Chevalley's theorem with restricted variables

David Brink

10 May 2010

First, a generalization of Chevalley's classical theorem from 1936 on polynomial equations $f(x_1, \ldots, x_N) = 0$ over a finite field K is given, where the variables x_i are restricted to arbitrary subsets $A_i \subseteq K$. The proof uses Alon's Nullstellensatz. Next, a theorem on integer polynomial congruences $f(x_1, \ldots, x_N) \equiv 0 \pmod{p^\nu}$ with restricted variables is proved, which generalizes a more recent result of Schanuel. Finally, an extension of Olson's theorem on zero-sum sequences in finite Abelian p-groups is derived as a corollary.

Chevalley's theorem states that a set of polynomials $f_j(X_1, \ldots X_N)$ over a finite field K without constant terms has a non-trivial common zero $(a_1, \ldots, a_N) \in K^N$ if the number of variables N exceeds the sum of total degrees $\sum_j \deg(f_j)$, thereby settling in the affirmative the conjecture of Artin that finite fields are *quasi-algebraically closed* [2].

Alon's *Nullstellensatz* is the assertion that a polynomial $f(X_1, \ldots, X_N)$ over an arbitrary field K cannot vanish on a set $\prod_{i=1}^N A_i$ with $A_i \subseteq K$ if it has a non-zero term $\delta X_1^{t_1} \cdots X_N^{t_N}$ of maximal total degree and such that $|A_i| > t_i$ for all i [1, Theorem 1.2]. This simple principle has become an all-conquering force in combinatorics with applications in numerous areas. Interestingly, the special case where K is finite and $A_i = K$ for all i appears already in Chevalley's proof.

The first theorem in the present note extends Chevalley's theorem to polynomials with restricted variables. The proof follows that of Chevalley, but uses Alon's Nullstellensatz rather than the above-mentioned special case (see also [1, Theorem 3.1]).

Theorem 1. *Consider the polynomials $f_1(X_1, \ldots, X_N), \ldots, f_R(X_1, \ldots, X_N)$ over the finite field $\mathbb{F}_q$. Let $A_1, \ldots, A_N$ be non-empty subsets of $\mathbb{F}_q$ such that*

$$\sum_i (|A_i| - 1) > \sum_j \deg(f_j)(q-1).$$

Then the solution set

$$V = \{\mathbf{a} \in \prod_i A_i \mid f_j(\mathbf{a}) = 0 \textit{ for all } j\}$$

with the variables restricted to the A_i is not a singleton.

Proof. Assume for a contradiction $V = \{\mathbf{a}\}$ with $\mathbf{a} = (a_1, \ldots, a_N)$. Then $P(\mathbf{X}) = \prod_j (1 - f_j(\mathbf{X})^{q-1})$ satisfies

$$P(\mathbf{x}) = \begin{cases} 1 & \text{for } \mathbf{x} = \mathbf{a}, \\ 0 & \text{for } \mathbf{x} \in \prod_i A_i \backslash \{\mathbf{a}\}. \end{cases}$$

Further, $Q(\mathbf{X}) = \prod_i \prod_{b \in A_i \backslash \{a_i\}} (X_i - b)$ satisfies

$$Q(\mathbf{x}) = \begin{cases} \delta & \text{for } \mathbf{x} = \mathbf{a}, \\ 0 & \text{for } \mathbf{x} \in \prod_i A_i \backslash \{\mathbf{a}\}, \end{cases}$$

with some (non-zero) $\delta \in \mathbb{F}_q$. It follows from the theorem's assumption that $X_1^{|A_i|-1} \cdots X_N^{|A_N|-1}$ is the term of maximal degree in $Q(\mathbf{X}) - \delta \cdot P(\mathbf{X})$. But this contradicts the Nullstellensatz since this polynomial vanishes on $\prod_i A_i$. ∎

If the polynomials are without constant terms, the trivial solution together with $|V| \neq 1$ thus imply the existence of a non-trivial solution. It is worth noting that in the case where $A_i = \mathbb{F}_q$ for all i, the above proof is easily modified to show a little more, namely that $|V| \equiv 0 \pmod{p}$ where p is the characteristic of $\mathbb{F}_q$. This result, which was shown by Warning with an entirely different method, is known as the *Chevalley-Warning theorem* [5].

Schanuel showed that a set of congruences $f_j(a_1, \ldots, a_N) \equiv 0 \pmod{p^{\nu_j}}$ with a prime p and polynomials $f_j(X_1, \ldots, X_N)$ over $\mathbb{Z}$ without constant terms has a non-trivial solution $(a_1, \ldots, a_N) \in A^N$ if N exceeds the sum $\sum_j \deg(f_j)(p^{\nu_j} - 1)(p-1)^{-1}$ [4]. Here $A = \{x \in \mathbb{Z}/p^\nu\mathbb{Z} \mid x^p = x\}$ is the set of so-called *Teichmüller representatives* modulo p^ν, $\nu = \max_j \nu_j$.

The second theorem given here generalizes Schanuel's result. The last part of the proof follows, and at one point simplifies, that of Schanuel.

Theorem 2. *Consider the polynomials $f_1(X_1, \ldots, X_N), \ldots, f_R(X_1, \ldots, X_N)$ over $\mathbb{Z}$. Let $\nu_1, \ldots, \nu_R$ be positive integers, p a prime, and $A_1, \ldots, A_N$ non-empty subsets of $\mathbb{Z}$ such that, for each i, the elements of A_i are pairwise incongruent modulo p. Assume further*

$$\sum_i (|A_i| - 1) > \sum_j \deg(f_j)(p^{\nu_j} - 1).$$

Then the solution set

$$V = \{\mathbf{a} \in \prod_i A_i \mid f_j(\mathbf{a}) \equiv 0 \ (mod\ p^{\nu_j}) \ for\ all\ j\}$$

with the variables restricted to the A_i is not a singleton.

Proof. First assume that all $\nu_j = 1$. Then Theorem 2 clearly reduces to Theorem 1 with $q = p$.

Now let the ν_j be arbitrary. We then define, for each i, a polynomial $\tau_i(X) \in \mathbb{Q}[X]$ of degree $< p$ such that $\tau_i(a) = (a - a^p)/p$ for every $a \in A_i$. Since A_i has at most p elements, such a polynomial can be constructed by Lagrange interpolation, i.e.

$$\tau_i(X) = \sum_{a \in A_i} \left(\frac{a - a^p}{p} \cdot \prod_{b \in A_i \setminus \{a\}} \frac{X - b}{a - b} \right).$$

Recall that a rational number n/m with $(n, m) = 1$ is called *p-adically integral* if $p \nmid m$, and that such numbers form a subring of $\mathbb{Q}$ denoted $\mathbb{Z}_{(p)}$. Since $(a - a^p)/p$ is an integer (by Fermat's little theorem), and a and b are distinct modulo p (being distinct elements of A_i), the coefficients of $\tau_i(X)$ are p-adically integral. Then put $\sigma_i(X) = X^p + p \cdot \tau_i(X)$ and note $\sigma_i(X) \in \mathbb{Z}_{(p)}[X]$, $\deg(\sigma_i) = p$, $\sigma_i(X) \equiv X^p \pmod{p}$ and $\sigma_i(a) = a$ for all $a \in A_i$.

Next define an operator $\Delta : \mathbb{Z}_{(p)}[X_1, \dots, X_N] \to \mathbb{Z}_{(p)}[X_1, \dots, X_N]$ by letting

$$(\Delta f)(X_1, \dots, X_N) = (f(X_1, \dots, X_N)^p - f(\sigma_1(X_1), \dots, \sigma_N(X_N)))/p.$$

As in [4], one observes that Δf has, in fact, coefficients in $\mathbb{Z}_{(p)}$; that $\deg(\Delta f) \leq p \cdot \deg(f)$; that $\Delta c = (c^p - c)/p$ for $f = c$ constant; that $c \equiv 0 \pmod{p^\nu}$ if and only if $c, \Delta c, \dots, \Delta^{\nu-1} c \equiv 0 \pmod{p}$; and that $(\Delta f)(\mathbf{a}) = \Delta(f(\mathbf{a}))$ for $\mathbf{a} \in \prod_i A_i$. For $\mathbf{a} \in \prod_i A_i$ it is concluded that $f(\mathbf{a}) \equiv 0 \pmod{p^\nu}$ if and only if $(\Delta^i f)(\mathbf{a}) \equiv 0 \pmod{p}$ for all $i = 0, \dots, \nu - 1$. Thus one congruence modulo p^ν of degree $\deg(f)$ can be replaced by ν congruences modulo p, the sum of whose degrees is at most $\deg(f)(1 + p + \cdots + p^{\nu-1}) = \deg(f)(p^\nu - 1)(p - 1)^{-1}$. This, together with Theorem 1, finishes the proof. ∎

Theorem 2 is stated only over $\mathbb{Z}$, but it is straightforwardly extended to the ring of integers in any algebraic number field. The prime p should then be replaced by a prime ideal $\mathfrak{p}$, and the last assumption by $\sum_i (|A_i| - 1) > \sum_j \deg(f_j)(q^{\nu_j} - 1)$ where $q = N(\mathfrak{p})$ is the norm of $\mathfrak{p}$.

It is a famous result of Olson, answering in part a question of Davenport, that a sequence $g_1, \dots, g_N$ of elements from a finite Abelian p-group with cyclic factors $\mathbb{Z}/p^{\nu_j}\mathbb{Z}$ has a non-empty subsequence with sum zero if its length N exceeds $\sum_j (p^{\nu_j} - 1)$ [3]. It is remarkable that Olson's theorem is equivalent to the special case of Schanuel's theorem where all f_j are of the form $f_j^*(X_1^{p-1}, \dots, X_N^{p-1})$ with linear f_j^*. Using Theorem 2 with linear f_j instead, one obtains the following extension of Olson's theorem:

Corollary. *Let $g_1, \dots, g_N$ be a sequence of elements from a finite Abelian p-group $\prod_j \mathbb{Z}/p^{\nu_j}\mathbb{Z}$. Let $A_1, \dots, A_N$ be subsets of $\mathbb{Z}$ such that each A_i contains 0 and has elements pairwise incongruent modulo p. Assume*

$$\sum_i (|A_i| - 1) > \sum_j (p^{\nu_j} - 1).$$

Then the equation $a_1 g_1 + \cdots + a_N g_N = 0$ has a non-trivial solution $(a_1, \dots, a_N)$ in $\prod_i A_i$. ▮

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29.

[2] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.

[3] J. E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8–10.

[4] S. H. Schanuel, *An extension of Chevalley's theorem to congruences modulo prime powers*, J. Number Theory **6** (1974), 284–290.

[5] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.