המחלקה למתמטיקה, בן-גוריון

אשנב למתמטיקה

ביום שלישי, 8 בדצמבר, 2020

בשעה *16:10 – 17:30*

במרשתת

ההרצאה

העתקות פולינומיאליות ולוגיקה

תינתן על-ידי

מנחם קוג'מן

תקציר: באשנב נדבר על מאמר של Walter Rudin, בו הוא מציע הוכחה קצרה למשפט אקס: העתקה פולינומיאלית חח"ע מהמרוכבים בחזקת n למרוכבים בחזקת n היא על. נציג הוכחה המבוססת על משפט הקומפקטיות מלוגיקה ושלמות של מערכות אקסיומות. תוכלו להחליט בסוף האשנב איזו משתי ההוכחות קצרה יותר, או לא להחליט.

Kronecker expansion is obtained

$$A = \mathbf{block}(\mathbf{A}) = \sum_{k=1}^{K} s_k \, \mathbf{block}\left(\mathbf{v}_k \mathbf{u}_k^T\right) = \sum_{k=1}^{K} s_k U_k \otimes V_k .$$

By (B-2), it is straight-forward to verify the orthogonality of the U_k's and the V_k's.

Remarks. Since the SVD also determines optimal reduced rank approximations, best approximations using a fixed number of Kronecker products can be obtained from this Kronecker expansion. The motivation for this Kronecker expansion or "block" SVD arose in an image-processing application. Illuminating discussions of image processing and applications of the SVD, block matrix computations, and Kronecker products are found in Gonzalez and Wintz [**6**] or Jain [**5**]. An excellent treatment of the Kronecker product is found in Horn and Johnson [**3**]. Further generalizations of the Kronecker product and signal-processing applications are found in [**4**], [**7**], [**2**], [**1**].

REFERENCES

1. Andrews, H. C. and J. Kane, Kronecker Matrices, Computer Implementation, and Generalized Spectra, *Journal of the Association for Computing Machinery*, Volume 17, Number 2, (1970) 260–268.
2. Henderson, Harold V. and S. R. Searle, The Vec-Permutation Matrix, the Vec Operator and Kronecker Products: A Review, *Linear and Multilinear Algebra*, Volume 9 (1981), 271–288.
3. Horn, Roger A. and Charles R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge (1991).
4. Hyland, David C. and Emmanuel G. Collins, Jr., Block Kronecker Products and Block Norm Matrices in Large-Scale Systems Analysis, *SIAM Journal of Matrix Analysis and Applications*, Volume 10, Number 1 (1989) 18–29.
5. Jain, Anil K. *Fundamentals of Digital Image Processing*, Prentice Hall (1989).
6. Gonzalez, Rafael C. and Paul Wintz, *Digital Image Processing*, Addison-Wesley Publishing Company (1977).
7. Regalia, Phillip A. and Sanjuit K. Mitra, Kronecker Products, Unitary Matrices and Signal Processing Applications, *SIAM Review*, Volume 31, Number 4 (1989) 586–613.

NCCOSC RDTE DIV 574
53560 Hull Street
San Diego, CA 92152-5001
allen@nosc.mil

Injective Polynomial Maps Are Automorphisms

Walter Rudin

This article presents a simple elementary proof of the following result.

Theorem A. *If* $F\colon \mathbb{C}^n \to \mathbb{C}^n$ *is a polynomial map which is one-to-one, then*

(a) $F(\mathbb{C}^n) = \mathbb{C}^n$, *and*

(b) $F^{-1}\colon \mathbb{C}^n \to \mathbb{C}^n$ *is also a polynomial map.*

Here n is a positive integer, and $\mathbb{C}^n$ is the set of all $z = (z_1, \ldots, z_n)$, each z_i lying in the complex field $\mathbb{C}$. In general, the notation $\Phi: X \to Y$ indicates that Φ is a map whose domain is X and whose range lies in Y. To say that F is a *polynomial* map means that $F = (f_1, \ldots, f_n)$ and each component f_i of F is a polynomial, mapping $\mathbb{C}^n$ into $\mathbb{C}$.

Theorem A may be regarded as a small step toward a confirmation of the so-called Jacobian conjecture, which claims that if $F: \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial map whose Jacobian is a non-zero constant, then F is a polynomial automorphism of $\mathbb{C}^n$, i.e., F is one-to-one and satisfies (a) and (b). This dates back to 1939 [**5**] but is still unproved (in June 1994), even for $n = 2$. Its history, many references, and some partial results, can be found in [**2**].

Theorem A shows that the Jacobian conjecture would be proved if one could show, for polynomial maps $F: \mathbb{C}^n \to \mathbb{C}^n$, that "locally one-to-one" implies "globally one-to-one." This formulation of the problem points to an interesting difference between $\mathbb{C}^n$ and $\mathbb{R}^n$: Serguey Pinchuk [**8**] has (surprisingly!) constructed a polynomial map $F: \mathbb{R}^2 \to \mathbb{R}^2$ whose Jacobian has no zero in $\mathbb{R}^2$ but which is not one-to-one. The difference is, of course, that on $\mathbb{R}^n$ there are nonconstant polynomials without zeros, whereas this cannot happen on $\mathbb{C}^n$.

Theorem A is not new. In [**7**] Don Newman proved (a) with $\mathbb{R}^2$ in place of $\mathbb{C}^n$. In [**3**] this was extended to $\mathbb{R}^n$, for arbitrary n, with the aid of a good dose of homology theory; that paper also contains a brief sketch of the analogous result for maps from k^n to k^n, for arbitrary algebraically closed fields k. Ax [**1**; Th. 2] extended this to morphisms of algebraic varieties, using nonprincipal ultraproducts of fields. Theorem (2.1) on p. 294 of [**2**] lists eight (mostly algebraic) conditions on polynomial maps F that are equivalent; Theorem A is one of those equivalences: F is one-to-one if and only if F is an automorphism.

I believe that the proof given here is much simpler than any of the above. (Proof: I have no trouble understanding it.) It uses two facts from complex analysis:

Fact 1. *If* (i) $u, v: \mathbb{C}^n \to \mathbb{C}$ *are polynomials with no common factor of positive degree*,

(ii) Ω *is an open subset of* $\mathbb{C}^n$, *and*

(iii) $v(p_0) = 0$ *at some point* p_0 *in* Ω,

then Ω *contains points* p *at which* $v(p) = 0$ *but* $u(p) \neq 0$.

This must be prehistoric. A proof can be found on pp. 14, 15 of [**11**]. Note that it fails on $\mathbb{R}^n$.

Example: $u(x, y) = x^2 + y^2$, $v(x, y) = x^2 + (y - x)^2$.

Fact 2. *If F satisfies the hypothesis of Theorem A, then the Jacobian of F is* $\neq 0$ *at every point of* $\mathbb{C}^n$.

This is in fact true for holomorphic maps from open sets in $\mathbb{C}^n$ into $\mathbb{C}^n$ that are locally one-to-one, and it used to be a fairly difficult theorem (see, for instance, [**6**; pp. 86–88]) until Jean-Pierre Rosay published a truly simple proof [**9**].

Combined with the inverse function theorem (Th. 9.24 in [**10**]), Fact 2 implies what will actually be used, namely:

The range $F(\mathbb{C}^n)$ *of F is an open subset of* $\mathbb{C}^n$.

(Remark: That $F(\mathbb{C}^n)$ is open is also an immediate consequence of Brouwer's "Invariance of Domain" theorem, concerning continuous one-to-one maps from $\mathbb{R}^N$ into $\mathbb{R}^N$ [**4**; p. 95] but that theorem is much more difficult than the route via Fact 2.)

We now start the proof.

Let $f_1, \ldots, f_n$ be the components of F, and let k be the subfield of $\mathbb{C}$ generated by the coefficients of the polynomials f_i. Since k is countable, there are only countably many polynomials with coefficients in k. The union of their zero-sets (ignoring the zero-polynomial) is thus a countable union of closed sets without interior, hence cannot cover the complete metric space $\mathbb{C}^n$. It follows that there is a point ξ in $\mathbb{C}^n$, fixed from now on, with the following property:

(∗) *If $f\colon \mathbb{C}^n \to \mathbb{C}$ is a polynomial with coefficients in k, and $f(\xi) = 0$, then $f(z) = 0$ for every z in $\mathbb{C}^n$.*

Put $\eta = F(\xi)$.

Claim. *The extension fields*

$$k(\eta) = k(\eta_1, \ldots, \eta_n)$$

and

$$k(\eta, \xi) = k(\eta_1, \ldots, \eta_n, \xi_1, \ldots, \xi_n)$$

are equal.

Here $k(\eta)$ is the smallest subfield of $\mathbb{C}$ that contains k and $\eta_1, \ldots, \eta_n$, and similarly for $k(\eta, \xi)$.

If the claim is false, there is an isomorphism φ of $k(\eta, \xi)$ into $\mathbb{C}$ that fixes every element of $k(\eta)$ but moves some ξ_i. (See the lemma at the end of the paper.) Put

$$\omega = (\varphi(\xi_1), \ldots, \varphi(\xi_n))$$

and note that $\omega \neq \xi$.

Since $f_j(\xi) = \eta_j$ is in $k(\eta)$ and the coefficients of f_j are in k, we have, for $1 \le j \le n$,

$$f_j(\xi) = \varphi(f_j(\xi_1, \ldots, \xi_n)) = f_j(\varphi(\xi_1), \ldots, \varphi(\xi_n)) = f_j(\omega).$$

Hence $F(\xi) = F(\omega)$, which contradicts the assumption that F is one-to-one. This proves the claim.

In particular, each ξ_j is in $k(\eta)$. This means that there are polynomials u_j, v_j, with coefficients in k, and without common factors of positive degree, such that $v_j(\eta) \neq 0$ and

$$\xi_j = u_j(\eta)/v_j(\eta) \qquad (1 \le j \le n). \tag{1}$$

Thus $\xi_j v_j(F(\xi)) - u_j(F(\xi)) = 0$. Property (∗) implies now that

$$z_j v_j(F(z)) = u_j(F(z)) \qquad (1 \le j \le n,\ z \in \mathbb{C}^n). \tag{2}$$

Put $\Omega = F(\mathbb{C}^n)$. We saw, as a consequence of Fact 2, that Ω is open. If v_j had a zero in Ω, Fact 1 would imply that there is a point in Ω where $v_j = 0$ but $u_j \neq 0$, contradicting (2).

Hence $v_j \circ F : \mathbb{C}^n \to \mathbb{C}$ is a polynomial without zeros, hence is constant, hence each v_j is constant. Without loss of generality, $v_j = 1$. Putting

$$G = (u_1, \dots, u_n), \tag{3}$$

(2) becomes

$$G(F(z)) = z \quad \text{for all } z \text{ in } \mathbb{C}^n. \tag{4}$$

Hence $F(G(F(z))) = F(z)$. This says that $F \circ G$ is the identity map on Ω. If two polynomials agree on Ω, they agree on $\mathbb{C}^n$. Thus

$$F(G(w)) = w \quad \text{for all } w \text{ in } \mathbb{C}^n. \tag{5}$$

The theorem follows from (4) and (5), with $F^{-1} = G$.

Lemma. *Suppose that $\mathscr{F}$ is a subfield of $\mathbb{C}$, $\xi_1, \dots, \xi_m$ are in $\mathbb{C}$, and $\mathscr{F}_1 = \mathscr{F}(\xi_1, \dots, \xi_m)$. Then either $\mathscr{F}_1 = \mathscr{F}$, or there is an isomorphism φ of $\mathscr{F}_1$ into $\mathbb{C}$ that fixes every element of $\mathscr{F}$ but moves at least one ξ_i.*

Proof: Assume $\mathscr{F}_1 \neq \mathscr{F}$. Then there is a nonempty subset of $\{\xi_1, \dots, \xi_m\}$, say $(\xi_1, \dots, \xi_j)$ (after reordering) that is minimal with respect to the property

$$\mathscr{F}_1 = \mathscr{F}(\xi_1, \dots, \xi_j).$$

Put $\mathscr{F}_2 = \mathscr{F}(\xi_1, \dots, \xi_{j-1})$. (This is $\mathscr{F}$ when $j = 1$.) Then

$$\mathscr{F} \subset \mathscr{F}_2 \subsetneqq \mathscr{F}_2(\xi_j) = \mathscr{F}_1.$$

Let φ fix every element of $\mathscr{F}_2$ and choose $\varphi(\xi_j)$ as follows:

If ξ_j is transcendental over $\mathscr{F}_2$, let $\varphi(\xi_j)$ be any complex number $\neq \xi_j$ that is also transcendental over $\mathscr{F}_2$ (such as $1 + \xi_j$).

If ξ_j is algebraic over $\mathscr{F}_2$, with minimal polynomial $p(x)$, let $\varphi(\xi_j)$ be another root of $p(x)$.

To every w in $\mathscr{F}_1$ corresponds a rational function r, with coefficients in $\mathscr{F}_2$, such that $w = r(\xi_j)$. Setting $\varphi(w) = r(\varphi(\xi_j))$ gives the desired isomorphism.

REFERENCES

1. J. Ax, A metamathematical approach to some problems in number theory, *Proc. Symp. Pure Math.* vol. 20, (1969), AMS (1971), pp. 161–190.
2. H. Bass, E. J. Connell, D. Wright, The Jacobian conjecture: Reduction of degree and formal expansion of the inverse, *Bull. AMS* 7 (1982), pp. 287–330.
3. A. Bialynicki-Birula and M. Rosenlicht, Injective morphisms of real algebraic varieties, *Proc. AMS* 13 (1962), pp. 200–203.
4. W. Hurewicz and H. Wallman, *Dimension Theory*, Princeton Univ. Press, 1948.
5. O. H. Keller, Ganze Cremona-Transformationen, *Monats. Math. Physik* 47 (1939), pp. 299–306.
6. R. Narasimhan, *Several Complex Variables*, Univ. of Chicago Press, 1971.
7. D. J. Newman, One-one polynomial maps, *Proc. AMS* 11 (1960), pp. 867–870.
8. S. Pinchuk, A counterexample to the real Jacobian conjecture, Preprint, May 1994.
9. J.-P. Rosay, Injective holomorphic mappings, *Amer. Math. Monthly*, 89 (1982), pp. 587–588.
10. W. Rudin, *Principles of Mathematical Analysis*, 3rd Ed., McGraw-Hill, 1976.
11. W. Rudin, *Function Theory in Polydiscs*, Benjamin, 1969.

Department of Mathematics
University of Wisconsin-Madison
Madison, WI 53706-1388