MATHEMATICS OF COMPUTATION
Volume 69, Number 230, Pages 797–810
S 0025-5718(99)01143-6
Article electronically published on August 18, 1999

TABLES OF CURVES WITH MANY POINTS

GERARD VAN DER GEER AND MARCEL VAN DER VLUGT

ABSTRACT. These tables record results on curves with many points over finite fields. For relatively small genus ($0 \leq g \leq 50$) and q a small power of 2 or 3 we give in two tables the best presently known bounds for $N_q(g)$, the maximum number of rational points on a smooth absolutely irreducible projective curve of genus g over a field $\mathbb{F}_q$ of cardinality q. In additional tables we list for a given pair (g, q) the type of construction of the best curve so far, and we give a reference to the literature where such a curve can be found.

INTRODUCTION

In recent years the question of how many points a curve of genus g over a finite field $\mathbb{F}_q$ can have has attracted a lot of attention. This was motivated partly by possible applications in coding theory and cryptography, but also by the fact that the question represents an attractive mathematical challenge.

It is well known that a smooth absolutely irreducible projective curve of genus g over a finite field $\mathbb{F}_q$ can possess at most $q + 1 + 2g\sqrt{q}$ rational points. By a *curve* we shall mean in this paper a smooth absolutely irreducible projective curve defined over a finite field. The bound mentioned is the celebrated Hasse-Weil bound, proved by Hasse for $g = 1$ and by Weil in general. We denote by $N_q(g)$ the maximum number of rational points on a curve of genus g over $\mathbb{F}_q$. The Hasse-Weil bound implies

$$N_q(g) \leq q + 1 + [2g\sqrt{q}],$$

where $[x]$ is the integer part of $x \in \mathbb{R}$.

After Weil proved his bound around 1940, the question of how many rational points may lie on a curve over a finite field $\mathbb{F}_q$ remained untouched for many years. In 1980 Goppa came up with the beautiful idea of associating an error-correcting code to a linear system on a curve over a finite field, see [G]. In order to construct good codes one needs curves with many points, and thus Goppa's work led to a revival of interest in rational points on curves over finite fields. Applications in cryptography and recent constructions of quasi-random point sets also require curves with many points, and added a further impetus to work in the field.

In 1981 Ihara showed in [I] by a simple and elegant argument that

$$N_q(g) \leq q + 1 + [(\sqrt{(8q+1)g^2 + 4(q^2 - q)g} - g)/2]. \tag{1}$$

Received by the editor October 2, 1997 and, in revised form, April 28, 1998.
1991 *Mathematics Subject Classification.* Primary 11G20, 14G15; Secondary 14H05.

For $g > (q-\sqrt{q})/2$ this bound is better than Weil's bound and gives the asymptotic bound

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g} \le \sqrt{2q+\frac{1}{4}} - \frac{1}{2}. \tag{2}$$

Ihara also showed that if q is a square one has $A(q) \ge \sqrt{q}-1$, using a sequence of modular curves. Refining Ihara's idea to derive (1), Drinfeld and Vladut proved that

$$A(q) \le \sqrt{q}-1. \tag{3}$$

In [S1] Serre started the investigation of the actual value of $N_q(g)$. One has $N_q(0) = q+1$. For $g = 1, 2$ there are explicit formulas for $N_q(g)$. From [S2], [S4] we quote the following result:

Proposition 1. *Let $q = p^m$ and set $\mu = [2\sqrt{q}]$. For $g = 1$ one has $N_q(1) = q+1+\mu$, except when m is odd, $m \ge 3$ and p divides μ, in which case we have $N_q(1) = q+\mu$. Similarly, for $g = 2$ we have $N_q(2) = q+1+2\mu$ except in the following cases:*

i) $N_4(2) = 10$, $N_9(2) = 20$;
ii) *m odd, p divides μ;*
iii) *m odd and q of the form x^2+1, x^2+x+1 or x^2+x+2 for $x \in \mathbb{Z}$.*

In cases ii) *and* iii) *we have $N_q(2) = q+2\mu$ if $2\sqrt{q}-\mu > (\sqrt{5}-1)/2$, or $N_q(2) = q+2\mu-1$ else.*

In [S1] Serre used a little arithmetic to show that the Hasse-Weil bound may be sharpened to

$$N_q(g) \le q+1+g[2\sqrt{q}].$$

In the same paper Serre introduced the idea of using a 'formule explicite' in analogy with number theory for obtaining a better upper bound for $N_q(g)$. Oesterlé used methods from linear programming to perfect this idea, see [S4].

In the tables we shall use as upper bound for $N_q(g)$ the best bound that these estimates of Hasse-Weil, Ihara, Serre and Oesterlé provide. We also take into account slight improvements by $1, 2$, or 3 of these upper bounds. They result from the following facts.

Proposition 2 ([F-T])**.** *If q is a square and if C is a curve of genus g which attains the Hasse-Weil bound, then*

$$g \le (\sqrt{q}-1)^2/4 \quad \text{or} \quad g = (q-\sqrt{q})/2.$$

Proposition 3 ([S4])**.** *A curve of genus ≥ 3 with $\#C(\mathbb{F}_q) < q+1+g[2\sqrt{q}]$ satisfies $\#C(\mathbb{F}_q) \le q-1+g[2\sqrt{q}]$.*

Proposition 4. *One has the following explicit results:*

1) $N_2(7) = 10$;
2) $N_3(5) \le 13$, $N_3(7) = 16$, $N_8(6) \le 35$, *and* $N_9(5) \le 35$;
3) $N_4(4) = 15$ *and* $N_9(4) = 30$;
4) $N_{27}(3) = 56$.

Here 1) and 2) are obtained by an analysis of the Frobenius eigenvalues and are due to Serre [S4] and Lauter [L2], [L3] respectively. Result 3) was proved by Serre for $q = 4$ and follows from [S-V] for $q = 9$. Also 4) is due to Serre. Each of these improvements involves detailed considerations.

Proposition 5 ([L3]). 1) *For pairs* $q = 8, g \geq 4$ *and* $q \in \{27, 32\}$, $g \geq 3$ *we have* $N_q(g) \leq q - 1 + g[2\sqrt{q}]$. 2) *For* $q = 2^m$ *with even* $m \geq 4$ *and* $(\sqrt{q} - 1)^2/4 < g < (q - \sqrt{q})/2$ *we have* $N_q(g) \leq q - 2 + 2g\sqrt{q}$.

Though it seems very difficult to improve the upper bounds for $N_q(g)$, one cannot expect in general that $N_q(g)$ equals the upper bound that we have, as examples over $\mathbb{F}_2$ and $\mathbb{F}_3$ already show. Therefore, to test how good these bounds really are, one tries to come as close to these bounds as one can by constructing curves with as many points as possible. With an eye towards feasibility of applications, it is important to have such curves in a form as explicit as possible.

The methods used for the construction of curves with many points are rather diverse, but roughly speaking one can distinguish the following approaches:

- I Methods from general class field theory;
- II Methods from class field theory based on Drinfeld modules of rank 1;
- III Fibre products of Artin-Schreier curves;
- IV Towers of curves with many points;
- V Miscellaneous methods such as:
  1) formulas for $N_q(1)$ and $N_q(2)$;
  2) explicit curves, e.g. Hermitean curves, Klein's quartic, Artin-Schreier curves, Kummer extensions or curves obtained by computer search;
  3) elliptic modular curves $X(n)$ associated to the full congruence subgroups $\Gamma(n)$;
  4) Deligne-Lusztig curves;
  5) quotients of curves with many points.

Methods from general class field theory were used by Serre, Schoof, Lauter, Niederreiter and Xing, and Auer. They exploit subfields of Hilbert class fields or more generally of ray class fields of the function field of a given curve C in which a substantial number of the rational points of C split completely. General class field theory is a powerful weapon, but has the drawback that often it produces a mere existence result and not an explicit curve.

Constructing curves with many points by employing properties of Drinfeld modules of rank 1 was introduced by Niederreiter and Xing. When such a construction is applied to the case where the base curve C is the projective line $\mathbb{P}^1$, one can produce good subfields of cyclotomic function fields which have the advantage of being explicit. For general base curves the curves produced correspond to subfields of narrow ray class fields, and explicit forms of these function fields are then much harder to find.

Fibre products are used by Stichtenoth, by van der Geer and van der Vlugt, and by Shabat. The method yields defining equations for the curves thus constructed. In category IV one finds mainly towers consisting of a combination of Kummer and Artin-Schreier extensions or composita of Kummer extensions. The function fields are explicit.

So far the curves constructed by method V-5 are all quotients of the Hermitean curve defined over $\mathbb{F}_{q^2}$ by

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

The tables

For $g \leq 50$ and for $q = 2^m$ with $1 \leq m \leq 7$ and $q = 3^m$ with $1 \leq m \leq 4$ we present tables which list values of $N_q(g)$ or an interval in which $N_q(g)$ lies. Note that $g = 50$ is the largest value for which the actual value $N_2(g)$ is known. We therefore restricted ourselves to $g \leq 50$. Of course $N_q(0) = q + 1$ for all q, and it is omitted from the tables. If the precise value of $N_q(g)$ is not known, we give either an interval $[a, b] = [a_q(g), b_q(g)]$ or nothing. The meaning of the interval $[a, b]$ is: we know that there exists a curve with *at least* a rational points over $\mathbb{F}_q$, and the best upper bound by Hasse-Weil, Serre, Ihara, Oesterlé or other means says $N_q(g) \leq b$. In the lion's share of the cases the value of a represents a curve with exactly a rational points; in about 20 cases (mostly constructed with method II), a represents a lower bound for $N_q(g)$. Sometimes we entered no value. This happens if no curve with at least $[b/\sqrt{2}]$ rational points is known, i.e. if

$$a_q(g) < [b_q(g)/\sqrt{2}].$$

The reason for this is that for $g \leq 50$ in many cases the upper bound $b_q(g)$ is Ihara's bound (1). Since the Drinfeld-Vladut asymptotic bound (3) is approximately $1/\sqrt{2}$ times the asymptotic Ihara bound (2), we think it is reasonable to impose this qualification requirement for $g \leq 50$ to filter out curves which should be considered 'poor'.

Two main tables, 'Table $p = 2$' and 'Table $p = 3$', present values of the function $N_q(g)$ or an interval in which $N_q(g)$ lies. In additional tables $q = x$*: sources* we list the construction method of a curve producing the value of $a_q(g)$ and the source where this curve occurs first.

Remarks. i) For $q = 2$ one can find explicit curves realizing the lower bound for $g \in \{5, 6, 7, 8, 9, 12, 13, 14, 15\}$ in [N-X2], for $g = 10$ in [G-V7] and for $g = 11$ in [N-X1]. For $q = 3, 4$, $g = 4$ there are explicit curves in [N-X3].

ii) A result communicated to us by R. Schoof (see [G-V4]) gives values for the lower bound $a_q(g)$ for the pairs $(q = 2, g \in \{26, 27, 32, 33, 38, 40, 46, 47, 48\})$, $(q = 4, g \in \{6, 16, 44, 45\})$ and $(q = 8, g \in \{16, 22, 23, 45\})$.

iii) The modular curves $X(9)$, $X(11)$ and $X(13)$ yield the results for $(q = 4, g \in \{10, 26, 50\})$, and $X(8)$, $X(10)$, $X(11)$ and $X(13)$ yield the results for $(q = 9, g \in \{5, 13, 26, 50\})$.

The results collected in our tables represent the work of many mathematicians. We tried to give credit to whom it is due, but may have failed due to ignorance. A closer look at the tables will convince the reader that there is still ample room for improvement. The tables should be seen as an attempt to record the state of the art. If the reader knows an improvement of an entry we shall appreciate if he/she let us know so that we can update or correct the tables.

TABLE p = 2

$g\backslash q$	2	4	8	16	32	64	128
1	5	9	14	25	44	81	150
2	6	10	18	33	53	97	172
3	7	14	24	38	63–64	113	191–195
4	8	15	25–27	45–46	70–75	129	200–217
5	9	17–18	29–32	49–54	76–86	130–145	227–239
6	10	20	33–35	65	86–97	161	225–261
7	10	21–22	33–39	63–70	90–108	177	258–283
8	11	21–24	34–43	61–76	97–119	169–193	257–305
9	12	26	45–47	72–81	108–130	209	258–327
10	13	27–28	42–50	81–87		225	289–349
11	14	26–30	48–54	80–92	113–152	201–241	
12	14–15	29–31	49–57	68–97	129–163	257	321–393
13	15	33	56–61	97–103	129–174	225–270	
14	15–16	32–35	65	97–108	146–185	241–286	353–437
15	17	33–37	56–68	98–113	158–196	258–302	386–459
16	17–18	36–38	56–71	93–118	147–204		
17	17–18	40	62–74	112–124	154–212		
18	18–19	41–42	65–77	113–129	161–220	281–350	
19	20	37–43	60–80	121–134	172–228		
20	19–21	37–45	68–83	121–140	177–236	297–382	
21	21	41–47	72–86	129–145	185–244		
22	21–22	41–48	74–89	129–150		321–414	
23	22–23	41–50	68–92	126–155			
24	21–23	49–52	81–95	129–161		337–446	513–657
25	24	51–53	84–97	144–166			
26	24–25	55	82–100	150–171		385–478	
27	22–25	49–56	96–103	145–176	209–290	401–494	
28	25–26	51–58	97–106	145–181	257–298	513	577–745
29	25–27	52–60	97–109	161–187	227–306		
30	25–27	53–61	96–112	162–192	273–313	401–536	609–789
31	27–28	60–63	89–115	165–197		386–547	578–811
32	26–29	57–65	90–118				
33	28–29	65–66	92-121	193–207			
34	27–30	57–68	98–124	156–213			
35	29–31	64–69	112–127		253–352		
36	30–31	64–71	107–130	185–223			
37	29–32	66–72	121–132	208–228			
38	28–33	64–74	129–135	193–233	289–375	449–627	
39	33	65–75	120–138	194–239			
40	32–34	75–77	103–141	197–244	293–390	489–560	
41	33–35	65–78	118–144	216–249	308–398		
42	33–35	68–80	129–147	209–254	307–405	513–672	
43	33–36	72–81	116–150	226–259	306–413		
44	33–37	68–83	130–153	226–264	325–420		
45	33–37	80–84	144–156	242–268	304–428		
46	34–38	81–86	129–158	243–273			
47	36–38	73–87	120–161				
48	34–39	77–89	126–164				
49	36–40	81–90	130–167				
50	40	91–92	130–170	225–291		561–762	

Table p = 3

$g\backslash q$	3	9	27	81
1	7	16	38	100
2	8	20	48	118
3	10	28	56	136
4	12	30	64–66	154
5	12–13	32–35	69–76	156–172
6	14–15	35–40	76–86	190
7	16	40–43	76–96	160–208
8	15–18	38–47	92–106	226
9	19	48–51	88–116	244
10	19–21	54–55	91–126	226–262
11	20–22	55–59		
12	22–24	55–63	109–146	298
13	24–25	60–66	136–156	224–316
14	24–26	56–70		
15	28	64–74	136–171	292–352
16	27–29	74–78	136–178	370
17	24–30	64–82		
18	26–31	67–85		
19	28–32	84–88		
20	30–34	68–91		
21	32–35	88–95	163–214	352–458
22	30–36	78–98		
23	30–37	92–101		
24	31–38	91–104	190–235	
25	36–40	82–108	196–242	
26	36–41	110–111		
27	39–42	91–114		
28	37–43	105–117		
29	42–44	104–120		
30	37–46	91–123		
31	40–47	101–127		460–638
32	38–48	92–130		
33	46–49	109–133	220–238	
34	44–50	111–136		
35	47–51	101–139		
36	46–52	118–142	244–319	730
37	48–54	120–145		
38		105–149		
39	46–56	119–152	271–340	
40	54–57	110–155	244–346	
41	50–58	119–158		
42	49–59	118–161	280–360	
43	55–60	120–164		
44		119–167		
45	49–62	128–170		
46	55–63	162–173		
47	54–65	154–177	299–395	
48	55–66	163–180	325–402	676–885
49	63–67	168–183		
50	56–68	182–186	299–416	

$q = 2$: **sources**

genus	N	type	source
1	5	V-1	S1,4
2	6	V-1	S1,4
3	7	V-2	D
4	8	V-2	S1,4
5	9	I	S1,4
6	10	I	S1,4
7	10	I	S1,4
8	11	I	S1,4
9	12	I	S1,4
10	13	I	S5
11	14	I	S5
12	14–15	I	S2,4
13	15	I	S5
14	15–16	I	S2,4
15	17	I	S1,4
16	17–18	I	A
17	17–18	I	S2,4
18	18–19	I	S2,4
19	20	I	S1,4
20	19–21	I	S2,4
21	21	I	S1,4
22	21–22	I	Sch
23	22–23	I	X-N
24	21–23	III	G-V5
25	24	I	X-N
26	24–25	I	G-V4
27	22–25	I	G-V4
28	25–26	I	A
29	25–27	II	X-N
30	25–27	I	A
31	27–28	II	X-N
32	26–29	I	G-V4
33	28–29	I	G-V4
34	27–30	II	X-N
35	29–31	I	A
36	30–31	II	X-N
37	29–32	I	A
38	28–33	I	G-V4
39	33	I	S1,4
40	32–34	I	G-V4
41	33–35	I	A
42	33–35	I	A
43	33–36	II	X-N
44	33–37	I	A
45	33–37	III	G-V5
46	34–38	I	G-V4
47	36–38	I	G-V4
48	34–39	I	G-V4
49	36–40	II	X-N
50	40	I	S1,4

$q = 4$: **sources**

genus	N	type	source
1	9	V-1	S2,4
2	10	V-1	S2,4
3	14	V-2	S2,4
4	15	IV	S3
5	17–18	III	St2
6	20	I	G-V4
7	21–22	II	N-X3
8	21–24	I	N-X3
9	26	II	N-X4
10	27–28	V-3	G-V4
11	26–30	III	G-V5
12	29–31	I	A
13	33	III	St2
14	32–35	III	G-V5
15	33–37	II	N-X3
16	36–38	I	G-V4
17	40	II	N-X4
18	41–42	II	N-X7
19	37–43	I	A
20	37–45	I	A
21	41–47	II	N-X4
22	41–48	I	A
23	41–50	I	A
24	49–52	III	Sh
25	51–53	II	N-X4
26	55	V-3	G-V4
27	49–56	III	G-V4
28	51–58	I	A
29	52–60	III	Sh
30	53–61	II	N-X7
31	60–63	II	N-X4
32	57–65	I	A
33	65–66	I	L1
34	57–68	III	G-V4
35	64–69	III	Sh
36	64–71	II	N-X4
37	66–72	II	N-X4
38	64–74	III	Sh
39	65–75	III	G-V7
40	75–77	II	N-X4
41	65–78	III	G-V4
42	68–80	III	Sh
43	72–81	II	N-X4
44	68–83	I	G-V4
45	80–84	I	G-V4
46	81–86	II	N-X7
47	73–87	I	A
48	77–89	II	N-X4
49	81–90	II	N-X4
50	91–92	V-3	G-V4

$q = 8$: **sources**

genus	N	type	source
1	14	V-1	S2,4
2	18	V-1	S2,4
3	24	V-2	S2,4
4	25–27	III	G-V5
5	29–32	III	G-V4
6	33–35	III	St2
7	33–39	III	G-V1
8	34–43	III	Sh
9	45–47	II	N-X7
10	42–50	III	Sh
11	48–54	III	G-V5
12	49–57	III	G-V5
13	56–61	III	Sh
14	65	V-4	H-S
15	56–68	III	Sh
16	56–71	I	G-V4
17	62–74	III	Sh
18	65–77	III	G-V5
19	60–80	III	Sh
20	68–83	II	N-X6
21	72–86	III	G-V5
22	74–89	III	Sh
23	68–92	I	G-V4
24	81–95	III	Sh
25	84–97	III	Sh
26	82–100	III	Sh
27	96–103	III	Sh
28	97–106	III	G-V5
29	97–109	III	G-V4
30	96–112	III	Sh
31	89–115	III	Sh
32	90–118	III	Sh
33	92–121	II	N-X6
34	98–124	III	Sh
35	112–127	III	Sh
36	107–130	III	Sh
37	121–132	III	G-V5
38	129–135	III	G-V5
39	120–138	III	Sh
40	103–141	III	Sh
41	118–144	III	Sh
42	129–147	III	G-V5
43	116–150	III	Sh
44	130–153	III	Sh
45	144–156	I	G-V4
46	129–158	III	G-V4
47	120–161	II	N-X6
48	126–164	II	N-X6
49	130–167	II	N-X6
50	130–170	II	N-X6

$q = 16$: **sources**

genus	N	type	source
1	25	V-1	S2,4
2	33	V-1	S2,4
3	38	V-2	S3,4
4	45–46	V-2	M-Z-Z
5	49–54	III	G-V4
6	65	V-2	Seg
7	63–70	II	N-X6
8	61–76	III	G-V4
9	72–81	II	N-X6
10	81–87	II	N-X6
11	80–92	II	N-X6
12	68–97	III	G-V5
13	97–103	III	G-V4
14	97–108	III	G-V4
15	98–113	III	G-V1
16	93–118	III	G-V4
17	112–124	III	G-V5
18	113–129	III	G-V5
19	121–134	II	N-X6
20	121–140	III	G-V4
21	129–145	III	G-V5
22	129–150	III	St2
23	126–155	II	N-X6
24	129–161	III	G-V5
25	144–166	II	N-X6
26	150–171	II	N-X6
27	145–176	I	A
28	145–181	III	Sh
29	161–187	III	Sh
30	162–192	III	Do
31	165–197	V-2	G-S
32			
33	193–207	I	A
34	156–213	II	N-X6
35			
36	185–223	II	N-X7
37	208–228	II	N-X7
38	193–233	I	A
39	194–239	III	Sh
40	197–244	III	Sh
41	216–249	III	Sh
42	209–254	I	A
43	226–259	II	N-X7
44	226–264	III	Sh
45	242–268	III	G-V5
46	243–273	II	N-X6
47			
48			
49			
50	225–291	I	A

$q = 32$: **sources**

genus	N	type	source
1	44	V-1	S2,4
2	53	V-1	S2,4
3	63–64	V-2	M-Z-Z
4	70–75	V-2	M-Z-Z
5	76–86	IV	Sem
6	86–97	III	Do
7	90–108	III	Do
8	97–119	III	Sh
9	108–130	III	Sh
10			
11	113–152	I	A
12	129–163	III	G-V1
13	129–174	I	A
14	146–185	III	Do
15	158–196	V-2	H-Le B
16	147–204	III	Sh
17	154–212	III	Sh
18	161–220	I	A
19	172–228	III	Sh
20	177–236	III	Sh
21	185–244	III	Sh
22			
23			
24			
25			
26			
27	209–290	I	A
28	257–298	III	G-V1
29	227–306	III	Sh
30	273–313	III	G-V1
31			
32			
33			
34			
35	253–352	III	G-V5
36			
37			
38	289–375	I	A
39			
40	293–390	III	Sh
41	308–398	III	Sh
42	307–405	III	Sh
43	306–413	III	Sh
44	325–420	III	Sh
45	304–428	III	Sh
46			
47			
48			
49			
50			

$q = 64$: **sources**

genus	N	type	source
1	81	V-1	S2,4
2	97	V-1	S2,4
3	113	V-2	Wi
4	129	V-2	Wo
5	130–145	V-2	M-Z-Z
6	161	III	G-V3
7	177	V-2	Wo
8	169–193	I	A
9	209	V-5	G-S-X
10	225	V-5	E
11	201–241	III	G-V5
12	257	V-2	Wi
13	225–270	I	A
14	241–286	I	A
15	258–302	III	Do
16			
17			
18	281–350	I	A
19			
20	297–382	III	Do
21			
22	321–414	I	A
23			
24	337–446	I	A
25			
26	385–478	I	A
27	401–494	III	G-V5
28	513	V-2	H
29			
30	401–536	III	Do
31	386–547	III	Do
32			
33			
34			
35			
36			
37			
38	449–627	I	A
39			
40	489–650	IV	O-S
41			
42	513–672	III	Do
43			
44			
45			
46			
47			
48			
49			
50	561–762	I	A

$q = 128$: **sources**

genus	N	type	source
1	150	V-1	S2,4
2	172	V-1	S2,4
3	191–195	V-2	Su
4	200–217	V-2	Wi
5	227–239	V-2	M-Z-Z
6	225–261	V-2	Wi
7	258–283	III	Do
8	257–305	V-2	Wi
9	258–327	III	Do
10	289–349	III	G-V3
11			
12	321–393	III	G-V1
13			
14	353–437	III	G-V3
15	386–459	III	Do
16			
17			
18			
19			
20			
21			
22			
23			
24	513–657	III	G-V1
25			
26			
27			
28	577–745	III	G-V1
29			
30	609–789	III	G-V3
31	578–811	III	Do

$q = 3$: **sources**

genus	N	type	source
1	7	V-1	S1,4
2	8	V-1	S1,4
3	10	V-2	S2,4
4	12	V-2	S3
5	12–13	IV	N-X3
6	14–15	IV	N-X3
7	16	II	N-X3
8	15–18	IV	N-X3
9	19	III	G-V4
10	19–21	III	G-V4
11	20–22	I	N-X3
12	22–24	I	N-X3
13	24–25	I	N-X3
14	24–26	IV	N-X3
15	28	III	G-V4
16	27–29	III	G-V4
17	24–30	IV	N-X5
18	26–31	IV	N-X5
19	28–32	III	G-V5
20	30–34	III	G-V4
21	32–35	IV	N-X5
22	30–36	III	G-V5
23	30–37	III	G-V5
24	31–38	I	A
25	36–40	I	N-X5
26	36–41	IV	N-X5
27	39–42	I	N-X5
28	37–43	IV	N-X5
29	42–44	I	N-X5
30	37–46	III	G-V7
31	40–47	II	N-X5
32	38–48	IV	N-X5
33	46–49	I	A
34	44–50	II	N-X5
35	47–51	III	G-V7
36	46–52	III	G-V7
37	48–54	I	N-X5
38			
39	46–56	III	G-V7
40	54–57	II	N-X5
41	50–58	II	N-X5
42	49–59	III	G-V7
43	55–60	II	X-N
44			
45	49–62	III	G-V7
46	55–63	III	G-V4
47	54–65	I	A
48	55–66	III	G-V4
49	63–67	III	G-V5
50	56–68	II	N-X5

$q = 9$: **sources**

genus	N	type	source
1	16	V-1	S2,4
2	20	V-1	S2,4
3	28	V-2	S2,4
4	30	IV	G-V5
5	32–35	V-3	G-V4
6	35–40	II	N-X7
7	40–43	IV	O-S
8	38–47	III	G-V2
9	48–51	IV	O-S
10	54–55	III	G-V5
11	55–59	III	G-V2
12	55–63	III	G-V2
13	60–66	V-3	G-V4
14	56–70	III	G-V5
15	64–74	III	Sh
16	74–78	III	G-V5
17	64–82	IV	O-S
18	67–85	III	Sh
19	84–88	II	N-X7
20	68–91	III	Sh
21	88–95	IV	O-S
22	78–98	II	N-X7
23	92–101	II	N-X7
24	91–104	II	N-X7
25	82–108	III	Sh
26	110–111	V-3	G-V4
27	91–114	III	Sh
28	105–117	II	N-X7
29	104–120	II	N-X7
30	91–123	III	Sh
31	101–127	III	Sh
32	92–130	III	Sh
33	109–133	III	Sh
34	111–136	II	N-X7
35	101–139	III	Sh
36	118–142	III	Sh
37	120–145	II	N-X7
38	105–149	II	N-X8
39	119–152	III	Sh
40	118–155	III	Sh
41	119–158	III	Sh
42	118–161	III	Sh
43	120–164	II	N-X7
44	119–167	III	Sh
45	128–170	III	Sh
46	162–173	III	Sh
47	154–177	II	N-X7
48	163–180	III	Sh
49	168–183	II	N-X7
50	182–186	V-3	G-V4

$q = 27$: **sources**

genus	N	type	source
1	38	V-1	S2,4
2	48	V-1	S2,4
3	56	IV	G-V5
4	64–66	III	G-V2
5	68–76	IV	Sem
6	76–86	III	G-V2
7	76–96	IV	Sem
8	92–106	III	G-V5
9	88–116	IV	Sem
10	91–126	I	A
11			
12	109–146	III	G-V2
13	136–156	III	G-V2
14			
15	136–171	I	A
16	136–178	I	A
17			
18			
19			
20			
21	163–214	III	G-V6
22			
23			
24	190–235	III	Sh
25	196–242	II	N-X7
26			
27			
28			
29			
30			
31			
32			
33	220–298	II	N-X7
34			
35			
36	244–319	III	G-V2
37			
38			
39	271–340	III	G-V6
40	244–346	III	G-V5
41			
42	280–360	II	N-X7
43			
44			
45			
46			
47	299–395	III	Sh
48	325–402	I	A
49			
50	299–416	III	Sh

$q = 81$: **sources**

genus	N	type	source
1	100	V-1	S2,4
2	118	V-1	S2,4
3	136	V-2	Wi
4	154	V-5	H
5	156–172	IV	Sem
6	190	V-2	Seg
7	160–208	V-2	Wi
8	226	V-5	E
9	244	V-2	Wo
10	226–262	V-2	Wi
11			
12	298	III	G-V2
13	224–316	IV	Sem
14			
15	292–352	IV	O-S
16	370	V-5	H
17			
18			
19			
20			
21	352–458	I	A
22			
23			
24			
25			
26			
27			
28			
29			
30			
31	460–638	I	A
32			
33			
34			
35			
36	730	V-2	St1
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48	676–885	I	A
49			
50			

Acknowledgments

We would like to thank R. Auer, A. Brouwer, N. Elkies, K. Lauter, H. Niederreiter, R. Schoof, S. Sémirat, J.-P. Serre, V. Shabat, H. Stichtenoth, M. Suzuki and C. P. Xing for communicating results to us.

References

[A] R. Auer: Ray class fields of global function fields with many rational places. Report University of Oldenburg, 1998.

[D] L.E. Dickson: Geometrical and invariantive theory of quartic curves modulo 2. *Am. J. Math.* **37** (1915), 337–354

[Do] J. Doumen: Master's thesis. Leiden University, 1998.

[E] N. Elkies: Private communication, 1997.

[F-T] R. Fuhrmann, F. Torres: The genus of curves over finite fields with many rational points. *Manuscripta Math.* **89** (1996), 103–106. MR **96m:**11046

[G-S] A. Garcia, H. Stichtenoth: A class of polynomials over finite fields. Preprint, 1998.

[G-S-X] A. Garcia, H. Stichtenoth, C.P. Xing: On subfields of the Hermitian function field. Preprint 1998.

[G-V1] G. van der Geer, M. van der Vlugt: Curves over finite fields of characteristic 2 with many rational points. *C.R. Acad. Sci. Paris* **317**, Série I (1993), 593–597. MR **94k:**11068

[G-V2] G. van der Geer, M. van der Vlugt: Generalized Hamming weights of codes and curves over finite fields with many points. In: *Israel Math Conf. Proc.* **9** (1996), 417–432. MR **96m:**11047

[G-V3] G. van der Geer, M. van der Vlugt: Quadratic forms, generalized Hamming weights of codes and curves with many points. *J. of Number Theory* **59** (1996), 20–36. MR **97i:**11068

[G-V4] G. van der Geer, M. van der Vlugt: How to construct curves over finite fields with many points. In: *Arithmetic Geometry*, (Cortona 1994), F. Catanese Ed., *Sympos. Math.* **37** Cambridge Univ. Press, Cambridge, 1997, 169–189. MR **98h:**11077

[G-V5] G. van der Geer, M. van der Vlugt: Tables for the function $N_q(g)$. Regularly updated tables at: `http://www.wins.uva.nl/ ˜geer` .

[G-V6] G. van der Geer, M. van der Vlugt: Generalized Reed-Muller codes and curves with many points. *J. of Number Theory* **72** (1998) 257–268. CMP 99:04

[G-V7] G. van der Geer, M. van der Vlugt: Constructing curves over finite fields with many rational points by solving linear equations. Report W 97-29, Leiden University 1997.

[G] V.D. Goppa : Codes on algebraic curves. *Sov. Math. Dokl.* **24** (1981), 170–172. MR **82k:**94017

[H] J.P. Hansen: Group codes and algebraic curves. Mathematica Gottingensis, Schriftenreihe SFB Geometrie und Analysis, Heft 9, 1987.

[H-Le B] G. Haché, D. Le Brigand: Effective construction of algebraic geometry codes. *IEEE Trans. Inform. Theory* **41** (1995), 1615–1628. MR **97g:**94037

[H-S] J.P. Hansen, H. Stichtenoth: Group codes on certain algebraic curves with many rational points. *Appl. Algebra Engrg. Comm. Comput.* **1** (1990), 67–77. MR **96e:**94023

[I] Y. Ihara: Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo* **28** (1981), 721–724. MR **84c:**14016

[L1] K. Lauter: Ray class field constructions of curves over finite fields with many rational points. In: *Algorithmic Number Theory* (Talence 1996), H. Cohen Ed., Lecture Notes in Computer Science 1122, Springer, Berlin, 1996, 187–195. MR **98a:**11076

[L2] K. Lauter: Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points. Preprint 1998.

[L3] K. Lauter: Improved upper bounds for the number of rational points on algebraic curves over finite fields. Preprint, University of Michigan, 1999.

[M-Z-Z] O. Moreno, D. Zinoviev, V. Zinoviev: On several new projective curves over $\mathbb{F}_2$ of genus $3, 4$ and 5. *IEEE Trans. Inform. Theory* **41** (1995), 1643–1645. MR **97b:**14032

[N-X1] H. Niederreiter, C. P. Xing: Quasi-random points and global function fields. In: *Finite Fields and Applications*, S.D. Cohen, H. Niederreiter Eds., Cambridge Univ. Press, Cambridge 1996, 269–296. MR **97j:**11037

[N-X2] H. Niederreiter, C. P. Xing: Explicit global function fields over the binary field with many rational places. *Acta Arithm.* **75** (1996), 383–396. MR **97d:**11177

[N-X3] H. Niederreiter, C. P. Xing: Cyclotomic function fields, Hilbert class fields and global function fields with many rational places. *Acta Arithm.* **79** (1997), 59–76. MR **97m:**11141

[N-X4] H. Niederreiter, C. P. Xing: Drinfeld modules of rank 1 and algebraic curves with many rational points II. *Acta Arithm.* **81** (1997), 81–100. CMP 97:14

[N-X5] H. Niederreiter, C. P. Xing: Global function fields fields with many rational points over the ternary field. *Acta Arithm.* **83** (1998), 65–86. MR **98j:**11110

[N-X6] H. Niederreiter, C. P. Xing: Algebraic curves with many rational points over finite fields of characteristic 2. To appear in: *Proc. Number Theory Conference* (Zakopane 1997), de Gruyter, Berlin.

[N-X7] H. Niederreiter, C. P. Xing: A general method of constructing global function fields with many rational places. To appear in: *Algorithmic Number Theory* (Portland 1998), Lecture Notes in Comp. Science, Springer, Berlin.

[N-X8] H. Niederreiter, C. P. Xing: Nets, (t, s)-sequences and algebraic geometry. To appear in *Pseudo- and quasi-random point sets*, P. Hellekalek, G. Larcher, Eds. Lecture Notes in Statistics, Springer, New York, 1998.

[O-S] F. Özbudak, H. Stichtenoth: Curves with many points and configurations of hyperplanes over finite fields. Preprint 1998.

[Sch] R. Schoof: Algebraic curves and coding theory. UTM 336, Univ. of Trento, 1990.

[Seg] B. Segre: Introduction to Galois geometries. *Atti Acad. Naz. Lincei (Mem. Cl. Sci. Fis. Mat. Natur.)* **8** (1967), 133–236. MR **39:**206

[Sem] S. Sémirat: Genus theory for quadratic fields and applications. Preprint Université Paris VI, 1998.

[S1] J-P. Serre : Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini. *C.R. Acad. Sci. Paris* **296**, Série I (1983), 397–402. (= Oeuvres III, No. 128, 658–663). MR **85b:**14027; MR **89h:**01109c

[S2] J-P. Serre : Nombre de points des courbes algébriques sur $\mathbb{F}_q$. Sém. de Théorie des Nombres de Bordeaux, 1982/83, exp. no. 22. (= Oeuvres III, No. 129, 664–668). MR **86d:**11051; MR **89h:**01109c

[S3] J-P. Serre : Quel est le nombre maximum de points rationnels que peut avoir une courbe algébrique de genre g sur un corps fini $\mathbb{F}_q$? Résumé des Cours de 1983-1984. (=Oeuvres III, No. 132, 701–705). MR **89h:**01109c

[S4] J-P. Serre: Rational points on curves over finite fields. Notes of lectures at Harvard University 1985.

[S5] J-P. Serre: Letter to G. van der Geer, September 1, 1997.

[Sh] V. Shabat: Unpublished manuscript, University of Amsterdam, 1997/98.

[St1] H. Stichtenoth: Self-dual Goppa codes. *J. Pure and Appl. Algebra* **55** (1988), 199–211. MR **90a:**11150

[St2] H. Stichtenoth: Algebraic-geometric codes associated to Artin-Schreier extensions of $\mathbb{F}_q(z)$. In: *Proc. 2nd Int. Workshop on Alg. and Comb. Coding Theory*, Leningrad (1990), 203–206.

[S-V] K.O. Stöhr, J. F. Voloch: Weierstrass points and curves over finite fields. *Proc. London Math. Soc.* **52** (1986), 1–19. MR **87b:**14010

[Su] M. Suzuki: Private communication, 1998.

[Wi] M. Wirtz : Konstruktion und Tabellen linearer Codes. Westfälische Wilhelms-Universität Münster, 1991.

[Wo] J. Wolfmann: Nombre de points rationnels de courbes algébriques sur des corps finis associées à des codes cycliques. *C.R. Acad. Sci. Paris* **305**, Série I (1987), 345–348. MR **88k:**11025

[X-N] C. P. Xing, H. Niederreiter: Drinfeld modules of rank 1 and algebraic curves with many rational points. Report Austrian Academy of Sciences, Vienna, 1996.

Faculteit WINS, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands

E-mail address: `geer@wins.uva.nl`

Mathematisch Instituut, Rijksuniversiteit te Leiden, Niels Bohrweg 1, 2300 RA Leiden, The Netherlands

E-mail address: `vlugt@wi.leidenuniv.nl`