Journal of Combinatorial Theory, Series A 136 (2015) 64–95

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

The lattice size of a lattice polygon

Wouter Castryck [a], Filip Cools [b]

[a] Vakgroep Wiskunde, Universiteit Gent, Krijgslaan 281, 9000 Gent, Belgium
[b] Department of Mathematics and Applied Mathematics, University of Cape Town, Private Bag X1, Rondebosch 7701, South Africa

A R T I C L E   I N F O

Article history:
Received 21 February 2014
Available online 29 June 2015

Keywords:
Newton polygon
Lattice width
Minimal degree
Minimal bidegree
Algebraic curve

A B S T R A C T

We give upper bounds on the minimal degree of a model in $\mathbb{P}^2$ and the minimal bidegree of a model in $\mathbb{P}^1 \times \mathbb{P}^1$ of the curve defined by a given Laurent polynomial, in terms of the combinatorics of the Newton polygon of the latter. We prove in various cases that this bound is sharp as soon as the polynomial is sufficiently generic with respect to its Newton polygon.

1. Introduction

Let k be an algebraically closed field and let $f \in k[x^{\pm 1}, y^{\pm 1}]$ be an irreducible Laurent polynomial whose Newton polygon, denoted by $\Delta(f)$, we assume to be two-dimensional. Let $\mathbb{T}^2 = k^* \times k^*$ be the two-dimensional torus over k, and denote by $U_f \subset \mathbb{T}^2$ the curve defined by f. (Throughout this paper, all curves are understood to be irreducible, but not necessarily non-singular and/or projective.) For a curve C/k we define $s_2(C)$ as the minimum of

$$S_2(C) = \left\{ \, d \in \mathbb{N} \, | \, C \simeq \text{a curve of degree } d \text{ in } \mathbb{P}^2 \, \right\}$$

E-mail addresses: wouter.castryck@gmail.com (W. Castryck), filip.cools@uct.ac.za (F. Cools).

http://dx.doi.org/10.1016/j.jcta.2015.06.005

and $s_{1,1}(C)$ as the lexicographic minimum of

$$S_{1,1}(C) = \left\{ (a, b) \in \mathbb{N}^2 \,\middle|\, a \leq b \text{ and } C \simeq \text{ a curve of bidegree } (a, b) \text{ in } \mathbb{P}^1 \times \mathbb{P}^1 \right\},$$

where $\simeq$ denotes birational equivalence. The aim of this article is to give upper bounds on the invariants $s_2(U_f)$ and $s_{1,1}(U_f)$ purely in terms of the combinatorics of $\Delta(f)$.

The invariant $s_2(C)$ has seen study in the past [11,17,19] but is not well-understood. On the other hand we are unaware of existing literature explicitly devoted to $s_{1,1}(C)$, even though for hyperelliptic curves the notion has made an appearance [14] in the context of cryptography. Note that at first sight, the definition of $s_{1,1}(C)$ has a non-canonical flavor: instead of lexicographic, one could also consider the minimum with respect to other types of monomial orders on $\mathbb{N}^2$. But in fact we conjecture:

Conjecture 1.1. *For each curve C/k the set $S_{1,1}(C)$ admits a minimum with respect to the product order $\leq \times \leq$ on $\mathbb{N}^2$.*

Because the product order is coarser than every monomial order, this would mean that the term 'lexicographic' can be removed without ambiguity. In Section 2 we will state a number of basic facts on $s_2(C)$ and $s_{1,1}(C)$, along with some motivation in favor of Conjecture 1.1.

Our central combinatorial notion is the *lattice size* $\mathrm{ls}_X(\Delta)$ of a lattice polygon Δ with respect to a set $X \subset \mathbb{R}^2$ with positive Jordan measure. In case $\Delta \neq \emptyset$ we define it as the smallest integer $d \geq 0$ for which there exists a unimodular transformation $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ such that

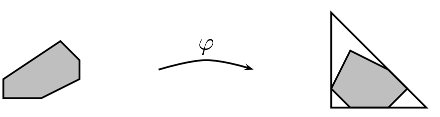
$$\varphi(\Delta) \subset dX.$$

A unimodular transformation that attains this minimum is said to compute the lattice size. We will restrict ourselves to three instances of X, namely

$$[0, 1] \times \mathbb{R}, \qquad \Sigma = \mathrm{conv}\{(0, 0), (1, 0), (0, 1)\}, \qquad \square = \mathrm{conv}\{(0, 0), (1, 0), (0, 1), (1, 1)\},$$

where it is convenient to define $\mathrm{ls}_X(\emptyset) = -1, -2, -1$, respectively.

In the case of $X = \Sigma$ the lattice size measures the smallest standard triangle containing a unimodular copy of Δ.



This was studied by Schicho [25], who designed an algorithm for finding a unimodular transformation that maps a given polygon Δ inside a small standard triangle. He did this in the context of simplifying parameterizations of rational surfaces. Our results below show that Schicho's algorithm works optimally, that is, its output computes the