

Algebra & Number Theory

Volume 5

2011

No. 2

Elliptic nets and elliptic curves

Katherine Stange



mathematical sciences publishers

Elliptic nets and elliptic curves

Katherine Stange

An elliptic divisibility sequence is an integer recurrence sequence associated to an elliptic curve over the rationals together with a rational point on that curve. In this paper we present a higher-dimensional analogue over arbitrary base fields. Suppose E is an elliptic curve over a field K , and P_1, \dots, P_n are points on E defined over K . To this information we associate an n -dimensional array of values in K satisfying a nonlinear recurrence relation. Arrays satisfying this relation are called *elliptic nets*. We demonstrate an explicit bijection between the set of elliptic nets and the set of elliptic curves with specified points. We also obtain Laurentness/integrality results for elliptic nets.

Introduction	197
1. Elliptic nets	200
2. Laurentness and integrality	201
3. Net polynomials over \mathbb{C}	210
4. Net polynomials over arbitrary fields	215
5. Elliptic nets from elliptic curves	219
6. Elliptic curves from elliptic nets	221
7. The curve-net theorem	225
Acknowledgements	228
References	228

Introduction

An *elliptic divisibility sequence* is an integer sequence W_n satisfying

$$W_{n+m}W_{n-m} = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2. \quad (1)$$

This definition was introduced by Morgan Ward [1948]. Let $\Psi_n(x, y)$ be the n -th division polynomial associated to an elliptic curve (the n -th division polynomial vanishes at the n torsion points). Ward showed that division polynomials satisfy

This work was supported by NSERC Awards PGS D2 331379 and PDF 373333.

MSC2000: primary 11G05, 11G07, 11B37; secondary 11B39, 14H52.

Keywords: elliptic net, elliptic curve, Laurentness, elliptic divisibility sequence, recurrence sequence.

the recurrence (1) and furthermore that all elliptic divisibility sequences have the form

$$W_n = \lambda^{n^2-1} \Psi_n(x, y)$$

for some constant λ , elliptic curve (or singular cubic) and point $P = (x, y)$ on the curve. This rich structure has led to number-theoretic results [Ayad 1993; Everest et al. 2006; Ingram 2009; Silverman 2004; 2005; Swart 2003] and to applications to Hilbert's Tenth Problem [Cornelissen and Zahidi 2007; Eisenträger and Everest 2009; Poonen 2003], to integrable systems [Hone 2005], and to cryptography [Chudnovsky and Chudnovsky 1986; Shipsey 2001; Stange 2007]. For a bibliography, see [Everest et al. 2003, Chapter 10].

There have been several attempts to generalize this theory. *Translated elliptic divisibility sequences* were studied in [Swart 2003; van der Poorten 2005; van der Poorten and Swart 2006]. Mazur and Tate [1991] generalize division polynomials to arbitrary endomorphisms in the p -adic setting, and Streng [2008] uses their definition to generalize to the endomorphism ring of an elliptic curve with complex multiplication. Elliptic divisibility sequences are closely related to the denominators of the multiples $[n]P$ of a fixed point P ; questions have been asked about the collection of denominators of the linear combinations $[n]P + [m]Q$ by Everest, Miller and Stephens [2004]. The hope of defining higher-rank elliptic divisibility sequences via a recurrence relation was discussed in correspondence by Elkies, Propp and Somos [Propp 2001].

The primary purpose of this paper is to generalize from integer sequences to multidimensional arrays with values in any field, which we call *elliptic nets*. A substantial part of the difficulty lies in finding the correct recurrence and defining a generalized division polynomial.

We define an *elliptic net* to be a function $W : A \rightarrow R$ from a finite-rank free abelian group A to an integral domain R satisfying the properties that $W(0) = 0$ and that

$$\begin{aligned} W(p+q+s) W(p-q) W(r+s) W(r) \\ + W(q+r+s) W(q-r) W(p+s) W(p) \\ + W(r+p+s) W(r-p) W(q+s) W(q) = 0 \end{aligned}$$

for all $p, q, r, s \in A$. If $A = R = \mathbb{Z}$, this is an equivalent definition of an elliptic divisibility sequence (this is not immediately obvious, but it is a consequence of results in this paper). By the *rank* of an elliptic net we shall mean the rank of A (this bears no relation to the *rank of apparition* defined in [Ward 1948] for elliptic divisibility sequences). Section 1 covers the basic definitions and gives examples.

Our primary interest is the relationship between elliptic curves and elliptic nets.

Main Theorem (introductory version). *For each field K and integer n , there is an explicit bijection of sets*

$$\left\{ \begin{array}{l} \text{scale equivalence classes} \\ \text{of nondegenerate elliptic} \\ \text{nets } W : \mathbb{Z}^n \rightarrow K \end{array} \right\}$$

$$\updownarrow$$

$$\left\{ \begin{array}{l} \text{tuples } (C, P_1, \dots, P_n) \text{ where } C \text{ is a cubic} \\ \text{curve in Weierstrass form defined over } K, \\ \text{considered modulo unihomothetic changes} \\ \text{of variables, and such that } \{P_i\} \in C_{\text{ns}}(K)^n \\ \text{is appropriate} \end{array} \right\}.$$

For a description of the relevant terminology, see [Section 5](#) (appropriate), page [221](#) (scale equivalent, nondegenerate) and page [222](#) (unihomothetic). See [Theorem 7.4](#) for a more detailed statement. The isomorphism itself is described explicitly in [Definition 5.1](#) (depending on [Theorem 4.6](#)) and [Theorem 6.7](#). For ranks 1 and 2, explicit formulae can be found in [Propositions 3.8, 6.3 and 6.4](#). For an example, see [\(4\)](#).

The other main aspect of elliptic nets studied in this paper is Laurentness. These results are needed for the proof of the main theorem, but are of independent interest. One property of elliptic divisibility sequences of particular interest is that they are integer sequences: if the sequence begins $1, a, b, ac, \dots$ ($a, b, c \in \mathbb{Z}$), then it will consist entirely of integers [[Ward 1948](#)]. This result has been studied in the more general framework of the Laurent phenomenon of [[Fomin and Zelevinsky 2002](#)].

Laurentness results are found in [Section 2](#), which is devoted to the inductive structure of elliptic nets: how some terms are determined by others via the recurrence relation. We define a universal ring ${}^{\circ}\mathcal{W}_A$ for elliptic nets on A , such that elliptic nets $W : A \rightarrow R$ are in bijection with homomorphisms ${}^{\circ}\mathcal{W}_A \rightarrow R$. We obtain results on the structure of this ring, and in turn, these imply integrality results. See [Theorem 2.2](#) for the case $n = 1$, [Theorem 2.5](#) for $n = 2$, and [Theorem 2.8](#) for $n \geq 3$. The proofs in this section are elementary but somewhat tedious. The author has not been successful in replacing them with methods similar to those of [[Fomin and Zelevinsky 2002](#)], although the possibility remains.

The next two sections define the higher-rank generalization of division polynomials called *net polynomials*: rational functions on the n -fold product E^n of an elliptic curve E , which vanish on tuples (P_1, \dots, P_n) satisfying a linear relation $[v_1]P_1 + \dots + [v_n]P_n = \mathcal{O}$ for fixed coefficients v_i . In [Section 3](#), we work with the complex uniformization of an elliptic curve defined over \mathbb{C} . In [Section 4](#) we

generalize the definition to arbitrary fields by analysing the arithmetic properties of net polynomials. The main result here is [Theorem 4.4](#).

The last three sections describe the bijection in the main theorem. [Section 5](#) makes explicit the production of an elliptic net from any cubic Weierstrass curve using the net polynomials. [Section 6](#) determines exactly those cubic curves which produce a given elliptic net. Finally, [Section 7](#) puts together the results of the previous sections to prove the main theorem, stated in its full form as [Theorem 7.4](#).

Computer software. The explicit isomorphism described in this paper has been implemented for Pari/GP and SAGE in ranks 1 and 2; see [[Stange 2010](#)].

1. Elliptic nets

Definition 1.1. Let A be a free finitely-generated abelian group and R an integral domain. An *elliptic net* is any map $W : A \rightarrow R$ with

$$W(0) = 0, \tag{2}$$

and such that, for all $p, q, r, s \in A$,

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned} \tag{3}$$

Functions $W : A \rightarrow R$ which satisfy (3) but not (2) can only appear in characteristic 3 (to see this, take $p = q = r = s = 0$ in (3)). Any constant function in characteristic 3 is an example. By definition, these are not elliptic nets.

We refer to the rank of A as the *rank* of the elliptic net. Suppose that $B \subset A$ is a subgroup of A . Then the restriction to B of an elliptic net $W : A \rightarrow R$ is also an elliptic net. We refer to this elliptic net as *the subnet associated to B* and write $W|_B : B \rightarrow R$.

Example 1.2. Let R be an integral domain. The following are elliptic nets.

- The *zero net* $W : \mathbb{Z}^n \rightarrow R$ defined by $W(v) = 0$ for all v .
- The identity map $W_{id} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $W(v) = v$.
- Let $W' : \mathbb{Z} \rightarrow R$ be an elliptic net. Then for each $1 \leq i \leq n$, we may define $W_i : \mathbb{Z}^n \rightarrow R$ by $W_i(v_1, \dots, v_n) = W'(v_i)$, and this will also be an elliptic net.
- More generally, if $W : A \rightarrow R$ is an elliptic net and $f : B \rightarrow A$ is a homomorphism of finitely generated free abelian groups, then $W \circ f : B \rightarrow R$ is also an elliptic net.
- If $W : A \rightarrow R$ is an elliptic net and $g : R \rightarrow S$ is a homomorphism of integral domains, then $g \circ W : A \rightarrow S$ is also an elliptic net.

- $W_{\text{Leg}} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $W(v) = \left(\frac{v}{3}\right)$, the Legendre symbol of v over 3. This can be verified by a finite examination of cases; observe that at least one of $p, q, r, p - q, q - r$, and $r - p$ is divisible by 3. See also [Ward 1948, p. 31].
- $W_{\text{Fib}} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by

$$W(v) = \begin{cases} F_{2v} & \text{if } v > 0, \\ -F_{2v} & \text{if } v < 0, \\ 0 & \text{if } v = 0, \end{cases}$$

where F_{2v} is the $2v$ -th Fibonacci number. One checks this example using the closed form for terms of the Fibonacci sequence. See also [Ward 1948, p. 31].

- Here is a portion of an elliptic net of rank 2, displayed as an array:

	3269	-2869	4335	5959	12016	-55287	23921	1587077	-7159461	
	-127	-299	94	479	919	-2591	13751	68428	424345	
	-44	-27	-31	53	-33	-350	493	6627	48191	
	-1	-7	-5	8	-19	-41	-151	989	-1466	
	3	-2	1	3	-1	-13	-36	181	-1535	
	1	-1	1	1	2	-5	7	89	-149	(4)
	-1	-1	0	1	1	-3	11	38	249	
\uparrow	-2	-1	-1	1	-1	-4	1	47	185	
Q	1	-3	-1	2	-3	-5	-17	63	-184	
	$P \rightarrow$									

This example arises from the curve $y^2 + y = x^3 + x^2 - 2x$ over \mathbb{Q} and the two points $P = (0, 0)$, $Q = (1, 0)$; see Example 5.3. The origin is at the term with value 0. Each axis forms an elliptic divisibility sequence, e.g., 0, 1, 1, -3, 11, 38, 249,

2. Laurentness and integrality

In this section we ask which terms of an elliptic net determine the others via the recurrence relation. In the case of $n = 1$, Ward [1948] showed that the terms $W(1), \dots, W(4)$ sufficed to determine the rest of the net (unless too many of these terms were zero). Our method also demonstrates Laurentness and integrality results. The main theorems of this section are used in Section 6.

Laurentness. Let I be a group, in additive notation, called the *indexing group*, whose elements are called *indices*. To each $i \in I$, we associate the symbol T_i . In what follows, the indexing group will be $I \cong \mathbb{Z}^n$ for some n .

Consider the ideal \mathcal{M} in the ring $\mathbb{Z}[T_i]_{i \in I}$ generated by T_0 and all polynomials encoding property (3), i.e., those of the form

$$T_{p+q+s}T_{p-q}T_{r+s}T_r + T_{q+r+s}T_{q-r}T_{p+s}T_p + T_{r+p+s}T_{r-p}T_{q+s}T_q \quad (5)$$

as p, q, r, s range over I . Polynomials of the form (5) will be called *recurrence relations*. Consider the ring ${}^{\circ}\mathcal{W}_I$ obtained from $\mathbb{Z}[T_i]_{i \in I} / \mathcal{M}$ as a quotient by its own nilradical. For each integral domain R , there is a bijection between elliptic nets $W : I \rightarrow R$ and homomorphisms ${}^{\circ}\mathcal{W}_I \rightarrow R$ (defined by taking $T_i \mapsto W(i)$).

Taking $p = q = i, r = s = 0$ shows that $T_i^3(T_i + T_{-i}) \in \mathcal{M}$ for each $i \in I$. In particular, $T_{-i}^3(T_i + T_{-i}) \in \mathcal{M}$ also. Therefore, any prime ideal containing \mathcal{M} contains $T_i + T_{-i}$; for if it did not, then it must contain T_i and T_{-i} , a contradiction. Therefore $T_{-i} = -T_i$ in ${}^{\circ}\mathcal{W}_I$. This implies the following.

Proposition 2.1. *Let $W : A \rightarrow R$ be an elliptic net. Then $W(-z) = -W(z)$ for all $z \in A$.*

The purpose of this section is to find a finite subset $0 \notin J \subset I$ such that the localisation ${}^{\circ}\mathcal{W}_I[T_i^{-1}]_{i \in J}$ is finitely generated as a \mathbb{Z} -algebra, and to give the generators. (The localisation is not the trivial ring ($1 = 0$) by the existence of a homomorphism from it to \mathbb{Q} given by Example 1.2, where one uses part (3) with $W' = W_{id}$ of part (2).) From this we show that every T_i can be expressed as a Laurent polynomial in integer coefficients in a finite number of terms T_j . This implies that any elliptic net which does not take zero values at the T_j is entirely determined by those values.

To illustrate, consider the rank-one case, which is essentially a result of Morgan Ward.

Theorem 2.2 [Ward 1948, Theorem 4.1]. *The ring ${}^{\circ}\mathcal{W}_{\mathbb{Z}}[T_1^{-1}, T_2^{-1}]$ is generated as a \mathbb{Z} -algebra by the six elements*

$$T_1, \quad T_1^{-1}, \quad T_2, \quad T_2^{-1}, \quad T_3, \quad T_4.$$

Furthermore, each T_i is expressible as a \mathbb{Z} -coefficient polynomial in

$$T_1, \quad T_1^{-1}, \quad T_2, \quad T_3, \quad T_4 T_2^{-1}.$$

In particular, let $W : \mathbb{Z} \rightarrow \mathbb{Q}$ be an elliptic net. If $W(1) = 1$, $W(2) \neq 0$, $W(i)$ is an integer for $i = 2, 3, 4$, and $W(2)$ divides $W(4)$, then the elliptic net consists entirely of integers.

Proof. Recall that $T_{-n} = -T_n$, so it suffices to prove the first two statements for positive n . Taking $(p, q, r, s) = (n+1, n, 1, 0)$ and $(n+1, n-1, 1, 0)$ respectively, in ${}^{\circ}\mathcal{W}_I$ we have

$$T_{2n+1}T_1^3 + T_{n-1}T_{n+1}^3 + T_{n+2}T_{-n}T_n^2 = 0, \tag{6}$$

$$T_{2n}T_2T_1^2 + T_nT_{n-2}T_{n+1}^2 + T_{n+2}T_{-n}T_{n-1}^2 = 0. \tag{7}$$

The equations (6) and (7) prove the first statement by induction. The base case consists of $0 \leq n \leq 4$; for $n > 4$, we have $2n > n + 2$.

For even i , it can be shown by induction on (7) that T_i is expressible as a \mathbb{Z} -coefficient polynomial in $T_1, T_1^{-1}, T_2, T_2^{-1}, T_3$, and T_4 in such a way that the combined degree of T_2 and T_4 in each monomial is positive. For $i = 2, 4$ this is clear. To complete the induction in general, observe that in (7), each of the rightmost two terms is divisible by at least two T_k where k is even and $k < 2n$.

For even i , the second statement of the theorem concerning the expressibility of all T_i in terms of T_1, T_1^{-1}, T_2, T_3 and $T_4 T_2^{-1}$ follows from the observation of the previous paragraph. The statement also holds for $i = 1, 3$. Consequently, it holds for odd i by induction on (6). \square

Proofs by induction. The inductive proofs in this section will be based on the following definitions. Consider finite sets $S, J \subset I$ where $0, i \notin S \cup J$. We say that an index $i \in I$ is *S-integrally implied by J* if there exists a \mathbb{Z} -coefficient monomial $P(T_s)$ (in variables indexed by S) and \mathbb{Z} -coefficient polynomial $Q(T_j)$ (in variables indexed by J) such that

$$T_i P(T_s) = Q(T_j) \tag{8}$$

in ${}^{\mathcal{W}}I$. A set $K \subset I$ is *S-integrally implied by the set J* if every index in K is *S-integrally implied by J*.

As an example (see Proposition 2.1 and the paragraph which precedes it), $-i$ is *S-integrally implied by any J containing i* (for any S). In what follows, this fact will often be used tacitly.

A set $B \subset I$ is an *S-integral baseset for ${}^{\mathcal{W}}I$* if all of I is *S-integrally implied by B*. If $B \subset I$ is an *S-integral baseset*, then each T_i can be expressed as a polynomial with integer coefficients in the set of variables $\{T_b\}_{b \in B} \cup \{T_s^{-1}\}_{s \in S}$ (when considered in the appropriate localisation).

It is straightforward to verify that if i is *S-integrally implied by J* and every $j \in J$ is *S-integrally implied by J'*, then i is *S-integrally implied by J'*. To show that B is an *S-integral baseset for I*, the proofs in this section show the following: for each index $i \in I$, there is a finite sequence $J_0 \subset J_1 \subset \dots \subset J_n$ such that $B = J_0, i \in J_n$ and for each $1 \leq k \leq n, J_k$ is *S-integrally implied by J_{k-1}*. At each stage, we show that each index of J_i is *S-integrally implied by J_{i-1}*. Recall that implication is simply the existence of an relation of the form (8), and in fact we simply give a relevant element of the form (5).

These elements are cumbersome to write out. For example, taking in the case $n = 3, \mathbf{p} = (1, 0, 0), \mathbf{q} = (0, 1, 0), \mathbf{r} = (0, 0, 1), \mathbf{s} = (0, 0, 0)$, we obtain

$$\begin{aligned} &T_{(1,1,0)}T_{(1,-1,0)}T_{(0,0,1)}T_{(0,0,1)} \\ &\quad + T_{(0,1,1)}T_{(0,1,-1)}T_{(1,0,0)}T_{(1,0,0)} \\ &\quad\quad\quad + T_{(1,0,1)}T_{(-1,0,1)}T_{(0,1,0)}T_{(0,1,0)}. \end{aligned}$$

For this information, let us instead use the more convenient notation

$$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix} \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array} \right]. \tag{9}$$

In this notation, the columns to the left of the brackets correspond to the columns of p, q, r and s , while the indices of the terms of the recurrence appear as the columns within the brackets.

To demonstrate that an index i is (S -integrally) implied by a set of indices J , it suffices to write down an appropriate such array. Notice that any array of the form (9) is a recurrence if each row is a recurrence. Therefore we may construct examples row by row.

The following definition will be useful for ordering inductions.

Definition 2.3. Let

$$N(\mathbf{v}) = \max_{i=1, \dots, n} |v_i|$$

be the *sup-norm* of the vector \mathbf{v} .

Basesets for rank 2. For the rank-two case, we require a lemma.

Lemma 2.4. *The ring ${}^{\circ}\mathcal{W}_{\mathbb{Z}^2}[T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(1,1)}^{-1}]$ is generated as a \mathbb{Z} -algebra by the elements*

$$\{T_{\mathbf{v}} : N(\mathbf{v}) \leq 4\} \cup \{T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(1,1)}^{-1}\}.$$

Proof. Let $S = \{(1, 0), (0, 1), (1, 1)\}$ and $B = \{\mathbf{v} \in \mathbb{Z}^2 : N(\mathbf{v}) \leq 4\}$. This proof proceeds by induction on the sup-norm. Trivially, any \mathbf{v} with $N(\mathbf{v}) \leq 4$ is S -integrally implied by B . Let $N_0 > 4$ and suppose that all terms with indices with sup-norm less than N_0 are S -integrally implied by B . Call the set of such indices K_{N_0} . Suppose \mathbf{v} is an index of sup-norm N_0 . We construct a recurrence demonstrating that \mathbf{v} is S -integrally implied by K_{N_0} row by row. For $i = 1, 2$, define $w_i = \lceil v_i/2 \rceil$.

Case I: \mathbf{v} has one odd entry and one even entry. For the odd entry, we use the row

$$w_i \ w_{i-1} \ 0 \ 0 \ [\ v_i \ 1 \ 0 \ 0 \ | \ w_{i-1} \ w_{i-1} \ w_i \ w_i \ | \ w_i \ -w_i \ w_{i-1} \ w_{i-1} \]$$

For the even entry, we use the row

$$w_i \ w_i \ 1 \ 0 \ [\ v_i \ 0 \ 1 \ 1 \ | \ w_{i+1} \ w_{i-1} \ w_i \ w_i \ | \ w_{i+1} \ -w_{i+1} \ w_i \ w_i \]$$

Case II: \mathbf{v} has two odd entries. Use the rows

$$\begin{matrix} w_1 & w_{1-1} & 0 & 0 \\ w_2 & w_{2-1} & 1 & 0 \end{matrix} \left[\begin{array}{ccc|ccc} v_1 & 1 & 0 & 0 & w_{1-1} & w_{1-1} & w_1 & w_1 \\ v_2 & 1 & 1 & 1 & w_2 & w_{2-2} & w_2 & w_2 \end{array} \middle| \begin{array}{cccc} w_1 & -w_1 & w_{1-1} & w_{1-1} \\ w_{2+1} & -w_{2+1} & w_{2-1} & w_{2-1} \end{array} \right]$$

Case III: \mathbf{v} has two even entries. Use the rows

$$\begin{array}{c} w_1 \ w_{1-1} \ 0 \ 1 \\ w_2 \ w_2 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} v_1 & 1 & 1 & 0 & w_1 & w_{1-1} & w_{1+1} & w_1 \\ v_2 & 0 & 1 & 1 & w_{2+1} & w_{2-1} & w_2 & w_2 \end{array} \right] \begin{array}{c} w_{1+1} \ -w_1 \ w_1 \ w_{1-1} \\ w_{2+1} \ -w_{2+1} \ w_2 \ w_2 \end{array}$$

For even v_i , either $|v_i| \leq 2$ or $|v_i| > 3$. In the former case, $|w_i| + 1 \leq 2 < N_0$. In the latter case, we have $|w_i| + 1 \leq (|v_i| + 2)/2 < |v_i| \leq N_0$. For odd v_i , either $|v_i| \leq 3$ or $|v_i| > 4$. In the former case $|w_i| + 2 \leq 4 < N_0$. In the latter case, we have $|w_i| + 2 \leq (|v_i| + 5)/2 < |v_i| \leq N_0$.

Therefore all the vectors in the recurrence have sup-norm less than N_0 with the exception of \mathbf{v} . In the monomial of \mathbf{v} in the recurrence, the other indices are $(1, 0)$, $(0, 1)$ or $(1, 1)$. This demonstrates that \mathbf{v} is S -integrally implied by K_{N_0} and hence by B . \square

Theorem 2.5. *The ring ${}^{\circ}W_{\mathbb{Z}^2}[T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}]$ is generated as a \mathbb{Z} -algebra by the eleven elements*

$$T_{(1,1)}, T_{(1,0)}, T_{(0,1)}, T_{(1,1)}^{-1}, T_{(1,0)}^{-1}, T_{(0,1)}^{-1}, T_{(2,1)}, T_{(1,2)}, T_{(2,0)}, T_{(0,2)}, T_{(2,2)},$$

and the following identities hold:

$$T_{(1,-1)}T_{(1,1)}^3 = T_{(1,0)}^3T_{(1,2)} - T_{(0,1)}^3T_{(2,1)},$$

$$T_{(2,2)}T_{(1,-1)}T_{(1,0)}T_{(0,1)} = T_{(1,1)}(T_{(0,2)}T_{(2,1)}T_{(1,0)} - T_{(0,1)}T_{(2,0)}T_{(1,2)}).$$

In particular, if $W : \mathbb{Z}^2 \rightarrow \mathbb{Q}$ is an elliptic net for which

- (a) $W(1, 0) = W(0, 1) = W(1, 1) = 1$,
- (b) $W(2, 0), W(0, 2), W(1, 2) \neq W(2, 1)$ are integers, and
- (c) $W(1, 2) - W(2, 1)$ divides $W(0, 2)W(2, 1) - W(2, 0)W(1, 2)$,

then all terms of the elliptic net are determined by these seven values and are integers.

Proof. The first and second stated identities are the recurrences

$$\begin{array}{c} 1 \ 0 \ 1 \ 0 \\ 0 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right], \tag{10}$$

$$\begin{array}{c} 1 \ 1 \ -1 \ 0 \\ 1 \ 2 \ 1 \ -1 \end{array} \left[\begin{array}{ccc|ccc} 2 & 0 & -1 & -1 & 0 & 2 & 1 & 1 & 0 & -2 & 1 & 1 \\ 2 & -1 & 0 & 1 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2 \end{array} \right].$$

Let $S = \{(1, 0), (0, 1), (1, 1)\}$, and $B = \{\mathbf{v} \in \mathbb{Z}^2 : N(\mathbf{v}) \leq 4\}$. By Lemma 2.4, it suffices to show that B is S -integrally implied by the set

$$\{(1, 0), (0, 1), (1, 1), (2, 0), (0, 2), (2, 1), (1, 2), (2, 2)\}.$$

We list the relevant recurrences in order. As each index is implied, it may be used to imply later indices. It is assumed that as (a, b) is implied, so is $(-a, -b)$. To begin, the index $(1, -1)$ is implied by (10). We then write

$$\begin{aligned}
 (2, -1): & \quad -1 \ 0 \ 1 \ 1 \left[\begin{array}{ccc|ccc} 0 & -1 & 2 & 1 & 2 & -1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right] \left[\begin{array}{ccc} 1 & 2 & 1 & 0 \\ 1 & -1 & 1 & 1 \end{array} \right], \\
 (-1, 2): & \quad 0 \ -1 \ -1 \ 0 \left[\begin{array}{ccc|ccc} -1 & 1 & -1 & -1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right] \left[\begin{array}{cccc} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \end{array} \right], \\
 (2, -2): & \quad 1 \ 1 \ -1 \ 0 \left[\begin{array}{ccc|ccc} 2 & 0 & -1 & -1 & 0 & 2 & 1 & 1 \\ -1 & -2 & -1 & 1 & -2 & -1 & 0 & -1 \end{array} \right] \left[\begin{array}{ccc} 0 & -2 & 1 & 1 \\ -1 & 0 & -1 & -2 \end{array} \right].
 \end{aligned}$$

At this point we have implied all indices of sup-norm at most 2. Next we have

$$\begin{aligned}
 (3, 0): & \quad 2 \ 1 \ 0 \ 0 \left[\begin{array}{ccc|ccc} 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & -1 & 0 & 0 \end{array} \right] \left[\begin{array}{ccc} 2 & -2 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{array} \right], \\
 (3, 1): & \quad 2 \ 1 \ 0 \ 0 \left[\begin{array}{ccc|ccc} 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 0 & 1 & 0 & 1 & -1 & 1 & 1 \end{array} \right] \left[\begin{array}{ccc} 2 & -2 & 1 & 1 \\ 2 & 0 & 0 & 0 \end{array} \right], \\
 (3, 2): & \quad 2 \ 1 \ 0 \ 0 \left[\begin{array}{ccc|ccc} 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 1 & 0 & 2 & 0 & 1 & 1 \end{array} \right] \left[\begin{array}{ccc} 2 & -2 & 1 & 1 \\ 2 & 0 & 1 & 1 \end{array} \right], \\
 (3, 3): & \quad 2 \ 1 \ 1 \ 0 \left[\begin{array}{ccc|ccc} 3 & 1 & 1 & 1 & 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \end{array} \right] \left[\begin{array}{ccc} 3 & -1 & 1 & 1 \\ 2 & -2 & 1 & 1 \end{array} \right].
 \end{aligned} \tag{11}$$

Simply by switching top rows with bottom rows, we similarly imply $(0, 3)$, $(1, 3)$, and $(2, 3)$. And by putting negatives on the second row of (11), we imply the index $(3, -2)$ (and $(-2, 3)$ by switching top and bottom). Next,

$$\begin{aligned}
 (3, -1): & \quad 2 \ 1 \ 0 \ 0 \left[\begin{array}{ccc|ccc} 3 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ -1 & -1 & -2 & 2 & -1 & 1 & 1 & -1 \end{array} \right] \left[\begin{array}{ccc} 2 & -2 & 1 & 1 \\ 0 & 0 & 0 & -2 \end{array} \right], \\
 (3, -3): & \quad 1 \ 2 \ 1 \ 0 \left[\begin{array}{ccc|ccc} 3 & -1 & 1 & 1 & 3 & 1 & 1 & 1 \\ -2 & -1 & 0 & 0 & -3 & -1 & 0 & 0 \end{array} \right] \left[\begin{array}{ccc} 2 & 0 & 2 & 2 \\ -2 & -2 & -1 & -1 \end{array} \right].
 \end{aligned}$$

Again by switching top and bottom we get $(-1, 3)$. We have now implied all indices with sup-norm at most 3. We continue with

$$\begin{aligned}
 (4, 0): & \quad 2 \ 1 \ 0 \ 1 \left[\begin{array}{ccc|ccc} 4 & 1 & 1 & 0 & 2 & 1 & 3 & 2 \\ 0 & 0 & 1 & 0 & 1 & -1 & 0 & 0 \end{array} \right] \left[\begin{array}{ccc} 3 & -2 & 2 & 1 \\ 1 & 1 & 0 & 0 \end{array} \right], \\
 (4, 1): & \quad 3 \ 2 \ 1 \ -1 \left[\begin{array}{ccc|ccc} 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{array} \right] \left[\begin{array}{ccc} 3 & -2 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{array} \right], \\
 (4, 2): & \quad 3 \ 2 \ 1 \ -1 \left[\begin{array}{ccc|ccc} 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 \\ 1 & 1 & 1 & 0 & 2 & 0 & 1 & 1 \end{array} \right] \left[\begin{array}{ccc} 3 & -2 & 1 & 2 \\ 2 & 0 & 1 & 1 \end{array} \right], \\
 (4, 3): & \quad 2 \ 2 \ 1 \ 0 \left[\begin{array}{ccc|ccc} 4 & 0 & 1 & 1 & 3 & 1 & 2 & 2 \\ 2 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \end{array} \right] \left[\begin{array}{ccc} 3 & -1 & 2 & 2 \\ 2 & -2 & 1 & 1 \end{array} \right], \\
 (4, 4): & \quad 3 \ 2 \ 1 \ -1 \left[\begin{array}{ccc|ccc} 4 & 1 & 0 & 1 & 2 & 1 & 2 & 3 \\ 2 & 2 & 1 & 0 & 3 & 1 & 2 & 2 \end{array} \right] \left[\begin{array}{ccc} 3 & -2 & 1 & 2 \\ 3 & -1 & 2 & 2 \end{array} \right].
 \end{aligned}$$

Again by switching top rows with bottom rows, we similarly imply $(0, 4)$, $(1, 4)$, $(2, 4)$ and $(3, 4)$. And by putting negatives on the second rows, we imply the indices $(4, -1)$, $(-1, 4)$, $(4, -3)$ and $(-3, 4)$. There remains to consider the

indices

$$(4, -2): \quad \begin{array}{c} 2 \ 1 \ -1 \ 1 \\ -1 \ -1 \ -1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 4 & 1 & 0 & -1 & 1 & 2 & 3 & 2 \\ -2 & 0 & -1 & -1 & -2 & 0 & -1 & -1 \end{array} \right],$$

$$(4, -4): \quad \begin{array}{c} 2 \ 1 \ -1 \ 1 \\ -2 \ -2 \ -1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 4 & 1 & 0 & -1 & 1 & 2 & 3 & 2 \\ -4 & 0 & -1 & -1 & -3 & -1 & -2 & -2 \end{array} \right].$$

By switching rows, we imply $(-2, 4)$. We have now demonstrated the calculation of all terms of index with sup-norm at most 4. The second part of the statement follows immediately from the first. \square

Basesets for ranks $n \geq 3$. Let \mathbf{e}_i denote the standard basis vectors.

Lemma 2.6. Define subsets of \mathbb{Z}^3 by

$$L_2 = \{\mathbf{e}_i\}_i \cup \{\mathbf{e}_i \pm \mathbf{e}_j\}_{i \neq j} \cup \{2\mathbf{e}_i\}_i,$$

$$L'_2 = \{a_i \mathbf{e}_i + a_j \mathbf{e}_j : a_i \in \mathbb{Z}, 1 \leq i \leq j \leq 3\}.$$

Then all indices $\mathbf{v} \in \mathbb{Z}^3$ with $N(\mathbf{v}) \leq 2$ are L_2 -integrally implied by L'_2 .

Proof. We make use of the recurrences

$$\begin{array}{c} 1 \ 1 \ 0 \ -1 \\ 0 \ 0 \ -1 \ 1 \\ 1 \ 0 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \end{array} \right], \quad (12)$$

$$\begin{array}{c} 0 \ 0 \ 1 \ -1 \\ 1 \ 1 \ 0 \ -1 \\ 0 \ 1 \ 1 \ 0 \end{array} \left[\begin{array}{ccc|ccc} -1 & 0 & 0 & 1 & 0 & -1 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1 & 2 & 0 & 0 & 0 \end{array} \right], \quad (13)$$

$$\begin{array}{c} 1 \ 0 \ 1 \ 0 \\ 0 \ 0 \ 0 \ 1 \\ 1 \ 1 \ 0 \ -1 \end{array} \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & -1 & 1 & 1 & 2 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{array} \right]. \quad (14)$$

Permute the rows of (12) by the cyclic permutations (123) and (132), calling the results (12)' and (12)'' respectively; for example, the rightmost column of (12)' is $(0, 1, 0)$. Do the same for (13) and (14).

Consider the equation obtained by the combination

$$\begin{aligned} & (12) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,-1,0)} T_{(0,1,0)}^2 + (12)' \times T_{(1,1,1)} T_{(1,0,0)} T_{(0,1,-1)} T_{(0,1,0)}^2 T_{(0,0,1)} \\ & + (14) \times T_{(1,-1,0)} T_{(0,1,0)}^2 T_{(0,1,1)} T_{(0,0,1)} T_{(1,0,1)}^2 + (14)' \times T_{(0,1,-1)} T_{(1,0,0)}^2 T_{(0,0,1)} T_{(1,0,1)} T_{(1,1,0)} \\ & + (13) \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(0,1,0)}^2 T_{(1,1,0)} + (13)' \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,0,0)} T_{(0,1,1)} T_{(0,0,1)} \\ & + (13)'' \times T_{(1,1,1)} T_{(1,0,0)}^2 T_{(1,0,1)} T_{(0,1,0)} T_{(0,0,1)}. \end{aligned}$$

The result has the form $aT_{(1,1,1)} + b = 0$, where a and b are polynomials in $T_{\mathbf{v}}$ where every \mathbf{v} has at least one zero coordinate. In particular,

$$a = T_{(1,0,0)}^3 T_{(0,1,0)} T_{(0,0,1)}^2 T_{(1,0,1)} T_{(0,2,0)} T_{(1,0,-1)}.$$

Thus $T_{(1,1,1)}$ is L_2 -integrally implied by L'_2 . To imply the terms $T_{(-1,1,1)}$, $T_{(1,-1,1)}$, and $T_{(1,1,-1)}$, use (12), (12)', and (12)". This covers all terms of sup-norm at most 1.

We have the following recurrence:

$$\begin{matrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 2 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{matrix} \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & -1 & 1 & 0 \\ 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2 & 2 & -1 & 0 & 1 \\ 2 & -1 & 1 & 0 & 2 & 1 & 1 & 0 & 1 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \end{array} \right].$$

If \mathbf{v} has exactly one coordinate of value ± 2 (the rest ± 1), then we imply \mathbf{v} by taking the first three rows in the recurrence above (possibly taking negatives and permutations of rows as necessary). If \mathbf{v} has exactly two ± 2 's, use the middle three rows in the same way. If \mathbf{v} has exactly three ± 2 's, use the last three rows (this relies on the previous cases). □

Remark 2.7. The four equations (12), (12)', (12)" and (13) in the four unknowns $T_{(1,1,1)}$, $T_{(-1,1,1)}$, $T_{(1,-1,1)}$ and $T_{(1,1,-1)}$, are linear with coefficients consisting of monomials in $T_{\mathbf{v}}$ where \mathbf{v} has at least one zero coordinate. The determinant of the system is

$$2T_{(1,0,0)}T_{(0,1,0)}T_{(0,0,1)}^2T_{(1,1,0)}T_{(1,0,1)}^2T_{(0,1,1)}^2T_{(1,-1,0)}T_{(1,0,-1)}T_{(0,1,-1)}.$$

This observation is useful for calculations where 2 is invertible.

Theorem 2.8. Let $n \geq 2$. For each ℓ in the set

$$L = \{0, 1\}^n \setminus \{(0, 0, \dots, 0), (1, 1, \dots, 1)\},$$

choose a vector \mathbf{x}_ℓ having $N(\mathbf{x}_\ell) = 1$ and having nonzero entries exactly where ℓ does. Let $G_n = \{\mathbf{x}_\ell\}_{\ell \in L}$. Let

$$\begin{aligned} H_n &= G_n \cup \{\mathbf{e}_i\} \cup \{\mathbf{e}_i \pm \mathbf{e}_j, i \neq j\} \cup \{2\mathbf{e}_i\}, \\ H'_n &= H_n \cup \{2\mathbf{e}_i + \mathbf{e}_j, i \neq j\}. \end{aligned}$$

Then \mathbb{Z}^n is H_n -integrally implied by H'_n .

Proof. The proof is by induction on n . The base case is $n = 2$, which is a consequence of Theorem 2.5.

Fixing any $1 \leq i \leq n$, we can identify H_{n-1} with a subset of H_n (and H'_{n-1} with a subset of H'_n) by adding a zero between the $(i - 1)$ -th and i -th positions of each vector of H_{n-1} (or H'_{n-1}). By this identification and by the inductive hypothesis (for $n - 1$), any $\mathbf{v} \in \mathbb{Z}^n$ with a zero in the i -th position is H_n -integrally implied by H'_n . Therefore it suffices to imply those $\mathbf{v} \in \mathbb{Z}^n$ having no zero coordinate.

The inductive step is itself an induction on the sup-norm of \mathbf{v} . The base cases are $N(\mathbf{v}) = 1$ and $N(\mathbf{v}) = 2$. Both of these for $n = 3$ are provided by Lemma 2.6,

so for the base cases, we may assume $n \geq 4$. To imply \mathbf{v} , we construct a recurrence row by row, so that the first column is exactly \mathbf{v} . For the first three rows, use the following, multiplied by -1 as necessary.

$$\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array} \right].$$

For all subsequent rows, use one of the following two recurrences (shown together in an array), multiplied by -1 as appropriate:

$$\begin{matrix} 1 & 1 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{matrix} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \end{array} \right].$$

For each row, the choice between the two possibilities can be made in such a way that the fourth column of the recurrence lies in G_n . Columns 2 and 4 have at most two nonzero entries (which are ± 1) and so are in H_n . The other columns, numbered 5 though 12, have at least one zero entry, and so are already implied by the inductive step. This completes the case $N(\mathbf{v}) = 1$.

For the remainder of the proof, we will repeatedly use the following recurrences. Let $w_i = \lceil v_i/2 \rceil$. If v_i is even, we call the recurrences shown in the following array (E1) through (E4):

$$\begin{matrix} w_{i-1} & w_i & 0 & 1 \\ w_i & w_{i-1} & 0 & 1 \\ w_i & w_i & 0 & 0 \\ w_i & w_i & 1 & 0 \end{matrix} \left[\begin{array}{ccc|ccc} v_i & -1 & 1 & 0 & w_{i+1} & w_i & w_i & w_{i-1} \\ v_i & 1 & 1 & 0 & w_i & w_{i-1} & w_{i+1} & w_i \\ v_i & 0 & 0 & 0 & w_i & w_i & w_i & w_i \\ v_i & 0 & 1 & 1 & w_{i+1} & w_{i-1} & w_i & w_i \end{array} \right] \left[\begin{array}{ccc|ccc} w_i & -w_{i+1} & w_{i+1} & w_i \\ w_{i+1} & -w_i & w_i & w_{i-1} \\ w_i & -w_i & w_i & w_i \\ w_{i+1} & -w_{i+1} & w_i & w_i \end{array} \right]$$

If v_i is odd, we call the following recurrences (O1) through (O5).

$$\begin{matrix} w_i & w_{i-1} & 0 & 0 \\ w_{i-1} & w_i & 0 & 0 \\ w_{i-1} & w_i & 1 & 0 \\ w_i & w_i & 0 & -1 \\ w_i & w_i & 1 & -1 \end{matrix} \left[\begin{array}{ccc|ccc} v_i & 1 & 0 & 0 & w_{i-1} & w_{i-1} & w_i & w_i \\ v_i & -1 & 0 & 0 & w_i & w_i & w_{i-1} & w_{i-1} \\ v_i & -1 & 1 & 1 & w_{i+1} & w_{i-1} & w_{i-1} & w_{i-1} \\ v_i & 0 & -1 & 0 & w_{i-1} & w_i & w_{i-1} & w_i \\ v_i & 0 & 0 & 1 & w_i & w_{i-1} & w_{i-1} & w_i \end{array} \right] \left[\begin{array}{ccc|ccc} w_i & -w_i & w_{i-1} & w_{i-1} \\ w_{i-1} & 1-w_i & w_i & w_i \\ w_i & -w_i & w_i & w_i \\ w_{i-1} & -w_i & w_{i-1} & w_i \\ w_i & 1-w_i & w_{i-1} & w_i \end{array} \right]$$

The second base case is $N(\mathbf{v}) = 2$ ($n \geq 4$ still). Since we may assume $v_i \neq 0$ (this is covered by previous cases in the induction on n), the other v_i have $|v_i| = \pm 1$. There are three cases:

Case I: \mathbf{v} has at least three odd v_i . Use for the first three odd v_i the recurrences (O1), (O4) and (O5) respectively. Use (E3) for all the even v_i . In this case, all the columns besides the first contain only digits 0 and ± 1 and so were implied in the case $N(\mathbf{v}) = 1$. Columns 2, 3, and 4 contain only one nonzero term each, and so are in H_n .

Case II: \mathbf{v} has one or two odd v_i . Use (O3) for one odd coordinate and (O1) for the other (if it exists). Use (E3) for all even coordinates. Then, columns 2–4 contain one or two nonzero entries, and columns 5–12 may contain at most one ± 2 ; but such a column was implied in the Case I.

Case III: \mathbf{v} has no odd v_i . Use (E1) and (E4) for the first two rows, and (E3) for all others. Columns 2–4 contain one or two nonzero entries and 5–12 at most two ± 2 's; but such a column was implied in Case I or II.

This completes the $N(\mathbf{v}) = 2$ base case.

Now suppose $N(\mathbf{v}) = N_0 \geq 3$ and $n \geq 3$. This is the inductive step; we will assume we have implied all indices of sup-norm less than N_0 . As before, $v_i \neq 0$. For $|v_i| = 3$, (O1), (O2), (O4), and (O5) have entries less than N_0 in columns 5–12. For $1 \leq |v_i| \leq 2$, and $3 < |v_i| \leq N_0$, all applicable recurrences have entries less than N_0 in those columns. We have two cases:

Case I: \mathbf{v} has at least one even entry. Use (E4) for the first even coordinate, and choose from (E1) and (E2) for the second even coordinate (if it exists). We use (E3) for all other even coordinates. We will use (O1) or (O2) for all odd entries (and make the choice between (E1) and (E2) above) in such a way that the second column is in G_n .

Case II: \mathbf{v} has no even entry. Use (O4) and (O5) for the first two odd coordinates, and (O1) or (O2) for all others, according so that the second column is an element of G_n . □

3. Net polynomials over \mathbb{C}

Fix an elliptic curve E defined over \mathbb{C} . Our purpose is to define rational functions $\Omega_{\mathbf{v}} : E^n \rightarrow \mathbb{C}$ for all $\mathbf{v} \in \mathbb{Z}^n$ such that for each $\mathbf{P} \in E^n$, the map

$$W_{E, \mathbf{P}} : \mathbb{Z}^n \rightarrow \mathbb{C}, \quad \mathbf{v} \mapsto \Omega_{\mathbf{v}}(\mathbf{P})$$

is an elliptic net. In this section we associate a lattice $\Lambda \subset \mathbb{C}$ to the elliptic curve E and consider the complex uniformization \mathbb{C}/Λ .

Elliptic functions over \mathbb{C} . For a complex lattice Λ , let $\eta : \Lambda \rightarrow \mathbb{C}$ be the quasiperiod homomorphism, and define a quadratic form $\lambda : \Lambda \rightarrow \{\pm 1\}$ by

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda, \\ -1 & \text{if } \omega \notin 2\Lambda. \end{cases}$$

Recall that the Weierstrass sigma function $\sigma : \mathbb{C}/\Lambda \rightarrow \mathbb{C}$ satisfies the following transformation formula for all $z \in \mathbb{C}$ and $\omega \in \Lambda$:

$$\sigma(z + \omega; \Lambda) = \lambda(\omega)e^{\eta(\omega)(z + \frac{1}{2}\omega)}\sigma(z; \Lambda). \tag{15}$$

Definition 3.1. Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . For $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$, define a function $\Omega_{\mathbf{v}}$ on \mathbb{C}^n in variables $\mathbf{z} = (z_1, \dots, z_n)$ as follows:

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = \frac{\sigma(v_1 z_1 + \dots + v_n z_n; \Lambda)}{\prod_{i=1}^n \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \leq i < j \leq n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}$$

(If $\mathbf{v} = \mathbf{0}$, we set $\Omega_{\mathbf{v}} \equiv 0$.) In particular, we have for each $n \in \mathbb{Z}$, a function Ω_n on \mathbb{C} in the variable z , namely

$$\Omega_n(z; \Lambda) = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}},$$

and for each pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Omega_{m,n}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w :

$$\Omega_{m,n}(z, w; \Lambda) = \frac{\sigma(mz + nw; \Lambda)}{\sigma(z; \Lambda)^{m^2 - mn} \sigma(z + w; \Lambda)^{mn} \sigma(w; \Lambda)^{n^2 - mn}}.$$

Remark 3.2. Compare the proof of [Lemma 4.5](#) to this definition.

Proposition 3.3. Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . The functions $\Omega_{\mathbf{v}}$ are elliptic functions in each variable.

Proof. Let $\omega \in \Lambda$. We show the function is elliptic in the first variable. Let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ and $\mathbf{z} = (z_1, \dots, z_n)$, $\mathbf{w} = (\omega, 0, \dots, 0) \in \mathbb{C}^n$. Using [\(15\)](#), we calculate

$$\frac{\Omega_{\mathbf{v}}(\mathbf{z} + \mathbf{w}; \Lambda)}{\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda)} = \frac{\lambda(v_1 \omega)}{\lambda(\omega) v_1^2} = 1$$

where the last equality holds because λ is a quadratic form. Thus $\Omega_{\mathbf{v}}$ is invariant under adding a period to the variable z_1 . Similarly $\Omega_{\mathbf{v}}$ is elliptic in each variable on $(\mathbb{C}/\Lambda)^n$. □

Proposition 3.4. Fix a lattice $\Lambda \in \mathbb{C}$. Let $\mathbf{v} \in \mathbb{Z}^m$ and $\mathbf{z} \in \mathbb{C}^n$. Let T be an $n \times m$ matrix with entries in \mathbb{Z} and transpose T^{tr} . Then

$$\Omega_{\mathbf{v}}(T^{tr}(\mathbf{z}); \Lambda) = \frac{\Omega_{T(\mathbf{v})}(\mathbf{z}; \Lambda)}{\prod_{i=1}^n \Omega_{T(\mathbf{e}_i)}(\mathbf{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \leq i < j \leq n} \Omega_{T(\mathbf{e}_i + \mathbf{e}_j)}(\mathbf{z}; \Lambda)^{v_i v_j}}$$

Proof. A straightforward calculation using [Definition 3.1](#). □

Let \wp and ζ denote the usual Weierstrass functions.

Lemma 3.5.

$$(a) \quad \wp(u) - \wp(v) = -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}.$$

$$(b) \quad \wp(\mathbf{v} \cdot \mathbf{z}) - \wp(\mathbf{w} \cdot \mathbf{z}) = -\frac{\Omega_{\mathbf{v}+\mathbf{w}}(\mathbf{z})\Omega_{\mathbf{v}-\mathbf{w}}(\mathbf{z})}{\Omega_{\mathbf{v}}(\mathbf{z})^2\Omega_{\mathbf{w}}(\mathbf{z})^2}.$$

Proof. Part (a) is well-known; see [Chandrasekharan 1985], for example. Part (b) follows by direct calculation using Definition 3.1. \square

Lemma 3.6.

$$(a) \quad \zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) = \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)}.$$

$$(b) \quad \zeta(x+a+b) - \zeta(x+a) - \zeta(x+b) + \zeta(x) = \frac{\sigma(2x+a+b)\sigma(a)\sigma(b)}{\sigma(x+a+b)\sigma(x+a)\sigma(x+b)\sigma(x)}.$$

Proof. (a) Denote by f and g the two sides of the equation to be proved. Considered as functions of any one of x , a or b , these are elliptic functions. Suppose that $a, b \notin \Lambda$. Consider f and g as functions of x . The set of poles of f or g is $\{-a, -b\}$. The zeroes of g (the right-hand side) are at $-a-b$ and 0 . These are also zeroes of f , since ζ is an odd function. Hence $f = cg$ for some c not depending on x . Now define instead

$$F = (\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b))\sigma(x+a)\sigma(x+b),$$

$$G = \sigma(x+a+b)\sigma(x).$$

We have $F = c'G$ for some constant c' independent of x . Taking derivatives and evaluating at $x = 0$, we have

$$(\wp(b) - \wp(a))\sigma(a)\sigma(b) = c'\sigma(a+b)\sigma'(0)$$

We have $\sigma'(0) = 1$. By Lemma 3.5, we then have

$$c' = -\frac{\sigma(a-b)}{\sigma(a)\sigma(b)}$$

which concludes the proof of (a). Part (b) is obtained by a change of variables $x \leftarrow a$, $a \leftarrow x+b$, $b \leftarrow x$. \square

Forming the elliptic net.

Theorem 3.7. Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E . Fix $z_1, \dots, z_n \in \mathbb{C}$. Then the function $W : \mathbb{Z}^n \rightarrow \mathbb{C}$ defined by

$$W(\mathbf{v}) = \Omega_{\mathbf{v}}(z_1, \dots, z_n; \Lambda)$$

is an elliptic net.

Proof. For notational simplicity, we drop the arguments z_i , Λ on Ω_v and also write $\sigma(\mathbf{v})$, $\wp(\mathbf{v})$ and $\zeta(\mathbf{v})$ for $\sigma(v_1z_1 + \cdots + v_nz_n)$, $\wp(v_1z_1 + \cdots + v_nz_n)$ and $\zeta(v_1z_1 + \cdots + v_nz_n)$. We observe that $\mathbf{v} = \mathbf{0}$ if and only if $\Omega_v \equiv 0$.

We intend to show that (3) holds for W in \mathbf{p} , \mathbf{q} , \mathbf{r} and \mathbf{s} . If any one of \mathbf{p} , \mathbf{q} or \mathbf{r} are zero, then (3) holds trivially (note that σ is an odd function, so that $\Omega_{-\mathbf{v}} = -\Omega_v$). Hence we may assume that none of Ω_p , Ω_q , or Ω_r is identically zero. For any quadratic form f defined on \mathbb{Z}^n , we have the following relation for all $\mathbf{p}, \mathbf{q}, \mathbf{s} \in \mathbb{Z}^n$:

$$f(\mathbf{p} + \mathbf{q} + \mathbf{s}) + f(\mathbf{p} - \mathbf{q}) + f(\mathbf{s}) - f(\mathbf{p} + \mathbf{s}) - f(\mathbf{p}) - f(\mathbf{q} + \mathbf{s}) - f(\mathbf{q}) = 0. \tag{16}$$

First we address the case that $\mathbf{s} = \mathbf{0}$. By (16) and Lemma 3.5,

$$\frac{\Omega_{\mathbf{p}+\mathbf{q}}\Omega_{\mathbf{p}-\mathbf{q}}}{\Omega_{\mathbf{p}}^2\Omega_{\mathbf{q}}^2} = \frac{\sigma(\mathbf{p} + \mathbf{q})\sigma(\mathbf{p} - \mathbf{q})}{\sigma(\mathbf{p})^2\sigma(\mathbf{q})^2} = \wp(\mathbf{q}) - \wp(\mathbf{p}).$$

Therefore, we have

$$\frac{\Omega_{\mathbf{p}+\mathbf{q}}\Omega_{\mathbf{p}-\mathbf{q}}}{\Omega_{\mathbf{p}}^2\Omega_{\mathbf{q}}^2} + \frac{\Omega_{\mathbf{q}+\mathbf{r}}\Omega_{\mathbf{q}-\mathbf{r}}}{\Omega_{\mathbf{q}}^2\Omega_{\mathbf{r}}^2} + \frac{\Omega_{\mathbf{r}+\mathbf{p}}\Omega_{\mathbf{r}-\mathbf{p}}}{\Omega_{\mathbf{r}}^2\Omega_{\mathbf{p}}^2} = 0,$$

which gives the relation (3) for $\mathbf{s} = \mathbf{0}$, that is,

$$\Omega_{\mathbf{p}+\mathbf{q}}\Omega_{\mathbf{p}-\mathbf{q}}\Omega_{\mathbf{r}}^2 + \Omega_{\mathbf{q}+\mathbf{r}}\Omega_{\mathbf{q}-\mathbf{r}}\Omega_{\mathbf{p}}^2 + \Omega_{\mathbf{r}+\mathbf{p}}\Omega_{\mathbf{r}-\mathbf{p}}\Omega_{\mathbf{q}}^2 = 0.$$

Now suppose that $\mathbf{s} \neq \mathbf{0}$ and so $\Omega_s \neq 0$. By (16) and Lemma 3.6,

$$\begin{aligned} \frac{\Omega_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{p}-\mathbf{q}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{p}}\Omega_{\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{q}}} &= \frac{\sigma(\mathbf{p} + \mathbf{q} + \mathbf{s})\sigma(\mathbf{p} - \mathbf{q})\sigma(\mathbf{s})}{\sigma(\mathbf{p} + \mathbf{s})\sigma(\mathbf{p})\sigma(\mathbf{q} + \mathbf{s})\sigma(\mathbf{q})} \\ &= \zeta(\mathbf{p} + \mathbf{s}) - \zeta(\mathbf{p}) - \zeta(\mathbf{q} + \mathbf{s}) + \zeta(\mathbf{q}). \end{aligned}$$

Therefore, we have

$$\frac{\Omega_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{p}-\mathbf{q}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{p}}\Omega_{\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{q}}} + \frac{\Omega_{\mathbf{q}+\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{q}-\mathbf{r}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{q}}\Omega_{\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{r}}} + \frac{\Omega_{\mathbf{r}+\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{r}-\mathbf{p}}\Omega_{\mathbf{s}}}{\Omega_{\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{r}}\Omega_{\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{p}}} = 0,$$

or, more simply,

$$\Omega_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{p}-\mathbf{q}}\Omega_{\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{r}} + \Omega_{\mathbf{q}+\mathbf{r}+\mathbf{s}}\Omega_{\mathbf{q}-\mathbf{r}}\Omega_{\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{p}} + \Omega_{\mathbf{r}+\mathbf{p}+\mathbf{s}}\Omega_{\mathbf{r}-\mathbf{p}}\Omega_{\mathbf{q}+\mathbf{s}}\Omega_{\mathbf{q}} = 0,$$

which is what was required to prove. □

The identity (3) for Ω_v is similar to several identities known in complex function theory [Gasper and Rahman 2004; Wenchang et al. 1996].

Explicit rational functions. Elliptic functions for a lattice Λ of \mathbb{C} give rational functions on the associated elliptic curve (via complex uniformization). If we give a Weierstrass model for the same elliptic curve, we can give explicit expressions for the rational functions as elements of the usual field of rational functions associated to the model. In the following proposition, we do this for $\Omega_{\mathbf{v}}$ for some small $\mathbf{v} \in \mathbb{Z}^n$, for $n = 1, 2, 3$.

Proposition 3.8. *Consider an elliptic curve E , and a Weierstrass model for E given by*

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

As usual, let

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & b_4 &= 2a_4 + a_1a_3, & b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

To E we can also associate a complex uniformization and elliptic functions $\Omega_{\mathbf{v}}$ as above. As rational functions on E , we have the following equalities.

For $n = 1$:

$$\begin{aligned} \Omega_1 &= 1, & \Omega_2 &= 2y + a_1x + a_3, \\ \Omega_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, & cr\Omega_4 &= (2y + a_1x + a_3) \\ & & & (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2). \end{aligned}$$

For $n = 2$:

$$\begin{aligned} \Omega_{(1,0)} &= \Omega_{(0,1)} = \Omega_{(1,1)} = 1, \\ \Omega_{(1,-1)} &= x_2 - x_1, & \Omega_{(-1,1)} &= x_1 - x_2, \\ \Omega_{(2,1)} &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2, \\ \Omega_{(1,2)} &= x_1 + 2x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2. \end{aligned}$$

For $n = 3$:

$$\begin{aligned} \Omega_{(1,0,0)} &= \Omega_{(0,1,0)} = \Omega_{(0,0,1)} = \Omega_{(1,1,0)} = \Omega_{(0,1,1)} = \Omega_{(1,0,1)} = 1, \\ \Omega_{(1,-1,0)} &= x_2 - x_1, & \Omega_{(0,1,-1)} &= x_3 - x_2, & \Omega_{(-1,0,1)} &= x_1 - x_3, \\ \Omega_{(-1,1,0)} &= x_1 - x_2, & \Omega_{(0,-1,1)} &= x_2 - x_3, & \Omega_{(1,0,-1)} &= x_3 - x_1, \\ \Omega_{(1,1,1)} &= \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)}, \end{aligned}$$

$$\begin{aligned} \Omega_{(-1,1,1)} &= \frac{y_1(x_2 - x_3) - y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_2 - x_3)} + a_1x_1 + a_3, \\ \Omega_{(1,-1,1)} &= \frac{-y_1(x_2 - x_3) + y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_3 - x_1)} + a_1x_2 + a_3, \\ \Omega_{(1,1,-1)} &= \frac{-y_1(x_2 - x_3) - y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)} + a_1x_3 + a_3. \end{aligned}$$

Proof. The division polynomial formulae (the $n = 1$ case) are well-known; see [Chandrasekharan 1985], [Frey and Lange 2006, p. 80], or [Silverman 2009, Exercise 3.7]. The formulae for $n = 2$ and the related first three lines of formulae for $n = 3$ are immediate consequences of Lemma 3.5 and the addition law for elliptic curves [Silverman 2009, Algorithm 2.3]. Only the cases where $n = 3$, $v_i \neq 0$ for all $i = 1, 2, 3$ are not immediate: these formulae are a result of the proof of Lemma 2.6. Note that using Remark 2.7 results in the same formulae. \square

4. Net polynomials over arbitrary fields

In the last section, we defined elliptic functions Ω_v in the case of \mathbb{C}/Λ . In this section we wish to define the same rational functions for any elliptic curve over any field, calling them Ψ_v , the *net polynomials*. We will start from the results of the last section.

Defining net polynomials. Let $R = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$ be a polynomial ring over \mathbb{Q} in the variables α_i . Define $f(x, y) \in R[x, y]$ by

$$f(x, y) = y^2 + \alpha_1xy + \alpha_3y - x^3 - \alpha_2x^2 - \alpha_4x - \alpha_6.$$

Consider the affine scheme $\mathcal{E} : f(x, y) = 0$ over R . Let $\mathbf{a} = (a_i) \in \mathbb{C}^5$. The association $(\alpha_i) \mapsto (a_i)$ gives a map $\phi_{\mathbf{a}} : R \rightarrow \mathbb{C}$. Consider the affine variety over \mathbb{C} given by

$$C_{\mathbf{a}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $\phi_{\mathbf{a}}$ gives rise to a Cartesian diagram

$$\begin{array}{ccc} \mathcal{E}^n & \longleftarrow & C_{\mathbf{a}}^n \\ \downarrow & & \downarrow \\ \text{Spec}(R) & \longleftarrow & \text{Spec}(\mathbb{C}) \end{array}$$

where $\mathcal{E}^n = \mathcal{E} \times_{\text{Spec } R} \cdots \times_{\text{Spec } R} \mathcal{E}$ is the n -fold fibre product of \mathcal{E} with itself over R .

The rational functions $\Omega_v \in \mathcal{K}(C_{\mathbf{a}}^n)$ have rational expressions in x, y and the a_i (in terms of the Weierstrass model, as in for example Proposition 3.8). These expressions have rational coefficients by construction and the general theory of

sigma functions (the divisors are Galois invariant). So these same expressions (with a_i replaced with α_i) give rational functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$.

Theorem 4.1. *Let $n \geq 1$. Denote by $\mathcal{K}(\mathcal{E}^n)$ the field of rational functions on \mathcal{E}^n . There exists a unique system of functions $\Psi_{\mathbf{v}} \in \mathcal{K}(\mathcal{E}^n)$ depending on $\mathbf{v} \in \mathbb{Z}^n$ such that*

(a) *the map*

$$W : \mathbb{Z}^n \rightarrow \mathcal{K}(\mathcal{E}^n), \quad \mathbf{v} \mapsto \Psi_{\mathbf{v}}$$

is an elliptic net, and

(b) *whenever C_a is elliptic, the restriction of $\Psi_{\mathbf{v}}$ to a fibre C_a^n is the rational function $\Omega_{\mathbf{v}}$ on C_a^n .*

Proof. The union of the C_a^n for which C_a is an elliptic curve is Zariski dense, and so the $\Psi_{\mathbf{v}}$ are determined uniquely by their restrictions to these fibres. \square

We call these $\Psi_{\mathbf{v}}$ the *net polynomials*; we will discuss shortly the “polynomial” ring \mathcal{R}_n in which they live.

We transfer some useful properties of the $\Omega_{\mathbf{v}}$ to properties of the $\Psi_{\mathbf{v}}$ on \mathcal{E}^n . Again, there are unique rational functions X and Y for \mathcal{E} whose restriction to elliptic C_a correspond to the Weierstrass functions \wp and $\frac{1}{2}\wp'$. Each $\mathbf{v} \in \mathbb{Z}^n$ gives rise to a map $\mathbf{v} : \mathcal{E}^n \rightarrow \mathcal{E}$ which is the linear combination associated to the vector \mathbf{v} (e.g., $(1, 1)$ is the usual group law). Define rational functions $X_{\mathbf{v}} = X \circ \mathbf{v}$ and $Y_{\mathbf{v}} = Y \circ \mathbf{v}$ on \mathcal{E}^n .

The next lemma follows immediately from [Lemma 3.5](#).

Lemma 4.2.
$$\Psi_{\mathbf{v}}^2 \Psi_{\mathbf{w}}^2 (X_{\mathbf{v}} - X_{\mathbf{w}}) = -\Psi_{\mathbf{v}+\mathbf{w}} \Psi_{\mathbf{v}-\mathbf{w}}.$$

More generally, there is a map $T : \mathcal{E}^m \rightarrow \mathcal{E}^n$ associated to any $T \in M_{n \times m}(\mathbb{Z})$. The next proposition follows from [Proposition 3.4](#).

Proposition 4.3. *Let $\mathbf{v} \in \mathbb{Z}^n$. Let T be any $n \times m$ matrix with entries in \mathbb{Z} and transpose T^{tr} . Then*

$$(\Psi_{\mathbf{v}} \circ T) \prod_{i=1}^n \Psi_{T^{tr}(\mathbf{e}_i)}^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{1 \leq i < j \leq n} \Psi_{T^{tr}(\mathbf{e}_i + \mathbf{e}_j)}^{v_i v_j} = \Psi_{T^{tr}(\mathbf{v})}. \quad (17)$$

Net polynomials at primes. In this section we determine a little more about the exact nature of the elliptic net $\Psi_{\mathbf{v}}$. In particular, we wish to restrict the possible divisor of $\Psi_{\mathbf{v}}$, and show that it has zero valuation for certain primes.

Consider the ring $S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6]$. Since $f(x, y)$ is defined over S , we may define $\mathcal{E}_S : f(x, y) = 0$ as a scheme over $\text{Spec } S$ whose fibre over $\text{Spec } R$ is

\mathcal{E} . Then $\mathcal{E}_S^n = \mathcal{E}_S \times_{\text{Spec } S} \cdots \times_{\text{Spec } S} \mathcal{E}_S$ is a scheme over $\text{Spec } S$ whose fibre over $\text{Spec } R$ is \mathcal{E}^n . Define

$$\mathcal{R}_n = S[x_i, y_i]_{1 \leq i \leq n} \left[(x_i - x_j)^{-1} \right]_{1 \leq i < j \leq n} / \langle f(x_i, y_i) \rangle_{1 \leq i \leq n}.$$

The ring \mathcal{R}_n is the affine coordinate ring of the affine piece of \mathcal{E}_S^n obtained by removing all the diagonals and antidiagonals, in the sense of the elliptic curve group law (in other words, on an elliptic curve fibre, $x_i = x_j$ if and only if the corresponding points satisfy $P_i = \pm P_j$). There is a natural identification of \mathcal{R}_n with a subset of $\mathcal{H}(\mathcal{E}^n)$.

Theorem 4.4. *The functions Ψ_v are elements of \mathcal{R}_n . Let \mathfrak{p} be any prime of \mathcal{R}_n which is a lift of a prime of S . Then $\Psi_v \notin \mathfrak{p}$.*

The lifted ideal $\mathfrak{p} = \mathfrak{q}\mathcal{R}_n$ is prime whenever \mathfrak{q} is a prime of S . The proof of the theorem will involve showing for all valuations v associated to such primes \mathfrak{p} that $v(\Psi_v)$ (slightly modified) is a quadratic form with certain vanishing. Then the following lemma will establish that this function is identically zero.

Let B and C be abelian groups written additively. The function $f : B \rightarrow C$ is a *quadratic form* if for all $x, y, z \in B$,

$$f(x + y + z) - f(x + y) - f(y + z) - f(x + z) + f(x) + f(y) + f(z) = 0.$$

If f is a quadratic form, then for all $x, y \in B$,

$$f(x + y) + f(x - y) - 2f(x) - 2f(y) = 0.$$

The converse holds if C is 2-torsion free.

Lemma 4.5. *Let $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a quadratic form. Suppose that $M(\mathbf{v}) = 0$ for all $\mathbf{v} = \mathbf{e}_i$ and $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ (i.e., for standard basis vectors and their two-term sums). Then $M(\mathbf{v}) = 0$ for all \mathbf{v} .*

Proof. It is well-known that any value of a quadratic form can be given in terms of its value at a certain “base” of vectors. In particular,

$$f\left(\sum_{i=1}^n a_i \mathbf{e}_i\right) = \sum_{i=1}^n \left(2a_i^2 - \sum_{j=1}^n a_i a_j\right) f(\mathbf{e}_i) + \sum_{1 \leq i < j \leq n} a_i a_j f(\mathbf{e}_i + \mathbf{e}_j). \quad \square$$

Proof of Theorem 4.4. Each $\Psi_v \in \mathcal{H}(\mathcal{E}^n)$ has a corresponding Weil divisor. Suppose a codimension-one subscheme X appears as a summand in this divisor, and let $\tilde{X} = X \cap C_a^n$. If C_a is elliptic, $\tilde{X} \neq \emptyset$, and $\tilde{X} \neq C_a^n$, then \tilde{X} is of codimension one in C_a^n and appears in the divisor of Ω_v to the same order as X appears in the divisor of Ψ_v . [Definition 3.1](#) determines the divisors of Ω_v and this restricts the possible divisors for Ψ_v . In particular, it shows that $s\Psi_v \in \mathcal{R}_n$, where $s \in S$.

Therefore, taking v to be a valuation of \mathcal{R}_n lifted from a valuation of S associated to a prime \mathfrak{q} of S , it will suffice to show that $v(\Psi_v) = 0$ for all $v \in \mathbb{Z}^n$.

[Lemma 4.2](#) implies

$$X_v - X_w = -\frac{\Psi_{v+w}\Psi_{v-w}}{\Psi_v^2\Psi_w^2}.$$

We claim that $v(X_v - X_w) = 0$ whenever $v \neq \pm w$, $v \neq 0$, and $w \neq 0$.

First suppose $v(X_v - X_w) < 0$; we show that $v = 0$ or $w = 0$. Indeed, we know that $v(X_v) < 0$ or $v(X_w) < 0$. Suppose $v(X_v) < 0$. This implies that $v(\mathbf{P}) = \mathbb{O}$ for all \mathbf{P} on the nonsingular part of the fibre over \mathfrak{q} of \mathcal{E}_S . Since \mathbf{P} ranges over all possible values (e.g., $\mathbf{P} = (P, \mathbb{O}, \dots, \mathbb{O})$), we find that this implies that $[v_i] = [0]$ for all i . In turn, this shows that $v = 0$. Similarly, if $v(X_w) < 0$, then $w = 0$.

Next suppose $v(X_v - X_w) > 0$; we show that $v = \pm w$. Suppose the valuation is positive. Then $v(\mathbf{P}) = \pm w(\mathbf{P})$ for all \mathbf{P} on the nonsingular part of the fibre over \mathfrak{q} of \mathcal{E}_S . Since \mathbf{P} ranges over all possible values (e.g., $\mathbf{P} = (P, \mathbb{O}, \dots, \mathbb{O})$ or $\mathbf{P} = (P, P, \mathbb{O}, \dots, \mathbb{O})$), we find that this implies, in particular, that for all $0 \leq i \leq j \leq n$, we have $[v_i \pm w_i] = [0]$ and $[v_i + v_j \pm (w_i + w_j)] = [0]$ on \mathcal{E}_S . In turn, this gives $v_i = \pm w_i$ and $v_i + v_j = \pm(w_i + w_j)$. Together these imply that $v = \pm w$. This demonstrates the claim.

Define a function $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ by

$$M(v) = \begin{cases} v(\Psi_v) & \text{if } v \neq 0, \\ 0 & \text{if } v = 0. \end{cases}$$

Note that $M(-v) = M(v)$, from which one can deduce that

$$M(v+w) + M(v-w) - 2M(v) - 2M(w) = 0 \tag{18}$$

whenever $v = 0$ or $w = 0$. Our work up until now has shown that (18) holds in all other cases except $v+w = 0$ or $v-w = 0$. These remaining two cases reduce to the statement that for all u , $M(2u) = 4M(u)$. To obtain this, take the sum of the four instances of (18) with (v, w) respectively taking the values $(4u, u)$, $(3u, u)$, $(3u, u)$ and $(2u, u)$, and then subtract the instance of (18) with $(v, w) = (3u, 2u)$.

We have shown that (18) holds for all v and w , and that therefore $M : \mathbb{Z}^n \rightarrow \mathbb{Z}$ is a quadratic form (since \mathbb{Z} is 2-torsion free). The other assumptions of [Lemma 4.5](#) are verified by [Proposition 3.8](#). Therefore, M is identically zero, which is what was required to prove. \square

Summary. Let $n \geq 1$. For any elliptic curve or scheme C , let \mathbb{O} denote the identity, $[m] : C \rightarrow C$ denote multiplication by m , $p_i : C^n \rightarrow C$ denote projection onto the i -th component, and $s : C^n \rightarrow C$ denote sum of all components. For $v \in \mathbb{Z}^n$, define

the expression

$$D_{C, \mathbf{v}} = ([v_1] \times \cdots \times [v_n])^* s^*(\mathbb{O}) - \sum_{1 \leq k < j \leq n} v_k v_j (p_k^* \times p_j^*) s^*(\mathbb{O}) - \sum_{k=1}^n \left(2v_k^2 - \sum_{j=1}^n v_k v_j \right) p_k^*(\mathbb{O}),$$

which is a divisor on the n -fold product C^n . Over the complex numbers, the functions $\Omega_{\mathbf{v}}$ have these divisors and satisfy the elliptic net recurrence (3) (see Section 3).

We now collect the results of the previous sections in one statement.

Theorem 4.6. *Let $n \geq 1$. There exists a unique collection of rational functions $\Psi_{\mathbf{v}} \in \mathcal{H}(\mathcal{E}_S^n)$ for each $\mathbf{v} \in \mathbb{Z}^n$ satisfying these conditions:*

- (a) *The map $\mathbf{v} \mapsto \Psi_{\mathbf{v}}$ gives an elliptic net $W : \mathbb{Z}^n \rightarrow \mathbb{R}_n$.*
- (b) *$\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v} = \mathbf{e}_i$ for some $1 \leq i \leq n$ or $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ for some $1 \leq i < j \leq n$.*
- (c) *$\text{Div}(\Psi_{\mathbf{v}}) = D_{\mathcal{E}_S, \mathbf{v}}$.*

Proof. Part (a) follows from Theorems 4.1 and 4.4. Part (b) follows from Proposition 3.8 and Theorem 4.1. Part (c) follows from Theorem 4.4. □

5. Elliptic nets from elliptic curves

In light of Theorem 4.6, it is now natural to define an elliptic net associated to any cubic Weierstrass curve over any field.

Definition 5.1. Let K be any field. Let $a_1, a_2, a_3, a_4, a_6 \in K$. To this we associate a map

$$S = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6] \rightarrow K, \quad \alpha_i \mapsto a_i.$$

Let

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

and let C be a curve defined by $f(x, y) = 0$. Then we have a Cartesian diagram

$$\begin{array}{ccc} \mathcal{E}_S^n & \longleftarrow & C^n \\ \downarrow & & \downarrow \\ \text{Spec}(S) & \longleftarrow & \text{Spec}(K) \end{array}$$

under which we may pullback $\Psi_{\mathbf{v}}$ to obtain $\phi_{\mathbf{v}} \in \mathcal{H}(C^n)$ (this is possible since the fibre on the right is not contained in the support of the divisor of $\Psi_{\mathbf{v}}$, by Theorem 4.6).

The nonsingular points of C defined over K , denoted $C_{\text{ns}}(K)$, form a group. We call a set of points $\{P_1, \dots, P_n\}$ on the nonsingular part C_{ns} of a cubic curve *appropriate* if

- (a) $P_i \neq 0$ for all i ,
- (b) $[2]P_i \neq 0$ for all i ,
- (c) $P_i \neq \pm P_j$ for any $i \neq j$, and (d) $[3]P_1 \neq 0$ whenever $n = 1$.

If we have an appropriate n -tuple of points $\mathbf{P} \in C_{\text{ns}}(K)^n$, we may define a map

$$W_{C,\mathbf{P}} : \mathbb{Z}^n \rightarrow K$$

by setting $W_{C,\mathbf{P}}(\mathbf{v}) = \phi_{\mathbf{v}}(\mathbf{P})$. By [Theorem 4.6](#), this will be an elliptic net. This will be called *the elliptic net associated to C and \mathbf{P}* .

We have the following additional corollary to [Theorem 4.6](#).

Corollary 5.2. *For an elliptic net $W_{C,\mathbf{P}} : \mathbb{Z}^n \rightarrow K$ associated to a curve C and nonsingular points \mathbf{P} , we have $W(\mathbf{v}) = 0$ if and only if $\mathbf{v}(\mathbf{P}) = \mathbb{O}$ on C_{ns} .*

Proof. This follows from the statement that $\Omega_{\mathbf{v}}(\mathbf{v} \cdot \mathbf{z}) = 0$ if and only if $\mathbf{v} \cdot \mathbf{z} \in \Lambda$ (see [Section 3](#)). □

Example 5.3. In [\(4\)](#) (page 201) we displayed an example elliptic net $W_{E,(P,Q)}$ associated to the elliptic curve and points

$$E : y^2 + y = x^3 + x^2 - 2x, \quad P = (0, 0), \quad Q = (1, 0)$$

Some of the smaller terms of this net can be calculated using [Proposition 3.8](#); for example,

$$\begin{aligned} W(0, 0) &= 0, & W(1, 0) &= W(0, 1) = W(1, 1) = 1, \\ W(2, 0) &= 2y_1 + a_1x_1 + a_3 = 1, & W(0, 2) &= 2y_2 + a_1x_2 + a_3 = 1, \\ & & W(1, -1) &= x_2 - x_1 = 1, \\ W(2, 1) &= 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2 = 2, \\ W(2, -1) &= (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 = -1. \end{aligned}$$

More terms can be calculated using the recurrence relation [\(3\)](#). Since P and Q are independent nontorsion points, there are no zeroes in the array except the zero located at the origin ($W(0, 0) = 0$). The row through the term 0 is the elliptic divisibility sequence associated to E and P , which begins

$$1, 1, -3, 11, 38, 249, -2357, 8767, 496035, -3769372, -299154043, \\ -12064147359, 632926474117, -65604679199921, \dots$$

The column through 0 is the elliptic divisibility sequence associated to Q .

6. Elliptic curves from elliptic nets

We are now in a position to use the results of [Section 2](#) to determine exactly which elliptic curves (or more generally cubic Weierstrass curves) give rise to any given elliptic net.

Scale equivalence and normalization.

Proposition 6.1. *Let $W : A \rightarrow K$ be an elliptic net. Let $f : A \rightarrow K^*$ be a quadratic form. Define $W^f : A \rightarrow K$ by*

$$W^f(v) = f(v)W(v).$$

Then W^f is an elliptic net.

Proof. Let $p, q, r, s \in A$. We use multiplicative notation in K^* , so that f satisfies

$$f(p + q + s)f(p)f(q)f(s)f(p + q)^{-1}f(q + s)^{-1}f(p + s)^{-1} = 1. \quad (19)$$

The parallelogram law for quadratic forms (written multiplicatively) states that

$$f(p - q)f(p + q) = f(p)^2f(q)^2. \quad (20)$$

Multiplying $f(r)f(r + s)$ and equations (19) and (20) together, we obtain

$$f(p + q + s)f(p - q)f(r + s)f(r) = f(q + s)f(p + s)f(r + s)f(p)f(q)f(r)f(s)^{-1},$$

which is symmetric in p, q , and r , so

$$\begin{aligned} f(p + q + s)f(p - q)f(r + s)f(r) &= f(q + r + s)f(q - r)f(p + s)f(p) \\ &= f(r + p + s)f(r - p)f(q + s)f(q), \end{aligned}$$

which shows that the recurrence (3) holds for W^f if it does for W . □

If two elliptic nets are related in the manner of W and W^f for some quadratic form f , then we call them *scale equivalent*. This is clearly an equivalence relation.

Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. We say that W is *normalized* if $W(e_i) = 1$ for all $1 \leq i \leq n$ and $W(e_i + e_j) = 1$ for all $1 \leq i < j \leq n$. An elliptic net arising from a curve and points is normalized. It should be stressed that the concept of *normalized* is only defined for elliptic nets with a preferred basis.

If any term of the form $W(e_i)$, $W(2e_i)$, $W(e_i + e_j)$, or $W(e_i - e_j)$ is zero (where $i \neq j$), or if $n = 1$ and any term of the form $W(3e_1)$ is zero, then we say that W is *degenerate*. Compare the definition of *degenerate* to the definition of *appropriate* in [Section 5](#).

Proposition 6.2. *If $W : \mathbb{Z}^n \rightarrow K$ is a nondegenerate elliptic net, there is exactly one scaling W^f which is normalized.*

Proof. Define

$$\begin{aligned}
 A_{ii} &= W(\mathbf{e}_i)^{-1}, \quad \text{for } 1 \leq i \leq n, \\
 A_{ij} &= \frac{W(\mathbf{e}_i)W(\mathbf{e}_j)}{W(\mathbf{e}_i + \mathbf{e}_j)}, \quad \text{for } 1 \leq i < j \leq n, \\
 f(\mathbf{v}) &= \prod_{1 \leq i \leq j \leq n} A_{ij}^{v_i v_j}.
 \end{aligned}$$

Then W^f is normalized. Uniqueness follows from the elementary properties of quadratic forms (as in the proof of [Lemma 4.5](#)). \square

The proof demonstrates that scale equivalence has $\binom{n+1}{2}$ degrees of freedom. If $W : \mathbb{Z}^n \rightarrow K$ is an elliptic net, then its *normalization* \tilde{W} is defined to be the unique normalized elliptic net which is a scaling of W . A *coordinate sublattice* of \mathbb{Z}^n is a sublattice of the form

$$\{\mathbf{v} \in \mathbb{Z}^n : v_i = 0 \text{ for } i \notin I\}$$

for some proper nonempty subset $I \subset \{1, 2, \dots, n\}$. The *rank* of the sublattice is the cardinality of I .

Curves from nets of ranks 1 and 2. Define a change of variables of a cubic curve in Weierstrass form to be *unihomothetic* if it is of the form

$$x' = x + r, \quad y' = y + sx + t, \tag{21}$$

for some r, s and t .

The rank-one result in the following form is due to Christine Swart.

Proposition 6.3 [[Swart 2003](#), Theorem 4.5.3]. *Let $W : \mathbb{Z} \rightarrow K$ be a normalized nondegenerate elliptic net. Then the family of curve-point pairs (C, P) such that $W = W_{C,P}$ is three dimensional. These are the curve and nonsingular point*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad P = (0, 0),$$

where

$$\begin{aligned}
 a_1 &= \frac{W(4) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)}, \\
 a_2 &= \frac{W(2)W(3)^2 + (W(4) + W(2)^5) - W(2)W(3)}{W(2)^3W(3)}, \\
 a_3 &= W(2), \quad a_4 = 1, \quad a_6 = 0,
 \end{aligned}$$

or any image of these under a unihomothetic change of coordinates.

Proof. A normalized rank 1 nondegenerate elliptic net has $W(2) \neq 0$ and $W(3) \neq 0$. Any singular point $P = (x, y)$ on a cubic Weierstrass curve has vanishing partial derivatives, which implies that $\Psi_2(P) = 2y + a_1x + a_3 = 0$ (see [Proposition 3.8](#)). Therefore, if any curve and singular point gives rise to W , then $W(2) = 0$, in contradiction to nondegeneracy. The division polynomials Ψ_1, Ψ_2, Ψ_3 and Ψ_4 are invariant under a change of coordinates of the form (21). Then, it is a simple calculation to check that $W_{C,P}$ agrees with W at the first four terms; hence $W_{C,P} = W$ by [Theorem 2.2](#). Conversely, suppose $W = W_{C',P'}$. After applying a transformation of the form (21) taking P' to $(0, 0)$ and taking a_4 to 1, substitution of the division polynomials into the equations above verifies that $a'_i = a_i$ for all i . \square

Proposition 6.4. *Let $W : \mathbb{Z}^2 \rightarrow K$ be a normalized nondegenerate elliptic net. Then the family of 3-tuples (C, P_1, P_2) such that $W = W_{C,P_1,P_2}$ is three dimensional. These are the curve and nonsingular points*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$$P_1 = (0, 0), \quad P_2 = (W(1, 2) - W(2, 1), 0),$$

with

$$a_1 = \frac{W(2, 0) - W(0, 2)}{W(2, 1) - W(1, 2)}, \quad a_2 = 2W(2, 1) - W(1, 2), \quad a_3 = W(2, 0),$$

$$a_4 = (W(2, 1) - W(1, 2))W(2, 1), \quad a_6 = 0,$$

or any image of these under a unihomothetic change of coordinates.

Proof. In a normalized nondegenerate elliptic net,

$$W(2, 1) - W(1, 2) = W(1, -1) \neq 0, \quad W(2, 0) \neq 0, \quad W(0, 2) \neq 0$$

(see [Theorem 2.5](#)). Thus (as in the previous theorem) if a curve and points give rise to W , then the points are nonsingular. The formulae for $W(2, 0)$, $W(0, 2)$, $W(2, 1)$ and $W(1, 2)$ are invariant under a change of coordinates of the form (21). The net W_{C,P_1,P_2} agrees with W at the terms $(2, 0)$, $(0, 2)$, $(2, 1)$ and $(1, 2)$; hence $W_{C,P_1,P_2} = W$ by [Theorem 2.5](#). Conversely, suppose $W = W_{C',P'_1,P'_2}$. After applying a unihomothetic transformation taking P'_1 to $(0, 0)$ and P'_2 to $(W(1, 2) - W(2, 1), 0)$, substitution of the net polynomials into the equations above verifies that $a'_i = a_i$ for all i . \square

Example 6.5. Plugging terms from the elliptic net of (4) into the formulae in the statement of [Proposition 6.4](#) we recover the corresponding E , P , and Q .

Remark 6.6. A more symmetric set of equations in the case of characteristic not equal to 2 is as follows:

$$P_1 = (v, 0), \quad P_2 = (-v, 0), \quad 2v = W(2, 1) - W(1, 2),$$

$$\begin{aligned}
 a_1 &= \frac{W(2, 0) - W(0, 2)}{W(2, 1) - W(1, 2)}, & 2a_2 &= W(2, 1) + W(1, 2), \\
 2a_3 &= W(2, 0) + W(0, 2), & 4a_4 &= -(W(2, 1) - W(1, 2))^2, \\
 8a_6 &= -(W(2, 1) - W(1, 2))^2(W(2, 1) + W(1, 2)).
 \end{aligned}$$

Curves from nets in general rank.

Theorem 6.7. *Let $n \geq 1$. Let $W : \mathbb{Z}^n \rightarrow K$ be a normalized nondegenerate elliptic net. Then the set of curves C and $\mathbf{P} \in C^n$ such that $W = W_{C, \mathbf{P}}$ forms a three-dimensional family of tuples (C, \mathbf{P}) . Further, none of the points $P \in \mathbf{P}$ are singular. In particular, the family consists of one such tuple and all its images under unihomothetic changes of coordinates.*

Proof. The proof is by strong induction on n , where the inductive statement has two parts:

- (I) The theorem holds for n .
- (II) $W(\mathbf{v}) \neq 0$ for some $\mathbf{v} \in \{\pm 1\}^n$.

The base case consists of ranks $n = 1, 2$. Part (I) is by Propositions 6.3 and 6.4; part (II) is by nondegeneracy, which implies $W(\mathbf{e}_1) \neq 0$ and $W(\mathbf{e}_1 + \mathbf{e}_2) \neq 0$.

Suppose $n \geq 3$ and the inductive statement holds for all $k < n$. Let W_1, \dots, W_n be the normalized elliptic subnets of W associated to the rank $n - 1$ coordinate sublattices $L_i = \{\mathbf{v} : v_i = 0\}$. These are defined as nets $W_i : L_i \rightarrow K$ but they can be identified with nets $W'_i : \mathbb{Z}^{n-1} \rightarrow K$ in the obvious way (by deleting the zero coordinate). They are normalized and nondegenerate (by definition, nondegeneracy at rank n implies nondegeneracy on rank $n - 1$ sublattices for $n > 2$). By part (I) the inductive hypothesis, we have $W'_i = W_{C_i, \mathbf{P}_i}$ for some curves C_i and nonsingular points $\mathbf{P}_i \in C_i^{n-1}$.

We observe a consequence of Proposition 4.3. Suppose $V_1 : \mathbb{Z}^m \rightarrow K$ is an elliptic net of rank m associated to C and \mathbf{P} . Also suppose

$$V_2 : \{\mathbf{v} \in \mathbb{Z}^m : v_m = 0\} \rightarrow K$$

is the elliptic subnet of V_1 associated to the coordinate sublattice of rank $m - 1$ which consists of vectors with last coordinate zero. Suppose $V'_2 : \mathbb{Z}^{m-1} \rightarrow K$ is naturally identified with V_2 by simply deleting the last coordinate of the domain. Then V'_2 is associated to C and \mathbf{P}' where \mathbf{P}' is simply \mathbf{P} with the last coordinate deleted. This statement, appropriately adjusted, holds for any coordinate hyperplane (not just the one with last coordinate zero).

Consider two of the rank $n - 1$ subnets, say W_i and W_j . Let $W_{ij} = W_i \cap W_j$ in W . Define $W'_{ij} : \mathbb{Z}^{n-2} \rightarrow K$ by the obvious identification. Then, $W'_{ij} = W_{C_{ij}, \mathbf{P}_{ij}}$ for some curve C_{ij} and $\mathbf{P}_{ij} \in C_{ij}^{n-2}$. By the foregoing, $C_i = C_j = C_{ij}$, \mathbf{P}_{ij} is just \mathbf{P}_j

with the i -th coordinate deleted, and \mathbf{P}_{ij} is just \mathbf{P}_i with the $(j - 1)$ -th coordinate deleted.

Considering every such pair, we may define a candidate curve C by $C = C_i$ for all i and $\mathbf{P} \in C^n$ defined as the unique n -tuple which results in \mathbf{P}_i upon deleting the i -th coordinate. By the foregoing, this is well-defined. Now we see that W agrees with $W_{C, \mathbf{P}}$ on all coordinate sublattices of rank $n - 1$. By part (II) of the inductive hypothesis and Theorem 2.8, we see that W is determined by its sublattices of rank $n - 1$. Therefore $W = W_{C, \mathbf{P}}$.

To show part (II) of the inductive statement, we observe that if $W(\mathbf{v}) = 0$ for all $\mathbf{v} \in \{\pm 1\}^n$, then $\mathbf{v}(\mathbf{P}) = \mathbb{O}$ for all such \mathbf{v} (by Corollary 5.2). But this is impossible, since it would imply $[2]P_i = \mathbb{O}$ for $1 \leq i \leq n$, a contradiction to nondegeneracy (again Corollary 5.2).

A change of coordinates of the form (21) for C does not change the elliptic net, as it is determined by its values on its coordinate hyperplanes, where this is true. Further, if two tuples *not* related by such a change of coordinates generate the same net W , then the same would hold for some coordinate hyperplane, a contradiction. This demonstrates part (I) of the inductive statement. □

7. The curve-net theorem

We set some remaining terminology, and then proceed to the statement and proof of the main theorem.

Homothety and singular elliptic nets. The only changes of coordinates of a Weierstrass equation into another are compositions of unihomothetic changes of coordinates and changes of coordinates of the form $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$, which we refer to as *homotheties* (since they correspond to homotheties of the lattice in the complex uniformization).

Proposition 7.1. *Consider the rank n elliptic net $W_{C, \mathbf{P}}$ associated to*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

defined over K and $\mathbf{P} \in C(K)^n$. Let λ be a nonzero element of K . Suppose $\phi_\lambda : C \rightarrow C_\lambda$ is the isomorphism of curves taking C to

$$C_\lambda : y^2 + \lambda a_1xy + \lambda^3 a_3y = x^3 + \lambda^2 a_2x^2 + \lambda^4 a_4x + \lambda^6 a_6$$

under the change of coordinates $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$. Then

$$\tilde{W}_{C_\lambda, \phi_\lambda(\mathbf{P})} = \lambda \tilde{W}_{C, \mathbf{P}}$$

In particular, let δ_{ij} be the Kronecker delta, and define

$$g(\mathbf{v}) = -1 - \sum_{1 \leq i < j \leq n} (-1)^{\delta_{ij}} v_i v_j.$$

Then

$$W_{C_\lambda, \phi_\lambda(P)} = \lambda^{g(v)} W_{C, P}.$$

Proof. The first statement is entailed by the second. From the general theory of Weierstrass sigma functions, $\sigma(\lambda z, \lambda \Lambda) = \lambda \sigma(z, \Lambda)$. Thus, by [Definition 3.1](#),

$$\Omega_v(\lambda z; \lambda \Lambda) = \lambda^{g(v)} \Omega_v(z; \Lambda).$$

As in [Section 4](#), this allows us to conclude that the same holds for Ψ_v , so that

$$\Psi_v(\lambda^2 x, \lambda^3 y, \lambda^i \alpha_i) = \lambda^{g(v)} \Psi_v(x, y, \alpha_i),$$

from which the result follows. □

Definition 7.2. Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. With the notation of [Proposition 7.1](#), we define

$$W^\lambda(v) := \lambda^{g(v)} W(v).$$

This gives an action of K on elliptic nets $W : \mathbb{Z}^n \rightarrow K$ called the *homothety action*. Two elliptic nets are *homothetic* if they are in the same orbit of the action of K .

The following proposition is immediate.

Proposition 7.3. *Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. Then for any nonzero $\lambda \in K$, W^λ is normalized if and only if W is.*

Let $W : \mathbb{Z}^n \rightarrow K$ be an elliptic net. If the curve C associated to its normalization is a nodal or cuspidal cubic, then W is called *singular*. If, instead, C is an elliptic curve, then W is called *nonsingular*. In either case, the discriminant Δ of W is defined to be the discriminant of the associated Weierstrass equation. Similarly, the j -invariant is the j -invariant of the associated Weierstrass equation. The discriminant of an elliptic net changes by a factor of λ^{12} under homothety, while the j -invariant remains unaltered.

The curve-net theorem. We may put a partial ordering on tuples (C, P_1, \dots, P_n) where C is a Weierstrass curve and P_i are nonsingular points on the curve. We do this by defining

$$(C, P_1, \dots, P_n) \leq (D, Q_1, \dots, Q_m)$$

if and only if $C = D$ and the groups they generate satisfy a containment

$$\langle P_1, \dots, P_n \rangle \subseteq \langle Q_1, \dots, Q_m \rangle.$$

The collection of all elliptic nets is partially ordered by the subnet relation. Collecting our work up to this point, we have now shown:

Theorem 7.4. *For each field K , there is an explicit isomorphism of partially ordered sets*

$$\left\{ \begin{array}{l} \text{scale equivalence classes of} \\ \text{nondegenerate elliptic nets} \\ W : \mathbb{Z}^n \rightarrow K, \text{ for some } n \end{array} \right\}$$

$$\updownarrow$$

$$\left\{ \begin{array}{l} \text{tuples } (C, P_1, \dots, P_m) \text{ for some } m, \text{ where } C \text{ is a} \\ \text{cubic curve in Weierstrass form over } K, \text{ consid-} \\ \text{ered modulo unihomothetic changes of variables} \\ \text{and such that } \{P_i\} \in C_{\text{ns}}(K)^m \text{ is appropriate} \end{array} \right\}.$$

Nonsingular nets correspond to elliptic curves. The action of K (by homothety) on the sets preserves the order and respects the isomorphism. The bijection takes an elliptic net of rank n to a tuple with n points. The elliptic net W associated to a tuple (C, P_1, \dots, P_n) satisfies the property that $W(v_1, \dots, v_n) = 0$ if and only if $v_1 P_1 + \dots + v_n P_n = 0$ on the curve C .

Proof. In the diagram in the statement of the theorem, call the upper set \mathcal{N} and the lower set \mathcal{C} . The first claim is that there is an injective map $\mathcal{N} \rightarrow \mathcal{C}$. [Proposition 6.2](#) shows that each scale equivalence classes in \mathcal{N} contains a unique normalized elliptic net, so we can define the map by [Theorem 6.7](#) (which also guarantees injectivity). [Corollary 5.2](#) shows that the result is an element of \mathcal{C} . This shows the first claim.

The second claim is that there exists an inverse map $\mathcal{C} \rightarrow \mathcal{N}$. The map is given by [Definition 5.1](#), which is well-defined as a result of [Theorem 4.6](#). It is required to check that the resulting elliptic net is normalized ([Proposition 3.8](#)) and nondegenerate ([Corollary 5.2](#)). [Theorem 6.7](#) says that this map is indeed an inverse to the map of the first claim. This gives the second claim and the bijection of sets.

It is clear that the bijection associates an elliptic net of rank n to a tuple with n points, and that it preserves the partial ordering. The action of homothety is preserved by [Proposition 7.1](#). And the final statement of the theorem is a result of [Corollary 5.2](#). □

Remark 7.5. The degenerate cases present several difficulties. One is that a degenerate elliptic net may not be determined by the usual initial set of terms as given in [Section 2](#). For example, the sequence given by

$$W(n) = \begin{cases} 0 & \text{if } n \neq k, \\ 1 & \text{if } n = k, \end{cases}$$

is an elliptic net for any nonzero integer k . However, some degenerate sequences can be thought of as arising from singular points on a singular cubic. For example, consider a sequence associated to an elliptic curve E and point P both defined over

\mathbb{Q} such that P reduces to a singular point modulo some prime p . Then the sequence regarded modulo p as living in \mathbb{F}_p (which is necessarily a degenerate elliptic net) should be associated to a point on the special fibre of the Néron model. It is likely that [Theorem 7.4](#) can be extended to include these cases (this is future work).

Acknowledgements

I thank my thesis advisor, Joseph Silverman, for many patient hours. I also thank Rafe Jones, Alf van der Poorten, and Jonathan Wise.

References

- [Ayad 1993] M. Ayad, “Périodicité (mod q) des suites elliptiques et points S -entiers sur les courbes elliptiques”, *Ann. Inst. Fourier (Grenoble)* **43**:3 (1993), 585–618. [MR 94f:11009](#)
- [Chandrasekharan 1985] K. Chandrasekharan, *Elliptic functions*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **281**, Springer, Berlin, 1985. [MR 87e:11058](#) [Zbl 0575.33001](#)
- [Chudnovsky and Chudnovsky 1986] D. V. Chudnovsky and G. V. Chudnovsky, “Sequences of numbers generated by addition in formal groups and new primality and factorization tests”, *Adv. in Appl. Math.* **7**:4 (1986), 385–434. [MR 88h:11094](#) [Zbl 0614.10004](#)
- [Cornelissen and Zahidi 2007] G. Cornelissen and K. Zahidi, “Elliptic divisibility sequences and undecidable problems about rational points”, *J. Reine Angew. Math.* **613** (2007), 1–33. [MR2009h:11196](#) [Zbl 1178.11076](#)
- [Eisenträger and Everest 2009] K. Eisenträger and G. Everest, “Descent on elliptic curves and Hilbert’s tenth problem”, *Proc. Amer. Math. Soc.* **137**:6 (2009), 1951–1959. [MR 2009k:11201](#)
- [Everest et al. 2003] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society, Providence, RI, 2003. [MR 2004c:11015](#) [Zbl 1033.11006](#)
- [Everest et al. 2004] G. Everest, V. Miller, and N. Stephens, “Primes generated by elliptic curves”, *Proc. Amer. Math. Soc.* **132**:4 (2004), 955–963. [MR 2005a:11076](#) [Zbl 1043.11051](#)
- [Everest et al. 2006] G. Everest, G. McLaren, and T. Ward, “Primitive divisors of elliptic divisibility sequences”, *J. Number Theory* **118**:1 (2006), 71–89. [MR 2007a:11074](#) [Zbl 0169.15902](#)
- [Fomin and Zelevinsky 2002] S. Fomin and A. Zelevinsky, “The Laurent phenomenon”, *Adv. in Appl. Math.* **28**:2 (2002), 119–144. [MR 2002m:05013](#) [Zbl 1012.05012](#)
- [Frey and Lange 2006] G. Frey and T. Lange, “Background on curves and Jacobians”, pp. 45–85 in *Handbook of elliptic and hyperelliptic curve cryptography*, edited by H. Cohen et al., CRC, Boca Raton, FL, 2006. [MR 2162720](#)
- [Gasper and Rahman 2004] G. Gasper and M. Rahman, *Basic hypergeometric series*, 2nd ed., Encyclopedia of Mathematics and its Applications **96**, Cambridge University Press, Cambridge, 2004. [MR 2006d:33028](#) [Zbl 1129.33005](#)
- [Hone 2005] A. N. W. Hone, “Elliptic curves and quadratic recurrence sequences”, *Bull. London Math. Soc.* **37**:2 (2005), 161–171. [MR 2005h:11111](#) [Zbl 1166.11333](#)
- [Ingram 2009] P. Ingram, “Multiples of integral points on elliptic curves”, *J. Number Theory* **129**:1 (2009), 182–208. [MR 2010a:11102](#) [Zbl 05485801](#)

- [Mazur and Tate 1991] B. Mazur and J. Tate, “The p -adic sigma function”, *Duke Math. J.* **62**:3 (1991), 663–688. [MR 93d:11059](#) [Zbl 0735.14020](#)
- [Poonen 2003] B. Poonen, “Hilbert’s tenth problem and Mazur’s conjecture for large subrings of \mathbb{Q} ”, *J. Amer. Math. Soc.* **16**:4 (2003), 981–990. [MR 2004f:11145](#) [Zbl 1028.11077](#)
- [van der Poorten 2005] A. J. van der Poorten, “Elliptic curves and continued fractions”, *J. Integer Seq.* **8**:2 (2005), [article] 05.2.5. [MR 2006h:11083](#)
- [van der Poorten and Swart 2006] A. J. van der Poorten and C. S. Swart, “Recurrence relations for elliptic sequences: every Somos 4 is a Somos k ”, *Bull. London Math. Soc.* **38**:4 (2006), 546–554. [MR 2007d:11024](#) [Zbl 1169.11013](#)
- [Propp 2001] J. Propp, [Robbins forum](#), various messages from January 2, 2001 through March 6, 2001, available at <http://faculty.uml.edu/jpropp/about-robbins.txt>.
- [Shipsey 2001] R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmiths, University of London, 2001.
- [Silverman 2004] J. H. Silverman, “Common divisors of elliptic divisibility sequences over function fields”, *Manuscripta Math.* **114**:4 (2004), 431–446. [MR 2005d:11096](#) [Zbl 1128.11015](#)
- [Silverman 2005] J. H. Silverman, “ p -adic properties of division polynomials and elliptic divisibility sequences”, *Math. Ann.* **332**:2 (2005), 443–474. [MR 2006f:11063](#) [Zbl 1066.11024](#)
- [Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. [MR 2010i:11005](#) [Zbl 1194.11005](#)
- [Stange 2007] K. E. Stange, “The Tate pairing via elliptic nets”, pp. 329–348 in *Pairing-based cryptography: Pairing 2007* (Tokyo, 2007), edited by T. Takagi et al., Lecture Notes in Comput. Sci. **4575**, Springer, Berlin, 2007. [MR 2009e:11233](#) [Zbl 1151.94570](#)
- [Stange 2010] K. E. Stange, [Scripts in PARI/GP 2.3.4 and SAGE 4.6.1](#), 2010, available at <http://math.katestange.net>.
- [Streng 2008] M. Streng, “Divisibility sequences for elliptic curves with complex multiplication”, *Algebra Number Theory* **2**:2 (2008), 183–208. [MR 2009e:11110](#) [Zbl 1158.14029](#)
- [Swart 2003] C. Swart, *Elliptic curves and related sequences*, Ph.D. thesis, Royal Holloway and Bedford New College, University of London, 2003.
- [Ward 1948] M. Ward, “Memoir on elliptic divisibility sequences”, *Amer. J. Math.* **70** (1948), 31–74. [MR 9,332j](#)
- [Wenchang et al. 1996] C. Wenchang, S. B. Ekhad, and R. J. Chapman, “Problems and Solutions: Solutions: 10226”, *Amer. Math. Monthly* **103**:2 (1996), 175–177. [MR 1542800](#)

Communicated by John H. Coates

Received 2010-04-28

Revised 2010-09-16

Accepted 2010-10-17

stange@math.stanford.edu

Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA, 94305, United States

<http://math.katestange.net>

Algebra & Number Theory

www.jant.org

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Shigefumi Mori	RIMS, Kyoto University, Japan
Dave Benson	University of Aberdeen, Scotland	Andrei Okounkov	Princeton University, USA
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Victor Reiner	University of Minnesota, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Karl Rubin	University of California, Irvine, USA
Brian D. Conrad	University of Michigan, USA	Peter Sarnak	Princeton University, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Michael Singer	North Carolina State University, USA
Hubert Flenner	Ruhr-Universität, Germany	Ronald Solomon	Ohio State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Joseph Gubeladze	San Francisco State University, USA	Bernd Sturmfels	University of California, Berkeley, USA
Ehud Hrushovski	Hebrew University, Israel	Richard Taylor	Harvard University, USA
Craig Huneke	University of Kansas, USA	Ravi Vakil	Stanford University, USA
Mikhail Kapranov	Yale University, USA	Michel van den Bergh	Hasselt University, Belgium
Yujiro Kawamata	University of Tokyo, Japan	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Andrei Zelevinsky	Northeastern University, USA
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA
Susan Montgomery	University of Southern California, USA		

PRODUCTION

contact@msp.org

Silvio Levy, Scientific Editor

Andrew Levy, Production Editor


See inside back cover or www.jant.org for submission instructions.

The subscription price for 2011 is US \$150/year for the electronic version, and \$210/year (+\$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**

<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2011 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 5 No. 2 2011

On the Hom-form of Grothendieck's birational anabelian conjecture in positive characteristic	131
MOHAMED SAÏDI and AKIO TAMAGAWA	
Local positivity, multiplier ideals, and syzygies of abelian varieties	185
ROBERT LAZARSFELD, GIUSEPPE PARESCHI and MIHNEA POPA	
Elliptic nets and elliptic curves	197
KATHERINE STANGE	
The basic geometry of Witt vectors, I The affine case	231
JAMES BORGER	
Correction to a proof in the article Patching and admissibility over two-dimensional complete local domains	287
DANNY NEFTIN and ELAD PARAN	