Title
On Katz's bound for the number of elements with given trace and norm

Journal
Journal für die reine und angewandte Mathematik (Crelles Journal), 2010(638)

ISSN
0075-4102

Authors
Moisio, Marko
Wan, Daqing

Publication Date
2010

DOI
10.1515/crelle.2010.002

Peer reviewed

ON KATZ'S BOUND FOR NUMBER OF ELEMENTS WITH GIVEN TRACE AND NORM

MARKO MOISIO AND DAQING WAN

ABSTRACT. In this note an improvement of the Katz's bound on the number of elements in a finite field with given trace and norm is given. The improvement is obtained by reducing the problem to estimating the number of rational points on certain toric Calabi-Yau hypersurface, and then to use detailed cohomological calculations by Rojas-Leon and the second author for such toric hypersurfaces.

1. INTRODUCTION

Let p be a prime and $\mathbb{F}_q$ be the finite field of q elements of characteristic p. Given $a, b \in \mathbb{F}_q$, and positive integer $m \geq 2$, let

$$N_m(a,b) = \#\{\alpha \in \mathbb{F}_{q^m} | \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = a, \mathrm{Norm}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = b\}.$$

Motivated by various applications, it is of interest to give a sharp estimate for the number $N_m(a,b)$. The case $b = 0$ is trivial.

Katz [2] proved the following bound:

Theorem 1.1. *Let $a, b \in \mathbb{F}_q^*$ and $n \geq 1$. Then*

$$|N_{n+1}(a,b) - \frac{q^{n+1}-1}{q(q-1)}| \leq (n+1)q^{\frac{n-1}{2}}.$$

This bound was used by Moisio [3] to improve some cases of the explicit bound in Wan [5] on the number of irreducible polynomials in an arithmetic progression of $\mathbb{F}_q[x]$. In the case $n+1 = 3$, the Katz bound also plays a significant role in Cohen and Huczynska [1] for their proof of the existence of a cubic primitive normal polynomial with given norm and trace.

If $a = 0$, Katz's bound can be improved in an elementary way using character sums [3]:

$$|N_{n+1}(0,b) - \frac{q^n - 1}{q-1}| \leq (d-1)q^{\frac{n-1}{2}},$$

where $d = \gcd(n+1, q-1)$.

In this note, we give a uniform improvement of Katz's bound in the case $a \neq 0$.

Theorem 1.2. *Let $a, b \in \mathbb{F}_q^*$ and $n \geq 1$. Then*

$$|N_{n+1}(a,b) - \frac{q^n - 1}{q-1}| \leq nq^{\frac{n-1}{2}}.$$

2000 *Mathematics Subject Classification.* 11T99, 14G10.

In the case that $n+1$ is a power of p, this improvement was first proved by Moisio [3] using Deligne's estimate for hyper-Kloosterman sums. Moreover, in the case $n+1=3$ also the bounds

$$3\left\lceil \frac{q+1-2\sqrt{q}}{3} \right\rceil \leq N_3(a,b) \leq 3\left\lfloor \frac{q+1+2\sqrt{q}}{3} \right\rfloor.$$

were obtained in [3] by using the Hasse's bound for elliptic curves together with a divisibility result. In corollary 2.4, we extend such divisibility bounds to $N_\ell(a,b)$, where $\ell \geq 3$ is any prime.

In the general case, our proof of Theorem 1.2 consists of two steps. The first step is to reduce it to estimating the number of $\mathbb{F}_q$-rational points on certain toric Calabi-Yau hypersurface over $\mathbb{F}_q$. The second step is to use the detailed cohomological calculations in Rojas-Leon and Wan [4] for such toric hypersurfaces. In the case $n+1=3$, the above improved bounds should significantly reduce the amount of calculations in [1].

2. Proof of Theorem 1.2

Let $u = b/a^{n+1} \in \mathbb{F}_q^*$. Let $N(u)$ denote the number of $\mathbb{F}_q$-rational points on the toric hypersurface

$$Y_u: \; X_1 + \cdots + X_n + \frac{u}{X_1 \cdots X_n} - 1 = 0.$$

Lemma 2.1.

$$N_{n+1}(a,b) = \frac{q^n-1}{q-1} + (-1)^n \left(N(u) - \frac{(q-1)^n - (-1)^n}{q} \right).$$

Proof. Write the equation of Y_u in the form

$$\begin{aligned} X_1 + \cdots + X_{n+1} &= 1 \\ X_1 \cdots X_{n+1} &= u. \end{aligned}$$

Let ψ be the canonical additive character of $\mathbb{F}_q$. Now

$$q(q-1)N(u) = \sum_{x_1,\ldots,x_{n+1}} \sum_{v} \psi(v(x_1 + \cdots + x_{n+1} - 1)) \sum_{\chi} \chi(u^{-1}x_1 \cdots x_{n+1}),$$

where $x_1,\ldots,x_{n+1}$ run over $\mathbb{F}_q^*$, v runs over $\mathbb{F}_q$, and χ runs over the multiplicative character group of $\mathbb{F}_q$.

Let $G(\chi)$ denote the Gauss sum

$$G(\chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x).$$

It follows that

$$\begin{aligned}
q(q-1)N(u) &= (q-1)^{n+1} + \sum_{v\neq 0}\psi(-v)\sum_{\chi}\bar{\chi}(u)\prod_{i=1}^{n+1}\sum_{x_i}\psi(vx_i)\chi(x_i) \\
&\overset{x_i\mapsto x_i/v}{=} (q-1)^{n+1} + \sum_{v\neq 0}\psi(-v)\sum_{\chi}\bar{\chi}(uv^{n+1})G(\chi)^{n+1} \\
&= (q-1)^{n+1} + \sum_{\chi}G(\chi)^{n+1}\bar{\chi}(u)\sum_{v\neq 0}\psi(-v)\bar{\chi}^{n+1}(v) \\
&= (q-1)^{n+1} + \sum_{\chi}G(\chi)^{n+1}G(\bar{\chi}^{n+1})\bar{\chi}((-1)^{n+1}u). \qquad (2.0.1)
\end{aligned}$$

Next we express $N_{n+1}(a,b)$ in terms of Gauss sums. We use the abbreviated notations Tr and Norm in place of $\mathrm{Tr}_{\mathbb{F}_{q^{n+1}}/\mathbb{F}_q}$ and $\mathrm{Norm}_{\mathbb{F}_{q^{n+1}}/\mathbb{F}_q}$. Let $\psi_{n+1} = \psi\circ\mathrm{Tr}$ be the canonical additive character of $\mathbb{F}_{q^{n+1}}$ and let $\alpha\in\mathbb{F}_{q^{n+1}}$ with $\mathrm{Tr}(\alpha)=1$. Now,

$$\begin{aligned}
q(q-1)N_{n+1}(a,b) &= \sum_{x\in\mathbb{F}^*_{q^{n+1}}}\sum_{v}\psi(v(\mathrm{Tr}(x-\alpha a)))\sum_{\chi}\chi(b^{-1}\mathrm{Norm}(x)) \\
&= \sum_{v}\psi(-av)\sum_{\chi}\bar{\chi}(b)\sum_{x}\psi_{n+1}(vx)\chi(\mathrm{Norm}(x)) \\
&= q^{n+1}-1+\sum_{v\neq 0}\psi(-av)\sum_{\chi}\bar{\chi}(b)\sum_{x}\psi_{n+1}(vx)\chi(\mathrm{Norm}(x)) \\
&\overset{x\mapsto x/v}{=} q^{n+1}-1+\sum_{v\neq 0}\psi(-av)\sum_{\chi}\bar{\chi}(bv^{n+1})\sum_{x}\psi_{n+1}(x)\chi(\mathrm{Norm}(x)),
\end{aligned}$$

since $\mathrm{Norm}(v)=v^{n+1}$.

By the Davenport-Hasse identity the inner sum

$$\sum_{x}\psi_{n+1}(x)\chi(\mathrm{Norm}(x)) = (-1)^n G(\chi)^{n+1},$$

and therefore

$$\begin{aligned}
q(q-1)N_{n+1}(a,b) &= q^{n+1}-1+(-1)^n\sum_{\chi}G(\chi)^{n+1}\bar{\chi}(b)\sum_{v\neq 0}\psi(-av)\bar{\chi}^{n+1}(v) \\
&= q^{n+1}-1+(-1)^n\sum_{\chi}G(\chi)^{n+1}G(\bar{\chi}^{n+1})\bar{\chi}((-1)^{n+1}b/a^{n+1}).
\end{aligned}$$

Comparing this expression with (2.0.1), one finds that

$$N_{n+1}(a,b) = \frac{q^{n+1}-1}{q(q-1)} + (-1)^n\left(N(u) - \frac{(q-1)^{n+1}}{q(q-1)}\right).$$

One checks that this is the same as the expression in Lemma 2.1. □

This lemma reduces Theorem 1.2 to the following

Theorem 2.2. *Let $u\in\mathbb{F}_q^*$. Then*

$$|N(u) - \frac{(q-1)^n-(-1)^n}{q}| \leq nq^{\frac{n-1}{2}}.$$

Proof. Over the algebraic closure $\bar{\mathbb{F}}_q$, we can write $u = \lambda^{-(n+1)}$ for some non-zero element λ. Then Y_u is isomorphic to the toric hypersurface

$$X_\lambda : \ X_1 + \cdots + X_n + \frac{1}{X_1 \cdots X_n} - \lambda = 0$$

whose zeta function over a finite field was studied in detail in [4], see [6] for more elementary description of the results. For a prime $\ell \neq p$, the ℓ-adic cohomology

$$H_c^j(Y_u \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell) \cong H_c^j(X_\lambda \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell)$$

was calculated in Theorem 2.1 in [4]. In particular, we have

$$H_c^j(Y_u \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell) = 0, \ j < n-1 \text{ or } j > 2n-1,$$

$$H_c^j(Y_u \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell^{\binom{n}{j-n+2}}(n-1-j), \ n \leq j \leq 2n-2,$$

and there is an exact sequence of Galois modules

$$0 \to \mathbb{Q}_\ell^n \to H_c^{n-1}(Y_u \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell) \to M_u \to 0,$$

where M_u is of rank at most n and mixed of weight at most $n-1$. It follows that

$$|\mathrm{Tr}(\mathrm{Frob}_u | M_u)| \leq n q^{\frac{n-1}{2}}.$$

By the ℓ-adic trace formula,

$$N(u) = \sum_{j=n}^{2n-2} (-1)^j \binom{n}{j-n+2} q^{(j-(n-1))} + (-1)^{n-1} n + (-1)^{n-1} \mathrm{Tr}(\mathrm{Frob}_u | M_u).$$

Replacing j by $j+n-2$, one finds

$$N(u) = \sum_{j=2}^{n} (-1)^{j-n} \binom{n}{j} q^{(j-1)} + (-1)^{n-1} n + (-1)^{n-1} \mathrm{Tr}(\mathrm{Frob}_u | M_u).$$

The theorem follows. □

Remark. If $u \neq (n+1)^{-(n+1)}$, i.e., $\lambda \notin \{(n+1)\zeta | \zeta^{n+1} = 1\}$, then M_u is pure of weight $n-1$ and of rank n. If $u = (n+1)^{-(n+1)}$ (necessarily $p \nmid n+1$), then the rank of M_u drops by 1 and thus

$$|\mathrm{Tr}(\mathrm{Frob}_u | M_u)| \leq (n-1) q^{\frac{n-1}{2}}.$$

If $u = (n+1)^{-(n+1)}$ and n is even, then one of the Frobenius eigenvalues has weight $n-2$ (instead of $n-1$), and thus

$$|\mathrm{Tr}(\mathrm{Frob}_u | M_u)| \leq (n-2) q^{\frac{n-1}{2}} + q^{\frac{n-2}{2}}.$$

All these follow from Proposition 2.6 in [4].

Corollary 2.3. *Let* $u = (n+1)^{-(n+1)}$. *Then*

$$|N(u) - \frac{(q-1)^n - (-1)^n}{q}| \leq (n-1) q^{\frac{n-1}{2}}.$$

If n is also even, then

$$|N(u) - \frac{(q-1)^n - (-1)^n}{q}| \leq (n-2) q^{\frac{n-1}{2}} + q^{\frac{n-2}{2}}.$$

Corollary 2.4. *Let $\ell \geq 3$ be a prime number. Let $a, b \in \mathbb{F}_q^*$. Then, we have*

$$\ell \left\lceil \frac{\frac{q^{\ell-1}-1}{q-1} - (\ell-1)q^{(\ell-2)/2}}{\ell} \right\rceil \leq N_\ell(a,b) \leq \ell \left\lfloor \frac{\frac{q^{\ell-1}-1}{q-1} + (\ell-1)q^{(\ell-2)/2}}{\ell} \right\rfloor .$$

Proof. Let R be the number of $c \in \mathbb{F}_q$ such that $\ell c = a$ and $c^\ell = b$. It is clear that R is either 0 or 1. Since ℓ is a prime, $N_\ell(a,b) - R$ is divisible by ℓ. If $R = 0$, the corollary is the consequence of Theorem 1.2 and the divisibility of $N_\ell(a,b)$ by ℓ.

Assume now that $R = 1$. Since $a \neq 0$, ℓ cannot be p. In this case, we have $a = \ell c$, $b = c^\ell$ and thus $u = b/a^\ell = \ell^{-\ell} \in \mathbb{F}_q^*$. We can apply the stronger estimate in the previous corollary to deduce the desired inequalities for $N_\ell(a,b)$.

References

[1] S. Huczynska and S.D. Cohen, Primitive free cubics with specified norm and trace, Trans. Amer. Math. Soc., 355(2003), 3099-3116.

[2] N. Katz, Estimates for Soto-Andrade sums, J. Reine Angew. Math., 438(1993), 143-161.

[3] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, Acta Arith., to appear.

[4] A. Rojas-Leon and D. Wan, Moment zeta functions for toric Calabi-Yau hypersurfaces, Communications in Number Theory and Physics, Vol. 1, No.3 (2007), 539-578.

[5] D. Wan, Generators and irreducible polynomials over finite fields, Math. Comp., 219(1997), 1195-1212.

[6] D. Wan, Lectures on zeta functions over finite fields, Proceedings of 2007 Göttingen summer school on higher dimensional geometry over finite fields, to appear. arXiv:0711.3651.

Department of Mathematics and Statistics, University of Vaasa, P.O. Box 700, FIN-65101, Vaasa, Finland

Email: mamo@uwasa.fi

Department of Mathematics, University of California, Irvine, Ca92697-3875

Email: dwan@math.uci.edu