COMPUTER SEARCH FOR CURVES WITH MANY POINTS THROUGH FAMILIES OVER $\mathbf{F}_{25}$ AND $\mathbf{F}_{49}$

KARL RÖKAEUS

Abstract.[1] Using class field theory one associates to each curve C over the finite field $\mathbf{F}_q$, and each integer $n > 1$, an unramified cover of C defined over $\mathbf{F}_{q^n}$ whose genus is determined by the L-polynomial of C. By listing all possible L-polynomials of curves of small genus over $\mathbf{F}_q$ one may get examples of curves with many points. In [1] this search was done for small fields of characteristic 2 and 3, and for all base curves of genus 2 and 3; we do it for all base curves of genus 2 over the prime fields of cardinality 5 and 7, giving new entries for the tables [3] over the fields with 25 and 49 elements. We remark that none of the methods used in this report are new; they where described *e.g.,* in [4] and used systematically in [1].

Background Material

Curves with many points. Let $N_q(g)$ denote the maximum number of rational places possible on a function field of genus g over $\mathbf{F}_q$. In [3] the current intervals in which $N_q(g)$ are known to lie are listed for genus up to 50 and for all primes q less than 100, and also for prime powers $q = p^e$ when $p < 20$ and $e \leq 5$. In this report we find curves over $\mathbf{F}_q$ for $q = 25, 49$ and 121 and some $g \geq 7$. For these values of q there where only a few entries of lower bounds in the tables, all coming from subfields of the Hermitian field; these are all maximal so in these cases the exact value of $N_q(g)$ was already known, see [5]. In all other cases the tables didn't have any lower bounds, so in order to make it to the tables all we had to do was to produce a curve with more than $b(q,g)/\sqrt{2}$ points, where $b(q,g)$ is a known upper bound of $N_q(g)$ (this is the benchmark criterium for a curve to be considered having many points, see [2] for a motivation).

Attaching an unramified cover to an L-polynomial: Let C be a smooth projective curve defined over the finite field k; let J be its Jacobian variety and let $L(C,t)$ be its L-polynomial. If G is a subgroup of $J(k)$ of index d then class field theory gives the existence of an unramified degree d cover of C in which all points in $C(k)$ that are mapped to G by the Abel-Jacobi map split completely. If the Jacobian is not known (and in fact even if C itself is not known), but only its isogeny class (which is determined by $L(C,t)$) then one can still use this to prove existence of covers of certain genera and with a guaranteed minimal number of points, but now defined over extensions of k: Let k_n be the degree n extension of k (inside a fixed algebraic closure), let $C_{k_n} := C \times k_n$ and let J_n be its Jacobian. Then $d_n := [J(k_n) : J(k)] = \prod_{\zeta^n=1,\zeta\neq 1} L(C,\zeta)$, and since $C(k) \subset C(k_n) = C_{k_n}(k_n)$ maps to $J(k) \subset J(k_n) = J_n(k_n)$ it follows that there exists an unramified degree d_n cover of C_{k_n} in which all points in $C(k) \subset C_{k_n}(k_n)$ split completely. This cover therefore has genus $d(g(C) - 1) + 1$ and at least $d \cdot \#C(k)$ rational points.

Date: February 10, 2011.

[1] The author is supported by The Wenner-Gren Foundations Postdoctoral Grant

Listing genus 2 curves: The function field F of any genus 2 curve over a perfect field k of characteristic different from 2 is of the form $k(x, y)$, where $y^2 = f(x)$ for some square-free $f \in k[x]$ of degree 5 or 6. (And conversely every such field has genus 2.) Moreover, the extension $F/k(x)$ is ramified precisely at the places P_α, where α is a root of f, and at P_∞ if $\deg f = 5$. The rational place P_α of $k(x)$ splits completely precisely when $f(\alpha)$ is a non-zero square in k. (See [6], Ch. *VI*.)

The Search

In Section 4 of [1] the author lists all L-polynomials of genus 2 and genus 3 curves over the fields $\mathbf{F}_q$ for $q = 2, 4, 8, 3, 9$, as well as some L-polynomials for higher genus curves, to obtain improvements of the records over the finite fields of cardinality $q = 4, 8, 16, 64, 9, 27, 81$. We did the same complete listing of all genus 2 curves for $q = 5, 7$. This was done using a standard laptop, and a non-specialized software (Mathematica). More precisely, we list all polynomials $f \in \mathbf{F}_p[x]$ of degree 5 and 6, for $p = 5, 7$, and then compute their number of $\mathbf{F}_p$ and $\mathbf{F}_{p^2}$-points. This allows us to compute their L-polynomials, and then the degree $d_n = [J(k_n) : J(k)]$ for $n = 2$ (and also for $n \geq 3$, but that gives covers of genus > 50). This leads to a number of new entries for the tables; for $q = 25$ when g in is in the range between 8 and 30; and for $q = 49$ when g is in the range between 16 and 50. We also listed some of the genus 2 curves over $\mathbf{F}_{11}$ and obtained some entries for the tables also in this case. However, the program we used was the naivest possible, and we didn't manage to list all possible L-polynomials in this case; doing it should give some more contribution to the tables.

It seems that for q larger than 11 this method, with genus 2 curves as base, won't give improvements of the tables; the reason is that the tables [3] only includes values up to genus 50, while the degree d_n, and hence the genus, of the obtained cover becomes big very quickly. We listed all genus 2 curves over $\mathbf{F}_5$ and $\mathbf{F}_7$, and some over $\mathbf{F}_{11}$. In all these cases this gave some reasonable values of d_n, but only for $n = 2$, *i.e.,* the cover is defined over the quadratic extension. We also tested some genus 2 curves over $\mathbf{F}_{17}$ and bigger fields, but here d_n became too large. However, it might be that when q grows it becomes better to use curves of higher genus as base, as these might give an L-polynomial that are nicer (meaning that its leading coefficient isn't that dominating and hence allows $L(-1)$ to be small).

The reason why we didn't do this search for elliptic curves is that an unramified cover of such a curve is again elliptic. However, it is also possible to get some information about covers that ramifies at one of the rational points, with known ramification index, only from looking at the L-polynomial. With genus 2 curves as base this method produces covers of genus greater than 50, but with elliptic curves as base it gave one contribution: any elliptic curve with L-polynomial $5t^2 + 3t + 1$, *e.g.,* $y^2 = x^3 + x + 1$, has a cover over $\mathbf{F}_{25}$ of genus 13 and at least 123 rational points. See Theorem 4.2.20 in [4] for the construction of this cover.

The results

Let $p = 5, 7, 11$ and $q = p^2$. The results are given in the following tables; the last three columns consist of integers g and N such that there exists a genus g curve with at least N points, and then the interval $[b(q, g)/\sqrt{2}, b(q, g)]$, where $b(q, g)$ is a known upper bound for $N_q(g)$ (no lower bound better than $b(q, g)/\sqrt{2}$ was listed in any of these cases). The first three columns consists of the data used to construct the curve; first the polynomial f that defines the base curve $y^2 = f(x)$ over $\mathbf{F}_p$, then $[N_1, N_2]$, its number of $\mathbf{F}_p$- and $\mathbf{F}_q$-points, and then its L-polynomial.

Curves over $\mathbf{F}_{25}$

The field $\mathbf{F}_5(x,y)$ with $y^2 = f$ has L-polynomial $L(t)$. Over $\mathbf{F}_{25}$ it has an extension of genus g with N rational places.

f	$[N_1, N_2]$	$L(t)$	g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$
$1+x^2+2x^3+2x^4+2x^5+x^6$	$[12,24]$	$1+6t+17t^2+30t^3+25t^4$	8	84	$[73,102]$
$1+4x^4+x^6$	$[12,26]$	$1+6t+18t^2+30t^3+25t^4$	9	96	$[80,112]$
$1+3x^2+4x^3+2x^4+x^5$	$[11,29]$	$1+5t+14t^2+25t^3+25t^4$	11	110	$[93,131]$
$1+x+4x^3+4x^4+x^5$	[11, 31]	$1+5t+15t^2+25t^3+25t^4$	12	121	[99, 139]
$1+x+x^3$	[9]	$1+3t+5t^2$	13	123	[104, 146]
$1+x^3+3x^5+x^6$	[10, 32]	$1+4t+11t^2+20t^3+25t^4$	14	130	[109, 153]
$2x+2x^2+3x^3+3x^4+x^5$	[10, 34]	$1+4t+12t^2+20t^3+25t^4$	15	140	[114, 160]
$1+2x^3+3x^4+4x^5+x^6$	[10, 36]	$1+4t+13t^2+20t^3+25t^4$	16	150	[119, 167]
$x+4x^3+x^5$	[10, 38]	$1+4t+14t^2+20t^3+25t^4$	17	160	[124, 174]
$1+x+3x^3+3x^4+x^5$	[9, 35]	$1+3t+9t^2+15t^3+25t^4$	18	153	[128, 180]
$1+x^3+x^5$	[9, 37]	$1+3t+10t^2+15t^3+25t^4$	19	162	[133, 187]
$1+x^2+x^3+4x^4+x^5$	[9, 39]	$1+3t+11t^2+15t^3+25t^4$	20	171	[138, 194]
$2x+x^2+2x^3+x^5$	[8, 34]	$1+2t+6t^2+10t^3+25t^4$	21	160	[143, 201]
$1+x^4+x^6$	[8, 36]	$1+2t+7t^2+10t^3+25t^4$	22	168	[148, 208]
$2x+x^2+x^3+4x^4+x^5$	[8, 38]	$1+2t+8t^2+10t^3+25t^4$	23	176	[152, 214]
$1+4x^2+x^3+3x^4+2x^5+x^6$	[8, 40]	$1+2t+9t^2+10t^3+25t^4$	24	184	[157, 221]
$x+x^2+4x^3+4x^4+x^5$	[8, 42]	$1+2t+10t^2+10t^3+25t^4$	25	192	[162, 228]
$1+2x^4+x^6$	[8, 44]	$1+2t+11t^2+10t^3+25t^4$	26	200	[167, 235]
$1+3x^3+2x^4+x^5$	[7, 37]	$1+t+6t^2+5t^3+25t^4$	27	182	[172, 242]
$1+x+x^2+2x^4+x^5$	[7, 39]	$1+t+7t^2+5t^3+25t^4$	28	189	[176, 248]
$2x+x^2+3x^3+x^5$	[7, 41]	$1+t+8t^2+5t^3+25t^4$	29	196	[181, 255]
$1+2x^3+3x^4+x^5$	[7, 43]	$1+t+9t^2+5t^3+25t^4$	30	203	[185, 261]

Remark: The curve of genus 13 is an extension of an elliptic field, defined as a subfield of a narrow ray class field with modulus P^2 for P a rational place, see Theorem 4.2.20 of [4], with $n = r = 2$.

Curves over $\mathbf{F}_{49}$

The field $\mathbf{F}_7(x, y)$ with $y^2 = f$ has L-polynomial $L(t)$. Over $\mathbf{F}_{49}$ it has an unramified extension of genus g with at least N rational places.

f	$[N_1, N_2]$	$L(t)$	g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$
$1 + x^2 + 2x^3 + 6x^5 + x^6$	[16, 44]	$1 + 8t + 29t^2 + 56t^3 + 49t^4$	16	240	[190,268]
$1 + x^6$	[16, 46]	$1 + 8t + 30t^2 + 56t^3 + 49t^4$	17	256	[200, 282]
$1 + x^2 + x^3 + 4x^4 + x^5$	[15, 49]	$1 + 7t + 24t^2 + 49t^3 + 49t^4$	19	270	[220, 310]
$1 + 4x^2 + 5x^3 + 5x^4 + x^5$	[15, 51]	$1 + 7t + 25t^2 + 49t^3 + 49t^4$	20	285	[230, 324]
$1 + 3x^2 + x^4 + 2x^5 + x^6$	[14, 52]	$1 + 6t + 19t^2 + 42t^3 + 49t^4$	22	294	[249, 352]
$3x + x^3 + 6x^4 + x^5$	[14, 54]	$1 + 6t + 20t^2 + 42t^3 + 49t^4$	23	308	[257, 363]
$1 + x^3 + x^4 + 5x^5 + x^6$	[14, 56]	$1 + 6t + 21t^2 + 42t^3 + 49t^4$	24	322	[264, 373]
$x + 2x^2 + 5x^3 + 2x^4 + x^5$	[14, 58]	$1 + 6t + 22t^2 + 42t^3 + 49t^4$	25	336	[271, 383]
$1 + x + x^2 + x^3 + 2x^4 + 6x^5 + x^6$	[14, 60]	$1 + 6t + 23t^2 + 42t^3 + 49t^4$	26	350	[278, 393]
$1 + 3x^2 + 3x^3 + x^4 + x^5$	[13, 57]	$1 + 5t + 16t^2 + 35t^3 + 49t^4$	27	338	[285, 403]
$1 + 5x^2 + 4x^4 + x^5$	[13, 59]	$1 + 5t + 17t^2 + 35t^3 + 49t^4$	28	351	[293, 413]
$1 + 5x^2 + 5x^3 + 3x^4 + x^5$	[13, 61]	$1 + 5t + 18t^2 + 35t^3 + 49t^4$	29	364	[300, 423]
$1 + 3x + 2x^2 + 5x^4 + x^5$	[13, 63]	$1 + 5t + 19t^2 + 35t^3 + 49t^4$	30	377	[307, 433]
$3x + x^2 + 4x^3 + 6x^4 + x^5$	[12, 58]	$1 + 4t + 12t^2 + 28t^3 + 49t^4$	31	360	[314, 443]
$1 + x^3 + 3x^4 + 5x^5 + x^6$	[12, 60]	$1 + 4t + 13t^2 + 28t^3 + 49t^4$	32	372	[320, 452]
$x + 2x^2 + x^3 + 3x^4 + x^5$	[12, 62]	$1 + 4t + 14t^2 + 28t^3 + 49t^4$	33	384	[327, 462]
$1 + x^2 + x^3 + 4x^4 + 2x^5 + x^6$	[12, 64]	$1 + 4t + 15t^2 + 28t^3 + 49t^4$	34	396	[334, 472]
$3x + x^2 + 2x^3 + x^4 + x^5$	[12, 66]	$1 + 4t + 16t^2 + 28t^3 + 49t^4$	35	408	[341, 482]
$1 + x^2 + 5x^4 + x^6$	[12, 68]	$1 + 4t + 17t^2 + 28t^3 + 49t^4,$	36	420	[348, 491]
$x + x^2 + 6x^3 + x^4 + x^5$	[12, 70]	$1 + 4t + 18t^2 + 28t^3 + 49t^4$	37	432	[355, 501]
$1 + 3x^2 + x^3 + x^5$	[11, 63]	$1 + 3t + 11t^2 + 21t^3 + 49t^4$	38	407	[362, 511]
$1 + x^2 + 2x^3 + 6x^4 + x^5$	[11, 65]	$1 + 3t + 12t^2 + 21t^3 + 49t^4$	39	418	[369, 521]
$1 + 2x^2 + 2x^4 + x^5$	[11, 67]	$1 + 3t + 13t^2 + 21t^3 + 49t^4$	40	429	[375, 530]
$x + 2x^3 + 5x^4 + x^5$	[11, 69]	$1 + 3t + 14t^2 + 21t^3 + 49t^4$	41	440	[382, 540]
$1 + 2x^2 + 4x^3 + 4x^4 + x^5$	[11, 71]	$1 + 3t + 15t^2 + 21t^3 + 49t^4$	42	451	[389, 550]
$3x + 4x^2 + x^3 + 2x^4 + x^5$	[10, 62]	$1 + 2t + 8t^2 + 14t^3 + 49t^4$	43	420	[396, 559]
$1 + 3x^4 + x^5 + x^6$	[10, 64]	$1 + 2t + 9t^2 + 14t^3 + 49t^4$	44	430	[403, 569]
$x + 6x^3 + 5x^4 + x^5$	[10, 66]	$1 + 2t + 10t^2 + 14t^3 + 49t^4$	45	440	[410, 579]
$1 + x^2 + 3x^3 + 6x^4 + x^5 + x^6$	[10, 68]	$1 + 2t + 11t^2 + 14t^3 + 49t^4$	46	450	[416, 588]
$3x + 4x^3 + 2x^4 + x^5$	[10, 70]	$1 + 2t + 12t^2 + 14t^3 + 49t^4$	47	460	[423, 598]
$1 + 3x^2 + 2x^3 + 4x^4 + 2x^5 + x^6$	[10, 72]	$1 + 2t + 13t^2 + 14t^3 + 49t^4$	48	470	[430, 608]
$x + 3x^2 + 3x^3 + 3x^4 + x^5$	[10, 74]	$1 + 2t + 14t^2 + 14t^3 + 49t^4$	49	480	[437, 618]
$1 + x^3 + x^6$	[10, 76]	$1 + 2t + 15t^2 + 14t^3 + 49t^4$	50	490	[444, 627]

Curves over $\mathbf{F}_{121}$

The field $\mathbf{F}_{11}(x, y)$ with $y^2 = f$ has L-polynomial $L(t)$. Over $\mathbf{F}_{121}$ it has an unramified extension of genus g with at least N rational places.

f	$[N_1, N_2]$	$L(t)$	g	N	$[\frac{b(g)}{\sqrt{2}}, b(g)]$
$1 + 6x^2 + 6x^4 + x^6$	[24, 94]	$1 + 12t + 58t^2 + 132t^3 + 121t^4$	37	864	[658, 930]
$1 + 3x^5$	[23, 103]	$1 + 11t + 51t^2 + 121t^3 + 121t^4$	42	943	[736, 1040]
$6 + x + x^2 + 6x^5 + x^6$	[22, 112]	$1 + 10t + 45t^2 + 110t^3 + 121t^4$	48	1034	[829, 1172]
$1 + x^4 + 3x^6$	[22,114]	$1 + 10t + 46t^2 + 110t^3 + 121t^4$	49	1056	[845, 1194]
$1 + x^2 + 2x^6$	[22,116]	$1 + 10t + 47t^2 + 110t^3 + 121t^4$	50	1078	[860, 1216]

Acknowledgments. The author would like to thank The Wenner-Gren Foundations for financial support; Korteweg-de Vries Institute at University of Amsterdam for hospitality; and Professor Gerard van der Geer for his hospitality and for helpful conversations and comments.

References

[1] G. van der Geer, *Hunting for curves with many points*, arXiv:0902.3882 (2009)

[2] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp 69, (2000), no 230 pp. 797–810

[3] *manyPoints.org*, tables of upper and lower bounds for the maximum number of points on a genus g curve over different finite fields.

[4] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*, LMS Lecture Note Series 285, 2001

[5] C. Rovi, *Algebraic Curves over finite fields*, Master Thesis, http://liu.diva-portal.org/smash/record.jsf?pid=diva2:321905

[6] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics 254, Springer-Verlag, 2009

Karl Rökaeus, Korteweg de Vries Instituut voor Wiskunde, Universiteit van Amsterdam, P.O. Box 94248, 1090 GE Amsterdam, The Netherlands

E-mail address: S.K.F.Rokaeus@uva.nl