Grid reduction of polynomials, Combinatorial Nullstellensätze and Chevalley-Warning theorems.

Anurag Bishnoi

June 28, 2016

Abstract

Inspired by [Cl14] we lay down the basic theory of polynomials over finite grids satisfying Condition (D). We see how the operation of Grid Reduction on polynomials provides the main link between the classical Chevallay-Warning theorem [Ch35], [Wa35] and Alon's Combinatorial Nullstellensatz [Al99]. We also give an easy proof of Ball and Serra's punctured combinatorial nullstellensatz [BS09] from which we prove a new generalisation of the Chevalley-Warning theorem.

Notation: Let R be a commutative ring with unity and let F be a field. A set $S \subseteq R$ is said to satisfy Condition (D) if for all distinct $x, y \in S$ the element $x - y \in R$ is not a zero divisor. For $f \in R[t_1, \ldots, t_n]$ we denote the maximum power of the variable t_i appearing in f by $\deg_{t_i} f$ and the total degree of f by $\deg f$. Let $A_1, \ldots, A_n$ be non-empty finite subsets of R. We will refer to the cartesian product $A_1 \times \cdots \times A_n$ as a **grid** in R^n and denote it by A.

Lemma 1. *Let $f, g, h \in R[t_1, \ldots, t_n]$ with $f = g + h$.*

(a) If $\deg f \geq \deg g$, then $\deg f \geq \deg h$.

(b) For every i, if $\deg_{t_i} f \geq \deg_{t_i} g$, then $\deg_{t_i} f \geq \deg_{t_i} h$.

Proof. This follows from looking at the highest degree monomials. □

Lemma 2. *Let $f, g, h \in R[t_1, \ldots, t_n]$ with g monic and $f = gh$. Then $\deg f = \deg g + \deg h$.*

Proof. Look at the highest degree monomials in g and h. Since g is monic [1], the coefficient of such monomial in g is 1, which is not a zero divisor in R. □

From Euclidean division algorithm it follows that a single variable polynomial of degree d with coefficients from an integral domain has at most d zeroes. For commutative rings with zero divisors this result is not true in general. For example, $f = 2x$ has two zeroes in $\mathbb{Z}/4\mathbb{Z}$. But, if we restrict ourselves to a subset $S \subseteq R$ that satisfies Condition (D), then we can show that a non-zero polynomial $f \in R[t]$ has at most $\deg f$ zeroes in S.

[1] Is there a standard definition of multivariate monic polynomials? We are considering g to be univariate here.

Lemma 3 (Euclidean Division Algorithm)**.** *Let $f, g \in R[t]$ with g monic. Then there exist polynomials $h, r \in R[t]$ such that $f = gh + r$ and $\deg r < \deg g$.*

Proof. Say $\deg f > \deg g$. Let m_f be the highest degree monomial in f, and m_g the highest degree monomial in g. Since g is monic, the coefficient of m_g in g is 1. Multiplying g by $c_f m_f / m_g$ where c_f is the coefficient of m_f in f, we get a polynomial g' such that $\deg(f - g') < \deg f$. Now use induction. □

Corollary 4. *Let $f \in R[t]$. If $S \subseteq R$ such that S satisfies Condition (D), then f as at most $\deg f$ zeroes in S.*

Proof. Let $\alpha \in S$ be a zero of f. We can write $f = (t - \alpha)h + r$ with $\deg r < 1$ (so $r \in R$). Substituting α in the equation we see that $r = 0$. Let $\beta \in S \setminus \{\alpha\}$. Then $f(\beta) = (\beta - \alpha)h(\beta)$. Since $\beta - \alpha$ is not a zero divisor, $f(\beta) = 0$ if and only if $h(\beta) = 0$. Thus, we can use induction on $\deg f$ to prove the result. □

In other words, if f has more than $\deg f$ zeroes in a set $S \subseteq R$ satisfying Condition (D), then $f = 0$. The following lemma is an easy generalisation of this fact to multivariate polynomials.

Lemma 5. *Let R be a ring and let $A_1, \ldots, A_n$ be non-empty finite subsets of R that satisfy Condition (D). Put $A := A_1 \times \cdots \times A_n$. Let $f \in R[t_1, \ldots, t_n]$ such that for all i with $1 \leq i \leq n$ we have $\deg_{t_i} f \leq \#A_i - 1$. If $f(x) = 0$ for all $x \in A$, then $f = 0$.*

Proof. We prove this by induction. The base case is clear from Corollary 4. For the inductive step write

$$f = \sum_{i=0}^{d_n} f_i(t_1, \ldots, t_{n-1}) t_n^i.$$

where $d_n = \deg_{t_n} f$. Let $x' \in A' = A_1 \times \cdots \times A_{n-1}$. Since $f(x) = 0$ for all A we see that the single variable polynomial $f(x', t_n)$ vanishes everywhere on A_n. Since $\deg f(x', t_n) = d_n < \#A_n$, this means that $f(x', t_n)$ is the zero polynomial. This implies that for all i, $f_i(x') = 0$ for all $x' \in A'$. By the induction hypothesis, $f_i = 0$ for al i and hence $f = 0$. □

Lemma 6. *Let $f \in R[t_1, \ldots, t_n]$ and let g be a monic polynomial in $R[t_i]$ for some $1 \leq i \leq n$. Then, there exist $h, r \in R[t_1, \ldots, t_n]$ such that*

$$f = gh + r$$

and $\deg_{t_i} r < \deg g$. Moreover, $\deg h \leq \deg f - \deg g$, and $\deg r \leq \deg f$.

Proof. WLOG, take $i = n$. Let $R' = R[t_1, \ldots, t_{n-1}]$. Then f and g can be seen as polynomials in $R'[t_n]$. By Lemma 3 $f = gh + r$ for some polynomials $h, r \in R'[t_n]$ such that $\deg r < \deg g$. If we now see h and r as polynomials in $R[t_1, \ldots, t_n]$ we get that $\deg_{t_n} r < \deg g$. Since $\deg_{t_n} r < d := \deg g$, for every monomial $t_1^{e_1} t_2^{e_2} \cdots t_n^{e_n}$ in h there exists a monomial $t_1^{e_1} t_2^{e_2} \cdots t_n^{e_n + d}$ in f. This shows that $\deg f \geq \deg h + \deg g$. Now from Lemmas 2 and 1 it follows that $\deg f \geq \deg r$. □

Definition A polynomial $f \in R[t_1, \ldots, t_n]$ is called A-reduced if for all i with $1 \leq i \leq n$, $\deg_{t_i} f \leq \#A_i - 1$.

Therefore, Lemma 5 shows that an A-reduced polynomial vanishes on all points of A if and only if it is the zero polynomial. To see that this is not true in general for polynomials that are not A-reduced, look at the polynomial $\prod_{\lambda \in A_1}(t_1 - \lambda)$ which vanishes everywhere on A and has degree equal to $\#A_i$. Here's another nice property of reduced polynomials.

Lemma 7. *Let $f \in R[t_1, \ldots, t_n]$ be A-reduced and let $\lambda \in A_i$ for some i. If $f_\lambda = f(t_1, \ldots, t_{i-1}, \lambda, t_i, \ldots, t_n)$ vanishes everywhere on $A_1 \times \cdots \times A_{i-1} \times A_{i+1} \times \cdots \times A_{n-1}$, then $t_i - \lambda$ divides f.*

Proof. Using Lemma 6 write $f = (t_i - \lambda)h + r$ with $\deg_{t_i} r < 1$, i.e., $r \in R[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n]$. From Lemma 1 it follows that r is also A-reduced. Say f_λ vanishes everywhere. Then r vanishes everywhere, and hence by Lemma 5 we get $r = 0$, i.e., $t_i - \lambda$ divides f. □

Now we show that if we are only concerned with the values of a polynomial f in A, we can look at a reduced polynomial which has the same values as f on A. The proof also defines what it means to reduce a polynomial modulo a grid A, which we refer to as **grid reduction**.

Lemma 8. *Let R be a ring and let $A_1, \ldots, A_n$ be non-empty finite subsets of R that satisfy Condition (D). Put $A = A_1 \times \cdots \times A_n$. For every polynomial $f \in R[t_1, \ldots, t_n]$ there exists a unique A-reduced polynomial $\widehat{f}$ such that $f(x) = \widehat{f}(x)$ for all $x \in A$. Moreover, $\deg \widehat{f} \leq \deg f$.*

Proof. For $1 \leq i \leq n$ define a polynomial $g_i = \prod_{\lambda \in A_i}(t_i - \lambda)$ of degree $\#A_i$. By using Lemma 3 repeatedly we get $f = r + g_1 h_1 + \cdots + g_n h_n$, where $\deg_{t_i} r < \#A_i$ for all i. Therefore, r is A-reduced. Moreover, Lemma 3 also shows that $\deg f \geq \deg r$. Since $g_i(x) = 0$ for all i and for all $x \in A$, we see that $f(x) = r(x)$ for all $x \in A$. The uniqueness of r follows from Lemma 5. We will denote this unique r by $\widehat{f}$. □

For each i, define $g_i := \prod_{\lambda \in A_i}(t_i - \lambda)$. Reducing a polynomial f modulo the grid A is to be understood as writing $f = \widehat{f} + \sum g_i h_i$ by repeatedly using Lemma 3 (as in the proof of Lemma 8).

Theorem 9 (All but one)**.** *Let $f \in R[t_1, \ldots, t_n]$ and let $A = A_1 \times \ldots A_n$ be a finite grid in R^n that satisfies Condition (D). If f vanishes on all points of A except one, then $\deg f \geq \sum(\#A_i - 1)$.*

Proof. Let $a = (a_1, \ldots, a_n)$ be the point where f doesn't vanish. The polynomial $\prod_i \prod_{\lambda \in A_i \setminus \{a_i\}}(t_i - \lambda)$ of degree $\sum(\#A_i - 1)$ is an A-reduced polynomial that vanishes everywhere except at a. By Lemma 8 this must be equal to $\widehat{f}$ and hence $\deg f \geq \deg \widehat{f} = \sum(\#A_i - 1)$. □

Theorem 9 already appears in the special case of $R = \mathbb{F}_q$ and $A = \mathbb{F}_q^n$ in the proof of Chevalley-Warning theorem by Chevalley [Ch35]. It is proved again in [BS78] to prove a bound on the size of affine blocking sets. Finally, we see it in [AF93] for the case when R is a field and A is a finite grid, where they use it to prove the following.

Corollary 10. *Let $A_1 \ldots A_n$ be finite subsets of F. The number of hyperplanes in F^n required to cover all points of $A_1 \times \cdots \times A_n$ except one is at least $\sum(\#A_i - 1)$.*

Proof. The points covered by a hyperplane are the zeroes of the degree one polynomial that defines the hyperplane. Take the product of these polynomials to get the union of points covered by the given hyperplanes. □

Another direct Corollary of Theorem 9 is the following generalisation of the Chevalley-Warning theorem by D. Brink [Br11].

Corollary 11 (Restricted Variable Chevalley-Warning Theorem)**.** *Let* $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ *and let* $A_1, \ldots, A_n$ *be non-empty subsets of* $\mathbb{F}_q$*. Let* $Z_A = \{x \in \prod A_i : \forall j \ f_j(x) = 0\}$*. If* $(q-1)\sum \deg f_j < \sum(\#A_i - 1)$*, then* $|Z_A| \neq 1$*.*

Proof. Let $f = \prod(1 - f_j^{q-1})$ be the polynomial of degree $(q-1)\sum \deg f_j$ which is equal to 1 on all common zeroes of f_j's and 0 otherwise. Then Z_A corresponds to the set of non-zeroes of f in $A = A_1 \times \cdots \times A_n$. Say $|Z_A| = 1$. Then by Theorem 9 we have $\deg f = (q-1)\sum \deg f_j \geq \sum(\#A_i - 1)$, which is a contradiction. □

Next we show a simple proof of Alon's Combinatorial Nullstellensatz that uses the ideas of grid reduction developed so far. We note that this proof is essentially the same as the first proof given by Alon in [Al99]. Its generalisation over rings is due to Schauz [Sc08] and the idea to look at this proof in the following way is essentially due to Clark [Cl14].

Theorem 12 (Combinatorial Nullstellensatz for Rings)**.** *Let* $f \in R[t_1, \ldots, t_n]$ *and let* $A = A_1 \times \cdots \times A_n$ *be a finite grid in* R^n *that satisfies Condition (D). For all* i *with* $1 \leq i \leq n$*, define* $g_i = \prod_{\lambda \in A_i}(t_i - \lambda)$*.*

(*a*) *If* f *vanishes on all points of* A*, then there exist* $h_1, \ldots, h_n$ *such that* $f = \sum g_i h_i$ *and* $\deg h_i \leq \deg f - \deg g_i$ *for all* i*.*

(*b*) *If there is a monomial term* $\prod t_i^{d_i}$ *in* f *with the property that* $d_1 + \cdots + d_n = \deg f$ *and* $d_i < \deg g_i = |A_i|$ *for all* i*, then* f *doesn't vanish everywhere on* A*.*

Proof. Reduce f modulo the grid A. Then $\widehat{f}$ vanishes everywhere on A, and hence by Lemma 5 it must be zero. For part (*b*) observe that such a monomial term is not affected by grid reduction, and hence the reduced form of f is non-zero. This would contradict f vanishing everywhere as that would imply $\widehat{f} = 0$. □

Theorem 13 (Coefficient Formula)**.** *Let* $f \in R[t_1, \ldots, t_n]$ *and let* $A = A_1 \times \cdots \times A_n$ *be a finite grid in* R^n *that satisfies Condition (F). Suppose* $\deg f = \sum d_i$ *where* $d_i = |A_i| - 1$*. For all* i *with* $1 \leq i \leq n$*, define* $g_i = \prod_{\lambda \in A_i}(t_i - \lambda)$*. Then the coefficient of* $t_1^{d_1} \cdots t_n^{d_n}$ *in* f *is equal to*

$$\sum_{(x_1, \ldots, x_n) \in A} \frac{f(x)}{\prod_{i=1}^n g_i'(x_i)},$$

where $g_i'(x_i) = \prod_{\lambda \in A_i \setminus \{x_i\}}(x_i - \lambda)$*.*

Proof. The coefficient remains the same for f and $\widehat{f}$ since the term $\prod t_i^{d_i}$ is not affected by grid reduction. For a fixed $a = (a_1, \ldots, a_n) \in A$, the polynomial

$\delta_a = \prod_{i=1}^{n} \frac{g_i(t_i)}{g_i'(a_i)(t_i - a_i)}$ has the property that $\delta_a(a) = 1$ and $\delta_a(x) = 0$ for all $x \in A \setminus \{a\}$. Thus, by uniqueness of $\widehat{f}$ we get

$$\widehat{f} = \sum_{x \in A} f(x)\delta_x.$$

[2] Note that $\deg \delta_a = d_1 + \cdots + d_n = \deg f = \deg \widehat{f}$. By comparing coefficient on both sides we get our result. □

Remark 14. The Coefficient formula is due to [Sc08]. Also see [La10] and [KP12]. If f is a single-variable polynomial of degree d over a field F and S is any set of $d+1$ elements from F, then f is completely determined by the values it takes in F. By Lagrange interpolation, we have $f(t) = \sum_{x \in S} f(x)\delta_x = \sum_{x \in S} \frac{f(x)}{g'(x)} \frac{g(t)}{(t-x)}$ where $g(t) = \prod_{s \in S}(t - s)$. But when f is as given in the statement of Theorem 13, then only the reduced form $\widehat{f}$ is completely determined by the values of f on the grid, from which we can derive some useful information about f but not everything. So, it is a weaker statement than the single variable Lagrange interpolation. For example, let $f(t_1, t_2) = t_1^2 t_2^4 + t_1^3 t_2^3$, $A = A_1 \times A_2$ where $|A_1| = 3$ and $|A_2| = 5$ so that $\deg f = |A_1| - 1 + |A_2| - 1$. Then the coefficient of $t_1^2 t_2^4$ in f is equal to the coefficient of $t_1^2 t_2^4$ in $\widehat{f}$, but the same cannot be said for $t_1^3 t_2^3$ as that monomial gets affected by grid reduction. Thus, we cannot simply write f as a linear combination of δ_a's for $a \in A$.

Note that Theorem 12 (b) is implied by Theorem 13 when the grid satisfies Condition (F). The following result of Simeon Ball and Oriol Serra is a generalisation of both Theorem 9 and part (a) of Theorem 12. Our proof is slightly simpler than the original proof which uses Combinatorial Nullstellensatz.

Theorem 15 (Punctured Combinatorial Nullstellensatz for Rings)**.** *Let $f \in R[t_1, \ldots, t_n]$ and let $A = A_1 \times \ldots A_n$ be a finite grid in R^n that satisfies Condition (D). Let $B = B_1 \times \cdots \times B_n$ be a sub-grid of A. For all i with $1 \leq i \leq n$, define $g_i = \prod_{\lambda \in A_i}(t_i - \lambda)$. If f vanishes on all points of A except at some point of B, then there exist polynomials $h_1, \ldots, h_n$ such that $f = r + \sum g_i h_i$ where r is a non-zero multiple of the polynomial $\prod_i \prod_{\lambda \in A_i \setminus B_i}(t_i - \lambda)$ and $\deg h_i \leq \deg f - \deg g_i$ for all i. Moreover, $\deg f \geq \deg r \geq \sum(\#A_i - \#B_i)$.*

Proof. Reduce f modulo A to get $f = \widehat{f} + \sum g_i h_i$. For a given i let $\lambda \in A_i \setminus B_i$. By the given condition on f, the polynomial $\widehat{f}_\lambda = \widehat{f}(t_1, \ldots, t_{i-1}, \lambda, t_{i+1}, \ldots, t_n)$ vanishes everywhere. Now use Lemma 7 to show that $t_i - \lambda$ divides $\widehat{f}$. Since all these divisors of $\widehat{f}$ are relatively prime, we get our result. □

From this we can easily derive the following generalisation of Chevalley-Warning theorem, which we call the **Punctured Chevalley-Warning Theorem**.

Theorem 16. *Let $A_1, \ldots, A_n, B_1, \ldots, B_n$ be non-empty finite subsets of $\mathbb{F}_q$ such that for all i we have $B_i \subseteq A_i$. Put $A := A_1 \times \cdots \times A_n$ and $B := B_1 \times \cdots \times B_n$. Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ such that $(q-1)\sum \deg f_j < \sum(\#A_i - \#B_i)$ and let $Z_A = \{x \in \prod A_i : \forall j \ f_j(x) = 0\}$. If $Z_A \cap B \neq \emptyset$, then $Z_A \cap (A \setminus B) \neq \emptyset$.*

[2] this is *very* similar to Lagrange interpolation

Proof. Let $f = \prod(1 - f_j^{q-1})$. Then we are given that $\deg f = (q-1)\sum \deg f_j < \sum(\#A_i - \#B_i)$. Say $Z_A \cap B \neq \emptyset$ and $Z_A \cap (A \setminus B) = \emptyset$. Then f vanishes everywhere on A, except at some point of B. Therefore, we get the contradiction that $\deg f \geq \sum(\#A_i - \#B_i)$. □

References

[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*. Eur. J. Comb. 14 (1993), 79–83.

[Al99] N. Alon, *Combinatorial Nullstellensatz*. Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7–29.

[BS09] S. Ball and O. Serra, *Punctured combinatorial Nullstellensätze*. Combinatorica 29 (2009), 511–522.

[Br11] D. Brink, *Chevalley's theorem with restricted variables*. Combinatorica 31 (2011), 127–130.

[BS78] A. E. Brouwer and A. Schrijver, *The blocking number of an affine space*. J. Comb. Theory Ser. A 24 (1978), 251-253.

[Ch35] C. Chevalley, *Démonstration dune hypothèse de M. Artin.* Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[Cl14] P. L. Clark, *The Combinatorial Nullstellensatz Revisited*. Electron. J. Combin. 21 (2014), no. 4, Research Paper 15, 16 pp.

[KP12] R. N. Karasev and F. V. Petrov, *Partitions of nonzero elements of a finite field into pairs*, Israel J. Math. 192 (2012), no. 1, 143–156.

[La10] Michal Lason, *A generalization of combinatorial Nullstellensatz*, Electron. J. Combin. 17 (2010), no. 1, Note 32, 6 pp.

[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*. Abh. Math. Sem. Hamburg 11 (1935), 76–83.