KURENAI

Kyoto University Research Information Repository

KYOTO UNIVERSITY

Title	Discrete Painleve equations and discrete KdV equation over finite fields (The breadth and depth of nonlinear discrete integrable systems)
Author(s)	KANKI, Masataka; MADA, Jun; TOKIHIRO, Tetsuji
Citation	= RIMS Kokyuroku Bessatsu (2013), B41: 125-145
Issue Date	2013-08
URL	http://hdl.handle.net/2433/209040
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

Discrete Painlevé equations and discrete KdV equation over finite fields

By

Masataka KANKI* and Jun MADA** and Tetsuji TOKIHIRO***

Abstract

We investigate some of the discrete Painlevé equations (dP_{II} , qP_I and qP_{II}) and the discrete KdV equation over finite fields. The first part concerns the discrete Painlevé equations. We review some of the ideas introduced in our previous papers [1, 2] and give some detailed discussions. We first show that they are well defined by extending the domain according to the theory of the space of initial conditions. We then extend them to the field of p-adic numbers and observe that they have a property that is called an 'almost good reduction' of dynamical systems over finite fields. We can use this property, which can be interpreted as an arithmetic analogue of singularity confinement, to avoid the indeterminacy of the equations over finite fields and to obtain special solutions from those defined originally over fields of characteristic zero. In the second part we study the discrete KdV equation. We follow the discussions in [3] and present a way to resolve the indeterminacy of the equation by treating it over a field of rational functions instead of the finite field itself. Explicit forms of soliton solutions and their periods over finite fields are obtained.

§ 1. Introduction

In this article, we study several discrete integrable equations over finite fields. One of the problems we encounter when we treat a discrete equation over a finite field

*Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8914, Japan
e-mail: `kanki@ms.u-tokyo.ac.jp`
**College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba 275-8576, Japan
e-mail: `mada.jun@nihon-u.ac.jp`
***Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8914, Japan
e-mail: `toki@ms.u-tokyo.ac.jp`

is that its time evolution is not always well defined. This problem cannot be solved even if we extend the domain from $\mathbb{F}_{p^m}$ (p is a prime number) to the projective space $\mathbb{PF}_{p^m} := \mathbb{F}_{p^m} \cup \{\infty\}$, because $\mathbb{PF}_{p^m}$ is no longer a field; we cannot determine the values such as $\frac{0}{0}$, $0 \cdot \infty$, $\infty + \infty$ and so on. In this paper we study two strategies to define the time evolution over a finite field without inconsistencies: [I] One is to reduce the domain so that the time evolution will not pass the indeterminate states. [II] The other is to extend the domain so that it can include all the orbits. We take the latter strategy [II] and adopt two approaches: (i) The first approach is the application of the theory of space of initial conditions developed by Okamoto [4, 5, 6, 7] and Sakai [8]. (ii) The second approach is to extend the domain of initial conditions to the field of p-adic numbers $\mathbb{Q}_p$.

The first part of this article concerns the one-dimensional dynamical systems, in particular the discrete Painlevé equations. Through the approach (i), we show that the dynamics of those equations can be well defined in the space of initial conditions even over the finite fields [2]. The approach (ii) is closely related to the so called arithmetic dynamics, which concerns the dynamics over arithmetic sets such as $\mathbb{Z}$ or $\mathbb{Q}$ or a number field that is of number theoretic interest [9]. In arithmetic dynamics, the change of dynamical properties of polynomial or rational mappings give significant information when reducing them modulo prime numbers. The mapping is said to have good reduction if, roughly speaking, the reduction commutes with the mapping itself [9]. The action of the projective linear group PGL_2 give typical examples of mappings with a good reduction. The QRT mappings [10] and several bi-rational mappings over finite fields have been investigated in terms of integrability by choosing the parameter values so that indeterminate points are avoided [11, 12, 13]. They also have a good reduction over finite fields. We prove that, although the integrable mappings generally do not have a good reduction modulo a prime, they do have an *almost good reduction*, which is a generalised notion of good reduction. We first treat in detail the discrete Painlevé II equation ($\mathrm{dP_{II}}$) [14] over finite fields, on which we have briefly reported in our previous letter [1], and then apply the method to the q-discrete Painlevé equations ($q\mathrm{P_I}$ and $q\mathrm{P_{II}}$). The time evolution of the discrete Painlevé equations can be well defined generically, via the reduction from a local field $\mathbb{Q}_p$ to a finite field $\mathbb{F}_p$. The theory is then used to obtain some special solutions directly from those over fields of characteristic zero such as $\mathbb{Q}$ or $\mathbb{R}$.

The second part concerns the two-dimensional evolution equation, in particular, the discrete KdV equation (dKdV). Since the dKdV equation evolves as a two-dimensional lattice, the number of singular patterns we obtain is too large to be investigated even for a system with small size. Therefore, it is difficult to determine the space of initial conditions through the approach (i) above. Instead, we take the second approach (ii).

We can well-define the dKdV equation by considering it over the local field $\mathbb{Q}_p$ just like the discrete Painlevé cases. We introduce another extension of the space of initial conditions. Since the dKdV equation has a parameter δ, we can see δ as an indeterminant (variable) and can define the dKdV equation over the field of rational functions $\mathbb{F}_r(\delta)$ where $r = p^m$ $(m \geq 1)$ [3]. We define the soliton solutions over the finite fields and discuss their periodicity.

§ 2.   The dP$_{\mathrm{II}}$ equation and its space of initial conditions

The discrete Painlevé equations are non-autonomous, integrable mappings which tend to some continuous Painlevé equations for appropriate choices of the continuous limit [14]. They are non-autonomous and nonlinear second order ordinary difference equations with several parameters. When they are defined over a finite field, the dependent variable takes only a finite number of values and their time evolution will attain an indeterminate state in many cases for generic values of the parameters and initial conditions. For example, the dP$_{\mathrm{II}}$ equation is defined as

$$(2.1) \qquad u_{n+1} + u_{n-1} = \frac{z_n u_n + a}{1 - u_n^2} \quad (n \in \mathbb{Z}),$$

where $z_n = \delta n + z_0$ and a, δ, z_0 are constant parameters [15]. Let $r = p^m$ for a prime p and a positive integer $m \in \mathbb{Z}_+$. When (2.1) is defined over a finite field $\mathbb{F}_r$, the dependent variable u_n will eventually take values ± 1 for generic parameters and initial values $(u_0, u_1) \in \mathbb{F}_r^2$, and we cannot proceed to evolve it. If we extend the domain from $\mathbb{F}_r^2$ to $(\mathbb{PF}_r)^2 = (\mathbb{F}_r \cup \{\infty\})^2$, $\mathbb{PF}_r$ is not a field and we cannot define arithmetic operation in (2.1). To determine its time evolution consistently, we have two choices: One is to restrict the parameters and the initial values to a smaller domain so that the singularities do not appear. The other is to extend the domain on which the equation is defined. In this article, we will adopt the latter approach. It is convenient to rewrite (2.1) as:

$$(2.2) \qquad \begin{cases} x_{n+1} = \dfrac{\alpha_n}{1 - x_n} + \dfrac{\beta_n}{1 + x_n} - y_n, \\ y_{n+1} = x_n, \end{cases}$$

where $\alpha_n := \frac{1}{2}(z_n + a)$, $\beta_n := \frac{1}{2}(-z_n + a)$. Then we can regard (2.2) as a mapping defined on the domain $\mathbb{F}_r \times \mathbb{F}_r$. To resolve the indeterminacy at $x_n = \pm 1$, we apply the theory of the state of initial conditions developed by Sakai [8]. First we extend the domain to $\mathbb{PF}_r \times \mathbb{PF}_r$, and then blow it up at four points $(x, y) = (\pm 1, \infty), (\infty, \pm 1)$ to obtain the space of initial conditions:

$$(2.3) \qquad \tilde{\Omega}^{(n)} := \mathcal{A}_{(1,\infty)}^{(n)} \cup \mathcal{A}_{(-1,\infty)}^{(n)} \cup \mathcal{A}_{(\infty,1)}^{(n)} \cup \mathcal{A}_{(\infty,-1)}^{(n)},$$

where $\mathcal{A}^{(n)}_{(1,\infty)}$ is the space obtained from the two dimensional affine space $\mathbb{A}^2$ by blowing up twice as

$$\mathcal{A}^{(n)}_{(1,\infty)} := \left\{ \left((x-1, y^{-1}), [\xi_1 : \eta_1], [u_1 : v_1] \right) \; \Big| \right.$$
$$\left. \eta_1(x-1) = \xi_1 y^{-1}, (\xi_1 + \alpha_n \eta_1)v_1 = \eta_1(1-x)u_1 \right\} \subset \mathbb{A}^2 \times \mathbb{P} \times \mathbb{P},$$

where $[a : b]$ denotes a set of homogeneous coordinates for $\mathbb{P}^1$. Similarly,

$$\mathcal{A}^{(n)}_{(-1,\infty)} := \left\{ \left((x+1, y^{-1}), [\xi_2 : \eta_2], [u_2 : v_2] \right) \; \Big| \right.$$
$$\left. \eta_2(x+1) = \xi_2 y^{-1}, (-\xi_2 + \beta_n \eta_2)v_2 = \eta_2(1+x)u_2 \right\},$$
$$\mathcal{A}^{(n)}_{(\infty,1)} := \left\{ \left((x^{-1}, y-1), [\xi_3 : \eta_3], [u_3 : v_3] \right) \; \Big| \right.$$
$$\left. \xi_3(y-1) = \eta_3 x^{-1}, (\eta_3 + \alpha_n \xi_3)v_3 = \xi_3(1-y)u_3 \right\},$$
$$\mathcal{A}^{(n)}_{(\infty,-1)} := \left\{ \left((x^{-1}, y+1), [\xi_4 : \eta_4], [u_4 : v_4] \right) \; \Big| \right.$$
$$\left. \xi_4(y+1) = \eta_4 x^{-1}, (-\eta_4 + \beta_n \xi_4)v_3 = \xi_4(1+y)u_4 \right\}.$$

The bi-rational map (2.2) is extended to the bijection $\tilde{\phi}_n : \tilde{\Omega}^{(n)} \to \tilde{\Omega}^{(n+1)}$ which decomposes as $\tilde{\phi}_n := \iota_n \circ \tilde{\omega}_n$. Here ι_n is a natural isomorphism which gives $\tilde{\Omega}^{(n)} \cong \tilde{\Omega}^{(n+1)}$, that is, on $\mathcal{A}^{(n)}_{(1,\infty)}$ for instance, ι_n is expressed as

$$\left((x-1, y^{-1}), [\xi : \eta], [u : v] \right) \in \mathcal{A}^{(n)}_{(1,\infty)}$$
$$\to \quad \left((x-1, y^{-1}), [\xi - \delta/2 \cdot \eta : \eta], [u : v] \right) \in \mathcal{A}^{(n+1)}_{(1,\infty)}.$$

The automorphism $\tilde{\omega}_n$ on $\tilde{\Omega}^{(n)}$ is induced from (2.2) and gives the mapping

$$\mathcal{A}^{(n)}_{(1,\infty)} \to \mathcal{A}^{(n)}_{(\infty,1)}, \; \mathcal{A}^{(n)}_{(\infty,1)} \to \mathcal{A}^{(n)}_{(-1,\infty)}, \; \mathcal{A}^{(n)}_{(-1,\infty)} \to \mathcal{A}^{(n)}_{(\infty,-1)}, \; \mathcal{A}^{(n)}_{(\infty,-1)} \to \mathcal{A}^{(n)}_{(1,\infty)}.$$

Under the map $\mathcal{A}^{(n)}_{(1,\infty)} \to \mathcal{A}^{(n)}_{(\infty,1)}$,

$$x = 1 \; \to \; E_2^{(\infty,1)} \qquad u_3 = \left(y - \frac{\beta_n}{2} \right) v_3,$$
$$E_1^{(1,\infty)} \; \to \; E_1^{(\infty,1)} \qquad [\xi_1 : -\eta_1] = [\alpha_n \xi_3 + \eta_3 : \xi_3],$$
$$E_2^{(1,\infty)} \; \to \; y' = 1 \qquad x' = \frac{u_1}{v_1} + \frac{\beta_n}{2},$$

where $(x, y) \in \mathcal{A}^{(n)}_{(1,\infty)}$, $(x', y') \in \mathcal{A}^{(n)}_{(\infty,1)}$, E_1^{p} and E_2^{p} are the exceptional curves in $\mathcal{A}^{(n)}_{\mathrm{p}}$ obtained by the first blowing up and the second blowing up respectively at the point p $\in \{(\pm 1, \infty), (\infty, \pm 1)\}$. Similarly under the map $\mathcal{A}^{(n)}_{(\infty,1)} \to \mathcal{A}^{(n)}_{(-1,\infty)}$,

$$E_1^{(\infty,1)} \; \to \; E_1^{(-1,\infty)} \qquad [\xi_3 : \eta_3] = [\eta_2 : (\beta_n - \alpha_n)\eta_2 - \xi_2],$$
$$E_2^{(\infty,1)} \; \to \; E_2^{(-1,\infty)} \qquad [u_3 : v_3] = [-\beta_n u_2 : \alpha_n v_2].$$

The mapping on the other points are defined in a similar manner. Note that $\tilde{\omega}_n$ is well-defined in the case $\alpha_n = 0$ or $\beta_n = 0$. In fact, for $\alpha_n = 0$, $E_2^{(1,\infty)}$ and $E_2^{(\infty,1)}$ can be identified with the lines $x = 1$ and $y = 1$ respectively. Therefore we have found that, through the construction of the space of initial conditions, the dP_{II} equation can be well-defined over finite fields. However there are some unnecessary elements in the space of initial conditions when we consider a finite field, because we are working on a discrete topology and do not need continuity of the map. Let $\tilde{\Omega}^{(n)}$ be the space of initial conditions and $|\tilde{\Omega}^{(n)}|$ be the number of elements of it. For the dP_{II} equation, we obtain $|\tilde{\Omega}^{(n)}| = (r+1)^2 - 4 + 4(r+1) - 4 + 4(r+1) = r^2 + 10r + 1$, since $\mathbb{PF}_r$ contains $r + 1$ elements. However an exceptional curve E_1^{p} is transferred to another exceptional curve $E_1^{\mathrm{p}'}$, and $[1:0] \in E_2^{\mathrm{p}}$ to $[1:0] \in E_2^{\mathrm{p}'}$ or to a point in $E_1^{\mathrm{p}'}$. Hence we can reduce the space of initial conditions $\tilde{\Omega}^{(n)}$ to the minimal space of initial conditions $\Omega^{(n)}$ which is the minimal subset of $\tilde{\Omega}^{(n)}$ including $\mathbb{PF}_r \times \mathbb{PF}_r$, closed under the time evolution. By subtracting unnecessary elements we find $|\Omega^{(n)}| = (r+1)^2 - 4 + 4(r+1) - 4 = r^2 + 6r - 3$. In summary, we obtain the following proposition:

Proposition 2.1.   *The domain of the dP_{II} equation over $\mathbb{F}_r$ can be extended to the minimal domain $\Omega^{(n)}$ on which the time evolution at time step n is well defined. Moreover $|\Omega^{(n)}| = r^2 + 6r - 3$.*

In figure 1, we show a schematic diagram of the map $\tilde{\omega}_n$ on $\tilde{\Omega}^{(n)}$, and its restriction map $\omega_n := \tilde{\omega}_n|_{\Omega^{(n)}}$ on $\Omega^{(n)}$ with $r = 3$, $\alpha_0 = 1$ and $\beta_0 = 2$. We can also say that the figure 1 is a diagram for the autonomous version of the equation (2.2) when $\delta = 0$. In the case of $r = 3$, we have $|\tilde{\Omega}^{(n)}| = 40$ and $|\Omega^{(n)}| = 24$.

The above approach is equally valid for the other discrete Painlevé equations and we can define them over finite fields by constructing isomorphisms on the spaces of initial conditions. Thus we conclude that a discrete Painlevé equation can be well defined over a finite field by redefining the initial domain properly. In the next section, we show another extension of the space of initial conditions: we extend it to $\mathbb{Z}_p \times \mathbb{Z}_p$[1].

§3.   The discrete dynamical systems over a local field and its reduction modulo a prime (review)

§3.1.   Almost good reduction

Let p be a prime number and for each $x \in \mathbb{Q}$ ($x \neq 0$) write $x = p^{v_p(x)} \dfrac{u}{v}$ where $v_p(x), u, v \in \mathbb{Z}$ and u and v are coprime integers neither of which is divisible by p. The p-adic norm $|x|_p$ is defined as $|x|_p = p^{-v_p(x)}$. ($|0|_p = 0$.) The local field $\mathbb{Q}_p$ is

---

[1] With the method in the next section, we can only deal with systems over the field $\mathbb{F}_{p^1}$. To apply it to those over the field $\mathbb{F}_{p^m}$ ($m > 1$), we have to use the field extension of $\mathbb{Q}_p$.
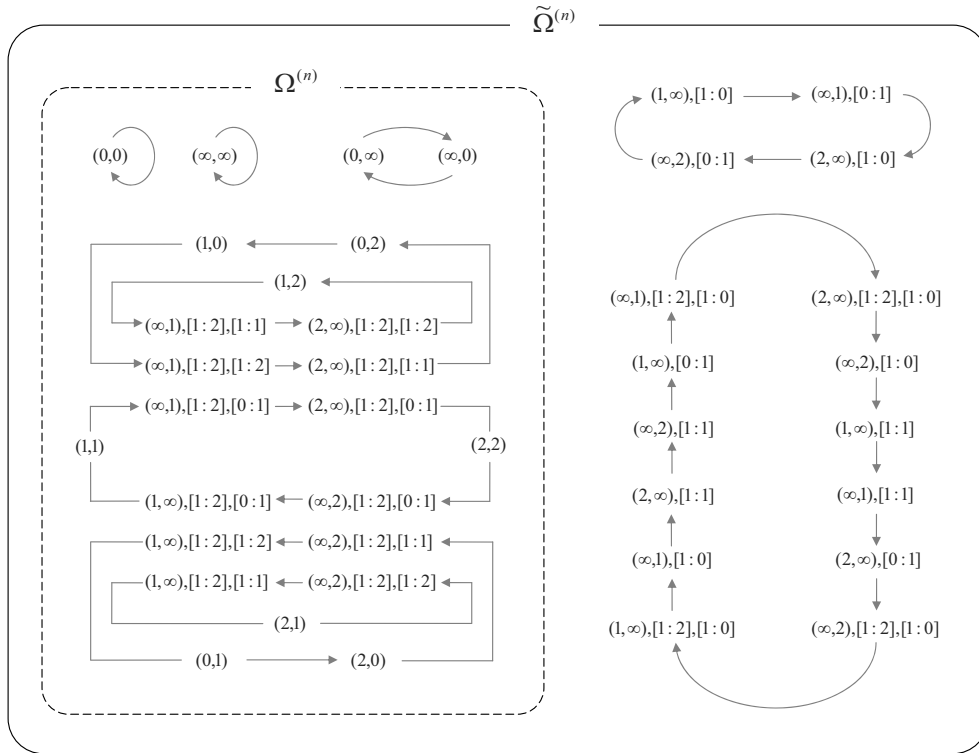
Figure 1. The orbit decomposition of the space of initial conditions $\tilde{\Omega}^{(n)}$ and the reduced one $\Omega^{(n)}$ for $p = r = 3$.

a completion of $\mathbb{Q}$ with respect to the p-adic norm. It is called the field of p-adic numbers and its subring $\mathbb{Z}_p := \{x \in \mathbb{Q}_p |\ |x|_p \leq 1\}$ is called the ring of p-adic integers [17]. The p-adic norm satisfies a non-Archimedean (ultrametric) triangle inequality $|x + y|_p \leq \max[|x|_p, |y|_p]$. Let $\mathfrak{p} = p\mathbb{Z}_p = \{x \in \mathbb{Z}_p |\ v_p(x) \geq 1\}$ be the maximal ideal of $\mathbb{Z}_p$. We define the reduction of x modulo $\mathfrak{p}$ as $\tilde{x} \colon \mathbb{Z}_p \ni x \mapsto \tilde{x} \in \mathbb{Z}_p/\mathfrak{p} \cong \mathbb{F}_p$. Note that the reduction is a ring homomorphism. The reduction is generalised to $\mathbb{Q}_p^\times$:

$$\mathbb{Q}_p^\times \ni x = p^k u\ (u \in \mathbb{Z}_p^\times) \mapsto \begin{cases} 0\ (k > 0) \\ \infty\ (k < 0) \\ \tilde{u}\ (k = 0) \end{cases} \in \mathbb{PF}_p,$$

which is no longer homomorphic. For a rational map $\phi(x, y) \in \mathbb{Z}_p(x, y)$: $\mathcal{D} \subseteq \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$, defined on some domain $\mathcal{D}$, $\tilde{\phi}(x, y) \in \mathbb{F}_p(x, y)$ is defined as the map whose coefficients are all reduced. The rational map ϕ is said to have a *good reduction* (modulo $\mathfrak{p}$ on the domain $\mathcal{D}$) if we have $\widetilde{\phi(x, y)} = \tilde{\phi}(\tilde{x}, \tilde{y})$ for any $(x, y) \in \mathcal{D}$ [9]. We have defined a generalised notion in our previous letter and have explained its usefulness;

Definition 3.1 ([1]).   A (non-autonomous) rational map ϕ_n: $\mathcal{D} \subseteq \mathbb{Z}_p^2 \to \mathbb{Q}_p$ $(n \in \mathbb{Z})$ is said to have an almost good reduction modulo $\mathfrak{p}$ if there exists a positive integer $m_{\mathrm{p};n}$ for any $\mathrm{p} = (x, y) \in \mathcal{D}$ and time step n such that

$$(3.1) \qquad \widetilde{\phi_n^{m_{\mathrm{p};n}}(x, y)} = \widetilde{\phi_n^{m_{\mathrm{p};n}}}(\tilde{x}, \tilde{y}),$$

where $\phi_n^m := \phi_{n+m-1} \circ \phi_{n+m-2} \circ \cdots \circ \phi_n$.

Let us first review some of the findings in [1] in order to see the significance of the notion of *almost good reduction*. Let us consider the mapping Ψ_γ:

$$(3.2) \qquad \begin{cases} x_{n+1} = \dfrac{ax_n + 1}{x_n^\gamma y_n}, \\ y_{n+1} = x_n, \end{cases}$$

where $a \in \{1, 2, \cdots, p - 1\}$ and $\gamma \in \mathbb{Z}_{\geq 0}$ are parameters. The map (3.2) is known to be integrable if and only if $\gamma = 0, 1, 2$. Note that when $\gamma = 0, 1, 2$, (3.2) is an autonomous version of the q-discrete Painlevé I equation and therefore is integrable. We also note that when $\gamma = 2$, (3.2) belongs to the QRT family and is integrable in the sense that it has a conserved quantity.

Let $\mathcal{D}$ be the domain $\{(x, y) \in \mathbb{Z}_p |\ x \neq 0, y \neq 0\}$, then clearly

$$\widetilde{\Psi_2(x_n, y_n)} = \tilde{\Psi}_2(\tilde{x}_n, \tilde{y}_n) \qquad \text{for } \tilde{x}_n \neq 0,\ \tilde{y}_n \neq 0.$$

For $(x_n, y_n) \in \mathcal{D}$ with $\tilde{x}_n = 0$ and $\tilde{y}_n \neq 0$, we find that $\widetilde{\Psi_2^k}(\tilde{x}_n = 0, \tilde{y}_n)$ is not defined for $k = 1, 2$, however it is defined if $k = 3$ and we have

$$\widetilde{\Psi_2^3(x_n, y_n)} = \widetilde{\Psi_2^3}(\tilde{x}_n = 0, \tilde{y}_n) = \left(\frac{1}{a^2 \tilde{y}}, 0 \right).$$

Finally for $\tilde{x}_n = \tilde{y}_n = 0$, we find that $\widetilde{\Psi_2^k}(\tilde{x}_n, \tilde{y}_n)$ is not defined for $k = 1, 2, .., 7$, however

$$\widetilde{\Psi_2^8(x_n, y_n)} = \widetilde{\Psi_2^8}(\tilde{x}_n = 0, \tilde{y}_n = 0) = (0, 0).$$

Hence the map Ψ_2 has almost good reduction modulo $\mathfrak{p}$ on $\mathcal{D}$. Note that, in the case $\gamma = 2$ and $a = 0$, if we take

$$f_{2k} := x_{2k} x_{2k-1}, \quad f_{2k-1} := (x_{2k-1} x_{2k-2})^{-1}$$

(3.2) turns into the trivial linear mapping $f_{n+1} = f_n$ which has apparently good reduction modulo $\mathfrak{p}$. In a similar manner, we find that Ψ_γ ($\gamma = 0, 1$) also has almost good reduction modulo $\mathfrak{p}$ on $\mathcal{D}$. On the other hand, for $\gamma \geq 3$ and $\tilde{x}_n = 0$, we easily find that

$$\forall k \in \mathbb{Z}_{\geq 0}, \quad \widetilde{\Psi_\gamma^k(x_n, y_n)} \neq \widetilde{\Psi_\gamma^k}(\tilde{x}_n = 0, \tilde{y}_n),$$

since the order of p diverges as we iterate the mapping. Thus we have proved the following proposition:

Proposition 3.2. *The rational mapping* (3.2) *has an almost good reduction modulo $\mathfrak{p}$ only for $\gamma = 0, 1, 2$.*

Note that having an almost good reduction is equivalent to the integrability of the equation in these examples.

§3.2. The dP$_{\text{II}}$ equation modulo a prime and its special solutions

Now let us examine the dP$_{\text{II}}$ (2.2) over $\mathbb{Q}_p$. We suppose that $p \geq 3$, and redefine the coefficients α_n and β_n so that they are periodic with period p:

$$\alpha_{i+mp} := \frac{(i\delta + z_0 + a + n_\alpha p)}{2}, \quad \beta_{i+mp} := \frac{(-i\delta - z_0 + a + n_\beta p)}{2},$$

$$(m \in \mathbb{Z}, \ i \in \{0, 1, 2, \cdots, p-1\}),$$

where the integer n_α (n_β) is chosen such that $0 \in \{\alpha_i\}_{i=0}^{p-1}$ ($0 \in \{\beta_i\}_{i=0}^{p-1}$). As a result, we have $\tilde{\alpha}_n = \widetilde{\frac{n\delta + z_0 + a}{2}}$, $\tilde{\beta}_n = \widetilde{\frac{-n\delta - z_0 + a}{2}}$ and $|\alpha_n|_p$, $|\beta_n|_p \in \{0, 1\}$ for any integer n.

Proposition 3.3. *Under the above assumptions, the dP$_{\text{II}}$ equation has an almost good reduction modulo $\mathfrak{p}$ on $\mathcal{D} := \{(x, y) \in \mathbb{Z}_p^2 \,|\, x \neq \pm 1\}$.*

Proof. We put $(x_{n+1}, y_{n+1}) = \phi_n(x_n, y_n) = \left(\phi_n^{(x)}(x_n, y_n), \phi_n^{(y)}(x_n, y_n) \right)$. When $\tilde{x}_n \neq \pm 1$, we have

$$\tilde{x}_{n+1} = \frac{\tilde{\alpha}_n}{1 - \tilde{x}_n} + \frac{\tilde{\beta}_n}{1 + \tilde{x}_n} - \tilde{y}_n, \quad \tilde{y}_{n+1} = \tilde{x}_n.$$

Hence $\phi_n\widetilde{(x_n, y_n)} = \tilde{\phi}_n(\tilde{x}_n, \tilde{y}_n)$.

When $\tilde{x}_n = 1$, we can write $x_n = 1 + p^k e$ ($k \in \mathbb{Z}_+$, $|e|_p = 1$). We have to consider four cases[2]:

(i) For $\alpha_n = 0$,

$$\tilde{x}_{n+1} = \tilde{\phi}_n^{(x)}(\tilde{x}_n, \tilde{y}_n) = \widetilde{\left(\frac{\beta_n}{2}\right)} - \tilde{y}_n.$$

Hence we have $\phi_n\widetilde{(x_n, y_n)} = \tilde{\phi}_n(\tilde{x}_n, \tilde{y}_n)$.

(ii) In the case $\alpha_n \neq 0$ and $\beta_{n+2} \neq 0$,

$$x_{n+1} = -\frac{(\alpha_n - \beta_n)(1 + ep^k) + a}{ep^k(2 + ep^k)} - y_n = -\frac{2\alpha_n + (\alpha_n - \beta_n)ep^k}{ep^k(2 + ep^k)} - y_n,$$

$$x_{n+2} = -\frac{\alpha_n^2 + \text{polynomial of } O(p)}{\alpha_n^2 + \text{polynomial of } O(p)},$$

$$x_{n+3} = \frac{\{2\alpha_n y_n + 2\delta\beta_{n+1} + (2 - \delta)a\}\alpha_n^3 + \text{polynomial of } O(p)}{2\beta_{n+2}\alpha_n^3 + \text{polynomial of } O(p)},$$

Thus we have

$$\tilde{x}_{n+3} = \frac{2\tilde{\alpha}_n\tilde{y}_n + 2\delta\tilde{\beta}_{n+1} + (2 - \delta)a}{2\tilde{\beta}_{n+2}}, \quad \tilde{y}_{n+3} = -1,$$

and $\phi_n^3\widetilde{(x_n, y_n)} = \widetilde{\phi_n^3}(\tilde{x}_n, \tilde{y}_n)$.

(iii) In the case $\alpha_n \neq 0$, $\beta_{n+2} = 0$ and $a \neq -\delta$, we have to calculate up to x_{n+5}. After a lengthy calculation we find

$$\tilde{x}_{n+4} = \widetilde{\phi_n^5}^{(y)}(1, \tilde{y}_n) = 1, \text{ and } \tilde{x}_{n+5} = \widetilde{\phi_n^5}^{(x)}(1, \tilde{y}_n) = -\frac{a\delta - (a - \delta)\tilde{y}_n}{a + \delta},$$

and we obtain $\phi_n^5\widetilde{(x_n, y_n)} = \widetilde{\phi_n^5}(\tilde{x}_n, \tilde{y}_n)$.

(iv) Finally, in the case $\alpha_n \neq 0$, $\beta_{n+2} = 0$ and $a = -\delta$ we have to calculate up to x_{n+7}. The result is

$$\tilde{x}_{n+6} = \widetilde{\phi_n^7}^{(y)}(1, \tilde{y}_n) = -1, \text{ and } \tilde{x}_{n+7} = \widetilde{\phi_n^7}^{(x)}(1, \tilde{y}_n) = \frac{1 + 2\tilde{y}_n}{2},$$

and we obtain $\phi_n^7\widetilde{(x_n, y_n)} = \widetilde{\phi_n^7}(\tilde{x}_n, \tilde{y}_n)$. Hence we have proved that the dP$_{\text{II}}$ equation has almost good reduction modulo $\mathfrak{p}$ at $\tilde{x}_n = 1$. We can proceed in the case $\tilde{x}_n = -1$ in an exactly similar manner. $\square$

From this proposition, the evolution of the dP$_{\text{II}}$ equation (2.1) over $\mathbb{PF}_p$ can be constructed from the initial values u_{n-1} and u_n.

---

[2]Precisely speaking, there are some special cases for $p = 3, 5$ where we have to consider the fact $\alpha_{n+p} = \alpha_n$ or $\beta_{n+p} = \beta_n$ during the iteration process. We can prove by straightforward calculations that similar results hold for these exceptional cases.

Now we consider special solutions to (2.1) over $\mathbb{PF}_p$. For the dP_{II} equation over $\mathbb{C}$, rational function solutions have already been obtained [19]. Let N be a positive integer and $\lambda \neq 0$ be a constant. Suppose that $a = -\frac{2(N+1)}{\lambda}, \quad \delta = z_0 = \frac{2}{\lambda},$

$$
L_k^{(\nu)}(\lambda) := \begin{cases} \sum_{r=0}^{k} (-1)^r \begin{pmatrix} k+\nu \\ k-r \end{pmatrix} \dfrac{\lambda^r}{r!} & (k \in \mathbb{Z}_{\geq 0}), \\ 0 & (k \in \mathbb{Z}_{<0}), \end{cases}
$$

and

$$(3.3) \qquad\qquad \tau_N^n := \det \left| L_{N+1-2i+j}^{(n)}(\lambda) \right|_{1 \leq i,j \leq N}.$$

Then a rational function solution of the dP_{II} equation is given by

$$(3.4) \qquad\qquad u_n = \frac{\tau_{N+1}^{n+1}\tau_N^{n-1}}{\tau_{N+1}^n \tau_N^n} - 1.$$

If we deal with the terms in (3.3) and (3.4) by arithmetic operations over $\mathbb{F}_p$, we encounter terms such as $\frac{1}{p}$ or $\frac{p}{p}$ and (3.4) is not well-defined. However, from proposition 3.3, we find that (3.4) gives a solution to the dP_{II} equation over $\mathbb{PF}_q$ by the reduction from $\mathbb{Q}$ ($\subset \mathbb{Q}_p$), as long as the solution avoids the points ($\tilde{\alpha}_n = 0$, $u_n = 1$) and ($\tilde{\beta}_n = 0$, $u_n = -1$), which is equivalent to the solution satisfying

$$(3.5) \qquad\qquad \tau_{N+1}^{-N-1}\tau_N^{-N-3} \not\equiv 0, \quad \frac{\tau_{N+1}^{N+1}\tau_N^{N-1}}{\tau_{N+1}^N \tau_N^N} \not\equiv 2,$$

where the superscripts are considered modulo p. Note that $\tau_N^n \equiv \tau_N^{n+p}$ for all integers N and n. In the table below, we give several *rational solutions to the dP_{II} equation* with $N = 3$ and $\lambda = 1$ over $\mathbb{PF}_q$ for $q = 3, 5, 7$ and 11. We see that the period of the solution is p.

p	$\tau_{N+1}^{-N-1}\tau_N^{-N-3}$	$\dfrac{\tau_{N+1}^{N+1}\tau_N^{N-1}}{\tau_{N+1}^N \tau_N^N}$	$\tilde{u}_1, \tilde{u}_2, \tilde{u}_3, \tilde{u}_4, \tilde{u}_5, \tilde{u}_6, \tilde{u}_7, \tilde{u}_8, \tilde{u}_9, \tilde{u}_{10}, \dots$
3	∞	∞	$\underbrace{1, 2, \infty}_{\text{period 3}}, 1, 2, \infty, 1, 2, \infty, 1, 2, \infty, 1, 2, \infty, \dots$
5	∞	4	$\underbrace{4, 2, 3, 1, \infty}_{\text{period 5}}, 4, 2, 3, 1, \infty, 4, 2, 3, 1, \infty, 4, \dots$
7	∞	0	$\underbrace{1, \infty, 6, 5, 1, \infty, 6}_{\text{period 7}}, 1, \infty, 6, 5, 1, \infty, 6, 1, \infty, \dots$
11	0	7	$\underbrace{\infty, 1, 6, 1, \infty, 10, \infty, 1, 0, 2, 10}_{\text{period 11}}, \infty, 1, 6, 1, \dots$

We see from the case of $p = 11$ that we may have an appropriate solution even if the condition (3.5) is not satisfied, although this is not always true. The dP_{II} equation

has linearized solutions also for $\delta = 2a$ [20]. With our new method, we can obtain the corresponding solutions without difficulty.

§4.   The p-adic analogue of the singularity confinement test

The above approach is closely related to the singularity confinement method which is an effective test to judge the integrability of the given equations [18]. In the proof of the Proposition 3.3, we have taken $x_n = 1 + ep^k$ and have shown that the limit

$$\lim_{|ep^k|_p \to 0} (x_{n+m}, x_{n+m+1})$$

is well defined for some positive integer m. Here ep^k $(k > 0, \ |e|_p = 1)$ is an alternative in $\mathbb{Q}_p$ for the infinitesimal parameter ϵ in the singularity confinement test in $\mathbb{C}$. Note that p^k $(k > 0)$ is a 'small' number in terms of the p-adic metric. From this observation and propositions 3.2, 3.3, we postulate that having almost good reduction in arithmetic mappings is similar to passing the singularity confinement test.

§5.   The q-discrete Painlevé equations over a finite field

In this section we study the q-discrete analogues of the Painlevé equations ($q\mathrm{P_I}$ and $q\mathrm{P_{II}}$ equations).

§5.1.   The $q\mathrm{P_I}$ equation

One of the forms of the $q\mathrm{P_I}$ equations is as follows:

$$(5.1) \qquad x_{n+1}x_{n-1} = \frac{aq^n x_n + b}{x_n^2},$$

where a and b are parameters. We rewrite (5.1) for our convenience as

$$(5.2) \qquad \Phi_n : \begin{cases} x_{n+1} = \dfrac{aq^n x_n + b}{x_n^2 y_n}, \\ y_{n+1} = x_n. \end{cases}$$

Similarly to the $\mathrm{dP_{II}}$ equation, we can prove the following proposition:

Proposition 5.1.   *Suppose that a, b, q are integers not divisible by p, then the mapping (5.2) has an almost good reduction modulo $\mathfrak{p}$ on the domain $\mathcal{D} := \{(x, y) \in \mathbb{Z}_p^2 \ | x \neq 0, y \neq 0\}$.*

Proof.   Let $(x_{n+1}, y_{n+1}) = \Phi_n(x_n, y_n)$. Just like we have done before, we have only to examine the cases $\tilde{x}_n = 0$ and $\tilde{y}_n = 0$. We use the abbreviation $\tilde{q} = q, \tilde{a} = a, \tilde{b} = b$ for simplicity. By direct computation we obtain;

(i) If $\tilde{x}_n = 0$ and $\tilde{y}_n \neq 0$, then

$$\Phi_n^3 \widetilde{(x_n, y_n)} = \widetilde{\Phi_n^3}(0, \tilde{y}_n) = \left(\frac{b^2}{a^2 q^2 \tilde{y}_n}, 0 \right).$$

(ii) If $\tilde{y}_n = 0$ and $\tilde{x}_n \neq 0$, then

$$\Phi_n^5 \widetilde{(x_n, y_n)} = \widetilde{\Phi_n^5}(\tilde{x}_n, 0) = \left(0, \frac{a^2 q^4}{b \tilde{x}_n} \right).$$

(iii) If $\tilde{x}_n = 0$ and $\tilde{y}_n = 0$, then

$$\Phi_n^8 \widetilde{(x_n, y_n)} = \widetilde{\Phi_n^8}(0, 0) = (0, 0).$$

$\square$

§5.2.   The $q\mathrm{P_{II}}$ equation

The $q\mathrm{P_{II}}$ equation is the following q-discrete equation:

(5.3) $$(z(q\tau)z(\tau) + 1)(z(\tau)z(q^{-1}\tau) + 1) = \frac{a\tau^2 z(\tau)}{\tau - z(\tau)},$$

where a and q are parameters [21]. It is also convenient to rewrite (5.3) as

(5.4) $$\Phi_n : \begin{cases} x_{n+1} = \dfrac{a(q^n \tau_0)^2 x_n - (q^n \tau_0 - x_n)(1 + x_n y_n)}{x_n(q^n \tau_0 - x_n)(x_n y_n + 1)}, \\ y_{n+1} = x_n, \end{cases}$$

where $\tau = q^n \tau_0$. Just like the $q\mathrm{P_I}$ equation, we can prove that $q\mathrm{P_{II}}$ has an almost good reduction:

Proposition 5.2.   *Suppose that a, q, τ_0 are integers not divisible by p, then the mapping (5.4) has an almost good reduction modulo $\mathfrak{p}$ on the domain $\mathcal{D} := \{(x, y) \in \mathbb{Z}_p^2 \,|\, x \neq 0, x \neq q^n \tau_0 \ (n \in \mathbb{Z}), xy + 1 \neq 0\}$.*

Proof.   Let $(x_{n+1}, y_{n+1}) = \Phi_n(x_n, y_n)$. Just like we have done before, we have only to examine the cases $\tilde{x}_n = 0, \widetilde{q^n \tau_0}$ and $-\tilde{y}_n^{-1}$. We obtain;
(i) If $\tilde{x}_n = 0$ and $-1 + q^2 - aq^2\tau^2 + q^3\tau^2 - q^2\tau\tilde{y}_n \neq 0$,

$$\Phi_n^3 \widetilde{(x_n, y_n)} = \widetilde{\Phi_n^3}(\tilde{x}_n = 0, \tilde{y}_n) = \left(\frac{1 - q^2 + aq^2\tau^2 - q^3\tau^2 - aq^4\tau^2 + q^2\tau\tilde{y}_n}{q^2\tau(-1 + q^2 - aq^2\tau^2 + q^3\tau^2 - q^2\tau\tilde{y}_n)}, q^2\tau \right).$$

(ii) If $\tilde{x}_n = 0$ and $-1 + q^2 - aq^2\tau^2 + q^3\tau^2 - q^2\tau\tilde{y}_n = 0$,

$$\Phi_n^5 \widetilde{(x_n, y_n)} = \widetilde{\Phi_n^5}(\tilde{x}_n = 0, \tilde{y}_n) = \left(\frac{1 - q^2 + q^7\tau^2 - aq^8\tau^2}{q^4\tau}, 0 \right).$$

(iii) If $\tilde{x}_n = \tau$ and $1 + \tau \tilde{y}_n \neq 0$,

$$
\begin{aligned}
\widetilde{\Phi_n^3(x_n, y_n)} &= \widetilde{\Phi_n^3}(\tilde{x}_n = \tau, \tilde{y}_n) \\
&= \left(\frac{1 - q^2 + (a + q - aq^2)q^2\tau^2 + (1 - q^2)\tau\tilde{y} + (1 - aq)q^3\tau^3\tilde{y}}{q^2\tau(1 + \tau\tilde{y}_n)}, 0 \right).
\end{aligned}
$$

(iv) If $\tilde{x}_n = \tau$ and $1 + \tau \tilde{y}_n = 0$,

$$
\widetilde{\Phi_n^7(x_n, y_n)} = \widetilde{\Phi_n^7}(\tilde{x}_n = \tau, \tilde{y}_n) = \left(\frac{1}{aq^{12}\tau^3}, -aq^{12}\tau^3 \right).
$$

(v) If $\tilde{x}_n \tilde{y}_n + 1 = 0$,

$$
\widetilde{\Phi_n^7(x_n, y_n)} = \widetilde{\Phi_n^7}(\tilde{x}_n = -\tilde{y}_n^{-1}, \tilde{y}_n) = \left(-\frac{1}{aq^{12}\tau^4\tilde{y}_n}, aq^{12}\tau^4\tilde{y}_n \right).
$$

Thus we complete the proof. $\square$

From this proposition we can define the time evolution of the $q\mathrm{P}_{\mathrm{II}}$ equation explicitly just like the $d\mathrm{P}_{\mathrm{II}}$ equation in the previous section.

Next we consider special solutions for $q\mathrm{P}_{\mathrm{II}}$ equation (5.3) over $\mathbb{PF}_p$. In [22] it has been proved that (5.3) over $\mathbb{C}$ with $a = q^{2N+1}$ ($N \in \mathbb{Z}$) is solved by the functions given by

$$
(5.5) \qquad z^{(N)}(\tau) = \begin{cases} \dfrac{g^{(N)}(\tau)g^{(N+1)}(q\tau)}{q^N g^{(N)}(q\tau)g^{(N+1)}(\tau)} & (N \geq 0), \\[3mm] \dfrac{g^{(N)}(\tau)g^{(N+1)}(q\tau)}{q^{N+1}g^{(N)}(q\tau)g^{(N+1)}(\tau)} & (N < 0), \end{cases}
$$

$$
(5.6) \qquad g^{(N)}(\tau) = \begin{cases} \left| w(q^{-i+2j-1}\tau) \right|_{1 \leq i,j \leq N} & (N > 0), \\[2mm] 1 & (N = 0), \\[2mm] \left| w(q^{i-2j}\tau) \right|_{1 \leq i,j \leq -N} & (N < 0), \end{cases}
$$

where $w(\tau)$ is a solution of the q-discrete Airy equation:

$$
(5.7) \qquad w(q\tau) - \tau w(\tau) + w(q^{-1}\tau) = 0.
$$

As in the case of the $d\mathrm{P}_{\mathrm{II}}$ equation, we can obtain the corresponding solutions to (5.5) over $\mathbb{PF}_p$ by reduction modulo $\mathfrak{p}$ according to the proposition 5.2. For that purpose, we have only to solve (5.7) over $\mathbb{Q}_p$. By elementary computation we obtain:

$$
(5.8) \qquad w(q^{n+1}\tau_0) = c_1 P_n(\tau_0; q) + c_0 P_{n-1}(q\tau_0; q),
$$

where c_0, c_1 are arbitrary constants and $P_n(x;q)$ is defined by the tridiagonal determinant:

$$P_n(x;q) := \begin{vmatrix} qx & -1 & & & \\ -1 & q^2x & -1 & & \text{\Large 0} \\ & \ddots & \ddots & \ddots & \\ & & -1 & q^{n-1}x & -1 \\ \text{\Large 0} & & & -1 & q^n x \end{vmatrix}.$$

The function $P_n(x;q)$ is the polynomial of nth order in x,

$$P_n(x;q) = \sum_{k=0}^{[n/2]} (-1)^k a_{n;k}(q) x^{n-2k},$$

where $a_{n;k}(q)$ are polynomials in q. If we let $i \ll j$ denotes $i < j-1$, and $c(j_1, j_2, ..., j_k) := \sum_{r=1}^{k}(2j_r + 1)$, then, we have

$$a_{n;k} = \sum_{1 \leq j_1 \ll j_2 \ll \cdots \ll j_k \leq n-1} q^{n(n+1)/2 - c(j_1, j_2, ..., j_k)}.$$

Therefore the solution of $q\mathrm{P_{II}}$ equation over $\mathbb{PF}_p$ is obtained by reduction modulo $\mathfrak{p}$ from (5.5), (5.6) and (5.8) over $\mathbb{Q}$ or $\mathbb{Q}_p$.

We can also prove that a type of q-discrete Painlevé III, IV and V equations have an almost good reduction on some appropriate domains. These facts justifies that almost good reduction can be a criterion for integrability of systems over finite fields. Proofs are fairly straightforward and will be reported in the future article [23].

§6.   The discrete KdV equation

In section 2, we have successfully determined the time evolution of the $\mathrm{dP_{II}}$ equation through the construction of the space of initial conditions of the $\mathrm{dP_{II}}$ equation by blowing-up twice at each of the singular points so that the mapping becomes bijective. However, for a general nonlinear equation, explicit construction of the space of initial conditions over a finite field is not so straightforward (for example see [16]) and it will not help us to obtain the explicit solutions.

In this section we study the soliton equations evolving as a two-dimensional lattice over finite fields by following the discussions made in [3]. For example, let us consider the discrete KdV equation

$$(6.1) \qquad\qquad \frac{1}{x_{n+1}^{t+1}} - \frac{1}{x_n^t} + \frac{\delta}{1+\delta}\left(x_n^{t+1} - x_{n+1}^t\right) = 0,$$

over a finite field $\mathbb{F}_r$ where $r = p^m$, p is a prime number and $m \in \mathbb{Z}_+$. Here $n, t \in \mathbb{Z}$ and δ is a parameter. If we put

$$\frac{1}{y_n^t} := (1 + \delta)\frac{1}{x_n^{t+1}} - \delta x_n^t$$

we obtain equivalent coupled equations

(6.2)
$$\begin{cases} x_n^{t+1} = \dfrac{(1+\delta)y_n^t}{1 + \delta x_n^t y_n^t}, \\[2mm] y_{n+1}^t = \dfrac{(1 + \delta x_n^t y_n^t)x_n^t}{1 + \delta}. \end{cases}$$

Clearly (6.2) does not determine the time evolution when $1 + \delta x_n^t y_n^t \equiv 0$. Over a field of characteristic 0 such as $\mathbb{C}$, the time evolution of (x_n^t, y_n^t) will not hit this exceptional line for generic initial conditions, but on the contrary, the evolution comes to this exceptional line in many cases over a finite field as a division by 0 appears. The mapping, $(x_n^t, y_n^t) \mapsto (x_n^{t+1}, y_{n+1}^t)$, is lifted to an automorphism of the surface $\tilde{X}$, where $\tilde{X}$ is obtained from $\mathbb{P}^1 \times \mathbb{P}^1$ by blowing up twice at $(0, \infty)$ and $(\infty, 0)$ respectively:

$$\tilde{X} = \mathbb{A}_{(0,\infty)} \cup \mathbb{A}_{(\infty,0)},$$
$$\mathbb{A}_{(0,\infty)} := \left\{ \left((x, y^{-1}), [\xi : \eta], [u : v]\right) \;\middle|\; x\eta = y^{-1}\xi, \; \eta u = y^{-1}(\eta + \delta\xi)v \right\} \subset \mathbb{A}^2 \times \mathbb{P}^1 \times \mathbb{P}^1,$$
$$\mathbb{A}_{(\infty,0)} := \left\{ \left((x^{-1}, y), [\xi : \eta], [w : z]\right) \;\middle|\; x^{-1}\eta = y\xi, \; (\eta + \delta\xi)u = y\eta v \right\} \subset \mathbb{A}^2 \times \mathbb{P}^1 \times \mathbb{P}^1.$$

To define the time evolution of the system with N lattice points from (6.2), however, we have to consider the mapping

$$(y_1^t; x_1^t, x_2^t, ..., x_N^t) \longmapsto (x_1^{t+1}, x_2^{t+1}, ..., x_N^{t+1}; y_{N+1}^t).$$

Since there seems no reasonable decomposition of $\tilde{X}$ into a direct product of two independent spaces, successive use of (6.2) becomes impossible. Note that if we blow down $\tilde{X}$ to $\mathbb{P}^1 \times \mathbb{P}^1$, the information of the initial values is lost in general. If we intend to construct an automorphism of a space of initial conditions, it will be inevitable to start from $\mathbb{P}^{N+1}$ and blow-up to some huge manifold, which is beyond the scope of the present paper. This difficulty seems to be one of the reasons why the singularity confinement method has not been used for construction of integrable partial difference equations or judgement for their integrability, though some attempts have been proposed in the bilinear form [26]. There should be so many exceptional hyperplanes in the space of initial conditions (if it does exist), and it is practically impossible to check all the "singular" patterns in the naïve extension of the singularity confinement test. On the other hand, when we fix the initial condition for a partial difference equation, the number of singular patterns is restricted in general and we have only to enlarge the domain so

that the mapping becomes well-defined. This is the strategy that we will adopt in this section.

First we explain how the indeterminate values appear through the time evolution by examining the discrete KdV equation (6.2) over $\mathbb{F}_7 := \{0, 1, 2, 3, 4, 5, 6\}$. If we take $\delta = 1$, (6.2) turns into

$$
\begin{cases}
x_n^{t+1} = \dfrac{2y_n^t}{1 + x_n^t y_n^t}, \\
y_{n+1}^t = \dfrac{(1 + x_n^t y_n^t)x_n^t}{2}.
\end{cases}
$$

Suppose that $x_1^0 = 6$, $x_2^0 = 5$, $y_1^0 = 2$, $y_1^1 = 2$, then we have

$$
x_1^1 = \frac{4}{13} \equiv 3, \quad y_2^0 = \frac{78}{2} \equiv 4 \quad \mod 7.
$$

With further calculation we have

$$
x_1^2 = \frac{4}{7} \equiv \frac{4}{0}, \quad y_2^1 = \frac{21}{2} \equiv 0, \quad x_2^1 = \frac{8}{21} \equiv \frac{1}{0}.
$$

Since $\dfrac{4}{0}$ and $\dfrac{1}{0}$ are not defined over $\mathbb{F}_7$, we now extend $\mathbb{F}_7$ to $\mathbb{PF}_7$ and take $\dfrac{j}{0} \equiv \infty$ for $j \in \{1, 2, 3, 4, 5, 6\}$. However, at the next time step, we have

$$
x_2^2 = \frac{2 \cdot 0}{1 + \infty \cdot 0}, \qquad y_3^1 = \frac{(1 + \infty \cdot 0) \cdot \infty}{2}
$$

and reach a deadlock.

Therefore we try the following two procedures: [I] we keep δ as a parameter for the same initial condition, and obtain as a system over $\mathbb{F}_7(\delta)$,

$$
x_1^1 = \frac{2(1 + \delta)}{1 + 5\delta}, \quad y_2^0 = \frac{6(1 + 5\delta)}{1 + \delta},
$$

$$
x_2^1 = \frac{6(1 + \delta)(1 + 5\delta)}{1 + 3\delta + 3\delta^2}, \quad y_2^1 = \frac{2(1 + 2\delta + 4\delta^2)}{(1 + 5\delta)^2}, \quad x_1^2 = \frac{2(1 + \delta)(1 + 5\delta)}{1 + 2\delta + 4\delta^2},
$$

$$
x_2^2 = \frac{4(1 + \delta)(2 + \delta)(3 + 2\delta)}{(1 + 5\delta)(5 + 5\delta + 2\delta^2)}, \quad y_3^1 = \frac{2(5 + 5\delta + 2\delta^2)}{(2 + \delta)^2}.
$$

[II] Then we put $\delta = 1$ to have a system over $\mathbb{PF}_7$ as

$$
x_1^1 = 3, \quad y_2^0 = 4, \quad x_2^1 = \frac{72}{7} \equiv \infty, \quad y_2^1 = \frac{14}{36} \equiv 0, \quad x_1^2 = \frac{24}{7} \equiv \infty,
$$

$$
x_2^2 = \frac{120}{72} \equiv 4, \quad y_3^1 = \frac{24}{9} \equiv 5.
$$

Thus all the values are uniquely determined over $\mathbb{PF}_7$. Figure 2 show a time evolution pattern of the discrete KdV equation (6.2) over $\mathbb{PF}_7$ for the initial conditions $x_1^0 = 6$, $x_2^0 = 5$, $x_3^0 = 4$, $x_4^0 = 3$, $x_j^0 = 2$ ($j \geq 5$) and $y_1^t = 2$ ($t \geq 0$).
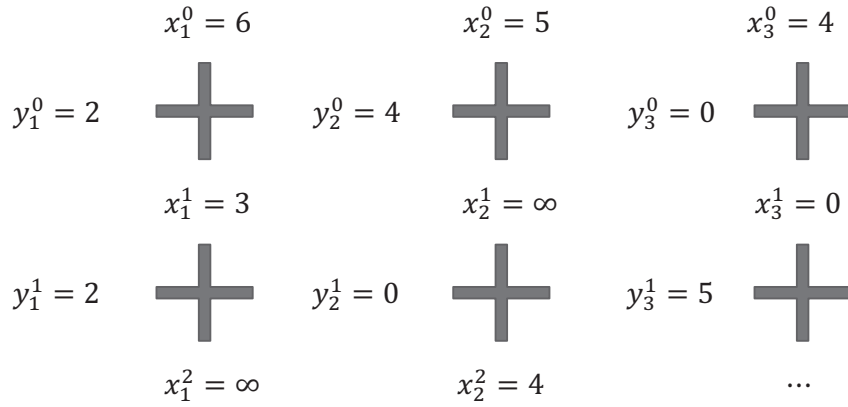
$$x_1^0 = 6 \qquad x_2^0 = 5 \qquad x_3^0 = 4$$

$$y_1^0 = 2 \qquad\qquad y_2^0 = 4 \qquad\qquad y_3^0 = 0$$

$$x_1^1 = 3 \qquad x_2^1 = \infty \qquad x_3^1 = 0$$

$$y_1^1 = 2 \qquad\qquad y_2^1 = 0 \qquad\qquad y_3^1 = 5$$

$$x_1^2 = \infty \qquad x_2^2 = 4 \qquad \cdots$$

Figure 2. An example of the time evolution of the coupled discrete KdV equation (6.2) over $\mathbb{PF}_7$ where $\delta = 1$.

This example suggests that the equation (6.2) should be understood as evolving over the field $\mathbb{F}_r(\delta)$, the rational function field with indeterminate δ over $\mathbb{F}_r$. To obtain the time evolution pattern over $\mathbb{PF}_r$, we have to substitute δ with a suitable value $\delta_0 \in \mathbb{F}_r$ ($\delta_0 = 1$ in the example above). This substitution can be expressed as the following reduction map:

$$\mathbb{F}_r(\delta)^\times \to \mathbb{PF}_r \;:\; (\delta - \delta_0)^s \frac{g(\delta - \delta_0)}{f(\delta - \delta_0)} \mapsto \begin{cases} 0 & (s > 0), \\ \infty & (s < 0), \\ \dfrac{g(0)}{f(0)} & (s = 0), \end{cases}$$

where $s \in \mathbb{Z}$, $f(h), g(h) \in \mathbb{F}_r[h]$ are co-prime polynomials and $f(0) \neq 0, g(0) \neq 0$. With this prescription, we know that $0/0$ does not appear and we can uniquely determine the time evolution for generic initial conditions defined over $\mathbb{F}_r$.

§ 6.1. Soliton solutions of the discrete KdV equation over finite fields

We consider the N-soliton solutions to (6.1) over $\mathbb{F}_r$. As mentioned in the introduction, the N-soliton solution is given as

$$x_n^t = \frac{\sigma_n^t \sigma_{n+1}^{t-1}}{\sigma_{n+1}^t \sigma_n^{t-1}},$$

$$\sigma_n^t := \det_{1 \leq i,j \leq N} \left(\delta_{ij} + \frac{\gamma_i}{l_i + l_j - 1} \left(\frac{1 - l_i}{l_i} \right)^t \left(\frac{l_i + \delta}{1 + \delta - l_i} \right)^n \right)$$

where γ_i, l_i $(i = 1, 2, ..., N)$ are arbitrary parameters but $l_i \neq l_j$ for $i \neq j$. When l_i, γ_i are chosen in $\mathbb{F}_r$, x_n^t becomes a rational function in $\mathbb{F}_r(\delta)$. Hence we obtain soliton
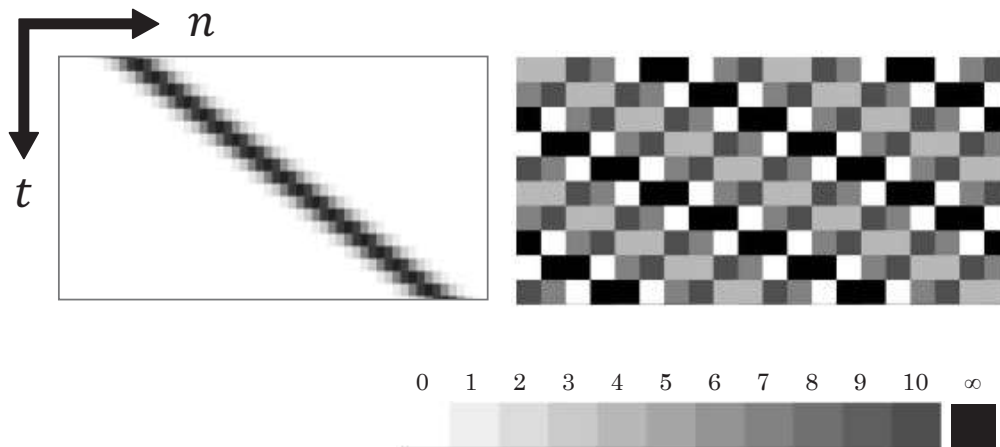
Figure 3. The one-soliton solution of the discrete KdV equation (6.1) over $\mathbb{R}$ (left) and $\mathbb{PF}_{11}$ (right) where $\delta = 7$, $\gamma_1 = 2$, $l_1 = 9$. Elements of $\mathbb{PF}_{11}$ are represented on the following grayscale: from 0 (white) to 10 (gray) and ∞ (black).

solutions over $\mathbb{PF}_r$ by substituting δ with a value in $\mathbb{F}_r$. The figures 3 and 4 show one and two soliton solutions for the discrete KdV equation (6.1) over the finite fields $\mathbb{PF}_{11}$ and $\mathbb{PF}_{19}$. The corresponding time evolutionary patterns on the field $\mathbb{R}$ are also presented for comparison.

The soliton solution of the discrete KdV equation over the finite field $\mathbb{F}_r$ has a period $r - 1$ since we have $a^{r-1} \equiv 1$ for all $a \in \mathbb{F}_r^{\times}$.

§6.2.   The discrete KdV equation over $\mathbb{Q}_p$

We can also define the time evolution of the discrete KdV equation over the field $\mathbb{F}_p$ by considering the system over the field of p-adic numbers $\mathbb{Q}_p$ instead of $\mathbb{F}_p(\delta)$, in the same way as we have done to the discrete Painlevé equations. We just have to compute the evolution of (6.2) or its soliton solutions over $\mathbb{Q}_p$ and then reduce the results to $\mathbb{F}_p$. (To deal with the equation over $\mathbb{F}_{p^m}$ ($m \geq 2$), we require the field extension of $\mathbb{Q}_p$.)

§7.   Concluding remarks

In this article we investigated the discrete Painlevé equations and discrete KdV equation over finite fields. To avoid indeterminacy, we examined two approaches. One is to extend the domain by blowing up at indeterminate points. According to the theory of the space of initial conditions, this approach is possible for all the discrete Painlevé equations. An interesting point is that the space of initial conditions over a finite field can be reduced to a minimal domain because of the discrete topology of the finite field. The other is to define the system over the larger field ($\mathbb{Q}_p$ in the case of dP$_{\text{II}}$, qP$_{\text{I}}$ and qP$_{\text{II}}$, or $\mathbb{F}_p(\delta)$ in the case of discrete KdV equation), and then
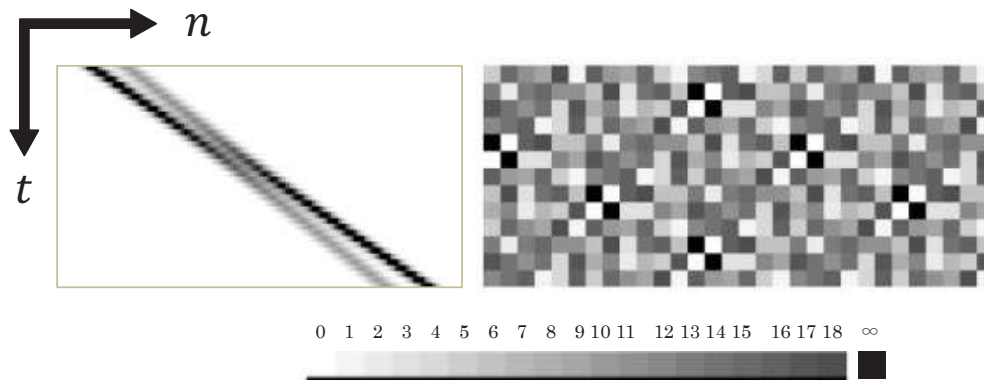
Figure 4. The two-soliton solution of the discrete KdV equation (6.1) over $\mathbb{R}$ (left) and $\mathbb{PF}_{19}$ (right) where $\delta = 8$, $\gamma_1 = 15$, $l_1 = 2$, $\gamma_2 = 9$, $l_2 = 4$. Elements of $\mathbb{PF}_{19}$ are represented on the following grayscale: from 0 (white) to 18 (gray) and ∞ (black). It is difficult to see the interaction of solitons over $\mathbb{PF}_{19}$.

reduce the results to finite fields. In particular the systems over $\mathbb{Q}_p$ attracted our attention. We defined a new integrability test (*almost good reduction*), which is an arithmetic analogue of the singularity confinement test, and proved that several types of the discrete Painlevé equations have this property. Thanks to this property, not only the time evolution of the discrete Painlevé equations can be well defined, but also a solution over $\mathbb{Q}$ (or $\mathbb{Q}_p$) can be directly transferred to a solution over $\mathbb{PF}_p$. This approach is equally valid in other discrete Painlevé equations and we expect that the same is true for its generalisations [24]. Furthermore, this 'almost good reduction' criterion is expected to be applied to finding higher order *integrable* mappings in arithmetic dynamics. In the last section, we studied the discrete KdV equation and showed that a similar approach is also useful in defining the discrete partial difference equations such as soliton equations over finite fields and in obtaining the soliton solutions of these equations. One of the future problems is to investigate the property of solitary waves of discrete KdV equation and other soliton equations such as discrete KP equation and discrete nonlinear Schrödinger equation over the finite field. Solving the initial value problems for these equations over the field of p-adic numbers, the field of rational functions and the finite fields is also an important problem to be studied.

Acknowledgement

References

[1] Kanki, M. Mada, J. Tamizhmani, K M. and Tokihiro, T., Discrete Painlevé II equation over finite fields, *J. Phys. A: Math. Theor.* **45** (2012), 342001 (8pp).

[2] Kanki, M. Mada, J. Tokihiro, T., The space of initial conditions and the property of an almost good reduction in discrete Painlevé II equations over finite fields, *preprint* arXiv:1209.0223.

[3] Kanki, M. Mada, J. and Tokihiro, T., Discrete integrable equations over finite fields, *SIGMA* **8** (2012) 054 (12pp).

[4] Okamoto, K., Studies on the Painlevé equations I, *Annali di Mathematica pura ed applicata*, **CXLVI** (1987) 337–381.

[5] Okamoto, K., Studies on the Painlevé equations II, *Japan J. Math.* **13** (1987), 47–76.

[6] Okamoto, K., Studies on the Painlevé equations III, *Math. Ann.* **275** (1986), 221–255.

[7] Okamoto, K., Studies on the Painlevé equations IV, *Funkcial. Ekvac. Ser. Int.* **30** (1987), 305–332.

[8] Sakai, H., Rational surfaces associated with affine root systems and geometry of the Painlevé equations, *Comm. Math. Phys.* **220**, (2001), 165–229.

[9] Silverman, J H., *The Arithmetic of Dynamical Systems*, (2007), Springer-Verlag, New York.

[10] Quispel, G R W. Roberts, J A G. and Thompson, C J., Integrable mappings and soliton equations II, *Physica D* **34** (1989), 183–192.

[11] Roberts, J A G., Order and symmetry in birational difference equations and their signatures over finite phase spaces, *Proceedings of the International Workshop Future Directions in Difference Equations*, Vigo, Spain, (2011), 213–221.

[12] Roberts, J A G. and Vivaldi, F., Arithmetical method to detect integrability in maps, *Phys. Rev. Lett.* **90** (2003), 034102.

[13] Roberts, J A G. and Vivaldi, F., Signature of time-reversal symmetry in polynomial automorphisms over finite fields, *Nonlinearity* **18** (2005), 2171–2192.

[14] Ramani, A. Grammaticos, B. and Hietarinta, J., Discrete versions of the Painlevé equations, *Phys. Rev. Lett.* **67** (1991), 1829–1832.

[15] Nijhoff, F W. and Papageorgiou, V G., Similarity reductions of integrable lattices and discrete analogues of the Painlevé II equation, *Phys. Lett. A* **153** (1991), 337–344.

[16] Takenawa, T., Discrete dynamical systems associated with root systems of indefinite type, *Comm. Math. Phys.* **224** (2001), 657–681.

[17] Murty, M R., *Introduction to p-adic Analytic Number Theory*, American Mathematical Society · International Press, (2002).

[18] Grammaticos, B. Ramani, A. and Papageorgiou, V., Do integrable mappings have the Painlevé property?, *Phys. Rev. Lett.* **67** (1991), 1825–1828.

[19] Kajiwara, K. Yamamoto, K. and Ohta, Y., Rational solutions for discrete Painlevé II equation, *Phys. Lett. A* **232** (1997), 189–199.

[20] Tamizhmani, K M. Tamizhmani, T. Grammaticos, B. and Ramani, A., Special Solutions for Discrete Painlevé Equations, in *Discrete Integrable Systems*, (2004), ed. by Grammaticos B, Tamizhmani T and Kosmann-Schwarzbach Y, Springer-Verlag Berlin Heidelberg.

[21] Kajiwara, K. Masuda, T. Noumi, M. Ohta, Y. and Yamada, Y., Hypergeometric solutions to the q-Painlevé equations, *Int. Math. Res. Not.* **2004** (2004), 2497–2521.

[22] Hamamoto, T. Kajiwara, K. and Witte, N S., Hypergeometric Solutions to the q-Painlevé Equation of Type $(A_1 + A_1')^{(1)}$, *Int. Math. Res. Not.* **2006** 84619 (2006), (26pp).

[23] Kanki, M., Integrability of discrete equations modulo a prime, *preprint* arXiv:1209.1715.

[24] Kajiwara, K. Noumi, M. and Yamada, Y., Discrete dynamical systems with $W(A_{m-1}^{(1)} \times A_{n-1}^{(1)})$ symmetry, *Lett. Math. Phys.* **60** (2002), 211–219.

[25] Doliwa, A. Białecki, M. and Klimczewski, P., The Hirota equation over finite fields: algebro-geometric approach and multisoliton solutions, *J. Phys. A: Math. Gen.* **36** (2003), 4827–4839.

[26] Ramani, A. Grammaticos, B. and Satsuma, J., Integrability of multidimensional discrete systems, *Phys. Lett. A* **169** (1992), 323–328.