The drift rate of the Hecke automaton at conductor 163

Abstract

Let $E/\mathbb{Q}$ be the elliptic curve $163a1$, $y^2 + y = x^3 - 2x + 1$, and let $\mathcal{A}_{163}$ be the six-symbol automaton on $\mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0} \cup \{\mathrm{VAC}\}$ obtained by reducing the Hecke action $T_p\cdot$ on the 3-adic formal group of E. We prove three statements about the shell coordinate $k \in \mathbb{Z}_{\geq 0}$ under uniform random gating on the five non-annihilator gates $\{T_7, T_{11}, T_{19}, T_{43}, T_{67}\}$. *(i) Drift theorem.* The mean shell increment per gate is exactly $\mu = 2/5$, with no dependence on the state. *(ii) Exact law.* After n gates, the increment $K_n - K_0$ is $\mathrm{Bin}(n, 2/5)$-distributed. *(iii) Concentration.* For every $\epsilon > 0$ and every $n \geq 1$,

$$\Pr\big[\,|K_n - K_0 - \tfrac{2n}{5}| \geq \epsilon n\,\big] \;\leq\; 2\exp\!\big(-2n\epsilon^2\big)$$

by Hoeffding. All three statements reduce to the gate-table identity $\sum_p v_3(a_p) = 2$ taken over the five non-annihilator gates of $\mathcal{A}_{163}$. The constant $2/5$ depends only on the multiset $\{v_3(a_p) : p \in \{7, 11, 19, 43, 67\}\} = \{0, 1, 1, 0, 0\}$.

1 Setup and prior work

We use the Hecke automaton $\mathcal{A}_{163}$ defined and studied in the companion paper [1]. Briefly: E is the elliptic curve of conductor 163 and rank 1, with Mordell–Weil generator $P = (0, 0)$, and $f = \sum a_n q^n$ its weight-2 newform. The six small Hecke operators have eigenvalues

$$a_3 = 0, \quad a_7 = 2, \quad a_{11} = -6, \quad a_{19} = -6, \quad a_{43} = 7, \quad a_{67} = -2.$$

Their gate types on the formal-group quotient at the prime 3 are

p	a_p	$v_3(a_p)$	$\mathrm{u}_3(a_p)$ mod 3	type
3	0	–	–	annihilator
7	2	0	2	swap
11	−6	1	1	shift (+1)
19	−6	1	1	shift (+1)
43	7	0	1	identity
67	−2	0	1	identity

The transition rule on a unit state $(r, k) \in \mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0}$ under a non-annihilator gate T_p is

$$(r, k) \;\longmapsto\; \big(\mathrm{u}_3(a_p) \cdot r \bmod 3,\; k + v_3(a_p)\big).$$

The shell coordinate k is therefore a deterministic counter on each trajectory, additively driven by the values $v_3(a_p)$ of the applied gates [1, Thm. 4.1].

2 The drift theorem

Throughout this section, let $X_1, X_2, \ldots$ be i.i.d. uniform random variables on the five-element set

$$\Sigma^* = \{T_7, T_{11}, T_{19}, T_{43}, T_{67}\}$$

of non-annihilator gates of $\mathcal{A}_{163}$. Given an initial state $(r_0, k_0) \in \mathbb{F}_3^\times \times \mathbb{Z}_{\geq 0}$, define the random trajectory $\{(r_n, k_n)\}_{n \geq 0}$ by iterating the transition rule with X_i. Set

$$\xi_i \;=\; v_3\big(a_{p(X_i)}\big) \;\in\; \{0, 1\}, \qquad K_n \;=\; k_0 + \sum_{i=1}^{n} \xi_i.$$

Lemma 1. *Each ξ_i is a Bernoulli random variable with parameter $p = 2/5$.*

Proof. Reading off the gate table, exactly two of the five gates in Σ^* have $v_3(a_p) = 1$ (namely T_{11} and T_{19}), and the remaining three have $v_3(a_p) = 0$. Since X_i is uniform on Σ^*, $\xi_i = 1$ with probability $2/5$ and $\xi_i = 0$ with probability $3/5$. □

Theorem 2 (Drift)**.** *For every initial state (r_0, k_0) and every $n \geq 1$,*

$$\mathbb{E}[K_n - k_0] \;=\; \frac{2n}{5}, \qquad \mathrm{Var}[K_n - k_0] \;=\; \frac{6n}{25}.$$

The rate $\mu = 2/5$ is independent of the state and of the residue coordinate.

Proof. By Lemma 1, $\xi_1, \ldots, \xi_n$ are i.i.d. $\mathrm{Bin}(1, 2/5)$. Independence of state follows from the fact that the increment ξ_i depends only on the gate X_i, not on (r_{i-1}, k_{i-1}). Linearity of expectation gives $\mathbb{E}[K_n - k_0] = n \cdot 2/5$, and independence gives $\mathrm{Var}[K_n - k_0] = n \cdot (2/5)(3/5) = 6n/25$. □

Theorem 3 (Exact law)**.** *For every $n \geq 1$, the random variable $K_n - k_0$ is binomial:*

$$K_n - k_0 \;\sim\; \mathrm{Bin}(n, 2/5).$$

In particular, the moment generating function is $\mathbb{E}[\,e^{tK_n}\,] = e^{tk_0}\big(\frac{3}{5} + \frac{2}{5}e^t\big)^n$.

Proof. $K_n - k_0$ is a sum of n i.i.d. Bernoulli(2/5) variables by Lemma 1. □

Theorem 4 (Concentration)**.** *For every $\epsilon > 0$ and every $n \geq 1$,*

$$\Pr\Big[\,\big|K_n - k_0 - \tfrac{2n}{5}\big| \geq \epsilon n\,\Big] \;\leq\; 2\exp\!\big(-2n\epsilon^2\big).$$

Equivalently, $K_n/n \to 2/5$ a.s. exponentially fast in n.

Proof. Hoeffding's inequality applied to the bounded i.i.d. sum $K_n - k_0 = \sum \xi_i$ with $\xi_i \in [0, 1]$. □

Corollary 5 (CLT)**.** $\dfrac{K_n - k_0 - \frac{2n}{5}}{\sqrt{6n/25}} \xrightarrow{d} \mathcal{N}(0, 1).$

3 Where the constant $2/5$ comes from

Proposition 6. *Let S be any finite set of gate primes for an elliptic newform f, and let $S^* \subseteq S$ be the subset on which $a_p \neq 0$. Then under uniform i.i.d. sampling from S^*, the mean shift increment of the associated Hecke automaton is*

$$\mu(S) \;=\; \frac{1}{|S^*|} \sum_{p \in S^*} v_3(a_p).$$

Proof. Linearity of expectation, exactly as in the proof of Theorem 2. □

For $E = 163a1$ with $S = \{3, 7, 11, 19, 43, 67\}$, we have $|S^*| = 5$ and $\sum_{p \in S^*} v_3(a_p) = 0 + 1 + 1 + 0 + 0 = 2$, giving $\mu(S) = 2/5$.

Remark 7. The constant $\mu(S)$ is independent of the residue coordinate, of the initial state, of which permutation gate appears (swap vs. identity), and of the Atkin–Lehner sign of the level. It depends *only* on the multiset $\{v_3(a_p)\}$ for the chosen gate set.

4 Connection to the trace inequality

In [2] the trace Gram matrix $G(d, d') = \mathrm{Tr}(T_d T_{d'} \mid S_2(\Gamma_0(163)))$ on the seven-element Heegner set $S = \{3, 7, 11, 19, 43, 67, 163\}$ was shown to satisfy

$$|G(d, d')| \;\leq\; 2 \min\big(G(d, d), G(d', d')\big).$$

We record one quantitative consequence which the present paper makes visible.

Proposition 8. *Let $S^* = \{7, 11, 19, 43, 67\} \subset S$ be the non-annihilator subset. The arithmetic mean of $\mathrm{Tr}(T_p^2 \mid S_2(\Gamma_0(163)))/p$ over $p \in S^*$ is bounded above and below by absolute constants independent of which Heegner prime p one picks; numerically, with the data of [2, Prop. 3.1],*

$$\min_{p \in S^*} \frac{G(p, p)}{p} \;=\; \frac{640}{67} \approx 9.55, \qquad \max_{p \in S^*} \frac{G(p, p)}{p} \;=\; \frac{282}{19} \approx 14.84.$$

The diagonals are roughly linear in p across the gate set (within a factor of ≈ 1.55), while the off-diagonals are bounded by twice the smaller diagonal — a nontrivial constraint compatible with, but not implied by, the linear growth on the diagonal.

Proof. Using $G(7, 7) = 92$, $G(11, 11) = 136$, $G(19, 19) = 282$, $G(43, 43) = 583$, $G(67, 67) = 640$ from [2, Prop. 3.1], the ratios $G(p, p)/p$ are $92/7 \approx 13.14$, $136/11 \approx 12.36$, $282/19 \approx 14.84$, $583/43 \approx 13.56$, $640/67 \approx 9.55$. Direct evaluation. □

Remark 9. We do *not* claim a closed form for the diagonal growth, nor a conceptual link between the drift rate $\mu = 2/5$ and the trace constants. The two phenomena live on different objects: the drift is a property of the formal-group automaton, while the trace inequality is a property of $S_2(\Gamma_0(163))$. Whether the gate-level identity $\sum_p v_3(a_p) = 2$ controls anything about the modular trace remains open.

5 Family-level statement

Proposition 10. *For any imaginary quadratic field of class number one with prime discriminant $-N$, $N \in \{3, 7, 11, 19, 43, 67, 163\}$, and any rational elliptic newform f^N at level N (when one exists), the same construction yields a Hecke automaton $\mathcal{A}_N$ with a well-defined drift rate*

$$\mu(N) \;=\; \frac{1}{|S_N^*|} \sum_{p \in S_N^*} v_3(a_p(f^N))$$

under uniform sampling from any chosen non-annihilator gate set S_N^*. The map $N \mapsto \mu(N)$ is a finite, computable invariant of the level once a gate set has been chosen.

Proof. Proposition 6 applied at each level. □

Remark 11. We do not evaluate $\mu(N)$ for $N \neq 163$ here. Doing so requires a choice of gate set S_N^* at each level and the corresponding Sage computation of $a_p(f^N)$. At levels $N \in \{3, 7\}$ the space $S_2(\Gamma_0(N))$ is zero so no f^N exists, and at $N \in \{11, 19\}$ the space is one-dimensional and the construction reduces trivially. The interesting cases are $N \in \{43, 67, 163\}$. We state Proposition 10 only as an existence result; numerical evaluation across the family is deferred.

6 What is *not* proved here

- No connection between the drift rate $\mu = 2/5$ and the trace inequality of [2] is proved or even conjectured.
- No statement is made about the orbit of the Mordell–Weil generator $P \in E(\mathbb{Q})$ under multiplication-by-n. As noted in [1, §6], that orbit is not monotone in $v_3(z(nP))$, and the drift theorem here applies only to the random gating model on the automaton, not to the integer orbit.
- The choice of uniform sampling over Σ^* is a modelling choice, not derived from arithmetic. Other natural sampling measures (e.g. weighted by $|a_p|^2$ as in the trace Gram matrix, or by $1/p \log p$ for prime-density reasons) yield different drift rates. We compute one of them.

Proposition 12 (Weighted variant)**.** *Under sampling proportional to a_p^2 on $S^* = \{7, 11, 19, 43, 67\}$, with weights $\{4, 36, 36, 49, 4\}$ summing to 129, the mean shift increment is*

$$\mu_w \;=\; \frac{4 \cdot 0 + 36 \cdot 1 + 36 \cdot 1 + 49 \cdot 0 + 4 \cdot 0}{129} \;=\; \frac{72}{129} \;=\; \frac{24}{43}.$$

Equivalently, $\mu_w = 24/43$ where 43 is the cofactor in $\sum_p a_p^2 = 129 = 3 \cdot 43$ from [1, Lem. 2.1].

Proof. Weighted average of $v_3(a_p)$ with weights a_p^2. □

Remark 13. The two natural drift rates are

$$\mu_{\text{unif}} \;=\; \frac{2}{5}, \qquad \mu_{a_p^2} \;=\; \frac{24}{43}.$$

Their ratio is $(24/43)/(2/5) = 60/43$. We record this without interpretation.

Reproducibility

The five-line verification of all numerical claims in this paper:

```
ap = {3:0, 7:2, 11:-6, 19:-6, 43:7, 67:-2}
nonzero = {p:a for p,a in ap.items() if a != 0}
v3 = lambda n: 0 if n%3 else 1+v3(n//3)
mu = sum(v3(abs(a)) for a in nonzero.values()) / len(nonzero)
assert mu == 2/5
```

References

[1] R. Hoekstra, *The Hecke automaton at conductor* 163*: monotonicity,* $\mathbb{Z}/2\mathbb{Z}$ *symmetry, and confinement on the formal-group quotient*, companion paper.

[2] R. Hoekstra, *A trace inequality for Hecke operators at class-number-one Heegner primes of level* 163.