F}_\ell)$. Clearly, the condition $p_2(\Gamma_k) > L$ is equivalent with $(X_k, Y_k) \pmod{\ell}$ not lying in Ω_ℓ for all $\ell \leq L$, and hence

$$\mathbf{P}(p_2(\Gamma_k) > L) \leq \Delta H^{-1}$$

with H computed for those Ω_ℓ .

Now a result of Kantor and Lubotzky [KL, Rem. at end of §2] shows that

$$\frac{|\Omega_\ell|}{|G(\mathbf{F}_\ell)|^2} \geq 1 - \frac{C(\log \ell)^2}{\ell^{n-1}},$$

for all $\ell \geq 2$, where the constant $C \geq 0$ depends on n . Hence we have

$$\Delta \geq \sum_{\ell \leq L} \frac{\ell^{n-1}}{C(\log \ell)^2} \left(1 - \frac{C(\log \ell)^2}{\ell^{n-1}}\right) \gg \frac{L^n}{(\log L)^3}$$

for $L \geq 2$, the implied constant depending only on n .

Next we observe that the conclusion of the proposition is stronger when ψ is smaller, so we may replace $\psi(k)$ with $\min(\psi(k), \exp(\frac{c}{2}kn^{-2}))$ and prove the result for this smaller function, which is still increasing and unbounded. We then take $L = \psi(k)$ in the sieve estimate and derive

$$\mathbf{P}(p_2(\Gamma_k) > \psi(k)) \leq 2H^{-1} \ll (\log \psi(k))^3 \psi(k)^{-n},$$

and the result follows. □

¹ The exponent of L is weaker than what can be done, but chosen for simplicity.

Remark 2. Note that Kantor and Lubotzky use the classification of finite simple groups (see [KL, p. 69]); it is necessary in particular to know that there are few simple groups of a given order (the classification implies there are at most 2, and [LS, Window 2, §7] gives more information about what is known independently of the classification). Moreover, their paper extends the result to classical groups over finite fields, and further work has generalized this to all finite groups of Lie type. With Clozel’s solution of Conjecture (τ), this means Proposition 1 should extend to all almost simple groups at least, possibly by assuming $1 \in S$ to avoid periodicity issues.

Remark 3. What we have here, in effect, is a “very large” sieve, in the classical terminology: the number of excluded residue classes is extremely large. When sieving integers, there is a clever and fairly simple sieve due to Gallagher (the “larger sieve”) which leads to very strong bounds in such setting. However, it seems difficult to adapt it to more general contexts, and moreover when such extensions are possible, it turns out that it is the *number* of excluded classes, rather than the *density*, which matters, and the complements of our Ω_ℓ , though their density is very small, are not that small in terms of cardinality.

Remark 4. The overall structure is vaguely reminiscent of Duke’s result that states that for most elliptic curves E/\mathbf{Q} , the Galois action on torsion points is onto $GL(2, \mathbf{F}_\ell)$ for *all* primes ℓ . There, apart from the sieve, a crucial ingredient is a strong result of Masser and Wüstholz that can be used to show that a prime where the action is not as large as possible is bounded polynomially in terms of the discriminant of the curve – in other words, the analogue of p_0 is *already* bounded.

Remark 5. One can do some numerics about this, for instance using **Magma**, which can compute the subgroup of $GL(n, \mathbf{F}_\ell)$ generated by a list of elements. The two natural numerical experiments are (1) to fix k and sample many random walks of length k , checking then for each one which reductions modulo primes in a given list are onto; (2) to go along one random walk, and at each step, to find the first p for which the reduction is onto. The results are quite boring: in all but incredibly few cases, there is surjection!

REFERENCES

- [HP] E. Hrushovski and A. Pillay: *Definable subgroups of algebraic groups over finite fields*, J. reine angew. Math 462 (1995), 69–91.
- [KL] W.M. Kantor and A. Lubotzky: *The probability of generating a finite classical group*, Geom. Dedicata 36 (1990), 67–87.
- [K] E. Kowalski: *The large sieve and its applications: arithmetic geometry, random walks and discrete groups*, Cambridge Tract in Mathematics, to appear.
- [LS] A. Lubotzky and D. Segal: *Subgroup growth*, Progr. Math. 212, Birkhäuser 2003.
- [MVW] C.R. Matthews, L.N. Vaserstein and B. Weisfeiler: *Congruence properties of Zariski-dense subgroups*, Proc. London Math. Soc. 48 (1984), 514–532.

UNIVERSITÉ BORDEAUX I - IMB, 351, COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`