Proof of the combinatorial nullstellensatz over integral domains, in the spirit of Kouba

Peter Heinig*

Lehr- und Forschungseinheit M9
für Angewandte Geometrie und Diskrete Mathematik,
Zentrum Mathematik, Technische Universität München,
Boltzmannstraße 3, D-85748 Garching bei München, Germany
heinig@ma.tum.de

Submitted: Jan 4, 2010; Accepted: Feb 11, 2010; Published: Feb 22, 2010
Mathematics Subject Classification 2010: 13G05, 15A06

Abstract

It is shown that by eliminating duality theory of vector spaces from a recent proof of Kouba [A duality based proof of the Combinatorial Nullstellensatz, *Electron. J. Combin.* 16 (2009), #N9] one obtains a direct proof of the nonvanishing-version of Alon's Combinatorial Nullstellensatz for polynomials over an arbitrary integral domain. The proof relies on Cramer's rule and Vandermonde's determinant to explicitly describe a map used by Kouba in terms of cofactors of a certain matrix.

That the Combinatorial Nullstellensatz is true over integral domains is a well-known fact which is already contained in Alon's work and emphasized in recent articles of Michałek and Schauz; the sole purpose of the present note is to point out that not only is it not necessary to invoke duality of vector spaces, but by not doing so one easily obtains a more general result.

1 Introduction

The Combinatorial Nullstellensatz is a very useful theorem (see [1]) about multivariate polynomials over an integral domain which bears some resemblance to the classical Nullstellensatz of Hilbert.

Theorem 1 (Alon, Combinatorial Nullstellensatz, ideal-containment-version, Theorem 1.1 in [1])**.** *Let K be a field, $R \subseteq K$ a subring, $f \in R[x_1, \ldots, x_n]$, $S_1, \ldots, S_n$ arbitrary nonempty subsets of K, and $g_i := \prod_{s \in S_i}(x_i - s)$ for every $1 \leqslant i \leqslant n$. If $f(s_1, \ldots, s_n) = 0$*

[*] The author was supported by a scholarship from the Max Weber-Programm Bayern and by the ENB graduate program TopMath.

for every $(s_1,\ldots,s_n) \in S_1 \times \cdots \times S_n$*, then there exist polynomials* $h_i \in R[x_1,\ldots,x_n]$ *with the property that* $\deg(h_i) \leqslant \deg(f) - \deg(g_i)$ *for every* $1 \leqslant i \leqslant n$*, and* $f = \sum_{i=1}^{n} h_i g_i$.

Theorem 2 (Alon, Combinatorial Nullstellensatz, nonvanishing-version, Theorem 1.2 in [1])**.** *Let* K *be a field,* $R \subseteq K$ *a subring, and* $f \in R[x_1,\ldots,x_n]$*. Let* $c \cdot x_1^{d_1} \cdots x_n^{d_n}$ *be a term in* f *with* $c \neq 0$ *whose degree* $d_1 + \cdots + d_n$ *is maximum among all degrees of terms in* f*. Then every product* $S_1 \times \cdots \times S_n$*, where each* S_i *is an arbitrary finite subset of* R *satisfying* $|S_i| = d_i + 1$*, contains at least one point* $(s_1,\ldots,s_n)$ *with* $f(s_1,\ldots,s_n) \neq 0$.

Three comments are in order. First, talking about subrings of a field is equivalent to talking about integral domains: every subring of a field clearly is an integral domain, and, conversely, every integral domain R is (isomorphic to) a subring of its field of fractions $\mathrm{Quot}(R)$. Second, strictly speaking, rings are mentioned in [1] only in Theorem 1, but Alon's proof in [1] of Theorem 2 is valid for polynomials over integral domains as well. Third, it is intended that the S_i are allowed to be subsets of K in Theorem 1 but required to be subsets of R in Theorem 2, but this is done only for convenience. Theorem 2 is easily seen to be equivalent to the formulation obtained when 'arbitrary finite subset of R' is replaced by 'arbitrary finite subset of K'.

In [1], Theorem 2 was deduced from Theorem 1. In [3], Kouba gave a beautifully simple and direct proof of the nonvanishing-version of the Combinatorial Nullstellensatz, bypassing the use of the ideal-containment-version. Kouba's argument was restricted to the case of polynomials over a field and at one step applied a suitably chosen linear form on the vector space $K[x_1,\ldots,x_n]$ to the given polynomial f in Theorem 2.

However, for Kouba's idea to work, it is not necessary to have recourse to duality theory of vector spaces and in the following section it will be shown how to make Kouba's idea work without it, thus obtaining a direct proof of the full Theorem 2.

Two relevant recent articles ought to be mentioned. A very short direct proof of Theorem 2 was given by Michałek in [5] who explicitly remarks that the proof works for integral domains as well. Moreover, the differences $\left\{ \pm(s - s') : \{s, s'\} \in \binom{S_k}{2} \right\}$ in the proof below play a similar role in Michałek's proof. In [6], Schauz obtained far-reaching generalizations and sharpenings of Theorem 2, expressly working with integral domains and generalizations thereof throughout the paper.

The present author wishes to emphasize that the proof in the present paper differs from Kouba's proof only in the setting and the way in which the coefficients for Kouba's linear form are obtained and he offers the following as its *raison d'être*: Mathematical proofs should be treated as mathematical objects in their own right and Kouba's argument is a mathematical proof which is worth being placed into what the present author feels is its proper generality. In [3], the argument was presented under the heading of vector space duality and with explicit reference to (dual) bases—notions which essentially depend on the ability to uniquely invert the scalar multiplication operation when the scalar ring of a module is a field. Casual readers hence might get away with the impression that Kouba's argument essentially rests on those things. However, the argument emerges unscathed and in greater generality when moved to the setting where the scalar ring is merely assumed to be an integral domain. What is essential in Kouba's proof is commutativity of the scalar ring and absence of zero-divisors (any substantial weakening of these two assumptions seems to require to vary the argument substantially), and it is the purpose of the present note to try to lay bare the basic mechanism of Kouba's proof.

2 Proof of Theorem 2

The proof of the Theorem 2 will be based on the following simple lemma.

Lemma 3. *Let R be an integral domain. Let $\emptyset \neq S = \{s_1, \ldots, s_m\} \subseteq R$ be an arbitrary finite subset. Then there exist elements $\lambda_1^{(S)}, \ldots, \lambda_m^{(S)}$ of R such that*

$$\lambda_1^{(S)} \cdot (1, s_1, s_1^2, \ldots, s_1^{m-1}) + \cdots + \lambda_m^{(S)} \cdot (1, s_m, s_m^2, \ldots, s_m^{m-1}) \\ = (0, 0, 0, \ldots, 0, \prod_{1 \leqslant i < j \leqslant m} (s_i - s_j)). \tag{1}$$

(Note that for $m = 1$ the claim is trivially true with $\lambda_1^{(S)} := 1$ and, as usual, taking the then empty product to be 1.)

Proof. Let $[m] := \{1, \ldots, m\}$. Define b to be the right-hand side of the claimed equation, taken as a column vector, and let $A = (a_{ij})_{(i,j) \in [m]^2}$ be the Vandermonde matrix defined by $a_{ij} := s_j^{i-1}$. Then the statement of the lemma is equivalent to the existence of a solution $\lambda^{(S)} \in R^m$ of the system of linear equations $A\lambda^{(S)} = b$. By the well-known formula for the determinant of a Vandermonde matrix (see [4], Ch. XIII, §4, example after Prop. 4.10), $\det(A) = \prod_{1 \leqslant i < j \leqslant m}(s_i - s_j)$.

Since S is a set, all factors of this product are nonzero, and since R has no zero-divisors, the determinant is therefore nonzero as well. Now let α_{ij} be the cofactors of A, i.e. $\alpha_{ij} := (-1)^{i+j} \det(A^{(ij)})$, where $A^{(ij)}$ is the $(m-1) \times (m-1)$ matrix obtained from A by deleting the i-th row and the j-th column (see [2], Ch. IX, §3, before Lemma 1). By Cramer's rule (which is valid in any commutative ring, see Ch. IX, §3, Theorem 6 in [2] or Ch. XIII, §4, Theorem 4.4 in [4]), for every $j \in [m]$,

$$\det(A) \cdot \lambda_j^{(S)} = \sum_{i=1}^{m} \alpha_{ij} b_i.$$

Using $b_m = \det(A)$, $b_i = 0$ for every $1 \leqslant i < m$, and the commutativity of an integral domain, this reduces to

$$\det(A) \cdot \left(\lambda_j^{(S)} - \alpha_{mj}\right) = 0.$$

Hence, since $\det(A) \neq 0$ and R has no zero-divisors, if follows that the cofactors $\lambda_j^{(S)} = \alpha_{mj} \in R$ provide explicit elements with the desired property. □

Using this lemma, Kouba's argument may now be carried out without change in the setting of integral domains.

Proof of Theorem 2. Let R be an arbitrary integral domain and $f \in R[x_1, \ldots, x_n]$ be an arbitrary polynomial. Let $d_1, \ldots, d_n \geqslant 0$ be the exponents of a term $c \cdot x_1^{d_1} \cdots x_n^{d_n}$ with $c \neq 0$ which has maximum degree in f. For each $k \in [n]$, choose an arbitrary finite subset $S_k \subseteq R$ of size $d_k + 1$ and apply Lemma 3 with $S = S_k$ and $m = |S|$ to obtain a family of elements $(\lambda_{s_k}^{(S_k)})_{s_k \in S_k}$ of R (where in order to avoid double indices the coefficients λ are now being indexed by the elements of S_k directly, not by an enumeration of each S_k) with the property that

$$\sum_{s_k \in S_k} \lambda_{s_k}^{(S_k)} \cdot s_k^{\ell} = 0 \qquad \text{for every } \ell \in \{0, \ldots, d_k - 1\}, \tag{2}$$

$$\sum_{s_k \in S_k} \lambda_{s_k}^{(S_k)} \cdot s_k^{d_k} = \prod_{\{s,s'\} \in \binom{S_k}{2}} (s - s') =: r_k, \tag{3}$$

where $\prod_{\{s,s'\} \in \binom{S_k}{2}} (s - s') = r_k$ is not a well-defined element of R but only defined up to a sign (since $(s - s') = -(s' - s) = (-1) \cdot (s' - s)$ and $(-1) \cdot (-1) = -(-1) = 1$, in every ring), depending on how the elements of S_k are labelled. However, whatever specific labelling one chooses, $r_k \neq 0$ since R does not have zero-divisors. Since the argument below does not make use of anything more specific about r_k than its not being zero, it does not seem to be worthwhile to introduce a labelling of the elements of each S_k.

Now, using the coefficient families $(\lambda_{s_k}^{(S_k)})_{s_k \in S_k}$, define, à la Kouba, the map

$$\begin{aligned} \Phi : \quad R[x_1, \ldots, x_n] &\longrightarrow R \\ g &\longmapsto \sum_{(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n} \lambda_{s_1}^{(S_1)} \cdots \lambda_{s_n}^{(S_n)} \cdot g(s_1, \ldots, s_n). \end{aligned} \tag{4}$$

Due to distributivity of $\cdot$ over $+$ and commutativity of $\cdot$ in an integral domain, Φ is an R-linear form on the R-module $R[x_1, \ldots, x_n]$. In particular, for every polynomial f, the value $\Phi(f)$ can be evaluated termwise as

$$\Phi(f) = \sum_{t \text{ a term in } f} \Phi(t). \tag{5}$$

If $t = c \cdot x_1^{d'_1} \cdots x_n^{d'_n}$ is an arbitrary term in $R[x_1, \ldots, x_n]$, then

$$\begin{aligned} \Phi(t) = c \cdot \Phi(x_1^{d'_1} \cdots x_n^{d'_n}) &= c \cdot \sum_{(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n} \lambda_{s_1}^{(S_1)} \cdots \lambda_{s_n}^{(S_n)} \cdot s_1^{d'_1} \cdots s_n^{d'_n} \\ &= c \cdot \sum_{s_1 \in S_1} \cdots \sum_{s_n \in S_n} \lambda_{s_1}^{(S_1)} \cdots \lambda_{s_n}^{(S_n)} \cdot s_1^{d'_1} \cdots s_n^{d'_n} \\ &= c \cdot \prod_{k=1}^{n} \Bigg(\sum_{s_k \in S_k} \lambda_{s_k}^{(S_k)} s_k^{d'_k} \Bigg), \end{aligned} \tag{6}$$

where in the last step again use has been made of the commutativity of an integral domain. By (6) and (2) it follows that for every term t, if there is at least one exponent d'_i with

$d_i' < d_i$, then $\Phi(t) = 0$. Moreover, by the choice of the term $c \cdot x_1^{d_1} \cdots x_n^{d_n}$, every term $c' \cdot x_1^{d_1'} \cdots x_n^{d_n'}$ of f which is different from the term $c \cdot x_1^{d_1} \cdots x_n^{d_n}$ must, even if it has itself maximum degree in f, contain at least one exponent d_i' with $d_i' < d_i$. Therefore

$$\sum_{(s_1,\ldots,s_n)\in S_1\times\cdots\times S_n} \lambda_{s_1}^{(S_1)} \cdots \lambda_{s_n}^{(S_n)} \cdot f(s_1,\ldots,s_n) \overset{(4)}{=} \Phi(f) \overset{(5),(6),(2)}{=} c \cdot \Phi(x_1^{d_1} \cdots x_n^{d_n}) =$$

$$\overset{(6),(3)}{=} c \cdot \prod_{k=1}^{n} \prod_{\{s,s'\}\in\binom{S_k}{2}} (s - s') = c \cdot \prod_{k=1}^{n} r_k \neq 0, \tag{7}$$

since R has no zero-divisors. Obviously this implies that there exists at least one point $(s_1,\ldots,s_n) \in S_1 \times \cdots \times S_n$ where f does not vanish. □

3 Concluding question

Is there any interesting use for the fact that even in the case of integral domains the coefficients of Kouba's map can be explicitly expressed in terms of cofactors of the matrices (s_j^{i-1})?

Acknowledgements

The author is very grateful to the department M9 of Technische Universität München for excellent working conditions, and to a referee for a remarkably careful report which pointed out quite a few inaccuracies.

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1, 7–29.

[2] G. D. Birkhoff and S. Mac Lane, *Algebra*, 3. ed., American Mathematical Society, 1987.

[3] O. Kouba, *A duality based proof of the Combinatorial Nullstellensatz*, Electron. J. Combin. **16** (2009), #N9.

[4] S. Lang, *Algebra*, 3. ed., Graduate Texts in Mathematics, vol. 211, Springer, 2002.

[5] M. Michałek, *A short proof of Combinatorial Nullstellensatz*, arXiv:0904.4573v1 [math.CO] (2009).

[6] U. Schauz, *Algebraically Solvable Problems: Describing Polynomials as Equivalent to Explicit Solutions*, Electron. J. Combin. **15** (2008), #R10.