On pattern structures of the N-soliton solution of the discrete KP equation over a finite field

2007 J. Phys. A: Math. Theor. 40 949

(http://iopscience.iop.org/1751-8121/40/5/006)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL
J. Phys. A: Math. Theor. **40** (2007) 949–959 doi:10.1088/1751-8113/40/5/006

On pattern structures of the *N*-soliton solution of the discrete KP equation over a finite field

Mariusz Białecki[1,2] **and Jonathan J C Nimmo**[1,3]

[1] Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8914, Japan
[2] Institute of Geophysics, Polish Academy of Sciences, ul. Księcia Janusza 64, 01-452 Warszawa, Poland

E-mail: bialecki@igf.edu.pl and j.nimmo@maths.gla.ac.uk

Received 8 September 2006, in final form 11 December 2006
Published 17 January 2007
Online at stacks.iop.org/JPhysA/40/949

Abstract
The existence and properties of coherent pattern in the multisoliton solutions of the dKP equation over a finite field are investigated. To that end, starting with an algebro-geometric construction over a finite field, we derive a 'travelling wave' formula for *N*-soliton solutions in a finite field. However, despite it having a form similar to its analogue in the complex field case, the finite-field solutions produce patterns essentially different from those of classical interacting solitons.

PACS numbers: 02.30.Ik, 02.10.De, 05.45.Yv

1. Introduction

There are many diverse methods in the modern theory of integrable systems. One of them, an algebro-geometric approach [8, 9], was applied to obtain solutions of discrete soliton equations over finite fields [1, 3, 5]. Within this approach efficient tools for finding algebro-geometric solutions based on hyperelliptic curves of arbitrary genus were proposed [2, 4]. These results are in direct analogy to the complex field case, but there are some peculiarities. For instance, since finite fields are never algebraically closed there are many more possibilities for the construction of breather-type solutions (for short discussion see [5]). Also other properties, such as finiteness or cyclic structure, reflect in the character of solutions.

Our aim here is to discuss the appearance of stable travelling patterns for a general *N*-soliton solution over a finite field. To do that we write a general determinant formula (8) for *N*-soliton solution in a travelling wave form (12). The formula obtained is analogous to the typical form of a soliton solution of a Hirota bilinear equation (see e.g. [14], p 23). Since

[3] Permanent address: Department of Mathematics, University of Glasgow, Glasgow G12 8QQ, UK.

the vacuum solution in this setting is $\tau \equiv 1$, it is necessary to make a slight modification of the algebro-geometric construction presented in [3].

The determinant form of the solutions of the dKP equation was already investigated [15]. Since the determinant formula is neither a Casorati nor a discrete Gram-type determinant, we provide a direct link to the travelling wave form without referring to the previous work. Moreover, even though we are mainly concerned with finite fields, we point out that the calculations performed are valid for arbitrary fields.

There is one more reason to transform the finite-field solutions into travelling wave form. There exists a well-established systematic procedure for deriving soliton cellular automata starting from discrete soliton equations in Hirota form [12, 16]. Since solutions over a finite field could be interpreted also as cellular automata, we need a convenient form to investigate relationships between them.

This paper is organized as follows. In section 2 we recall and transpose some results from an algebro-geometric construction of finite-field-valued solutions of the discrete KP equation with explicit determinant formula for N-soliton solutions [3] to the case of dKP with arbitrary coefficients (2). In the next section, we prove that the N-soliton solution can be rewritten in travelling wave form. As a remark we also give an alternative proof which explains why only pairwise interaction terms appear in the N-soliton solutions which appear as substitution operations for matrix elements. In section 4, we discuss the patterns produced by finite-field solitons and give some examples. The main conclusion is that travelling wave patterns in N-soliton solutions obtained by the algebro-geometric approach are generally absent for $N > 2$. We finish with some conclusions and remarks on possible future work in the last section.

2. Algebro-geometric construction of solutions of dKP equation over finite fields with simple vacuum

A finite-field version of an algebro-geometric construction of solutions $\tau : \mathbb{Z}^3 \to \mathbb{F}$ for the discrete KP equation

$$(T_1\tau)(T_{23}\tau) - (T_2\tau)(T_{13}\tau) + (T_3\tau)(T_{12}\tau) = 0 \tag{1}$$

was studied in [3]. By T_i we denoted here a shift operator in a variable n_i, for example $T_2\tau(n_1, n_2, n_3) = \tau(n_1, n_2 + 1, n_3)$. If we prefer to have vacuum solution $\bar{\tau}(n_1, n_2, n_3) \equiv 1$ then we need to consider the dKP equation with coefficients $Z_i \in \mathbb{F}$, i.e.,

$$Z_1(T_1\bar{\tau})(T_{23}\bar{\tau}) - Z_2(T_2\bar{\tau})(T_{13}\bar{\tau}) + Z_3(T_3\bar{\tau})(T_{12}\bar{\tau}) = 0 \tag{2}$$

with the constraint

$$Z_1 - Z_2 + Z_3 = 0. \tag{3}$$

Note that a correspondence between τ and $\bar{\tau}$ is achieved by taking

$$\bar{\tau} = (Z_3/\delta)^{-n_1n_2}(Z_1/\delta)^{-n_2n_3}(Z_2/\delta)^{-n_1n_3}\tau \tag{4}$$

for nonzero constants Z_1, Z_2, Z_3 and any nonzero $\delta \in \mathbb{F}$.

It follows from [3], in the case of purely soliton solutions (i.e. from a curve of genus $g = 0$), that N-soliton solutions can be expressed in a determinant form (theorem 1). As a component of this formula we need a vacuum solution of (1)

$$\tau_0 = (A_1 - A_2)^{n_1n_2}(A_1 - A_3)^{n_1n_3}(A_2 - A_3)^{n_2n_3}, \tag{5}$$

where $A_i \in \mathbb{F}$, and auxiliary functions ϕ^0_α, $\alpha = 1, 2, \ldots, N$, in the form

$$\phi_\alpha(t) = \frac{1}{t - C_\alpha}\prod_{k=1}^{3}\left(\frac{t - A_k}{C_\alpha - A_k}\right)^{n_k}. \tag{6}$$

Parameters C_α, where $\alpha = 1, \ldots, N$, may take value in some finite algebraic extension $\mathbb{L} \supset \mathbb{K}$, but they are constrained to the $\mathbb{K}$-rationality conditions $\forall \sigma \in G(\mathbb{L}/\mathbb{K}), \sigma(C_\alpha) = C_{\alpha'}$. By $G(\mathbb{L}/\mathbb{K})$ we denoted the Galois group, i.e. the group of automorphisms of $\mathbb{L}$, with fixed field $\mathbb{K}$. Similarly, N pairs $D_\beta, E_\beta \in \mathbb{L}$, for $\beta = 1, \ldots, N$, satisfy the $\mathbb{K}$-rationality conditions $\forall \sigma \in G(\mathbb{L}/\mathbb{K}) : \sigma(\{D_\beta, E_\beta\}) = \{D_{\beta'}, E_{\beta'}\}$. These conditions give rise to some generalization of breather-type solutions (see [5]). We assume that all parameters in the construction are distinct. Finally, denote by $\phi_{\boldsymbol{A}}(\boldsymbol{D}, \boldsymbol{E})$ the $N \times N$ matrix with element in row β and column α given by

$$[\phi_{\boldsymbol{A}}(\boldsymbol{D}, \boldsymbol{E})]_{\alpha\beta} = \phi_\alpha(D_\beta) - \phi_\alpha(E_\beta). \tag{7}$$

Theorem 1. *The function $\tau(n_1, n_2, n_3)$ given by*

$$\tau = \tau_0 \cdot \gamma \det \phi_{\boldsymbol{A}}(\boldsymbol{D}, \boldsymbol{E}), \tag{8}$$

where $\gamma \in \mathbb{F}$ is some constant, is the $\mathbb{F}$-valued N-soliton solution of the discrete KP equation (1).

In the case of dKP equation (2), it follows from (4) that a vacuum function $\bar{\tau}_0$ can be chosen in the form

$$\bar{\tau}_0 = \left(\frac{A_1 - A_2}{Z_3}\right)^{n_1 n_2} \left(\frac{A_1 - A_3}{Z_2}\right)^{n_1 n_3} \left(\frac{A_2 - A_3}{Z_1}\right)^{n_2 n_3}.$$

Then for parameters $A_1 - A_2 = Z_3$, $A_1 - A_3 = Z_2$, $A_2 - A_3 = Z_1$ we have $\bar{\tau}_0 \equiv 1$ and

$$\bar{\tau} = \det \phi_{\boldsymbol{A}}(\boldsymbol{D}, \boldsymbol{E}) \tag{9}$$

is the $\mathbb{F}$-valued N-soliton solution of equation (2).

Remark. The same result can also be derived using the general algebro-geometric construction of solutions of the version of the dKP equation given in (2). To do this, the wavefunction ψ is given by definition 1 in [3], but with a different definition of the expansions of $\psi(n_1, n_2, n_3)$ at A_i, namely, for $i, j, k = 1, 2, 3$ with $i \neq j \neq k \neq i$,

$$\psi(n_1, n_2, n_3) = t_i^{n_i} \sum_{s=0}^{\infty} Z_j^{n_k} Z_k^{n_j} \bar{\zeta}_s^{(i)}(n_1, n_2, n_3) t_i^s,$$

where t_i are the fixed $\mathbb{K}$-rational local parameters at A_i. The linear equation for ψ in the general case is of the form

$$(T_i \psi - T_j \psi) + Z_k \frac{T_j \bar{\zeta}_0^{(i)}}{\bar{\zeta}_0^{(i)}} \psi = 0.$$

The remaining part of the construction is the same as in [3].

3. Travelling wave form for the *N*-soliton solution

In this section, we wish to transform the soliton solutions given in (8) into an equivalent but more convenient form. In doing this, we will use the fact, referred as a gauge invariance, that for any solution τ of the dKP equation, $\tau' = \alpha^{n_1} \beta^{n_2} \gamma^{n_3} \delta \cdot \tau$ is also a solution for any constant $\alpha, \beta, \gamma, \delta$. We write $\tau' \simeq \tau$ if τ' can be obtained from τ using this gauge invariance.

Lemma 1. *Let $M(\mathbf{x},\mathbf{y})$, where $\mathbf{x}=(x_1,\ldots,x_n)$ and $\mathbf{y}=(y_1,\ldots,y_n)$, denote the Cauchy matrix, the matrix with (i,j)th entry $1/(x_i-y_j)$. It is well known that*

$$\det M(\mathbf{x},\mathbf{y})=\frac{\prod_{p<q}(x_p-x_q)(y_q-y_p)}{\prod_{p,q}(x_p-y_q)}=\prod_{p<q}\frac{(x_p-x_q)(y_q-y_p)}{(x_p-y_q)(x_q-y_p)}\prod_p\frac{1}{(x_p-y_p)}. \tag{10}$$

Also we have

$$M(\mathbf{x},\mathbf{y})^{-1}M(\mathbf{x},\mathbf{z})=\operatorname{diag}\left(\frac{\prod_p(x_p-y_i)}{\prod_{p\neq i}(y_p-y_i)}\right)M(\mathbf{y},\mathbf{z})\operatorname{diag}\left(\frac{\prod_p(y_p-z_i)}{\prod_p(x_p-z_i)}\right). \tag{11}$$

Proof. Let $\mathbf{x}_{\hat{k}}=(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n)$. Then, the (i,j)th entry in the inverse of $M(\mathbf{x},\mathbf{y})$ is

$$[M(\mathbf{x},\mathbf{y})^{-1}]_{i,j}=(-1)^{i+j}\frac{\det M(\mathbf{x}_{\hat{j}},\mathbf{y}_{\hat{i}})}{\det M(\mathbf{x},\mathbf{y})}=(x_j-y_i)\prod_{p\neq j}\frac{(x_p-y_i)}{(x_j-x_p)}\prod_{p\neq i}\frac{(x_j-y_p)}{(y_p-y_i)}.$$

Further, the (i,j)th entry in the product $M(\mathbf{x},\mathbf{y})^{-1}M(\mathbf{x},\mathbf{z})$ is

$$\frac{\prod_p(x_p-y_i)}{\prod_{p\neq i}(y_p-y_i)}\sum_{k=1}^{n}\frac{\prod_{p\neq i}(x_k-y_p)}{(x_k-z_j)\prod_{p\neq k}(x_k-x_p)}$$
$$=\frac{\prod_p(x_p-y_i)}{\prod_{p\neq i}(y_p-y_i)V(\mathbf{x})\prod_p(x_p-z_j)}\sum_{k=1}^{n}(-1)^{n-k}V(\mathbf{x}_{\hat{k}})\prod_{p\neq i}(x_k-y_p)\prod_{p\neq k}(x_p-z_j),$$

where $V(\mathbf{x})=\prod_{p>q}(x_p-x_q)$ is the Vandermonde determinant in variables $x_1,\ldots,x_n$ and $V(\mathbf{x}_{\hat{k}})$ is the Vandermonde determinant in variables $x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n$. In the (i,j)th entry, the sum is of degree $(n-1)(n-2)/2+2(n-1)=n(n-1)/2+n-1$ and we will factorize it by identifying all of its zeros. First, there are $n(n-1)/2$ coming when $x_r=x_s$ for any $r<s$ and $n-1$ from $y_r=z_j$ for $r\neq i$. This argument uses the fact that for any polynomial function f of degree less than $n-1$ one has $\sum_{k=1}^{n}(-1)^{n-k}V(\mathbf{x}_{\hat{k}})f(x_k)=0$ since the left-hand side is the expansion by the final column of the vanishing determinant

$$\begin{bmatrix}1 & x_1 & \cdots & x_1^{n-2} & f(x_1)\\ \vdots & \vdots & & \vdots & \vdots\\ 1 & x_n & \cdots & x_n^{n-2} & f(x_n)\end{bmatrix}.$$

Hence, the (i,j)th entry is, up to a constant factor,

$$\frac{\prod_p(x_p-y_i)}{\prod_{p\neq i}(y_p-y_i)}\frac{\prod_{p\neq i}(y_p-z_j)}{\prod_p(x_p-z_j)}=\frac{\prod_p(x_p-y_i)}{\prod_{p\neq i}(y_p-y_i)}\frac{1}{y_i-z_j}\frac{\prod_p(y_p-z_j)}{\prod_p(x_p-z_j)}.$$

To verify that it is precisely correct, and hence complete the proof of (11), we observe that, as it should, the above equals δ_{ij}, the Kronecker delta, when $\mathbf{z}=\mathbf{y}$. □

Theorem 2. *Let q denote any fixed generator of $\mathbb{F}^*$, i.e., a multiplicative subgroup of the finite field $\mathbb{F}$. The N-soliton solution (9) of the dKP equation over a finite field $\mathbb{F}$ admits the following form:*

$$\tau'=\sum_{J\subset\{1,\ldots,N\}}(-1)^{\#J}\left(\prod_{i,i'\in J;i<i'}a_{ii'}\right)q^{(\sum_{j\in J}\hat{\eta}_j)}, \tag{12}$$

where the sum is taken over all subsets of $\{1,\ldots,N\}$ *and* $\#J$ *denotes the cardinality of* J. *In (12),*

$$a_{ij} := \frac{(D_i - D_j)(E_i - E_j)}{(D_i - E_j)(D_j - E_i)}, \tag{13}$$

the exponents are $\hat{\eta}_j = \eta_j + \eta_j^0$ *where*

$$\eta_j := \sum_{k=1}^{3} p_j^k n_k, \tag{14}$$

and the parameters p_j^k *and phase constants* η_j^0 *are defined by*

$$q^{p_i^k} := \frac{E_i - A_k}{D_i - A_k} \qquad \text{and} \qquad q^{\eta_i^0} := \prod_{p=1}^{N} \frac{(C_p - D_i)}{(C_p - E_i)} \prod_{p=1;\, p\neq i}^{N} \frac{(D_p - E_i)}{(D_p - D_i)}. \tag{15}$$

The name travelling wave form comes from the form of $q^{\hat{\eta}_j}$, which are in direct analogy with the usual term $\exp(\vec{k}\vec{x} - \omega t)$ of linear plane waves. Note that for any τ satisfying (2) $\tau(1,0,0)$, $\tau(0,1,0)$ and $\tau(0,0,1)$ depend only on cross-ratio of appropriate points on the projective line. We also point out that to find p_i^k and η_{ij}^0 we need to solve a discrete logarithm problem.

Proof. The determinant in (9) is

$$\bar{\tau} = \det\left(-M(\boldsymbol{C},\boldsymbol{D})\,\mathrm{diag}\left(\prod_{k=1}^{3}\left(\frac{D_i - A_k}{C_i - A_k}\right)^{n_k}\right) + M(\boldsymbol{C},\boldsymbol{E})\,\mathrm{diag}\left(\prod_{k=1}^{3}\left(\frac{E_i - A_k}{C_i - A_k}\right)^{n_k}\right)\right),$$

where M denotes the Cauchy matrix as defined in lemma 1, and so

$$\bar{\tau} \simeq \tau' := \det\left(I - M(\boldsymbol{C},\boldsymbol{D})^{-1} M(\boldsymbol{C},\boldsymbol{E})\,\mathrm{diag}\left(\prod_{k=1}^{3}\left(\frac{E_i - A_k}{D_i - A_k}\right)^{n_k}\right)\right).$$

Using (11) and the fact that for any matrices P, Q, $\det PQ = \det QP$, we get

$$\tau' = \det(I - M(\boldsymbol{D},\boldsymbol{E})\,\mathrm{diag}(D_i - E_i)\,\mathrm{diag}(q^{\hat{\eta}_i})).$$

Now the determinant $\det(P+Q)$, of the sum of two $N\times N$ matrices, may be expressed as the sum over all subsets $J\subset\{1,\ldots,N\}$ of $\det R_J$ where the ith column of R_J equals the ith column of Q if $i\in J$ and otherwise equals the ith column of P. Using this fact,

$$\tau' = \sum_{J\subset\{1,\ldots,N\}} (-1)^{\#J} \det M_J(\boldsymbol{D},\boldsymbol{E}) \prod_{i\in J} (D_i - E_i) q^{\hat{\eta}_i},$$

where M_J denotes the Cauchy matrix with row and column indices restricted to J. Formula (12) now follows immediately from (10). □

Remark. We also present here an alternative proof of theorem 2. The argument presented shows why there is only pairwise interaction of solitons.

Starting from (9), for each i one divides the ith column of (7) by $\phi_i(D_i)$ and we see that $\bar{\tau} \simeq \tau' = \det\Phi$ where

$$[\Phi]_{ij} = \left(\left(\frac{D_i - C_i}{D_j - C_i}\right) - \left(\frac{D_i - C_i}{E_j - C_i}\right) q^{\eta_j}\right) \prod_{k=1}^{3}\left(\frac{D_j - A_k}{D_i - A_k}\right)^{n_k}, \tag{16}$$

where η_j is given by (14), is also a solution of (2). Further, if we define

$$[\hat{\Phi}]_{ij} := \left(\frac{D_i - C_i}{D_j - C_i}\right) - \left(\frac{D_i - C_i}{E_j - C_i}\right) q^{\eta_j} \tag{17}$$

it is easy to see that $\det \Phi \simeq \det \hat{\Phi}$.

We will next show how $\det \hat{\Phi}$ can be obtained from a vacuum solution $\det \hat{\Phi}_0$ where $[\hat{\Phi}_0]_{ij} = \left(\frac{D_i - C_i}{D_j - C_i}\right)$ by means of *substitution* operations. The key idea we use in finding coefficients of different powers of q in formula (12) is the observation that, according to (17), for each term including q^{η_k} we should make the substitution

$$\left(\frac{D_i - C_i}{D_k - C_i}\right) \quad \longrightarrow \quad -\left(\frac{D_i - C_i}{E_k - C_i}\right) \tag{18}$$

for each i, in the kth row of $\hat{\Phi}_0$. Then, $\det \hat{\Phi}$ can be expressed in terms of determinants obtained by making appropriate replacements in $\det \hat{\Phi}_0$.

First note that

$$\det \hat{\Phi}_0 = M(-\boldsymbol{C}, -\boldsymbol{D}) \prod_i (D_i - C_i) = \prod_{i,j=1;i<j}^{N} \frac{(C_i - C_j)(D_i - D_j)}{(C_i - D_j)(D_i - C_j)}. \tag{19}$$

Denote by Φ_J the matrix with replacements (18) in the rows $k \in J$. We first consider the case $J = \{k\}$ for fixed k. Since D_k appears only in the kth row and kth column, then Φ_J after multiplying kth column by $-\left(\frac{E_k - C_k}{D_k - C_k}\right)$ becomes the determinant (19) with D_k replaced by E_k. Then,

$$\begin{aligned}
\det \Phi_J &= -\left(\frac{D_k - C_k}{E_k - C_k}\right) \det \hat{\Phi}_0 \Big|_{D_k \to E_k} \\
&= -\left(\frac{D_k - C_k}{E_k - C_k}\right) \prod_{i,j=1;i<j}^{N} \frac{(C_i - C_j)(D_i - D_j)}{(C_i - D_j)(D_i - C_j)} \Big|_{D_k \to E_k} \\
&= -\left(\frac{D_k - C_k}{E_k - C_k}\right) \left(\prod_{j'=1;j' \neq k}^{N} \left(\frac{D_k - D_{j'}}{D_k - C_{j'}}\right)^{-1} \left(\frac{E_k - D_{j'}}{E_k - C_{j'}}\right) \right) \det \hat{\Phi}_0.
\end{aligned}$$

In the notation of the theorem, the coefficient of q^{η_j} is $\det \Phi_{\{k\}} = -q^{\eta_k^0} \det \hat{\Phi}_0$.

Now we consider coefficient of $q^{\sum_{k \in J} \eta_k}$. This is the determinant $\det \Phi_J$ obtained from $\det \hat{\Phi}_0$ by making replacements (18) in rows $k \in J$ for general $J \subset I$. The number of elements in J is denoted by $\#J$. Repeating the procedure described above for each $k \in J$ we arrive at

$$\det \Phi_J = (-1)^{\#J} \left(\prod_{k \in J} \frac{D_k - C_k}{E_k - C_k} \right) \det \hat{\Phi}_0 \Big|_{D_k \to E_k; k \in J}. \tag{20}$$

Then, we have

$$\begin{aligned}
\det \hat{\Phi}_0|_{D_k \to E_k; k \in J} = &\left(\prod_{\{k_i, k_j\} \subset J} \frac{(D_{k_1} - D_{k_2})(E_{k_1} - E_{k_2})}{(E_{k_1} - D_{k_2})(D_{k_1} - E_{k_2})} \right) \\
&\times \prod_{k \in J} \left(\prod_{j'=1; j' \neq k}^{N} \left(\frac{D_k - D_{j'}}{D_k - C_{j'}}\right)^{-1} \left(\frac{E_k - C_{j'}}{E_k - C_{j'}}\right) \right) \det \hat{\Phi}_0.
\end{aligned}$$

The extra terms for pairs $\{k_i, k_j\} \in J$ are present because, since $k_j \neq k_i$, we also need to perform the replacements $D_{k_j} \to E_{k_j}$ in the factor $\prod_{j'=1;j' \neq k_i}^{N} \left(\frac{D_{k_i} - D_{j'}}{D_{k_i} - C_{j'}}\right)^{-1} \left(\frac{E_{k_i} - D_{j'}}{E_{k_i} - C_{j'}}\right)$. This is done by multiplying by $\frac{(D_{k_1}-D_{k_2})(E_{k_1}-E_{k_2})}{(E_{k_1}-D_{k_2})(D_{k_1}-E_{k_2})}$. We point out here that the extra corrections are for *pairs* $\{k_i, k_j\} \in J$ and it is this that is responsible for the existence of only *pairwise* interaction terms in formula (12). So finally, the coefficient of $q^{\sum_{j\in J}\eta_j}$ is

$$\det \Phi_J = (-1)^{\#J} \left(\prod_{i,i'\in J; i<i'} a_{ii'} \right) \left(\prod_{k\in J} q^{\eta_k^0} \right) \det \hat{\Phi}_0. \tag{21}$$

After dividing all terms by $\det \hat{\Phi}_0$ and collecting them together we obtain formula (12).

Note that our considerations are valid for any field of definition of the parameters C_i and D_j.

Remark. The results obtained above also apply to the discrete analogue of generalized Toda equation [6]

$$Z_1 f_{m_1+1,m_2,m_3} f_{m_1-1,m_2,m_3} + Z_2 f_{m_1,m_2+1,m_3} f_{m_1,m_2-1,m_3} + Z_3 f_{m_1,m_2,m_3+1} f_{m_1,m_2,m_3-1} = 0.$$

The transition from dKP to DAGTE (where we assume $(m_1+m_2+m_3) \equiv 0 \bmod 2$) is given by $f_{m_1,m_2,m_3} := \tau(n_1, n_2, n_3)$ where $n_i = \frac{1}{2}(m_i - m_j - m_k)$ for $i \neq j \neq k \neq i$ or, equivalently, $m_i = -(n_j + n_k)$ for $i \neq j \neq k \neq i$. In this situation, $f_{0,0,0} = \tau(0, 0, 0)$. With the variables m_1, m_2, m_3 the exponents of a travelling wave given by (14) have similar form, namely $\eta_i = \sum_{j=1}^{3} \hat{p}_i^j m_j$, where $\hat{p}_i^j = \sum_{k=1}^{3} (2\delta_{jk} - 1) p_k$ and δ_{jk} is the Kronecker delta.

4. Pattern structures in soliton interactions

So far we have seen that the finite-field N-soliton solutions we obtained have the same structure as the complex field case. In particular, the travelling wave form (12) is completely analogous to the complex field case. Despite this correspondence, the typical soliton-like interaction pattern is not present in the finite-field case. Below we argue that one cannot expect that an arbitrary N-soliton solution over a finite field will be a collection of asymptotically separated waves interacting as in the way characteristic of the complex field case.

These differences in the interaction properties follow naturally from the differences in structure between finite fields and the complex numbers. First, finite fields have no good (total) ordering which are consistent for both addition and multiplication and so it is impossible to find in the finite filed case a direct analogue of wave amplitude; rather than following a wave propagation by observing how its points of maximum amplitude move we may only trace the propagation of patterns. The appearance of a one-soliton solution however in the finite-field case mimics the usual appearance quite well, as can be seen in figure 1.

The next difference results from the replacement of exponentials in the complex case by powers of a generator q of the multiplicative group $\mathbb{F}^*$ of the finite field $\mathbb{F}$. Since $q^{|\mathbb{F}|-1} = 1$, this implies periodicity of $\tau(n_1, n_2, n_3)$ with respect to each variable n_i. As a consequence, we cannot discuss the asymptotic behaviour of the solution in usual sense. Moreover, for any given solution one could restrict analysis to a finite *base cube* containing all information about the solution, but the rest is periodic repetition. The length of any edge of a base cube is at most $|\mathbb{F}| - 1$.

Considering theorem 2, the ith one-soliton component of the N-soliton solution is unchanged by a shift in the lattice by $\vec{n}^i = \left(n_1^i, n_2^i, n_3^i\right)$ for any n_1^i, n_2^i, n_3^i satisfying $q^{\eta_i} = 1$ or, equivalently,

$$\eta_i = \sum_{k=1}^{3} p_i^k n_k^i \equiv 0 \qquad \bmod \quad (|\mathbb{F}| - 1). \tag{22}$$

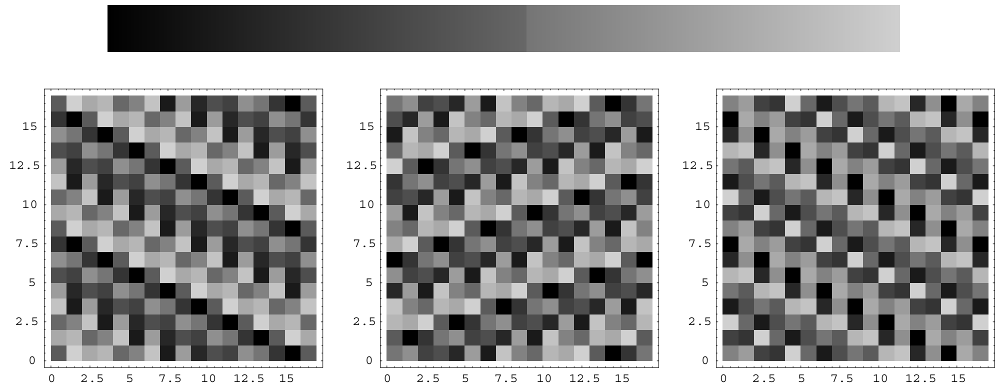

Figure 1. A plot of $\tau(n_1, n_2, n_3)$ function of three one-soliton solutions (see examples for details). We fix $n_1 = 0$, and $n_2, n_3 \in \{0, \ldots, 16\}$. The n_2 axis is directed to the right and the n_3 axis is directed upwards. Elements of $\mathbb{F}_{17}$ are represented on the following scale: from 0 (dark) to 16 (light grey).

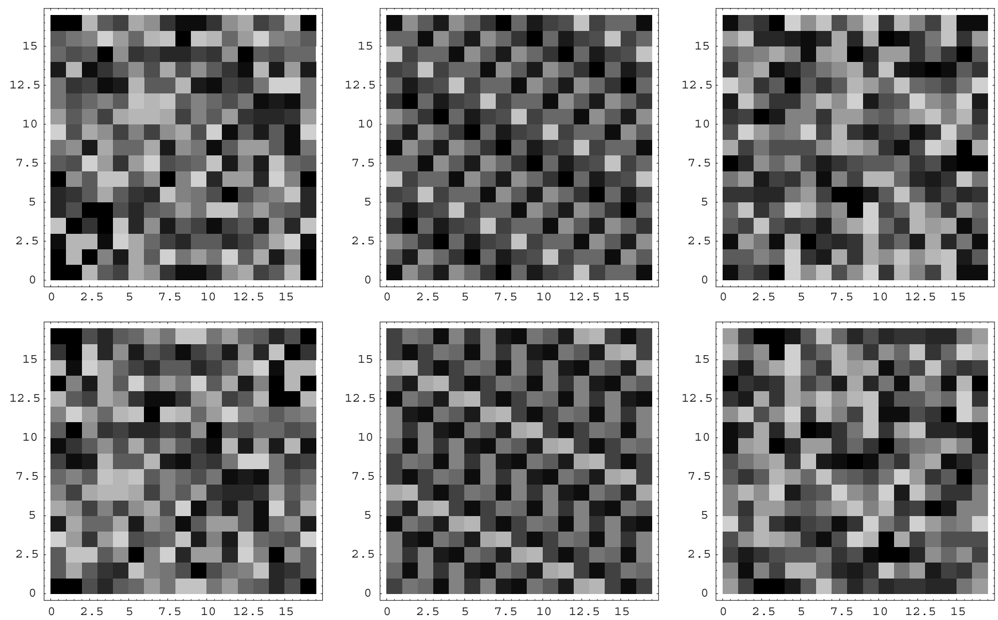

Figure 2. A plot of $\tau(n_1, n_2, n_3)$ for the three two-soliton interactions (AB, AC, BC) of one-soliton solutions presented in figure 1. We fix $n_1 = 0$, and $n_2, n_3 \in \{0, \ldots, 16\}$. In the second row we have $n_1 = 1$. The n_2 axis is directed to the right and the n_3 axis is directed upwards.

Since expression (12) contains q^{η_i} for $i \in \{1, 2, \ldots, N\}$, a period vector $\vec{n} = (n_1, n_2, n_3)$ for this solution should be a common solution of (22) for all i. In general, it is impossible to find a nonzero solution for $N \geqslant 3$ and it means there is no additional structure within the base cube in this case. An example of such a three-soliton solution is shown in figure 3 and the structure of a base cube is discussed below in more detail.

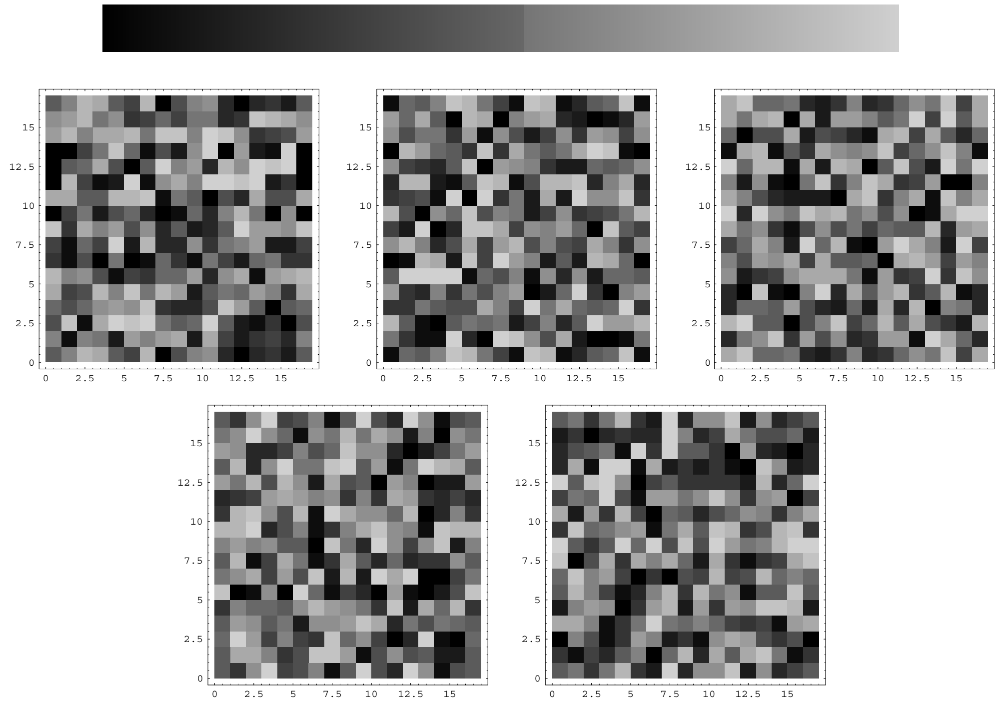

Figure 3. A three-soliton solution $\tau(n_1, n_2, n_3)$ being the solitonic sum of those from figure 1 for $n_1 = 0, 1, 2, 4$ and 8. The n_2 axis is directed to the right and the n_3 axis is directed upwards. Elements of $\mathbb{F}_{17}$ are represented on the following scale: from 0 (dark) to 16 (light grey).

Examples. Fix the finite field to be $\mathbb{F} = \mathbb{F}_{17}$, i.e. the field of integers modulo 17. As a generator of $\mathbb{F}^*$ we choose $q = 3$. Let us fix $A_1 = 7$, $A_2 = 4$ and $A_3 = 3$ so that the coefficients in the dKP equation are $A_2 - A_3 = Z_1 = 1$, $A_1 - A_3 = Z_2 = 4$ and $A_1 - A_2 = Z_3 = 3$.

One-soliton solutions. In figure 1, we present three one-soliton solutions of the dKP equation over $\mathbb{F}$. For the solution A on the left, denoted by subscript $_1$ we have chosen $C_1 = 11, D_1 = 6, E_1 = 9$; for the solution B in the middle, denoted by $_2$, we have $C_2 = 10, D_2 = 12, E_2 = 14$ and finally $C_3 = 8, D_3 = 13, E_3 = 15$ for the solution C on the right. The respective parameters in the exponent (14) are

$$\vec{p}_1 = \left(p_1^1, p_1^2, p_1^3\right) = (6, 7, 14), \qquad \vec{p}_2 = \left(p_2^1, p_2^2, p_2^3\right) = (6, 9, 5),$$
$$\vec{p}_3 = \left(p_3^1, p_3^2, p_3^3\right) = (11, 5, 10).$$

Thus periods in variables n_1, n_2, n_3 are as follows: 8, 16, 8 for the soliton $_1$, 8, 16, 16 for the soliton $_2$ and 16, 16, 8 for $_3$. We fixed $n_1 = 0$, since increasing any variable by 1 results in shift in the other two variables and so the plots for any value of n_1 are simply a translation of the plots we present. This comes from the fact that in general there exists a nonzero solution in two variables n_j, n_k of the single equation (22) with the third variable n_i being fixed ($i, j, k \in \{1, 2, 3\}$, $i \neq j \neq k \neq i$). The special case is if p^i is not a linear combination of p^j and p^k with coefficients from $\mathbb{Z} \bmod (|\mathbb{F}| - 1)$. (This could happen for instance if p^j and p^k are zero divisors of $|\mathbb{F}| - 1$.) In the case presented in figure 1, period vectors might be chosen to be $\vec{n}_1 = (1, 0, 3)$ for A, $\vec{n}_2 = (1, 0, 2)$ for B and $\vec{n}_3 = (1, 1, 0)$ for C. Further, the period vectors $\vec{n}$ for these solutions in the plane n_2, n_3 are $\vec{n}_{1a} = \vec{n}_{3a} = (0, 2, -1), \vec{n}_{1b} = \vec{n}_{3b} = (0, 0, 8), \vec{n}_{2a} = (0, 3, 1)$ and $\vec{n}_{2b} = (0, -1, 5)$. (All periods vectors are not uniquely determined.)

Two-soliton solutions. In figure 2, the two-soliton solutions representing the interaction of two of the one-soliton solutions shown in figure 1 are presented. The upper line is for $n_1 = 0$ while the lower is for $n_1 = 1$. In the cases A interacting with B (called AB) and B interacting with C (AC) it is a simple shift by respective vectors $(1, -1, -4)$ and $(1, -5, -5)$. (*Note.* Since $q^{16} = 1$, the lines $n = 0$ and $n = 16$ are identical but both of them are shown on plots.) For the case AC there are no such a shift, because the two equations (22) for $i = 1$ and $i = 3$ for n_2 and n_3 have no nonzero solution for any value of n_1. This is because $n_1 \cdot (6, 11) \notin \mathbb{Z}_{16} \cdot (7, 5)$. Since $\mathrm{span}(\vec{n}_{1a}, \vec{n}_{1b}) \cap \mathrm{span}(\vec{n}_{2a}, \vec{n}_{2b}) = \{\vec{0}\}$, there are no nonzero period vectors in the plane n_2, n_3 for either AB or BC. In contrast, for AC the period vectors in this plane are exactly the same as for soliton A and C (since they are the same). Similarly, one could examine other planes obtaining plane period vectors $(0, 0, 8)$ for AC, $(8, 0, 0)$ and $(4, 8, 0)$ for AB and none for BC. Periods for AB are $(8, 16, 16)$, for AC are $(16, 16, 8)$ and for BC are the maximal $(16, 16, 16)$. Note that BC shows that it is possible for a two-soliton solution to have no structure within the base cube.

A three-soliton solution. In this case, there are three equations (22) for three variables, so in general there are no nonzero solutions. The example presented in figure 3 using parameters in A, B and C is of this kind. Because of this, there are no extra period vectors and so this solution has no structure within a base cube.

It is clear that this is also the generic situation for the interaction of N-soliton solutions obtained by the algebro-geometric approach for $N > 2$.

5. Concluding remarks

In summary, we have seen that the interaction of three or more finite-field soliton solutions of the dKP equation has no more structure in the base cube than random data. Given a finite field $\mathbb{F}$ of sufficient size, it would seem to be computationally impractical to attempt to reconstruct the parameters C_α, D_α and E_α which define the solution, from the seemingly random data that they generate. This leads one to imagine possible applications of such solutions in encrypted data transmission. In conclusion, we note that applications of elliptic curves over finite fields have already been studied for some time [7, 13]

Examining soliton solutions over finite fields is a relatively new subject and requires further study. The approach we presented here is related to periodicity in two different ways. The first is because of the algebro-geometric construction and the second comes from the properties of finite fields. Moreover, finite extensions of finite fields are never algebraically closed and this fact is reflected in the existence of many new possibilities in the construction of breather-type solutions. In contrast with the case of the field of complex numbers, which is an algebraically closed extension of the field of real numbers of degree two, for finite fields we can have extensions of arbitrary degree. Simple examples and relevant terminology were presented in [5]. From the other side, in the classical continuous case many types of breather-type solutions are known, including 'sophisticated' complexitons (see [10, 11] and references therein). It should be very interesting to investigate analogues of these for the finite field case. However, it will require both substantial development of the theory discussed in this paper and clarification of some details of complexiton solutions in a discrete setting. For these reasons, we leave this topic for future research.

Acknowledgments

The authors thank Professors T Tokihiro and R Willox for creating a friendly environment for research at the Graduate School of Mathematical Sciences, University of Tokyo and for their overall help. MB is partially supported by Grant-in-Aid of the JSPS Postdoctoral Fellowship for Foreign Researchers of Japan Society for the Promotion of Science (ID No P 05050) and by Polish Ministry of Science and Information Society Technologies (Grant No 1 P03B 01728).

References

[1] Białecki M 2005 Integrable 1D Toda cellular automata *J. Nonlinear Math. Phys.* **12** (Suppl. 2) 28–35

[2] Białecki M 2005 Integrable KP and KdV cellular automata out of a hyperelliptic curve *Glasgow Math. J.* A **47** 33–44

[3] Białecki M and Doliwa A 2003 The discrete KP and KdV equations over finite fields *Theor. Math. Phys.* **137** 1412–8

[4] Białecki M and Doliwa A 2005 Algebro-geometric solution of the discrete KP equation over a finite field out of a hyperelliptic curve *Commun. Math. Phys.* **253** 157–70

[5] Doliwa A, Białecki M and Klimczewski P 2003 The Hirota equation over finite fields: algebro-geometric approach and multisoliton solutions *J. Phys. A: Math. Gen.* **36** 4827–39

[6] Hirota R 1981 Discrete analogue of a generalized Toda equation *J. Phys. Soc. Japan* **50** 3785–91

[7] Koblitz N 1998 *Algebraic Aspects of Cryptography* (Berlin: Springer)

[8] Krichever I M 1977 Methods of algebraic geometry in the theory of nonlinear equations *Usp. Mat. Nauk* **32** 183–208

[9] Krichever I M 1978 Algebraic curves and nonlinear difference equations *Usp. Mat. Nauk* **33** 215–6

[10] Ma W X 2002 Complexiton solutions to the Korteweg-de Vries equation *Phys. Lett.* A **301** 35–44

[11] Ma W X and You Y 2005 Solving the Korteweg-de Vries equation by its bilinear form: Wronskian solutions *Trans. Am. Math. Soc.* **357** 1753–78

[12] Matsukidaira J, Satsuma J, Takahasi D, Tokihiro T and Torii M 1997 Toda-type cellular automaton and its N-soliton solution *Phys. Lett.* A **225** 287–95

[13] Miller V S 1986 *Advances in Cryptology—CRYPTO'85 (Santa Barbara, CA, 1985) (Lecture Notes in Computer Science* vol 218) (Berlin: Springer) pp 417–26

[14] Miwa T, Jimbo M and Date E 2000 *Solitons: Differential Equations, Symmetries and Infinite Dimensional Algebras* (Cambridge: Cambridge University Press)

[15] Ohta Y, Hirota R and Tsujimoto S 1993 Casorati and discrete Gram type determinant representations of solutions of the discrete KP hierarchy *J. Phys. Soc. Japan* **62** 1872–86

[16] 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