ARE THERE FIELD DEPENDENT FORMULAS FOR THE ROOTS TO POLYNOMIALS?

Robert Cacioppo

Northeast Missouri State University

Some four thousand years ago the Babylonians knew how to find roots to polynomials of degree two such as $x^2 - bx + 1$, which they recognized as the solution to the following problem: given $b > 0$, find a number which when added to its reciprocal gives b. The technique they used was completing the square. But several millenia would pass before an algebraic formula for the roots to the general polynomial of degree three would be found. In the intervening time, the Greeks, Arabs, and Hindus made contributions to the study of the quadratic and cubic equations. One hinderance was their reluctance to recognize negative, much less complex, roots as important. Euclid's geometrical solutions to the quadratic naturally placed emphasis on positive roots. The Arabs in the ninth century followed in the Greek tradition and solved certain types of cubic equations using intersecting conics. The Hindus of the twelfth century had begun to accept the role of negative numbers but not their square roots.

When the Europeans of the Renaissance began studying equations again, they remained encumbered by their lack of notation for powers and roots as well as their suspicion of quantities negative or complex. Descartes (1596–1650) verbalized the general feeling when he called the radicals of negatives imaginary. Nonetheless, in the sixteenth century Tartaglia, Cardan, and Ferrari succeeded in finding formulas for the roots to the general cubic and quartic equations. Even then, it was suspected that no such formulas could exist for the general polynomial of degree n, $n \geq 5$, but without justification despite the later efforts of mathematicians such as Ruffini, Euler, Lagrange, Gauss, and Cauchy. By the early part of the nineteenth century algebra had progressed far enough through the efforts of these men for Abel to show that this was indeed the case. A few years later Galois' pioneering work put the problem and its solution in what may be called a modern perspective [4].

We begin by examining the roots to the polynomial

$$p_n(x) = x^n + t_1 x^{n-1} + t_2 x^{n-2} + \cdots + t_{n-1}x + t_n \in P(\vec{t})[x]$$

where P is a prime subfield and $\vec{t}$ denotes the indeterminates $t_1, t_2, \ldots, t_n$ which, without loss of generality, we can assume to be algebraically independent over P (for an explanation of other notation and a reference for results mentioned here without proof, see [2]). For any characteristic, this polynomial has n distinct roots, which we denote by $u_1, u_2, \ldots, u_n$ (Appendix A). For $n = 2, 3$, or 4, the roots to $p_n(x)$ provide the usual formulas for quadratic, cubic, or quartic polynomials, respectively. They give all roots for all n^{th} degree polynomials ($n = 2, 3$, or 4) with coefficients from any field K for which char $K > n$ (Appendix B). For example, the roots to $x^3 + a_1x^2 + a_2x + a_3$ are given by the following formulas $u_1(\vec{t})$, $u_2(\vec{t})$, and $u_3(\vec{t})$ after substituting a_i for t_i, $i = 1, 2, 3$.

$$\begin{array}{lll} u_1 = P + Q - t_1/3, & P = [-q/2 + (p^3/27 + q^2/4)^{1/2}]^{1/3}, & p = t_2 - t_1^2/3 \\ u_2 = \omega P + \omega^2 Q - t_1/3, & Q = [-q/2 - (p^3/27 + q^2/4)^{1/2}]^{1/3}, & q = 2t_1^3/27 - t_1t_2/3 + t_3 \\ u_3 = \omega^2 P + \omega Q - t_1/3, & \omega = -1/2 + \sqrt{-1}\sqrt{3}/2 & \end{array}$$

Definition 1. A K–formula ϕ_n is an expression which gives a root to all polynomials of degree n with coefficients from a field K and which involves the indeterminates $t_1, t_2, \ldots, t_n$ (into which the coefficients of a particular polynomial are placed), a finite subset of K, and a finite number of field operations and extractions of roots (in particular, roots of unity may be used).

One could be more liberal in defining 'formula'; Hermite did this when he expressed the roots to the general polynomial of degree 5 in terms of elliptic modular functions [3]. But if we are to use only field–theoretic descriptions for formulas (that is, first order expressions in the language of rings) then we must use, as K–formulas, elements from the algebraic closure of $K(\vec{t})$. Furthermore, if the substitutions $t_i \mapsto a_i \in K$ are to be well–defined then the elements must also be in a radical extension of $K(\vec{t})$ (Appendix E). So we are led back to Definition 1.

Why do we allow a formula to use a finite subset of K rather than restricting this subset to be from K's prime subfield P? After all, the quadratic, cubic, and quartic formulas only use elements from the prime subfield. One reason, as we will see, is that the two approaches are equivalent if K is infinite. But more importantly, this 'field specific' definition only requires the formula to work for polynomials from $K[x]$. Of course, the usual formulas for polynomials of degree less than five are not field dependent in this manner. They are examples of our next definition.

Definition 2. A formula is universal if it is a K–formula for every field K of a given characteristic.

We can always assume that the indeterminates in a (universal) formula have been chosen to be algebraically independent over the particular field to which it is being applied. Generally we will use $t_1, \ldots, t_n$ for these indeterminates. However, for a field of the form $K(\vec{t})$ we will take $x_1, \ldots, x_n$ to be the (algebraically independent) indeterminates.

Since a universal formula ϕ_n (for $\mathrm{char}\, P$) is valid for the field $P(\vec{t})$, replacing x_i by t_i in ϕ_n yields a root to $p_n(x) \in P(\vec{t})[x]$. As a universal formula, ϕ_n can only involve a subset of P (not $P(\vec{t})$). So this root to $p_n(x)$ is the universal formula ϕ_n, only expressed in the indeterminates t_i rather than the x_i. Thus, the roots to $p_n(x)$ provide the only possible universal formulas.

Conversely, these roots will be universal formulas if and only if they lie within a radical extension of $P(\vec{t})$ and are well–defined under any substitution $\vec{t} \mapsto \vec{a}$ (Appendix B). This condition insures that the roots can be expressed in the form which we require of formulas in general (Definition 1).

To determine when universal formulas exist, then, is to first determine when the roots to $p_n(x)$ are contained in some radical extension of $P(\vec{t})$; that is, when $p_n(x)$ is solvable by radicals over $P(\vec{t})$. Noting that $p_n(x) \in P(\vec{t})[x]$ is irreducible (Appendix A) and recalling that the normal closure of a radical extension of a field is again a radical extension of that field, it follows that if one root of $p_n(x)$ yields a universal formula then each of the other roots to $p_n(x)$ must as well.

If there exist n K–formulas, yielding all the roots to all the polynomials over K of degree n, then, by definition, each such root must lie within some radical extension of K. Thus, the simplest instance in which one can determine that there does not exist a K–formula ϕ_n is if there exists a specific polynomial $f(x) \in K[x]$ of degree n with a root which is not in any radical extension of K. This is fairly common when K is the field of rational numbers and $n \geq 5$; e.g. $x^5 - 6x + 3$ (this occurs because the polynomial's Galois group over Q is not solvable [2]).

But this is not the only situation in which a K–formula does not exist. All of the roots to polynomials with real coefficients lie within a single radical extension of the reals since

$C = R(i)$ is an algebraically closed radical extension of the reals (thus, any polynomial's Galois group over R is solvable). For instance, even though the roots to $x^5 - 6x + 3$ can be written in terms of field operations and radicals over R, they cannot be the result of using some universal formulas for the roots to 5^{th} degree polynomials over fields of characteristic zero; just consider the example given in the previous paragraph. The reason why there are no R–formulas for the roots to 5^{th} degree polynomials is that any such formula would necessarily be universal, as we shall see. Of course, if there are no R–formulas for 5^{th} degree polynomials then there cannot be R–formulas for n^{th} degree polynomials for any $n > 5$ (otherwise we could multiply by a power of x and solve the $n = 5$ case).

Galois theory tells us precisely when the roots to $p_n(x)$ will be K–formulas (hence, universal formulas). It is based on the following two results.

(1) $p_n(x)$ is solvable by radicals over $K(\vec{t})$ implies that its Galois group $Aut_{K(\vec{t})}K(\vec{u})$ is solvable (the converse is true if either char $K = 0$ or char $K > n$).

(2) $Aut_{K(\vec{t})}K(\vec{u}) \cong S_n$, hence is solvable if and only if $n \leq 4$.

Hence, if a root to $p_n(x)$ is a (universal) formula then $n \leq 4$. Conversely, for $n \leq 4$ and either char $K = 0$ or char $K > n$ then these roots provide the (usual) universal formulas for quadratics, cubics, and quartic polynomials. Also, these results show that the roots to $p_n(x)$, $n \geq 5$, do not provide K–formulas, much less universal formulas.

However, we can ask why there could not still be formulas which are not roots to $p_n(x)$. In particular, might there exist such formulas even if $p_n(x)$ is not solvable by radicals? Of course one could only expect such formulas to work for polynomials over some restricted set of fields, perhaps even a single field. In search of such formulas, we begin in the same manner that gave rise to the roots u_i.

Let K denote a field (of arbitrary characteristic) and suppose $v_1, \ldots, v_n$ are from the algebraic closure of $K(\vec{t})$. The v_i are roots to the polynomial

$$q_n(x) = x^n - f_1(\vec{v})x^{n-1} + \cdots + (-1)^{n-1} f_{n-1}(\vec{v})x + (-1)^n f_n(\vec{v}) \in K(f_1(\vec{v}), \ldots, f_n(\vec{v}))[x],$$

where the f_i, $1 \leq i \leq n$, denote the symmetric polynomials in n variables and $\vec{v}$ denotes $v_1, \ldots, v_n$.

The elements $v_1, \ldots, v_n$ are K–formulas for polynomials of degree n if and only if

(3) $v_1(\vec{t}), \ldots, v_n(\vec{t})$ are contained within a radical extension of $K(\vec{t})$, and

(4a) for each substitution $\vec{t} \mapsto \vec{a} \in K^n$, $v_1(\vec{a}), \ldots, v_n(\vec{a})$ are each well–defined, and for each i, $f_i(v_1(\vec{a}), \ldots, v_n(\vec{a})) = a_i$. Does this imply that the new formulas v_i must be the roots

u_i to $p_n(x)$? One can show the answer would be yes if the v_i's were within a radical extension of $K(f_1(\vec{v}), \ldots, f_n(\vec{v}))$, but we are not assuming this to be true.

From a model theory perspective, condition (4a) is simply

(4b) if K satisfies $(-1)^i f_i(v_1(\vec{t}), \ldots, v_n(\vec{t})) \approx t_i$, $1 \leq i \leq n$,
then must $(-1)^i f_i(v_1(\vec{t}), \ldots, v_n(\vec{t})) = t_i$, $1 \leq i \leq n$? If so, then the v_i's are the roots to $p_n(x)$.

We show this must be the case when K is an infinite field (Appendix D). Thus, the only K–formulas, K an infinite field, are the universal formulas given by the roots to $p_n(x)$, $n \leq 4$.

If K is a finite field could there exist formulas for the roots to all polynomials of degree n even if $n \geq 5$ or if $\operatorname{char} K \leq n$? In view of Galois' results, (1) and (2), it may not seem likely. But despite the failure of the roots to $p_n(x)$ to provide formulas in these cases, perhaps there are other formulas which work only for K. After all, such a K–formula need only solve a finite number of polynomials.

The problem of finding roots within a specific finite field arises in some applications (for example, coding theory). Of course this can be accomplished by trying all the elements; a method for this which makes use of the cyclic structure of the finite field's multiplicative group is the Chien search [1].

I would like to thank Dan Cazacu and Suren Fernando whose interest and comments were very helpful in preparing this note.

Appendix

All notation and assumptions are the same as in the body of the paper.

A. $p_n(x) = x^n + t_1x^{n-1} + \cdots + t_{n-1}x + t_n$ is irreducible and separable over $K(t_1, \ldots, t_n)$.

Proof. First we show that $p_n(x)$ is separable over $K(\vec{t})$. It certainly would suffice to show that its set of roots $\{u_1, \ldots, u_n\}$ is algebraically independent over K. This follows from the algebraic independence over K of the set $t_1, \ldots, t_n$ and the fact that $K(t_1, \ldots, t_n) = K(f_1(\vec{u}), \ldots, f_n(\vec{u})) \subseteq K(u_1, \ldots, u_n)$.

Now we show $p_n(x)$ is irreducible over $K(\vec{t})$. Let E denote the symmetric rational functions in $K(x_1, \ldots, x_n)$. Then $Aut_{K(\vec{t})}K(\vec{u}) \cong Aut_E K(\vec{x}) \cong S_n$. If $p_n(x)$ is factored over $K(\vec{t})$ then the coefficients of the factor polynomials would be in $K(\vec{t})$ hence, fixed by the Galois group of $p_n(x)$. But these coefficients are symmetric polynomials (in $m < n$ variables) of m of the roots to p_n. Since the roots to $p_n(x)$ are distinct and its Galois group is S_n, these coefficients cannot be fixed by the Galois group, a contradiction.

B. Let $u_1(\vec{t}), \ldots, u_n(\vec{t})$ lie within a radical extension of $K(\vec{t})$ and assume they are each defined under the substitution $\vec{t} \mapsto \vec{a} \in K^n$. Then $u_1(\vec{a}), \ldots, u_n(\vec{a})$ are the roots to $\overline{p}_n(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$. Also, each $u_i(\vec{a})$ lies within a radical extension of K.

Proof. This can be thought of as an extension of the fact that the 'evaluation map' (on a commutative polynomial ring) is a morphism, to include the evaluation of radical expressions as well. While most people would not doubt this, one can become frustrated if pressed by a student for a proof. This may be because it is implicitly assuming certain notational conventions.

Convention has it that a root of $x^m - q(\vec{t}) \in K(\vec{t})[x]$, as a function of x, is denoted by $(q(\vec{t}))^{1/m}$. Similarly, assuming that $q(\vec{a})$ is defined, $(q(\vec{a}))^{1/m}$ denotes a primitive root of $x^m - q(\vec{a})$ (the apparent limitations of such conventions is discussed in Appendix E).

First, we prove the result for polynomials of this basic form. We assume $q(\vec{a})$ is defined and write $x^m - q(\vec{t})$ as $g(\vec{t})x^m - f(\vec{t}) \in K[\vec{t}][x]$, where $q(\vec{t}) = g(\vec{t})/f(\vec{t})$.

We begin with the usual evaluation map, ϕ, from the polynomial ring, $K[\vec{t}][x]$, to the ring $K[(q(\vec{a}))^{1/m}]$, which maps $\vec{t} \mapsto \vec{a} \in K^n$ and $x \mapsto (q(\vec{a}))^{1/m}$. This map is an epimorphism which fixes K.

Essentially, we need to show ϕ factors through the ring $K[\vec{t}][(q(\vec{t}))^{1/m}]$. Since this latter ring is isomorphic to the quotient ring $K[\vec{t}][x]/(g(\vec{t})x^m - f(\vec{t}))$, it suffices to show that $(g(\vec{t})x^m - f(\vec{t})) \subseteq \ker\phi$. But this follows immediately from the fact that ϕ is a morphism and the conventions previously mentioned.

To show that we can substitute into the expression $u_i(\vec{t})$ as well, we note that since it lies in a radical extension of $K(\vec{t})$, each $u_i(\vec{t})$ is a nested expression of the basic type just considered. So it suffices to repeat the previous argument (for example, by next using the ring $K[(q(\vec{a}))^{1/m}]$ in place of K) a finite number of times. The assumption that $u_i(\vec{a})$ is defined ensures that each of the basic expressions $q(\vec{a})$ involved is defined.

C. If $h \in K[x_1, \ldots, x_n]$, K an infinite field, and h vanishes on K^n then h is the zero polynomial.

Proof. Basically, each 'cross–section' can have only a finite number of roots. More precisely, h, as an element of $K[x_1, \ldots, x_{n-1}][x_n]$, has an infinite number of roots hence each coefficient (which is a polynomial in $K[x_1, \ldots, x_{n-1}]$) is zero. Continuing in this way, we see that each coefficient of h must be zero hence, h is the zero polynomial.

D. Suppose $v_1(\vec{t}), \ldots, v_n(\vec{t})$ lie within a radical extension of $K(\vec{t})$, K an infinite field. For each i, if K satisfies $(-1)^i f_i(v_1(\vec{x}), \ldots, v_n(\vec{x})) \approx x_i$ then $(-1)^i f_i(v_1(\vec{t}), \ldots, v_n(\vec{t})) = t_i$.

Proof. $(-1)^i(f_i(v_1(\vec{t}), \ldots, v_n(\vec{t})) - t_i)$ is an element of this radical extension; denote it by $w(\vec{t})$. Let $g(x) \in K(\vec{t})[x]$ denote the monic, irreducible polynomial for which it is a root. If $w(\vec{t}) \neq 0$ then the constant term in $g(x)$ must be nonzero since otherwise we could factor an x out. The coefficients of $g(x)$ are elements of $K(\vec{t})$ (rational functions). Multiply $g(x)$ by the product of the denominators of these coefficients to get a polynomial $h(\vec{t}, x)$ with coefficients from K. The constant coefficient of h is a nonzero polynomial $h_0(\vec{t}) \in K[\vec{t}]$. As in the proof of (B), since $w(\vec{t})$ is a root to $h(\vec{t}, x)$, $w(\vec{a})$ is a root to $h(\vec{a}, x)$. Thus, $h_0(\vec{a})$ must be zero whenever $w(\vec{a})$ is zero. So h_0 vanishes on K^n hence, by (C), h_0 is the zero polynomial, a contradiction. So $w(\vec{t}) = 0$.

In other words, as with polynomials in n variables, a nonzero radical expression in n variables defined over an infinite field cannot have all n–tuples as roots.

E. An element w from the algebraic closure of $K(\vec{t})$ is a root to a unique monic, irreducible polynomial $h(x) \in K(\vec{t})[x]$. As in the proof to (D), we may assume $h(\vec{t}, x) \in K[\vec{t}, x]$. One might try defining $w(\vec{a})$ to be a root to $h(\vec{a}, x) = x^n + \sum_{i=0}^{n-1} h_i(\vec{a})x^i \in K[x]$. However, unless dealing with a certain set of polynomials such as $x^n - h_0(\vec{a})$, it is not clear how to generally specify which root to assign $w(\vec{a})$ to for the purposes of computation (recall the conventions stated in the proof to Appendix B). Besides, the purpose of a formula is to express the roots of a complicated polynomial in terms of field operations and roots of simpler polynomials, e.g. radicals. This is not to say that some specific variation of a radical extension could not be used.

References

1. E. Berlekamp, *Algebraic Coding Theory*, McGraw–Hill, 1968.
2. T. Hungerford, *Algebra*, Springer–Verlag, 1974.
3. F. Klein, *Lectures on the Icosahedron*, Dover, 1956.
4. M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, 1972. æ