Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 149 NOVEMBER 2010 PART 3

Math. Proc. Camb. Phil. Soc. (2010), **149**, 385 © *Cambridge Philosophical Society* 2010
doi:10.1017/S0305004110000320
First published online 7 July 2010

Cubic surfaces over finite fields

BY SIR PETER SWINNERTON–DYER

*DPMMS, Centre for Mathematical Sciences, Wilberforce Rd, Cambridge, CB*3 0*WB.*
e-mail: H.P.F.Swinnerton-Dyer@dpmms.cam.ac.uk

(*Received* 24 *February* 2010; *revised* 13 *April* 2010)

Let V be a nonsingular cubic surface defined over the finite field $\mathbf{F}_q$. It is well known that the number of points on V satisfies $\#V(\mathbf{F}_q) = q^2 + nq + 1$ where $-2 \leqslant n \leqslant 7$ and that $n = 6$ is impossible; see for example [1], Table 1. Serre has asked if these bounds are best possible for each q. In this paper I shall show that this is so, with three exceptions:

THEOREM. *The bounds above are best possible, except that when* $q = 2, 3$ *or* 5 *the upper bound can be improved to* $n \leqslant 5$.

To prove this, we need to construct V which attain each of these bounds and to show that $n = 7$ is impossible if $q = 2, 3$ or 5. We start with the lower bound, for which we need two lemmas.

LEMMA 1. *Suppose that* W *is an absolutely irreducible cubic surface, defined over* $\mathbf{F}_q$ *and not a cone, and that* W *has either a singular point defined over* $\mathbf{F}_q$ *or two singular points whose union is defined over* $\mathbf{F}_q$. *(It may have other singular points as well.) Then* $\#W(F_q) \geqslant q^2 - q + 1$.

Proof. Suppose first that W has a singular point defined over $\mathbf{F}_q$; then we can take this point to be $(1, 0, 0, 0)$, so that W has the form

$$X_0 Q + C = 0 \quad \text{where } Q \text{ is quadratic and } C \text{ cubic in } X_1, X_2, X_3.$$

Since W is not a cone, Q does not vanish identically; so there are at least $q^2 - q$ essentially different triples X_1, X_2, X_3 in $\mathbf{F}_q$ at which Q does not vanish. Each of these gives a point of V, and we must also count the singular point.

A similar argument works in the other case. We can now take the line joining the two singularities to be $X_2 = X_3 = 0$, so that W has the form

$$X_0 X_1 L + X_0 Q_0 + X_1 Q_1 + C = 0$$

with L linear, Q_0, Q_1 quadratic and C cubic in X_2, X_3. Since W is not a cone, there are at least $q-1$ distinct pairs X_2, X_3 at which L, Q_0, Q_1 do not all vanish, and each of them gives at least $q-1$ points of W. There are also $q+1$ points on $X_2 = X_3 = 0$.

LEMMA 2. *Suppose that W is an absolutely irreducible cubic surface with at least three singularities. If they are collinear then $\#W(\mathbf{F}_q) \geqslant q^2 - q + 1$. Otherwise even over an algebraically closed extension K of $\mathbf{F}_q$ all but three of the lines on W pass through at least one of these singularities.*

Proof. Suppose first that these three singular points are collinear. Working over K we can take them to be $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and $(1, 1, 0, 0)$. Then W has the form

$$X_0Q_0 + X_1Q_1 + C = 0 \quad \text{with } Q_0,\ Q_1 \text{ quadratic and } C \text{ cubic in } X_2,\ X_3.$$

Thus every point of $X_2 = X_3 = 0$ is singular. If W had another singularity, then W would contain a plane because the join of any two singularities lies entirely in W. Hence the line containing the singularities was originally defined over $\mathbf{F}_q$; thus W contains a singularity defined over $\mathbf{F}_q$ and the result follows from Lemma 1.

Now suppose that there are three singularities which are not collinear. Working over K, we take the singular points to be $(1, 0, 0, 0)$, $(0, 1, 0, 0)$ and $(0, 0, 1, 0)$. Thus the equation of W is linear in each of X_0, X_1, X_2 separately, so that it has the form

$$X_0X_1X_2 + X_3Q = 0$$

where Q is quadratic in $X_0, \ldots, X_3$ and does not include any terms in X_0^2, X_1^2 or X_2^2. By adding multiples of X_3 to each of the other three variables, we can reduce this equation to the form

$$X_0X_1X_2 + X_3^2L + cX_3^3 = 0 \quad \text{where } L \text{ is linear in } X_0,\ X_1,\ X_2.$$

There are three obvious lines on $W \bigcap \{X_3 = 0\}$. Any other line can be parametrized by writing X_0, X_1, X_2 as linear forms in X_3 and a further variable Y. If we substitute this parametrization into the equation of W, the only possible multiples of Y^2 come from $X_0X_1X_2$; so on this line

either two of X_0, X_1, X_2 are simply multiples of X_3,
or one of X_0, X_1, X_2 vanishes.

In the latter case, the line must also lie on $L + cX_3 = 0$, so there are at most three lines of this kind.

We can now prove the existence of a surface V with $\#V(\mathbf{F}_q) = q^2 - 2q + 1$ as follows. Choose three planes Π_1, Π_2, Π_3 each defined over $\mathbf{F}_q$ and having only one point in common. Choose a point P_{12} on the intersection of Π_1 and Π_2 and defined over $\mathbf{F}_{q^3}$ but not over $\mathbf{F}_q$. Choose P_{13} similarly, but with the additional condition that the line $P_{12}P_{13}$ contains no point defined over $\mathbf{F}_q$. (This is possible, being easier to satisfy than the condition below on P_{23}.) Now choose P_{23} similarly, with neither $P_{12}P_{23}$ nor $P_{13}P_{23}$ containing a point defined over $\mathbf{F}_q$; this is possible because there are $q^3 - q$ candidates for P_{23} and for example only $q^2 - q$ of them for which $P_{12}P_{23}$ passes through a point defined over $\mathbf{F}_q$.

Now consider the pencil of cubic surfaces generated by the following two degenerate surfaces:

the union of the three Π_i,
the union of $P_{12}P_{13}P_{23}$ and its two conjugates over $\mathbf{F}_q$.

https://doi.org/10.1017/S0305004110000320 Published online by Cambridge University Press

Each of these is defined over $\mathbf{F}_q$; the first of them contains $3q^2 + 1$ points defined over $\mathbf{F}_q$ and the second contains at least one. The base of the pencil consists of the three lines like $P_{12}P_{13}$ and their six conjugates, so the pencil contains no other degenerate surface. Suppose first that it contains a surface with at least three singularities. If they are not collinear then at least six of the nine base lines must pass through one of these three singularities; and this can only happen if one of the singularities is a P_{ij} or one of its conjugates. But in this case its conjugates are also singularities, so (by Lemma 2 again) this surface contains at least $q^2 - q + 1$ points defined over $\mathbf{F}_q$.

Any other singular surface in the pencil must satisfy Lemma 1. Hence if the pencil does not contain a nonsingular surface V with $\#V(\mathbf{F}_q) = q^2 - 2q + 1$ then each of the $q - 1$ nondegenerate surfaces in the pencil must contain at least $q^2 - q + 1$ points defined over $\mathbf{F}_q$. But our nine base lines contain no such point, so each point defined over $\mathbf{F}_q$ in the ambient space lies on just one surface of the pencil. This contradicts

$$(3q^2 + 1) + 1 + (q - 1)(q^2 - q + 1) > q^3 + q^2 + q + 1;$$

thus the lower bound in the Theorem is best possible.

By [**1**], Table 1, constructing a V with $\#V(\mathbf{F}_q) = q^2 + 7q + 1$ is equivalent to constructing a V each of whose 27 lines is defined over $\mathbf{F}_q$. Since each line meets ten others, this requires each line to contain at least five points defined over $\mathbf{F}_q$ even if all these are Eckhardt points; so it is certainly impossible when $q = 2$ or 3. For $q > 3$ we consider a configuration consisting of two mutually skew lines Λ' and Λ'' and five mutually skew transversals to them, each of these seven lines being defined over $\mathbf{F}_q$. For this pupose we choose five points $P'_1, \ldots, P'_5$ of $\Lambda'(\mathbf{F}_q)$ and denote the points of $\Lambda''(\mathbf{F}_q)$ by $P''_0, \ldots, P''_q$; we now join each P'_i to a $P''_{\nu(i)}$ to form five transversals. Here the $\nu(i)$ are to be all different, so that the five transversals are mutually skew. This configuration of seven lines will define a pencil of cubic surfaces, for a cubic surface will contain them if it contains $P'_1, \ldots, P'_4, P''_{\nu(1)}, \ldots, P''_{\nu(4)}$ (and therefore necessarily P'_5 and $P''_{\nu(5)}$) and two other chosen points on each of the five transversals. We shall say that a configuration is *of the first kind* if there is a quadric which contains at least four of its five transversals (and therefore also Λ' and Λ'') and of the second kind otherwise. Note that a configuration of the first kind can only be associated with one quadric; for if it were associated with two they would have three transversals in common, and the intersection of two quadrics cannot contain three mutually skew lines. It can be checked by enumeration of cases that it is impossible for this configuration of lines to lie on a cubic surface which is singular but nondegenerate. If the pencil contains a degenerate surface W, then W must be the union of a plane and a nondegenerate quadric, and the configuration must be of the first kind. Now suppose that Λ', Λ'' and $P'_1, \ldots, P'_5$ have been chosen; then there are

$$(q + 1)q(q - 1)(q - 2)(q - 3)$$

possible configurations. There are $q^3 - q$ nondegenerate quadrics containing Λ' and Λ'' and defined over $\mathbf{F}_q$, and each of them is associated with $5q - 19$ configurations of the first kind. Since

$$(q + 1)q(q - 1)(q - 2)(q - 3) > (q^3 - q)(5q - 19)$$

except when $q = 5$, there exist configurations of the second kind except when $q = 5$. Now let V defined over $\mathbf{F}_q$ be a member of the pencil of cubic surfaces associated with a configuration of the second kind. We have just seen that V is nonsingular, and by forming

https://doi.org/10.1017/S0305004110000320 Published online by Cambridge University Press

the matrix of intersection numbers we can check that the seven lines of the configuration are linearly independent as divisors on V. Hence the Néron–Severi group of V has rank 7, and by [1], Table 1 we have $\#V(\mathbf{F}_q) = q^2 + 7q + 1$. We observe that a surface with $q = 4$ and $n = 7$ has 45 Eckhardt points, which is the maximum possible number.

To complete the proof of the Theorem it is now enough to exhibit for $q = 2, 3$ and 5 a surface V with $\#V(\mathbf{F}_q) = q^2 + 5q + 1$. We shall in fact construct such a V for every q. For this we use a configuration rather similar to that of the previous paragraph. This time we take Λ' and Λ'' to be two skew lines conjugate over $\mathbf{F}_q$ and each defined over $\mathbf{F}_{q^2}$. The transversals we use will be the join of a point P' in $\Lambda'(\mathbf{F}_{q^2})$ to its conjugate P'' in $\Lambda''(\mathbf{F}_{q^2})$; any such transversal $P'P''$ is defined over $\mathbf{F}_q$ and there are $q^2 + 1$ of them. A configuration will consist of Λ', Λ'' and five such transversals; and we define configurations of the first and second kinds as before. Once Λ' and Λ'' have been chosen, the total number of configurations is

$$(q^2 + 1)q^2(q^2 - 1)(q^2 - 2)(q^2 - 3)/120.$$

There are $q^3 + q$ nondegenerate quadrics containing Λ' and Λ'', and each of them is associated with

$$(q + 1)q(q - 1)(q - 2)(5q^2 - 5q + 1)/120$$

configurations of the first kind. Comparing these two counts, we find that there are always configurations of the second kind. Now let V defined over $\mathbf{F}_q$ be a member of the pencil of cubic surfaces associated with a configuration of the second kind. As in the previous paragraph, V is nonsingular, and this time the Néron-Severi group of V over $\mathbf{F}_q$ has rank 6. A final appeal to [**1**], Table 1 shows that V must belong to class 24 in the notation of that Table, and therefore $\#V(\mathbf{F}_q) = q^2 + 5q + 1$.

REFERENCE

[**1**] YU. I. MANIN. *Cubic Forms: Algebra, Geometry, Arithmetic* (Amsterdam, 1974).

https://doi.org/10.1017/S0305004110000320 Published online by Cambridge University Press