Let X be a smooth, projective and absolutely irreducible curve over a field $\mathbf{F}_q$ of q elements. In this note we estimate $\#X(\mathbf{F}_{q^2})$ following Stepanov and Bombieri. Let g denote the genus of X.

Theorem 1. *If $q > (g+1)^2$, then $\#X(\mathbf{F}_{q^2}) \leq q^2 + (2g+1)q$.*

We may assume that $X(\mathbf{F}_{q^2}) \neq \emptyset$ and choose a point $\infty \in X(\mathbf{F}_{q^2})$. For f in the function field $\mathbf{F}_{q^2}(X)$ we let $\deg f$ denote the order of the pole of f at ∞. For $a \in \mathbf{Z}$ we put

$$H_a = \{f \in \mathbf{F}_{q^2}(X) : f \text{ has no poles outside } \infty \text{ and satisfies } \deg f \leq a\}.$$

The spaces H_a are finite dimensional $\mathbf{F}_{q^2}$-subvector spaces of $\mathbf{F}_{q^2}(X)$. When $a > 2g-2$, the Riemann-Roch Theorem implies that they have dimension $a-g+1$. By H_a^q we denote the $\mathbf{F}_{q^2}$-vector space $\{f^q : f \in H_a\}$. The dimensions of the vector spaces H_a and H_a^q are equal. For $a, b \in \mathbf{Z}$ we denote by $H_a^q H_b$ the $\mathbf{F}_{q^2}$-vector space generated by the functions $f^q g$ where $f \in H_a$ and $g \in H_b$.

Lemma 2. *If $b < q$, then*

$$\dim\, H_a^q H_b \;=\; \dim H_a \cdot \dim\, H_b.$$

Proof. Let $e_1, \ldots, e_d$ be an $\mathbf{F}_{q^2}$-basis of H_a and let $f_1, \ldots, f_{d'}$ be an $\mathbf{F}_{q^2}$-basis of H_b. The lemma follows if we show that the products $e_i^q f_j$ form an $\mathbf{F}_{q^2}$-basis of $H_a^q H_b$.

It is clear that the functions $e_i^q f_j$ generate $H_a^q H_b$. Since we have

$$\deg e_i^q f_j \;=\; q \deg e_i + \deg f_j,$$

the inequality $\deg f_j \leq b < q$ implies that the orders of the poles of the functions $e_i^q f_j$ at infinity are all *different*. Therefore, for certain coefficients $\lambda_{ij} \in \mathbf{F}_{q^2}$ the $\mathbf{F}_{q^2}$-linear combination $\sum_{i,j} \lambda_{ij} e_i^q f_j$ is the zero function, then necessarily $\lambda_{ij} = 0$ for all i, j.

This proves the lemma.

From now on we assume $b < q$. Then Lemma 2 implies that the $\mathbf{F}_q$-linear map

$$\vartheta : H_a^q H_b \longrightarrow H_a H_b^q$$

given by

$$\lambda e_i^q f_j \;\mapsto\; \lambda^q e_i f_j^q, \qquad (\text{for } 1 \leq i \leq d,\ 1 \leq j \leq d' \text{ and } \lambda \in \mathbf{F}_{q^2})$$

is well defined. The key observation in the proof of Theorem 1 is the following.

Remark. *If $F \in \ker \vartheta$, then F is zero in all points of $X(\mathbf{F}_{q^2}) - \{\infty\}$.*

Proof. Let $P \neq \infty$ be in $X(\mathbf{F}_{q^2})$ and let $F = \sum \lambda_{ij} e_i^q f_j$ be in the kernel of ϑ. Then

$$F(P)^q = \sum \lambda_{ij}^q e_i(P)^{q^2} f_j(P)^q = \sum \lambda_{ij}^q e_i(P) f_j(P)^q = (\sum \lambda_{ij}^q e_i f_j^q)(P) = \vartheta(F)(P) = 0$$

and therefore $F(P) = 0$. Here the second equality follows from the fact that P is in $X(\mathbf{F}_{q^2})$, so that $f(P) = f(P)^{q^2}$ for every function $f \in \mathbf{F}_{q^2}(X)$.

If the function F in the "key" remark is not zero, then we obtain the estimate

$$\#X(\mathbf{F}_{q^2}) - 1 \;\leq\; \#\{\text{zeroes of } F\} \;=\; \#\{\text{poles of } F\} \;=\; \deg(F) \;\leq\; aq + b. \qquad (*)$$

The rightmost inequality follows from the fact that $H_a^q H_b$ is contained in H_{aq+b}. The existence of a non-zero function F is guaranteed when a, b have the property that

$$\dim H_a^q H_b \;>\; \dim H_a H_b^q.$$

Since $b < q$, Lemma 3 implies that the dimension of $H_a^q H_b$ is dim $H_a \cdot$ dim H_b. Under the assumption $a, b > 2g-2$ this is $(a-g+1)(b-g+1)$ by Riemann-Roch. Lemma 3 does not apply to $H_a H_b^q$. This is in some sense the point of the proof. But since $H_a H_b^q$ is contained in H_{a+bq}, the dimension of $H_a H_b^q$ is at most dim $H_{a+bq} = a + bq - g + 1$. So a non-zero function F exists when

$$(a - g + 1)(b - g + 1) \;>\; a + bq - g + 1.$$

Theorem 1 is now proved by suitably chosing a and b. In order to deduce a good estimate from the inequality $(*)$, we choose a as small as possible. If $a \leq q + g - 1$, the inequality $(a-g+1)(b-g+1) > a+bq-g+1$ clearly does not hold. We need to take a a little larger. A good choice is $a = q + 2g$. The choice of b is not so critical. We take $b = q - 1$. Since $q > (g+1)^2$, we have $a, b > 2g-2$ and $(a-g+1)(b-g+1) > a+bq-g+1$, so everything is fine. These choices of a, b lead to the estimate $\#X(\mathbf{F}_{q^2}) \leq 1 + aq + b = q^2 + (2g+1)q$ as required.