Glasgow Math. J. **47A** (2005) 33–44. © 2005 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089505002260. Printed in the United Kingdom

INTEGRABLE KP AND KdV CELLULAR AUTOMATA OUT OF A HYPERELLIPTIC CURVE

MARIUSZ BIAŁECKI
Institute of Geophysics, Polish Academy of Sciences, ul. Księcia Janusza 64, 01-452 Warszawa, Poland,
Institute of Theoretical Physics, University of Bialystok, ul. Lipowa 41, 15-424 Białystok, Poland
e-mail: bialecki@igf.edu.pl

(Received 19 December, 2003; accepted 17 May, 2004)

Abstract. The goal of this paper is to present a solution of the cellular automaton associated with the discrete KdV equation, using an algebro-geometric solution of the discrete KP equation over a finite field out of a hyperelliptic curve.

2000 *Mathematics Subject Classification.* 14H70, 37K10, 37B15.

1. Introduction. Cellular automata (CA) are (solutions of) completely discrete dynamical systems, for which values of both independent and dependent variables are discrete. The concept of CA emerged in interaction with computational machines, and hence, CA are convenient tools for computer simulations of various phenomena. There is also an approach to CA, in which the main objective is to obtain "analytic" solutions (or full solutions or in a form good for investigation of their global properties) without need of performing step by step calculations. This leads naturally to the notion of integrability and integrable cellular automata (ICA). (For references to ICA see [**3**] or [**6**] .)

Recently a new method of construction of ICA was proposed in [**6**]. Its main idea is to keep the form of a given integrable discrete system and to transfer the algebro-geometric method of construction of its solutions [**10**, **1**], from the complex field $\mathbb{C}$ to a finite field case. In this framework, there were constructed finite field versions of multisoliton solutions for the fully discrete 2D Toda system (the Hirota equation) in [**6**], and for discrete KP and KdV equations (in Hirota form) in [**4**], and also algebro-geometric solutions of the discrete KP equation out of a hyperelliptic curve in [**3**].

In this paper we extend previous works to construct an algebro-geometric solution of the discrete KdV equation out of a hyperelliptic curve. To reach this aim we obtain a solution of the dKP equation in a form compatibile with the reduction from the dKP equation to the dKdV equation.

The paper is constructed as follows. In section 2 we first summarize the finite field version of the algebro-geometric construction of solutions of the discrete KP and KdV equations. In section 3 we apply the method to construct a solution of the discrete KP and KdV equations starting from an algebraic curve of genus two.

2. The finite field solution of the discrete KP equation out of nonsingular algebraic curves. We first shortly recall the algebro-geometric construction of solutions of

Key words and phrases. integrable systems; cellular automata; algebraic curves over finite fields; discrete KP equation; discrete KdV equation.

the discrete KP equation over finite fields and its reduction to the discrete KdV equation [**6**, **4**, **3**]. An algebro-geometric approach in case of a complex field $\mathbb{C}$ is described in [**1**]. Algebraic curves over finite fields are exposed for example in [**15**, **17**].

2.1. General construction for the dKP equation. For the general construction we need an algebraic projective curve $\mathcal{C}/\mathbb{K}$ (or simply $\mathcal{C}$), absolutely irreducible, nonsingular, of genus g, defined over the finite field $\mathbb{K} = \mathbb{F}_q$ with q elements. By $\mathcal{C}(\mathbb{K})$ we denote the set of $\mathbb{K}$-rational points of the curve. By $\overline{\mathbb{K}}$ we denote the algebraic closure of $\mathbb{K}$, i.e., $\overline{\mathbb{K}} = \bigcup_{\ell=1}^{\infty} \mathbb{F}_{q^\ell}$, and by $\mathcal{C}(\overline{\mathbb{K}})$ we denote the corresponding infinite set of $\overline{\mathbb{K}}$-rational points of the curve. Denote by $\mathrm{Div}(\mathcal{C})$ the abelian group of the divisors on the curve $\mathcal{C}$. The action of the Galois group $G(\overline{\mathbb{K}}/\mathbb{K})$ (of automorphisms of $\overline{\mathbb{K}}$ which are identity on $\mathbb{K}$) extends naturally to action on $\mathcal{C}(\overline{\mathbb{K}})$ and $\mathrm{Div}(\mathcal{C})$. A field of $\mathbb{K}$-rational functions on the curve $\mathcal{C}$ we denote by $\mathbb{K}(\mathcal{C})$ and the vector space $L(D)$ is defined as $\{f \in \overline{\mathbb{K}}(\mathcal{C}) \mid (f) > -D\}$, where $D \in \mathrm{Div}(\mathcal{C})$ and $(f) = \sum_{P\in\mathcal{C}} ord_P(f)\cdot P$ is the divisor of the function $f \in \mathbb{K}(\mathcal{C})$.

On the curve $\mathcal{C}$ we choose:

(1) four points $A_i \in \mathcal{C}(\mathbb{K})$, $i = 0, 1, 2, 3$,

(2) an effective $\mathbb{K}$-rational divisor of order g, i.e., g points $B_\gamma \in \mathcal{C}(\overline{\mathbb{K}})$, $\gamma = 1, \ldots, g$, which satisfy the following $\mathbb{K}$-rationality condition

$$\forall\sigma \in G(\overline{\mathbb{K}}/\mathbb{K}), \quad \sigma(B_\gamma) = B_{\gamma'}.$$

We assume that all the points used are distinct and in general positions. In particular, the divisor $\sum_{\gamma=1}^{g} B_\gamma$ (and a divisor $D(n_1, n_2, n_3)$ defined below) is non-special.

Definition 1. Fix a $\mathbb{K}$-rational local parameter t_0 at A_0. For any integers $n_1, n_2, n_3 \in \mathbb{Z}$ let the divisor $D(n_1, n_2, n_3)$ be of the form

$$D(n_1, n_2, n_3) = n_1(A_0 - A_1) + n_2(A_0 - A_2) + n_3(A_0 - A_3) + \sum_{\gamma=1}^{g} B_\gamma.$$

The function $\psi(n_1, n_2, n_3)$ (called a wave function) is a rational function on the curve $\mathcal{C}$ with the following properties

(1) the divisor of the function satisfies $(\psi) > -D$, i.e. $\psi \in L(D)$,

(2) the first nontrivial coefficient of its expansion in t_0 at A_0 is normalized to one.

Existence and uniqueness of the function $\psi(n_1, n_2, n_3)$ is due to application of the Riemann–Roch theorem with general position assumption and due to normalization. Moreover, the function $\psi(n_1, n_2, n_3)$ is $\mathbb{K}$-rational, which follows from $\mathbb{K}$-rationality conditions for sets of points in their definition.

Remark. Notice that the function $\psi(n_1, n_2, n_3)$ has g zeros not explicitly specified in the Definition 1.

The next step of the construction is to obtain linear equations for the wave functions. The full form of such equation is in the case when the pole of $\psi(n_1, n_2, n_3)$ at A_0 is of the order exactly $(n_1 + n_2 + n_3)$ and respective zeros at A_i are of the order n_i, for $i = 1, 2, 3$. We will call this case generic. Having fixed $\mathbb{K}$-rational local parameters t_i at A_i, $i = 1, 2, 3$, denote by $\zeta_k^{(i)}(n_1, n_2, n_3)$, $i = 1, 2, 3$, the $\mathbb{K}$-rational coefficients of expansion of $\psi(n_1, n_2, n_3)$ at A_i, respectively, i.e.,

$$\psi(n_1, n_2, n_3) = t_i^{n_i} \sum_{k=0}^{\infty} \zeta_k^{(i)}(n_1, n_2, n_3) t_i^k, \quad i = 1, 2, 3.$$

Denote by T_i the operator of translation in the variable n_i, $i = 1, 2, 3$, for example $T_2\psi(n_1, n_2, n_3) = \psi(n_1, n_2 + 1, n_3)$. The full linear equation is of the form

$$T_i\psi - T_j\psi + \frac{T_j\zeta_0^{(i)}}{\zeta_0^{(i)}}\psi = 0, \quad i \neq j, \quad i, j = 1, 2, 3. \tag{1}$$

It follows from observation, that $T_i\psi - T_j\psi \in L(D)$, hence must be proportional to the wave function ψ. Coefficients of proportionality can be obtained from comparison (the lowest degree terms) of expansions of left and right sides of (1) at the point A_i.

REMARK. When the genericity assumption fails then the linear problem (1) degenerates to the form $T_i\psi = \psi$ or even to $0 = 0$.

Notice that equation (1) gives

$$\frac{T_j\zeta_0^{(i)}}{\zeta_0^{(i)}} = -\frac{T_i\zeta_0^{(j)}}{\zeta_0^{(j)}}, \quad i \neq j, \quad i, j = 1, 2, 3. \tag{2}$$

Define

$$\rho_i = (-1)^{\sum_{j<i} n_j} \zeta_0^{(i)}, \quad i = 1, 2, 3, \tag{3}$$

then equation (2) implies existence of a $\mathbb{K}$-valued potential (the τ-function) defined (up to a multiplicative constant) by the formulas

$$\frac{T_i\tau}{\tau} = \rho_i, \quad i = 1, 2, 3. \tag{4}$$

Finally, equations (1) give rise to the condition

$$\frac{T_2\rho_1}{\rho_1} - \frac{T_3\rho_1}{\rho_1} + \frac{T_3\rho_2}{\rho_2} = 0, \tag{5}$$

which written in terms of the τ-function gives the discrete KP equation **[8]** called also the Hirota equation

$$(T_1\tau)\,(T_2T_3\tau) - (T_2\tau)\,(T_3T_1\tau) + (T_3\tau)\,(T_1T_2\tau) = 0. \tag{6}$$

REMARK. Equation (5) can be obtained also from expansion of equation (1) at A_k, where $k = 1, 2, 3$, $k \neq i, j$.

Absence of a term in the linear problem (1) reflects, due to the Remark above, in absence of the corresponding term in equation (6). This implies that in the non-generic case, when we have not defined the τ-function yet, we are forced to put it to zero.

2.2. Reduction to the dKdV equation. The discrete KdV equation [**7**, **11**]

$$(T_1\tau)\,\tau - \big(T_3^{-1}\tau\big)(T_3T_1\tau) + (T_3\tau)\big(T_1T_3^{-1}\tau\big) = 0, \tag{7}$$

is obtained from the discrete KP equation by imposing the constraint

$$T_2T_3\tau = \gamma\tau, \tag{8}$$

where γ is a non-zero constant. Algebro-geometric solutions of the discrete KdV equation can be constructed using the following the facts (see [**4**]).

LEMMA 1. *Assume that on the algebraic curve $\mathcal{C}$ there exists a rational function h with the following properties*

(1) *the divisor of the function is $(h) = A_2 + A_3 - 2A_0$,*

(2) *the first nontrivial coefficient of its expansion in the parameter t_0 at A_0 is normalized to one.*

Then the wave function ψ satisfies the following condition

$$T_2T_3\psi = h\psi. \tag{9}$$

REMARK. Existence of such a function h implies that the algebraic curve $\mathcal{C}$ is hyperelliptic.

PROPOSITION 2. *Let h be the function as in Lemma 1. Assume additionally that*

$$h(A_1) = 1. \tag{10}$$

Denote by δ_2 and δ_3 the respective first coefficients of the local expansion of h in parameters t_2 and t_3 at A_2 and A_3, i.e. $h = t_2(\delta_2 + \cdots)$, $h = t_3(\delta_3 + \cdots)$. Then the function

$$\tilde{\tau} = \tau\delta_2^{-n_2(n_2-1)/2}(-\delta_3)^{-n_3(n_3-1)/2} \tag{11}$$

satisfies the discrete KdV equation (7).

3. A "hyperelliptic" solution of the discrete KP and KdV equation.

Our goal here is to construct a solution of the dKP equation to which we can apply the reduction scheme described above. We are forced to perform steps of the construction (see also [**2**] for details) starting from a hyperelliptic curve. In detail we deal with a curve of genus $g = 2$ but the technical tools used here can be applied directly to hyperelliptic curves of arbitrary genus.

3.1. Hyperelliptic curves and Jacobian picture of the construction. In the following we use an affine picture of a hyperelliptic curve. It is motivated by the fact that a general hyperelliptic curve can be tranformed to a form with only one point at infinity (see [**16**]).

DEFINITION 2. A hyperelliptic curve $\mathcal{C}$ of genus g over a field $\mathbb{K}$ is given by

$$\mathcal{C}: \quad v^2 + h(u)v - f(u) = 0, \tag{12}$$

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

where $h(u) \in \mathbb{K}[u]$ is a polynomial of degree at most g, $f(u) \in \mathbb{K}[u]$ is a monic polynomial of degree $2g+1$, if there is no points $(u = x,\, v = y) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ which satisfy equation (12) and equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$.

By $\tilde{P}$ we denote the point opposite to P, i.e. conjugate with respect to hyperelliptic automorphism. Denote by $\mathrm{Div}^0(\mathcal{C};\mathbb{K})$ the abelian group of the $\mathbb{K}$-rational divisors on the curve $\mathcal{C}$ and by $J(\mathcal{C};\mathbb{K})$ the group of equivalence classes of $\mathbb{K}$-rational degree zero divisors $\mathrm{Div}^0(\mathcal{C};\mathbb{K})$ modulo the $\mathbb{K}$-rational principal divisors, i.e. divisors of a functions $\mathbb{K}(\mathcal{C})$. (In terms of algebraic geometry, $J(\mathcal{C};\mathbb{K})$ is identified with the group of $\mathbb{K}$-rational points of the Jacobian of the curve $\mathcal{C}$ [**12**, **14**].)

Two divisors $A, B \in \mathrm{Div}^0(\mathcal{C};\mathbb{K})$ are equivalent (we write $A \sim B$) if $B = A + (f)$ for some function $f \in \mathbb{K}(\mathcal{C})$. The class of a divisor A in the divisor class group $J(C;\mathbb{K})$ is denoted by $[A]$. For a hyperelliptic curve $\mathcal{C}$ (of genus g), each equivalence class $[A] \in J(C;\mathbb{K})$ has a unique representant in the form of a reduced divisor [**13**].

Definition 3. A divisor $D \in \mathrm{Div}^0(\mathcal{C};\mathbb{K})$ of the form

$$D = \sum_{\gamma=1}^{k} X_\gamma - k \cdot A_0,$$

where $X_\gamma \in \mathcal{C}\backslash\{A_0\}$ is called reduced if

(1) $k \le g$

(2) $\tilde{X}_\gamma \neq X_{\gamma'}$ for all $\gamma \neq \gamma'$.

Let us present in this picture the description of the wave function ψ and of the τ-function. Consider the following divisor $D(n_1, n_2, n_3) \in \mathrm{Div}^0(\mathcal{C};\mathbb{K})$ of degree zero

$$D(n_1, n_2, n_3) = n_1(A_0 - A_1) + n_2(A_0 - A_2) + n_3(A_0 - A_3) + \sum_{\gamma=1}^{g} B_\gamma - g \cdot A_0,$$

with linear dependence on n_1, n_2 and n_3. Its equivalence class in $J(\mathcal{C};\mathbb{K})$ has the unique $\mathbb{K}$-rational representant of the form of a reduced divisor

$$X(n_1, n_2, n_3) = \sum_{\gamma=1}^{k} X_\gamma(n_1, n_2, n_3) - k \cdot A_0.$$

This equivalence is given by a function whose divisor is

$$n_1(A_1 - A_0) + n_2(A_2 - A_0) + n_3(A_3 - A_0) + \sum_{\gamma=1}^{k} X_\gamma(n_1, n_2, n_3) - \sum_{\gamma=1}^{g} B_\gamma + (g-k)A_0.$$

If we normalize such a function at A_0, according to Definition 1, it becomes the wave function ψ. Notice that if $k \neq g$, it means that the pole of the wave function at A_0 is of order less then $(n_1 + n_2 + n_3)$, and it is a non-generic case, thus $\tau(n_1, n_2, n_3) = 0$.

Remark. Points X_γ indicate zeros of the wave function which are not explicitely specified in the previous construction.

Table 1. $\mathbb{F}_7$-rational points of the curve $\mathcal{C}$. The point opposite to P (conjugate with respect to the hyperelliptic automorphism) is denoted by $\tilde{P}$.

i	P_i	$\tilde{P}_i$
0	∞	P_0
1	(1, 1)	(1, 5)
2	(2, 2)	(2, 3)
3	(5, 3)	(5, 6)
4	(6, 4)	P_4

Table 2. $\mathbb{F}_{49}$-rational points of the curve $\mathcal{C}$ (which are not $\mathbb{F}_7$-rational); P^σ denotes conjugate to P with respect to the action of the Frobenius automorphism.

i	P_i	$\tilde{P}_i$	P_i^σ	$\tilde{P}_i^\sigma$
5	(0, 21)	(0, 28)	$\tilde{P}_5$	P_5
6	(3, 9)	(3, 44)	$\tilde{P}_6$	P_6
7	(4, 26)	(4, 33)	$\tilde{P}_7$	P_7
8	(7, 5)	(7, 44)	(42, 5)	(42, 9)
9	(8, 22)	(8, 26)	(43, 29)	(43, 33)
10	(11, 5)	(11, 47)	(46, 5)	(46, 12)
11	(12, 6)	(12, 45)	(47, 6)	(47, 10)
12	(13, 14)	(13, 29)	(48, 35)	(48, 22)
13	(14, 8)	(14, 34)	(35, 43)	(35, 27)
14	(15, 13)	(15, 28)	(36, 48)	(36, 21)
15	(16, 17)	(16, 23)	(37, 38)	(37, 30)
16	(17, 0)	(17, 39)	(38, 0)	(38, 18)
17	(18, 4)	(18, 41)	(39, 4)	(39, 20)
18	(19, 9)	(19, 28)	(40, 44)	(40, 21)
19	(20, 12)	(20, 31)	(41, 47)	(41, 24)
20	(22, 4)	(22, 30)	(29, 4)	(29, 23)
21	(25, 6)	(25, 32)	(32, 6)	(32, 25)
22	(27, 7)	(27, 22)	(34, 42)	(34, 29)

3.2. A curve and its Jacobian. Consider a hyperelliptic curve $\mathcal{C}$ of genus $g = 2$, defined over the field $\mathbb{F}_7$ and given by the equation

$$\mathcal{C}: \quad v^2 + uv = u^5 + 5u^4 + 6u^2 + u + 3. \tag{13}$$

The (u, v) coordinates of its $\mathbb{F}_7$-rational points are presented in Table 1. The only two special points of the curve are (6, 4) and the infinity point ∞.

We identify the field $\mathbb{F}_{49}$ with the extension of $\mathbb{F}_7$ by the polynomial $x^2 + 2$, i.e., $\mathbb{F}_{49} = \mathbb{F}_7[x]/(x^2 + 2)$. It is convenient to introduce the following notation: the element $k \in \mathbb{F}_{49}$ represented by the polynomial $\beta x + \alpha$ is denoted by the *natural* number $7\beta + \alpha$. The Galois group $G(\mathbb{F}_{49}/\mathbb{F}_7) = \{id, \sigma\}$, where σ is the Frobenius automorphism, acts on elements of $\mathbb{F}_{49}\backslash\mathbb{F}_7$ in the following way: $k = 7\beta + \alpha \mapsto \sigma(k) = 7(7 - \beta) + \alpha$. The coordinates of $\mathbb{F}_{49}$-rational points of the curve (which are not $\mathbb{F}_7$-rational) are presented in Table 2.

The full description of the group $J(\mathcal{C}; \mathbb{F}_7)$ is given in Table 3, where we have choosen as a reference point A_0 the infinity point ∞. The divisor $D_1 = P_1 - \infty$ generates the subgroup of order 31 and the divisor $D_4 = P_4 - \infty$ generates the subgroup of order 2. For $n \in \{0, 1, \dots, 30\}$ and $m \in \{0, 1\}$ we present the reduced representants of elements $[nD_1 + mD_4]_r$ of $J(\mathcal{C}; \mathbb{F}_7)$ and the transition functions $g_m(n)$ which are given by the equation

$$[nD_1 + mD_4]_r + D_1 = (g_m(n)) + [(n+1)D_1 + mD_4]_r,$$

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

Table 3. The group $J(\mathcal{C};\mathbb{F}_7)$ as the simple sum of its cyclic subgroups; $[X]_r$ denotes the reduced representant of the equivalence class of the divisor X; $g_0(n)$, $g_1(n)$ – transition functions (see main text).

n	$[nD_1]_r$	$g_0(n)$	$[nD_1+D_4]_r$	$g_1(n)$
0	0	1	$(6,4)-\infty$	1
1	$\mathbf{(1,1)-\infty}$	1	$(1,1)+(6,4)-2\infty$	$\frac{5+5u+3u^2+v}{6+4u+u^2}$
2	$(1,1)+(1,1)-2\infty$	$\frac{u+5u^2+v}{(2+u)^2}$	$(12,45)+(47,10)-2\infty$	$\frac{1+5u^2+v}{2+5u+u^2}$
3	$(5,6)+(5,6)-2\infty$	$\frac{1+u+4u^2+v}{(2+u)(5+u)}$	$(15,28)+(36,21)-2\infty$	$\frac{6u^2+v}{2+u^2}$
4	$(2,3)+(5,3)-2\infty$	$\frac{2+4u^2+v}{5+4u+u^2}$	$(7,44)+(42,9)-2\infty$	$\frac{5+u+v}{4+6u+u^2}$
5	$(19,9)+(40,44)-2\infty$	$\frac{4u+2u^2+v}{5+5u+u^2}$	$(11,5)+(46,5)-2\infty$	$\frac{6+6u+u^2+v}{3+6u+u^2}$
6	$(22,4)+(29,4)-2\infty$	$\frac{5+2u+6u^2+v}{(2+u)(5+u)}$	$(18,41)+(39,20)-2\infty$	$\frac{5+3u+5u^2+v}{5+3u+u^2}$
7	$(2,3)+(5,6)-2\infty$	$\frac{5+6u+2u^2+v}{5+2u+u^2}$	$(16,17)+(37,38)-2\infty$	$\frac{5+4u+4u^2+v}{3+u+u^2}$
8	$(27,22)+(34,29)-2\infty$	$\frac{1+3u+2u^2+v}{1+u^2}$	$(17,39)+(38,18)-2\infty$	$\frac{3+2u+u^2+v}{(5+u)(6+u)}$
9	$(14,34)+(35,27)-2\infty$	$\frac{1+5u+v}{(1+u)(5+u)}$	$(1,5)+(2,2)-2\infty$	$6+u$
10	$(2,2)+(6,4)-2\infty$	$\frac{3+5u+5u^2+v}{(5+u)^2}$	$\mathbf{(2,2)-\infty}$	1
11	$(2,3)+(2,3)-2\infty$	$\frac{6+u+6u^2+v}{3+2u+u^2}$	$(1,1)+(2,2)-2\infty$	$\frac{4+2u^2+v}{3+5u+u^2}$
12	$(13,14)+(48,35)-2\infty$	$\frac{3+6u+4u^2+v}{2+2u+u^2}$	$(8,22)+(43,29)-2\infty$	$\frac{2+4u+v}{(2+u)(6+u)}$
13	$(20,12)+(41,47)-2\infty$	$\frac{5u+u^2+v}{(1+u)(2+u)}$	$(1,5)+(5,3)-2\infty$	$6+u$
14	$(5,3)+(6,4)-2\infty$	$\frac{6+5u+2u^2+v}{6+6u+u^2}$	$(5,3)-\infty$	1
15	$(25,32)+(32,25)-2\infty$	$\frac{5+u^2+v}{6+6u+u^2}$	$(1,1)+(5,3)-2\infty$	$\frac{u+5u^2+v}{(2+u)(6+u)}$
16	$(25,6)+(32,6)-2\infty$	$\frac{6+5u+2u^2+v}{(1+u)(2+u)}$	$(1,5)+(5,6)-2\infty$	$6+u$
17	$(5,6)+(6,4)-2\infty$	$\frac{5u+u^2+v}{2+2u+u^2}$	$(5,6)-\infty$	1
18	$(20,31)+(41,24)-2\infty$	$\frac{3+6u+4u^2+v}{3+2u+u^2}$	$(1,1)+(5,6)-2\infty$	$\frac{2+4u+v}{3+5u+u^2}$
19	$(13,29)+(48,22)-2\infty$	$\frac{6+u+6u^2+v}{(5+u)^2}$	$(8,26)+(43,33)-2\infty$	$\frac{4+2u^2+v}{(5+u)(6+u)}$
20	$(2,2)+(2,2)-2\infty$	$\frac{3+5u+5u^2+v}{(1+u)(5+u)}$	$(1,5)+(2,3)-2\infty$	$6+u$
21	$(2,3)+(6,4)-2\infty$	$\frac{1+5u+v}{1+u^2}$	$(2,3)-\infty$	1
22	$(14,8)+(35,43)-2\infty$	$\frac{1+3u+2u^2+v}{5+2u+u^2}$	$(1,1)+(2,3)-2\infty$	$\frac{3+2u+u^2+v}{3+u+u^2}$
23	$(27,7)+(34,42)-2\infty$	$\frac{5+6u+2u^2+v}{(2+u)(5+u)}$	$(17,0)+(38,0)-2\infty$	$\frac{5+4u+4u^2+v}{5+3u+u^2}$
24	$(2,2)+(5,3)-2\infty$	$\frac{5+2u+6u^2+v}{5+5u+u^2}$	$(16,23)+(37,30)-2\infty$	$\frac{5+3u+5u^2+v}{3+6u+u^2}$
25	$(22,30)+(29,23)-2\infty$	$\frac{4u+2u^2+v}{5+4u+u^2}$	$(18,4)+(39,4)-2\infty$	$\frac{6+6u+u^2+v}{4+6u+u^2}$
26	$(19,28)+(40,21)-2\infty$	$\frac{2+4u^2+v}{(2+u)(5+u)}$	$(11,47)+(46,12)-2\infty$	$\frac{5+u+v}{2+u^2}$
27	$(2,2)+(5,6)-2\infty$	$\frac{1+u+4u^2+v}{(2+u)^2}$	$(7,5)+(42,5)-2\infty$	$\frac{6u^2+v}{2+5u+u^2}$
28	$(5,3)+(5,3)-2\infty$	$\frac{u+5u^2+v}{(6+u)^2}$	$(15,13)+(36,48)-2\infty$	$\frac{1+5u^2+v}{6+4u+u^2}$
29	$(1,5)+(1,5)-2\infty$	$(6+u)$	$\mathbf{(12,6)+(47,6)-2\infty}$	$\frac{5+5u+3u^2+v}{(1+u)(6+u)}$
30	$\mathbf{(1,5)-\infty}$	$(6+u)$	$(1,5)+(6,4)-2\infty$	$6+u$

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

and normalized (numerators and denominators are monic polynomials). We will use them in the construction below.

3.3. Construction of the wave and τ functions. In order to find a solution of the discrete KdV equation let us fix the following points of the curve $\mathcal{C}$:

$$A_0 = \infty, \quad A_1 = (2, 2), \quad A_2 = (1, 5), \quad A_3 = (1, 1),$$

with the uniformizing parameters $t_0 = u^2/v,\ t_1 = u - 2,\ t_2 = t_3 = u - 1$, and

$$B_1 = (12, 6), \quad B_2 = (47, 6).$$

Then

$$A_1 - A_0 \sim 10D_1 + D_4, \qquad A_2 - A_0 \sim -D_1 \sim 30D_1, \qquad A_3 - A_0 \sim D_1,$$
$$B_1 + B_2 - 2A_0 \sim 29D_1 + D_4,$$

and the points $X_1(n_1, n_2, n_3)$ and $X_2(n_1, n_2, n_3)$, where the wave function $\psi(n_1, n_2, n_3)$ has additional zeros (here X_i **can** be ∞) can be found from Table 3 and

$$X_1(n_1, n_2, n_3) + X_2(n_1, n_2, n_3) - 2\infty = [nD_1 + mD_4]_r, \tag{14}$$

where $n \in \{0, 1, \ldots, 30\}$ and $m \in \{0, 1\}$ are given by

$$n \equiv 29 - (n_3 - n_2 + 10n_1) \mod 31, \tag{15}$$
$$m \equiv 1 - n_1 \mod 2. \tag{16}$$

Remark. The choice of the infinity point ∞ as A_0 is a violation of the assumption of general position of points used in the construction (∞ is the Weierstrass point of the curve $\mathcal{C}$). This will not destroy the construction but in some situations, which we will point out, will affect uniqueness of the wave function. We remark that such a choice is indispensable in reduction of the method from the discrete KP equation to the discrete KdV equation (see, for example [**11**, **4**]).

The key idea in constructing of the wave function is to express $\psi(n_1, n_2, n_3)$ for any parameters from $(n_1, n_2, n_3) \in \mathbb{Z}^3$ by a set of functions related to $J(\mathcal{C}; \mathbb{K})$ (transition functions and few auxiliary functions). Let us introduce functions h_1 and h_4 corresponding to generators of the two cyclic subgroups of $J(\mathcal{C}; \mathbb{F}_7)$. The function h_1 with the divisor $31D_1 \sim 0$ and normalized at the infinity point is equal to

$$h_1 = \prod_{i=0}^{30} g_0(i),$$

and reads

$$h_1 = 1 + 2u + u^2 + 4u^3 + 3u^5 + u^6 + 3u^7 + u^8 + 4u^9 + 4u^{10} + 2u^{11} + 5u^{12}$$
$$+ 2u^{13} + 4u^{14} + 3u^{15} + (5u + 2u^2 + 5u^3 + 4u^5 + 6u^6 + 4u^7 + 3u^9$$
$$+ 5u^{10} + 5u^{11} + 4u^{12} + u^{13})v,$$

where we also used the equation of the curve (13) to reduce higher order terms in v. The normalized function h_4 with the divisor $2D_4 \sim 0$ is

$$h_4 = u - 6.$$

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

Let us introduce other auxilliary functions f_1 and f_2 to factorise the zeros at A_1 and A_2 of the wave function. Notice that

$$(2,2) + 21(1,1) + (6,4) - 23\infty \sim 0,$$

which implies that there exists a polynomial function on $\mathcal{C}$ with simple zero at A_1 and other zeros in the distinguished (by our choice of description of $J(\mathcal{C};\mathbb{F}_7)$) points $(1,1)$ and $(6,4)$. Define f_1 as the unique such function normalized at the infinity point ∞, then

$$\begin{aligned} f_1 = {} & 1 + 5u + u^2 + 4u^4 + 6u^5 + 4u^6 + 4u^7 + 3u^8 + 4u^9 \\ & + 6u^{11} + (6 + 4u + 2u^2 + 5u^3 + 6u^4 + 6u^6 + u^7 + u^8 + u^9)v. \end{aligned}$$

The zeros at A_2 can be factorised using function

$$f_2 = (u-1).$$

Uniqueness of the wave function ψ implies that it can be decomposed as follows

$$\psi(n_1,n_2,n_3) = \frac{f_1^{n_1} f_2^{n_2}}{h_1^p h_4^q} W(m_1,m_2), \tag{17}$$

where new variables m_1 and m_2 are given by

$$21n_1 - n_2 + n_3 = 31p - m_1, \quad m_1 \in \{0,1,\ldots,30\}, \tag{18}$$

$$n_1 = 2q - m_2, \quad m_2 \in \{0,1\}, \tag{19}$$

and the function $W(m_1,m_2)$ has the divisor

$$m_1 D_1 + m_2 D_4 + Y_1(m_1,m_2) + Y_2(m_1,m_2) - (12,6) - (47,6). \tag{20}$$

The additional zeros

$$Y_1(m_1,m_2) + Y_2(m_1,m_2) = X_1(n_1,n_2,n_3) + X_2(n_1,n_2,n_3),$$

can be found by projection from n-variables into the m-variables.

To find the functions $W(m_1,m_2)$ for all $m_1 \in \{0,1,\ldots,30\}$ and $m_2 \in \{0,1\}$ let us notice that $W(0,0) = 1$ and $W(0,1)$ is given by

$$(W(0,1)) = D_4 + (1,5) + (1,5) - (12,6) - (47,6),$$

and hence can be written in a form

$$W(0,1) = \frac{2 + 3u + 4u^2 + v}{6 + 4u + u^2}.$$

Define the multipliers $w_{m_2}(m_1)$ as follows

$$W(m_1,m_2) = w_{m_2}(m_1) W(m_1 - 1, m_2),$$

for $m_1 \in \{0,1,\ldots,30\}$ and $m_2 \in \{0,1\}$. Equations (14)–(16) and (18)–(20) give

$$w_{m_2}(m_1) = g_m(n),$$

where

$$m_2 = 1 - m \mod 2, \qquad m_1 = 29 - n \mod 31.$$

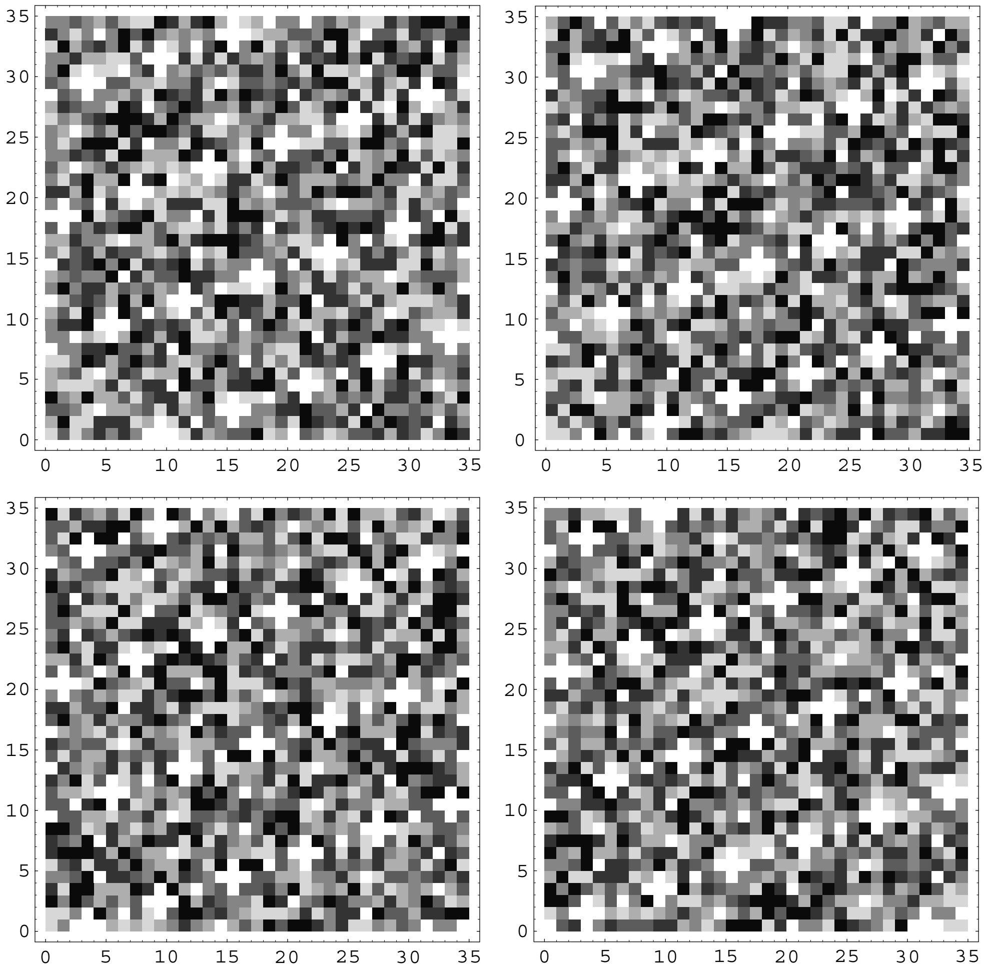
https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

Setting $w_{m_2}(0) = W(0, m_2)$ we obtain

$$W(m_1, m_2) = \prod_{i=0}^{m_1} w_{m_2}(i).$$

Together with factorisation (17) it gives the wave function ψ for all $(n_1, n_2, n_3) \in \mathbb{Z}^3$.

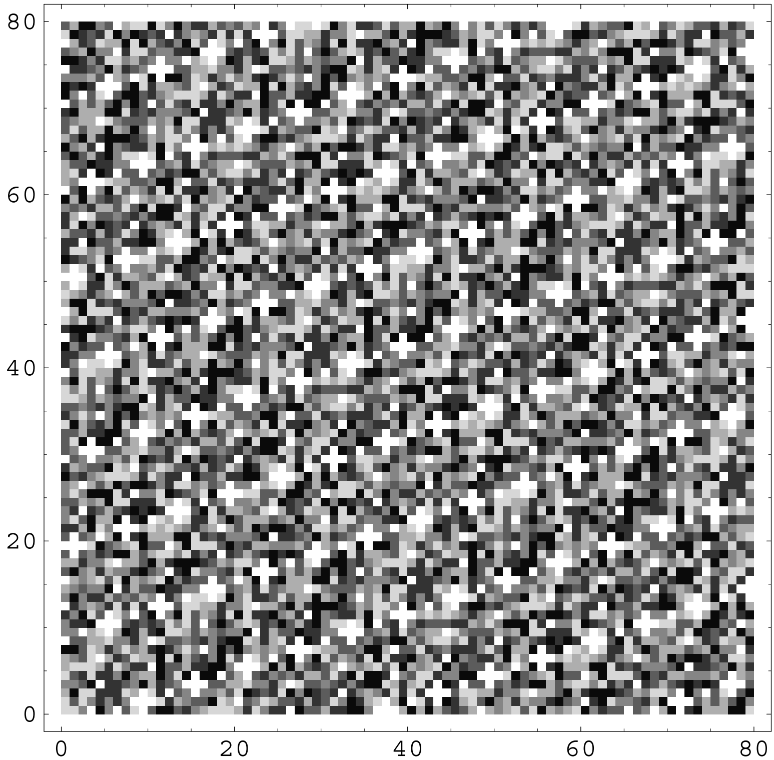
Remark. For $(m_1, m_2) = (29, 1)$ we have $X_1 = X_2 = \infty$. Because the infinity point ∞ is the Weierstrass point of order two, there exist functions with divisor of poles equal to 2∞. This means that ψ is not uniqely determined in this case. However it is natural to keep the divisor of ψ, and therefore ψ itself, exactly like it is given from the flow on $J(\mathcal{C}; \mathbb{K})$. Notice that because for $X_1 = X_2 = \infty$ we stay in the non-generic case, then this ambiguity does not affect construction of the τ-function.



□ – (00), □ – (01), □ – (02), □ – (03), □ – (04), □ – (05), □ – (06)

Figure 1. The $\mathbb{F}_7$-valued solution of the discrete KP equation out of genus $g = 2$ hyperelliptic curve $\mathcal{C}$; $n_2 = -1, 0, 1, 2$ for subsequent figures, $n_1 = 0, 1, \ldots, 34$ (horizontal axis), $n_3 = 0, 1, \ldots, 34$ (vertical axis)

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press



□ – (00), □ – (01), □ – (02), □ – (03), ■ – (04), ■ – (05), ■ – (06)

Figure 2. The $\mathbb{F}_7$-valued solution of the discrete KdV equation out of genus $g = 2$ hyperelliptic curve $\mathcal{C}$; $n_1 = 0, 1, \ldots, 79$ (horizontal), $n_3 = 0, 1, \ldots, 79$ (vertical), $(n_2 = 0)$

The coefficients $\zeta_0{}^{(k)}(n_1, n_2, n_3)$, $k = 1, 2, 3$, of expansion of the wave function can be obtained from factorisation (17) and are given by

$$(2,2): \quad \zeta_0^{(1)}(n_1, n_2, n_3) = 6^{n_1} 5^q 4^p W(m_1, m_2)|_{t_1=0}, \tag{21}$$

$$(1,5): \quad \zeta_0^{(2)}(n_1, n_2, n_3) = 2^{n_1} 4^q W(m_1, m_2)|_{t_2=0}, \tag{22}$$

$$(1,1): \quad \zeta_0^{(3)}(n_1, n_2, n_3) = 6^p 4^q \left.\frac{W(m_1, m_2)}{t_3^{m_1}}\right|_{t_3=0}. \tag{23}$$

Using the definition of the τ-function for nonzero ρ_i, i.e. equation (4), and putting $\tau = 0$ for points related with nongeneric case we obtain a solution of the discrete KP equation (6) taking value in the finite field $\mathbb{F}_7$. This τ-function is presented in Figure 1.

To obtain a $\tilde{\tau}$-function which is a solution of the discrete KdV equation we use the formula (11). For our settings we have $\delta_2 = \delta_3 = 1$, so finally

$$\tilde{\tau} = \tau(-1)^{-n_3(n_3-1)/2}.$$

The $\tilde{\tau}$-function which is a solution of the discrete KdV equation is presented in Figure 2.

https://doi.org/10.1017/S0017089505002260 Published online by Cambridge University Press

Equations (21)–(23) with (18)–(19) and the cyclic structure of the multiplicative group $\mathbb{K}^*$ (of nonzero elements of finite field $\mathbb{K}$) imply periodicity of the functions $\zeta_0^{(i)}$ and ρ_i for $i = 1, 2, 3$. In finite field case the τ-function and $\tilde{\tau}$-function are also periodic. Positions of the zeros of the τ-function (and the $\tilde{\tau}$-function), marked in figures, directly reflect the cyclic structure of the group $J(\mathcal{C}; \mathbb{K})$.

ACKNOWLEDGMENTS. The author would like to thank prof. Adam Doliwa for "multidimensional" help. The paper was partially supported by the KBN grant 2 P03B 12622.

REFERENCES

1. E. D. Belokolos, A. I. Bobenko, V. Z. Enol'skii, A. R. Its and V. B. Matveev, Algebro-geometric approach to nonlinear integrable equations (Springer-Verlag, 1994).

2. M. Białecki, *Methods of algebraic geometry over finite fields in construction of integrable cellular automata*, PhD dissertation, Warsaw University, Institute of Theoretical Physics, 2003 (in Polish).

3. M. Białecki and A. Doliwa, Algebro-geometric solution of the dKP equation over a finite field out of a hyperelliptic curve, *Commun. Math. Phys.* **253** (2005), 157–170.

4. M. Białecki and A. Doliwa, The discrete KP and KdV equations over finite fields, *Theor. Math. Phys*. **137**(1) (2003), 1412–1418.

5. G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry* (Springer-Verlag, 1986).

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

7. R. Hirota, Nonlinear partial difference equations. I. A difference analogue of the Korteweg-de Vries equation, *J. Phys. Soc. Japan* **43** (1977), 1424–1433.

8. R. Hirota, Discrete analogue of a generalized Toda equation, *J. Phys. Soc. Japan* **50** (1981), 3785–3791.

9. N. Koblitz, *Algebraic aspects of cryptography* (Springer-Verlag, 1998).

10. I. M. Krichever, Algebraic curves and nonlinear difference equations, *Uspiekhi Mat. Nauk* **33:4** (1978), 215–216.

11. I. M. Krichever, P. Wiegmann and A. Zabrodin, Elliptic solutions to difference non-linear equations and related many body problems, *Commun. Math. Phys*. **193** (1998), 373–396.

12. S. Lang, *Abelian varieties* (Interscience Publishers, Inc., New York, 1958).

13. A. J. Menezes, Y. H. Wu and R. J. Zuccherato, An elementary introduction to hyperelliptic curves, Appendix in [**9**].

14. J. S. Milne, *Jacobian varieties*, Chapter VII in [**5**].

15. C. Moreno, *Algebraic curves over finite fields* (Cambridge University Press, 1991).

16. I. Shafarevich, *Basic Algebraic Geometry* (Springer-Verlag, 1974).

17. H. Stichtenoth, *Algebraic function fields and codes* (Springer-Verlag, 1993).