Annihilating polynomials for quadratic forms

David W. Lewis

email address david.lewis@ucd.ie

Abstract. This is a short survey of the main known results concerning annihilating polynomials for the Witt ring of quadratic forms over a field.

1991 A.M.S. Subject Classification : 11E81, 12F10, 19A22
Keywords : quadratic form, trace form, Witt ring, Burnside ring, étale algebra

Let F be a field of characteristic different from two. We recall briefly the Witt ring $W(F)$ of quadratic forms over F. Consider first the set S of isometry classes of non-singular quadratic forms over F. We write $G(F)$ for the free abelian group generated by the set S. We factor out by the subgroup generated by all elements of the form $\{\phi_1 \perp \phi_2\} - \{\phi_1\} - \{\phi_2\}$ where ϕ_1 and ϕ_2 are non-singular quadratic forms, $\perp$ denotes the orthogonal sum of forms (defined via the direct sum of the underlying vector spaces), and $\{\phi\}$ denotes the isometry class of a form ϕ. The product of two forms (defined via the tensor product of the underlying vector spaces) is used to make $G(F)$ into a commutative ring. This is sometimes known as the Witt-Grothendieck ring. The set of all hyperbolic forms, i.e. orthogonal sums of copies of the two-dimensional hyperbolic plane, is an ideal in this ring and the Witt ring $W(F)$ is the quotient ring obtained by factoring out this ideal. We will use the terminology and notation of [18] where further details about quadratic forms and Witt rings may be found.

The Witt ring was invented in 1937 [20] and Witt seemed aware that his ring was an integral ring in the sense that each element is annihilated by some monic polynomial with integer coefficients. This integral property was exploited in [10] in 1972 in the context of quotients of abelian group rings. However it was not until 1987 that the first examples were given of explicit polynomials which annihilated particular classes of quadratic forms in $W(F)$. Consider the polynomials $p_n(x)$ defined as follows;

for n even, $p_n(x) = x(x^2 - 2^2)(x^2 - 4^2)...(x^2 - n^2)$

for n odd, $p_n(x) = (x^2 - 1^2)(x^2 - 3^2)...(x^2 - n^2)$

(Note that $p_n(x)$ is an odd polynomial for n even, i.e. $p_n(-x) = -p_n(x)$ for all x, while $p_n(x)$ is an even poynomial for n odd, i.e. $p_n(-x) = p_n(x)$ for all x.)

Theorem 1. *[11] The polynomials $p_n(x)$ have the property that $p_n(\phi) = 0$ in $W(F)$ for any non-singular quadratic form of dimension n over any field F.*

There are many different ways to prove this theorem. The quickest proof, suggested by K.H. Leung, is via induction on n and using the recurrence relation $p_n(x) = (x+n)p_{n-1}(x-1)$.

(It should be remarked that this theorem holds more generally than for just for the Witt ring of quadratic forms. If R is any commutative ring with identity and $t_1, t_2, ..., t_n$ are elements of R such that $t_i^2 = 1$ for each i and if $t = t_1 + t_2 + ... + t_n$ then $p_n(t) = 0$ in R. The Witt ring $W(F)$ is generated by the one-dimensional forms each of which squares to equal the identity in $W(F)$).

If one imposes other conditions on the quadratic form ϕ, e.g. that ϕ has determinant one, or that $\phi \epsilon I^n$, the n-th power of the fundamental ideal in $W(F)$, then one may find a smaller degree polynomial which annihilate ϕ. See [11] for details.

Independently, and at around the same time as theorem 1 was discovered, Pierre Conner was considering trace forms of separable extension fields. (These are non-singular quadratic forms over F) He looked at the polynomials $q_n(x)$ defined as follows;

for n even, $q_n(x) = x(x-2)(x-4)...(x-n)$

for n odd, $q_n(x) = (x-1)(x-3)...(x-n)$

One may think of $q_n(x)$ as the "positive half" of $p_n(x)$.

Theorem 2. *[2] The polynomials $q_n(x)$ have the property that $q_n(\phi) = 0$ in $W(F)$ for any quadratic form ϕ which is the trace form of a separable field extension L of degree n of F.*

(Recall that the trace form of L over F is the quadratic form $q : L \longrightarrow F, q(x) = tr(x^2)$ where tr denotes the reduced trace map from L to F.)

The proof of this theorem by Conner used the Burnside ring of permutation representations of a group, finding identities in this ring which translate, via a ring homomorphism to the Witt ring, into the annihilating polynomials $q_n(x)$. Conner did not publish this theorem in 1987 because he believed correctly that a better result was possible. See the Beaulieu-Palfrey theorem later which gives some smaller degree polynomials annihilating trace forms.

Remark 1. *The standard structure theorems for the Witt ring [18] can be deduced in a quick and elementary way from the fact that $W(F)$ is integral and from the specific nature of the polynomials $p_n(x)$. See [12] for full details.*

Remark 2. *Hurrelbrink [9] used elementary Fourier analysis on groups to obtain annihilating polynomials for group rings of abelian torsion groups. The group of square classes of F is an abelian 2-group and $W(F)$ can be regarded as a quotient of the integral group ring of this group. Theorem 1, on the annihilating polynomials $p_n(x)$, can then be quickly deduced from Hurrelbrink's result.*

Remark 3. *Lewis [13] showed that the polynomials $q_n(x)$ annihilate all positive forms of dimension n in the case when the field F has the property that I^3F is torsion-free. Here I^3F denotes the cube of the fundamental ideal IF of even-dimensional forms in $W(F)$. Such fields are precisely the ones for which the standard invariants, (i.e. dimension, determinant, signatures, Hasse invariant), give a complete isometry classification of non-singular quadratic forms over F. A positive form is one with a non-negative signature at each ordering of F. Trace forms of separable field extensions are examples of positive forms.*

Remark 4. *Another approach to annihilating polynomials is via exterior powers of quadratic forms. This was mentioned first in a talk by Serre at a conference in Luminy 1994 although Serre did not subsequently publish his ideas. McGarraghy [15] has recently investigated this approach in detail. The basic idea is to show that the exterior powers $\Lambda^k\phi$ of a quadratic form ϕ (or strictly speaking the sum of $k!$ copies of $\Lambda^k\phi$) may be expressed as an integer polynomial in ϕ. Then the fact that $\Lambda^{n+1}\phi = 0$ if ϕ has dimension n leads to the polynomials $p_n(x)$ which annihilate ϕ.*

Remark 5. *Sladek [19] has defined, in a formal way, the Witt ring of any skewfield and a notion of dimension for elements of this ring. He shows that Theorem 1 is valid for this Witt ring of a skew field and uses it to show that his Witt ring is an abstract Witt ring in the sense of [10].*

One may define the *annihilator ideal* $A(F)$ of the field F as an ideal in the polynomial ring $\mathbb{Z}[x]$ given by $A(F) = \{p(x) \; \varepsilon \; \mathbb{Z}[x] : p(\phi) = 0 \text{ for all } \phi \text{ in } W(F)\}$. This ideal is finitely generated and one may try to find a set of generators for $A(F)$. In the case of the field F not being formally real, i.e. admitting no orderings, this has been done by Ongenae and Van Geel [17] in the case that F has level at most 16. To be more precise Ongenae and Van Geel have defined a sequence of ideals J_r in $\mathbb{Z}[x]$. The first six of these ideals are as follows;

$J_1 = (2, x^2(x-1)^2)$;
$J_2 = (4, 2x^2(x-1)^2, x^4(x-1)^4)$;
$J_3 = (8, 4x^2(x-1)^2, x^4(x-1)^4)$;
$J_4 = (16, 8x^2(x-1)^2, 2x^4(x-1)^4, x^6(x-1)^6)$;
$J_5 = (32, 16x^2(x-1)^2, 4x^4(x-1)^4, 2x^6(x-1)^6, x^8(x-1)^8)$;
$J_6 = (64, 32x^2(x-1)^2, 8x^4(x-1)^4, 4x^6(x-1)^6, x^8(x-1)^8)$.

We refer the reader to [17] for the definition of the ideals J_r in general. They conjecture that $A(F) = J_r$ whenever F has level 2^{r-1} and they prove the conjecture for $r \leq 5$.

Conner did not publish Theorem 2 on trace forms of finite separable field extensions because he believed that if one had some information about the Galois group

of the field extension then an improvement on Theorem 2 was possible. Following Conner's ideas Beaulieu and Palfrey [1] introduced the notion of the *Galois number* of a separable irreducible polynomial $f(t)$ of degree n over F. This is the smallest natural number g such that any g roots of the polynomial $f(t)$ generate the splitting field N of $f(t)$ over F.

They introduce the polynomials

$$r_{n,g}(x) = (x-n) \prod_{\substack{k=0 \\ k \equiv n (\mathrm{mod}\, 2)}}^{g-1} (x-k)$$

i.e. the product is taken over all integers k between 0 and $g-1$ and such that $k \equiv n (\mathrm{mod}\, 2)$.

Theorem 3. *[1] The polynomials $r_{n,g}(x)$ have the property that $r_{n,g}(\phi) = 0$ in $W(F)$ for any quadratic form ϕ which is the trace form of a field extension $L = F(\theta)$ where θ is a single root of the separable irreducible polynomial $f(t)$ over F of degree n and Galois number g.*

Their proof, like that of the earlier Conner theorem on trace forms, involves obtaining identities in the Burnside ring and translating these to $W(F)$ via a ring homomorphism to $W(F)$. The polynomials $r_{n,g}(x)$ improve on the Conner polynomials $q_n(x)$ since they are divisors of the $q_n(x)$ but generally will be of lower degree.

Remark 6. *For some groups G it is easy to determine the Galois number g. For example if G is a subgroup of the symmetric group S_n and G contains a transposition then $g = n-1$. Also if G is a subgroup of the symmetric group S_n and G contains a 3-cycle but no transposition then $g = n-2$. For more on calculating Galois numbers see [1], [5], [8].*

There is another approach [14] which yields even lower degree annihilating polynomials for trace forms. This also involves Burnside rings but uses an alternative interpretation of the Burnside ring as the Grothendieck ring of étale F-algebras. Recall that an étale F-algebra is a direct product of finite separable field extensions of F. We briefly outline this approach.

Let $f(t)$ be a separable irreducible polynomial of degree n over F, let $L = F(\theta)$ where θ is a single root of $f(t)$, and let N be a splitting field of $f(t)$ over F. Then N will be a normal closure of L over F. For any intermediate field E, i.e. where $F \subseteq E \subseteq N$, we define the integer $\phi_E(L)$ to be the number of monomorphisms from L to E. Equivalently $\phi_E(L)$ equals the number of roots of the polynomial $f(t)$ which lie in E. Also one may interpret $\phi_E(L)$ as the number of components of the étale

algebra $L \otimes_F E$ which are isomorphic to E. It is easy to see that $\phi_E(L) = 0$ whenever $E \subset L$ but $E \neq L$, and also that $\phi_N(L) = n$ since $L \otimes_F N$ is a product of n copies of N. Observe that $L \otimes_F N = F[t]/(f(t)) \otimes_F N \cong N[t]/(f(t)) \cong \prod N$. Let the set $S_L = \{\phi_E(L) : F \subseteq E \subseteq N\}$, i.e. the set of integers $\phi_E(L)$ where E runs through all intermediate fields between F and N. Note that $S_L \subseteq \{0, 1, 2, 3, ..., n-1, n\}$.

Define the polynomial

$$r_L(x) = \prod_{\substack{k \epsilon S_L \\ k \equiv n (\mathrm{mod}\, 2)}} (x - k)$$

Note that, apart from n, the largest value in the set S_L will be $g - 1$ where g is the Galois number of the polynomial $f(t)$. (This follows from the definition of Galois number). Consequently the polynomial $r_L(x)$ will be a divisor of the polynomial $r_{n,g}(x)$.

Theorem 4. *[14] The polynomials $r_L(x)$ have the property that $r_L(\phi) = 0$ in $W(F)$ for any quadratic form ϕ which is the trace form of a field extension $L = F(\theta)$ where θ is a single root of the separable irreducible polynomial $f(t)$ over F of degree n and with splitting field N as above.*

Remark 7. *The proof of this theorem depends on the fact that there is an injective ring homomorphism from the Burnside ring $\Omega(F)$ of étale F-algebras into $\prod \mathbb{Z}$, a product of finitely many copies of the ring of integers. The above definition of the integer-valued mappings ϕ_E can easily be extended to étale F-algebras and the collection of all ϕ_E will yield the imbedding into $\prod \mathbb{Z}$. The fact that $\Omega(F)$ imbeds into $\prod \mathbb{Z}$. was observed by [4]. (It is really a consequence of an old result of Burnside on permutation representations). This imbedding will ensure that the polynomial $r_L(x)$ annihilates the element of the Burnside ring given by the field extension L. The result for $W(F)$ follows using the ring homomorphism from $\Omega(F)$ to $W(F)$ taking L to the trace form of L.*

Remark 8. *The polynomials $r_L(x)$ will definitely be of lower degree than the polynomials $r_{n,g}(x)$ in very many cases. See [16] for some examples. In particular it is shown that for an irreducible polynomial whose Galois group G is a Sylow 3-subgroup of the symmetric group on 9 letters, and if L is the subfield fixed by a subgroup H of order 9, then $r_L(x) = (x-3)(x-9)$ but that $r_{n,g}(x) = (x-1)(x-3)(x-5)(x-7)(x-9)$. Note that $n = 9$ and $g = 7$ because G contains a 3-cycle but no transpositions. Thus the polynomials $r_L(x)$ improve on the polynomials $r_{n,g}(x)$ since they are divisors of the $r_{n,g}(x)$ but generally will be of lower degree.*

Remark 9. *Also, as suggested in [6], we may exploit Springer's theorem on odd degree extensions, see p46-47 of [18], to sometimes replace $r_L(x)$ by a smaller annihilating polynomial. Specifically we take a maximal odd degree extension M of F where $F \subseteq M \subseteq N$, (here M will correspond to a Sylow 2-subgroup of G). We replace S_L by the set $S_L^{(2)} = \{\phi_E(L) : M \subseteq E \subseteq N\}$, and replace $r_L(x)$ by a polynomial $r_L^{(2)}(x)$ defined like $r_L(x)$ except that we sum over $S_L^{(2)}$ instead of S_L. Springer's theorem ensures that the Witt ring $W(F)$ maps injectively to $W(M)$ and one deduces that the polynomial $r_L^{(2)}(x)$ annihilates the trace form of L in $W(F)$.*

Some recent work by Epkenhans [5],[6], [7] provides a new variation on the subject of annihilating polynomials for quadratic forms. We now describe some of this work.

Let M denote some class of quadratic forms, e.g. we could have M being the class of all forms of dimension n for a fixed value of n, or M being the class of all trace forms of dimension n, or M being the class of all n-fold Pfister forms. Then the *vanishing ideal of* M is the ideal denoted I_M in $\mathbb{Z}[x]$ defined by

$$I_M = \{f(x) \in \mathbb{Z}[x] : f(\phi) = 0 \text{ in } W(F) \text{ for all } \phi \in M \text{ and all fields } F\}$$

If M is the class of all n-fold Pfister forms then I_M is the principal ideal generated by the polynomial $x^2 - 2^n x$. If M is the class of all forms of dimension n then I_M is the principal ideal generated by $p_n(x)$. If M is the class of all trace forms of dimension n then I_M is the principal ideal generated by $q_n(x)$. In view of these examples it is natural to seek a class M of forms such that I_M is the principal ideal generated by the Beaulieu-Palfrey polynomials $r_{n,g}(x)$. Given a finite group G and subgroup H the class $M(G,H)$ is defined by Epkenhans as the class of all quadratic forms ϕ satisfying the following:

(i) there is a separable irreducible polynomial $f(t)$ in $F[t]$ with Galois group G,

(ii) the action of G on the roots of $f(t)$ is equivalent to the action of G on the cosets G/H,

(iii) ϕ is isometric to the trace form of the field extension $L = F[t]/(f(t))$ of F.

Note that the action of G on G/H is necessarily faithful for (ii) to hold so that we are implicitly restricting ourselves to faithful actions.

If n is the degree of $f(t)$ and g is the Galois number of G one might hope that $I_{M(G,H)}$ is generated by the polynomial $r_{n,g}(x)$. However this is not the case in general since for any Galois extension of odd degree n the trace form will be $n \times \langle 1 \rangle$, see [3], so that $x - n \in I_{M(G,H)}$ but is not a multiple of $r_{n,g}(x)$ unless $g = 1$.

In order to investigate $I_{M(G,H)}$ Epkenhans introduced the *signature polynomials*

$$q_{G,H}(x) = \prod_{k \varepsilon S}(x - k)$$

where S is defined as follows;

For any element $\sigma \epsilon G$ we let $\text{sign}_\sigma \chi_H$ = number of fixed points of the subgroup $\langle\sigma\rangle$ acting on G/H, and then S is the set of all values of $\text{sign}_\sigma \chi_H$ as σ runs through all elements of G of order at most two. One might hope that $I_{M(G,H)} = (q_{G,H})$ but this is not the case. In [6] Epkenhans gives an example of a group G, subgroup H, and field extension L whose trace form is not annihilated by $q_{G,H}(x)$. The group G in his example is one which has a Sylow 2-subgroup isomorphic to the quaternion group of order 8. However Epkenhans does show in [5] that, in general, there exists a natural number l,depending only on G and H, such that

$$(2^l q_{G,H}(x)) \subseteq I_{M(G,H)} \subseteq (q_{G,H}).$$

Let L be the field described earlier in the definition of the class $M_{G,H}$. It can be shown that the values of $\text{sign}_\sigma \chi_H$ all occur in the set S_L since the integer $\phi_E(L)$ in S_L may be equivalently defined as the number of fixed points of the subgroup U of G acting on G/H. (Here U is the subgroup of G corresponding to the subfield E under the Galois correspondence). Hence the polynomials $q_{G,H}(x)$ will divide the polynomials $r_L(x)$. In the example of Remark 8 it is easy to see that $q_{G,H}(x) = x - 9$. Indeed whenever the index n of H in G is odd we see that $q_{G,H}(x) = x - n$.

REFERENCES

[1] Pat Beaulieu and Tommy Palfrey, The Galois number, Math. Annalen **309,** 81-96, (1997).

[2] P.E. Conner, unpublished preprint (1987).

[3] P.E. Conner and R. Perlis, A survey of trace forms of algebraic number fields, World Scientific, Singapore, (1984).

[4] A. Dress, Notes on the theory of representations of finite groups, unpublished notes, Bielefeld, (1971).

[5] Martin Epkenhans, On vanishing theorems for trace forms, Acta Mathematica et Informatica Universitatis Ostraviensis **6,** 69-85, (1998).

[6] Martin Epkenhans, On trace forms and the Burnside ring, (Proc. 1999 Dublin conference on "Quadratic Forms and their Applications"), to appear in A.M.S. Contemporary Mathematics series.

[7] Martin Epkenhans, An analogue of Pfister's Local-Global Principle in the Burnside ring, Journal de Théorie des Nombres de Bordeaux **11** (1999), 31-44.

[8] M. Epkenhans and O. Gerstengarbe, On the Galois number of doubly transitive groups, preprint, (1998).

[9] Jurgen Hurrelbrink, Annihilating polynomials for group rings and Witt rings, Canadian Math. Bull. **32** (2), 412 -416, (1989).

[10] M. Knebusch, A. Rosenberg, and R. Ware, Structure of Witt rings and quotients of abelian group rings, American J. Math. **94,** 119-155, (1972),

[11] D.W. Lewis, Witt rings as integral rings, Inventiones Math. **90,** 631-633, (1987).

[12] D.W. Lewis, New proofs of the structure theorems for Witt rings, Expositiones Math.**7**, 83-88, (1989).

[13] D.W. Lewis, Annihilating polynomials and positive forms, Canadian Math.Bull. **35** (1), 103-107, (1992).

[14] David W. Lewis and Sean McGarraghy, Annihilating polynomials, étale algebras, trace forms, and the Galois number, (to appear in Archiv der Math.).

[15] Sean Mc Garraghy, Exterior powers of symmetric bilinear forms, (in preparation).

[16] Sean McGarraghy, Annihilating polynomials, trace forms, and the Galois number, (to appear in Bull. Irish Math. Soc.)

[17] Veerle Ongenae and Jan Van Geel, Polynomials annihilating the Witt ring, Math. Nachr. **185**, 213-226, (1997).

[18] W. Scharlau, Quadratic and hermitian forms, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo (1985).

[19] A. Sladek, Witt rings of skew fields, Prace Naukowa, Uniwersytet Slaski, Katowice, (1989).

[20] E. Witt, Theorie der quadratischen Formen in Beliebigen Korpern, J. Reine Angew. Math. **176**, 31-44, (1937).

Address

Department of Mathematics,

University College Dublin,

Belfield,

Dublin 4,

Ireland