Integrable equations over finite fields

Tetsuji Tokihiro (Univ. Tokyo, Japan)
Joint work with
Masataka Kanki (Univ. Tokyo, Japan)
Jun Mada (Nihon Univ., Japan)
K.M. Tamizhmani (Pondicherry Univ., India)

Conference on Nonlinear Mathematical Physics: Twenty Years of JNMP,
2013 June 4-14 @ Lie Conference Center, Norway
Research Purposes

• Investigate the dynamical systems over finite fields. We want to realize and study the integrable systems over finite fields.

• Define an integrability of systems over finite fields. We try to construct a criterion which is an analogue of the singularity confinement test or the algebraic entropy.

• Construct significant cellular automata. We identify cellular automata with the discrete dynamical systems over finite fields which have good properties.
Example: a QRT mapping over $\mathbb{F}_p$

An integrable mapping: 
\[
x_{n+1} = \frac{x_n + 1}{x_{n-1} x_n} \quad (x_0 = 1, \ x_1 = 1)
\]

if $x_n \in \mathbb{R}$, \(\{x_n\}_{2 \leq n} = 2, \frac{3}{2}, \frac{5}{6}, \frac{22}{15}, \ldots\)

if $x_n \in \mathbb{F}_3$, \(\{x_n\}_{2 \leq n} = 2, \frac{3}{2} \equiv 0, \frac{0+1}{2 \cdot 0} = \frac{1}{0} \rightarrow \infty, \frac{\infty+1}{0 \cdot \infty} = ?\)

Problem in the nonlinear dynamics over the finite fields:
We cannot determine the time evolution over $\mathbb{F}_p$ when we come to the point at which *division by 0 mod $p$* or *indeterminancy* such as $0/0$, $\infty \pm \infty$ appears.
Previous researches on integrable equations over finite fields

Two approaches:

➢ Study the equations without division terms (such as bilinear forms.)
  [1](d-Schrödinger eq.), [2](dKP eq.)
  → Initial value problem is not always well defined.

➢ Restrict the domain of definition so that indeterminacies do not appear. [3](QRT mapping), [4](d-Toda eq.)
  → the space of initial states is restricted and not suitable for non-autonomous systems.

• Another problem:

- Integrability over finite fields?

ex.) $dP_\parallel$ eq.

\[
\begin{aligned}
x_{n+1} &= \frac{nx_n + a}{1 - x_n^2} - y_n \\
y_{n+1} &= x_n
\end{aligned}
\]

- If $x_n \in \mathbb{F}_p$, $y_n \in \mathbb{F}_p$, $dP_\parallel$ eq. is the map: $\mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{F}_p \times \mathbb{F}_p$

- If $p=3$, the domain of definition for $dP_\parallel$ eq. is a finite set: $\mathbb{F}_3 \times \mathbb{F}_3 \ (|\mathbb{F}_3 \times \mathbb{F}_3| = 9)$.

- How can we define the “integrability” of dynamical systems, which consists of transitions between just 9 points?
Our approach:

Extend the domain of definition to make the mapping well-defined.

Use the field of $p$-adic numbers

1. Define the mapping over the field of $p$-adic numbers.
2. Define the mapping over the finite field so that it is compatible with the reduction from (1).
3. We try to resolve the problems by studying the pair $\left( \mathbb{F}_p, \mathbb{Q}_p \right)$.

Today’s topics:

• Investigate the property of the reduction (modulo prime) of the discrete Painlevé equations\textsuperscript{[5]}.
• Prove that the reduction has a “good” property.
• Explain that the property can be a test for integrability.

Reduction to finite fields (preparation)

• The $p$-adic metric $| \cdot |_p$

A rational number $x \in \mathbb{Q}^x := \mathbb{Q} - \{0\}$ is expressed as

$$x = p^k \frac{u}{v} \quad (k \in \mathbb{Z}), \quad (u, v \text{ are not divisible by } p.)$$

We define the $p$-adic valuation as $\text{ord}_p (x) = k$.
We define the $p$-adic metric as $|x|_p = p^{-k}$. ($|0|_p = 0$.)

• The field of $p$-adic numbers $\mathbb{Q}_p$

[Definition] $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ by the $p$-adic metric.

• The ring of $p$-adic integers $\mathbb{Z}_p$

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \ (\leftrightarrow k \geq 0) \right\}$$

• $p\mathbb{Z}_p$ is the maximal ideal of $\mathbb{Z}_p$ and we have

$$\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$$
Reduction to finite fields

**NOTE:** a *p*-adic number has a unique power series expansion with respect to *p*.

\[ x \in \mathbb{Z}_p \Rightarrow x = c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \cdots \quad (c_k \in \{0, 1, \ldots, p-1\}) \]

\[ x \in \mathbb{Q}_p - \mathbb{Z}_p \Rightarrow x = c_{-m} \left(\frac{1}{p}\right)^m + \cdots + c_{-1} \left(\frac{1}{p}\right) + c_0 + c_1 p + c_2 p^2 + \cdots \]

**Reduction:** \( \pi : \mathbb{Q}_p \to \mathbb{F}_p \cup \{\infty\} \quad \pi(x) := \begin{cases} c_0 & \cdots x \in \mathbb{Z}_p \\ \infty & \cdots x \in \mathbb{Q}_p - \mathbb{Z}_p \end{cases} \)

**Ex) *p=5***

\[ 10 = 0 + 2 \cdot 5 \in \mathbb{Z}_5 \quad \Rightarrow \quad \pi(10) = 0 \]

\[ \frac{1}{2} = 3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \cdots \in \mathbb{Z}_5 \quad \Rightarrow \quad \pi\left(\frac{1}{2}\right) = 3 \]

\[ \frac{1}{15} = 2 \left(\frac{1}{5}\right) + 3 + 1 \cdot 5 + 3 \cdot 5^2 + \cdots \in \mathbb{Q}_5 \quad \Rightarrow \quad \pi\left(\frac{1}{15}\right) = \infty \]
Good Reduction (GR)

[Definition] A rational mapping $\phi \in \mathbb{Z}_p(x, y)$ has a **good reduction** on the domain $D \subset \mathbb{Z}_p \times \mathbb{Z}_p$ if the following relation is satisfied for every $(x, y) \in D$. [6] J. H. Silverman: GTM241, (2007) Springer.

$$\pi(\phi(x, y)) = \bar{\phi}(\bar{x}, \bar{y})$$

Here the map $\bar{\phi}$ denotes coefficients’ reduction $\phi \in \mathbb{Z}_p(x, y) \rightarrow \bar{\phi} \in \mathbb{F}_p(x, y)$. (The map $\bar{\phi}(\bar{x}, \bar{y})$ needs to be well-defined.)
Example of Good Reduction (GR)

• Examples of mappings with GR:

\[ PGL_2 : \phi(x) = \frac{ax + b}{cx + d}, \ (a,b,c,d \in \mathbb{Z}_p, ad - bc \in \mathbb{Z}_p^\times). \]

• Examples of mappings without GR (with Bad Reduction):

One variable case: \[ \phi(z) = \frac{z^2 - z}{p} \]

Two variables case: Mappings like the discrete Painlevé equations\[^7\], which have indeterminacies after reducing them.

Almost Good Reduction (AGR)

[Definition] Rational mappings $\phi \in \mathbb{Z}_p(x, y)$ have AGR on the domain $D \subset \mathbb{Z}_p \times \mathbb{Z}_p$ if there exists a positive integer $m$ for every point $(x, y) \in D$ such that

$$
\pi\left(\phi^m(x, y)\right) = \phi^m(\tilde{x}, \tilde{y})
$$

Example) a QRT mapping

\[ \phi : (x_{n+1}, y_{n+1}) = \left( \frac{1 + x_n}{y_n x_n}, x_n \right) \]

\[
(2, 1) \rightarrow \left( \frac{3}{2}, 2 \right) \rightarrow \left( \frac{5}{6}, \frac{3}{2} \right) \rightarrow \left( \frac{22}{15}, \frac{5}{6} \right) \rightarrow \left( \frac{111}{55}, \frac{22}{15} \right) \rightarrow \left( \frac{415}{407}, \frac{111}{55} \right) \rightarrow \left( \frac{3014}{3071}, \frac{415}{407} \right) \rightarrow \ldots
\]

\[ \bar{\phi} : (2, 1) \rightarrow (0, 2) \quad \ldots \quad (\infty, 0) \quad \ldots \quad (\infty, \infty) \quad \ldots \quad (0, \infty) \quad \ldots \quad (2, 0) \rightarrow (1, 2) \rightarrow \ldots \]

\[ \bar{\phi}^4(\tilde{0}, \tilde{2}) \text{ makes sense.} \]

**Proposition:** The mapping \( \phi \) has an AGR.

**NOTE:** The above mapping \( \phi \) is integrable.

(Relation between AGR and integrability is suggested.)
AGR for non-autonomous discrete mapping

[Definition] A map \( \phi_n : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p \times \mathbb{Q}_p \) \( ((x_n, y_n) \to (x_{n+1}, y_{n+1})) \) has an AGR, when it satisfies the following condition;

\( \bigstar \) Let \( X_n \) be the set \( X_n := \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid \phi(x, y) \in \mathbb{Q}_p \times \mathbb{Q}_p \} \).

For any integer \( n \) and for any point \( (x_n, y_n) \in X_n \) there exists an integer \( k = k(n) \geq 1 \), such that \( (\phi_n \circ \phi_{n+1} \circ \cdots \circ \phi_{n+k})(x_n, y_n) \in X_{n+k} \) and \( (\phi_{n+k-1} \circ \cdots \circ \phi_{n+1} \circ \phi_n)(\tilde{x}_n, \tilde{y}_n) = (\tilde{x}_{n+k}, \tilde{y}_{n+k}) \).

AGR: Commutative diagram of green lines.

Evolution over finite fields: Blue dotted lines.
Ex.) The $q$-discrete Painlevé I equation ($qP_1$)

$qP_1$ is the following non-autonomous discrete dynamical system which tends to $P_1$ with an appropriate continuous limit.

\[
[qP_1] \quad \phi_n : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1 \\
(x_n, y_n) \mapsto (x_{n+1}, y_{n+1})
\]

\[
\begin{cases}
    x_{n+1} = \frac{aq^n x_n + b}{x_n^2 y_n}, \\
    y_{n+1} = x_n.
\end{cases}
\]

**Proposition:** $qP_1$ has an AGR, where the domain is

\[
X_n := \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid x \neq 0, y \neq 0\}
\]
Definition of time evolution over finite field

A definition of time evolution over finite fields:

\[ \overline{\phi}_n : \mathbb{PF}_p \times \mathbb{PF}_p \rightarrow \mathbb{PF}_p \times \mathbb{PF}_p \quad \left( \mathbb{PF}_p := \mathbb{F}_p \cup \{\infty\} \right) \]

1) \((x_0, y_0) \in \pi(\mathbb{X}_0) \subseteq \mathbb{F}_p \times \mathbb{F}_p\)

2) \((x_n, y_n) \in \pi(\mathbb{X}_n) \Rightarrow (x_{n+1}, y_{n+1}) = \overline{\phi}_n(x_n, y_n)\)

3) \((x_n, y_n) \notin \pi(\mathbb{X}_n) \Rightarrow \exists m \in \mathbb{Z}_{>0} \text{ s.t. } (x_{n-m}, y_{n-m}) \in \pi(\mathbb{X}_n), (x_{n+1}, y_{n+1}) = \pi((\phi_n \circ \cdots \circ \phi_{n-m})(x_{n-m}, y_{n-m}))\)

Ex) \(qP\) eq. \(a = b = 1, q = 2, p = 5, (x_0, y_0) = (1,1)\)

\[ \mathbb{R} : \begin{pmatrix} x_0, x_1, x_2, \cdots, x_6 \end{pmatrix} = \begin{pmatrix} 1, 2, \frac{5}{4}, \frac{48}{25}, \frac{2045}{576}, \frac{230141952}{167281}, \frac{602433257141 \times 167281}{230141952 \times 399552} \end{pmatrix}. \]

\[ \mathbb{PF}_5 : \begin{pmatrix} x_0, x_1, x_2, \cdots, x_6 \end{pmatrix} = \begin{pmatrix} 1, 2, 0, \infty, 0, 2, 4 \end{pmatrix}. \]
AGR as an integrability detector

\[
\begin{align*}
\begin{cases}
x_{n+1} = \frac{x_n + 1}{x_n^\gamma y_n}, \\
y_{n+1} = x_n.
\end{cases}
\end{align*}
\]
(If \( \gamma = 2 \), it is an autonomous \( qP_1 \).)

[Fact] The system is integrable if \( \gamma = 0, 1, 2 \),
non-integrable if \( \gamma \geq 3 \).

[Proposition] The system has an AGR if \( \gamma = 0, 1, 2 \).
(Proof is similar to the case of \( qP_1 \))

[Proposition] The system does not have an AGR if \( \gamma \geq 3 \).
(By iterating the mapping, we can prove that the order of \( p \) diverges.)
AGR as an integrability detector 2

- AGR of other integrable equations\cite{10}
  The \( dP_{II}, qP_{II}, qP_{III}, qP_{IV}, qP_{V} \) equations have AGR.
- The Hietarinta-Viallet equation\cite{13} also has an AGR, despite that it is a non-integrable, chaotic system.

- Postulation
AGR is an \textbf{integrability detector} for dynamical systems over finite fields. AGR is an arithmetic analogue of the singularity confinement test.

Cf.) prime \( p \leftrightarrow \) infinitesimal parameter \( \varepsilon \)

Cf.) application of Sakai’s theory[8]

- Extend $\mathbb{F} \times \mathbb{F}$ to $\mathbb{P} \mathbb{F} \times \mathbb{P} \mathbb{F}$ and blow up so that the mapping becomes birational mapping (or bijective mapping for discrete topology).

- Ex)
  \[
  \begin{cases}
  x_{n+1} = \frac{nx_n + a}{1 - x_n^2} - y_n \\
  y_{n+1} = x_n
  \end{cases}
  \]
  blowing up twice at 4 points $(x_n, y_n) = (\pm 1, \infty), (\infty, \pm 1)$.

- $\mathbb{P} \mathbb{F}_p \times \mathbb{P} \mathbb{F}_p \to \tilde{\Omega}^{(n)} := A_{(1,\infty)}^{(n)} \cup A_{(-1,\infty)}^{(n)} \cup A_{(\infty,1)}^{(n)} \cup A_{(\infty,-1)}^{(n)}$.

- $A_{(1,\infty)}^{(n)} := \left\{ \left((x-1, y^{-1}), [\xi_1 : \eta_1], [u_1 : v_1]\right) \mid \eta_1(x-1) = \xi_1 y^{-1}, \right. \\
  \left. (\xi_1 + (n+a)\eta_1 / 2)v_1 = \eta_1(1-x)u_1 \right\} \subset \mathbb{A}^2 \times \mathbb{P} \times \mathbb{P}$

  dP$_{II}$ eq. becomes a bijection from $\tilde{\Omega}^{(n)}$ to $\tilde{\Omega}^{(n+1)}$.

Space of initial conditions for $dP_{||}$ over $\mathbb{F}_3$
Special solution of d\(P_{\|}\)

- Laguerre polynomials

\[
L^{(\nu)}_k(\lambda) := \begin{cases} 
\sum_{r=0}^{k} (-1)^{k} \left( \begin{array}{c} k + \nu \\ k - r \end{array} \right) \frac{\lambda^{r}}{r!} & (k \geq 0) \\
0 & (k < 0)
\end{cases}
\]

We define the tau function as the determinant of the \(N \times N\) matrix:

\[
\tau_n := \det \left( L_{n-2i+j+1}(\lambda) \right)_{1 \leq i, j \leq N}
\]

Then, \(x_n = \frac{\tau_{n+1}^{N+1}\tau_n^{n-1}}{\tau_{n+1}^n\tau_n^n} - 1\)

is a special solution of d\(P_{\|}\) for the parameters \(\alpha_0 = -\frac{N}{\lambda}, \beta_0 = -\frac{N+2}{\lambda}\) [11].

Special solution of $dP_{II}$ and its reduction

- The rational solution of $dP_{II}$ when $N = 3, \lambda = 1$.

\[
\frac{1864}{2431}, \frac{46534}{6013}, \frac{137996}{875877}, \frac{102987326}{124416701}, \frac{4029720776}{5563710625}, \ldots
\]

- Since the $dP_{II}$ has AGR property, reducing this solution gives a solution of $dP_{II}$ over $\mathbb{F}_p$.

(Ex.)

- $p = 3$: $1, 2, \infty, 1, 2, \infty, 1, 2, \infty, \ldots$
- $p = 7$: $1, \infty, 6, 5, 1, \infty, 6, 1, \infty, 6, 5, 1, \infty, 6, \ldots$

The period of these solutions are $p$. 
Conclusion

We studied integrable equations over finite fields.

- Utilize the system over the field of \( p \)-adic numbers \( \mathbb{Q}_p \) and reduction to the finite field \( \overline{\mathbb{F}}_p \cup \{\infty\} \).

We defined the notion of ‘Almost Good Reduction (AGR)’.

- Criterion for integrability of dynamics over finite fields.
- Arithmetic analogue of the singularity confinement test.

We constructed integrable dynamical systems over finite fields.

- Thanks to AGR, indeterminacies are resolved.

Remark: We have preliminary results for the soliton systems over finite fields\(^6\).

- Investigation of the discrete KdV equation and its solitons.

Future Problems

Soliton systems over finite fields

✓ Solving the initial value problem over $p$-adic numbers or finite fields.

Further study of the ‘Almost Good Reduction’

✓ Studying further the reduction properties of two-dimensional systems.

(Not only dKdV eq., but also the discrete Toda eq., discrete versions of Schrödinger eq., discrete sine-Gordon eq., …)


Thank you for your attention.