Sharp Effective Finite-Field Nullstellensatz

Guy Moshkovitz and Jeffery Yu

Abstract. The (weak) Nullstellensatz over finite fields says that if $P_1, \ldots, P_m$ are $n$-variate degree-$d$ polynomials with no common zero over a finite field $\mathbb{F}$ then there are polynomials $R_1, \ldots, R_m$ such that $R_1P_1 + \cdots + R_mP_m \equiv 1$. Green and Tao [14, Proposition 9.1] used a regularity lemma to obtain an effective proof, showing that the degrees of the polynomials $R_i$ can be bounded independently of $n$, though with an Ackermann-type dependence on the other parameters $m, d,$ and $|\mathbb{F}|$. In this paper we use the polynomial method to give a proof with a degree bound of $md(|\mathbb{F}| - 1)$. We also show that the dependence on each of the parameters is the best possible up to an absolute constant. We further include a generalization, offered by Pete L. Clark, from finite fields to arbitrary subsets in arbitrary fields, provided the polynomials $P_i$ take finitely many values on said subset.

Hilbert’s Nullstellensatz is a linchpin of algebraic geometry, providing a bridge between algebra (ideals in polynomial rings) and geometry (solution sets of polynomial equations) when the underlying field is algebraically closed. Kollár [18] famously obtained an effective proof of Hilbert’s Nullstellensatz with a sharp bound on the degrees of the polynomials involved. When the underlying field is finite, Green and Tao [14] proved an effective analogue of Hilbert’s Nullstellensatz, but the bound furnished by their proof is extremely poor. In this paper we obtain new, much better bounds for the finite-field analogue of Hilbert’s Nullstellensatz.

1. UPPER BOUND. Two polynomials $P, Q \in \mathbb{F}[x] := \mathbb{F}[x_1, \ldots, x_n]$ over a finite field $\mathbb{F}$ are functionally equal, denoted $P \equiv Q$, if $P(x) = Q(x)$ for every $x \in \mathbb{F}^n$; put differently, $P \equiv Q$ if and only if $P = Q + C$ for some polynomial $C \in \mathbb{F}[x]$ in the ideal $\langle x_1^{[\mathbb{F}]} - x_1, \ldots, x_n^{[\mathbb{F}]} - x_n \rangle$. We denote by $\mathbb{F}_{\leq d}[x] = \{P \in \mathbb{F}[x] \mid \deg P \leq d\}$ the set of polynomials over a field $\mathbb{F}$ of (total) degree at most $d$, and we denote by $Z(\mathbb{F}, P_1, \ldots, P_m) = \{x \in \mathbb{F}^n \mid P_1(x) = \cdots = P_m(x) = 0\}$ the set of zeros over $\mathbb{F}$ (not over the algebraic closure!) of the polynomials $P_1, \ldots, P_m \in \mathbb{F}[x]$.

Over an algebraically closed field $\mathbb{K}$, Hilbert’s Nullstellensatz [17] says that if polynomials $P_1, \ldots, P_m, Q \in \mathbb{K}_{\leq d}[x]$ satisfy $Z(\mathbb{K}, P_1, \ldots, P_m) \subseteq Z(\mathbb{K}, Q)$, then there exist polynomials $R_1, \ldots, R_m \in \mathbb{K}_{\leq D}[x]$ such that $Q^{D'} = \sum_{i=1}^m R_iP_i$ for some finite $D, D' \in \mathbb{N}$. A result of Hermann [16] gives an effective proof of Hilbert’s Nullstellensatz with a double-exponential bound on $D, D'$. This bound was greatly improved by Brownawell [6], and an influential work of Kollár [18] finally achieved a sharp bound, showing that $D, D'$ can be bounded by roughly $d^m$, and in particular, be bounded independently of $n$.

Over a finite field $\mathbb{F}$, for an analogue of Hilbert’s Nullstellensatz to hold, one has to replace polynomial equality with functional equality. It is easy to see that $Z(\mathbb{F}, P_1, \ldots, P_m) \subseteq Z(\mathbb{F}, Q)$ implies the existence of functions $R_i : \mathbb{F}^n \to \mathbb{F}$ satisfying $Q \equiv \sum_{i=1}^m R_iP_i$ (no need for a radical). Since every function over a finite field can be written as a polynomial, this trivially implies the degree bound $\deg(R_i) \leq n(|\mathbb{F}| - 1)$ (recall $x_i^{[\mathbb{F}]} \equiv x_i$, so the degree of each variable can be assumed to be at most $|\mathbb{F}| - 1$).

\footnotesize
\begin{itemize}
  \item doi.org/10.1080/00029890.2023.2230810
  \item MSC: 11T06, 03F20
  \item In terms of ideals, $I(Z(\mathbb{F}, P_1, \ldots, P_m)) = \sqrt{\langle P_1, \ldots, P_m \rangle}$.
\end{itemize}

© THE MATHEMATICAL ASSOCIATION OF AMERICA [Monthly 130]
Green and Tao, in a seminal work on the relation between structure and randomness of polynomials, devised a certain regularity lemma for polynomials over finite fields and applied it to obtain (among other applications) an effective version of the Nullstellensatz over finite fields [14, Proposition 9.1]. Specifically, they showed that if \( \mathbb{F} \) is a prime finite field and \( P_1, \ldots, P_m, Q \in \mathbb{F}_{\leq d}[x] \) are polynomials of degree at most \( d < |\mathbb{F}| \) satisfying \( \mathbb{F}(P_1, \ldots, P_m) \subseteq \mathbb{F}(Q) \), then \( Q = \sum_{i=1}^m R_i P_i \) holds for some polynomials \( R_1, \ldots, R_m \in \mathbb{F}_{\leq D}[x] \) of degree at most some \( D = D(m, d, |\mathbb{F}|) \) that does not depend on \( n \). Unfortunately, the dependence of \( D \) on the other parameters, \( m, d, \) and \( |\mathbb{F}| \), is atrocious, being some Ackermann-type function.\(^2\)

We use the polynomial method to give a sharp effective proof of the finite-field Nullstellensatz (which is also short and elementary).

**Theorem 1 (Sharp finite-field Nullstellensatz).** Let \( \mathbb{F} \) be a finite field. If polynomials \( P_1, \ldots, P_m, Q \in \mathbb{F}_{\leq d}[x] \) satisfy \( \mathbb{F}(P_1, \ldots, P_m) \subseteq \mathbb{F}(Q) \), then \( Q = \sum_{i=1}^m R_i P_i \) for some polynomials \( R_1, \ldots, R_m \in \mathbb{F}_{\leq D}[x] \) with \( D = md(|\mathbb{F}| − 1) \).

We note that an immediate corollary is a finite-field analogue of the weak Nullstellensatz, obtained by taking \( Q = 1 \) so that the assumption is \( \mathbb{F}(P_1, \ldots, P_m) = 0 \).\(^3\) We also note that the proof of Theorem 1 has a generalization to arbitrary fields; see Section 3.

Theorem 1 is proved roughly as follows. Over a finite field \( \mathbb{F} \), the indicator function for nonmembership in the zero set \( \mathbb{F}(P_1, \ldots, P_m) \) can be written as a polynomial \( I \) in the ring \( \mathbb{F}(P_1, \ldots, P_m) \) of degree at most \( m(|\mathbb{F}| − 1) \), which moreover has a zero constant term. The Nullstellensatz assumption implies that \( Q = QI \), and so we can write \( Q \) as a combination of \( P_1, \ldots, P_m \). Since the coefficients of this combination are polynomials in \( \mathbb{F}(P_1, \ldots, P_m, Q) \), the desired degree bound follows. The underlying idea is similar to some other applications of the polynomial method. Broadly speaking, the polynomial method analyzes an object of interest by studying the algebraic properties of a polynomial associated with it. In our case, the object of interest is a zero set over a finite field, which we analyze via a polynomial vanishing on it; this particular idea can be traced back at least to Chevalley [7] (see also Ax’s proof of the Chevalley-Warning Theorem [2]). A more recent relevant example of the polynomial method is the solution of the cap-set problem by Ellenberg-Gijswijt [11] following Croot-Lev-Pach [10]. The main idea in our proof is that nonmembership in the zero set of \( m \) polynomials over a finite field can itself be expressed as a polynomial which lies in the ideal generated by the \( m \) polynomials. The crucial point is that the number of inputs to the nonmembership function is the number \( m \) of polynomials rather than the number \( n \) of variables of these polynomials.

**Proof.** Put \( q = |\mathbb{F}|, \) and recall that for every \( x \in \mathbb{F} \) we have \( x^{q−1} \equiv [x \neq 0] \).\(^4\) Let \( I: \mathbb{F}^n \to \{0, 1\} \) be the indicator function \( I(x) = [x \notin \mathbb{F}(P_1, \ldots, P_m)] \). We claim that \( I = \sum_i I_i P_i \), where each \( I_i \in \mathbb{F}[x] \) is explicitly given by

\[
I_i = P_i^{q−2} \prod_{j=i+1}^m (1 - P_j^{q−1}).
\]

\(^2\)See, e.g., the remark following Lemma 2.4 in [14] for a discussion on the Ackermann-type dependence.

\(^3\)For \( Q = 1 \) the proof gives the slightly better bound \( md(|\mathbb{F}| − 1) − d \); see (1).

\(^4\)The Iverson bracket \([P]\) is 1 if the predicate \( P \) is true, and 0 otherwise.
Indeed,
\[ \sum_{i=1}^{m} I_i P_i = \sum_{i=1}^{m} P_i^{q-1} \prod_{j=i+1}^{m} (1 - P_j^{q-1}) = \sum_{i=1}^{m} \sum_{J \subseteq [m] : \min J = i} - \prod_{j \in J} (-P_j^{q-1}) \]
\[= - \sum_{J \subseteq [m] : \min J = i} \prod_{j \in J} (-P_j^{q-1}) = - \left( \prod_{j=1}^{m} (1 - P_j^{q-1}) - 1 \right) \equiv 1. \]

Using the statement’s assumption \( Z_F(P_1, \ldots, P_m) \subseteq Z_F(Q) \) we deduce that
\[ Q \equiv QI \equiv \sum_{i=1}^{m} (QI_i) P_i. \]

Each \( R_i := QI_i \) can be viewed, by (1), as a polynomial in the ring \( \mathbb{F}[P_1, \ldots, P_m, Q] \), which is thus of degree at most \((m+1)(q-1)\); in fact, the explicit definition in (1) implies the slightly better bound \( m(q-1) \). It follows that \( R_i \), viewed as a polynomial in \( \mathbb{F}[x] \), is of degree at most \( md(q-1) = D \), thus completing the proof. \( \blacksquare \)

2. LOWER BOUNDS. We next show that a dependence in Theorem 1 of the degree bound \( D \) on each of the parameters \(|\mathbb{F}|, d, m \) is inevitable, even for the weak form of the finite-field Nullstellensatz.

For the dependence of \( D \) on the field size \(|\mathbb{F}|\), let us consider the polynomial \( P = x^2 + 1 \in \mathbb{F}[x] \) where \( \mathbb{F} = \mathbb{F}_q \) is any prime finite field with the prime number \( q \) congruent to 3 modulo 4. Then \( Z_F(P) = \emptyset \) by Euler’s criterion [12, 13], and so trivially \( Z_F(P) \subseteq Z_F(1) \). However, if \( 1 \equiv RP \) for some \( R \in \mathbb{F}[x] \) then, as we show next, \( \deg(R) \geq q - 1 \). First, note that \( R \equiv P^{q-2} \) since \( R(x) = 1/P(x) \) for every \( x \in \mathbb{F} \). Next, note that for every \( i \neq 0 \) \( \pmod q \), we have over \( \mathbb{F} \) the functional equality of polynomials \( x^i \equiv x^i \pmod{q-1} \); indeed, for all integers \( d, i \geq 1 \),
\[ x^{d(q-1)+i} = x^{q+(d-1)(q-1)+i-1} \equiv x \cdot x^{(d-1)(q-1)+i-1} = x^{(d-1)(q-1)+i}, \]
as none of the exponents is negative. Denote \( t = q - 2 \) and \( b = \frac{1}{2}(q-1) \in \mathbb{N} \), so
\[ R \equiv (x^2 + 1)^t = \sum_{i=0}^{t} \binom{t}{i} x^{2i} \equiv \binom{t}{b} x^{2b} + \sum_{j=1}^{b-1} \left( \binom{t}{j} + \binom{t}{j+b} \right) x^{2j+1} \]
as \( x^{2j} \equiv x^{2(j+b)} \) for \( j \neq 0 \pmod b \). Note that the coefficient \( \binom{t}{b} \) is \( \left( \frac{q-2}{2} \right) \neq 0 \pmod{q} \), as \( q \) is prime and so does not divide the numerator of the binomial coefficient. Since every exponent of \( x \) in the right hand side of the identity above is at most \( 2b = q - 1 \), and since the coefficient of \( x^{q-1} \) is nonzero in \( \mathbb{F} \), we deduce that \( \deg(R) \geq q - 1 = |\mathbb{F}| - 1 \), as claimed.

Note, however, that since the example above assumes that \( \mathbb{F} \) is a prime finite field, it could be that \( D \) depends on just the characteristic of \( \mathbb{F} \) rather than its size \(|\mathbb{F}|\). Nevertheless, with a little effort one can extend the example to non-prime fields: simply let \( \mathbb{F} = \mathbb{F}_q \) with \( q = p^k \), where \( k \geq 1 \) is any odd integer and \( p \) is a prime congruent to 3 modulo 4, and take \( P = x^2 + 1 \in \mathbb{F}[x] \) as before. Then \( Z_F(P) = \emptyset \) again; indeed, if \( \sqrt{-1} \in \mathbb{F}_q \) then, since \( \sqrt{-1} \notin \mathbb{F}_p \), the field extension \( \mathbb{L}/\mathbb{F}_p \) with \( \mathbb{L} = \mathbb{F}_p(\sqrt{-1}) \) has degree \( [\mathbb{L} : \mathbb{F}_p] = 2 \), which is impossible as \( k = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{F}_p] \) is odd. Since we still have the identity \( x^q \equiv x \), the only part of the argument above that remains to be checked is that the leading coefficient is nonzero in \( \mathbb{F} \), that is,
Here we use a corollary of another classical result, Lucas’s theorem [20] (though it would suffice to use the earlier Kummer’s theorem [19], which itself follows from Legendre’s formula): for every prime $p$ and binomial coefficient $\binom{n}{m}$, we have $\binom{n}{m} \not\equiv 0 \pmod{p}$ if and only if $m_i \leq n_i$ for every $i$, where $n = \sum_{i \geq 0} n_i \cdot p^i$ and $m = \sum_{i \geq 0} m_i \cdot p^i$ are the expansions in base $p$ of $n$ and $m$, respectively. For our binomial coefficient $\binom{q^2-2}{\frac{1}{2}(q^2-1)}$ we have the following expansions in base $p$, where we recall that $q = p^k$:

$$p^k - 2 = \sum_{i=1}^{k-1} (p-1)p^i + (p-2)p^0 \quad \text{and} \quad \frac{1}{2}(p^k - 1) = \sum_{i=0}^{k-1} \left(\frac{1}{2}(p-1)\right)p^i.$$ 

Since $\frac{1}{2}(p-1) \leq p-2$ for every $p \geq 3$, it follows from the above that $\binom{q^2-2}{\frac{1}{2}(q^2-1)} \not\equiv 0 \pmod{p}$, as needed.

For the dependence of $D$ on the degree bound $d$, consider instead the polynomial $P = H^2 + 1$ where $H \in \mathbb{F}[x_1, \ldots, x_n]$ is any polynomial with individual degrees $\deg_x(H) = 1$ (e.g., the elementary symmetric polynomial $H(x) = \sum_{i \in [n]} \prod_{j \in [i]} x_j$ of any degree $1 \leq k \leq n$). As before, $\emptyset = \mathbb{F}^\emptyset(1) \subseteq \mathbb{F}^1(1)$; and if $1 \equiv R \neg P$ then, as is not hard to check, the argument above implies that $\deg(R) \geq \deg(H)(|\mathbb{F}| - 1) = \frac{1}{2} \deg(P)(|\mathbb{F}| - 1)$.

Finally, the dependence of $D$ on the number $m$ of polynomials follows from results in theoretical computer science. The Nullstellensatz over finite fields is also studied in the area of proof complexity [3], where an identity of the form

$$1 = \sum_{i=1}^{m} R_i P_i + \sum_{i=1}^{n} C_i (x_i^2 - x_i) \quad \text{(2)}$$

for $n$-variate polynomials $R_1, \ldots, R_m, C_1, \ldots, C_n \in \mathbb{F}[x_1, \ldots, x_n]$ over any finite field $\mathbb{F}$ is known as a Nullstellensatz refutation for $P_1, \ldots, P_m$ (as it refutes the satisfiability of the polynomial equations $P_1(x) = \cdots = P_m(x) = 0$ with $x \in \{0, 1\}^n$). In that context, the number $m$ of polynomials $P_i$ typically grows with the number of variables $n$, and $m$-tuples of polynomials $(P_1, \ldots, P_m)$ for which $\max_i \deg(R_i) = \Omega(n)$ are known to exist, over every finite field [1,4,5,15]. In the setting of Theorem 1, however, the crucial point is that the number of polynomials $m$ is a given parameter while the number $n$ of variables may go to infinity. Nevertheless, as we next explain, the proof complexity lower bounds easily give polynomials in an arbitrarily large number $N$ of variables, yielding a lower bound for Theorem 1 of $D \geq \Omega(m)$. Indeed, the aforementioned lower bounds say that for any $\mathbb{F}$, any $m$, and some $n = \Theta(m)$, there are polynomials $P_1, \ldots, P_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that the identity (2) implies $\deg(R_i) = \Omega(m)$ for every $1 \leq i \leq m$ (or more conventionally, $P_i$ exist for any $n$ and some $m = \Theta(n)$, and $\deg(R_i) = \Omega(n)$). Now, for any $\mathbb{F}$, any $m$, and any $N \geq n$, let $P_1, \ldots, P_m$ be the polynomials from before but viewed as elements of the larger polynomial ring $\mathbb{F}[x_1, \ldots, x_n, x_{n+1}, \ldots, x_N]$. If $1 \equiv \sum_{i=1}^{m} R'_i P_i$, meaning

$$1 = \sum_{i=1}^{m} R'_i P_i + \sum_{i=1}^{N} C'_i (x_i^{[\mathbb{F}]} - x_i)$$

for some polynomials $R'_1, \ldots, R'_m, C'_1, \ldots, C'_N \in \mathbb{F}[x_1, \ldots, x_N]$, then by setting $x_i = 0$ for every $n + 1 \leq i \leq N$ and factoring $x_i^{[\mathbb{F}]} - x_i = S(x_i)(x_i^2 - x_i)$ with $S(x) :=$
Let $F$ be any field, $X \subseteq \mathbb{F}^n$ any set, and $P_1, \ldots, P_m, Q \in \mathbb{F}_{\leq d}[x]$ $n$-variate polynomials satisfying $|P_i(X)| \leq F$ for every $1 \leq i \leq m$. If $Z(P_1, \ldots, P_m) \cap X \subseteq Z(Q)$ then $Q \equiv_X \sum_{i=1}^{m} R_i P_i$ for some $R_1, \ldots, R_m \in \mathbb{F}_{\leq d}[x]$ with

$$D = md \cdot \begin{cases} F - 1 & m \geq 2 \\ F & m = 1 \end{cases}.$$ 

Theorem 2 in particular implies a qualitative statement proved in a paper of Clark ([8, Theorem 7], “Finitesatz”): For any field $F$, if $X \subseteq \mathbb{F}^n$ is finite then $I(Z(P_1, \ldots, P_m) \cap X) = \langle P_1, \ldots, P_m \rangle + I(X)$ (without a radical, unlike Hilbert’s Nullstellensatz). In fact, Theorem 2 implies the same conclusion for infinite $X$, as long as the images $P_i(X)$ are finite; this qualitative statement already appears to be new.

**Proof.** First, suppose $Z(P_i) \cap X = \emptyset$ for some $1 \leq i \leq m$. By interpolation, there is a univariate polynomial $I_i \in \mathbb{F}[x]$ with $\deg(I_i) \leq |P_i(X)| - 1$ satisfying $I_i(x) = 1/x$ for every $x \in P_i(X)$ (which is well defined as $0 \notin P_i(X)$). Then the polynomial $R_i := Q \cdot (I_i \circ P_i) \in \mathbb{F}[x]$ satisfies $Q \equiv_X R_i P_i$ as needed; indeed, this is because $R_i P_i(x) = Q(x) \cdot I_i(P_i(x)) \cdot P_i(x) = Q(x)$ for every $x \in X$. We have

$$\deg(R_i) \leq \deg(Q) + \deg(P_i)(F - 1).$$  

(3)

Thus $\deg(R_i) \leq d + d(F - 1) = dF$. Note that $dF \leq D$; indeed, for $m \geq 2$ we have $dF \leq 2d(F - 1)$ if $F \geq 2$, whereas if $F \leq 1$ then the statement is clearly true as $\deg(R_i) = 0$ suffices. This completes the proof in this case.

Henceforth, assume $Z(P_i) \cap X \neq \emptyset$ for every $1 \leq i \leq m$. For a set $Y \subseteq \mathbb{F}$, let $C_Y \in \mathbb{F}[x]$ be the univariate polynomial

$$C_Y(x) = 1 - \frac{\prod_{y \in Y \setminus \{0\}} (y - x)}{\prod_{y \in Y \setminus \{0\}} y}.$$ 

Note that $C_Y(x) = [x \neq 0]$ for every $x \in Y$, and $\deg(C_Y) \leq |Y \setminus \{0\}|$. Let $\hat{P}_j := C_{P_j(x)} \circ P_j \in \mathbb{F}[x]$, and note that

$$\forall x \in X : \hat{P}_j(x) = [P_j(x) \neq 0] \quad \text{and} \quad \deg(\hat{P}_j) \leq \deg(P_j)(|P_j(X)| - 1),$$  

(4)

(I(X) = \{ f \in \mathbb{F}[x_1, \ldots, x_n] | \forall x \in X : f(x) = 0 \} is the ideal of polynomials vanishing on $X \subseteq \mathbb{F}^n$.)
where the inequality uses the assumption that 0 ∈ \( P_i(X) \). For every 1 ≤ i ≤ m, let \( I_i \in \mathbb{F}[x] \) be the polynomial

\[
I_i = \frac{\hat{P}_i}{P_i} \prod_{j=i+1}^{m} (1 - \hat{P}_j). \tag{5}
\]

Observe that \( \hat{P}_i/P_i \) (and thus \( I_i \)) is indeed a polynomial since \( C_Y(x)/x \in \mathbb{F}[x] \) is, which follows from the fact that the univariate polynomial \( C_Y \) satisfies \( C_Y(0) = 0 \). Let the function \( I: X \to \{0, 1\} \) be given by \( I(x) = [x \notin Z(P_1, \ldots, P_m)] \). We claim that \( I \equiv_X \sum_{i=1}^{m} I_i P_i \). Indeed,

\[
\sum_{i=1}^{m} I_i P_i = \sum_{i=1}^{m} \frac{\hat{P}_i}{P_i} \prod_{j=i+1}^{m} (1 - \hat{P}_j) = \sum_{i=1}^{m} \sum_{J \subseteq [m]; \min J = i} \prod_{j \in J} (-\hat{P}_j)
\]

\[= - \sum_{J \subseteq [m]; J \neq \emptyset} \prod_{j \in J} (-\hat{P}_j) = -\left( \prod_{j=1}^{m} (1 - \hat{P}_j) - 1 \right) \equiv_X I,
\]

where the last step follows as \( \prod_{i=1}^{m} (1 - \hat{P}_j(x)) = \prod_{j=1}^{m} [P_j(x) = 0] = [x \in Z(P_1, \ldots, P_m)] \) for every \( x \in X \).

Using the statement’s assumption \( Z(P_1, \ldots, P_m) \cap X \subseteq Z(Q) \) we deduce that \( Q \equiv_X Q I \equiv_X \sum_{i=1}^{m} (Q I_i) P_i \).

Each \( R_i := Q I_i \in \mathbb{F}[x] \) is, by (4) and (5), of degree

\[
\deg(R_i) \leq \deg(Q) + \deg(P_i)(|P_i(X)| - 2) + \sum_{j=i+1}^{m} \deg(P_j)(|P_j(X)| - 1).
\]

In particular, \( \deg(R_i) \leq md(F - 1) \). This completes the proof.

Let us remark that it is indeed necessary to separate the case \( m = 1 \) in Theorem 2, since the bound \( D \leq md(F - 1) \) does not hold for \( m = 1 \). To see this, consider for example the univariate real polynomials \( P, Q \in \mathbb{R}[x] \) given by \( P = x^2 \) and \( Q = x \), and the set \( X = \{-F, \ldots, -1, 1, \ldots, F\} \subseteq \mathbb{R} \), so that \( |P(X)| = |\{1^2, \ldots, F^2\}| = F \). Since \( 0 \notin P(X) \), if \( Q \equiv_X RP \) then \( R(x) = Q(x)/P(x) = 1/x \) for every \( x \in X \). By Lagrange interpolation (originally due to Waring [21]), the unique univariate polynomial \( \hat{R}(x) \) with \( \deg(R) < |X| \) satisfying \( \hat{R}(x) = 1/x \) for every \( x \in X \) has the maximal degree, \( |X| - 1 \); explicitly, the coefficient of \( x^{|X|-1} \) in \( \hat{R} \) is\(^6\)

\[
\sum_{i \in X} \frac{1}{i} \prod_{j \in X \setminus \{i\}} \frac{1}{i - j} = \sum_{k=0}^{2F} \sum_{k' = 0, k' \neq k, k' \neq F} \frac{1}{k - k'} = \sum_{k=0}^{2F} \frac{(-1)^k}{(2F)!} \left( \frac{2F}{k} \right) = \frac{(-1)^F}{(2F)!} \left( \frac{2F}{F} \right) = \frac{(-1)^{F+1}}{(F!)^2} \neq 0.
\]

Therefore \( \deg(R) = 2F - 1 \) (which matches (3)) is indeed larger than \( 2(F - 1) \). The reason that in Theorem 1 the analogous bound \( D \leq md(|\mathbb{F}| - 1) \) holds even for \( m = 1 \)

\(^6\)The first equality uses the change of variables \((k, k') = (F + i, F + j)\).
is that over a finite field $\mathbb{F}$, the univariate function $x \mapsto 1/x$ for $x \neq 0$ can actually be interpolated by a polynomial of degree strictly smaller than $|\mathbb{F}| - 1$; indeed, $x^{|\mathbb{F}|-2} = 1/x$ for every $x \in \mathbb{F} \setminus \{0\}$.

**ACKNOWLEDGMENTS.** We thank Shachar Lovett and Robert Robere for helpful discussions. We thank Pete L. Clark for communicating to us the generalization of the main theorem to arbitrary fields (Theorem 2). We thank the anonymous referees for useful comments. This project was conducted as part of the 2021 New York Discrete Mathematics REU, funded by NSF grant DMS 2051026, and partially supported by award PSC-CUNY TRADB-52-76.

**REFERENCES**

[1] Alekhnovich, M., Razborov, A. (2003). Lower bounds for polynomial calculus: non-binomial case. Proc. Steklov Inst. Math. 242: 18–35.

[2] Ax, J. (1964). Zeros of polynomials over finite fields. Amer. J. Math. 86(2): 255–261.

[3] Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., Pudlák, P. (1996). Lower bounds on Hilbert’s Nullstellensatz and propositional proofs. Proc. London Math. Soc. 73(1): 1–26.

[4] Ben-Sasson, E., Impagliazzo, R. (2010). Random CNF’s are hard for the polynomial calculus. Comput. Complex. 19(4): 501–519.

[5] Buss, S. R., Grigoriev, D., Impagliazzo, R., Pitassi, T. (2001). Linear gaps between degrees for the polynomial calculus modulo distinct primes. J. Comput. Syst. Sci. 62(2): 267–289.

[6] Brownawell, W. D. (1987). Bounds for the degrees in the Nullstellensatz. Ann. Math. 126(3): 577–591.

[7] Chevalley, C. (1935). Démonstration d’une hypothèse de M. Artin. Abh. Math. Sem. Univ. Hamburg. 11(1): 73–75.

[8] Clark, P. L. (2014). The combinatorial Nullstellensätze revisited. Electron. J. Comb. 21(4): P4.15.

[9] Clark, P. L. (2021). An effective Semifinitesatz. http://alpha.math.uga.edu/~pete/SemiFiniteSatz.pdf.

[10] Croot, E., Lev, V. F., Pach, P. P. (2017). Progression-free sets in $\mathbb{Z}_n^4$ are exponentially small. Ann. Math. 185(1): 331–337.

[11] Ellenberg, J. S., Gijswijt, D. (2017). On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Ann. of Math. 185(1): 339–343.

[12] Euler, L. (1750). Theorematia circa divisores numerorum. Novi Comment. Acad. Sci. Imp. Petropol. 1: 20–48.

[13] Euler, L. (1761). Theorematia circa residua ex divisione potestatum relictæ. Novi Comment. Acad. Sci. Imp. Petropol. 7: 49–82.

[14] Green, B., Tao, T. (2009). The distribution of polynomials over finite fields, with applications to the Gowers norms. Contrib. Discrete Math. 4(2): 1–36.

[15] Grigoriev, D. (1998). Tseitin’s tautologies and lower bounds for Nullstellensatz proofs. Presented at the 39th IEEE Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 1998.

[16] Hermann, G. (1926). Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. 95(1): 736–788.

[17] Hilbert, D. (1893). Über die vollen invariantensysteme. Math. Ann. 42: 313–373.

[18] Kollár, J. (1988). Sharp effective Nullstellensatz. J. Am. Math. Soc. 1(4): 963–975.

[19] Kummer, E. (1852). Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. J. für die Reine und Angew. Math. 44: 93–146.

[20] Lucas, E. (1878). Théorie des Fonctions Numériques Simplement Périodiques. Am. J. Math. 1(4): 184–240, 289–321.

[21] Waring, E. (1779). Problems concerning interpolations. Philos. Trans. Royal Soc. A. 69: 59–67.

**GUY MOSHKOVITZ** completed his doctorate in mathematics at Tel Aviv University, followed by postdoctoral positions at Harvard, DIMACS, and the Institute for Advanced Study. He has a broad interest in discrete mathematics, with a particular focus on extremal combinatorics, applications of algebraic geometry to combinatorics and computer science, and complexity theory. He is currently an assistant professor at the City University of New York.

Department of Mathematics, City University of New York (Baruch College and the Graduate Center), New York, NY 10010, USA
guymoshkov@gmail.com

© THE MATHEMATICAL ASSOCIATION OF AMERICA
The Fundamental Theorem of Algebra via Real Polynomials

The fundamental theorem of algebra states that every polynomial $p(z)$ over $\mathbb{C}$ of degree $m \geq 1$ has a zero in $\mathbb{C}$. There are many proofs of this theorem, but we have not found the elementary one presented here. Splitting the coefficients of $p(z)$ into their real and imaginary parts, we find polynomials $a(z)$ and $b(z)$ with real coefficients such that $p(z) = a(z) + ib(z)$. Then

$$q(z) := p(z)p(\bar{z}) = a(z)^2 + b(z)^2$$

is a polynomial of degree $2m \geq 2$ with real coefficients, and $q(x) \geq 0$ for all $x \in \mathbb{R}$. Moreover, $q(z) = 0$ if and only if $p(z) = 0$ or $p(\bar{z}) = 0$. If $q(z) \neq 0$ for all $z \in \mathbb{C}$, then $F(z) := \int_0^1 z/q(tz) \, dt$ defines a primitive of $1/q(z)$ on $\mathbb{C}$. Hence the integral over the piecewise smooth closed curve given by the interval $[-r, r]$ and the positively oriented semi-circle $C_r := \{re^{i\theta}: \theta \in [0, \pi]\}$ vanishes, that is,

$$\int_{-r}^r \frac{1}{q(x)} \, dx + \int_{C_r} \frac{1}{q(z)} \, dz = 0 \quad (6)$$

for all $r > 0$ (special case of the Cauchy integral theorem). As $q(z)$ has degree $2m$ there exist constants $c, R > 0$ such that $|q(z)| \geq c|z|^{2m}$ whenever $|z| \geq R$. Using that $m \geq 1$

$$\lim_{r \to \infty} \left| \int_{C_r} \frac{1}{q(z)} \, dz \right| \leq \lim_{r \to \infty} \int_0^\pi \frac{r}{|q(re^{i\theta})|} \, d\theta \leq \lim_{r \to \infty} \frac{\pi r}{cr^{2m}} = 0.$$

Taking into account (6) and that $q(x) > 0$ for all $x \in \mathbb{R}$ we deduce that

$$0 = \lim_{r \to \infty} \left( \int_{-r}^r \frac{1}{q(x)} \, dx + \int_{C_r} \frac{1}{q(z)} \, dz \right) = \int_{-\infty}^\infty \frac{1}{q(x)} \, dx > 0,$$

which is a contradiction. Hence $q(z)$ and thus $p(z)$ must have a zero.

ORCID
Daniel Daners  http://orcid.org/0000-0002-0122-3789
Laurentiu Paunescu  http://orcid.org/0000-0001-5796-276X

—Submitted by Daniel Daners and Laurentiu Paunescu
The University of Sydney, Australia

doi.org/10.1080/00029890.2023.2230811
MSC: Primary 30C15, Secondary 12D05; 30C10