THE FINITE FIELD KAKEYA CONJECTURE

COSMIN POHOATA

ABSTRACT. In this paper we introduce the celebrated Kakeya Conjecture in the original real case setting and discuss the proof of its finite field analogue.

The story begins in 1917 when, with the hope of figuring out a mathematical formalization of the movement of a samurai during battle, Sochi Kakeya proposed the following problem:

What is the least area in the plane required to continuously rotate a needle of unit length and zero thickness around completely (i.e. by 360°)?

Clearly, the circle of radius \( \frac{1}{2} \) is a set where you can perform the rotation. Thus, this least area should be less than the area of this circle, i.e. less than \( \frac{\pi}{4} \). In the same paper, Kakeya noticed that the three-cornered hypocycloid inscribed in a circle of radius \( \frac{1}{4} \) also works. This is less trivial to justify, but we can see this, for example, by noticing that the tangent line at any point of the hypocycloid meets the hypocycloid at two points, which are at unit distance from each other. The area of the hypocycloid is \( 2\pi \left( \frac{1}{4} \right)^2 = \frac{\pi}{8} < \frac{\pi}{4} \), and for a while this was conjectured to be the least area that can be attained. Surprisingly, however, it turns out there exists sets with arbitrarily small area that satisfy Kakeya’s condition. This was proven by Besicovitch in 1928 in [3], where he also gave a first explicit construction of a so-called Kakeya set with (Lebesgue) measure zero. Alternative constructions can be found in [19].

It was subsequently conjectured that a Kakeya set \( K \subset \mathbb{R}^n \) (a compact set in \( \mathbb{R}^n \) containing a line segment in every direction - or more formally, a set so that for every \( x \in S^{n-1} \), there exists \( y = f(x) \in K \) such that \( \{y + tx \mid t \in [0,1]\} \subset K \)) has Hausdorff dimension \( n \). (We won’t get into facts about Hausdorff dimension here, but we refer to [13, pp. 323-380] and [16] for the definition, properties, and several computations). Note that if \( K' \subset \mathbb{R}^2 \) is a Kakeya set, then \( K := K' \times [0,1]^{n-2} \) is a Kakeya set in \( \mathbb{R}^n \), and moreover, if \( K' \) has measure zero, then \( K \) also has measure zero, so Kakeya sets, even when considered in \( \mathbb{R}^n \), can be of arbitrarily small measure, given Besicovitch’s result. Thus, it is natural to ask if there’s any difference between small Kakeya sets of different (Euclidean) dimensions. And indeed, such a difference is believed to exist. They can be of zero measure, but they have Hausdorff dimension equal to the Euclidean dimension of the space they lie in. We record this claim below once again for reference purposes.

**Conjecture 1 (Kakeya Conjecture).** If \( K \subset \mathbb{R}^n \) is a Kakeya set, then its Hausdorff dimension is \( n \).

For \( n = 1 \), this is trivially true. For \( n = 2 \), this was confirmed by Davies in [5], with a relatively short proof. The proof is also available in [13], which we mentioned above. For \( n \geq 3 \), however, the claim turns out significantly more difficult to approach, being still open today, after almost a century from its naissance in literature. In 1995, in [17], Thomas Wolff, using purely geometric methods, proved the first important partial result, showing that the Hausdorff dimension of a Kakeya set in \( \mathbb{R}^n \) must be at least \( \frac{1}{2}(n+2) \). For \( n = 3 \) and \( n = 4 \), this still almost represents the best known
result so far.\footnote{As a matter of fact, to be more precise, there were some more recent improvements by Tao of Wolff’s incidence geometry approach that managed to push the bound for $n = 4$ to $3 + \frac{1}{16}$, but there’s a lot of machinery involved for that extra $\frac{1}{16}$.} For larger $n$, the lower bound has been improved to $\frac{13}{25}n + \frac{12}{15}$ by Bourgain in 2000, using additive combinatorics ideas, and afterwards, in 2002, to $(2 - \sqrt{2})(n - 4) + 4$ by Katz and Tao, who refined Bourgain’s approach. We refer to [9] for the exposition of this line of thought.

Given the incredibly numerous connections the Kakeya Conjecture has with areas of mathematics such as number theory, combinatorics, analysis, and PDE’s, there have been numerous attempts to consider different analogous of the question instead, with the hope of getting some indirect information about this mysterious Hausdorff dimension that turns so difficult to establish for Kakeya sets. More popular surveys about such connections are the one by Wolff [19] and the one by Tao [14].

In this paper, we will focus only on one particular analogue which Wolff proposed in 1999 in [18]: the finite field version of the Kakeya problem. The setting is very simple and it is extremely convenient, since it avoids all the technical issues involving the Hausdorff dimension. We will be working over a finite field $F$ with $q$ elements. A Kakeya set in $F^n$ is a set $K \subset F^n$ containing a line in every direction, i.e. for all nonzero directions $v \in F^n$ there is an $a \in F^n$ such that $a + tv \in K$ for all $t \in F$. Will then such sets, no matter how small, always be $n$-dimensional? Or more precisely formulated, is there a positive constant $C_n$ (depending on $n$) so that if $K \subset F^n$ is a Kakeya set, then $|K| \geq C_n q^n$?\footnote{Here, one should think of $n$ as fixed and the field size, $q$, as going to infinity.}

Modulo minor technicalities, the progress on answering this question was, until very recently, essentially the same as that of the original Euclidean Kakeya conjecture, with all the lower bounds on the Hausdorff dimension carrying to the finite field case. Nevertheless, in 2009, the finite field analogue was finally settled by Zeev Dvir, using the so-called polynomial method from algebraic extremal combinatorics. The proof is surprisingly short and really beautiful, and so the plan is to cover it in full detail below.

**Conjecture 2** (Finite Field Kakeya Conjecture). Let $K \subset F^n$ be a Kakeya set. Then, $K$ has cardinality at least $C_n q^n$.

The proof is essentially after Dvir’s original paper [8] - with some minor technical simplifications that have appeared afterwards in literature (essentially due to Alon and Tao).

**Proof of Conjecture 2.** The idea is incredibly simple. First, one has to note that if $F$ is any field, and $K \subset F^n$ is any ”small” set, then there exists a polynomial $P \in F[X_1, \ldots, X_n] - \{0\}$, which has ”low” total degree, and vanishes on all of $K$. Afterwards, the only thing one has to do is to see that if $K$ is a Kakeya set, then this polynomial $P$, which vanishes on all of $K$, must be in fact the zero polynomial. Combining these two facts shows that a Kakeya set cannot be ”small”.

We isolate the two preliminary results that lie at the heart of the proof. The first one is a formalization of the first step mentioned above.

**Lemma 3.** Let $F$ be any field (not necessarily finite). If $S \subset F^n$ is a finite set, and $d$ is an integer such that $|S| < \binom{n+d}{n}$, then there exists a nonzero polynomial in $F[X_1, \ldots, X_n] - \{0\}$ which has degree at most $d$, and vanishes on all of $S$.

Note that the $n = 1$ case of this Lemma is simply that for any subset $S \subset F$, there is a polynomial in $F[X] - \{0\}$ of degree (at most) $|S|$, which vanishes on all of $S$, namely,

$$\prod_{s \in S} (X - s).$$
The lemma implies that if \( n \) is fixed, then for any \( S \subset \mathbb{F}^n \), there is a non-trivial polynomial of degree at most \( O(n(|S|^{\frac{1}{n}})) \) which vanishes on all of \( S \) or in algebraic geometry language, any set \( S \subset \mathbb{F}^n \) is contained in an algebraic variety which is the zero-set of a polynomial of degree \( O(|S|^{\frac{1}{n}})) \).

**Proof of Lemma 3.** Let \( V \) denote the \( \mathbb{F} \)-vector space of all polynomials in \( \mathbb{F}[X_1, \ldots, X_n] \) with degree at most \( d \), and note that \( V \) has a basis consisting of the set of all monomials in \( X_1, \ldots, X_n \) of degree at most \( d \). These monomials are in bijection with the set of \( n \)-tuples of exponents \((d_1, \ldots, d_n)\), where each \( d_i \) is a nonnegative integer and \( d_1 + \ldots + d_n \leq d \), and we know from elementary combinatorics that the number of these \( n \)-tuples is \( \binom{n+d}{n} \). Thus, it follows that \[ \dim V = \binom{n+d}{n}. \]

Now, consider the linear map \( T : V \to \mathbb{F}^{|S|} \) defined by
\[
T(P) = (P(s))_{s \in S}.
\]
By hypothesis, we have that \( \dim \mathbb{F}^{|S|} = |S| < \binom{n+d}{n} = \dim V \), hence, from linear algebra, we get that the kernel of \( T \) is non-trivial, i.e. there is some polynomial \( P \in V \setminus \{0\} \) which vanishes on all of \( S \), thus proving the claim. \( \square \)

The second result is the very popular Schwartz-Zippel Lemma from probabilistic polynomial identity testing.

**Lemma 4 (Schwartz-Zippel Lemma).** Let \( P \in \mathbb{F}[X_1, \ldots, X_n] \setminus \{0\} \) be a polynomial of degree \( d \). Let \( S \) be a finite subset of \( \mathbb{F} \) and let \( r_1, \ldots, r_n \) be selected randomly from \( S \). Then,
\[
\Pr[P(r_1, \ldots, r_n) = 0] \leq \frac{d}{|S|}.
\]

In the single variable case, this follows directly from the fact that a polynomial of degree \( d \) can have no more than \( d \) roots. It seems logical, then, to think that a similar statement would hold for multivariable polynomials (also given the existence of Lemma 3). This is, in fact, the case.

**Proof of Lemma 4.** The proof is by induction on \( n \). For \( n = 1 \), as was mentioned before, \( P \) can have at most \( d \) roots. This gives us the base case. Now, assume that the theorem holds for all polynomials in \( n-1 \) variables. We can consider then \( P \) to be a polynomial in \( x_1 \) and by writing it as
\[
P(x_1, \ldots, x_n) = \sum_{i=0}^{d} x_1^i P_i(x_2, \ldots, x_n).
\]
Since \( P \) is not identically 0, there is some \( i \) such that \( P_i \) is not identically 0. Take the largest such \( i \). Then, \( \deg P_i \leq d - i \), since the degree of \( x_1^i P_i \) is at most \( d \). Thus, we can use the inductive hypothesis for \( P_i \). Namely, we have that
\[
\Pr[P_i(r_2, \ldots, r_n) = 0] \leq \frac{d - i}{|S|},
\]
for any randomly selected \( r_2, \ldots, r_n \) in \( S \). If \( P_i(r_2, \ldots, r_n) \neq 0 \), then \( P(x_1, r_2, \ldots, r_n) \) is of degree \( i \) (as a polynomial in \( x_1 \), so
\[
\Pr[P(r_1, \ldots, r_n) \mid P_i(r_2, \ldots, r_n) \neq 0] \leq \frac{i}{|S|}.
\]
This motivates us to denote the event $P(r_1, \ldots, r_n) = 0$ by $A$, the event $P_t(r_2, \ldots, r_n) = 0$ by $B$, and the complements of $A$ and $B$ by $A^c$ and $B^c$, respectively; with these notations, it follows from above that

$$
\Pr[P(r_1, \ldots, r_n) = 0] \leq \Pr[A] = \Pr[A \cap B] + \Pr[A \cap B^c]
$$

$$
= \Pr[B] \Pr[A \mid B] + \Pr[B^c] \Pr[A \mid B^c]
$$

$$
\leq \Pr[B] + \Pr[A \mid B^c]
$$

$$
= \frac{d - i + i}{|S| + |S|}
$$

$$
= \frac{d}{|S|}.
$$

This completes the proof of the Schwartz-Zippel Lemma.

Note that if $F$ is finite and $S = F$, the above says that any non-trivial polynomial $P$ of degree $d$ from $F[X_1, \ldots, X_n]$ has at most $dq^{n-1}$ roots. This particular case will be sufficient for our purposes.

We are now ready to return to the proof of the finite field Kakeya conjecture. We will show that if $K \subset F^n$ is a Kakeya set, then $K$ has cardinality at least $\frac{1}{n!}q^n$. We do this by contradiction. Suppose that $|K| < \frac{1}{n!}q^n$. Then, note that we actually have that

$$
|K| < \frac{q^n}{n!} < \frac{q(q+1) \cdots (q+n-1)}{n!} = \binom{n+q-1}{n}.
$$

Thus, by Lemma 3, there exists some non-trivial polynomial $P$ in $\mathbb{F}[X_1, \ldots, X_n]$, which has degree $d$ satisfying $1 \leq d \leq q - 1$, and which vanishes on all of $K$. Write

$$
P = \sum_{i=0}^d P_i,
$$

where $P_i$ is the $i$th homogeneous component\(^3\) of $P$.

Let $v \in \mathbb{F}^n - \{0\}$ be an arbitrary direction. Since $K$ is a Kakeya set, there exists an $a \in \mathbb{F}^n$ such that $a + tv \in K$ for all $t \in K$. But $P$ vanishes on all $K$, so in particular we get that $P(a + tv) = 0$ for all $t \in \mathbb{F}$. This means that the univariate polynomial

$$
Q(T) := P(a + Tv) = P(a_1 + Tv_1, \ldots, a_n + Tv_n) \in \mathbb{F}[T],
$$

which has degree $d \leq q - 1$, vanishes on all of $\mathbb{F}$. Hence, it follows that $Q$ is the zero polynomial (by the Fundamental Theorem of Algebra or case $n = 1$ of Lemma 4). In particular, this means that the $T^d$-coefficient of $Q$, which is precisely $P_d(v)$, must be zero. Hence, we get that $P_d(v) = 0$ for all nonzero directions $v \in \mathbb{F}^n$. In addition, $d \geq 1$, and since $P_d$ is the $d$th homogeneous component of $P$, we have that $P_d(0) = 0$ too, so we can in fact say that $P_d$ vanishes on all of $\mathbb{F}^n$. However, we know that $P_d$ is of degree $d \leq q - 1$, therefore, by Lemma 4, it follows that $P_d$ is the zero polynomial (since otherwise, the Schwarz-Zippel Lemma tells us that $P_d$ has at most $dq^{n-1} < q^n = |\mathbb{F}^n|$ roots). This contradicts the initial assumption on $P$ (which was supposedly non-trivial and of degree $d$). Thus, the proof is complete.

\(^3\)The $i$th homogeneous component of a multivariate polynomial is simply the sum of all monomials of degree $i$. 

Mathematical Reflections 3 (2013)
Note that we have actually proven that every Kakeya set $K$ in $\mathbb{F}^n$ satisfies

$$|K| \geq \left( \frac{n + q - 1}{n} \right) = \frac{1}{n!} q^n + O(n^{q-1}),$$

which, for lower dimensions is quite tight. This is indeed true, and an example of Mockenhaupt and Tao shows that Kakeya sets of cardinality $\frac{\vert F \vert \times (\vert F \vert + 1)}{2} + \frac{1}{2} \vert F \vert + O(1)$ actually exist in $\mathbb{F}^2$. See [11]. For higher dimensions, this is not really the case. Nonetheless, the constant $\frac{1}{n!}$ has been subsequently improved to $\frac{1}{2n}$ by Dvir et al. in [6] after the publication of the original paper. More precisely, they showed that the following stronger claim holds.

**Theorem 5.** For all Kakeya sets $K \subset \mathbb{F}^n$, we have $|K| \geq \frac{1}{2n} q^n$.

In essence, their idea is similar to what we did above, the only difference being that the authors use a slightly more sophisticated polynomial argument with zeros of high multiplicities (thus, the two Lemmas are replaced by slightly more qualitative versions). We refer to [6] for details.

As Tao also writes in [15], it is really unfortunate that the polynomial method is extremely dependent on the algebraic nature of the finite field setting, and does not seem to extend directly to the Euclidean case. On the other hand, however, this result lends significant indirect support to the Euclidean Kakeya conjecture, since in particular, it morally rules out any algebraic counterexample to the Euclidean conjecture, as a highly algebraic example to this conjecture would likely be adaptable to the finite field setting. (The examples of zero measure Kakeya sets in the Euclidean plane have no finite field analogue, but they are non-algebraic in nature, and in particular take advantage of the multiple scales available in the Euclidean setting.)

We continue with a description of the smallest known Kakeya sets $K \subset \mathbb{F}^n$ - that are of size

$$|K| \leq \frac{q^n}{2^{n-1}} + O(q^{n-1}),$$

which is, asymptotically as $q$ tends to infinity, to within a factor of 2 of the lower bound from Theorem 5. The construction is due to Dvir [6] (for the case when $\mathbb{F}$ is of odd characteristic) and Saraf and Sudan [12] (for the case when $\mathbb{F}$ is of even characteristic), and comes as a generalization of the Mockenhaupt-Tao construction for the $n = 2$ case that we mentioned above.

**Odd characteristic.** Consider

$$K_n = \{ (\alpha_1, \ldots, \alpha_{n-1}, \beta) \in \mathbb{F}^n \mid \alpha_i, \beta \in \mathbb{F}, \alpha_i + \beta^2 \text{ is a square in } \mathbb{F} \text{ for all } i \},$$

and let $K = K_n \cup (\mathbb{F}^{n-1} \times \{0\})$ where $\mathbb{F}^{n-1} \times \{0\}$ denotes the set $\{ (a, 0) \mid a \in \mathbb{F}^{n-1} \}$. We claim that $K$ is a Kakeya set of the appropriate size.

Indeed, consider a direction $v = (v_1, \ldots, v_n)$. If $v_n = 0$, for $a = (0, \ldots, 0)$ we have that $a + tv \in \mathbb{F}^{n-1} \times \{0\} \subset K$. If $v_n \neq 0$, let

$$a = \left( \frac{v_1}{2v_n}, \ldots, \frac{v_{n-1}}{2v_n}, 0 \right).$$

The point $a + tv$ has coordinates $(\alpha_1, \ldots, \alpha_{n-1}, \beta)$ where $\alpha_i = \left( \frac{v_i}{2v_n} \right)^2 + tv_i$ and $\beta = tv_n$. We have that

$$\alpha_i + \beta^2 = \left( \frac{v_i}{2v_n} + tv_n \right)^2$$

which is a square for every $i$ and so $a + tv \in K_n \subset K$. This proves that $K$ is indeed a Kakeya set.
Finally, we verify that the size of $K$ is as claimed. First, note that the size of $K_n$ is exactly
\[ |K_n| = q \left( \frac{q + 1}{2} \right)^{n-1} = \frac{q^n}{2^{n-1}} + O(q^{n-1}) \]
(q choices for $\beta$ and $\frac{2^{n-1}}{2}$ choices for each $\alpha_i + \beta^2$). Hence, as claimed, the size of $K$ is at most
\[ |K| = |K_n| + q^{n-1} = \frac{q^n}{2^{n-1}} + O(q^{n-1}). \]

**Even characteristic.** Let
\[ K = \{ (\alpha_1, \ldots, \alpha_n, \beta) \in \mathbb{F}^n \mid \alpha_i, \beta \in \mathbb{F}, \exists \gamma_i \in \mathbb{F} \text{ such that } \alpha_i = \gamma_i^2 + \gamma_i \beta \}. \]
(Note that $K$ here contains from start the set $\mathbb{F}^{n-1} \times \{0\}$ that was ”added” in the above construction, since every element $\alpha$ of $\mathbb{F}$, when the characteristic is even, is a square in $\mathbb{F}$ - we refer again to [2] for this basic algebra fact).

Consider the direction $v = (v_1, \ldots, v_n)$. If $v_n = 0$, then take again $a = (0, \ldots, 0)$, and note that
\[ a + tv = (tv_1, \ldots, tv_{n-1}, 0) = (\gamma_1^2 + \beta \gamma_1, \ldots, \gamma_{n-1}^2 + \beta \gamma_{n-1}, \beta) \]
for $\beta = 0$ and $\gamma_i = \sqrt{tv_i} = (tv_i)^{\frac{q}{2}}$. We conclude that $a + tb \in K$ for every $t \in \mathbb{F}$ in this case.

If $v_n \neq 0$, let
\[ a = \left( \frac{v_1}{v_n}, \ldots, \frac{v_{n-1}}{v_n}, 0 \right). \]

The point $a + tv$ has coordinates $(\alpha_1, \ldots, \alpha_n, \beta)$ where $\alpha_i = \left( \frac{v_i}{v_n} \right)^2 + tv_i$ and $\beta = tv_n$. For $\gamma_i = \frac{v_i}{v_n}$, we get
\[ \gamma_i^2 + \gamma_i \beta = \left( \frac{v_i}{v_n} \right)^2 + tv_i = \alpha_i. \]

Hence, $a + tv \in K$, which proves that $K$ is a Kakeya set.

We have to verify again that the size of $K$ is as claimed. The number of points of the form $(\alpha_1, \ldots, \alpha_{n-1}, 0) \in K$ is exactly $q^{n-1}$. We now determine the number of $n$-tuples $(\alpha_1, \ldots, \alpha_{n-1}, \beta)$ in $K$ for fixed $\beta \neq 0$. We first claim that the set
\[ \{ \gamma^2 + \beta \gamma \mid \gamma \in \mathbb{F} \} \]
has size exactly $\frac{q}{2}$. This is so since for every $\gamma \in \mathbb{F}$, we have
\[ \gamma^2 + \beta \gamma = \tau^2 + \beta \tau^2 \text{ for } \tau = \gamma + \beta \neq \gamma, \]
and so the map $\gamma \rightarrow \gamma^2 + \beta \gamma$ is a 2-to-1 map on its image. Thus, for $\beta \neq 0$, the number of points of the form $(\alpha_1, \ldots, \alpha_{n-1}, \beta)$ in $K$ is exactly $\left( \frac{q}{2} \right)^{n-1}$. We conclude that $K$ has cardinality
\[ |K| = (q - 1) \left( \frac{q}{2} \right)^{q-1} + q^{n-1} = \frac{q^n}{2^{n-1}} + O(q^{n-1}). \]

We end this story with a short remark about the way we finished the proof of Conjecture 2. Note that there are other ways in which we could have concluded that $P_d$ is the zero polynomial. For instance, we could have used the following alternative Lemma usually attributed to Alon and Tarsi (also present as Corollary 1.6 in [10, pp. 176]).

\[ \text{This is where we are using the fact that we are working in odd characteristic. Recall from elementary algebra that in any field of odd order, exactly half of the elements are squares. For sake of completeness, we refer to [2, Exercise M4, pp. 476] for a proof.} \]

*Mathematical Reflections* 3 (2013) 6
Lemma 6. Let $F$ be a field, and let $P \in F[X_1, \ldots, X_n]$ be a non-trivial polynomial. Suppose $S_1, \ldots, S_n$ are all subsets of $F$ which satisfy $|S_i| > \deg_{X_i}(P)$, where the latter denotes the highest power of $X_i$ occurring in any monomial from $P$. Then, $P$ cannot vanish on all of $S_1 \times \ldots \times S_k$.

As a matter of fact, it is precisely this Lemma 6 that represented the foundation of the so-called polynomial method from algebraic extremal combinatorics. It turns out that the conclusion of the Alon-Tarsi Lemma holds under a weaker hypothesis.

Lemma 6’ (Combinatorial Nullstellensatz). Let $F$ be a field, let $S_1, \ldots, S_n \subset F$, and let $P \in F[X_1, \ldots, X_n]$ be a polynomial. Suppose there exist integers $t_1, \ldots, t_n \geq 0$ such that the coefficient of $X_{t_1}^1 \ldots X_{t_n}^n$ in $P$ is non-zero, $P$ has degree $\sum_{i=1}^n t_i$, and $|S_i| > t_i$ for each $i \in \{1, \ldots, n\}$. Then, $P$ cannot vanish on all of $S_1 \times \ldots \times S_n$.

This is the content of Alon’s Combinatorial Nullstellensatz, which has been introduced by Noga Alon in literature in 1999 in [1], and became more or less the center piece of the method, a decade prior to Dvir’s proof of the finite field Kakeya conjecture, when Alon proved a series of important results from extremal combinatorics using this simple result. Nonetheless, Dvir was the first to use the Nullstellensatz (read: the Schwartz-Zippel Lemma) to prove a result that essentially deals with incidence/algebraic geometry, and his surprising idea led immediately to solutions to other important open questions of similar flavor. One such example is the famous Joints Conjecture, which Guth and Katz settled in 2010 with virtually the same proof (modulo some additional technicalities).

Conjecture 3 (Joints Conjecture). Let $L$ be a set of lines in $\mathbb{R}^3$. We define a joint with respect to the arrangement $L$ to be a point $p \in \mathbb{R}^3$ through which pass at least three, non coplanar, lines. Then, the number of joints determined by $L$ is at most $C|L|^\frac{3}{2}$, for some positive constant $C$.

We refer to [7] for a beautiful survey of similar applications of the polynomial method to incidence geometry flavored results.

References


5The proof is very similar to that of the Schwartz-Zippel Lemma. Instead of doing induction on $n$, the idea now is to do induction on the sum $t_1 + \ldots + t_n$. Then, one just has to choose some $a \in S_1$ and write $P$ as $P = (X_1 - a)Q + R$, where $Q \in F[X_1, \ldots, X_n]$ and $R \in F[X_2, \ldots, X_n]$, and note that we can apply the inductive hypothesis to $Q$. We refer to [1] for more details.


E-mail address: apohoata@princeton.edu