An Algebraic Approach to Image De-smearing: Symmetries of Polynomials and Their Zeros

D. L. Johnson
Communications Systems Research Section

Frequently a photograph received from a spacecraft will be "smeared" by some process, e.g., by camera motion. Algebraically such smearing can be represented as $p = \sigma f$, where σ is the true picture, p is the received picture, and f is the smearing function. (p, σ, and f are polynomials in two variables x and y.) Thus, in principle, σ can be recovered by multiplying p by $1/f$. However, there are problems involved in computing $1/f$; this paper investigates some of them.

I. Introduction

It is often the case that a photograph received from a spacecraft will be "smeared" by some process, e.g., by the motion of the camera while the shutter is open. In this article we will study one aspect of the problem of smear compensation.

We assume the original picture is uniformly sampled, and thereby discretized into cells which are labeled with coordinates (a,b); we shall represent the picture by a polynomial in two abstract variables x,y:

$$\sigma(x,y) = \sum_{a,b} \sigma_{a,b}\, x^a y^b$$

This representation means simply that the pixel with integer coordinates (a,b) has brightness level $\sigma_{a,b}$. We further assume that the smearing process can be represented by a *point-smear polynomial* $f(x,y)$, i.e., that the smeared version of the original picture is given by

$$p(x,y) = \sigma(x,y)\, f(x,y)$$

(In particular, $f(x,y)$ itself represents the smeared version of the "unit impulse signal," $\sigma(x,y) = 1$.) If we are given p (the received picture) and f (which can be computed from knowledge of spacecraft geometry), we can hope to recover the original picture σ as

$$\sigma = p(x,y)/f(x,y)$$

So we need a practical representation of the rational function $p(x,y)/f(x,y)$.

One approach is to expand $1/f(x,y)$ as a power series in x and y (with negative powers permitted). This power series can then be multiplied formally by p to recover σ. However, in order for this procedure to give physically meaningful results, it is necessary (for technical reasons we shall omit) that the power series (a) has coefficients approaching 0 as $|a|$ or $|b| \rightarrow \infty$, or, even better, (b) converges for all values on the "unit torus" = $\{(x,y):|x| = |y| = 1\}$ (Condition (b) implies condition (a).) These two conditions turn out to be equivalent to (a) f has only a finite number of zeros on the unit torus; (b) f has no such zeros.

The purpose of this paper is then to study the zeros of a polynomial on the unit torus.

II. L-Polynomials

I want to examine the zeros of a polynomial $f(x,y)$ in two (complex) variables lying on the "unit torus," that is, the points (x,y), where $|x| = |y| = 1$ (this is the generalization of the "unit circle" to two complex variables; I shall call such zeros "unimodular"). We shall find that a certain symmetry operation is useful in this context, and in fact that certain "symmetric" polynomials always do have roots.

First note the following: the function $kx^ay^bf(x,y)$, where $k \neq 0$ is a constant and a,b are integers, has exactly the same zeros on the unit torus U^2 as does f (this is true even when a or b is less than zero); for this reason we will call two polynomials f,g *equivalent*, written $f \simeq g$, if $g = kx^ay^bf$. It will be convenient to include in our considerations not only polynomials in x,y, but all functions of the form $x^ay^bf(x,y)$, where f is a polynomial function, and a,b may be negative—that is, polynomials in x,y, $1/x$, and $1/y$. Our notion of equivalence clearly extends to these functions, which we will call *L-polynomials.* Every equivalence class of *L-polynomials* has an obvious representative, namely, a *polynomial* having *no factors of x or y.* That is, if f is an L-polynomial, multiply it (if there are negative degree terms) or divide it (if the degrees of the terms are all positive) by suitable powers of x and y to achieve a function equivalent to f and having the above italicized properties. This polynomial (which is only determined up to a constant multiple) will be called the *reduced form* of f, and any polynomial without factors of x or y, *reduced.*

We introduce these definitions:

(a) The *x-degree* of f (an L-polynomial), written $\deg_xf$, is the highest power of x occurring in f; likewise $\deg_yf$.

(b) The x-subdegree sbdg_xf is the *lowest* power of x occurring in (the terms of) f; likewise sbdg_yf.

(c) The range of x (in f), written rng_xf, is $\mathrm{rng}_xf = \deg_xf - \mathrm{sbdg}_xf$; likewise for rng_yf.

Note that if f is a *polynomial*, then sbdg_xf is just the largest power of x dividing f; in fact more generally, we have for any L-polynomial f, $x^{-\mathrm{sbdg}_xf} \cdot y^{-\mathrm{sbdg}_yf} \cdot f$ is a reduced form of f.

The set of L-polynomials form a *ring*, that is, the product, sum, and difference of two L-polynomials is another L-polynomial. In this ring we have a greatest common divisor (GCD)) d of any two elements f,g; we write $d = (f,g)$. The GCD here is the usual GCD of polynomials, but as in all rings, it is only defined up to a multiple by a *unit*; a unit is an L-polynomial u such that $1/u$ is *also* an L-polynomial. Later we will need to work with the GCD of L-polynomials, and we will have use for the following:

If u is a unit in the ring L of L-polynomials, then u is a *monomial*, that is, $u = kx^ay^b$.

Proof: Let $1/u = v$, v an L-polynomial. Then $uv = 1$. Let U,V be reduced forms of u, v, with $U = x^\alpha y^\beta u$ and $V = x^\gamma y^\delta v$: then $UV = x^{\alpha+\gamma}y^{\beta+\delta}$. Since U and V are *polynomials*, the unique factorization of polynomials tells us that U must be of the form kx^ay^b, as well as V. Q.E.D.

The above has the following corollary: The GCD $d = (f,g)$ of two L-polynomials is only defined up to multiple by a unit; but the units are kx^ay^b: thus d is defined up to the *equivalence* of L-polynomials. Hence we would be more correct to write: $d \simeq (f,g)$.

III. The Adjoint Operation

We now introduce our main tool in investigating the unimodular zeros of $(L-)$ polynomials, an operation * on L-polynomials which we call the *adjoint*, defined by:

$$f^*(x,y) = \overline{f(1/\bar{x}, 1/\bar{y})}$$

where the bar denotes complex conjugation. This operation simply replaces x by $1/x$ and y by $1/y$, and conjugates all the coefficients of f. Thus, f^* is also an L-polynomial in x,y. We also have:

(1) $(f^*)^* = f$

(2) $(f + g)^* = f^* + g^*$

(3) $(fg)^* = f^*g^*$

(4) $\deg_xf^* = -\mathrm{sbdg}_xf$ (ditto y)

(5) $(f,g)^* \simeq (f^*,g^*)$

The first four are clear. To prove the last statement, suppose d divides f and g, with $f = Fd$, $g = Gd$, where d, F, G are also L-polynomials. Then we have, using (3),

$$f^* = F^*d^*, \qquad g^* = G^*d^*$$

i.e., d^* divides f^* and g^*, *i.e.*, d^* divides (f^*,g^*). In particular, putting $d = (f,g)$, we get $(f,g)^*$ divides (f^*,g^*). Replacing f by f^* and g by g^* and using (1), we have then also:

$$(f^*,g^*)^* \text{ divides } (f,g), \text{ and so } (f^*,g^*) \text{ divides } (f,g)^*$$

Thus, $(f,g)^*$ and (f^*,g^*) divide each other, that is, they are unit multiples of each other, or as we saw in Section II, $(f,g)^* \simeq (f^*,g^*)$. Q.E.D.

The connection of the unimodular zeros of f and the adjoint operation lies in the following:

Proposition 1: If $(x,y) = (\alpha,\beta)$ is a root of $f(x,y) = 0$ on U^2, i.e., $f(\alpha,\beta) = 0$ and $|\alpha| = |\beta| = 1$, then $f^*(\alpha,\beta) = 0$ also.

Proof: $f^*(\alpha,\beta) = \overline{f(1/\bar{\alpha}, 1/\bar{\beta})}$; but $|\alpha| = |\beta| = 1$ means $1/\bar{\alpha} = \alpha$, $1/\bar{\beta} = \beta$, so

$$f^*(\alpha,\beta) = \overline{f(\alpha,\beta)} = \bar{0} = 0$$

Corollary: If f is an L-polynomial, then the unimodular roots of f lie among the common roots of f and f^*. Hence, either these roots are *finite* in number, or f and f^* have a common polynomial factor.

Proof: We may assume f is reduced, and replace f^* by its reduced form g, since these have the same unimodular roots. Then the zeros of f on U^2 are also zeros of g. It is well known (Bezout's theorem) that two polynomials in x,y have either a common factor or otherwise only a finite number of common roots; in the latter case, there are *a fortiori* only a finite number of zeros of f on U^2.

IV. Self-Adjoint Polynomials

The previous proposition told us that if f and f^* have no (nontrivial) common divisor, that is, $(f,f^*) \simeq 1$, then f has only a finite number of zeros on U^2. If f has an infinite number of zeros, then $d \simeq (f,f^*)$ is not $\simeq 1$ (that is, d is not a monomial kx^ay^b). Let's see how this d behaves under the adjoint operation. We have:

$$d^* \simeq (f,f^*)^* \simeq (f^*,f^{**}) \simeq (f^*,f) \simeq (f,f^*) \simeq d$$

That is, d is *equivalent to its adjoint*. This gives rise to the ***Definition:*** An L-polynomial f is called self-adjoint if $f^* \simeq f$, that is, if $f^* = kx^ay^bf$ for some constant $k \neq 0$ and integers a,b. The triple (k,a,b), which indicates how f must be changed to get f^*, we will call the *translation character* of f.

Note that this definition entails that $|k| = 1$: for if $r > 0$ is the maximum absolute value of the coefficients in f, then it is also that of f^*, since these coefficients are conjugate to those of f. But the maximum absolute value of the coefficients of kx^ay^bf is clearly $|k|r$: so $|k|r = r$ and $|k| = 1$. In particular, if f is a *real* L-polynomial (i.e., real coefficients), then k is clearly also real and so $k = \pm 1$.

Here are some examples of self-adjoint polynomials:

(a) $f = x^2 + 1$: $f^* = x^{-2} + 1 = x^{-2}(x^2 + 1)$: so $(k,a,b) = (1, -2,0)$.

(b) $f = \alpha x^2 + e^{i\theta}\bar{\alpha}y$: $f^* = \bar{\alpha}x^{-2} + e^{-i\theta}\alpha y^{-1} = e^{-i\theta}x^{-2}y^{-1}(e^{i\theta}\bar{\alpha}y + \alpha x^2)$ so $(k,a,b) = (e^{-i\theta},-2, -1)$.

(c) For any L-polynomial g, $f = g + g^*$; then $f^* = f$, and $(k,a,b) = (1,0,0)$.

(d) For any L-polynomial g, $f = g - g^*$; then $f^* = g^* - g = -f$ so $(k,a,b) = (-1,0,0)$.

(e) For any L-polynomial $g,f = g \pm xg^*$; then $f^* = g^* \pm x^{-1}g = \pm x^{-1}(g \pm xg^*)$: so $(k,a,b) = (\pm 1,-1,0)$.

Other examples can be formed in this way.

Let's now see how self-adjointness behaves under equivalence. We have:

Proposition 2: If f is self-adjoint with translation character (k,a,b), then $g = \lambda x^\alpha y^\beta f$ is also self-adjoint, with translation character

$$\left(\frac{\bar{\lambda}}{\lambda}k, a - 2\alpha, b - 2\beta\right)$$

Proof:

$$g^* = \bar{\lambda}x^{-\alpha}y^{-\beta}f^* = \bar{\lambda}x^{-\alpha}y^{-\beta}(kx^ay^bf)$$

$$= \bar{\lambda}x^{-\alpha}y^{-\beta}\left(kx^\alpha y^b \frac{1}{\lambda x^\alpha y^\beta} g\right)$$

$$= \frac{\bar{\lambda}}{\lambda} kx^{a-2\alpha}y^{b-2\beta}g \qquad \text{Q.E.D.}$$

The above shows us that $g \simeq f$ and f self-adjoint → g self-adjoint; further, if we are permitting complex coefficients, by appropriately choosing λ, we can "normalize" f so that its k is 1: in fact if k_f is $e^{i\theta}$, then choose $\lambda = e^{i\theta/2}$. Then the k for $g = \lambda_f$ is

$$\frac{\bar{\lambda}}{\lambda}\, k = \frac{e^{-i\theta/2}}{e^{i\theta/2}}\, e^{i\theta} = 1$$

If we are restricting to real coefficients, however (as when f itself is real), then λ will be real, $\bar{\lambda}/\lambda = 1$, and so $k = \pm 1$ is *unchanged* under equivalence: k is thus an invariant of the self-adjoint equivalence class. We can also see that there are two other invariants of this class: the translation exponents a and b, while not invariant themselves, *are* invariant *mod* 2 since $a - 2\alpha \equiv a$ mod 2, $b - 2\beta \equiv b$ mod 2. Thus, in the complex case, the vector $[(a,b) \bmod 2]$ of numbers mod 2 gives us an invariant of the self-adjoint type of f, which we will call simply the *character* of f. If f is real, k is also an invariant, and if we define $\epsilon = 0$ mod 2 for $k = 1$, $\epsilon = 1$ mod 2 for $k = -1$, then we have a "character" for f consisting of *three* mod 2 numbers (ϵ,a,b). These "characteristic vectors" for f depend only on the equivalence class of f. Recall that the unimodular zero set of f also depends only on its equivalence class; it should not be surprising then that (as we shall see) the character of f influences the behavior of its zero set.

Here is a table of real examples (in some sense minimal ones) showing that every mod 2 vector (ϵ,a,b) actually occurs as the character of some polynomial:

Polynomial	Mod 2		
	ϵ	a	b
1	0	0	0
$x^2 - 1 \left(\text{or } x - \dfrac{1}{x}\right)$	1	0	0
$x + 1$	0	1	0
$x - 1$	1	1	0
$y + 1$	0	0	1
$y - 1$	1	0	1
$x + y$	0	1	1
$x - y$	1	1	1

Here now is how the character influences the zero set of a self-adjoint f:

Proposition 3: If the character of a self-adjoint L-polynomial f is not 0 (that is, the zero vector, mod 2), then f has zeros on U^2.

Proof: In the complex case we have seen that we may assume $k = 1$; then

$$f^*(x,y) = \overline{f(1/\bar{x}, 1/\bar{y})} = \overline{f(x,y)} \text{ for } (x,y)\epsilon U^2$$

But since f is self-adjoint,

$$f^*(x,y) = x^a y^b f(x,y) \qquad (k = 1)$$

Hence,

$$\overline{f(x,y)} = x^a y^b f(x,y)$$

Were f never zero on U^2, we could write uniquely

$$f(x,y) = r(x,y) \cdot u(x,y),$$

where $r = |f| > 0$ and $u = f/r$ is of unit modulus, and r and u are continuous functions of $(x,y)\epsilon U^2$. We have then

$$x^a y^b = \frac{\overline{f(x,y)}}{f(x,y)} = [\bar{u}(x,y)]^2$$

Now, as (x,y) travels around any closed curve in the unit torus U^2, u will travel around the unit circle U an integral number of times, by continuity, and hence u^2 will travel around U an *even* integral number of times. But if we let x travel once around the unit circle while holding $y = 1$, $x^a y^b$ goes a times around U, and likewise let $x = 1$ and y move around U, $x^a y^b$ goes b times around U. Hence a and b must both be *even*, i.e., the character (a,b) mod 2 is zero.

In the real case we have a simpler proof: for now f is real when x and y are, i.e., when x and y are ± 1. We have, then, for such x and y,

$$\overline{f(x,y)} = f(x,y) = kx^a y^b f(x,y)$$

so $f(x,y) \neq 0 \rightarrow kx^a y^b = 1$. But if either a or b is odd, or $k = -1$, we can clearly choose $(x,y) = (\pm 1, \pm 1)$ so that $kx^a y^b = -1$, which implies $f = 0$. Q.E.D.

V. The Case of Infinite Zeros

Henceforth, we are going to confine our attention to the case when f has an *infinite number of zeros* on U^2, which implies $d = (f,f^*)$ is not $\simeq 1$. We can strengthen this statement to:

Proposition 4: f has an infinite number of zeros on U^2 iff the self-adjoint L-polynomial $d \simeq (f,f^*)$ does; in fact, all but a finite number of the zeros of f are zeros of d.

Proof: Putting $f = Fd$, $f^* = Gd$, where F,G are also L-polynomials, then

$$f^* = F^*d^* \simeq F^*d \text{ and } f^* = Gd$$

so

$$G \simeq F^*$$

Hence also $(F,F^*) \simeq (F,G) \simeq 1$: so F and F^* have no common factor, and by the Corollary to Proposition 1, F has only a finite number of zeros on U^2. The zeros of f (on U^2) are the union of those of F and those of d. Q.E.D.

Thus, the zeros of f consist of those of the "self-adjoint part" of f (that is, d), plus a finite number of other, isolated, zeros; so henceforth we shall spend our time elucidating the structure of the zeros of a self-adjoint polynomial d. We already know that if d has non-zero character, it has zeros; the results below will actually show that if d has any zeros, it has an infinite number.

Proposition 5: Let d be a self-adjoint L-polynomial; then its zero set on U^2 consists of a finite number (possibly zero) of real, closed curves on U^2. If the algebraic curve given by $d(x,y) = 0$ is non-singular, or, more generally, if its singularities do not lie on U^2, then these curves are smooth and disjoint.

Proof: We will only prove this for the case when the singularities are off U^2—the full statement follows from an overdose of algebraic geometry. In any case, the locus of $d = 0$ in the complex projective plane* is (a) compact, (b) outside of the singularities, a smooth orientable surface M. The zeros of d on U^2 are simply all points of M satisfying $x = 1/\bar{x}$, $y = 1/\bar{y}$.

Let's consider in more detail the transformation I of the plane given by $x \to 1/\bar{x}$, $y \to 1/\bar{y}$. First of all, I takes M into itself: for $d(x,y) = 0 \to d^*(x,y) = 0$ (since $d^* \simeq d$ and $(x,y)\epsilon U^2$), i.e., $\overline{d(1/\bar{x},\ 1/\bar{y})} = 0$, i.e., $d(1/\bar{x},\ 1/\bar{y}) = 0$, i.e., $(1/\bar{x},\ 1/\bar{y})\epsilon M$. Second, the fixed points of I are precisely the points of the unit torus, and so if we consider I to be a mapping of M into itself, its fixed points are precisely the zeros of d in U^2. For any non-singular (finite) point (α,β) of M (in particular, for $(\alpha,\beta)\ \epsilon U^2$, which was by assumption non-singular), either x or y is an analytic function on M which is one to one on a neighborhood (in M) of (α,β): thus, we may examine the behavior of M and the transformation I in a neighborhood (in M) of (α,β) by examining either the x-values alone or the y-values alone. (That is: either the x-values or y-values *determine* the point in a neighborhood of (α,β), so we may identify it from this one value alone, as well as what I has done to it, if I takes it into the same neighborhood.)

In particular, suppose $(\alpha,\beta)\epsilon U^2$, so $|\alpha| = |\beta| = 1$, I fixes (α,β), and x sends (α,β) to α and a neighborhood of (α,β) in M to a neighborhood of α in the complex number line C. The way I acts in this neighborhood in M is faithfully mirrored by the transformation I_x:$x \to 1/\bar{x}$ in C. This I_x fixes α (as it should, since I fixes (α,β) and everything is mirrored faithfully in C), but also a smooth arc passing through α in the x-plane, namely, all points x in a neighborhood α for which $|x| = 1$; the same is thus true in M: the inverse image of these fixed points of I_x in C are fixed points of I, and are a smooth arc in M. Since they are fixed by I, they are also *in* U^2: thus, we have shown that, if $(\alpha,\beta)\epsilon\ M \cap U^2$ (i.e., is a zero of d in U^2), then there is a smooth arc passing through (α,β), entirely in $M \cap U^2$; also, in our neighborhood of (α,β) these arc's points are the only points in $M \cap U^2$ (again, because this is true of α in C): Thus, $M \cap U^2$ consists locally of smooth arcs; since it is also compact (both M and U^2 are so in the projective plane), then $M \cap U^2$ must be a finite collection of disjoint smooth closed (real) curves.

As an easy Corollary: if d is self-adjoint and has one zero on U^2, then it has an infinite number. Also: d has no isolated zeros. (These apply, for example, to any d with non-zero character.)

VI. Winding Numbers

Let us think of the smooth closed curves of $M \cap U^2$ as *curves on* U^2. We would like to investigate a bit more thoroughly how these curves are situated in U^2. If then α is any closed curve on U^2, it may be parameterized as

$$\alpha(u) = (x(u), y(u)), |x(u)| = |y(u)| = 1$$

*The *complex plane* means here the set of all pairs (x,y) with x and y *complex*; the *real* plane has x,y *real*. Thus, the real plane is two-dimensional, but the complex plane is 4-dimensional (over the *reals*). The real dimension is always twice the complex dimension; thus, an algebraic curve over the *complexes* is two *real* dimensions, although the very word "curve" means one-dimensional.

and u is a parameter, which we may assume travels around the unit circle once as $\alpha(u)$ travels the closed curve once. We then have the *winding numbers of* α, $W_x(\alpha)$ = the number of times $x(u)$ goes around U (in the positive sense) as u goes around U once (also in the positive sense); likewise for $W_y(\alpha)$.

Note that we have chosen an orientation of α in this definition, namely, via our parameterization. If we were to change the parameterization by $u \to \bar{u}$, the curve would be traced in reverse, likewise $x(u)$ and $y(u)$, and so both winding numbers would negate. These winding numbers are, however, well defined mod 2, independent of this choice of orientation.

Likewise, if we have a collection $A = \{\alpha_i\}$ of closed curves (not necessarily disjoint) on U^2, we may define their *total winding numbers*

$$W_x(A) = \sum_i W_x(\alpha_i)$$

and

$$W_y(A) = \sum_i W_y(\alpha_i)$$

The orientations of the various α_i may be chosen in various ways, so the total winding numbers are not well defined (even up to sign); they *are* still, however, well-defined mod 2.

A winding number may be computed in various ways; we shall do it as follows: $W_x(\alpha)$ = the number of times $x(u)$ passes any fixed point $\theta \epsilon U$ in the *positive direction*, counting -1 for passing it in the negative (i.e., clockwise) direction. Modulo 2, this total sum of $+1$'s and -1's is just the number of times $x(u)$ takes any particular value $\theta \epsilon U$ on the curve α; that is, the number of roots u of $x(u) = \theta$.

In particular, let $A = \{\alpha_i\}$ be the collection of curves given by the equation $d = 0$ on U^2, where d is a self-adjoint L-polynomial with translation character (k,a,b). If we put $x = \theta$ in d, we get an L-polynomial

$$Y_\theta(y) = d(\theta,y)$$

an L-polynomial in y alone. The total mod 2 winding number $W_x(A)$ is the number (mod 2) of points on A with $x = \theta$; i.e., it is just the number of solutions of $Y_\theta(y) = 0$ with $|y| = 1$. We have now the following two lemmas:

Lemma 1. $Y_\theta(y)$ is an L-polynomial which for general θ has the same degree, subdegree, and range as that of y in d. Furthermore, Y is self-adjoint in y, with translation monomial $k\theta^a y^b$.

Proof: The first statement is clear (if we just choose θ to be a non-root of the coefficients of the highest and lowest powers of y). As to the second:

$$\begin{aligned} Y^*(y) &= (\text{by definition}) \overline{Y(1/\bar{y})} = \overline{d(\theta,1/\bar{y})} \\ &= d(1/\bar{\theta},1/\bar{y}) \text{ (since } |\theta| = 1) = d^*(\theta,y) \\ &= k\theta^a y^b d(\theta,y) = k\theta^a y^b\, Y(y) \qquad \text{Q.E.D.} \end{aligned}$$

Lemma 2. If $Y(y)$ is a self-adjoint L-polynomial of range r, then the number of roots of Y on the unit circle $|y| = 1$ is $\equiv r \bmod 2$.

Proof: The non-zero roots of Y are just the roots of the reduced form of Y: $y^{-\mathrm{sbdg}_y Y} \cdot Y(y)$; also r is the degree of this reduced form. Hence we may assume Y is already reduced, and $\deg_y Y = r$. In this case $Y^* = \overline{Y(1/\bar{y})} = ky^{-r}Y$. Since the roots of Y are non-zero (it is reduced, after all, and has no y-factors), any root y_0 inside the unit circle corresponds to a root $1/\bar{y}_0$ of Y^*, and hence also Y, *outside* the unit circle. Thus, the total number of roots of Y is (the # on $|y| = 1$) + 2 • (# roots inside $|y| = 1$); this is, of course, also the *degree* of Y (double roots are counted twice). Hence we have:

$$r \equiv \#\text{ roots on } |y| = 1 \bmod 2 \qquad \text{Q.E.D.}$$

Applying this to $Y_\theta(y) = d(\theta,y)$, we have

$$\begin{aligned} W_x(A) &\equiv \#\text{ roots of } Y_\theta(y) \text{ on } |y| = 1 \equiv \mathrm{rng}_y Y(y) \\ &= \mathrm{rng}_y d = \deg_y d - \mathrm{sbdg}_y d \\ &\equiv -\deg_y d - \mathrm{sbdg}_y d \bmod 2 \end{aligned}$$

If now (k,a,b) is the translation character of d, then note that $b = -\deg_y d - \mathrm{sbdg}_y d$: for the higher power of y in d, that is, $\deg_y d$, becomes the lowest power $-\deg_y d$ in d^*, that is, the subdegree term; to bring the subdegree term of d down to $y^{-\deg_y d}$, we must clearly multiply by $y^{-\deg_y d - \mathrm{sbdg}_y d}$, that is, $b = -\deg_y d - \mathrm{sbdg}_y d$.

Thus, we have, finally,

$$W_x(A) \equiv b \bmod 2$$

Similarly, we find $W_y(A)$ mod 2, and thus our final

Proposition 6: The winding numbers (W_x,W_y) of the zero set (in U^2) of a self-adjoint L-polynomial d with (complex) character (a,b) satisfy:

$$(W_x,W_y) \equiv (b,a) \bmod 2$$