Signatures over finite fields of growth properties for lattice equations

2015 J. Phys. A: Math. Theor. 48 085201

(http://iopscience.iop.org/1751-8121/48/8/085201)

IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **48** (2015) 085201 (20pp) doi:10.1088/1751-8113/48/8/085201

Signatures over finite fields of growth properties for lattice equations

John A G Roberts[1,3] **and Dinh T Tran**[1,2]

[1] School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
[2] Department of Mathematics and Statistics, La Trobe University, Bundoora, VIC 3086, Australia

E-mail: jag.roberts@unsw.edu.au and dinh.tran@latrobe.edu.au

Received 23 September 2014, revised 6 January 2015
Accepted for publication 9 January 2015
Published 30 January 2015

Abstract

We study integrable lattice equations and their perturbations over finite fields. We write these equations in projective coordinates and assign boundary values along axes in the first quadrant. We propose some growth diagnostics over finite fields that can often distinguish between integrable equations and their non-integrable perturbations. We also discuss the limitations of the diagnostic. Finally, we show that conducting parameter searches over finite fields for lattice equations that satisfy a factorization test leads to potential new equations that have vanishing entropy.

Keywords: lattice equation, integrable lattice equation, algebraic entropy, integrability, finite fields

(Some figures may appear in colour only in the online journal)

1. Introduction

Integrability is a rare phenomenon but it possesses many interesting properties. Integrability for discrete systems has been investigated via some detectors such as algebraic entropy, Diophantine integrability, singularity confinement [4, 6]. These detectors were introduced based on the 'low complexity' of integrable systems. The low complexity of integrable equations can be also seen through finite fields. In the literature, there has been some research concerning discrete integrable equations over finite fields. In 2003, Roberts and Vivaldi used the so called 'Hasse–Weil' bound to work with rational maps over finite fields [15]. They were able to distinguish integrable maps and their perturbations by counting the number of

[3] Author to whom any correspondence should be addressed.

Table 1. A list of the integrable lattice equations considered in this paper. Free parameters are taken to be integers.

Name	Lattice equation	Reference
Q_1	$\alpha(u-u_2)(u_1-u_{12})-\beta(u-u_1)(u_2-u_{12})+\delta^2\alpha\beta(\alpha-\beta)=0$	[1]
Q_2	$\alpha(u-u_2)(u_1-u_{12})-\beta(u-u_1)(u_2-u_{12})+\alpha\beta(\alpha-\beta)$ $\times(u+u_1+u_2+u_{12})-\alpha\beta(\alpha-\beta)(\alpha^2-\alpha\beta+\beta^2)=0$	[1]
Q_3	$(\beta^2-\alpha^2)(uu_{12}+u_1u_2)+\beta(\alpha^2-1)(uu_1+u_2u_{12})-\alpha(\beta^2-1)$ $\times(uu_2+u_1u_{12})-\delta^2(\alpha^2-\beta^2)(\alpha^2-1)(\beta^2-1)/(4\alpha\beta)=0$	[1]
H_1	$(u-u_{12})(u_1-u_2)+\beta-\alpha=0$	[1, 13]
H_2	$(u-u_{12})(u_1-u_2)+(\alpha-\beta)(u+u_1+u_2+u_{12})+\beta^2-\alpha^2=0$	[1]
H_3	$\alpha(uu_1+u_2u_{12})-\beta(uu_2+u_1u_{12})+\delta(\alpha^2-\beta^2)=0$	[1]
KdV	$u_1^{-1}-u_2^{-1}-u+u_{12}=0$	[13]

orbits over finite fields. There was another approach given by Doliwa and Bialecki, namely an algebro-geometric one to study soliton solutions of discrete KdV and KP equations [2, 3]. In 2012, Kanki *et al* studied the discrete KdV equation and its soliton solutions over finite fields by introducing a parameter in the equation [9]. He and his collaborators also studied Painlevé equations and the analog of singularity confinement over finite fields [8].

In this paper, we investigate growth properties of lattice equations over finite fields (having systematically studied this over $\mathbb{Q}$ recently in [14]). We study integrable equations and their perturbations. The advantage of working over $\mathbb{F}_p$ is that computations are fast and that parameter searches are sharp. We wish to ask if and how concepts of Diophantine integrability [6] and factorization over small lattice squares [7, 14] have analogues or signatures over finite fields.

This paper is organized as follows. In section 2, we give a setting to measure the complexity of certain lattice equations. We give a list of integrable lattice equations that we consider in this paper and a list of their corresponding projective versions. We give a brief summary of growth of degrees over the integers and the results of [14]. Over the integers, integrable equations and non-integrable equations can be distinguished by looking at the degree of the gcd of the projective coordinates at each vertex in general and along the diagonal in particular. In section 3, we study signatures of the growth of degrees over the finite fields using the number of common roots (mod p) of the projective lattice variables. It is possible to separate to some extent integrable cases and non-integrable cases. In section 4, we build two models for integrable cases and their perturbations that agree well with our numerical experiments. We then introduce a universal curve to fit our data and our models for both integrable and non-integrable cases. In the final section, we add some cubic terms to some known integrable equations and use a factorization test over finite fields to obtain some asymmetric lattice equations whose algebraic entropy vanishes.

2. The setting and preliminary results

In this section, we give a setting that will be used in this paper to measure the complexity of certain lattice equations.

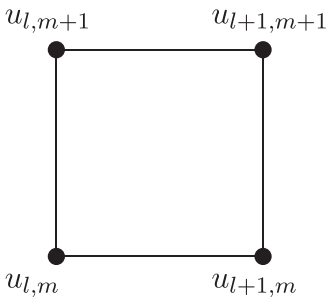

Figure 1. An elementary square of the integer lattice with field variables on the vertices.

2.1. Lattice rules in projective coordinates

We consider a multi-affine equation on a quad graph

$$Q\left(u_{l,m},\, u_{l+1,m},\, u_{l,m+1},\, u_{l+1,m+1};\, \alpha,\, \beta\right) = 0, \tag{1}$$

whose (field) variables $u_{l,m}$ depend on coordinates $(l,\, m) \in \mathbb{Z} \times \mathbb{Z}$ (see figure 1). In other words, this equation is linear in each field variable and is defined on a square. Table 1 is the list of lattice equations that we will consider in this paper. For convenience, we have used the shorthand there:

$$u := u_{l,m},\quad u_1 := u_{l+1,m},\quad u_2 := u_{l,m+1},\quad u_{12} := u_{l+1,m+1}. \tag{2}$$

Free parameters in the equations are shown by Greek letters and in this paper, will be taken to be rational, equivalently integer after multiplying through. These equations (except KdV) belong to the Adler–Bobenko–Suris (ABS) classification [1] and satisfy *consistency around a cube*. Therefore, they are integrable in the sense of possessing a Lax pair.

Generically, we can solve (1) for the variable in the top right corner to obtain

$$u_{l+1,m+1} = \frac{h_2\left(u_{l,m},\, u_{l+1,m},\, u_{l,m+1}\right)}{h_1\left(u_{l,m},\, u_{l+1,m},\, u_{l,m+1}\right)}, \tag{3}$$

where the degree of each of three arguments in h_1 and h_2 is at most 1 and we assume that h_1 and h_2 have no non-constant common factor and that

$$\frac{\partial h_i}{\partial v} \neq 0 \text{ for } i = 1 \text{ or } i = 2, \tag{4}$$

and v is u, u_1 or u_2 of (2). We then introduce projective coordinates $(x_{l,m},\, z_{l,m})$ at the site $(l,\, m)$ by taking $u_{l,m} = \frac{x_{l,m}}{z_{l,m}}$. Substituting into (3) we obtain the projective version of (3)

$$x_{l+1,m+1} = f\left(x_{l,m},\, x_{l+1,m},\, x_{l,m+1},\, z_{l,m},\, z_{l+1,m},\, z_{l,m+1}\right), \tag{5}$$

$$z_{l+1,m+1} = g\left(x_{l,m},\, x_{l+1,m},\, x_{l,m+1},\, z_{l,m},\, z_{l+1,m},\, z_{l,m+1}\right), \tag{6}$$

where f and g are homogeneous polynomials of degree 3. It can be seen that each term in f and g includes exactly one projective coordinate from each of the remaining 3 vertices of the square, see [14] for more details. We call (5) and (6) a lattice rule associated with the equation (1). The associated lattice rules of the equations in table 1 are given explicitly in table 2.

Table 2. Projective versions of the the rules of table 1, cf (5) and (6).

Equation	$x_{l+1,m+1}$	$z_{l+1,m+1}$
Q_1	$\alpha x_{l+1,m}x_{l,m}z_{l,m+1} - \alpha x_{l+1,m}x_{l,m+1}z_{l,m} - \beta x_{l,m+1}x_{l,m}z_{l+1,m}$ $+\beta x_{l,m+1}x_{l+1,m}z_{l,m} + (\delta\alpha^2\beta - \delta\alpha\beta^2)z_{l+1,m}z_{l,m}z_{l,m+1}$	$(\alpha - \beta)x_{l,m}z_{l+1,m}z_{l,m+1} - \alpha x_{l,m+1}z_{l,m}z_{l+1,m}$ $+\beta x_{l+1,m}z_{l,m}z_{l,m+1}$
Q_2	$(\beta x_{l,m+1}z_{l+1,m} - \alpha x_{l+1,m}z_{l,m+1} + (\alpha\beta^2 - \alpha^2\beta)z_{l+1,m}z_{l,m+1})x_{l,m}$ $+((\alpha - \beta)z_{l,m}x_{l+1,m} + (\alpha\beta^2 - \alpha^2\beta)z_{l+1,m}z_{l,m})x_{l,m+1}$ $+(\alpha\beta^2 - \alpha^2\beta)z_{l,m+1}z_{l,m}x_{l+1,m} + (-\alpha\beta^4 + 2\alpha^2\beta^3 + \alpha^4\beta - 2\alpha^3\beta^2)$ $\times z_{l+1,m}z_{l,m+1}z_{l,m}$	$(-\alpha + \beta)z_{l+1,m}z_{l,m+1}x_{l,m}+\alpha x_{l,m+1}z_{l,m}z_{l+1,m}$ $-\beta x_{l+1,m}z_{l,m}z_{l,m+1} + (\alpha^2\beta - \alpha\beta^2)z_{l+1,m}z_{l,m+1}z_{l,m}$
Q_3	$(4\alpha^2\beta^3 - 4\alpha^2\beta)x_{l,m}z_{l+1,m}x_{l,m+1} + (-4\alpha^3\beta^2 + 4\alpha\beta^2)z_{l,m+1}x_{l+1,m}x_{l,m}$ $+(4\delta\alpha^3\beta - 4\delta\alpha\beta^3)z_{l,m}x_{l+1,m}x_{l,m+1}$ $+(-\alpha^4 + \beta^4 + \alpha^4\beta^2 - \alpha^2\beta^4 + \alpha^2 - \beta^2)z_{l+1,m}z_{l,m+1}z_{l,m}$	$4(-\delta\alpha^2 + \delta\beta^2)\beta\alpha z_{l+1,m}z_{l,m+1}x_{l,m}$ $+4(\alpha^2\beta - \beta)\beta\alpha z_{l+1,m}z_{l,m}x_{l,m+1}$ $+4(-\alpha\beta^2 + \alpha)\beta\alpha z_{l,m+1}z_{l,m}x_{l+1,m}$
H_1	$-x_{l,m}x_{l+1,m}z_{l,m+1} + x_{l,m}x_{l,m+1}z_{l+1,m}+(\alpha - \beta)z_{l,m}z_{l+1,m}z_{l,m+1}$	$(-x_{l+1,m}z_{l,m+1} + x_{l,m+1}z_{l+1,m})z_{l,m}$
H_2	$x_{l,m}x_{l+1,m}z_{l,m+1} - x_{l,m}x_{l,m+1}z_{l+1,m}+(\beta - \alpha)x_{l,m}z_{l+1,m}z_{l,m+1}$ $+(\beta - \alpha)x_{l+1,m}z_{l,m}z_{l,m+1} + (\beta - \alpha)x_{l,m+1}z_{l,m}z_{l+1,m}$ $+(\beta^2 - \alpha^2)z_{l,m}z_{l+1,m}z_{l,m+1}$	$(x_{l+1,m}z_{l,m+1} - x_{l,m+1}z_{l+1,m} + (\alpha - \beta)z_{l+1,m}z_{l,m+1})z_{l,m}$
H_3	$-\alpha x_{l+1,m}x_{l,m}z_{l,m+1} + \beta x_{l,m+1}x_{l,m}z_{l+1,m} + (\delta\beta^2 - \delta\alpha^2)z_{l+1,m}z_{l,m}z_{l,m+1}$	$(\alpha x_{l,m+1}z_{l+1,m} - \beta x_{l+1,m}z_{l,m+1})z_{l,m}$
KdV	$-x_{l,m+1}z_{l,m}z_{l+1,m} + x_{l+1,m}z_{l,m}z_{l,m+1} + x_{l,m}x_{l+1,m}x_{l,m+1}$	$z_{l,m}x_{l+1,m}x_{l,m+1}$

We will also be interested in perturbations of (1) or (3) that keep it multi-affine. A typical one we use is

$$u_{l+1,m+1} = \frac{h_2\left(u_{l,m},\, u_{l+1,m},\, u_{l,m+1}\right)}{h_1\left(u_{l,m},\, u_{l+1,m},\, u_{l,m+1}\right)} + r, \tag{7}$$

with $r \in \mathbb{Z}$.

2.2. Lattice rules over the integers

In this section, we summarize some results that we obtained on the growth of degrees of certain lattice equations [14]. These results will be useful in the transition to finite fields in the next section.

The boundary conditions that we use to study the lattice equations in this paper are corner boundary conditions prescribed on the axes in the first quadrant and involving an indeterminate w (called case I in [14]):

$$\text{Case I:} \begin{cases} x_{0,0} = aw + b \text{ and } z_{0,0} = cw + d, & \text{where } a,\, b,\, c,\, d \in \mathbb{Z}, \\ x_{0,m} \in \mathbb{Z} \text{ and } z_{0,m} = 1, & m = 1,\, 2,\, \ldots, \\ x_{l,0} \in \mathbb{Z} \text{ and } z_{l,0} = 1, & l = 1,\, 2,\, \ldots. \end{cases} \tag{8}$$

All integers are positive and generated randomly. Working out from the origin using the boundary conditions and the lattice rule, we generate the top right entries in each lattice square. This gives the polynomials $x_{l+1,m+1}(w)$, $z_{l+1,m+1}(w) \in \mathbb{Z}[w]$ given by (5)–(6). In particular, calculating $x_{m,m}(w)$ and $z_{m,m}(w)$, $m \in \mathbb{N}$, requires having built all polynomials on all other lattice sites in the $m \times m$ square extending out from the origin in the first quadrant.

Let $\gcd_{l,m}(w)$ be the greatest common divisor of $x_{l,m}(w)$ and $z_{l,m}$ in $\mathbb{Z}[w]$. Therefore, one can write

$$x_{l,m}(w) = \gcd_{l,m}(w)\, \bar{x}_{l,m}(w), \tag{9}$$

$$z_{l,m}(w) = \gcd_{l,m}(w)\, \bar{z}_{l,m}(w), \tag{10}$$

where $\gcd_{l,m}(w)$ is taken to be a monic polynomial. We also define

$$d\,(l,\, m) = \max\left(\deg\left(x_{l,m}\right), \deg\left(z_{l,m}\right)\right) \geqslant 0, \tag{11}$$

$$\bar{d}\,(l,\, m) = \max\left(\deg\left(\bar{x}_{l,m}\right), \deg\left(\bar{z}_{l,m}\right)\right) \geqslant 0, \tag{12}$$

$$g\,(l,\, m) = \deg\left(\gcd_{l,m}\right). \tag{13}$$

We call $d\,(l,\, m)$ the *ambient degree* at the vertex whereas $\bar{d}\,(l,\, m)$ is the *reduced degree* after cancellation of the possible common factor $\gcd_{l,m}(w)$, whence

$$\bar{d}\,(l,\, m) = d\,(l,\, m) - g\,(l,\, m).$$

Cancellation of $\gcd_{l,m}(w)$ from $x_{l,m}(w)$ and $z_{l,m}$ corresponds to its cancellation in the numerator and denominator of the rational function $u_{l,m}(w)$.

As proven in ([14], theorem 10) (subject to an enabling conjecture), the lattice rules of table 1 with case I boundary conditions have a linear growth of $\bar{d}\,(l,\, m)$ along the principal diagonal. Furthermore, the ambient degrees $d\,(l,\, m)$ are the Delannoy numbers. For the equations in table 1, we find for $m \geqslant 0$

Table 3. List of common factors $A_{l+1,m+1}$ of $x_{l+1,m+1}$ and $z_{l+1,m+1}$ of the rules of table 2 —see also figure 2.

Q_1	$(\alpha\delta z_{l,m-1}z_{l-1,m} - \beta\delta z_{l,m-1}z_{l-1,m} + x_{l,m-1}z_{l-1,m} - x_{l-1,m}z_{l,m-1})$ $\times(\alpha\delta z_{l,m-1}z_{l-1,m} - \beta\delta z_{l,m-1}z_{l-1,m} - x_{l,m-1}z_{l-1,m} + x_{l-1,m}z_{l,m-1})$
Q_2	$z_{l-1,m}^2 x_{l,m-1}^2 - 2\,\alpha^2 z_{l-1,m}^2 z_{l,m-1}x_{l,m-1} + \alpha^4 z_{l-1,m}^2 z_{l,m-1}^2$ $-4\,\beta\,\alpha^3 z_{l-1,m}^2 z_{l,m-1}^2 + 4\,\beta\,\alpha z_{l,m-1}z_{l-1,m}^2 x_{l,m-1} + 6\,\beta^2\alpha^2 z_{l-1,m}^2 z_{l,m-1}^2$ $-4\,\beta^3\alpha\, z_{l,m-1}^2 z_{l-1,m}^2 - 2\,\beta^2 z_{l,m-1}z_{l-1,m}^2 x_{l,m-1} + \beta^4 z_{l-1,m}^2 z_{l,m-1}^2$ $-2\,z_{l-1,m}z_{l,m-1}x_{l-1,m}x_{l,m-1} + z_{l,m-1}^2 x_{l-1,m}^2$ $+4\,\beta\,\alpha\, z_{l,m-1}^2 z_{l-1,m}x_{l-1,m} - 2\,\alpha^2 z_{l,m-1}^2 z_{l-1,m}x_{l-1,m} - 2\,\beta^2 z_{l,m-1}^2 z_{l-1,m}x_{l-1,m}$
Q_3	$\alpha^4\delta^2\, z_{l-1,m}^2 z_{l,m-1}^2 - 4\,\beta\,\alpha^3 z_{l-1,m}z_{l,m-1}x_{l-1,m}x_{l,m-1} - 2\,\beta^2\alpha^2\delta^2 z_{l-1,m}^2 z_{l,m-1}^2$ $+4\,\beta^2\alpha^2 z_{l,m-1}^2 x_{l-1,m}^2 + 4\,\beta^2\alpha^2 z_{l-1,m}^2 x_{l,m-1}^2$ $-4\,\beta^3\alpha z_{l-1,m}z_{l,m-1}x_{l-1,m}x_{l,m-1} + \beta^4\delta^2 z_{l-1,m}^2 z_{l,m-1}^2$
H_1	$\left(x_{l-1,m}z_{l,m-1} - z_{l-1,m}x_{l,m-1}\right)^2$
H_2	$(x_{l,m-1}z_{l-1,m} - z_{l,m-1}x_{l-1,m} + (\alpha-\beta)z_{l,m-1}z_{l-1,m})(-x_{l,m-1}z_{l-1,m}$ $+z_{l,m-1}x_{l-1,m} + (\alpha-\beta)z_{l,m-1}z_{l-1,m})$
H_3	$(\alpha x_{l-1,m}z_{l,m-1} - \beta x_{l,m-1}z_{l-1,m})(\alpha z_{l-1,m}x_{l,m-1} - \beta z_{l,m-1}x_{l-1,m})$
KdV	$x_{l,m-1}^2\, x_{l-1,m}^2$

Table 4. Some features of $\gcd_{m,m}(w)$ for the lattice rules of table 2 with $\alpha = 2$ and $\beta = 5$: numbers of distinct linear factors and quadratic factors present as a function of $m \geqslant 0$.

Rule	# distinct linear factors	# distinct quadratic factors
$Q_1^{\delta=1}$	0, 0, 0, 4, 7, 9, 11, 13, 15, 17, 18, 20, ...	0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, ...
Q_2	0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 4, ...	0, 0, 0, 2, 4, 5, 7, 9,11, 13, 15, 16, ...
$Q_3^{\delta=1}$	0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ...	0, 0, 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, ...
H_1	0, 0, 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, ...	0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...
H_2	0, 0, 0, 4, 8, 12, 16, 20, 27, 30, 34, ...	0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, ...
H_3	0, 0, 0, 4, 8, 12, 16, 20, 24, 28,32, 36, ...	0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, ...
KdV	0, 0, 0, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...	0, 0, 0, 0, 3, 5, 7, 9, 11, 13, 15, 17,…

$$d(m,\,m) = 1,\,1,\,3,\,13,\,63,\,321,\,1683,\,8989,\,48639,\,265729,\,1462563,\,8097453,\,\ldots. \quad (14)$$

$$g(m,\,m) = 0,\,0,\,0,\,8,\,56,\,312,\,1672,\,8976,\,48624,\,265712,\,1462544,\,8097432,\,\ldots. \quad (15)$$

$$\bar{d}(m,\,m) = 1,\,1,\,3,\,5,\,7,\,9,\,11,\,13,\,15,\,17,\,19,\,21,\,\ldots. \quad (16)$$

One can see clearly that it is the *sufficiently exponential* growth of $g(m,\,m)$ that allows cancellations to result in the *linear growth* of $\bar{d}(l,\,m)$. As shown in [7, 14], the reason for this exponential growth is that the rules of table 2 apart from KdV have the factorization property that for any 2×2 lattice square $[l-1,\,l+1]\times[m-1,\,m+1]$, we obtain a common factor $A_{l+1,m+1}$ of $x_{l+1,m+1}$ and $z_{l+1,m+1}$ of (5)–(6) for *arbitrary* initial values at the 5 corner sites $\{(l-1,\,m-1),\,(l-1,\,m),\,(l-1,\,m+1),\,(l,\,m-1),\,(l+1,\,m-1)\}$—see figure 2 and

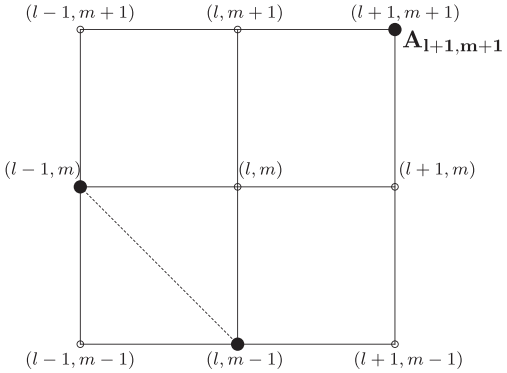

Figure 2. Some lattice equations produce a common factor $A_{l+1,m+1}$ of $x_{l+1,m+1}$ and $z_{l+1,m+1}$ over any 2 × 2 square that often only depends on x and z at the 2 sites $(l-1, m)$ and $(l, m-1)$.

table 3. (For the KdV equation, a similar factorization property holds but over any 3 × 3 lattice square.) For most equations, as indicated in the figure, the common factor $A_{l+1,m+1}$ can actually be written in terms of coordinates x and z at just the 2 sites $(l-1, m)$ and $(l, m-1)$. Crucially, as shown in table 3, $A_{l+1,m+1}$ is *quartic* in the x and z variables at these sites and this ensures enough growth of $g(m, m)$ (whereas a quadratic dependence will not—see below). Whilst it is well known that the rules of table 2 apart from KdV can be written as special cases of an equation Q_V of [16], table 3 highlights that $A_{l+1,m+1}$ can have a different number of factors depending on the rule itself. This will play a role later over finite fields.

In table 4, we take a closer look at $\gcd_{m,m}(w)$ to see how it factors for $0 \leqslant m \leqslant 11$ and one case of randomly generated case I boundary values. Obviously, for each m, the sum of the corresponding number of linear and quadratic factors is a lower bound for $g(m, m)$.

If we perturb the lattice rules of table 2, or choose an arbitrary multi-affine rule (1), we now find typically that $d(m, m) = \bar{d}(m, m)$ is given by the Delannoy sequence (14), i.e. there are *no* cancellations so $g(m, m) = 0$. We also observe that it takes much longer to iterate these rules from a computational viewpoint.

On the other hand, there are many equations that have the factorization property of figure 2 with $g(m, m)$ growing exponentially, but *insufficiently*, so that $\bar{d}_{m,m}$ also grows exponentially. For example, consider equation (30) of [7] (E30 in [14]):

$$uu_1 + u_2u_{12} + p_3(uu_{12} + u_1u_2) + \big(p_3 - 1\big)(uu_2 + u_1u_{12}) + r_4(u - u_2 + u_1 - u_{12}) + r_4^2 = 0. \tag{17}$$

Taking $p_3 = 3$, $r_4 = 2$ and random case I boundary values gives

$$d(m, m) = 1, 1, 3, 13, 63, 321, 1683, \ldots. \tag{18}$$

$$g(m, m) = 0, 0, 0, 4, 30, 194, 1178, \ldots. \tag{19}$$

$$\bar{d}(m, m) = 1, 1, 3, 9, 33, 127, 505, \ldots. \tag{20}$$

The number of distinct linear factors and quadratic factors in $\gcd_{m,m}(w)$ are given, respectively, as follows

0, 0, 0, 2, 4, 6, 8, … and 0, 0, 0, 1, 1, 1, 1….

The rule E30 has a common factor on a 2 × 2 lattice square of

$$A_{l+1,m+1} = x_{l-1,m}z_{l,m-1} + x_{l,m-1}z_{l-1,m} + r_4 z_{l,m-1}z_{l-1,m}. \tag{21}$$

The factor is *quadratic* in its arguments and E30 is proved to have exponential degree growth of $\bar{d}(m, m)$ in ([14], theorem 13).

3. Lattice rules over finite fields

We repeat the experiments of [14], summarized in the previous section, but now over finite fields $\mathbb{F}_p$ for p prime. We wish to see if we can detect a signature of polynomial degree growth, suggesting integrability, versus exponential degree growth. We desire the detection to be fast and decisive.

So we take case I (8) boundary values (mod p). We apply the lattice rules (mod p) to create polynomials denoted $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$ in $\mathbb{F}_p[w]$. We have

$$x^p_{l,m}(w) \equiv x_{l,m}(w) \pmod p, \tag{22}$$

$$z^p_{l,m}(w) \equiv z_{l,m}(w) \pmod p. \tag{23}$$

We divide and factorize polynomials now over the finite field so that

$$x^p_{l,m}(w) = \gcd^p_{l,m}(w)\, \bar{x}^p_{l,m}(w) \pmod p, \tag{24}$$

$$z^p_{l,m}(w) = \gcd^p_{l,m}(w)\, \bar{z}^p_{l,m}(w) \pmod p. \tag{25}$$

From (22)–(23) together with (9)–(10), we have that

$$\gcd_{l,m}(w) \pmod p \;\Big|\; \gcd^p_{l,m}(w) \tag{26}$$

When $\gcd^p_{l,m}(w)$ exceeds $\gcd_{l,m}(w) \pmod p$ in degree, it is because $\bar{x}_{l,m}(w) \pmod p$ and $\bar{z}_{l,m}(w) \pmod p$ share a common factor (mod p). We can define degrees in the finite field case analogous to (11)–(13), respectively: $d^p(l, m)$, $\bar{d}^p(l, m)$ and $g^p(l, m)$.

The following is the analogue of proposition 2 of [14] and is largely a consequence of (4).

Proposition 1. *For the projective lattice rules over* $\mathbb{F}_p$*, we have the following:*

1. $0 \leqslant d^p_{l+1,m+1} \leqslant d^p_{l,m} + d^p_{l+1,m} + d^p_{l,m+1}$.
2. *If* $x^p_{l,m}(w) = z^p_{l,m}(w) \equiv 0 \pmod p$*, then* $x^p_{l+i,m+j}(w) = z^p_{l+i,m+j}(w) \equiv 0 \pmod p$*, for all integers* $i, j \geqslant 1$.
3. $\gcd^p_{l,m}(w)\ \gcd^p_{l+1,m}(w)\ \gcd^p_{l,m+1}(w) \mid \gcd^p_{l+1,m+1}(w)$.

Working (mod p) as described above is much faster computationally and gives degree sequences similar to working over the integers (albeit that $g^p(l, m)$ can exceed $g(l, m)$ because of (26). Nevertheless, it is precisely the size and growth of the degrees that prevents us going too far from the origin, i.e. the size of the square we can compute over in the first quadrant is often small.

One way to obviate this problem is to cap the degrees of polynomials by using the identity known as Fermat's little theorem:

$$w^p = w \pmod p. \tag{27}$$

At each application of the lattice rule, we can apply this identity to represent $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$ differently, as polynomials with degree not exceeding $p-1$. As a result of this, we are able to analyse the behaviour of a given rule in a much larger box. Although this changes their appearance as polynomials, it preserves their values $\pmod p$, and in particular their zeroes. We introduce

$$\text{roots}^p_{l,m} := \left\{ w\text{: } x^p_{l,m}(w) = z^p_{l,m}(w) = 0\big(\bmod \text{p}\big)\right\}. \tag{28}$$

Each $w^* \in \text{roots}^p_{l,m}$ implies the existence of a common linear factor $(w - w^*)$ dividing $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$, and hence dividing $\gcd^p_{l,m}(w)$. Conversely, each distinct zero $\pmod p$ of $\gcd^p_{l,m}(w)$ provides an element of $\text{roots}^p_{l,m}$.

We will use $\text{roots}^p_{l,m}$ as our analogue of $\gcd_{l,m}$ of the previous section to measure 'commonality' between $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$. Analogous to the degree $g(l, m)$, we take the cardinality $\#\text{roots}^p_{l,m}$ to measure growth in this commonality. Clearly $\#\text{roots}^p_{l,m}$ is integer-valued and satisfies $0 \leqslant \#\text{roots}^p_{l,m} \leqslant \text{p}$. When the upper limit is achieved, we have

$$w^p - w = \prod_{i=0}^{p-1} (w - i) | \gcd^p_{l,m}(w). \tag{29}$$

Analogous to part 3 of proposition 1 we have the readily-verified.

Proposition 2. *For the projective lattice rules over the finite field* $\mathbb{F}^p$*, we have*

$$\text{roots}^p_{l,m} \bigcup \text{roots}^p_{l+1,m} \bigcup \text{roots}^p_{l,m+1} \subseteq \text{roots}^p_{l+1,m+1}. \tag{30}$$

This implies that the roots at (l, m), $(l+1, m)$ *and* $(l, m+1)$ *are inherited at* $(l+1, m+1)$ *and therefore,*

$$\#\text{roots}^p_{l+1,m+1} \geqslant \max\left\{\#\text{roots}^p_{l,m}, \#\text{roots}^p_{l+1,m}, \#\text{roots}^p_{l,m+1}\right\}. \tag{31}$$

This shows that the non-negative double-index integer sequence $(\#\text{roots}^p_{l,m})$ is non-decreasing as we move to the right and/or upwards on the lattice. We now report our investigations of this bounded sequence along the diagonal $l = m$ to see if and how it discriminates between integrable and non-integrable lattice rules (for which lattice entropy would be a discriminator). We make a remark about the more general non-diagonal behaviour of $\#\text{roots}^p_{l,m}$ in our concluding remarks.

Definition 3. We will say that the non-decreasing sequence

$$r^p(m) := \#\text{roots}^p_{m,m} \tag{32}$$

saturates at $m = m^*(p)$ if $m^*(p)$ is the smallest value of m achieving $r^p(m^*) = p$. We call $m^*(p)$ the *saturation point*.

If saturation occurs, it follows from (29) that $w^p - w | \gcd^p_{m,m}(w)$. It follows from proposition 2 that $r^p(m) = p$ for $m \geqslant m^*(p)$.

We have performed extensive numerical experiments in Maple on all the lattice rules of table 2 plus various perturbations of these rules. They have revealed the following:

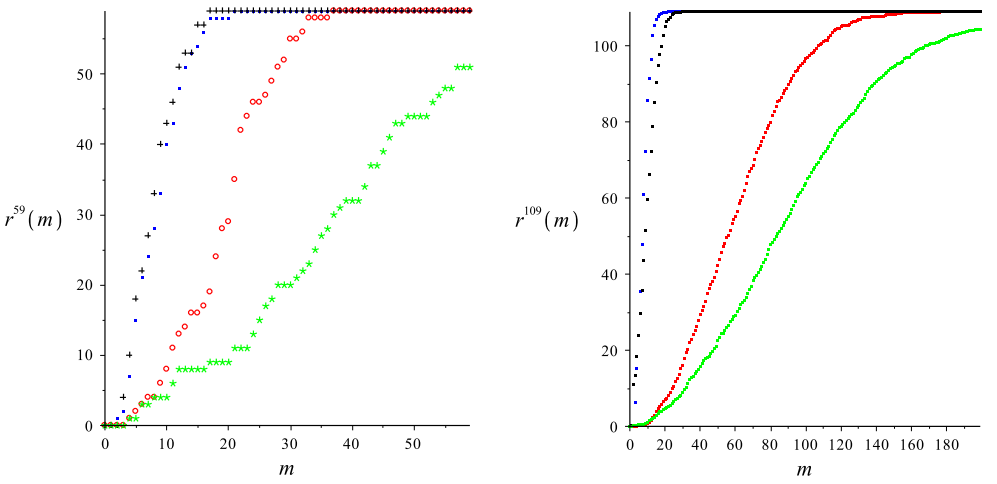

Figure 3. Plots of averaged $r^p(m)$ of (32) for two primes and various rules, where each curve is an average of 10 random case I boundary value simulations. Left: prime $p = 59$ for KdV (blue) of table 2 and its perturbation (red) together with E30 (black) of (17) and its perturbation (green). Right: prime $p = 109$ for Q_1 (blue) and its perturbation (red) together with Q_2 (black) and its perturbation (green).

Observation 4.

(1) Saturation always occurs for the sequences $r^p(m)$ derived from the integrable lattice rules with $m^*(p) \ll p$ and for many of their perturbations in the range of m tested. The saturation point $m^*(p)$ for an integrable lattice rule is much lower than the corresponding saturation point for its perturbations, if saturation does occur. The growth of $r^p(m)$ is markedly faster for integrable rules as compared to their perturbations.
(2) The first m such that $r^p(m) > 0$ is much smaller for integrable rules than for their perturbations.

We illustrate these observations in figure 3. With reference to table 1, and using notation (2), the perturbations of KdV and E30 used are (7) with $r = 1$ and E30 $+ u = 0$, respectively. The perturbations of Q_1 and Q_2 used are $Q_1 + u = 0$ and $Q_2 + uu_1u_{12} = 0$, respectively. Observation 4 is based on many simulations of the equations of table 2 for primes of the order of a few hundred. But the observed behaviour can already be seen for primes well below one hundred. More experimental data are presented in the next section where the veracity of observation 4 is supported by its agreement with two models that are constructed to analyse and explain the growth of roots. The models allow (asymptotic) estimates of $m^*(p)$ for lattice equations as a function of p and give a form for $r^p(m)$.

We already see from figure 3 that E30 behaves similarly to KdV, despite the fact that $\bar{d}(m, m)$ has exponential growth in the former case and linear growth in the latter case. So $r^p(m)$ has not detected a difference between integrability and non-integrability. However, the perturbations of the equations have markedly different behaviour. We can explain this by the presence of the factors $A_{l+1,m+1}$ of E30 and KdV over any 2×2 lattice square, which leads to more common roots than an arbitrary lattice equation where such factorization would not be expected. In the latter case, even though one expects there to be no non-trivial $\gcd_{l,m}(w)$ at any site when factoring over $\mathbb{Z}[w]$, roots do arise over $\mathbb{F}_p$ through a random process.

4. Models that explain the observations

In this section, we present two models that predict the behaviour of $r^p(m)$ of (32) for integrable rules and their non-integrable perturbations. Moreover, we will bring our models and data for both integrable rules and their perturbations to a universal curve. The first model is based on a Bernoulli trials process and the second model is based on several combinatorial arguments.

Both models make use of:

Fact: Over $\mathbb{F}_p$, a polynomial has on average 1 root, independent of its degree [10].

Assumption. On average, one spontaneous common root of $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$ over $\mathbb{F}_p$ appears every T vertices of the lattice (spontaneous refers to the fact that the root is not inherited via proposition 2). T can be found by trial and error to fit our data but essentially it depends on common factors of $x_{l,m}(w)$ and $z_{l,m}(w)$, e.g.

- $T = 1$ if these have one common factor over $\mathbb{Z}$;
- $T = \frac{1}{2}$ if two common factors over $\mathbb{Z}$;
- $T = \frac{p+1}{2}$ or $T = p$ if there are no common factors over $\mathbb{Z}$.

We assume that T is essentially independent of vertex, i.e. it does not depend on lattice sites (l, m). However, T can depend on p. An alternative description of T is that there are $1/T$ spontaneous common roots expected at a vertex.

4.1. Model 1

We present a model that predicts saturation points of integrable rules and their perturbations. Suppose over a lattice rectangle of M vertices, we assume that there are j distinct roots already having appeared at the top right corner. The following process that we consider is described as follows. We add new vertices to these M vertices and we keep doing this until we see a root which is different from those j roots. This root is called a *new root*. Each vertex has two possible outcomes namely 'success' and 'failure' in a Bernoulli trials process corresponding to providing a new root or not providing a new root. It is noted that failure means that there is no root or the additional roots are not new. Therefore, one can regard this process as a Bernoulli trials process.

The probability of a success at any added vertex is $(p - j)/(Tp)$. Therefore, the expected number of vertices that we need to add until the first new root is $\frac{1}{(p-j)/(Tp)} = \frac{Tp}{p-j}$, see [5]. Hence the expected numbers of vertices to see i roots is

$$F(T, p, i) := \frac{Tp}{p} + \frac{Tp}{p-1} + \ldots + \frac{Tp}{p-i+1} = Tp\left(\sum_{j=0}^{i-1}\frac{1}{p-j}\right). \tag{33}$$

The square root of the number of vertices is our effective distance coordinate m from the origin, subject to an adjustment relating to how far in from the boundary do vertices begin to contribute roots.

For integrable rules, it is likely that there is no common factor between $x_{l,m}$ and $z_{l,m}$ if $l < 2$ or $m < 2$ or $l = m = 2$. Hence we assume that the starting points for common roots for integrable rules are at (2, 3) and (3, 2). Along the diagonal, at the point (i, i), the number of vertices in the square (0, 0), $(0, i)$, (i, i), $(i, 0)$ that contribute some roots is $(i - 1)^2 - 1$. Therefore, the expected saturation point is

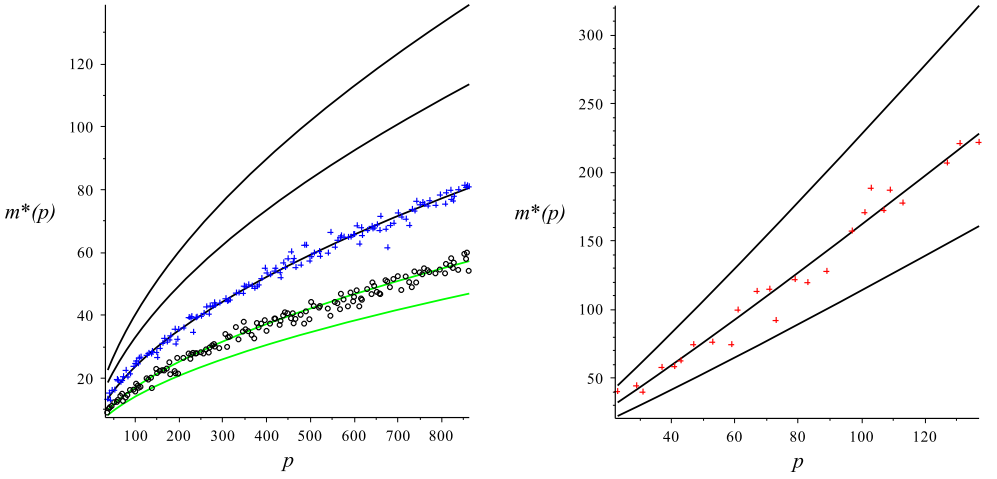

Figure 4. Left: saturation points $m^*(p)$ of definition 3. Each cross and circle show the averaged saturation points of H_1 and H_3 respectively. The solid curves are (34) for $T = 1/3,\ 1/2,\ 1,\ 2,\ 3$ (bottom to top). Right: saturation points of the perturbation $Q_3 + u = 0$. The cross shows the average saturation points, whereas the solid curves are (35) with $T = p/4,\ (p+1)/2,\ p$ (bottom to top).

$$m^*(p) := \sqrt{F(T, p, p) + 1} + 1.$$

By using the estimation of the harmonic series, we predict that

$$m^*(p) \approx \sqrt{Tp}\sqrt{\ln p + \gamma + 1/(Tp)} + 1, \tag{34}$$

where $\gamma = .5772156649$ is Euler's constant.

For a general lattice rule (1) with no non-trivial $\gcd_{l,m}$, our boundary values do not give us common factors on the boundary. We treat $x^p_{l,m}$ and $z^p_{l,m}$ or $\bar{x}_{l,m}$ and $\bar{z}_{l,m}$, where $l,\ m \geqslant 1$ as random polynomials with certain degrees. We then can assume that the starting point is $(1,\ 1)$. Thus, the expected saturation point for a general non-integrable lattice rule is

$$m^*(p) := \sqrt{F(T, p, p)} \approx \sqrt{Tp}\sqrt{\ln p + \gamma}. \tag{35}$$

In figure 4, we plot averaged saturation points for a sequence of primes (averaged from 10 sets of boundary values for integrable rules or 5 sets of boundary values for the non-integrable rules) and the corresponding expected saturation points from the model with various T values. For integrable rules (left) we take $p = 37,\ 41,\ \ldots,\ 863$ and for non-integrable rules we take $p = 23,\ 29,\ \ldots,\ 113$.

Figure 4 shows that the data for H_1 and H_3 fit quite well with $T = 1$ and $T = 1/2$ respectively. This can be understood through their different factorization pattern at the point $(2,\ 2)$ for arbitrary initial values. Given case I boundary values, table 3 shows that the common factor of H_3 can be written as a product of two different polynomials in w. Therefore over $\mathbb{F}_p$, the fact above leads to the expectation of two common roots for $x^p_{l,m}$ and $z^p_{l,m}$, i.e. $T = 1/2$. This also applies to H_2, Q_1 and KdV. For other equations such as H_1, the commmon factor contributes one common root for $x^p_{l,m}$ and $z^p_{l,m}$, so $T = 1$ for H_1 as well as Q_2 and Q_3.

For non-integrable rules without any obvious common factor $A_{l+1,m+1}$, common roots appear as we work over finite fields and treat $x^p_{l,m}$ and $z^p_{l,m}$ as random polynomials over $\mathbb{F}_p[w]$. Given these two polynomials with each of them having one expected root in the set

$\{0, 1, \ldots, p-1\}$, there are $p(p-1)/2 + p = p(p+1)/2$ possible choices of pairing the two roots and p of these pairings correspond to each having the same root. Thus, the probability of having one common root at a vertex is $\frac{p}{p(p+1)/2} = \frac{2}{p+1}$, corresponding to $T = (p+1)/2$. On the other hand, the probability of having a vanishing resultant of two polynomials over $\mathbb{F}_p[x]$ is $1/p$, see [12]. That means the probability of two random polynomials having a common factor is $1/p$, corresponding to $T = p$. Again, on average we take an assumption that this common factor has one root in $\mathbb{F}_p$. The right-hand plot of figure 4 supports this analysis.

Finally, using (33), we can build a simple model ('the R model') that approximates $r^p(m)$. We denote $R_f^p(m)$ and $R_{nf}^p(m)$ as the expected number of common roots between $z_{m,m}^p$ and $x_{m,m}^p$ for rules with *factorization* (starting at (2, 2)) and with *no factorization*, respectively. It is noted that in the first $m \times m$ box, there are $(m-1)^2 - 1$ or m^2 vertices that contribute some roots at each vertex. We define

$$R_f^p(m) = \begin{cases} p & \text{if } m \geqslant \sqrt{F(T,p,p)+1} + 1 \\ \dfrac{(m-1)^2-1}{T} & \\ & \text{if } 2 \leqslant m < \sqrt{F(T,p,1)+1} + 1 = \sqrt{T+1} + 1 \\ 0 & \text{if } m = 0 \text{ or } m = 1 \\ j + \dfrac{\Big((m-1)^2 - 1 - F(T,p,j)\Big)(p-j)}{Tp} & \\ & \text{if } \sqrt{F(T,p,j)+1} + 1 \leqslant m < \sqrt{F(T,p,j+1)+1} + 1 \end{cases} \tag{36}$$

and

$$R_{nf}^p(m) = \begin{cases} p & \text{if } m \geqslant \sqrt{F(T,p,p)} \\ \dfrac{m^2}{T} & \text{if } m < \sqrt{F(T,p,1)} = \sqrt{T} \\ j + \dfrac{\Big(m^2 - F(T,p,j)\Big)(p-j)}{Tp} & \text{if } \sqrt{F(T,p,j)} \leqslant m < \sqrt{F(T,p,j+1)}\,. \end{cases} \tag{37}$$

We will compare the R models and data for $r^p(m)$ in the next section.

4.2. Model 2

In this section, we present another model ('the L model') that predicts the root curve $r^p(m)$ of definition 3. The model uses several combinatorial facts, given in the appendix.

We denote by $L_f^p(m)$ and $L_{nf}^p(m)$ the number of common roots that we expect to see at the lattice vertex (m, m) for integrable rules and their perturbations, respectively. It is clear that $L_f^p(m) = 0$ for $m \leqslant 2$. For lattice rules with a factorization property at (2, 2) and for KdV, the $L_f^p(m)$ roots at the point (m, m) with $m \geqslant 2$ are inherited at the point $(m+1, m+1)$. There are then an extra $(2m-1)$ vertices that, by our model assumption above at the beginning of the section, contribute an additional $(2m-1)/T$ roots to the point $(m+1, m+1)$. Of these, the expected number of distinct roots is

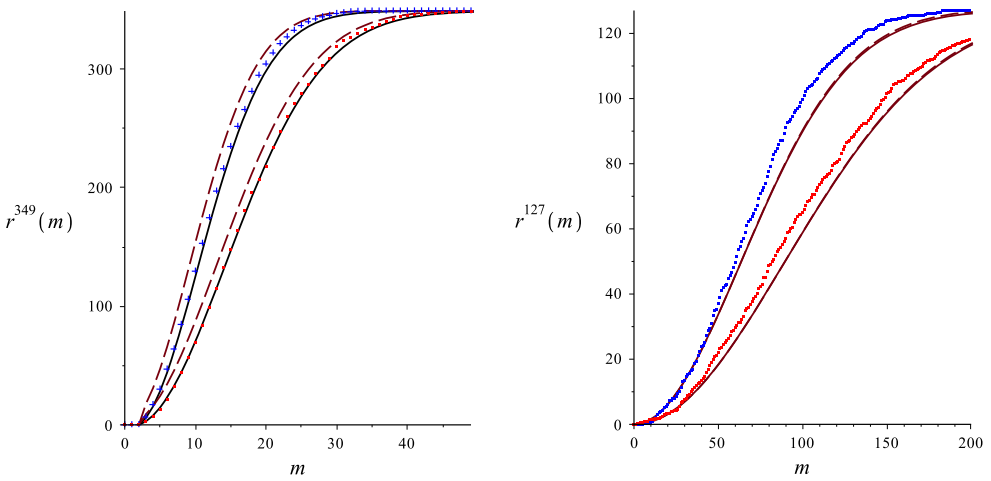

Figure 5. Left: plots of averaged $r^p(m)$ of (32) for $p = 349$ and Q_1 (cross) and Q_2 (circle) (averaged over ten sets of boundary values for both cases). The dashed curve and the solid curves represent, respectively, the $R_f^p(m)$ and $L_f^p(m)$ models for $T = 1/2$ (upper curves) and $T = 1$ (lower curves). Right: Plots of averaged $r^p(m)$ of (32) for $p = 127$ for perturbations of Q_1 (higher point curve) and Q_2 (lower point curve). The cross and the point represent the $L_{nf}^p(m)$ and $R_{nf}^p(m)$ model. The higher curves represent our models with $T = (p + 1)/2$, the lower ones show our models with $T = p$.

$$\frac{p(2m-1)/T}{p-1+(2m-1)/T}.$$

Therefore the expected number of new common roots that appear at $(m + 1, m + 1)$ is

$$\frac{p(2m-1)/T}{p-1+(2m-1)/T}\frac{\left(p-L_f^p(m)\right)}{p}.$$

Therefore we build the following model

$$L_f^p(m) = 0, \qquad \text{if } m \leqslant 2,$$

$$L_f^p(m+1) = L_f^p(m) + \frac{p(2m-1)/T}{p-1+(2m-1)/T}\frac{\left(p-L_f^p(m)\right)}{p} \quad \text{if } m \geqslant 2.$$

Similarly, the model for lattice rules without factorization properties is given by

$$L_{nf}^p(1) = 1/T,$$

$$L_{nf}^p(m+1) = L_{nf}^p(m) + \frac{p(2m+1)/T}{p-1+(2m+1)/T}\frac{\left(p-L_{nf}^p(m)\right)}{p} \qquad \text{if } m \geqslant 1.$$

Figure 5 compares the expected number of roots $R^p(m)$, $L^p(m)$ and the average number of roots from some rules.

4.3. The universal curve

We now show that both integrable and non-integrable models can be brought to a universal curve via a T-dependent scaling. Recall that in the R model, it requires at least $F(T, p, m)$

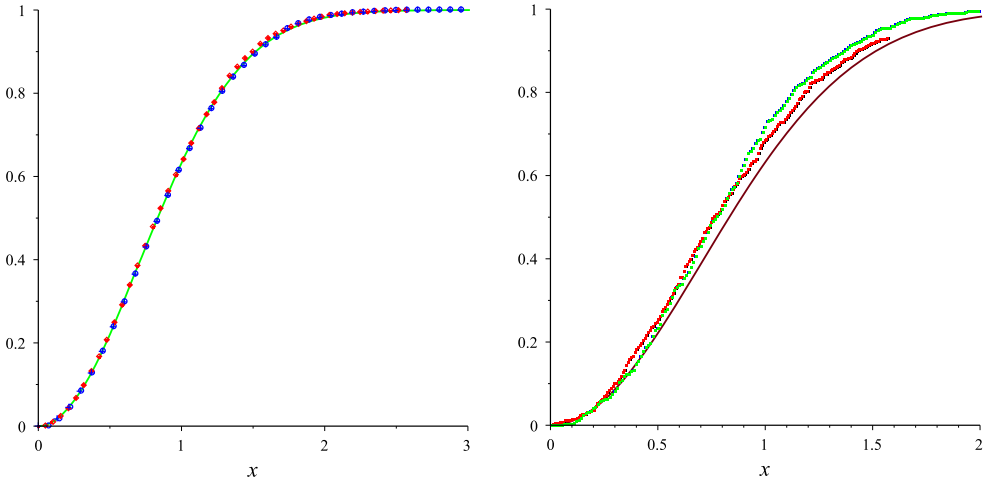

Figure 6. Left: the green represents the universal curve $y = 1 - e^{-x^2}$. The diamond (red) and point (red) represent L and R models of average data of Q_2, Q_3 and Q_V respectively. The circle (blue) and cross (blue) represent L and R scalings of average data of H_1, H_2, H_3 and Q_1 respectively. The data are obtained for prime $p = 349$. Right: the curve represents the universal curve $y = 1 - e^{-x^2}$. The blue and green represent R and L scalings with $T = (p + 1)/2$ of average data of $Q_1 + u = 0$ respectively. The red and black represent R and L scalings of average data of $Q_2 + uu_1u_{12} = 0$. The data are obtained for prime $p = 127$.

vertices from the starting point to get m roots. Using the approximation of the harmonic series, we obtain

$$\frac{F(T, p, m)}{Tp} \approx \ln p - \ln(p - m) = \ln \frac{p}{p - m} := x^2.$$

This gives us $y = m/p = 1 - e^{-x^2}$. Therefore, for integrable rules we can do the following scaling $x = \sqrt{\frac{(m-1)^2 - 1}{Tp}}$ and $y = r^p(m)/p$. For non-integrable rules with no common factor, one can take $x = m/\sqrt{Tp}$ and $y = r^p(m)/p$. For the L model, let $a_m = 1 - L^p(m)/p$. For integrable rules, we have $a_2 = 1$ and

$$a_{m+1} = \frac{p - 1}{p - 1 + \frac{2m-1}{T}} a_m = \frac{a_m}{1 + \frac{(2m-1)}{T(p-1)}},$$

for $m \geqslant 2$. Thus $a_m > 0$ and

$$\ln a_m = -\ln\left(1 + \frac{2m - 3}{T(p - 1)}\right) - \ln\left(1 + \frac{2m - 5}{T(p - 1)}\right) - \ldots - \ln\left(1 + \frac{1}{T(p - 1)}\right).$$

Using the first order Taylor expansion of ln, we have

$$\ln a_m \approx -\sum_{j=1}^{m-1}\left(\frac{2j - 1}{T(p - 1)}\right) = -\frac{(m - 1)^2}{T(p - 1)}.$$

Similarly, for the cases of no common factor, we have $\ln a_m = -m^2/(T(p-1))$. Therefore, for integrable cases we can use the following scaling $x = (m-1)/\sqrt{T(p-1)}$ and $y = r^p(m)/p$. For non-factor cases, we take $x = m/\sqrt{T(p-1)}$ and $y = r^p(m)/p$.

We conclude that with suitable scaling, both integrable and non-integrable cases lead to the universal model $y = 1 - e^{-x^2}$. We compare the universal curve and average data for both cases in figure 6.

One can see clearly that the data for integrable rules fit very well with the universal curve. There is a small gap between the data for perturbations of Q_1 and Q_2 and the universal curve. This might be because the values for T for these perturbations varied between $(p+1)/2$ and p. We also remark that the universal curve $D(x) = 1 - e^{-x^2}$ can be regarded as the proportion of $\mathbb{F}_p$ that appear as roots at the (scaled) distance x along the diagonal from the origin. $D(x)$ is a cumulative distribution function [5].

5. Embedding integrable equations

In the previous two sections, we have shown that over finite fields, we can get a suggestion of integrability of a lattice rule but it is not definitive as our diagnostic is really related to common factorization properties of a lattice rule in projective coordinates and non-integrable rules can still exhibit such factorization.

In this section, we want to illustrate the usefulness and economy of searching parameter space over finite fields (which is necessarily finite) so as to find equations of interest (see also [15] for an illustration of this). In particular, we will add more general terms to some known integrable lattice equations to see if the equations can be embedded in more general integrable forms. It is important to note that all the equations in the ABS list except Q_4 and equations given by Hietarinta and Viallet in [7] do not have any cubic terms. Therefore, one question that arises here is if one can add cubic terms to these equations. The key point for this search is using a factorization property over $\mathbb{Z}$ restricted to finite fields. Therefore, we propose the following test:

- add cubic terms in the original integrable equations with free coefficients a_1, a_2, a_3, a_4 and then write the new rule in projective coordinates.
- Impose case I (8) boundary values along axes in the first quadrant over $\mathbb{F}_p$.
- Calculate $x^p_{l,m}(w)$ and $z^p_{l,m}(w)$ for l, $m \leqslant 3$.
- Require that $\deg(\gcd^p_{3,3}(w)) \geqslant 8$ and then record coefficient vectors (a_1, a_2, a_3, a_4) that satisfy this requirement.
- Generate different sets of boundary values and run again.
- Intersect the sets of parameters (a_1, a_2, a_3, a_4) to get common patterns, also over different primes.

The origin of the test condition $\deg(\gcd^p_{3,3}(w)) \geqslant 8$ is that $\deg(\gcd_{3,3}(w)) \geqslant 8$ was shown in [14] to hold for many integrable lattice equations over $\mathbb{Z}$.

For example, we took the equation E_{21} in the Hietarinta–Viallet list

$$\alpha\left(u_{l,m}u_{l,m+1} + u_{l+1,m}u_{l+1,m+1}\right) + \beta\left(u_{l,m}u_{l+1,m} + u_{l,m+1}u_{l+1,m+1}\right) + \gamma = 0,$$

where α, β and γ are constant. It is noted that this equation is a more general form of the discrete pKdV or H_1 equation in the ABS list. We added all the cubic terms in this equation. The new equation is given as follows

$$a_1u_{l,m}u_{l+1,m}u_{l,m+1} + a_2u_{l,m}u_{l+1,m}u_{l+1,m+1} + a_3u_{l,m}u_{l,m+1}u_{l+1,m+1} + a_4u_{l+1,m}u_{l,m+1}u_{l+1,m+1} + \alpha\left(u_{l,m}u_{l,m+1} + u_{l+1,m}u_{l+1,m+1}\right) + \beta\left(u_{l,m}u_{l+1,m} + u_{l,m+1}u_{l+1,m+1}\right) + \gamma = 0. \tag{38}$$

We took fixed values of α, β and γ. We then recorded all the values of a_1, a_2, a_3, a_4 in $\mathbb{F}_p$ that passed the factorization test. For example we take $\alpha = 1, \beta = 2$ and $\gamma = 3$. Working in $\mathbb{F}_7[w]$, and using 6 different sets of boundary values, we get the set of 'potential' $[a_1, a_2, a_3, a_4]$ as follows

$$\{[1, 1, 1, 1], \quad [2, 1, 3, 0], \quad [2, 2, 2, 2], \quad [3, 3, 3, 3], \quad [4, 1, 1, 4] \quad [5, 5, 5, 5], \quad [6, 6, 6, 6]\}.$$

For $p = 11$, we obtain the following sets

$$\{[1, 1, 1, 1], \quad [2, 2, 2, 2], \quad [3, 3, 3, 3], \quad [5, 5, 5, 5], \quad [6, 6, 6, 6], \quad [8, 8, 8, 8]\}.$$

The results suggest that $a_2 = a_3 = a_4 = a_1 \pmod p$. Moreover, we also note that if we do the test for larger prime numbers p and $0 \leqslant a_1, a_2, a_3, a_4 \leqslant q$, where $q \ll p$, we are likely to get $a_2 = a_3 = a_4 = a_1 = i \pmod p$ for all $0 \leqslant i \leqslant q$. Therefore the only choice for adding cubic terms to E_{21} appears to be $a_2 = a_3 = a_4 = a_1$, which turns out to be a special case of the Q_V equation of [16].

We have done this test similarly for ABS equations and other equations given in [7]. We take $p = 7, 11$ and the number of boundary value sets that we used is 6. For ABS equations we have found that $a_1 = a_2 = a_3 = a_4 \pmod p$. It suggests that we can add cubic terms to ABS equations (except for Q_4), however these new equations are just special cases of Q_V of [16]. For equations in [7], we have obtained $a_1 = a_2 = a_3 = a_4 = 0$ for many cases. Moreover, it would be worth mentioning that by using some special parameter choices, we identified the following equations

$$\alpha u_{l,m}u_{l+1,m+1}\left(u_{l+1,m} + u_{l,m+1}\right) + \left(u_{l,m} + u_{l,m+1}\right) \times \left(u_{l+1,m} + u_{l+1,m+1}\right) + \beta\left(u_{l+1,m} + u_{l,m+1}\right) = 0, \tag{39}$$

$$\alpha u_{l,m}u_{l+1,m+1}\left(u_{l+1,m} - u_{l,m+1}\right) + \left(u_{l,m} - u_{l,m+1}\right) \times \left(u_{l+1,m} - u_{l+1,m+1}\right) + \beta\left(u_{l+1,m} - u_{l,m+1}\right) = 0, \tag{40}$$

$$\alpha u_{l+1,m}u_{l,m+1}\left(u_{l,m} - u_{l+1,m+1}\right) + \beta u_{l,m}u_{l+1,m+1}\left(u_{l+1,m} - u_{l,m+1}\right) + \left(u_{l,m} - u_{l,m+1}\right)\left(u_{l+1,m} - u_{l+1,m+1}\right) + \alpha\left(u_{l,m} - u_{l+1,m+1}\right) + \beta\left(u_{l+1,m} - u_{l,m+1}\right) = 0, \tag{41}$$

$$\alpha u_{l,m}u_{l+1,m+1}(u_{l+1,m} - u_{l,m+1}) + \beta u_{l+1,m}u_{l,m+1} \times (u_{l,m} - u_{l+1,m+1}) + \alpha(u_{l+1,m} - u_{l,m+1}) + (u_{l,m} - u_{l+1,m})(u_{l,m+1} - u_{l+1,m+1}) + \gamma(u_{l,m} - u_{l+1,m+1}) \times (u_{l+1,m} - u_{l,m+1}) + \beta(u_{l,m} - u_{l+1,m+1}) = 0. \tag{42}$$

Equations (39) and (40) can be seen as general forms of equation E_{18} in the Hietarinta–Viallet list when $p_3 = \pm 1$. The equations (41) and (42) were derived from equations (19) and (26) in [7], where the free coefficient is 0. We have checked the Diophantine integrability [6] and factorization at the point (2, 2) of these equations (see our earlier discussion in section 2.2

and figure 2). Hence ([14], theorem 10) suggests that these equations are integrable in the sense of vanishing entropy. Equations (39) and (40) can be brought to 'normal forms' via respective transformations $u \mapsto B(u-1)/(A(u+1))$ and $u \mapsto \mathrm{i}B(u-1)/(A(u+1))$, where $A^2 = \alpha$ and $B^2 = \beta$. The term 'normal form' refers to multi-affine equations without cubic and linear terms. Moreover, the normal form of equation (40) is a special case of equation (16) given in [7], however equation (39) seems to be new. Equations (41) and (42) can be transformed to the 'normal form' by using this transformation $u \mapsto -\mathrm{i}(u+1)/u$, $\alpha \mapsto \mathrm{i}\alpha$, $\beta \mapsto \mathrm{i}\beta$. These equations can also be transformed to equation (16) given in [7] via the transformation $u = -(u+1)/2$.

Moreover, by loosening our degree requirement above to $\deg(\gcd(x_{3,3}(w), z_{3,3}(w))) \geqslant 1$ or $\deg(\gcd(x_{3,3}(w), z_{3,3}(w))) = -\infty$, we have found that the following equations

$$\alpha u_{l,m}u_{l+1,m+1}\left(u_{l+1,m} - u_{l,m+1}\right) + \beta\left(u_{l,m} - u_{l+1,m+1}\right)\left(u_{l+1,m} - u_{l,m+1}\right) + \gamma = 0,$$

$$\alpha u_{l+1,m}u_{l,m+1}\left(u_{l,m} - u_{l+1,m+1}\right) + \beta\left(u_{l,m} - u_{l+1,m+1}\right)\left(u_{l+1,m} - u_{l,m+1}\right) + \gamma = 0,$$

which can be seen as extensions of H_1. These equations have factorization at the point (2, 2) but their degrees grow exponentially. Actually, these non-integrable equations also fit in the framework of our paper [14]. We also note that by adding cubic terms in the linear equation $\beta(u_{l+1,m} + u_{l,m+1}) + \gamma = 0$ and using the looser degree requirement, we obtain the following equation

$$\alpha u_{l,m}u_{l+1,m+1}\left(u_{l+1,m} + u_{l,m+1}\right) + \beta\left(u_{l+1,m} + u_{l,m+1}\right) + \gamma = 0.$$

Taking $\alpha = 1$, $\beta = 0$, $\gamma = 1$, one gets the new equation introduced recently in [11].

6. Concluding remarks

We have studied lattice equations and their perturbations over finite fields. Using the fact that integrable equations have a factorization property, we have been able to distinguish integrable equations and their non-integrable perturbations without common factors over $\mathbb{F}_p$. The differences between integrable equations and the non-integrable ones that we can see clearly are the growth and the saturation point of the root curve $r^p(m)$ of (32). However, it is important to note that we cannot necessarily separate integrable equations and non-integrable equations with the factorization property with this diagnostic. The analysis of sections 3 and 4 raises the question of the general value $\#\mathrm{roots}^p_{l,m}$ of the root function (28) in the first quadrant and its saturation behaviour other than on the main diagonal. We have made some first investigations of this and found a saturation contour for some integrable rules, shaped like a branch of a hyperbola with closest point to the origin along the diagonal. An extension of our model of section 4 gives some hope to modelling the experimental results and we hope to report on this elsewhere.

In section 5, we have used the factorization test at the vertex (3, 3) of lattice equations to successfully add cubic terms to some equations to obtain a new integrable equation (39), in the sense of having vanishing entropy. It is important to note that the (1, 1)-reduction of equation (39) gives us a map with period 4. This equation can be brought to a normal form, i.e. there are only even terms in this equation via a Möbius transformation. Therefore, it would be worth studying this equation in more detail.

Acknowledgments

This research was supported by the Australian Research Council. Both authors acknowledge the generous hospitality of the Department of Mathematics, Universitat Autonoma de Barcelona, where some of this research was done. Additionally, JAGR acknowledges financial support via the Sabbatical Fellowship SAB2011-0025 from the Spanish Ministry of Science. We also would like to thank Joshua Capel for some useful suggestions.

Appendix

We present more details about the combinatorial results used to create the model of section 4.2.

Problem 1

Given p numbers 0, 1, 2, …, $p-1$ and N boxes, fill the boxes with these numbers such that each box contains one number. How many ways are there of filling these boxes with the numbers such that it is not necessary to use all the numbers?

Answer: We denote x_i the number of boxes that contains i. We note that $x_0 + x_1 + \ldots + x_{p-1} = N$. We then group boxes that contains numbers i and then put the number x_i after these boxes. We omit the last number x_{p-1} as we can write $x_{p-1} = N - \left(x_0 + x_1 + \ldots + x_{p-2}\right)$. In the case, if we see two number x_i and x_{i+1} next to each other, this means that the number $i+1$ does not appear in any box. We draw N stars to represent the boxes and draw $p-1$ bars to represents numbers x_0, x_1, …, x_{p-2}. To solve our problem, we need to reorder the stars and bars by choosing $p-1$ spots in $N+p-1$ spots for the bars. This gives us $\binom{N+p-1}{p-1} = \binom{N+p-1}{N}$ ways.

Problem 2

What is the probability of seeing j distinct numbers in N boxes?

Answer: Given N boxes and and number j, we first choose j boxes with j numbers. The number of ways of filling $N-j$ boxes with j numbers is $\binom{j+N-j-1}{N-j} = \binom{N-1}{N-j}$. The number of ways of choosing j distinct numbers from p numbers is $\binom{p}{j}$. Therefore, the probability of seeing j distinct numbers is $\binom{p}{j}\binom{N-1}{N-j} \Big/ \binom{p+N-1}{N}$.

Problem 3

How many distinct numbers do we expect to see in N boxes?

Answer: The expected number of distinct numbers in N boxes is

$$\sum_{i=j}^{p} \frac{j\binom{p}{j}\binom{N-1}{N-j}}{\binom{p+N-1}{N}} = \frac{Np}{N+p-1}.$$

Problem 4

Given a set B with l distinct numbers in the set $0, 1, \ldots, p-1$, we choose n distinct numbers from p distinct numbers. How many distinct numbers which do not belong to B are expected?

Answer: The number of ways of choosing n numbers from p numbers is $\binom{p}{n}$. The number of ways of choosing i numbers which do not belong to B and $n-i$ numbers that are in B is $\binom{p-l}{i}\binom{l}{n-i}$. Therefore, the probability of having i numbers that do not belong to B is $\binom{p-l}{i}\binom{l}{n-i}\Big/\binom{p}{n}$. Therefore, the expected number of numbers that do not belong to B is

$$\sum_{i=0}^{n} \frac{i\binom{p-l}{i}\binom{l}{n-i}}{\binom{p}{n}} = \frac{n(p-l)}{p}.$$

References

[1] Adler V, Bobenko A and Suris Y 2003 Classification of integrable equations on quad-graphs. The consistency approach *Commun. Math. Phys.* **233** 513–43

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

[3] Bialecki 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

[4] Grammaticos B, Halburd R G, Ramani A and Viallet C M 2009 How to detect the integrability of discrete systems *J. Phys. A: Math. Theor.* **42** 454002–30

[5] Grinstead C M and Snell J L 1997 *Introduction to Probability* 2nd revised edn (Providence, RI: American Mathematical Society)

[6] Halburd R G 2005 Diophantine integrability *J. Phys. A: Math. Gen.* **38** 263–9

[7] Hietarinta J and Viallet C 2007 Searching for integrable lattice maps using factorization *J. Phys. A: Math. Theor.* **40** 12629–43

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

[9] Kanki M, Mada J and Tokihiro T 2012 Discrete integrable equations over finite fields *SIGMA* **8** 054

[10] Leont'ev V K 2006 On the roots of random polynomials over a finite field *Mat. Zametki* **80** 313–6

[11] Mikhailov A V and Xenitidis P 2014 Second order integrability conditions for difference equations: an integrable equation *Lett. Math. Phys.* **104** 431–50

[12] Morrison K E 1999 Random polynomials over finite fields *Preprint* http://calpoly.edu/kmorriso/Research/RPFF.pdf

[13] Nijhoff F and Capel H 1995 The discrete Korteweg–de Vries equation *Acta Appl. Math.* **39** 133–58

[14] Roberts J A G and Tran D T 2014 Towards some exact results for the (vanishing) algebraic entropy of (integrable) lattice equations *Preprint* http://web.maths.unsw.edu.au/~jagr/RT14a.pdf

[15] Roberts J A G and Vivaldi F 2003 Arithmetical method to detect integrability in maps *Phys. Rev. Lett.* **4** 034102

[16] Viallet C M 2009 Integrable lattice maps: Q_V, a rational version of Q_4 *Glasg. Math. J.* **51** 157–63