

Structure Computer :

離散力学系の構造に関する問いに、証明書付きの厳密な答えを返すシステム

Yuta Ogura

Independent researcher

第 1 版 — 2026 年 10 月

概要

Structure Computer は、有理写像で与えられる離散力学系についての構造に関する問い（とりわけ「状態 s から状態 t には何歩で着くか、あるいは決して着かないか」）に、有限体上と有理数上で厳密に答え、すべての答えに、計算したプログラムを信頼せずに独立の検査器が確かめる証明書を付ける。Lyness 写像、Euler のコマの Kahan–Hirota–Kimura 離散化、面積を保つ線形写像、双曲測地線の Kahan 離散化については、答えは Lean で証明した定理にもとづき、保存量の等位集合に付随する群の離散対数として計算される。 10^{17} 個の状態を持つ軌道についての問いが 1 秒未満で解け、 $\mathbb{Q}$ 上では反復では得られない答え「決して」も得られる。計算し、証明書を作り、独立に検査し、すべての結果に保証の種類を付けるという同じ方針を、次の十一の問いにも適用する。可逆性、周期構造、可積分性、保存量の発見と検証、ホロノミー、整数不変量の復元、道と系の同値、共役に沿った検査済みの結果の輸送、力学の型理論の閉じた項の評価である。系は名前か短いテキストファイルで与え、見慣れない座標で書かれた系も、アフィン座標変換で既知の族に移るならその族として認識され、変換は証明書に記録されて検査器が検証し直す。 $\mathbb{F}_q$ 上の Lyness 写像については検査器が Lean で書かれ健全性を証明された第二の形で存在する。長い反復は、オプションとして、ミリ秒単位で検証できる STARK 証明で証明することもできる。小さい体上の総当たりとの比較では 12,156 組の状態で、軌道を実際にたどって得た正解と一致し 5,950 通の証明書が検査器を通った。改竄試験では改変した 1,363 件をすべて検査器が却下した。Lean の検査器と独立の検査器は、両方が読めた範囲で、2,004 通の証明書と 14,025 件の改変について判定が一致した。2 コアの機械で、 $\mathbb{F}_{2^{61}-1}$ 上 7.9×10^{15} 歩先にある Lyness の状態の歩数が、証明書の作成と検査を含めて 0.4 秒で求まる。

目次

1	序論	2
1.1	問題	2
1.2	設計の原則	3
1.3	構成	3
2	問い、答え、種類	4
3	アーキテクチャ	4
3.1	構成要素	4
3.2	一つの答えの流れ	5

4	証明書	5
5	検査器	6
5.1	$\text{Id}(s, t)$ について検証するもの	6
5.2	Lean 検証済みの検査器	7
6	答えの根拠	7
7	正則性	7
8	有理数上	8
9	系ファイルと認識	8
9.1	記述言語	8
9.2	式どおりの認識とアフィン座標変換を許す認識	9
10	十一の問い	9
11	長い歩きの STARK 証明	10
12	インターフェースとバンドル	10
13	評価	11
13.1	正しさ	11
13.2	性能	11
14	関連研究	12
15	範囲と今後	12

1 序論

1.1 問題

状態が固定された有理な規則 σ で一歩ずつ変わる。与えられた状態 t に s から着くか、着くなら何歩でか、軌道に沿って何がかわらないか、規則は逆向きに回せるか、といったことが問われる。

既存の道具はこれらに部分的にしか答えない。浮動小数点のシミュレーションは軌道をしばらく追うが、状態を厳密に比較できず「決して」とは言えない。数式処理系は $\mathbb{F}_q$ や $\mathbb{Q}$ 上で厳密に反復するが、 $\mathbb{F}_{2^{61}-1}$ 上の軌道は 10^{17} 個の状態を持ちうるし $\mathbb{Q}$ 上の軌道は一般に無限である。結果が得られても、第三者が計算をやり直さずに確かめられる証拠は残らない。証明支援系は写像についての定理を証明するものであり、特定の状態の組について答えを計算するものではない。有限体上の力学系の算術的な方法は周期の統計から可積分性を検出するもので、個々の軌道については何も言わない。

Structure Computer は、これらの問いに (i) 厳密で、(ii) 系が理論を持つ族に属する限り、軌道の長さではなく群の位数の算術で決まる時間で計算され、(iii) 証明書を伴い、(iv) 小さく依存のない独立の検査器 (Lyness 写像については、さらに Lean で正しさを証明した第二の検査器) が検証し、

(v) 保証の種類を明示した答えを出すために作られた。表 1 に既存の道具との位置関係を示す。

	厳密	証明書	「決して」	大きい $\mathbb{F}_q$	$\mathbb{Q}$	形式証明	速さ
浮動小数点シミュレーション	×	×	×	—	×	×	非常に速い
数式処理 (反復)	○	×	小さい $\mathbb{F}_q$ のみ	×	×	×	反復に縛られる
証明支援系	○	証明	述べた定理 のみ	—	—	○	計算しない
算術力学系 (周期の統計)	○	×	×	統計的	×	×	速い
線形写像の軌道の証明書 [4]	○	○	○	線形のみ	×	×	反復に縛られる
Structure Computer	○	○・検査 済み	○	○	○	○	群の位数で決まる

表 1 軌道の問いについて各種の道具が提供するもの。「大きい $\mathbb{F}_q$ 」は q が 2^{61} 程度 (Euler のコマでは 2^{45} 程度) まで軌道を反復せずに答えること、「 $\mathbb{Q}$ 」は有理数上で (ある素数が状態を分けるとき) 無条件の否定の答えを返せること。

1.2 設計の原則

計算し、それから検査する。 答えを出すエンジンは信頼しない。すべての答えが後で別のプログラムにより証明書だけから検査されるので、エンジンはどんなアルゴリズム、どんな発見的手法、速いネイティブのカーネルも使える。信頼される部分は検査器である。検査器は小さく、標準ライブラリだけで書かれ (STARK 証明の検証だけは Rust の検証器に委ねる)、一つの族については Lean で書いて健全性を証明した第二の検査器がある。

定理は族ごとに一度だけ証明する。 問いが尋ねられたとき Lean は走らない。「検査器が確かめる条件が成り立てば答えは正しい」という主張を族ごとに一度証明し [6]、証明書は定理を引用して検査器が確かめるデータ (位数、対数、証拠) を運ぶ。

すべての答えに種類がある。 **確定** (定理を適用し全仮定を検査)、**確率的に確定** (STARK 証明により、明記した誤り上界まで)、**復元値** (明記した上界の下で一意)、**統計的** (統計量つきの推定)、**結果なし** (主張なし、理由つき)。確かめられないものを確定と呼ばず、解消できなかった前提は明記し、黙って仮定しない。

ローカルで、点検できる。 すべて利用者の機械の上で動作し、ネットワークには接続しない。証明書は公開されたスキーマを持つ JSON で、証明書のバンドルは検査器と Lean のソースとともに配布され、オフラインで検査される。

1.3 構成

2–6 節で問い、アーキテクチャ、証明書、検査器を、7–12 節でそれ以外の仕組みを、13 節で評価、14 節で関連研究、15 節で範囲を述べる。

2 問い、答え、種類

系とは状態空間 K^n と部分有理写像 σ およびその部分的な逆である。状態が**正則**とは、前向きの軌道も後ろ向きの軌道も写像が未定義の点に当たらないことをいう。状態 s, t についてシステムは

$$\text{Id}(s, t) = \{n \in \mathbb{Z} : \sigma^n s = t\}$$

を計算する。これは前後両方向のすべての歩数の集合であり、力学系の作用亜群における s から t への射の集合、また型理論の亜群モデルにおける s, t の間の恒等型の解釈でもある [6]。答えは次のどれかである。

- **歩数** (r, M) : すべての整数 n について、 $\sigma^n s = t$ と $n \equiv r \pmod{M}$ が同値。
- **道なし** : すべての整数 n について $\sigma^n s \neq t$ 。
- **正則でない** : s は正則でない。答えは前向きの連鎖の長さ、連鎖上で $f^n s = t$ ($n \geq 0$) または $g^{-n} s = t$ ($n < 0$) となる (高々一つの) n を与える。ここで f, g は部分写像とその逆である。

$\mathbb{F}_q$ 上では q は任意の奇素数 (ネイティブのカーネルで 2^{63} 未満、参照実装では任意)。 $\mathbb{Q}$ 上では $|n|$ の上界 B つきで問い、「道なし」は無条件 (ある素数が状態を分ける) か「上界の範囲で」かである。

$\text{Id}(s, t)$ の種類は**確定**、**確率的に確定** (STARK 証明が歩きを置き換えるときだけ)、**結果なし** である。確定の答えは、軌道を歩くことも 7 節の定理で正則性を決めることもできなかったときに限り、前提「 s と t は正則」を付けたまま返される。

3 アーキテクチャ

3.1 構成要素

エンジン (Python)。 状態の組を分類し (族、等位、定理の場合)、位相・位数・離散対数を計算し、証明書を組み立て、問いを走らせる。記号計算 (逆写像、認識) は SymPy。

カーネル (Rust、外部依存なし)。 パイプ越しに行単位の JSON でやり取りする別プロセス。軌道の歩き、零空間、楕円曲線上と $\mathbb{F}_q^\times, \mathbb{F}_{q^2}^\times, \mathbb{F}_{q^4}^\times$ の位数と対数、根、素因数分解、素数判定。 2^{63} 未満の任意の奇素数に Montgomery 演算、Mersenne 素数 $2^{31} - 1$ と $2^{61} - 1$ にはシフトと加算。各系は一步の計算を小さな直線プログラム (straight-line program) として記述し、カーネルが実行する。カーネルはエンジンと同じく信頼されない。すべての演算の純 Python の参照実装が残り、試験で両者を比べる。

検査器 (Python、標準ライブラリのみ)。 $\mathbb{F}_q$ 上と $\mathbb{Q}$ 上の $\text{Id}(s, t)$ 、十一の問い、STARK の主張の証明書を検証する。エンジンを決して読み込まず、自身のプロセスで走り、系ファイルを自身のパーサで読む。

Lean の開発。 証明書が引用する定理 (1,146 個、sorry なし、標準の公理のみ) と、健全性の証明つきの Lean の検査器。

STARK の証明器と検証器 (Rust)。 Plonky3 の上に作った Mersenne-31 上の Circle STARK [3]。主張は「すべての一步が定義されて $\sigma^n s = t$ 」。 $q = 2^{31} - 1$ のときにオプションで使える。

インターフェース。 Python API、標準入出力上の行指向 JSON プロトコル、ジョブつきのローカル HTTP サービス、コマンドライン。Web フロントエンドは HTTP サービスを使う。

3.2 一つの答えの流れ

1. 要求（系、パラメータ、状態、体または上界、オプション）を検証し、乱数の種を生成する。
2. エンジンが証明書の本体を計算する：分類、位相のデータ、素因数分解つきの位数、対数または非所属の証拠、正則性の項目、主張。
3. 本体を、問い・主張・種類・前提・引用定理を改めて記した外枠（エンベロープ）で包む。
4. 検査器が別プロセスで、状態から場合を計算し直し、すべての補助データを検証し、主張を計算し直して比べる。
5. 検査器が却下するかエンジンが失敗すれば、新しい種で参照実装によりもう一度だけ計算し直す（ $\mathbb{Q}$ 上では別の素数でも）。それも失敗すれば、答えは検査器の理由つきの**結果なし**。未検査の結果は明示的な要求があるときだけ、印をつけて返す。
6. 型つきの結果と検査済みの証明書を返す。

4 証明書

すべての証明書は公開された JSON Schema を持つ JSON 文書である。

■**外枠。** すべての問いのすべての答えは同じ外枠を持つ。問い、答えた入力、種、結果（種類、値、前提、誤り上界、仮定、統計量、理由）、本体のどこかで引用されるすべての定理の一覧、本体、エンジンの情報、検査のされ方。検査器は本体をその問いの規則で検証し、次に外枠の記述が、本体が証明する内容と過不足なく一致することを要求する。

■ **$\mathbb{F}_q$ 上の $\text{Id}(s, t)$ の本体。** 系とパラメータ、 q, s, t 。方法（位相、不変量、固定点、空虚な等位、歩いた軌道、共役、認識した系ファイル）。適用される定理の**場合**（たとえば楕円的な Lyness の等位、Euler のコマの場合 A）。定理。主張。前提（解消されていれば null）。補助データ：等位と平行移動の点（Euler のコマではさらに縮尺、巡回置換、符号変換の選択）、位相の群の各成分—楕円曲線、 $\mathbb{F}_q \cdot \mathbb{F}_{q^2} \cdot \mathbb{F}_{q^4}$ の乗法群、加法群、 $\mathbb{Z}/2$ 因子—について平行移動の点の素因数分解つきの位数と、対数または非所属の証拠。各状態の**正則性**の項目：歩いた閉路（周期つき）、歩いた連鎖（長さつき）、位相の判定（等位の詰まる状態が剰余類にない。詰まる候補とその証拠つき）、非正則性（詰まる候補が剰余類にある。対数つき）と部分軌道。系ファイルや共役では、一致（座標変換 $u = Mv + c$ を含む）を記録し、変換した状態についての族の証明書を含む。リスト 1 は [6] の例 A.1 の本体の抜粋である。証明書全体は 4.3 kB。

■ **$\mathbb{Q}$ 上の本体。** 有理数のデータと上界。使った素数（それぞれ還元した問いの証明書つき）。中国剰余の結合。候補の歩数の厳密な反復。主張。引用する還元定理。

■**他の問いの本体。** 十一の問いが共有する一つの形式：問い、系とそのソース、入力、種類、主張、補助データ、定理、そして種類が要求する誤り上界・仮定・統計量・理由。

リスト 1 steps の証明書の本体 (抜粋)。P は [6] の平行移動の点 Q 。

```
{
  "system": "lyness", "params": {"a": 3},
  "q": 2305843009213693951, "s": [2, 5],
  "t": [813066766938016773, 992646061924517494],
  "method": "phase", "case": "lyness/elliptic",
  "theorems": [...],
  "presupposition": null,
  "data": {"k": 18, "P": [36, 2305843009213692799]},
  "components": [
    {
      "type": "ec", "order": 576460752629115698,
      "order_fac": [[2,1],[6673,1],[3612179,1],[11957747,1]],
      "log": 7863588611074867
    }
  ],
  "claim": {"kind": "steps", "residue": 7863588611074867,
    "modulus": 576460752629115698},
  "regularity": {
    "s": {"status": "phase", "k": 18,
      "stuck": [{
        "dir": "F", "z": [26, 2305843009213693948],
        "components": [{
          "type": "ec", "order": 576460752629115698,
          "order_fac": [...], "witness": 2
        }],
        "dir": "G", "z": [2305843009213693948, 26],
        "components": [...]}
      ]},
    "t": {...},
    "kind": "certain"
  }
}
```

5 検査器

5.1 $\text{Id}(s, t)$ について検証するもの

位相の方法による証明書について、検査器は証明書だけから：

- q と素因数分解のすべての素数の素数性を検証する（使う体の大きさをはるかに超えて有効な決定的 Miller–Rabin。Lean の検査器は代わりに Pratt の証明書を使う）。
- 状態から場合を計算し直し（Lyness 写像では等位、曲線、判別式、非退化の条件、 $\varphi(s), \varphi(t)$ の非特異性。Euler のコマでは定義式に対する縮尺、等位、曲線、場合。線形の系では固有値の方程式）、述べられた場合と一致しない証明書を却下する。
- すべての位数（すべての素数 $\ell \mid N$ について $NP = 0$ 、 $(N/\ell)P \neq 0$ 。乗法群ではさらに $N \mid |K^\times|$ ）、すべての対数（べき乗で）、すべての非所属の証拠（曲線では、差が ℓ 部分で位数が違うか、網羅的な baby-step giant-step によりそこで巡回部分群の外にあること。巡回群では差 c について $c^N \neq 1$ ）を検証する。
- 成分の類を中国剰余定理で合わせ、主張された (r, M) に等しいことを要求する。小さい剰余では $\sigma^r s = t$ も直接反復する。等位による「道なし」では保存量を計算し直す。
- 等位の詰まる候補を自分で計算し直し（Euler のコマでは根の一覧が完全であることを $\gcd(P_D P_P, m^{|K|} - m)$ (P_D, P_P は [6] の詰まる状態の多項式) の次数で確かめ平方根を検査

する)、各証拠または対数を検証し、歩いた閉路と連鎖を歩き直し、 s が正則と示され t が正則と示されるか道が反復されたときだけ前提を外すことを認める。

歩いた軌道では歩き直す。系ファイルや共役ではまず多項式恒等式で一致を導き直し (9 節)、次に内側の証明書を検査する。十一の問いでは 10 節の規則を適用する。

5.2 Lean 検証済みの検査器

$\mathbb{F}_q$ 上の Lyness 写像については検査器が第二の形でも存在する。実行時に Mathlib を使わない Lean で書かれ、健全性定理を伴う。受理するなら q は素数で、主張は Lean の開発で定義された $\mathbb{Z}/q$ 上の Lyness の流れについて真である。すなわち、**歩数**では正則状態について $\sigma^n s = t \iff n \equiv r \pmod{M}$ 、**道なし**ではどの n も成り立たないこと、**正則でない**では s が正則でなく述べられた連鎖の長さの部分軌道を持つこと。証明済みの Lucas 判定で Pratt の証明書 [7] を検証し、Mathlib の群演算に等しいと証明したアフィンな加法公式を使い、楕円的な等位と結節点を持つ等位を、正則性のすべての判定結果も含めて扱う。他の場合は未対応として独立の検査器に委ねる。二つの検査器はどの証明書についても並べて走らせられる。

6 答えの根拠

答え	根拠
楕円的・結節点の等位上の $\mathbb{F}_q$ 上の Lyness 写像の $\text{Id}(s, t)$ 、Lean の検査器で検査	Lean のカーネルと Mathlib、Lean の検査器の健全性定理
それ以外のすべての $\text{Id}(s, t)$ (可約な等位、Euler のコマ、線形の系、 $\mathbb{Q}$) 十一の問い	独立の検査器による場合と補助データの計算し直しと、ちょうどその条件の下で結論を述べる Lean の定理 独立の検査器の問いごとの規則 ($\mathbb{Q}$ 上の恒等式の再証明、列挙した全状態の一步の再計算、階数の再計算) と引用する定理
STARK 証明付きの答え (確率的に確定)	Plonky3 の検証器と、検査器が系そのものから作る制約系、明記した誤り上界

表 2 答えの種類ごとの根拠。エンジンとカーネルはどこにも現れない。

7 正則性

有理写像は分母が消えるところで未定義で、軌道がそのような点に達する状態は正則でなく、平行移動の定理の対象外である。システムはまず各方向に有界の距離を歩く。軌道が閉じれば正則であることが確定し、詰まる状態は歩いた連鎖付きの「正則でない」を与える。大きい q では [6] の位相の判定を適用する。Lyness の等位では二つの詰まる状態 $F = (c, -a)$ 、 $G = (-a, c)$ 、 $c = -(ka + 1 - a)/(1 - a)$ ($a \neq 1$) が明示的で、 s が正則であることと、どちらも剰余類 $\varphi(s) + \langle Q \rangle$ にないことは同値である。したがって二つの離散対数 (または非所属の証拠二つ) で、正則か否かを判定できる。Euler のコマでは詰まる候補は、乗数 m (等位 $\alpha \in \mathbb{P}^2$ について $y(u) = m\alpha$ 。[6] 参照) の次数 ≤ 3 、 ≤ 4 の二つの多項式の根 m について $u_i = \pm\sqrt{1 - m\alpha_i}$ となる高々 56 個の状態

で、 $\mathbb{F}_q$ または $\mathbb{F}_{q^2}$ での根の抽出で見つかる。詰まる候補のどれも剰余類になれば s は正則、剰余類にある候補が詰まっていて、しかも反対向きに二歩進めるなら正則でない。残る場合はシステムは数歩歩き、それでも決まらなければ、前提を明記して答えを返す。

位相で正則でないと示された Lyness の状態について、答えは部分軌道を含む。前向きの連鎖は非負の対数が最小の詰まる状態で終わり、 t に着くのは、 t の対数が非負の値として定まり、その値より小さいときに限る ([6] の例 A.2. 8.8×10^{17} 個の状態の連鎖で t は 4.0×10^{17} 番目)。検査器は詰まる候補を計算し直し連鎖の端を導き直す。

8 有理数上

有理数のデータについてシステムは、設定可能な開始点より上の素数を、データが p 整でないか還元した s が正則と示されない素数を飛ばして取り、各素数で還元した問いに答える。ある素数で「道なし」が得られれば探索を終える。[6] の還元定理により状態は $\mathbb{Q}$ 上で決して結ばれない。そうでなければ剰余類を法が上界の二倍を超えるまで中国剰余定理で合わせ、高々一つ残る候補 n を有理数の厳密な反復で確かめるか除外する。検査器もその反復を繰り返す。ある素数での「道なし」を有効とするために、検査器は還元した s がその素数で正則と示されていることを要求する。これがちょうど還元定理の仮定である。 2^{31} より上から始めるのが有用で、位相の判定が通常最初の素数で正則性を決める。

9 系ファイルと認識

9.1 記述言語

名前付きの系 (a の Lyness。 a_1, a_2, a_3, h の Euler のコマ (Kahan–Hirota–Kimura)。 c の振動子。二次形式の E2 (双曲測地線の Kahan 離散化)。共役を通して答える Lyness 型、反転 Lyness、線形、放物的、平行移動の写像) のほかに、系は短いテキストファイルである：

```
name: a rational map of the plane
vars: x, y
params: a = 3, b = 2
map:
  x' = y
  y' = (a + b*y)/x
```

一步は六通りのどれかで与える。任意の `inverse` を伴う `map`。Kahan の刻み幅を伴う二次のベクトル `field`。名前付きの系の `use`。指数 α を伴う `potential` (対数を含みうるポテンシャルの Hessian 計量の α -測地流の Kahan の一步)。 `lagrangian` (離散 Euler–Lagrange の一步)。いくつかの `generator` ブロック (群作用)。任意のブロックで素数の方針、多項式の制約、観測量、対称性 (行列または二次形式)、尋ねる問いを宣言する。意味は書かれたままの式の部分流である。 $\sigma(x) = F(x)$ 、ただし F は x で、逆 G は $F(x)$ で定義され $G(F(x)) = x$ 。零除算は未定義。欠けた逆写像は計算して証明書に記録する。計算の前に静的検査が走る：特異集合、次数、Kahan・測地・Legendre 行列の正則性、宣言した対称性の下の変換性、素数ごとの平方根。

9.2 式どおりの認識とアフィン座標変換を許す認識

書かれたままの式が既知の族のもので、族と同じところで未定義であるファイルは族の定理で答えられ、証明書は一致を記録して族の証明書を含む。エンジンは標本点で候補を当てはめ、分子と分母が多項式として一致し、未定義集合も一致するときだけ受け入れる。検査器はファイルを読み直し両方を検査し直す。

別の座標でだけ既知の族になるファイルも見つける。任意のアフィン座標変換の後の Lyness 写像。固定点を持つ面積を保つアフィン平面写像（そこでの線形写像、または放物的な標準形）。アフィン座標で Euler のコマになる二次の場合。その中心はすべての偏導関数が消える点、軸は斉次部分の $\mathbb{P}^2$ における零点である。候補の変換は、変換した式が同じ未定義集合を持つ書かれたままの族の式であるときだけ受け入れられ、証明書は $u = Mv + c$ を記録する。検査器は $v = M^{-1}(u - c)$ を代入して多項式恒等式を検証する。射影・双有理の共役は与えられたとき検査される（10 節、Q9/Q10）。式は約分した形で書くのがよい。検査器はすべての恒等式を式を展開して導き直すので、共通因子を約分した式は秒、約分していない式は分かかる。

10 十一の問い

$\text{Id}(s, t)$ のほかにシステムは同じ流れで十一の構造の問いに答える。表 3 に挙げる。

表 3: 十一の問いと、それぞれの証明書の内容と検査の仕方。

	問い	計算するもの。検査器が検証するもの
Q1	可逆性	$\mathbb{Q}$ 上の有理恒等式として $G \circ F = \text{id}$ 、 $F \circ G = \text{id}$ を満たす逆 G （確定）。または双有理でない理由——変数での次数 $\neq 1$ 、Jacobian の消滅、被覆変換（確定）。それ以外は小さい素数を法とする衝突の数（統計的）。検査器は恒等式を証明し直し特異集合を計算し直す。
Q2	周期構造	$\mathbb{F}_q$ 上：小さい状態空間では全列挙（素数ごとに確定）、そうでなければ標本の軌道（統計的）。各標本には根拠の種別（歩いて確認、位相の証明書、STARK 証明）を記す。検査器は列挙のすべての状態を一步進め直し標本を検証し直す。
Q3	可積分性	保存量（Q4）とその Jacobian の階数。階数が $\geq n - 1$ なら「可積分」（確定）。そうでなければいくつかの素数での Roberts–Vivaldi の周期統計 [8] と反転子の探索（統計的）。
Q4	保存量	ある次数までの多項式の保存量。2 ⁶² 近くの素数を法とする零空間として見つけ、CRT と有理数復元 [10] で持ち上げ、 $\mathbb{Q}$ 上の恒等式 $P \circ F = P$ として検証（確定）。完全性の証拠と、不変曲線法・Darboux 多項式法による有理保存量。検査器はすべての恒等式を証明し直し階数を計算し直す。
Q5	検証	与えられた式が保存される（恒等式、確定）か、 q を法とする反例の点（確定）。
Q6	ホロノミー	直交対称性を持つ系について、軌道の最初の帰還とそれを実現する群の元。分類、離散対数としての長さ・ねじれ・回転、位数。4 × 4 の Lorentz 型の形式では Hodge スターを通して得る 2 × 2（スピノル）の代表元（確定。STARK 証明つきなら確率的に確定）。

	問い	計算するもの。検査器が検証するもの
Q7	整数不変量	上界の下で剰余から復元した整数の歩数・巻き数・平行移動（復元値。上界の仮定を外せれば確定）。
Q8	道の同値	生成元の二つの語が等しく作用するか。指数和、式の合成、異なる点（確定）、それ以外は標本（統計的）。
Q9	系の同値	アフィン写像の範囲で見つけた共役、または射影・双有理写像として与えられた共役を恒等式として検証（確定）、不変量の指紋（次元、一步のハッシュ、Jacobian、保存量の基底、周期の分解）で反証、または統計的。
Q10	輸送	一方の系の検査済みの結果を、種類が 確定 の共役 φ に沿って他方へ（保存量を φ^{-1} と合成、状態を写し、ホロノミーを共役）、元とともに全面的に検査し直す。
Q11	評価	力学の理論 $(X, s, t, \text{step}, \text{path})$ の閉じた項の亜群モデルでの値。 $\text{step}^n s \mapsto \sigma^n s_0$ （確定）。

系の**ライブラリ**（二つの Hénon 写像、動径方向の Störmer–Verlet の Kepler の一步、McMillan 写像、対称 QRT 写像、三次のキックの標準写像、離散戸田格子）は Q1–Q4 の検査済みの証明書を伴い、問い合わせの系は指紋で照合され、Q9 が確定の共役を見つければ保存された証明書が Q10 で輸送される。

11 長い歩きの STARK 証明

$q = 2^{31} - 1$ では軌道・周期・ホロノミーの問いがオプションを受け付け、検査器が本来繰り返す歩きを Circle STARK [3] で証明し、検査器は代わりに証明を検証する。主張は「すべての一步が定義されて $\sigma^n s = t$ 」で、歩数のカウンタ、すべての除算の逆元の証拠、次の行に適用した逆写像が現在の状態を返すことを持つトレースとして表され、オプションで最小周期、状態の回避、帰還、不変量を表す。制約系は検査器が系そのものから作るので、証明器は何を証明するかを選べない。STARK 証明に基づく答えは、証明の健全性誤差（一つの証明あたり約 2^{-99} ）を誤り上界とする**確率的に確定**である。実測： $2^{20} - 1$ 歩の Lyness の歩きで 498 kB の証明、証明生成 132 秒、検証 0.075 秒（純 Python の検査器による歩き直しは 14 秒）。六変数の E2 の $2^{16} - 1$ 歩で証明生成 12 秒、検証 0.05 秒（歩き直し 2.1 秒）。検証器は改変した入力 13 件すべてを却下し、検査器は証明付きの証明書の改変 25 件すべてを捕らえた。

12 インターフェースとバンドル

各要求に一つの応答が返る。系（名前とパラメータ、または系ファイルの本文）、問い、入力を名指しする JSON の要求が、型付きの結果（種類、値、前提、誤り上界、仮定、統計量、理由）を検査済みの証明書とともに返す。長い計算はジョブとして走る（投入、状態、結果、取消。各ジョブは自身のプロセス）。プロトコルは標準入出力で要求一行ごとの JSON として、またループバックの HTTP でベアラ認証つきで提供される。Python API は同じものを型付きの結果クラス—Certain、ProbablyCertain、Reconstructed、Statistical、NoResult—と、確定より弱いものに例外を投げる関数で提供し、バッチはプロセスプールで走る。 2^{53} を超える整数もすべての経路で厳密に扱

う。バンドルは証明書を検査器、スキーマ、Lean のソース、引用定理と公理の一覧、チェックサムとともに詰め、自身の検査器でオフラインで検査される。

13 評価

13.1 正しさ

- **総当たり。** $q = 11, 13, 17, 19, 23$ の $\mathbb{F}_q$ 上で、すべての族とパラメータのすべての状態を歩いて分類する。分析のすべての場合について正則状態 s を標本にし、標的 t を s の軌道、等位、全体から取る。30% は歩きを飛ばして正則性を位相の判定で確立し、正則でない状態も標本にする。結果：12,156 組、軌道をたどって得た正解との不一致なし。検査器を通した証明書 5,950 通、失敗なし。
- **改竄試験。** 200 通の正しい証明書から、一か所だけを改変した版を複数作り（主張した類、対数、位数、証拠、縮尺、根、場合、状態、詰まる候補、平方根、正則性の状態値。計 1,363 件）：すべて却下。元の却下なし。
- **Lean の検査器と独立の検査器。** 2,004 通の証明書と 14,025 件の改変：両方が読めた証明書での食い違いなし。Lean の検査器は元 1,842 通を受理し改変 12,632 件を却下。
- **大きい体と $\mathbb{Q}$ 。** $q = 2^{31} - 1$ で 48 問、未決定なし、24 問では位相の判定により前提が外れた。 $\mathbb{Q}$ 上では 10007 より上と 2^{31} より上の素数で 22 例、すべて答えが得られ検査を通った。
- **カーネルと参照実装。** 一步、歩き、位数、対数、素因数分解、零空間を 9223372036854775783 までの素数で比べ、すべて一致。
- **一覧と公理。** エンジンが引用するすべての定理（241 個）が Lean の開発に存在し、標準の公理だけに依存する。開発のすべての定理の監査は他の公理を報告しない。
- **エンドツーエンド試験。** 新規インストールから、26 の答えを 10,497 件の正解との比較で検査し、27 の偽の主張を却下し、25 のジョブと、HTTP と API を通した 24 段階を実行して、すべて誤りなし。

総当たり、改竄、大きい体、 $\mathbb{Q}$ 、カーネル、STARK の試験は 2026 年 10 月 22 日に 2 コアの Intel Xeon 2.1 GHz でカーネルと証明器をソースからビルドして再実行し、これらの数字を正確に再現した。Lean の比較は 2026 年 10 月 21 日の全回帰のものである。

13.2 性能

表 4 に [6] 付録 A の十の高度な例題をこの論文のために計算し直した結果を示す（3 回の中央値。起動・計算・独立の検査を含む一コマンドの壁時計時間で、検査は高々 0.2 秒）。比較のため、この機械のカーネルは $\mathbb{F}_{2^{61}-1}$ 上の Lyness の軌道を毎秒 2.6×10^6 歩、 $\mathbb{F}_{2^{40}+15}$ 上の Euler のコマの軌道を毎秒 2.4×10^6 歩で歩く。他の問いは 0.1–0.6 秒（周期統計を伴う Q3 は 12 秒）。対照として、 $a = 1$ （周期 5）の Lyness 写像の浮動小数点の反復 200,000 歩は 5 の倍数で s から 5.6×10^{-17} 以内に来るが 40,000 回のどれでも等しくならず、したがって $\sigma^n s = t$ を決められない。

	系、体	答え	反復なら	時間 [秒]
1	Lyness $a=3$, $\mathbb{F}_{2^{61}-1}$	$n \equiv 7.86 \times 10^{15} (5.76 \times 10^{17})$	96 年	0.39
2	同じ	正則でない。 t は $n = 4.04 \times 10^{17}$	1.1×10^4 年	18.4
3	同じ、同じ等位	道なし	2,300 年	0.48
4	Lyness $a=3$, $\mathbb{Q}$, $(3, 7) \rightarrow (7, 3)$	道なし (素数 10009)	不可能	0.19
5	Euler のコマ $(1, 2, -3, \frac{1}{2})$, $\mathbb{F}_{2^{40}+15}$	$n \equiv 1.37 \times 10^{11} (2.75 \times 10^{11})$	16 時間	0.35
6	同じ、 $\mathbb{Q}$	道なし (素数 10039)	不可能	0.26
7	同じ、 $\mathbb{F}_{2^{40}+15}$, $(3, 1, 4) \rightarrow (-3, -1, 4)$	道なし	32 時間	0.42
8	平面の写像 (アフィン Lyness), $\mathbb{F}_{2^{61}-1}$	1 と同じ	96 年	0.44
9	同じ、 $\mathbb{Q}$	道なし	不可能	0.26
10	三変数の場 (アフィン Euler のコマ), $\mathbb{F}_{2^{40}+15}$	5 と同じ	16 時間	0.41

表 4 高度な例題。「反復なら」は実測の速さで反復により答えを確立する時間 ($\mathbb{F}_q$ 上の「道なし」では軌道一周。 $\mathbb{Q}$ 上では有限の反復では足りない)。

例 2 が唯一遅い場合で、時間はその等位の群のデータに費やされる。平行移動の点の位数は $3 \cdot 29 \cdot 859 \cdot 30854415206297$ で、検査自体は高々 0.2 秒である。今日実用的な体の大きさは Lyness 写像で $q \leq 2^{61}$ 、曲線が $\mathbb{F}_{q^2}$ 上でしか定義されないことのある Euler のコマで $q \leq 2^{45}$ である。

14 関連研究

証明書つきアルゴリズム (certifying algorithm) [5] は、各出力とともに、簡単な検査器で検証できる証拠を返す。本稿の証明書はこの種のもので、二つが加わる。検査器の受理条件が Lean で証明した定理の仮定であること、一つの族については検査器自身が証明されていること。信頼できないソルバの証明書を検証済みの検査器で確かめる手法は、SAT [11]、停止性 [9]、最近では Markov 決定過程 [2] について知られている。我々の知る限り、有理写像の軌道や、証明書の中での楕円曲線の算術を対象とするのはこれが初めてである。証拠を数式処理で見つけ証明支援系で検査する組合せは、Mathlib の `polyrith` でも用いられている。STARK による長い反復の簡潔な証明は検証可能遅延関数 [1] や仮想機械の証明系で標準であり、本システムでは検査を速めるためのオプションにすぎず、**確定**の答えの根拠にはならない。**線形**写像の $\mathbb{F}_p$ 上の到達時刻の証明書を独立の検査器つきで出すものが最近現れた [4]。本システムは拡大体上と有理数上の非線形の可積分写像を扱い、楕円曲線の算術を用い、形式的に検証された定理に立脚し、反復せずに答える。Roberts と Vivaldi [8] の可積分性の算術的検出は Q3 が統計的な判定の一つとして使う。数学的な理論は [6] で述べた。

15 範囲と今後

定理が扱うのは四つの族とそのアフィン共役であり、他の系は有界の反復で答える。認識はアフィン座標変換までで、射影・双有理の共役は与えられたとき検証する。Euler のコマは $q \approx 2^{45}$ まで実用的である。計画：定理を他の QRT 写像と高次元の Kahan 離散化へ広げること、Euler のコマの点の数え上げ、Lean 検証済みの検査器を残る族と $\mathbb{Q}$ に広げること。

AI の利用について

このシステムと本稿は AI アシスタント (Claude、Anthropic) が中心的な役割を担って作られた。目標の設定、何を作るかの決定、設計上の決定、結果の確認は著者が行い、著者の指示の下で AI アシスタントがエンジン、カーネル、検査器、Lean の開発、試験の大部分と本稿の本文を書き、13 節の実測を行った。内容の責任は著者にある。

謝辞

システムは Lean 4、Mathlib、HoTTLean、SymPy、Plonky3 の上に築かれている。その貢献者に感謝する。

参考文献

- [1] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In *Advances in Cryptology – CRYPTO 2018*, volume 10991 of *Lecture Notes in Computer Science*, pages 757–788. Springer, 2018. doi: 10.1007/978-3-319-96884-1_25.
- [2] Krishnendu Chatterjee, Tim Quatmann, Maximilian Schäffeler, Maximilian Weininger, Tobias Winkler, and Daniel Zilken. Fixed point certificates for reachability and expected rewards in MDPs. arXiv:2501.11467, 2025.
- [3] Ulrich Haböck, David Levit, and Shahar Papini. Circle STARKs. Cryptology ePrint Archive, Paper 2024/278, 2024.
- [4] Ruge Lin. Algebraic-Loop-Certificates: certificates for reachability times and periods of linear maps over $\mathbb{F}_p$. <https://github.com/GoGoKo699/Algebraic-Loop-Certificates>, 2026. Software repository.
- [5] Ross M. McConnell, Kurt Mehlhorn, Stefan Näher, and Pascal Schweitzer. Certifying algorithms. *Computer Science Review*, 5(2):119–161, 2011. doi: 10.1016/j.cosrev.2010.09.009.
- [6] Yuta Ogura. Step counts in integrable rational maps as discrete logarithms: phases, regularity and reduction, formalised in Lean. Companion paper, same site, 2026.
- [7] Vaughan R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4(3):214–220, 1975. doi: 10.1137/0204018.
- [8] John A. G. Roberts and Franco Vivaldi. Arithmetical method to detect integrability in maps. *Physical Review Letters*, 90(3):034102, 2003. doi: 10.1103/PhysRevLett.90.034102.
- [9] René Thiemann and Christian Sternagel. Certification of termination proofs using CeTA. In *Theorem Proving in Higher Order Logics – TPHOLs 2009*, volume 5674 of *Lecture Notes in Computer Science*, pages 452–468. Springer, 2009. doi: 10.1007/978-3-642-03359-9_31.
- [10] Paul S. Wang, M. J. T. Guy, and J. H. Davenport. P-adic reconstruction of rational numbers. *ACM SIGSAM Bulletin*, 16(2):2–3, 1982. doi: 10.1145/1089292.1089293.

- [11] Nathan Wetzler, Marijn J. H. Heule, and Warren A. Hunt. DRAT-trim: Efficient checking and trimming using expressive clausal proofs. In *Theory and Applications of Satisfiability Testing – SAT 2014*, volume 8561 of *Lecture Notes in Computer Science*, pages 422–429. Springer, 2014. doi: 10.1007/978-3-319-09284-3_31.