

danger of confusion. We fix a character χ of order ℓ . Then we have

$$(5) \quad N_g = q + \sum_{1 \leq j, k \leq \ell-1} \chi^j(-g^{-2}) \chi^k(-g^{-1}) J(\chi^j, \chi^k)$$

where

$$J(\chi^j, \chi^k) = \sum_{a \in \mathbb{F}_q} \chi^j(a) \chi^k(1-a)$$

is a *Jacobi sum* with respect to χ^j and χ^k . The following properties of Jacobi sums are useful.

Lemma 2.2 ([LN97] Theorem 5.19, 5.21, 5.22). *Let λ, ψ be two extended characters of \mathbb{F}_q .*

- (i) $J(\lambda, \psi) = J(\psi, \lambda)$;
- (ii) $J(\varepsilon, \varepsilon) = q$;
- (iii) $J(\lambda, \varepsilon) = 0$ if $\lambda \neq \varepsilon$;
- (iv) $J(\lambda, \lambda^{-1}) = -\lambda(-1)$ if $\lambda \neq \varepsilon$;
- (v) $|J(\lambda, \psi)| = \sqrt{q}$ if λ, ψ and $\lambda\psi$ are all nontrivial.

Note that $|\chi^i(a)| = 1$ for all $a \in \mathbb{F}_q^\times$. By (iv) and (v) of Lemma 2.2 one has the following estimate of N_g from (5)

$$|N_g - q| \leq M_0 + M_1 \sqrt{q}$$

where M_0 (resp. M_1) is the number of pairs (j, k) with $\chi^j \chi^k = \varepsilon$ (resp. $\chi^j \chi^k \neq \varepsilon$). Observe that $M_0 = \ell - 1$ and $M_1 = (\ell - 1)(\ell - 2)$. Thus, if

$$(6) \quad q > (\ell - 1) + (\ell - 1)(\ell - 2)\sqrt{q},$$

then $N_g > 0$. Consequently, for q large enough (for example $q > (\ell - 1)^4$), one has $N_g > 0$ for any $g \in \mathbb{F}_q^\times$.

For the numbers of rational solutions to equations over finite fields, the Hasse-Weil bound [Wei48] provides more precise information than the crude estimate given above.

Theorem 1 (Hasse-Weil bound). *Let \mathcal{C} be a non-singular, absolutely irreducible projective curve over \mathbb{F}_q and let $N_{\mathcal{C}} = |\mathcal{C}(\mathbb{F}_q)|$ be the number of \mathbb{F}_q -rational points of \mathcal{C} . Then,*

$$|N_{\mathcal{C}} - (q + 1)| \leq 2g\sqrt{q}$$

where g is the genus of \mathcal{C} .

Applying the Hasse-Weil bound to $\widetilde{\mathcal{C}}_g$, we see that

$$|\widetilde{N}_g - (q + 1)| \leq (\ell - 1)(\ell - 2)\sqrt{q}$$

since the genus of $\widetilde{\mathcal{C}}_g$ is $g_\ell = (\ell - 1)(\ell - 2)/2$ by the degree-genus formula [Har77]. Consequently, $\widetilde{N}_g > 0$ for any generator g of \mathbb{F}_q^\times provided that $q + 1 > (\ell - 1)(\ell - 2)\sqrt{q}$ and therefore $\widetilde{\mathcal{C}}_g(\mathbb{F}_q)$ is non-empty if $q \geq (\ell - 1)^2(\ell - 2)^2$.