The Hirota equation over finite fields: algebro-geometric approach and multisoliton solutions

2003 J. Phys. A: Math. Gen. 36 4827

(http://iopscience.iop.org/0305-4470/36/17/309)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **36** (2003) 4827–4839 PII: S0305-4470(03)56674-4

The Hirota equation over finite fields: algebro-geometric approach and multisoliton solutions

A Doliwa[1], **M Białecki**[2,3,4] **and P Klimczewski**[2]

[1] Wydział Matematyki i Informatyki, Uniwersytet Warmińsko–Mazurski, ul. Żołnierska 14A, 10-561 Olsztyn, Poland
[2] Instytut Fizyki Teoretycznej, Uniwersytet Warszawski, ul. Hoża 69, 00-681 Warszawa, Poland
[3] Instytut Geofizyki PAN, ul. Księcia Janusza 64, 01-452 Warszawa, Poland
[4] Instytut Fizyki Teoretycznej, Uniwersytet w Białymstoku, ul. Lipowa 41, 15-424 Białystok, Poland

Received 25 November 2002
Published 16 April 2003
Online at stacks.iop.org/JPhysA/36/4827

Abstract

We consider the Hirota equation (the discrete analogue of the generalized Toda system) over a finite field. We present the general algebro-geometric method of construction of solutions of the equation. As an example we construct analogues of the multisoliton solutions for which the wavefunctions and the τ-function can be found using rational functions. Within the class of multisoliton solutions we isolate generalized breather-type solutions which have no direct counterparts in the complex field case.

PACS numbers: 02.30.Ik, 02.10.−v, 05.45.−a

(Some figures in this article are in colour only in the electronic version)

1. Introduction

Cellular automata are mathematical models of physical systems in which space and time variables are discrete, and physical quantities take only a finite number of values [34]. In spite of a simple formulation they are capable of describing a wide variety of phenomena, for example, traffic flow, immune systems, flow through porous media, fluid dynamics and ferromagnetism. Due to their completely discrete nature, cellular automata are naturally suitable for computer simulations. However, in this field there are not so many exact analytical results providing solutions with a given global behaviour. The aim of this paper is to present a general method of construction of solutions to the cellular automaton associated with the Hirota equation.

The Hirota equation [18], the integrable discretization of the generalized Toda system [27], is one of the most important soliton equations. Its various limits give rise to a variety of integrable equations, moreover it is the basic system for studying solvable quantum models [21].

Like many other integrable systems the Hirota equation has a simple geometric interpretation. In this paper, we will use the following (geometric) form of the Hirota equation:

$$\tau_m(n_1, n_2)\tau_m(n_1+1, n_2+1) \\ = \tau_m(n_1+1, n_2)\tau_m(n_1, n_2+1) - \tau_{m-1}(n_1+1, n_2)\tau_{m+1}(n_1, n_2+1). \qquad (1)$$

One can describe it as the equation governing the so-called Laplace sequence of two-dimensional lattices of planar quadrilaterals [7, 10]. This interpretation can be embedded into a more general theory of multidimensional lattices of planar quadrilaterals and their transformations [12–15]. It was noted in [8, 9] that geometric constructions in the integrable discrete geometry (in particular, those leading to the Hirota equation) should work also on the level of finite geometries [19], i.e. geometries over finite fields [24]. This observation has been developed in this paper.

The question of construction of integrable systems with solutions taking values in a discrete set (soliton cellular automata) is not new and it was undertaken in a number of papers, see, for example, [5, 6, 28, 33]. In particular, in [5] the other Hirota equation (equivalent to the discrete sine-Gordon equation [17]) is investigated in the context of finite fields.

In this paper, we present the general method of finding solutions of the Hirota equation (1) over finite fields by using algebro-geometric methods, standard in a complex domain in the soliton theory [3, 22]. We change, however, the field of definition of the underlying algebraic curves from complex numbers to a finite field (see also earlier algebro-geometric papers [2, 16, 29, 32] where such a possibility was considered).

It turns out that algebraic geometry over finite fields has recently become very important in practical use, especially in modern approaches to public key cryptography [20] and in the theory of error correcting codes [31]. With respect to the last application we would like to mention [30] where the dynamics of the finite Toda molecule (a reduction of the Hirota equation) over finite fields was studied from the point of view of a decoding algorithm.

We do not present here a direct connection of the objects of this paper with the integrable discrete geometry over finite fields. This connection becomes clear when the approach to the Hirota equation presented here (see also [22]) is compared with the results of [1, 11, 12], where the methods of algebraic geometry over the field of complex numbers have been applied to construct integrable geometric lattices.

The layout of this paper is as follows. In section 2 we present the general algebro-geometric scheme for construction of solutions of the Hirota equation. Section 3 is devoted to the construction of a multisoliton solution on an algebraic curve starting from the vacuum solution. Finally, in section 4 we give in explicit form the solutions of the Hirota equation for the background algebraic curve being the projective line. In particular, we present the mechanism (based on the action of the Galois group) of generation of generalized breather-type solutions and discuss the periodicity of the solutions.

2. Solutions of the Hirota equation from algebraic curves over finite fields

This section is motivated by an algebro-geometric (over the complex field) approach to the Hirota equation (in a different form) [22] and by [1, 11, 12] on the application of algebro-geometric methods to integrable discrete geometry. It turns out that the basic ideas of the algebro-geometric approach to soliton theory can be transferred to the level of integrable systems in finite fields. The notions and results forming the theory of algebraic curves over finite fields which we use here can be found in [31].

Consider an algebraic projective curve, absolutely irreducible, nonsingular, of genus g, defined over the finite field $\mathbb{K} = \mathbb{F}_q$ with q elements, where q is a power of a prime integer p.

We denote by $\mathcal{C}_{\mathbb{K}}$ the set of $\mathbb{K}$-rational points of the curve. We denote by $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$, i.e. $\overline{\mathbb{K}} = \bigcup_{\ell=1}^{\infty} \mathbb{F}_{q^\ell}$, and by $\mathcal{C}_{\overline{\mathbb{K}}}$ the corresponding (infinite) set of $\overline{\mathbb{K}}$-rational points of the curve. 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 the action on $\mathcal{C}_{\overline{\mathbb{K}}}$.

Let us choose:

1. two pairs of points $a_i, b_i \in \mathcal{C}_{\mathbb{K}}$, $i = 1, 2$;
2. N points $c_\alpha \in \mathcal{C}_{\overline{\mathbb{K}}}$, $\alpha = 1, \ldots, N$, which satisfy the following $\mathbb{K}$-rationality condition:
$$\forall \sigma \in G(\overline{\mathbb{K}}/\mathbb{K}) \qquad \sigma(c_\alpha) = c_{\alpha'}.$$
3. N pairs of points $d_\beta, e_\beta \in \mathcal{C}_{\overline{\mathbb{K}}}$, $\beta = 1, \ldots, N$, which satisfy the following $\mathbb{K}$-rationality condition:
$$\forall \sigma \in G(\overline{\mathbb{K}}/\mathbb{K}) : \qquad \sigma(\{d_\beta, e_\beta\}) = \{d_{\beta'}, e_{\beta'}\}. \tag{2}$$
4. g points $f_\gamma \in \mathcal{C}_{\overline{\mathbb{K}}}$, $\gamma = 1, \ldots, g$, which satisfy the following $\mathbb{K}$-rationality condition:
$$\forall \sigma \in G(\overline{\mathbb{K}}/\mathbb{K}) \qquad \sigma(f_\gamma) = f_{\gamma'}.$$
5. the infinity point $h_\infty \in \mathcal{C}_{\mathbb{K}}$.

Remark. We consider here only the generic case and assume that all the points used in the construction are generic and distinct. In particular, genericity assumption implies that the divisor $D = \sum_{\gamma=1}^{g} f_\gamma$ is non-special.

Remark. It is enough to the check the $\mathbb{K}$-rationality conditions in any extension field $\mathbb{L} \supset \mathbb{K}$ of rationality of all the points used in the construction.

Definition 1. *Fix $\mathbb{K}$-rational local parameters t_i at b_i, $i = 1, 2$. For any integers $n_1, n_2, m \in \mathbb{Z}$ define the wavefunction $\psi_{1,m}(n_1, n_2)$ as a rational function with the following properties:*

1. *It has a pole of order at most $n_1 + m + 1$ at b_1 and a pole of order at most $n_2 - m$ at b_2.*
2. *Its first nontrivial coefficient of the expansion in t_1 at b_1 is normalized to 1.*
3. *It has zeros of order at least n_1 at a_1, and of order at least n_2 at a_2.*
4. *It has at most simple poles at points c_α, $\alpha = 1, \ldots, N$.*
5. *It has zero at least of the first order at the infinity point h_∞.*
6. *It has at most simple poles at points f_γ, $\gamma = 1, \ldots, g$.*
7. *It satisfies N constraints*
$$\psi_{1,m}(n_1, n_2)(d_\beta) = \psi_{1,m}(n_1, n_2)(e_\beta) \qquad \beta = 1, \ldots, N. \tag{3}$$

For the same set of points we define the wavefunction $\psi_{2,m}(n_1, n_2)$ as a rational function which differs from the function $\psi_{1,m}(n_1, n_2)$ only in the properties 1 and 2.

1_2. *It has a pole of order at most $n_1 + m$ at b_1 and it has a pole of order at most $n_2 - m + 1$ at b_2.*

2_2. *Its first nontrivial coefficient of the expansion in t_2 at b_2 is normalized to 1.*

Remark. The functions $\psi_{i,m}(n_1, n_2)$ are $\mathbb{K}$-rational, which follows from $\mathbb{K}$-rationality conditions of the sets of points in their definition.

Remark. As usual, zero (pole) of a negative order means pole (zero) of the corresponding positive order. Correspondingly one should interchange the expressions 'at most' and 'at least' coming before orders of poles and zeros.

Proposition 1. *The wavefunctions $\psi_{i,m}(n_1, n_2)$ are unique.*

Proof. We show this for the first function. By the Riemann–Roch theorem the dimension (over $\mathbb{K}$) of the divisor

$$\sum_{\alpha=1}^{N} c_\alpha + \sum_{\gamma=1}^{g} f_\gamma - h_\infty - n_1 a_1 - n_2 a_2 + (n_1 + 1 + m) b_1 + (n_2 - m) b_2$$

is equal to $N+1$. Under the genericity assumption the N constraints (3) and the normalization condition at b_1 remove the freedom. □

Corollary 2. *In the next section we show that, starting from the wavefunctions for $N = 0$, one can construct the functions for arbitrary N.*

Remark. To make subsequent formulae more transparent, from now on we will frequently skip the dependence on the parameters n_1, n_2.

In the generic case, which we assume in the following, when the order of the pole of $\psi_{1,m}$ at b_1 is n_1+m+1 and the order of the pole of $\psi_{2,m}$ at b_2 is n_1-m+1, we denote by $Q_{12,m}(n_1, n_2)$ the first nontrivial coefficient of expansion of $\psi_{1,m}$ at b_2, and by $Q_{21,m}(n_1, n_2)$ the first nontrivial coefficient of expansion of $\psi_{2,m}$ at b_1, i.e.

$$\psi_{1,m} = \frac{1}{t_2^{n_2-m}}(Q_{12,m} + \cdots) \qquad \psi_{2,m} = \frac{1}{t_1^{n_1+m}}(Q_{21,m} + \cdots).$$

Remark. The functions $Q_{12,m}$ and $Q_{21,m}$ take values in the field $\mathbb{K}$ of the definition of the curve.

Denote by T_i the operator of translation in the variable n_i, $i = 1, 2$, for example, $T_1\psi_{2,m}(n_1, n_2) = \psi_{2,m}(n_1 + 1, n_2)$.

Proposition 3. *The function $\psi_{1,m}$ satisfies equations*

$$T_2\psi_{1,m} - \psi_{1,m} = (T_2 Q_{12,m})\psi_{2,m} \tag{4}$$

$$\psi_{1,m+1} - T_1\psi_{1,m} = -\frac{T_1 Q_{12,m}}{Q_{12,m}}\psi_{1,m} \tag{5}$$

$$\psi_{1,m-1} = \frac{1}{Q_{21,m}}\psi_{2,m}. \tag{6}$$

The analogous system for $\psi_{2,m}$ is obtained by exchanging indices 1 and 2 and reversing the shift in the discrete variable m:

$$T_1\psi_{2,m} - \psi_{2,m} = (T_1 Q_{21,m})\psi_{1,m} \tag{7}$$

$$\psi_{2,m-1} - T_2\psi_{2,m} = -\frac{T_2 Q_{21,m}}{Q_{21,m}}\psi_{2,m} \tag{8}$$

$$\psi_{2,m+1} = \frac{1}{Q_{12,m}}\psi_{1,m}. \tag{9}$$

Proof. To prove the first equation (4) note that the left-hand side has all the properties of the function $\psi_{2,m}$ except for the normalization and must therefore be proportional to $\psi_{2,m}$. The coefficient of proportionality can be fixed by comparing the expansions at b_2. Other equations can be proved in the same way. □

Fix $\mathbb{K}$-rational local parameters $\tilde{t}_i$ at a_i, $i = 1, 2$. In the generic case when the order of $\psi_{i,m}$ at a_i is n_i, we denote by $\rho_{i,m}(n_1, n_2)$ the first nontrivial coefficients of the expansion of $\psi_{i,m}$ at a_i, i.e.

$$\psi_{i,m} = \tilde{t}_i^{n_i}(\rho_{i,m} + \cdots).$$

Similarly, in the generic case when the order of $\psi_{i,m}$ at a_j, $j \neq i$, is n_j, we denote by $\chi_{ij,m}(n_1, n_2)$ the first nontrivial coefficients of the expansion of $\psi_{i,m}$ at a_j, i.e.

$$\psi_{i,m} = \tilde{t}_j^{n_i}(\chi_{ij,m} + \cdots) \qquad i \neq j.$$

Proposition 4. *There exists a* $\mathbb{K}$*-valued potential (the* τ*-function) defined (up to a constant) by formulae*

$$T_1\tau_m = \rho_{1,m}\tau_m \tag{10}$$

$$T_2\tau_m = \rho_{2,m}\tau_m \tag{11}$$

$$\tau_{m+1} = (-1)^{n_1+n_2} Q_{12,m}\tau_m. \tag{12}$$

Proof. The first terms in the expansion of equations (4) and (7) at a_1 give

$$T_2\rho_{1,m} - \rho_{1,m} = (T_2 Q_{12,m})\chi_{21,m} \qquad 0 - \chi_{21,m} = (T_1 Q_{21,m})\rho_1$$

which combined together give

$$T_2\rho_{1,m} = (1 - (T_2 Q_{12,m})(T_1 Q_{21,m}))\rho_{1,m}. \tag{13}$$

Similarly, but changing the expansion point to a_2 we obtain

$$T_1\rho_{2,m} = (1 - (T_2 Q_{12,m})(T_1 Q_{21,m}))\rho_{2,m}.$$

Both equations imply

$$(T_2\rho_{1,m})\rho_{2,m} = (T_1\rho_{2,m})\rho_{1,m}$$

which is the compatibility condition of equations (10) and (11).

Expansion of equation (5) at a_1 gives

$$\rho_{1,m+1} = -\frac{T_1 Q_{12,m}}{Q_{12,m}}\rho_{1,m} \tag{14}$$

which is the compatibility condition of equations (10) and (12). Finally, by comparing equations (6) and (9) we obtain

$$Q_{21,m+1} = \frac{1}{Q_{12,m}} \tag{15}$$

which, combined with the following consequence of expansion of (8) at a_2

$$\rho_{2,m-1} = -\frac{T_2 Q_{21,m}}{Q_{21,m}}\rho_{2,m}$$

gives the compatibility condition of equations (11) and (12). □

Corollary 5. *Equation (13) written in terms of the* τ*-function reads*

$$\tau_m T_1 T_2 \tau_m = T_1\tau_m T_2\tau_m - T_1\tau_{m-1} T_2\tau_{m+1} \tag{16}$$

which is the Hirota equation [18].

Corollary 6. *The compatibility condition of equations (13) and (14) written in terms of the function* $Q_{12,m}$ *reads*

$$\frac{T_1 T_2 Q_{12,m}}{T_2 Q_{12,m}} - \frac{T_1 Q_{12,m}}{Q_{12,m}} = \frac{T_1 T_2 Q_{12,m}}{T_1 Q_{12,m-1}} - \frac{T_2 Q_{12,m+1}}{Q_{12,m}}. \tag{17}$$

3. Construction of solutions using vacuum functions

The results of this section were motivated by papers on the fundamental transformation of quadrilateral lattices in a vectorial formulation [15, 25, 26] and on the algebro-geometric interpretation of this transformation [11, 12].

In the case $N = 0$ let us add the superscript 0 to all functions defined above and call them the vacuum functions. The functions for arbitrary N can be constructed with the help of N new functions, which we define below.

Definition 2. *Fix local parameters t_α at c_α, $\alpha = 1, \ldots, N$. For any α define the function $\phi^0_{\alpha,m}$ by the following conditions:*

1. *It has a pole of order at most $n_1 + m$ at b_1 and a pole of order at most $n_2 - m$ at b_2.*
2. *It has zeros of order at least n_1 at a_1, and of order at least n_2 at a_2.*
3. *It has at most a simple pole at the point c_α and the first nontrivial coefficient of the expansion in t_α at c_α is normalized to 1.*
4. *It has zero at least of the first order at the infinity point h_∞.*
5. *It has at most simple poles at points f_γ, $\gamma = 1, \ldots, g$.*

Remark. The function $\phi^0_{\alpha,m}$ is unique but usually it is not $\mathbb{K}$-rational.

Lemma 7. *Denote by $\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e})$, $i = 1, 2$, the column with N entries of the form*

$$\left[\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e})\right]_\beta = \psi^0_{i,m}(d_\beta) - \psi^0_{i,m}(e_\beta) \qquad \beta = 1, \ldots, N,$$

denote by $\phi^0_{\boldsymbol{A},m}$ the row with N entries

$$\left[\phi^0_{\boldsymbol{A},m}\right]_\alpha = \phi^0_{\alpha,m} \qquad \alpha = 1, \ldots, N$$

and denote by $\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})$ the $N \times N$ matrix whose element in row α and column β is

$$\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]_{\alpha\beta} = \phi^0_{\alpha,m}(d_\beta) - \phi^0_{\alpha,m}(e_\beta) \qquad \alpha, \beta = 1, \ldots, N.$$

Then the wavefunctions $\psi_{i,m}$ read

$$\psi_{i,m} = \psi^0_{i,m} - \phi^0_{\boldsymbol{A},m}\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e}). \tag{18}$$

Proof. Denote the right-hand side of equation (18) by $\widehat{\psi^0_{i,m}}$. By building the column $\widehat{\psi^0_{i,m}}(\boldsymbol{d}, \boldsymbol{e})$ with N entries of the form $\widehat{\psi^0_{i,m}}(d_\beta) - \widehat{\psi^0_{i,m}}(e_\beta)$ we can easily show that $\widehat{\psi^0_{i,m}}(\boldsymbol{d}, \boldsymbol{e}) = 0$. This demonstrates that the function $\widehat{\psi^0_{i,m}}$ satisfies constraints (3). One can check that $\widehat{\psi^0_{i,m}}$ also satisfies other properties which define uniquely the function $\psi_{i,m}$. □

In the generic case denote by $H^0_{i,\alpha,m}$ the first nontrivial coefficient of expansion of the function $\phi^0_{\alpha,m}$ in the uniformization parameter t_i at b_i, for example,

$$\phi^0_{\alpha,m} = \frac{1}{t_1^{n_1+m}}\left(H^0_{1,\alpha,m} + \cdots\right).$$

Lemma 8. *The corresponding expressions for $Q_{ij,m}$, $i \neq j$, and for $\rho_{i,m}$ read*

$$Q_{ij,m} = Q^0_{ij,m} - H^0_{j,\boldsymbol{A},m}\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e}) \qquad i \neq j \tag{19}$$

$$\rho_{i,m} = \rho^0_{i,m}\left(1 + \left(T_i H^0_{i,\boldsymbol{A},m}\right)\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e})\right) \tag{20}$$

where $H^0_{i,\boldsymbol{A},m}$ is the row with N entries $H^0_{i,\alpha,m}$.

Proof. Because equation (19) can be obtained by expansion of formula (18) at b_j, only equation (20) needs an explanation. Note first the equation

$$T_i\phi^0_{\alpha,m} - \phi^0_{\alpha,m} = \left(T_i H^0_{i,\alpha,m}\right)\psi^0_{i,m} \tag{21}$$

which can be shown in the same way as the equations of proposition 3. Denote by $F^0_{i,\alpha,m}$ the first nontrivial coefficient of expansion of $\phi^0_{\alpha,m}$ at a_i, for example

$$\phi^0_{\alpha,m} = \frac{1}{\tilde{t}_1^{n_1}}\left(F^0_{1,\alpha,m} + \cdots\right).$$

Expansion of equation (18) at a_i gives

$$\rho^0_{i,m}\left(T_i H^0_{i,\alpha,m}\right) = -F^0_{i,\alpha,m}$$

which concludes the proof. □

We will use the following result, which can be proved by induction with respect to the dimension of the vector space $\mathbb{V}$.

Lemma 9. *Given $\boldsymbol{u} \in \mathbb{V}$ and $\boldsymbol{v}^* \in \mathbb{V}^*$, if $1_{\mathbb{V}}$ is the identity operator on $\mathbb{V}$ then*

$$\det(1_{\mathbb{V}} + \boldsymbol{u} \otimes \boldsymbol{v}^*) = 1 + \langle \boldsymbol{v}^*, \boldsymbol{u}\rangle.$$

Proposition 10. *Using the above notation the τ-function can be constructed by the following formula:*

$$\tau_m = \tau^0_m \det \phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e}). \tag{22}$$

Proof. Note that equation (21) implies

$$\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1} T_i\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e}) = 1_{\mathbb{K}^N} + \left(\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e})\right) \otimes \left(T_i H^0_{i,\boldsymbol{A},m}\right)$$

which gives, by lemma 9,

$$\frac{\det T_i\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})}{\det \phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})} = 1 + \left(T_i H^0_{i,\boldsymbol{A},m}\right)\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{i,m}(\boldsymbol{d}, \boldsymbol{e}). \tag{23}$$

Comparing equation (23) with equation (20) and taking into account equations (10), (11) we obtain

$$\frac{\det T_i\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})}{\det \phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})} = \frac{T_i\tau_m / T_i\tau^0_m}{\tau_m/\tau^0_m}. \tag{24}$$

Note the following equation:

$$\phi^0_{\alpha,m+1} - \phi^0_{\alpha,m} = -\frac{H^0_{2,\alpha,m}}{Q^0_{12,m}}\psi^0_{1,m}$$

which can be shown in the same way as the equations of proposition 3. It implies that

$$\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\phi^0_{\boldsymbol{A},m+1}(\boldsymbol{d}, \boldsymbol{e}) = 1_{\mathbb{K}^N} - \frac{1}{Q^0_{12,m}}\left(\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{1,m}(\boldsymbol{d}, \boldsymbol{e})\right) \otimes \left(H^0_{2,\boldsymbol{A},m}\right)$$

which gives

$$\frac{\det \phi^0_{\boldsymbol{A},m+1}(\boldsymbol{d}, \boldsymbol{e})}{\det \phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})} = 1 - \frac{1}{Q^0_{12,m}}H^0_{2,\boldsymbol{A},m}\left[\phi^0_{\boldsymbol{A},m}(\boldsymbol{d}, \boldsymbol{e})\right]^{-1}\psi^0_{1,m}(\boldsymbol{d}, \boldsymbol{e}). \tag{25}$$

Comparing equation (25) with equation (19) and taking into account equation (12) we obtain

$$\frac{\det \phi^0_{\boldsymbol{A},m+1}(\boldsymbol{d},\boldsymbol{e})}{\det \phi^0_{\boldsymbol{A},m}(\boldsymbol{d},\boldsymbol{e})} = \frac{\tau_{m+1}/\tau^0_{m+1}}{\tau_m/\tau^0_m} \tag{26}$$

which, together with equation (24), concludes the proof. □

Corollary 11. *Note that equation (22) is valid up to a (nonessential) change of the initial value of the τ-function, which is due to the introduction of the integration constant from formulae (24) and (26).*

Corollary 12. *Starting with $\mathbb{K}$-valued function τ^0_m and the local parameters t_α at c_α chosen in a consistent way with the action of the Galois group $G(\overline{\mathbb{K}}/\mathbb{K})$ on $\mathcal{C}_{\overline{\mathbb{K}}}$ we obtain $\mathbb{K}$-valued function τ_m.*

4. Multisoliton solutions

We present here explicit formulae for the vacuum functions in the simplest case $g = 0$. Then with the help of these expressions we present some examples of N-soliton solutions. In constructing the vacuum functions we will use the standard parameter t on the projective line $\mathbb{P}(\mathbb{K})$ and we put $h_\infty = \infty$.

Explicit forms of the wavefunctions read

$$\psi^0_{1,m} = \frac{1}{(t-b_1)^{n_1+1+m}} \frac{(t-a_1)^{n_1}(t-a_2)^{n_2}(b_1-b_2)^{n_2-m}}{(b_1-a_1)^{n_1}(b_1-a_2)^{n_2}(t-b_2)^{n_2-m}}$$

$$\psi^0_{2,m} = \frac{1}{(t-b_2)^{n_2+1-m}} \frac{(b_2-b_1)^{n_1+m}(t-a_1)^{n_1}(t-a_2)^{n_2}}{(t-b_1)^{n_1+m}(b_2-a_1)^{n_1}(b_2-a_2)^{n_2}}$$

which give formulae for the functions $Q^0_{12,m}$ and $Q^0_{21,m}$,

$$Q^0_{12,m} = \frac{(-1)^{n_2-m}}{(b_2-b_1)^{n_1-n_2+1+2m}} \frac{(b_2-a_1)^{n_1}(b_2-a_2)^{n_2}}{(b_1-a_1)^{n_1}(b_1-a_2)^{n_2}}$$

$$Q^0_{21,m} = \frac{(-1)^{n_1+m}}{(b_1-b_2)^{n_2-n_1+1-2m}} \frac{(b_1-a_1)^{n_1}(b_1-a_2)^{n_2}}{(b_2-a_1)^{n_1}(b_2-a_2)^{n_2}}$$

and for the functions $\rho_{1,m}$ and $\rho_{2,m}$,

$$\rho^0_{1,m} = \frac{(-1)^{n_1}}{(a_1-b_1)^{2n_1+1+m}} \frac{(a_1-a_2)^{n_2}(b_1-b_2)^{n_2-m}}{(b_1-a_2)^{n_2}(a_1-b_2)^{n_2-m}}$$

$$\rho^0_{2,m} = \frac{(-1)^{n_2}}{(a_2-b_2)^{2n_2+1-m}} \frac{(b_2-b_1)^{n_1+m}(a_2-a_1)^{n_1}}{(a_2-b_1)^{n_1+m}(b_2-a_1)^{n_1}}.$$

The explicit form of the vacuum τ-function reads

$$\tau^0_m = \frac{(-1)^{[n_1(n_1-1)+n_2(n_2-1)+m(m+1)]/2}}{(a_1-b_1)^{n_1(n_1+m)}(a_2-b_2)^{n_2(n_2-m)}} \frac{(a_1-a_2)^{n_1n_2}(b_1-b_2)^{(n_2-m)(m+n_1)}}{(b_1-a_2)^{n_2(n_1+m)}(a_1-b_2)^{n_1(n_2-m)}}.$$

The functions $\phi^0_{\alpha,m}$, $\alpha = 1, \ldots, N$ have the form

$$\phi^0_{\alpha,m} = \frac{1}{t-c_\alpha} \frac{(t-a_1)^{n_1}(t-a_2)^{n_2}(c_\alpha-b_1)^{n_1+m}(c_\alpha-b_2)^{n_2-m}}{(c_\alpha-a_1)^{n_1}(c_\alpha-a_2)^{n_2}(t-b_1)^{n_1+m}(t-b_2)^{n_2-m}}$$

and can be used, due to proposition 10, to construct the τ-function for arbitrary N.

Let $\mathbb{L} = \mathbb{F}_{q^\ell} \subset \overline{\mathbb{K}}$ be a field of rationality of all the points used in the construction. Recall [23] that if $q = p^k$ then the Galois group $G(\mathbb{L}/\mathbb{K})$ is the cyclic group of order ℓ and is generated by σ_F^k, where σ_F is the Frobenius automorphism of $\mathbb{L}$ defined as $\sigma_F(a) = a^p$. Therefore possible systems of points c_α and pairs $\{d_\beta, e_\beta\}$ can be grouped into $\mathbb{K}$-rational clusters (orbits of the group $G(\mathbb{L}/\mathbb{K})$) with lengths being divisors of ℓ. In the standard nomenclature the clusters of length 1 correspond to solitons, and clusters of length 2 give rise to breathers (the positions of poles c_α of the wavefunctions must be symmetric with respect to the complex conjugation). In finite fields we encounter new types of solutions (without direct analogues in the complex field case) which come from clusters of lengths greater then 2. The analogue of the breather solution will be presented in example 1. Let us call the N-soliton solution of order ℓ the $\mathbb{K}$-rational N-soliton solution with parameters in extension of $\mathbb{K}$ of order ℓ. In this terminology the standard N-soliton solutions are of order 1, while the breather solution is a two-soliton solution of order 2. A three-soliton solution of order 3 and a two-soliton solution of order 4 are presented in examples 2 and 3. We remark that the above terminology is not completely distinctive.

Note that the variables n_1, n_2 and m enter exponentially in the functions τ_m^0 and $\phi_{\alpha,m}^0$ This implies that the τ-function is periodic in n_1, n_2 and m with the periods being divisors of $q^\ell - 1$, which is the order of the cyclic multiplicative group $\mathbb{L}_*$.

Finally, we present examples. For any example we describe the fields $\mathbb{K}$ and $\mathbb{L}$ giving first the numbers $q = p^k$ and ℓ and then writing down the polynomial $w(x)$ over $\mathbb{F}_p$ used to construct multiplication in the field $\mathbb{L}$. We represent elements of $\mathbb{L}$ as elements of the vector space $\mathbb{F}_p^{kl}$. Then we give the points used in the construction of the solution of the Hirota equation presenting also the action of the Galois group $G(\mathbb{L}/\mathbb{K})$ on them.

Example 1. A breather solution of the Hirota equation in $\mathbb{F}_5$. Parameters of the solution take values in extension $\mathbb{F}_{5^2}$ of $\mathbb{F}_5$ by the polynomial $w(x) = x^2 + x + 1$. The corresponding Galois group reads $G(\mathbb{F}_{5^2}/\mathbb{F}_5) = \{\mathrm{i}d, \sigma\}$, where $\sigma^2 = \mathrm{i}d$. The parameters of the solution are chosen as follows:

$$a_1 = (00), a_2 = (02), b_1 = (01), b_2 = (04)$$
$$c_1 = (10), c_2 = \sigma(c_1) = (44)$$
$$d_1 = (11), d_2 = \sigma(d_1) = (40)$$
$$e_1 = (13), e_2 = \sigma(e_1) = (42).$$

This solution is presented in figures 1 and 2. The elements of $\mathbb{F}_5$ are represented by: ■—(00), ■—(01), ■—(02), ■—(03), ■—(04).

The periods in variables n_1, n_2 and m are 12, 24 and 24, respectively. Note that the figure for $m = 5$ can be obtained from the figure for $m = 1$ by a shift in n_2 by 4.

Example 2. A three-soliton solution of order 3 of the Hirota equation in $\mathbb{F}_5$. This solution is the first one in the generalized breather class, a new type not present in the standard complex field case. Parameters of the solution take values in extension $\mathbb{F}_{5^3}$ of $\mathbb{F}_5$ by the polynomial $w(x) = x^3 + x^2 + 1$. The corresponding Galois group reads $G(\mathbb{F}_{5^3}/\mathbb{F}_5) = \{\mathrm{id}, \sigma, \sigma^2\}$, where $\sigma^3 = \mathrm{id}$. The parameters of the solution are chosen as follows:

$$a_1 = (004), a_2 = (003), b_1 = (002), b_2 = (001)$$
$$c_1 = (022), c_2 = \sigma(c_1) = (120), c_3 = \sigma^2(c_1) = (412)$$
$$d_1 = (020), d_2 = \sigma(d_1) = (123), d_3 = \sigma^2(d_1) = (410)$$
$$e_1 = (010), e_2 = \sigma(e_1) = (314), e_3 = \sigma^2(e_1) = (230).$$

This solution is presented in figures 3 and 4. The elements of $\mathbb{F}_5$ are represented as in example 1. From the figures one can deduce that the periods in all variables n_1, n_2 and m are maximal and equal to 124.

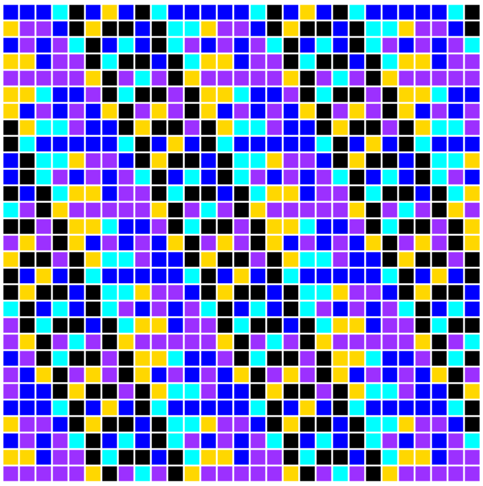

Figure 1. A breather solution of the Hirota equation in $\mathbb{F}_5$ described in example 1; n_1 ranges from 0 to 28 (directed to the right), n_2 ranges from 0 to 28 (directed up), $m = 1$.

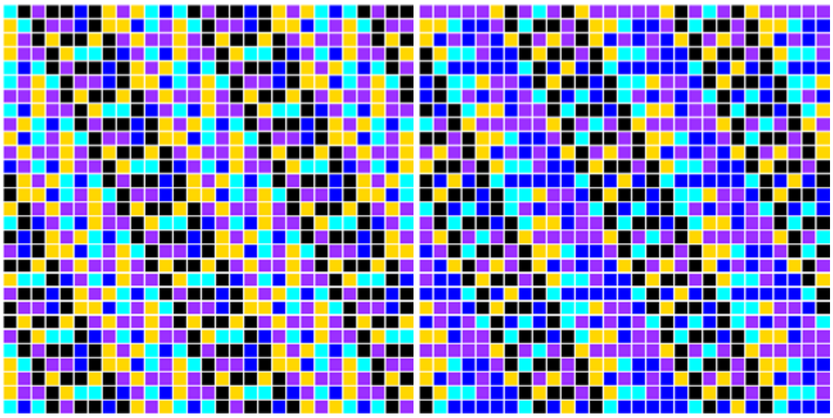

Figure 2. A breather solution as in figure 1 for $m = 2$ and $m = 5$.

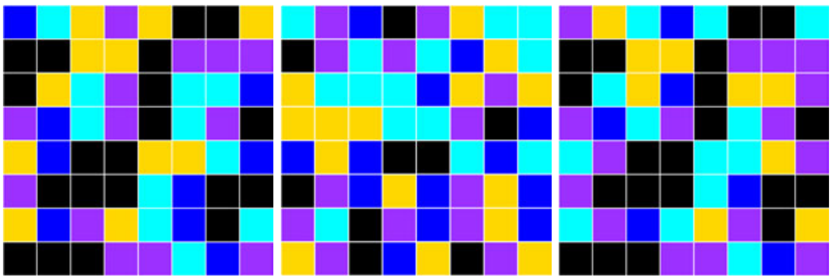

Figure 3. A breather solution of order 3 of the Hirota equation in $\mathbb{F}_5$ described in example 2; n_1 ranges from 0 to 8 (directed to the right), n_2 ranges from 0 to 8 (directed up), $m = 0$, 4 and 62.

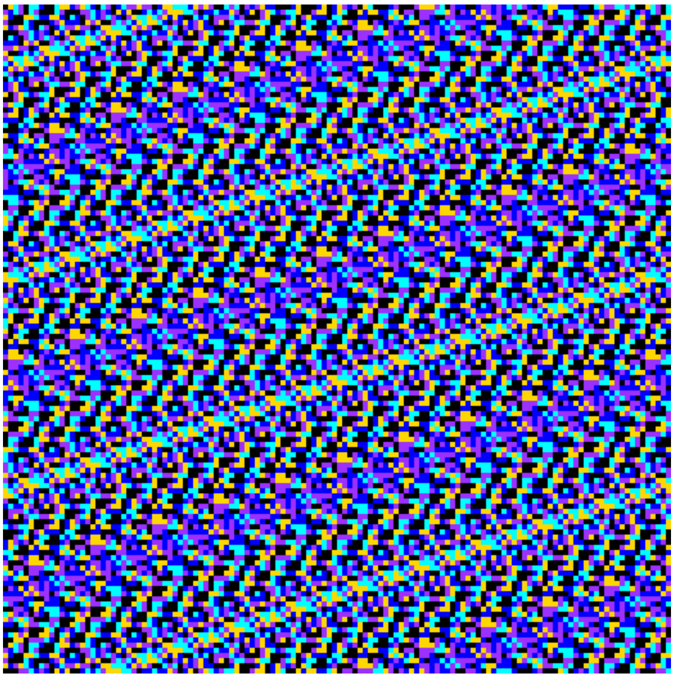

Figure 4. A 'global' view of the first picture ($m = 0$) of the generalized breather solution presented in figure 3; n_1 and n_2 range from 0 to 129.

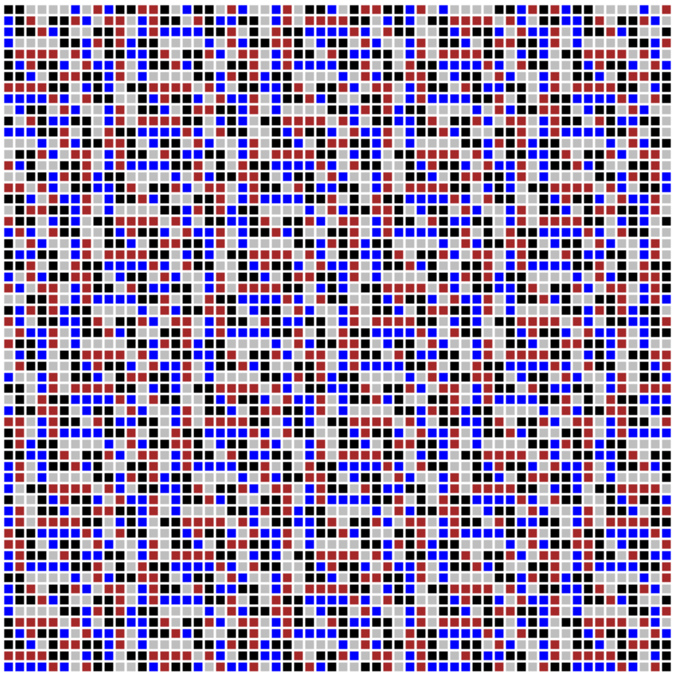

Figure 5. A two-soliton solution of order 4 of the Hirota equation in $\mathbb{F}_4$; n_1 and n_2 range from 0 to 59, $m = 0$.

Example 3. The aim of this example is to present a solution in a 'small' field $\mathbb{F}_4$ obtained from parameters taking values in a relatively bigger field $\mathbb{F}_{256}$. The field $\mathbb{F}_{256}$ is chosen as the extension of $\mathbb{F}_2$ by the polynomial $w(x) = x^8 + x^6 + x^5 + x + 1$. The elements (00 000 000), (00 000 001), (11 110 000) and (11 110 001) of $\mathbb{F}_{256} = \mathbb{F}_{2^8}$ form a subfield isomorphic to $\mathbb{F}_4$. The Galois group is generated by $\sigma = \sigma_F^2$, and reads $G(\mathbb{F}_{256}/\mathbb{F}_4) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$, where $\sigma^4 = \mathrm{id}$. The parameters of the solution are as follows:

$$a_1 = (00000000), a_2 = (00000001), b_1 = (11110000), b_2 = (11110001)$$
$$c_1 = (00010010), c_2 = \sigma(c_1) = (11100011)$$
$$d_1 = (00001010), d_2 = \sigma(d_1) = (00001001)$$
$$e_1 = \sigma^2(d_1) = (00011000), e_2 = \sigma^3(d_1) = (11101010).$$

Here the points c_1 and c_2 are chosen from a subfield of $\mathbb{F}_{256}$ isomorphic to $\mathbb{F}_{16}$ and form a cluster of length 2. The points c_1, c_2, d_1 and d_2 form a cluster of length 4 in a way compatible with the $\mathbb{F}_4$-rationality condition (2). We obtain therefore a two-soliton solution of order 4, which also has no direct counterpart in the complex field case.

The solution is presented in figure 5 for $m = 0$; The elements of $\mathbb{F}_4$ are represented by: —(00000000), —(00000001), —(11110000), —(11110001). The period in all variables is the same and equals 51.

5. Conclusion and remarks

In this paper, motivated by recent developments of integrable discrete geometry, we presented the algebro-geometric method of construction of solutions of the Hirota equation over finite fields. It turns out that the main ideas used for integrable systems over the field of complex numbers, e.g., application of the Riemann–Roch theorem, can be transferred to the level of finite fields without essential modifications. We would like to stress that although finite fields consist of a finite number of elements the corresponding algebraic curves have an infinite number of points (taking into account the algebraic completion of the field) which gives rise to infinite families of solutions of the equation.

We have presented examples of pure (for the simplest algebraic curve being the projective line) multisoliton solutions of the Hirota equation. Less trivial examples which use techniques on Jacobians of algebraic curves will be the subject of another paper [4].

Acknowledgment

This paper was partially supported by KBN grant no 2P03B12622.

References

[1] Akhmetshin A A, Krichever I M and Volvovski Y S 1999 Discrete analogs of the Darboux–Egoroff metrics *Preprint* hep-th/9905168
[2] Anderson G W 1994 Rank one elliptic A-modules and A-harmonic series *Duke Math. J.* **73** 491–542
[3] Belokolos E D, Bobenko A I, Enol'skii V Z, Its A R and Matveev V B 1994 *Algebro-Geometric Approach to Nonlinear Integrable Equations* (Berlin: Springer)
[4] Białecki M and Doliwa A in preparation
[5] Bobenko A, Bordemann M, Gunn Ch and Pinkall U 1993 On two integrable cellular automata *Commun. Math. Phys.* **158** 127–34
[6] Bruschi M and Santini P M 1994 Cellular automata in 1 + 1, 2 + 1 and 3 + 1 dimensions, constants of motion and coherent structures *Physica* D **70** 185–209
[7] Doliwa A 1997 Geometric discretisation of the Toda system *Phys. Lett.* A **234** 187–92

[8] Doliwa A 1999 Discrete integrable geometry with ruler and compass *Symmetries and Integrability of Difference Equations* ed P Clarkson and F Nijhoff (Cambridge: Cambridge University Press) pp 122–36
[9] Doliwa A 1999 Quadratic reductions of quadrilateral lattices *J. Geom. Phys.* **30** 169–86
[10] Doliwa A 2000 Lattice geometry of the Hirota equation *SIDE III—Symmetries and Integrability of Difference Equations (CMR Proc. and Lecture Notes vol 25)* ed D Levi and O Ragnisco (Providence, RI: American Mathematical Society) pp 93–100
[11] Doliwa A 2001 The Darboux-type transformations of integrable lattices *Rep. Math. Phys.* **48** 59–66
[12] Doliwa A 2001 Integrable multidimensional discrete geometry: quadrilateral lattices, their transformations and reductions *Integrable Hierarchies and Modern Physical Theories* ed H Aratyn and A S Sorin (Dordrecht: Kluwer) pp 355–89
[13] Doliwa A and Santini P M 1997 Multidimensional quadrilateral lattices are integrable *Phys. Lett.* A **233** 365–72
[14] Doliwa A 2000 The symmetric, D-invariant and Egorov reductions of the quadrilateral lattice *J. Geom. Phys.* **36** 60–102
[15] Doliwa A, Santini P M and Mañas M 2000 Transformations of quadrilateral lattices *J. Math. Phys.* **41** 944–90
[16] Drinfeld V 1977 Commutative subrings of some noncommutative rings *Funct. Anal. Appl* **11** 9–12
[17] Hirota R 1977 Nonlinear partial difference equations: III. Discrete sine-Gordon equation *J. Phys. Soc. Japan* **43** 2079–86
[18] Hirota R 1981 Discrete analogue of a generalized Toda equation *J. Phys. Soc. Japan* **50** 3785–91
[19] Hirschfeld J W P 1998 *Projective Geometries over Finite Fields* (Oxford: Clarendon)
[20] Koblitz N 1998 *Algebraic Aspects of Cryptography* (Berlin: Springer)
[21] Krichever I M, Lipan O, Wiegmann P and Zabrodin A 1997 Quantum integrable models and discrete classical Hirota equations *Commun. Math. Phys.* **188** 267–304
[22] Krichever I M, Wiegmann P and Zabrodin A 1998 Elliptic solutions to difference nonlinear equations and related many body problems *Commun. Math. Phys.* **193** 373–96
[23] Lang S 1970 *Algebra* (Reading, MA: Addison-Wesley)
[24] Lidl R and Niederreiter H 1986 *Introduction to Finite Fields and their Applications* (Cambridge: Cambridge University Press)
[25] Mañas M 2001 Fundamental transformations for quadrilateral lattices: first potentials and τ-functions, symmetric and pseudo-Egorov reductions *J. Phys A: Math. Gen.* **34** 10413–21
[26] Mañas M, Doliwa A and Santini P M 1997 Darboux transformations for multidimensional quadrilateral lattices: I *Phys. Lett.* A **232** 99–105
[27] Mikhailov A V 1979 Integrability of a two-dimensional generalization of the Toda chain *JETP Lett.* **30** 414–8
[28] Moriwaki S, Nagai A, Satsuma J, Tokihiro T, Torii M, Takahashi D and Matsukidaira J 1999 2 + 1 dimensional soliton cellular automaton *Symmetries and Integrability of Difference Equations* ed P Clarkson and F Nijhoff (Cambridge: Cambridge University Press) pp 334–42
[29] Mumford D 1978 An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg–de Vries equation, and related nonlinear equations *Proc. Int. Symp. on Algebraic Geometry* ed M Nagata (Tokyo: Kinokuniya) pp 115–53
[30] Nakamura Y and Mukaihira A 1998 Dynamics of the finite Toda molecule over finite fields and a decoding algorithm *Phys. Lett.* A **249** 295–302
[31] Stichtenoth H 1993 *Algebraic Function Fields and Codes* (Berlin: Springer)
[32] Thakur D S 2001 Integrable systems and number theory in finite characterictic *Physica* D **152–153** 1–8
[33] Tokihiro T, Takahashi D, Matsukidaira J and Satsuma J 1996 From soliton equations to integrable cellular automata through a limiting procedure *Phys. Rev. Lett.* **76** 3247–50
[34] Wolfram S 1986 *Theory and Application of Cellular Automata* (Singapore: World Scientific)