An upper bound and explicit criteria for the finite Galois group of weighted walks with rational coefficients

Ruichao Jiang
University of British Columbia Okanagan

TRANSCENDANCE ET COMBINATOIRE

Model

We shall consider walks in $\mathbb{Z}_+^2$ with conditions

- Step length limited to 1 (nearest-neighbor);
- Transition matrix $p_{i,j}$ $(-1 \leq i, j \leq 1)$ is independent of the current place (homogeneous).

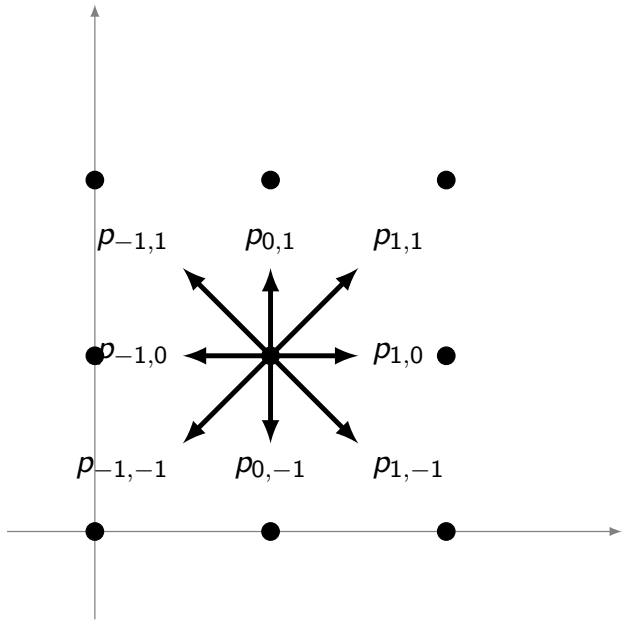

Figure: The model. $p_{0,0}$ is not shown.

Functional equation and kernel

To find the stationary distribution π_{ij} of the model, generating function method is used and the **functional equation** of $\pi(x,y) = \sum_{i,j\geq 1} \pi_{ij} x^{i-1} y^{j-1}$, $x, y \in \mathbb{C}$ and $|x|, |y| < 1$, is obtained

$$Q(x,y)\pi(x,y) = q(x,y)\pi(x) + \tilde{q}(x,y)\tilde{\pi}(y) + \pi_0(x,y), \tag{1}$$

where $Q(x,y) = xy\left(\sum_{i,j} p_{i,j} x^i y^j - 1\right)$ is called the **kernel**. Other terms represent boundary conditions and do not concern us.

Functional equation and kernel

To find the stationary distribution π_{ij} of the model, generating function method is used and the **functional equation** of $\pi(x,y) = \sum_{i,j\geq 1} \pi_{ij} x^{i-1} y^{j-1}$, $x, y \in \mathbb{C}$ and $|x|, |y| < 1$, is obtained

$$Q(x,y)\pi(x,y) = q(x,y)\pi(x) + \tilde{q}(x,y)\tilde{\pi}(y) + \pi_0(x,y), \qquad (1)$$

where $Q(x,y) = xy\left(\sum_{i,j} p_{i,j} x^i y^j - 1\right)$ is called the **kernel**. Other terms represent boundary conditions and do not concern us.
$Q(x,y)$ is *a prior* defined in the same domain as $\pi(x,y)$, but $Q(x,y)$ is a polynomial, so it can be analytically-continued to all $\mathbb{C} \times \mathbb{C}$.
Note that $Q(x,y)$ is a biquadratic polynomial

$$Q(x,y) = a(x)y^2 + b(x)y + c(x) = \tilde{a}(y)x^2 + \tilde{b}(y)x + \tilde{c}(y) \qquad (2)$$

Partial discriminants

If we regard one variable, for example x, in $Q(x, y)$ as a parameter, then $Q(x, y)$ may be seen as a quadratic polynomial with coefficients from the ring $\mathbb{C}[x]$. Analogous to a common quadratic polynomial, the **partial discriminants** of the kernel Q are defined as

$$\Delta_1(y) := \tilde{b}^2(y) - 4\tilde{a}(y)\tilde{c}(y),$$

and

$$\Delta_2(x) := b^2(x) - 4a(x)c(x).$$

Eisenstein invariants

The partial discriminants of the kernel are quartic polynomials. The **Eisenstein invariants** for a general quartic function $f(x) = ax^4 + 4bx^3 + 6cx^2 + 4dx + e$ are

$$D(f) := ae + 3c^2 - 4bd, \tag{3}$$

and

$$E(f) := ad^2 + b^2e - ace - 2bcd + c^3. \tag{4}$$

The name Eisenst

Eisenstein invariants

Where does $D(f)$ and $E(f)$ come from and why they are important to us? We projectivize the quartic f:

$$F(X, Y) = aX^4 + 4bX^3Y + 6cX^2Y^2 + 4dXY^3 + eY^4,$$

which is a bi-variables quartic form. From invariant theory, the algebra of invariants of F is generated by two invariants, which turn out to be D and E. This ring is isomorphic to the ring of modular forms of level 1, with the two generator E and F corresponding to two coefficients in the Eisenstein series E_4 and E_6. Finally, the modular invariants of a complex elliptic curve are $g_2 = 60E_4$ and $g_3 = 140E_6$.

Eisenstein invariants

Schematically,

$$\text{invariant theory} \sim \text{modular form} \sim \text{elliptic curve}$$
$$\text{Eisenstein invariants} \sim \text{Eisenstein series} \sim \text{modular invariant}$$

Of course the above theory are not equivalent. They are just related, like everything in mathematics.
Historically, the expression for our D and E appears first in Eisenstein's study of the zeros of quartic polynomials in 1844. And the name Eisenstein invariants was proposed by Duistermaat.

QRT map

Denote by Q the complex curve defined by $Q(x, y) = 0$. On Q the following maps are defined:
The vertical switch ξ:

$$\xi(x, y) := \left(x, -\frac{b(x)}{a(x)} - y\right).$$

The horizontal switch η:

$$\eta(x, y) := \left(-\frac{\tilde{b}(y)}{\tilde{a}(y)} - x, y\right).$$

Their composition is known as **QRT map** (Quispel, Roberts, and Thompson) in dynamical system community.

$$\delta := \eta \circ \xi. \tag{5}$$

Poncelet theorem

The QRT map is so named by dynamical system community. But it was Poncelet who first found this phenomenon in his **Poncelet theorem** in 1813 in a Russian jail after the failure of Napoleon's war against Russia. The connection between the random walk in positive quarter plane and Poncelet's theorem is carefully investigated in Flato's book [3].

Frobenius invariants

After Eisenstein invaraint

Galois group

Malyshev introduced the group $\mathcal{H} = \langle \xi, \eta \rangle$ and called it the **Galois group** where

$$\begin{aligned} \xi(u(x)) &:= u(x), \\ \xi(y(x)) &:= -\frac{b(x)}{a(x)} - y(x), \\ \eta(w(y)) &:= w(y), \\ \eta(x(y)) &:= -\frac{\tilde{b}(y)}{\tilde{a}(y)} - x(y), \\ \delta &:= \eta \circ \xi. \end{aligned} \tag{6}$$

Galois group

Malyshev introduced the group $\mathcal{H} = \langle \xi, \eta \rangle$ and called it the **Galois group** where

$$\begin{aligned} \xi(u(x)) &:= u(x), \\ \xi(y(x)) &:= -\frac{b(x)}{a(x)} - y(x), \\ \eta(w(y)) &:= w(y), \\ \eta(x(y)) &:= -\frac{\tilde{b}(y)}{\tilde{a}(y)} - x(y), \\ \delta &:= \eta \circ \xi. \end{aligned} \tag{6}$$

Why is this group called Galois group? One answer comes from considering $\mathbb{C}(x, y)$ as a field extension of $\mathbb{C}(x, y)/Q(x, y)$, and to this field extension we can associate a Galois group. This group is also known as the monodromy group.

Finite group

If δ has finite order, then $\mathcal{H}$ has finite order.
But brutal force computation will quickly blow up the complexity. It is better if we can find some invariants encoding this computation. In fact we can enlarge our scheme

$$\text{invariant theory} \sim \text{modular form} \sim \text{elliptic curve}$$
$$\text{Eisenstein invariants} \sim \text{Eisenstein series} \sim \text{modular invariant}$$
$$\text{Frobenius invariants} \sim \text{image of infinity under } \delta$$

This is the rationale of my paper, a corollary of Duistermaat's book [1].

Another history

For the real origin of the QRT map and Galois group a là Malyshev, look at the following

Lemma

Given $b \in E \subset \mathbb{CP}^2$, an elliptic curve, define automorphism $\iota_b(x)$ as the third intersection of the line $\overline{bx}$ with E. If $x = b$ then use the tangent trick. Then ι_b is an inversion on E. Given another point $b' \in E$, then $\delta = \iota_b \circ \iota_{b'}$ is the unique translation on E sending b to b'.

The following is quoted from page 134 of Duistermaat's book
" Lemma 4.2.1 can be found in [Poincaré], together with the observation that if E is defined over $\mathbb{Q}$ and if b, b' are rational points on E, then ι_b and δ map rational points to rational points. Poincaré did not give any reference, but A. Weil observed that the geometric construction of ι_b and δ together with its application to the generation of rational points on a cubic plane curve, had been found in its full generality in the late 1670s by Newton... "

Summary

In summary, the trick of my paper is by cutting the computation by some invariants (Eisenstein invariants, Frobenius invariants). Then applying Mazur's theorem.
All calculational technicalities can be found in Duistermaat's book (however his book is really arcane).
Before we go on, I would like to share some physical thoughts on QRT and Galois group.

Dynamical system and random walk

Here we want to ask: What is in common between dynamical system with QRT and random walks with Galois group?

Dynamical system and random walk

Here we want to ask: What is in common between dynamical system with QRT and random walks with Galois group?
The definitions of QRT and Galois group, despite minor difference (one acts on points on Q, the other one acts on the function field on Q, but we have categorical equivalence between elliptic curve with function field on elliptic curve), they look really like each other.
And as the famous American slang goes, if it looks like a duck, swims like a duck, quacks like a duck, then it is a duck.

Dynamical system and random walk

Here we want to ask: What is in common between dynamical system with QRT and random walks with Galois group?
The definitions of QRT and Galois group, despite minor difference (one acts on points on Q, the other one acts on the function field on Q, but we have categorical equivalence between elliptic curve with function field on elliptic curve), they look really like each other.
And as the famous American slang goes, if it looks like a duck, swims like a duck, quacks like a duck, then it is a duck.
A dynamical system is described by its initial condition and a map or a flow describing its evolution.
A random walk, being a Markov process, depends also on an initial condition and a transition matrix (assume homogeneity otherwise a distribution of transition matrix parametrised by positions).

Dynamical system and random walk

Here we want to ask: What is in common between dynamical system with QRT and random walks with Galois group?
The definitions of QRT and Galois group, despite minor difference (one acts on points on Q, the other one acts on the function field on Q, but we have categorical equivalence between elliptic curve with function field on elliptic curve), they look really like each other.
And as the famous American slang goes, if it looks like a duck, swims like a duck, quacks like a duck, then it is a duck.
A dynamical system is described by its initial condition and a map or a flow describing its evolution.
A random walk, being a Markov process, depends also on an initial condition and a transition matrix (assume homogeneity otherwise a distribution of transition matrix parametrised by positions).
So it is tempted to regard the transition matrix as the Lie algebra generating the flow.

Hamiltonian system

For a special kind of dynamical system, the Hamiltonian system, the evolution is described via the **Hamiltonian** H by the Hamiltonian equation

$$\begin{aligned} \frac{\mathrm{d}x}{\mathrm{d}t} &= \frac{\partial H}{\partial y}, \\ \frac{\mathrm{d}y}{\mathrm{d}t} &= -\frac{\partial H}{\partial x}. \end{aligned} \tag{7}$$

The **Hamiltonian vector field** is

$$X_H \coloneqq \left(\frac{\partial H}{\partial y}, -\frac{\partial H}{\partial x} \right). \tag{8}$$

More generally, given a symplectic 2-form ω, one say that a vector field X is symplectic if the contraction of X and ω is closed, and that X is Hamiltonian if the contraction is exact. So being Hamiltonian is really special.

Hamiltonian system

It turns out that our kernel function $Q(x, y)$ plays the role of a Hamiltonian.
Duistermaat uses this fact to show that the Riemann surface determined by $Q(x, y)$ is a torus, by first calculating the vector $\left(\frac{\partial Q(x,y)}{\partial y}, -\frac{\partial Q(x,y)}{\partial x}\right)$ to show it vanishes nowhere, then use **Poincaré-Hopf** theorem (among compact smooth surfaces only torus can accommodate a non-vanishing vector field).

Hamiltonian system

It turns out that our kernel function $Q(x, y)$ plays the role of a Hamiltonian.
Duistermaat uses this fact to show that the Riemann surface determined by $Q(x, y)$ is a torus, by first calculating the vector $\left(\frac{\partial Q(x,y)}{\partial y}, -\frac{\partial Q(x,y)}{\partial x}\right)$ to show it vanishes nowhere, then use **Poincaré-Hopf** theorem (among compact smooth surfaces only torus can accommodate a non-vanishing vector field).
In FIM [2] book, the genus is computed by computing ramification properties of branch points, then more or less use **Riemann-Hurwitz** formula (counting fibres twice in 2 different ways).

Symmetry

Since the QRT map and the Galois group are transformation on the Hamiltonian/kernel, they describe a symmetry if their iteration is periodic. In physics, the symmetries of the Hamiltonian is very important. In fact, modern physics goes the other way around, starting with some prescribed symmetries, then find a unique Hamiltonian (or Lagrangian) respecting these symmetries.

Symmetry again

Dynamical systems are everywhere, integrable systems are exceptional. In physics, an integrable system is certain theory that has an explicit solution, e.g. Kepler problem, harmonic oscillator, kdV equation, anti self-dual Yang-Mills theory, etc. It is difficult define integrable system mathematically. I will cite how Hitchin [4] describes it:

- the existence of many conserved quantities
- the presence of algebraic geometry
- the ability to give explicit solutions

In random walk system, we have seen the presence of elliptic curves and Flato's explicit solution. One may wonder what the first criterion means.

Symmetry again

There are two types of symmetries, discrete symmetry and continuous symmetry.
Continuous symmetry is described mathematically by Lie groups. And **Noether's theorem** associates to each continuous symmetry a conserved quantity. For example, if the Hamiltonian is time-independent, then it is invariant under the action of the Lie group $\mathbb{R}$. The conserved quantity corresponding to $\mathbb{R}$ is called **energy**. So our random walk model has conserved energy.

Symmetry again

Unfortunately (or maybe fortunately), the QRT map and Galois group are not continuous. So Noether's theorem does not apply.
Discrete symmetries may have conserved quantities (like parity, helicity in quantum mechanics), but not necessarily. In fact, the QRT map has a conserved quantity, called

Differential Galois theory?

Since some participants of this seminar have interest in differential Galois theory, it is interesting to consider what differential Galois theory can say on this symmetry. I found a paper on this called Picard–Vessiot theory and integrability [5].

Strategy for rational coefficients

Suppose all $p_{i,j}$'s are rational numbers, then the structure of $\mathcal{H}_0$ is completely determined. To reach this conclusion, we adopt a two transformations

1. $\mathcal{J} : Q \to \mathbb{C}/\Lambda$,
2. $\mathcal{J}'^{-1} : \mathbb{C}/\Lambda \to E(\mathbb{C})$,

where Λ is some lattice determined by $p_{i,j}$'s and $E(\mathbb{C})$ is an elliptic in the Weierstrass normal form.
Both $\mathcal{J}$ and $\mathcal{J}'^{-1}$ are defined analytically and given by transcendental functions. However, the composition of them becomes an polynomial function.
Hence, if all $p_{i,j}$'s are rationals, $E(\mathbb{C})$ will also have rational coefficients.

$\mathbb{C}/\Lambda$ and Abel-Jacobi map

- The Hamiltonian vector field $v_H = (\partial Q/\partial y, -\partial Q/\partial x)$ is nonvanishing
- So is the unique Abelian differential ω_H, such that $(\omega_H, v_H) = 1$.
- The lattice Λ is generated by

$$\omega_i = \int_{\gamma_i} \omega_H,$$

where $i = 1, 2$ and γ_i's form a basis for $H_1(Q, \mathbb{Z})$, the first homology group.

- The **Abel-Jacobi map** $\mathcal{J}$

$$\mathcal{J} : p \mapsto \int_{p_0}^{p} \omega \ (\text{mod } \Lambda).$$

is well defined. The dependence on the choice of p_0 can be eliminated by a $\mathrm{PSL}(2, \mathbb{Z})$ action on Λ so that ω_1 is fixed.

$E(\mathbb{C})$ and the uniformozation map

The **uniformization map** $\mathcal{J}'^{-1}$ maps $\mathbb{C}/\Lambda$ to an elliptic curve over $\mathbb{C}$ in the **Weierstrass normal form**:

$$\begin{aligned}\mathcal{J}'^{-1} : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)),\end{aligned}$$

where $\wp$ and $\wp'$ are Weierstrass $\wp$ function and its derivative:

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{(m,n)\neq(0,0)\\ m,n\in\mathbb{Z}}} \left\{ \frac{1}{(z - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right\},$$

and g_2, g_3 are modular invariants

$$g_2(\Lambda) := 60 \sum_{\substack{(m,n)\neq(0,0)\\ m,n\in\mathbb{Z}}} \frac{1}{(m\omega_1 + n\omega_2)^4}$$

$$g_3(\Lambda) := 140 \sum_{\substack{(m,n)\neq(0,0)\\ m,n\in\mathbb{Z}}} \frac{1}{(m\omega_1 + n\omega_2)^6}.$$

Rational coefficients theorem

Both the Abel-Jacobi and the uniformization map are defined analytically. However, their composition is a polynomial function [1]:

$$g_2(Q) := g_2(\Lambda) = D(\Delta_1) = D(\Delta_2), \tag{9}$$

$$g_3(Q) := g_3(\Lambda) = -E(\Delta_1) = -E(\Delta_2), \tag{10}$$

where E and D are Eisenstein invariants and Δ_1 and Δ_2 are partial discriminants of Q.
Hence if Q is a rational biquadratic polynomial, then E has coefficients over Q.

Induced effect of δ

The second ingredient is to look at how the QRT map δ transforms under $\mathcal{J}$ and $\mathcal{J}'^{-1}$. The result is gathered in the following diagram

$$\begin{array}{ccc} Q & \xrightarrow{\delta} & Q \\ \downarrow{\scriptstyle \mathcal{J}} & & \downarrow{\scriptstyle \mathcal{J}} \\ \mathbb{C}/\Lambda & \xrightarrow{\delta^*} & \mathbb{C}/\Lambda \\ \downarrow{\scriptstyle \mathcal{J}'^{-1}} & & \downarrow{\scriptstyle \mathcal{J}'^{-1}} \\ E(\mathbb{C}) & \xrightarrow{\delta^{**}} & E(\mathbb{C}) \end{array}$$

1. δ induces an addition by constant in $\mathbb{C}/\Lambda$, say ω_3

$$\delta^*(z) = z + \omega_3 \pmod{\Lambda}$$

2. δ^* induces an addition by point Ω_3 in $E(\mathbb{C})$,

$$\delta^{**}(P) = P + \Omega_3,$$

where the addition is the usual chord-tangent construction on a Weierstrass normal curve.

Rational point theorem

If the first miracle is that $\mathcal{J}'^{-1} \circ \mathcal{J}$ transform rational Q to rational $E(\mathbb{C})$.
The second miracle is that the rational function δ is also carried to an addition by rational point on $E(\mathbb{C})$.
The coordinates of $\Omega_3 = (X, Y)$ are given by Frobenius invariant

$$X = (p_{0,0}^2 - 4p_{0,-1}p_{0.1} - 4p_{-1,0}p_{1,0} + 8p_{-1,1}p_{1,-1} + 8p_{-1,-1}p_{1,1})/12,$$

$$Y = -\det \mathbb{P},$$

where

$$\mathbb{P} = \begin{pmatrix} p_{1,1} & p_{1,0} & p_{1,-1} \\ p_{0,1} & p_{0,0} - 1 & p_{0,-1} \\ p_{-1,1} & p_{-1,0} & p_{-1,-1} \end{pmatrix}$$

Mazur's theorem and final result

Since $E(\mathbb{C})$ has rational coefficients (Eisenstein invariants) and $\Omega_3 = (X, Y) \in E(\mathbb{Q}) \subset E(\mathbb{C})$ (Frobenius invariants), we have

$$\mathcal{H}_0 \cong \langle \Omega_3 \rangle \subset E(\mathbb{Q}), \tag{11}$$

which means $\mathcal{H}_0$ contains only rational points (good job Newton). Mazur's theorem says for an elliptic curve over $\mathbb{Q}$, its torsion group has only the following possibilities

1. $\mathbb{Z}/N\mathbb{Z}$, where $1 \leq N \leq 10$ or $N = 12$,
2. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$, where $1 \leq N \leq 4$.

Hence $\mathcal{H}_0$ has most order 12, if it has finite order. Then $\mathcal{H}$ can have order at most 24, if it has finite order.

Criteria for order 4 or 6

Using geometric argument, criteria for $\mathcal{H}$ having order 4 or 6 are easily given. Following geometric facts are needed

1. A point on an elliptic curve in Weierstrass normal form has order 2 if and only if it is on x-axis. So $\mathcal{H}$ has order 4 if and only if $\det \mathbb{P} = 0$
2. A point on an elliptic curve has order 3 if and only if it is a flex point, i.e. the determinant of Hessian vanishes at that point. So $\mathcal{H}$ has order 6 if and only if

$$\begin{vmatrix} -12X & 0 & D \\ 0 & 1 & Y \\ D & Y & DX + 3E \end{vmatrix} = 0$$

Division polynomial and criteria for order $4m$ or $4m+2$

For general case, we need division polynomials, which for an elliptic curve in form

$$y^2 = x^3 + ax + b$$

are given by

$$\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \ m \geq 2, \\
\psi_{2m} &= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \ m \geq 3.
\end{aligned}$$

They are called division polynomials because $m|n \Rightarrow \psi_m|\psi_n$ in $\mathbb{Z}[x, y, a, b]$ and (x, y) has order dividing n if and only if (x, y) is a zero of ψ_n.

Division polynomial

These division polynomials may be calculated explicitly, algebraically. But if we work in $\mathbb{C}$, they have a good representation

$$\psi_n(z) = (-1)^{n+1} \frac{\sigma(nz)}{\sigma^{n^2}(z)} \tag{12}$$

where σ is Weierstrass σ function

$$\sigma(z) = z \prod_{w \in \lambda} (1 - \frac{z}{w}) e^{z/w + \frac{1}{2}(z/w)^2} \tag{13}$$

Division polynomial and criteria for order $4m$ or $4m+2$

For our case, we need to transform coordinate to Weierstrass normal form

$$y^2 = 4x^3 - g_2 x - g_3$$

So the division polynomials in Weierstrass normal form are

$$\Psi_1 = 1,$$
$$\Psi_2 = y,$$
$$\Psi_3 = 48x^4 - 24g_2x^2 - 48g_3x - g_2^2$$
$$\Psi_4 = y(64x^6 - 80g_2x^4 - 320g_3x^3 - 20g_2^2x^2 - 16g_2g_3x + g_2^3 - 32g_3^2),$$
$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \ m \geq 2,$$
$$\Psi_{2m} = \frac{1}{y}\Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2), \ m \geq 3.$$

The criteria are given by requiring that corresponding division polynomial vanish at $\Omega_3 = (X, Y)$.

Example:Criterion for order 8

By using the 4th division polynomial, $\mathcal{H}$ has order 8 if and only if $Y \neq 0$ and

$$64X^6 - 80DX^4 - 320EX^3 - 20D^2X^2 - 16DEX + D^3 - 32E^2 = 0.$$

where $\Omega_3 = (X, Y)$ and D, E are Eisenstein invariants.

Reference

[1] J. Duistermaat. *Discrete Integrable Systems*. Springer, 2010.

[2] G. Fayolle, R. Iasnogorodski, and V. Malyshev. *Random Walks in the Quarter Plane*. Springer, 2 edition, 2017.

[3] L. Flato. *Poncelet theorem*. Springer, 2010.

[4] N. J. Hitchin, G. B. Segal, and R. S. Ward. *Integrable systems*. Oxford Graduate Texts in Mathematics. Oxford University Press, 1999.

[5] J. J. Moralez-Ruiz. Picard–vessiottheoryandintegrability. *Journal of Geometry and Physics*, 87:314–443, 2015.