Finite Fields and Their Applications 47 (2017) 145–160

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Curves of medium genus with many points

Everett W. Howe

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121, USA

ARTICLE INFO

Article history:
Received 13 September 2016
Received in revised form 6 June 2017
Accepted 8 June 2017
Available online 17 July 2017
Communicated by Igor Shparlinski

MSC:
primary 11G20
secondary 14G05, 14G10, 14G15

Keywords:
Curve
Jacobian
Rational point
Defect

ABSTRACT

The *defect* of a curve over a finite field is the difference between the number of rational points on the curve and the Weil–Serre upper bound for the number of points on the curve. We present algorithms for constructing curves of genus 5, 6, and 7 with small defect. Our aim is to be able to produce, in a reasonable amount of time, curves that can be used to populate the online table of curves with many points found at manypoints.org.

1. Introduction

For every prime power q and non-negative integer g, we let $N_q(g)$ denote the maximum number of rational points on a smooth, projective, absolutely irreducible curve of genus g over the finite field $\mathbf{F}_q$. At the turn of the present century, van der Geer and van der Vlugt published tables [5] of the best upper and lower bounds on $N_q(g)$ known at the

E-mail address: however@alumni.caltech.edu.
URL: http://www.alumni.caltech.edu/~however/.

http://dx.doi.org/10.1016/j.ffa.2017.06.006
1071-5797/

time, for $g \leq 50$ and for q ranging over small powers of 2 and 3. In 2010, van der Geer, Lauter, Ritzenthaler, and the author (with technical assistance from Gerrit Oomens) created the manypoints web site [4], which gives the currently-known best upper and lower bounds on $N_q(g)$ for $g \leq 50$ and for a range of prime powers q: the primes less than 100, the prime powers p^i for $p < 20$ and $i \leq 5$, and the powers of 2 up to 2^7.

The *Weil–Serre upper bound* [16, Théorème 1, p. 397] for $N_q(g)$ states that

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor .$$

When $q \geq (g + \sqrt{g+1})^2$ the Weil–Serre bound is almost always the best upper bound currently known for $N_q(g)$; the exceptions come from "exceptional" prime powers [8, Theorem 4, p. 1682] and from careful case-by-case analyses — see the introduction to [9] for a summary. On the other hand, lower bounds for $N_q(g)$ are generally obtained by producing more-or-less explicit examples of curves with many points. Typically, this is done by searching through specific families of curves — for instance, families of curves obtained via class field theory as covers of lower-genus curves, or families of curves with specific nontrivial automorphism groups. For small finite fields of characteristic 2 and 3, such searches have been carried out for many genera, so even the earliest versions of the van der Geer–van der Vlugt tables gave nontrivial lower bounds for many values of $N_q(g)$.

One of the goals of the manypoints web site is to encourage researchers to consider curves over finite fields of larger characteristics. Curves over these fields have received far less attention than curves in characteristic 2 or 3, so at present the table entries for lower bounds for $N_q(g)$ remain unpopulated for most q and g.

Of course, there are trivial lower bounds for $N_q(g)$: for instance, if C is a hyperelliptic curve of any genus over $\mathbf{F}_q$, then either C or its quadratic twist will have at least $q+1$ points. To avoid having to worry about such "poor" lower bounds, van der Geer and van der Vlugt decided not to print a lower bound for $N_q(g)$ in their tables unless it was greater than $1/\sqrt{2}$ times the best upper bound known for $N_q(g)$. This restriction was adopted for the manypoints table as well, but it turns out that it is not a strong enough filter when q is large with respect to g. The administrators of the manypoints site are considering replacing it with the requirement that a lower bound not be published unless the difference between the lower bound and $q+1$ is at least $1/\sqrt{2}$ times the difference between the best proven upper bound and $q+1$.

Every genus-0 curve over a finite field is isomorphic to $\mathbf{P}^1$, so $N_q(0) = q+1$ for all q. For $g = 1$ and $g = 2$, the value of $N_q(g)$ is also known for all q. For $g = 1$ this is due to a classical result of Deuring [3] (see [20, Theorem 4.1, p. 536]); for $g = 2$, this is due to work of Serre [15–17] (see also [11]). There is no easy formula known for $N_q(3)$, but for all q in the manypoints table the value has been computed; see the introduction to [14]. For genus 4, the exact value of $N_q(4)$ is known for 45 of the 59 prime powers q in the manypoints table, and for the remaining 14 prime powers the lower bound for $N_q(4)$ is within 4 of the best proven upper bound; see [6] and [7].