

# The number of solutions of certain Catalan equations in finite fields

MARKO MOISIO AND KEIJO VÄÄNÄNEN

**Abstract.** We calculate by an elementary method the number of solutions of certain equations of the form  $ax^m + by^n = 1$  in finite fields, as a function of  $a$  and  $b$ . We also calculate the number of rational places of the function fields which correspond our equations and as a corollary we get a complete characterization of those of them which are maximal (resp. minimal).

## 1. Introduction and results

Let  $m$  and  $n$  be natural numbers greater than 1. We shall consider the number of solutions  $(x, y) \in \mathbb{F}_q^2$  of certain Catalan equations

$$ax^m + by^n = 1, \quad a, b \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}, \quad (1)$$

in finite fields  $\mathbb{F}_q$  with  $q = p^{2ls}$  elements. In fact, if  $m$  and  $n$  are factors of  $p^s + 1$  we shall explicitly determine, in an elementary way, the number of solutions of (1) as a function of the coefficients  $a$  and  $b$ . When we interpret (1) as the defining equation of an algebraic function field  $F := \mathbb{F}_q(x, y)$  we are able to calculate the number of rational places of  $F$ , or equivalently the number of  $\mathbb{F}_q$ -rational points of the nonsingular model of an algebraic curve with (1) as the defining equation. As a corollary we get a complete characterization of those function fields  $F$  which are maximal (resp. minimal), i.e. when the number of rational places of  $F$  attains the upper (resp. lower) Hasse-Weil bound (cf. [1, pp. 1557-1558]).

Typeset by  $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$

More precisely we shall prove the following theorems, where  $\gamma$  is a fixed primitive element of  $\mathbb{F}_q$ , and for an element  $a = \gamma^i$  we denote  $i(a) := i = \text{ind}_\gamma(a)$ .

**Theorem 1.** *If  $\gcd(m, n) = d$  and  $m, n \mid p^s + 1$ , then the number of solutions of (1) is*

$$\begin{aligned} q + 1 + (-1)^{l-1}((m-1)(n-1) + 1 - d)\sqrt{q} - d & \quad \text{if } m \mid i(a) \text{ and } n \mid i(b), \\ q + 1 + (-1)^l(m-1)\sqrt{q} + \delta(a, b) & \quad \text{if } m \mid i(a) \text{ and } n \nmid i(b), \\ q + 1 + (-1)^l(n-1)\sqrt{q} + \delta(a, b) & \quad \text{if } m \nmid i(a) \text{ and } n \mid i(b), \\ q + 1 + (-1)^{l-1}\sqrt{q} + \delta(a, b) & \quad \text{if } m \nmid i(a) \text{ and } n \nmid i(b), \end{aligned}$$

where

$$\delta(a, b) = \begin{cases} (-1)^l(d-1)\sqrt{q} - d & \text{if } i(a) \equiv i(b) \pmod{d}, \\ (-1)^{l-1}\sqrt{q} & \text{if } i(a) \not\equiv i(b) \pmod{d}. \end{cases}$$

**Theorem 2.** *Let  $F := \mathbb{F}_q(x, y)$  be the algebraic function field obtained by adjoining a root  $y$  of the polynomial  $bT^n + ax^m - 1 \in \mathbb{F}_q(x)[T]$  to the rational function field  $\mathbb{F}_q(x)$ . The number of rational places of  $F$  is*

$$\begin{aligned} q + 1 + (-1)^{l-1}((m-1)(n-1) + 1 - d)\sqrt{q} & \quad \text{if } m \mid i(a) \text{ and } n \mid i(b), \\ q + 1 + (-1)^l(m-1)\sqrt{q} + \delta(a, b) & \quad \text{if } m \mid i(a) \text{ and } n \nmid i(b), \\ q + 1 + (-1)^l(n-1)\sqrt{q} + \delta(a, b) & \quad \text{if } m \nmid i(a) \text{ and } n \mid i(b), \\ q + 1 + (-1)^{l-1}\sqrt{q} + \delta(a, b) & \quad \text{if } m \nmid i(a) \text{ and } n \nmid i(b), \end{aligned}$$

where

$$\delta(a, b) = \begin{cases} (-1)^l(d-1)\sqrt{q} & \text{if } i(a) \equiv i(b) \pmod{d}, \\ (-1)^{l-1}\sqrt{q} & \text{if } i(a) \not\equiv i(b) \pmod{d}. \end{cases}$$

**Corollary.** *The number of rational places of  $F$  attains upper (resp. lower) Hasse-Weil bound  $q + 1 + 2g\sqrt{q}$  (resp.  $q + 1 - 2g\sqrt{q}$ ), where  $g$  is the genus of  $F$ , if and only if one of the following five cases is valid:*

- (1)  $m \mid i(a)$ ,  $n \mid i(b)$ ,  $2 \nmid l$  (resp.  $2 \mid l$ );
- (2)  $n = 2$ ,  $m \mid i(a)$ ,  $n \nmid i(b)$ ,  $2 \mid l$  (resp.  $2 \nmid l$ );
- (3)  $m = 2$ ,  $m \nmid i(a)$ ,  $n \mid i(b)$ ,  $2 \mid l$  (resp.  $2 \nmid l$ );

(4)  $(m, n) = (2, 4), (4, 2)$  or  $(3, 3)$ , and  $m \nmid i(a), n \nmid i(b), 2 \nmid l$  (resp.  $2 \mid l$ );

(5)  $(m, n) = (2, 2)$ .

*Proof.* The genus of  $F$  is  $((m-1)(n-1) + 1 - d)/2$  (see [3, p. 197]).

## 2. Notations and fundamental equality

We denote by  $e$  the canonical additive character of  $\mathbb{F}_q$ . In the following we frequently use the notations

$$S(a, m) = \sum_{x \in \mathbb{F}_q} e(ax^m), \quad S^*(a, m) = \sum_{x \in \mathbb{F}_q^*} e(ax^m).$$

It follows from the ortogonality of the characters of a finite group that the number  $N$  of solutions  $(x, y) \in \mathbb{F}_q^2$  of (1) is

$$\begin{aligned} N &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} e(-c) \left( \sum_{x \in \mathbb{F}_q} e(cax^m) \right) \left( \sum_{y \in \mathbb{F}_q} e(cby^n) \right) \\ &= q + \frac{1}{q} \sum_{c \in \mathbb{F}_q^*} e(-c) S(ca, m) S(cb, n). \end{aligned}$$

Let  $S$  denote the sum  $\sum_{c \in \mathbb{F}_q^*} e(-c) S(ca, m) S(cb, n)$  above. Now

$$\begin{aligned} S &= \sum_{j=0}^{n-1} \sum_{i=0}^{\frac{q-1}{n}-1} e(-\gamma^{ni+j}) S(\gamma^{ni+j}a, m) S(\gamma^{ni+j}b, n) \\ &= \sum_{j=0}^{n-1} \sum_{i=0}^{\frac{q-1}{n}-1} e(-\gamma^{ni+j}) S(\gamma^{ni+j}a, m) S(\gamma^j b, n) \\ &= \sum_{j=0}^{n-1} S(\gamma^j b, n) \sum_{t=0}^{\frac{m}{d}-1} \sum_{k=0}^{\frac{q-1}{D}-1} e(-\gamma^{Dk+nt+j}) S(\gamma^{Dk+nt+j}a, m), \end{aligned}$$

where we denote  $D = mn/d$ . From this we get an important fundamental equality

$$S = \frac{1}{D} \sum_{j=0}^{n-1} S(\gamma^j b, n) \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j}a, m) S^*(-\gamma^{nt+j}, D), \quad (2)$$

where we have used the fact

$$\sum_{k=0}^{\frac{q-1}{D}-1} e(-\gamma^{nt+j}\gamma^{Dk}) = \frac{1}{D} S^*(-\gamma^{nt+j}, D).$$

As we shall see, the equality (2) is very useful for the calculation of  $N$ . In the case  $m, n \mid p^s + 1$ , which we shall assume from now on, we may apply the following theorem proved in [2] (and in [3]).

**Theorem A.** *If  $k \mid p^s + 1$ ,  $k > 1$ , then*

$$S(a, k) = \begin{cases} (-1)^l \sqrt{q} & \text{if } i(a) \not\equiv r \pmod{k}, \\ (-1)^{l-1} (k-1) \sqrt{q} & \text{if } i(a) \equiv r \pmod{k}, \end{cases}$$

where  $r = 0$  if

(i)  $p = 2$ ; or  $p > 2$  and  $2 \mid l$ ; or  $p > 2$ ,  $2 \nmid l$  and  $2 \mid (p^s + 1)/k$ ,

and  $r = k/2$  if

(ii)  $p > 2$ ,  $2 \nmid l$  and  $2 \nmid (p^s + 1)/k$ .

*Remark.* We have either  $-1 = 1$  or  $-1 = \gamma^{(q-1)/2}$  and  $D \mid (q-1)/2$  which means that we have above

$$S^*(-\gamma^{nt+j}, D) = S^*(\gamma^{nt+j}, D).$$

### 3. The consideration of $S$

Clearly  $nt + j \equiv r \pmod{D}$  has a unique solution  $(t', j')$  satisfying  $0 \leq j' \leq n-1$ ,  $0 \leq t' \leq m/d-1$ . Therefore Theorem A implies

$$\begin{aligned} S &= \frac{1}{D} ((A-1)S(\gamma^{j'}b, n)S(\gamma^r a, m) + (B-1) \sum_{j=0}^{n-1} \sum_{\substack{t=0 \\ (t,j) \neq (t',j')}}^{\frac{m}{d}-1} S(\gamma^j b, n)S(\gamma^{nt+j} a, m)) \\ &= \frac{1}{D} ((A-B)S(\gamma^{j'}b, n)S(\gamma^r a, m) + (B-1)S_1), \end{aligned}$$

where

$$A = (-1)^{l-1} (D-1) \sqrt{q}, \quad B = (-1)^l \sqrt{q},$$

and

$$S_1 = \sum_{j=0}^{n-1} S(\gamma^j b, n) \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j} a, m). \quad (3)$$

In the above expression for  $S$  we can calculate  $S(\gamma^{j'} b, n)S(\gamma^r a, m)$  directly by Theorem A.

We have  $r = 0$  unless  $p > 2$  and  $2 \nmid l$  and  $2 \nmid (p^s + 1)/D$  in which case  $r = D/2$ . Assume  $r = 0$ . If  $(p^s + 1)/D$  is even clearly  $(p^s + 1)/m$  and  $(p^s + 1)/n$  are even. Since also  $j' = 0$  Theorem A implies

$$\begin{aligned} S(\gamma^{j'} b, n)S(\gamma^r a, m) &= S(b, n)S(a, m) \\ &= \begin{cases} CE & \text{if } m \mid i(a), \quad n \mid i(b), \\ BE & \text{if } m \mid i(a), \quad n \nmid i(b), \\ CB & \text{if } m \nmid i(a), \quad n \mid i(b), \\ B^2 & \text{if } m \nmid i(a), \quad n \nmid i(b), \end{cases} \end{aligned} \quad (4)$$

where

$$C = (-1)^{l-1}(n-1)\sqrt{q}, \quad E = (-1)^{l-1}(m-1)\sqrt{q}.$$

Next we consider the case  $r = D/2$ . Since  $D/2 = mn/2d$  and  $nt' + j' = D/2$  we have

$$j' \equiv \frac{D}{2} \equiv \begin{cases} 0 \ (n) & \text{if } 2 \mid \frac{m}{d}, \\ \frac{n}{2} \ (n) & \text{if } 2 \nmid \frac{m}{d}. \end{cases}$$

In the same way

$$r \equiv \begin{cases} 0 \ (m) & \text{if } 2 \mid \frac{n}{d}, \\ \frac{m}{2} \ (m) & \text{if } 2 \nmid \frac{n}{d}. \end{cases}$$

Because  $(p^s + 1)/D$  is odd we have

$$2 \mid \frac{(p^s + 1)}{h} \Leftrightarrow 2 \mid \frac{h}{d}$$

whether  $h$  is  $n$  or  $m$ .

Thus we have two cases. If  $m/d$  is even then  $(p^s + 1)/n$  is even and  $j' + i(b) \equiv i(b) \ (n)$ . In the other case both  $m/d$  and  $(p^s + 1)/n$  are odd and  $j' + i(b) \equiv n/2 + i(b) \ (n)$ . In both cases Theorem A implies

$$S(\gamma^{j'} b, n) = \begin{cases} B & \text{if } n \nmid i(b), \\ C & \text{if } n \mid i(b). \end{cases}$$

Just in the same way we get

$$S(\gamma^r b, m) = \begin{cases} B & \text{if } m \nmid i(a), \\ C & \text{if } m \mid i(a). \end{cases}$$

Thus the equality (4) is valid also in the case  $r = D/2$ .

#### 4. The sum $S_1$

To consider sum  $S_1$  in (3) we denote by  $j''$ ,  $0 \leq j'' \leq n-1$ , the solution of  $j+i(b) \equiv r_n \pmod{n}$ , where  $r_n = 0$  or  $n/2$  depending on the cases (i) or (ii) of Theorem A. By this theorem

$$\begin{aligned} S_1 &= \sum_{j=0}^{n-1} S(\gamma^j b, n) \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j} a, m) \\ &= C \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j''} a, m) + B \sum_{\substack{j=0 \\ j \neq j''}}^{n-1} \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j} a, m) \\ &= (C - B)S_2 + BS_3, \end{aligned}$$

where

$$S_2 = \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j''} a, m), \quad S_3 = \sum_{j=0}^{n-1} \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+j} a, m).$$

To calculate  $S_3$  we give it in the form

$$S_3 = \sum_{k=0}^{\frac{n}{d}-1} \sum_{i=0}^{d-1} \sum_{t=0}^{\frac{m}{d}-1} S(\gamma^{nt+kd+i} a, m).$$

For fixed  $k$  the congruence  $nt + kd + i + i(a) \equiv r_m \pmod{m}$ , where  $r_m = 0$  or  $m/2$ , is solvable if and only if  $d$  is a factor of  $r_m - i - kd - i(a)$ . This is satisfied by unique  $i$ ,  $0 \leq i \leq d-1$ , say  $i = i'$ , and then the congruence above has a unique solution  $t = t'$ ,  $0 \leq t' \leq m/d - 1$ . Thus Theorem A implies

$$S_3 = \sum_{k=0}^{\frac{n}{d}-1} (E - (m-1)B) = \frac{n}{d} ((-1)^{l-1} (m-1) \sqrt{q} + (-1)^l (m-1) \sqrt{q}) = 0.$$

There still remains the sum  $S_2$ . For the consideration of this we give the following lemmas.

**Lemma 1.**  $r_m \equiv r_n \pmod{d}$ .

*Proof.* If  $p = 2$  or  $2 \mid l$ , we have  $r_m = r_n = 0$ , and the result follows. Assume  $p > 2$  and  $2 \nmid l$ . We then have the following possibilities:

- 1)  $r_m = r_n = 0$  if both  $(p^s + 1)/m$  and  $(p^s + 1)/n$  are even.
- 2)  $r_m = 0$ ,  $r_n = n/2$  if  $(p^s + 1)/m$  is even and  $(p^s + 1)/n$  is odd. In this case clearly  $2d \mid n$  and  $r_m \equiv r_n \pmod{d}$ .
- 3)  $r_m = m/2$ ,  $r_n = 0$  if  $(p^s + 1)/m$  is odd and  $(p^s + 1)/n$  is even. Analogously to the above case  $r_m \equiv r_n \pmod{d}$ .
- 4)  $r_m = m/2$ ,  $r_n = n/2$  if both  $(p^s + 1)/m$  and  $(p^s + 1)/n$  are odd. In this case we have  $p^s + 1 = 2^l L$ ,  $m = 2^l H$ ,  $n = 2^l K$ , where  $L$ ,  $H$  and  $K$  are odd integers. Thus  $d = 2^l \gcd(H, K)$  and

$$r_m - r_n = 2^l \frac{H - K}{2} \equiv 0 \pmod{d}.$$

This proves Lemma 1.

**Lemma 2.** *The congruence  $nt + j'' + i(a) \equiv r_m \pmod{m}$  is solvable if and only if  $i(a) \equiv i(b) \pmod{d}$ . The solution is unique modulo  $m/d$ .*

*Proof.* The congruence is solvable if and only if  $d$  divides  $r_m - j'' - i(a)$ . From the definition of  $j''$  it follows that  $n$  divides  $r_n - j'' - i(b)$ , and thus the above condition for the solvability of the congruence is true if and only if

$$r_m - r_n \equiv i(a) - i(b) \pmod{d}.$$

By Lemma 1 this is equivalent with the condition  $i(a) \equiv i(b) \pmod{d}$ . Clearly the solution is unique modulo  $m/d$ . This completes the proof of Lemma 2.

We now use Lemma 2 and Theorem A to obtain for the sum  $S_2$  the value

$$S_2 = \begin{cases} E + \left(\frac{m}{d} - 1\right)B & \text{if } i(a) \equiv i(b) \pmod{d}, \\ \frac{m}{d}B & \text{if } i(a) \not\equiv i(b) \pmod{d}. \end{cases}$$

Thus we are ready with the sum  $S_2$ .

## 5. The proofs of Theorem 1 and Theorem 2

By the above considerations we have

$$\begin{aligned} N &= q + \frac{1}{q}S \\ &= q + \frac{1}{qD}(A - B)S(a, m)S(b, n) + \frac{1}{qD}(B - 1)(C - B)S_2. \end{aligned}$$

By using (4) and the above value of  $S_2$  together with the definitions of  $A$ ,  $B$ ,  $C$  and  $E$  we immediately obtain Theorem 1.

To prove Theorem 2 we denote by  $\overline{\mathbb{F}}_q$  a fixed algebraic closure of  $\mathbb{F}_q$  and by  $C'$  the projective closure of the curve  $C = \{(x, y) \in \overline{\mathbb{F}}_q^2 \mid ax^m + by^n = 1\}$ .

Since every finite point of  $C'$  is non-singular the solutions of (1) in  $\mathbb{F}_q^2$ , i.e. the finite  $\mathbb{F}_q$ -rational points of  $C'$ , are in bijection with those rational places of  $F$  lying above finite places of the rational function field  $\mathbb{F}_q(x)$ . Thus to prove Theorem 2 we need only calculate the number of rational places of  $F$  lying above the infinity place  $P_\infty$  of  $\mathbb{F}_q(x)$ . This is easily done with the theory of Kummer extensions [4, p. 110].

First we notice that  $y$  is a root of  $T^n + ab^{-1}x^m - b^{-1}$ . Since the roots of  $-ab^{-1}x^m + b^{-1}$  are simple  $F/\mathbb{F}_q(x)$  is a Kummer extension. Let  $M := \mathbb{F}_q(x, z)$  with  $z = y^{n/d}$ . Now  $z^d = -ab^{-1}x^m + b^{-1}$  and  $[M : \mathbb{F}_q(x)] = d$ . Since

$$\left(\frac{z}{x^{\frac{m}{d}}}\right)^d = b^{-1} \left(\frac{1}{x}\right)^m - ab^{-1}$$

we see that to determine the number of places of  $M$  lying above  $P_\infty$  we only have to calculate the number of places of the field  $\mathbb{F}_q(u, w)$  with  $u = 1/x$ ,  $w = z/x^{m/d}$ ,  $w^d = b^{-1}u^m - ab^{-1}$  lying above  $P_0$ , the place of  $\mathbb{F}_q(u)$  with an uniformizing parameter  $u$ . It follows from Kummer's theorem [4, p. 80] that the number of rational places  $Q_i$  of  $M$  lying above  $P_\infty$  equals  $d$  if  $i(a) \equiv i(b) \pmod{d}$  and zero otherwise.

If  $i(a) \not\equiv i(b) \pmod{d}$  the transitivity of degrees of places and the fact that every place of  $F$  lying above  $P_\infty$  lies above some place of  $M$  prove Theorem 2.

Assume  $i(a) \equiv i(b) \pmod{d}$ . Let  $R$  be any place of  $F$  lying above  $P_\infty$ . By Theorem III.7.3 of [4, p. 110] the ramification index  $e(R \mid P_\infty) = n/d$ , since the value of

$-ab^{-1}x^m + b^{-1}$  at  $P_\infty$  equals  $-m$ . But  $R$  lies above  $Q_i$  for some  $i = 1, \dots, d$ , and therefore the transitivity relation  $e(R | P_\infty) = e(R | Q_i)e(Q_i | P_\infty)$  and the fact that  $P_\infty$  does not ramify in  $M$  imply  $e(R | Q_i) = n/d$ . Now the fundamental equation  $e(R | Q_i)f(R | Q_i)r = n/d$  implies  $r = f(R | Q_i) = 1$  or there exists only one place  $R$  of  $F$  lying above  $Q_i$  and it is rational. Furthermore, since for each  $Q_i$  there exists a place  $R$  lying above  $P_\infty$  we deduce that there are exactly  $d$  rational places of  $F$  lying above  $P_\infty$  and thus Theorem 2 follows.

### References

- [1] A. Garcia and H. Stichtenoth, Algebraic Function Fields over Finite Fields with Many Rational Places, *IEEE Trans. Inform. Theory*, **41** (1995), 1548-1563.
- [2] M. Moisio, "Exponential sums, Gauss sums and cyclic codes," Dissertation, Acta Univ. Oul. A 306, 1998.
- [3] M. Moisio, "A note on evaluations of some exponential sums," Acta Arithmetica, submitted.
- [4] H. Stichtenoth, "Algebraic Function Fields and Codes," Berlin-Heidelberg-New York, Springer-Verlag, 1993.