ABOUT HERMAN AUERBACH'S PROBLEM ON FACTORS OF REAL POLYNOMIALS WITH CONNECTED ZERO SET COMPLEMENT

J. MAURICE ROJAS

In memory of Herman Auerbach, 26 October 1901 – 17 August 1942.

1. Introduction. Between September 4 and November 6 in 1936 Herman Auerbach posed...

Problem #148. *Let $P(x_1,\ldots,x_n)$ denote a polynomial with real coefficients. Consider the set of points defined by the equation $P(x_1,\ldots,x_n)=0$. A necessary and sufficient condition for this set not to cut the Euclidean (real) space is: All the irreducible factors of the polynomial P in the real domain should be always nonnegative or always nonpositive.*

We will interpret "not to cut" to mean that the real zero set of P has (non-empty) path-connected complement. We are unaware of any published solution to Problem #148 so we provide a self-contained solution below, using a reduction to...

Lemma 1.1. *If $Q\in\mathbb{R}[x_1,x_2]$ and each irreducible factor of Q (in $\mathbb{R}[x_1,x_2]$) is either always nonnegative on $\mathbb{R}^2$ or always nonpositive on $\mathbb{R}^2$ then the complement of the real zero set of Q is path-connected.*

The example $(x_1-x_2)^2$ shows the necessity of the sign condition on the irreducible factors.

2. From Auerbach's Problem to Recent Research. Problem #148 naturally leads to important recent advances in parts of algorithmic algebraic geometry: polynomial factorization and nonnegativity.

Algorithms that are practical and efficient (as of early 2015) for multivariate polynomial factorization over $\mathbb{C}$ are detailed in [Gao03, CL07]. Algorithms that take numerical instability into account (in the coefficients and/or the final answer) appear in [SVW04, Che04, GKMYZ04, KMYZ08, Zen09]. Definitive references for background on algebraic sets (over $\mathbb{R}$ and/or $\mathbb{C}$), and algorithms for determining their topological structure, include [BCR98, SW05, BPR10].

For an arbitrary $f\in\mathbb{R}[x_1]$ with degree D and exactly t monomial terms, all general algorithms for factorization over $\mathbb{R}$ have complexity super-linear in the degree D. However, since such an f has at most $2t-1$ real roots (thanks to Descartes' Rule) one can ask for faster algorithms to just count, say, the degree 1 factors when t is fixed. Such algorithms, with complexity polynomial in $\log D$ (and the total bit size of all the coefficients when $f\in\mathbb{Z}[x_1]$), appear in [BRS09, BHPR11] (counting bit operations, for $t\leq 4$) and [Sag14] (counting field operations, for any fixed t). Deciding the existence of a real root for $f\in\mathbb{Z}[x_1]$ (with coefficients of modulus at most 2^h) using just $(t+h+\log D)^{O(1)}$ bit operations remains an open problem.

For $f\in\mathbb{Z}[x_1,x_2]$, deciding whether an input degree 1 polynomial divides f can be done using just $(t+h+\log D)^{O(1)}$ operations [Ave09]. Grenet has recently found similar complexity bounds for finding bounded degree factors of multivariate sparse polynomials over arbitrary number fields [Gre15]. A deeper discussion of the role of sparsity in real analytic geometry can be found in [Kho91] and a remarkable connection between real roots of structured univariate polynomials and the **P** vs. **NP** problem can be found in [KPT15].

While nonnegative univariate polynomials are always sums of squares of polynomials, Theodore Motzkin observed in 1967, via the concrete example $x_1^4x_2^2+x_1^2x_2^4-3x_1^2x_2^2+1$, that this equivalence fails for multivariate polynomials. The relationship between nonnegativity

Date: April 3, 2015.

Key words and phrases. exponential sum, amoeba, Hausdorff distance, tropical variety, complexity, metric.

Partially supported by NSF grant CCF-1409020.

and sums of squares was advanced by Hilbert and Artin and, more recently, quantitative estimates have been derived for how often nonnegative polynomials are sums of squares of polynomials. Such estimates are important because, when a polynomial is a sum of squares, its minimum can be found efficiently via semi-definite programming. This beautiful intersection of optimization, real algebraic geometry, and convexity is detailed in [BPT12] and the references therein.

3. Reducing Auerbach's Problem to a Simplified Bivariate Case.

Our key reduction to Lemma 1.1 hinges on the following fact:

Lemma 3.2. *(Special case of* [Sch00, Thm. 17, Pg. 75, Sec. 1.9]*) Suppose $x_1,\ldots,x_n,w_1,\ldots,w_{n-1}$, $y_1,\ldots,y_{n-1}$ are algebraically independent indeterminates and $P\in\mathbb{R}[x_1,\ldots,x_n]\setminus\mathbb{R}[x_1]$ is irreducible in $\mathbb{R}[x_1,\ldots,x_n]$. Then there is a polynomial $\Phi\in\mathbb{R}[w_1,\ldots,w_{n-1},y_1,\ldots,y_{n-1}]\setminus\{0\}$ with the following property: If $\alpha_2,\beta_2,\ldots,\alpha_n,\beta_n\in\mathbb{R}$ and $\Phi(\alpha_2,\ldots,\alpha_n,\beta_2,\ldots,\beta_n)\neq 0$ then $P(x_1,\alpha_2x_2+\beta_2,\ldots,\alpha_nx_2+\beta_n)$ is irreducible in $\mathbb{R}[x_1,x_2]$.* ■

Lemma 3.2 is due to Schinzel, extends to arbitrary fields, and refines a 1931 result of Franz [Fra31]. Variations of Lemma 3.2 date back work of Hilbert [Hil92] and have been used in numerous factorization algorithms since the 1980s (see, e.g., [Kal85]) to reduce general multivariate factorization problems to bivariate factorization.

Solution to Problem #148: The case $n=1$ follows immediately upon observing that, up to real affine transformations, the only irreducible non-constant polynomials in $\mathbb{R}[x_1]$ are x_1 and x_1^2+1. So assume $n\geq 2$ and let Z be the zero set of P in $\mathbb{R}^n$.
(Sufficiency): Suppose each irreducible factor of P is either always nonnegative on $\mathbb{R}^n$ or always nonpositive on $\mathbb{R}^n$. Let $u=(u_1,\ldots,u_n)$ and $v=(v_1,\ldots,v_n)$ lie in $\mathbb{R}^n\setminus Z$. Since Z is closed, u (resp. v) in fact lies in an open neighborhood U (resp. V) of points contained in the same connected component of $\mathbb{R}^n\setminus Z$ as u (resp. v). Since the complement of any real algebraic hypersurface is open, Lemma 3.2 implies we can find $\alpha_2,\beta_2,\ldots,\alpha_n,\beta_n$ such that the specialization $Q(x_1,x_2):=P(x_1,\alpha_2x_2+\beta_2,\ldots,\alpha_nx_2+\beta_n)$ satisfies: (a) each irreducible factor P_i of P specializes to an irreducible factor Q_i of Q and (b) P_i is nonnegative on all of $\mathbb{R}^n$ (resp. nonpositive on all of $\mathbb{R}^n$) if and only if Q_i is nonnegative on all of $\mathbb{R}^2$ (resp. nonpositive on all of $\mathbb{R}^2$). In particular, the condition $\Phi\neq 0$ from Lemma 3.2 enables us to pick $(\beta_2,\ldots,\beta_n)$ arbitrarily close to $(u_2,\ldots,u_n)$, and $(\alpha_2,\ldots,\alpha_n)$ arbitrarily close to $(v_2-u_2,\ldots,v_n-u_n)$, so that both $Q(u_1,0)$ and $Q(v_1,1)$ are nonzero.

Let W denote the zero set of Q in $\mathbb{R}^2$ and note that

$$H:=\{(x_1,\alpha_2x_2+\beta_2,\ldots,\alpha_nx_2+\beta_n)\}_{(x_1,x_2)\in\mathbb{R}^2}\subset\mathbb{R}^n$$

is a real 2-plane with the pair $(H,H\cap Z)$ affinely equivalent to $(\mathbb{R}^2,W)$. By Lemma 1.1 (and Conditions (a) and (b)), $\mathbb{R}^2\setminus W$ is path-connected, and thus $H\setminus Z$ is path-connected. Moreover, by our choice of the α_i and β_i, both U and V intersect $H\setminus Z$. So U and V, and thus u and v, are connected by a path in $\mathbb{R}^n\setminus Z$. ■
(Necessity): Suppose now that $\mathbb{R}^n\setminus Z$ is path-connected, but P has an irreducible factor P_i attaining both positive and negative values on $\mathbb{R}^n$. Then P_i must be positive (resp. negative) at some point u_+ (resp. u_-) in $\mathbb{R}^n\setminus Z$ since $\mathbb{R}^n\setminus Z$ is open. By assumption, there is a path in $\gamma:[0,1]\longrightarrow\mathbb{R}^n\setminus Z$ connecting u_+ and u_-. In particular, $P_i(\gamma(0))P_i(\gamma(1))<0$, so by the Intermediate Value Theorem, $P_i(\gamma(s))=0$ for some $s\in(0,1)$. In other words, $\gamma([0,1])$ intersects Z, which is a contradiction. ■

One can give a much shorter solution to Auerbach's Problem, applying to arbitrary real-closed fields as well: Combine a higher-dimensional version of Proposition 3.3 below with [BCR98, Thm. 4.5.1]. The latter result, on real principal ideals, dates back to [DE70].

Under Auerbach's sign condition on irreducible factors, our solution leads to the following construction for a path connecting any distinct $u, v \in \mathbb{R}^n \setminus Z$: Pick a random $w \in \mathbb{R}^n$ and let Γ be the path obtained by joining the line segments $\overline{uw}$ and $\overline{wv}$. Then Γ lies in $\mathbb{R}^n \setminus Z$ with probability 1 (with respect to any bounded, continuous positive probability measure) or high probability (with respect to the uniform measure on $\{-N, \ldots, N\}^n$ for N sufficiently large). This can be made precise by observing that the polynomial Φ from Lemma 3.2 has degree $O(d^2)$ (see, e.g., [Lec07, Thm. 6]).

To prove Lemma 1.1 we will apply the following two facts:

Proposition 3.3. *If $X \subset \mathbb{R}^2$ is finite then $\mathbb{R}^2 \setminus X$ is path connected. Moreover, we can connect any two points of $\mathbb{R}^2 \setminus X$ with a smooth quadric curve $\Gamma \subset \mathbb{R}^2 \setminus X$.* ■

Lemma 3.4. *Suppose $f, g \in \mathbb{C}[x_1, x_2]$ have respective degrees d and e, and no common factor of positive degree. Then $f = g = 0$ has no more than de solutions in $\mathbb{C}^2$.* ■

Proposition 3.3 follows easily by using an invertible affine map to reduce to the special case of connecting $(0, 0)$ and $(1, 0)$ via the graph of $cx_1(1 - x_1)$ for suitable c: The finiteness of X guarantees that all but finitely many c will work. Lemma 3.4 is a special case of Bézout's Theorem (see, e.g., [Sha94]) but can also be easily derived from the basic properties of the univariate resultant (see, e.g., [Sch00, App. B]).

Proof of Lemma 1.1: Let W denote the real zero set of Q in $\mathbb{R}^2$. By Proposition 3.3 it clearly suffices to prove that, under the hypotheses of Lemma 1.1, W is finite. It clearly suffices to restrict to the special case where Q is non-constant and irreducible in $\mathbb{R}[x_1, x_2]$. Note also that the irreducibility of Q and the assumption on the sign of Q are invariant under composition with any invertible real affine map.

Consider now any root $\zeta = (\zeta_1, \zeta_2) \in \mathbb{R}^2$ of Q. If $\delta := \left(\frac{\partial Q}{\partial x_1}(\zeta), \frac{\partial Q}{\partial x_2}(\zeta)\right) \neq 0$ then, by composing with a suitable invertible real affine map, we may assume $\delta = (1, 0)$. In particular, by Taylor expansion, we see that Q changes sign in a non-empty horizontal line segment containing ζ. Therefore, *every* root of ζ of Q must satisfy $\frac{\partial Q}{\partial x_1}(\zeta) = \frac{\partial Q}{\partial x_2}(\zeta) = 0$.

Let $Q_1 \cdots Q_r$ be the factorization of Q over $\mathbb{C}[x_1, x_2]$ into factors of positive degree, irreducible in $\mathbb{C}[x_1, x_2]$. The Galois group $G := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ has order 2, is generated by complex conjugation $\overline{(\cdot)}$, and acts naturally on the Q_i. In particular, G acts trivially on Q_i if and only if $Q_i \in \mathbb{R}[x_1, x_2]$. So r must be even when $r \geq 2$, since Q is irreducible over $\mathbb{R}[x_1, x_2]$. Furthermore, $r \leq 2$ since $Q_i \bar{Q}_i$ is invariant under complex conjugation. So we either have $r = 1$ (with Q irreducible over $\mathbb{C}[x_1, x_2]$) or $r = 2$ (with $\bar{Q}_1 \neq Q_1 = \bar{Q}_2 \neq Q_2$). A simple calculation then shows that, in either case, $\frac{\partial Q}{\partial x_1}$ has no common factors with Q. So W is finite by Lemma 3.4. ■

Acknowledgements I am grateful to Dan Mauldin for his invitation to write this brief commentary and Joe Buhler for bringing Auerbach's problem to my attention. I also thank Zbigniew Szafraniec, Michel Coste, and Marie-Francoise Roy for pointing out [BCR98, Thm. 4.5.1]; and Guillaume Chèze and Erich Kaltofen for help with tracking down references to the fastest current factoring algorithms.

References

[Ave09] Avendaño, Martín, *"The number of roots of a lacunary bivariate polynomial on a line,"* J. Symb. Comp. **44** (2009), pp. 1280–1284.

[BHPR11] Bastani, Osbert; Hillar, Chris; Popov, Dimitar; and Rojas, J. Maurice, *"Randomization, Sums of Squares, and Faster Real Root Counting for Tetranomials and Beyond,"* Randomization, Relaxation, and Complexity in Polynomial Equation Solving, Contemporary Mathematics, vol. 556, pp. 145–166, AMS Press, 2011.

[BPR10] Basu, Saugata; Pollack, Ricky; and Roy, Marie-Françoise, *Algorithms in Real Algebraic Geometry,* Algorithms and Computation in Mathematics (Book 10), Spring-Verlag, 2010.

[BRS09] Bihan, Frederic; Rojas, J. Maurice; Stella, Case E., *"Faster Real Feasibility via Circuit Discriminants,"* proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC 2009, July 28–31, Seoul, Korea), pp. 39–46, ACM Press, 2009.

[BPT12] Blekherman, Grigoriy; Parrilo, Pablo A.; and Thomas, Rekha R., *"Semidefinite Optimization and Convex Algebraic Geometry,"* MPS-SIAM series on optimization, book 13, SIAM, 2012.

[BCR98] Bochnak, Jarek; Coste, Mihcel; Roy, Marie-Françoise, *Real Algebraic Geometry,* Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 36, Springer-Verlag, 1998.

[Che04] Chèze, Guillaume, *"Absolute polynomial factorization in two variables and the knapsack problem,"* in proceedings of ISSAC 2004, pp. 87–94, ACM, New York, 2004.

[CL07] Chèze, Guillaume and Lecerf, Grégoire, *"Lifting and recombination techniques for absolute factorization,"* J. Complexity, **23**, no. 3, pp. 380–420, 2007.

[DE70] Dubois, D. W. and Efroymson, G., *"Algebraic theory of real varieties I,"* Studies and Essays (Presented to Yu-Why Chen on his 60th Birthday, April 1, 1970), pp. 107–135, Math. Res. Center, Nat. Taiwan Univ., Taipei.

[Fra31] Franz, W., *"Untersuchungen zum Hilbertschen Irreduzibilitätssatz,"* Math. Z., **33**, pp. 275–293.

[Gao03] Gao, Shuhong, *"Factoring multivariate polynomials via partial differential equations,"* Math. Comp., **72**, no. 242, pp. 801–822, 2003.

[GKMYZ04] Gao, Shuhong; Kaltofen, Erich; May, John P.; Yang, Zhengfeng; and Zhi, Lihong, *"Approximate factorization of multivariate polynomials via differential equations,"* in proceedings of ISSAC 2004, pp. 167–174, ACM, New York, 2004.

[Gre15] Grenet, Bruno, *"Bounded-degree factors of lacunary multivariate polynomials,"* Math ArXiV preprint `http://arxiv.org/abs/1412.3570` . Submitted for publication.

[Hil92] Hilbert, David, *"Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten,"* J. Reine Angew. Math. 110, 1892.

[Kal85] Kaltofen, Erich, *"Effective Hilbert irreducibility,"* Inform. Control 66 (3), pp. 123–137, 1985.

[KMYZ08] Kaltofen, Erich; May, John; Yang, Zhengfeng; and Zhi, Lihong, *"Approximate Factorization of Multivariate Polynomials Using Singular Value Decomposition,"* J. Symb. Compu., **43**, no. 5, pp. 359–376, 2008.

[Kho91] Khovanskiĭ, Askold G., *Fewnomials,* AMS Press, Providence, Rhode Island, 1991.

[KPT15] Koiran, Pascal; Portier, Natacha; and Tavenas, Sebastien, *"A Wronskian approach to the real τ-conjecture,"* J. Symb. Comp., 68(2):195–214, 2015.

[Lec07] Lecerf, Grégoire, *"Improved dense multivariate polynomial factorization algorithms,"* J. Symb. Comp. **42** (2007), pp. 477–494.

[Sag14] Sagraloff, Michael, *"A near-optimal algorithm for computing real roots of sparse polynomials,"* in proceedings of ISSAC 2014, pp. 359–366, ACM, 2014.

[Sch00] Schinzel, Andrzej, *Polynomials with Special Regard to Reducibility,* Encyclopedia of Mathematics and its Applications, Book 77, Cambridge University Press, 2000.

[Sha94] Shafarevich, Igor R., *Basic Algebraic Geometry I,* second edition, Springer-Verlag (1994).

[SVW04] Sommese, Andrew J.; Verschelde, Jan; Wampler, Charles W., *"Numerical factorization of multivariate complex polynomials,"* Theoretical Comput. Sci., **315**, no. 2–3, pp. 651–669, 2004.

[SW05] Sommese, Andrew J. and Wampler, Charles, *Numerical solution of polynomial systems arising in engineering and science,* World Scientific Press, 2005.

[Zen09] Zeng, Zhonggang, *"The approximate irreducible factorization of a univariate polynomial. Revisited,"* in proceedings of ISSAC 2009, pp. 367–374, ACM, New York, 2009.

Department of Mathematics, Texas A&M University TAMU 3368, College Station, Texas 77843-3368, USA.
E-mail address: rojas@math.tamu.edu