Annihilating polynomials for quadratic forms and Stirling numbers of the second kind

Stefan De Wannemacker

August 4, 2005

Abstract

We present a set of generators of the full annihilator ideal for the Witt ring of an arbitrary field of characteristic unequal to two satisfying a non-vanishing condition on the powers of the fundamental ideal in the torsion part of the Witt ring. This settles a conjecture of Ongenae and Van Geel. This result could only be proved by first obtaining a new lower bound on the 2-adic valuation of Stirling numbers of the second kind.

1 Introduction

In 1937, Witt already observed that the Witt ring was integral in the sense that each element was annihilated by a monic integer polynomial. Fifty years later, in 1987, Lewis was the first to give explicit examples of such polynomials [4]. He showed that the monic polynomial, $p_n(X)$, defined as

$$p_n(X) = (X - n)(X - (n - 2)) \dots (X + (n - 2))(X + n)$$

annihilates every non-singular quadratic form of dimension n over every field F of characteristic unequal to two.
Since then, many other polynomials in $\mathbb{Z}[X]$ were found annihilating all or a family of classes of nonsingular quadratic forms in the Witt ring and we refer the reader to [3] for a nice survey of the main results on this topic.

Let F be a field of characteristic not 2. The object we want to consider here is the torsion annihilator ideal

$$A_t(F) = \{f(X) \in \mathbb{Z}[X] \mid f(\phi) = 0, \ \forall \ \phi \in I_t(F)\}$$

where $I_t(F) = W_t(F) \cap I(F)$, $W_t(F)$ the torsion part of the Witt ring and $I(F)$ the ideal of all even-dimensional forms in the Witt ring. Since $A_t(F)$ is an ideal in the noetherian ring $\mathbb{Z}[X]$, it is finitely generated. The main problem is to find a set of generators for this ideal.
We will prove the following result.

For fields F satisfying the conditions that $2^r W_t(F) = 0$ and $2^{r-1}(I_t(F))^{2k-1} \neq 0$ with k uniquely determined by r, the torsion annihilator ideal $A_t(F)$ is the ideal *generated by the monomials*

$$\{2^{r-\nu_2((2i)!)}X^{2i}\}_{0\leq i\leq k-1} \;\cup\; \{X^{2k}\},$$

where ν_2 denotes the 2-adic valuation function.

In the case of a nonreal field F this theorem was conjectured (see Corollary 3.4) by Ongenae and Van Geel [5]. They gave a proof for fields with level $s(F) \leq 16$ and using the same technique, you can check that the theorem holds for all nonreal fields F with level $s(F) \leq 64$, but a general method was lacking.
The general method, used to prove the theorem, consists in evaluating a polynomial $f(X) \in \mathbb{Z}[X]$ in the even-dimensional forms $\perp_{i=1}^{n} \langle\langle a_i \rangle\rangle$ with $1 \leq n \leq deg(f)$. This evaluation can be rewritten as a linear combination of sums of m-fold Pfister forms and the coefficients that appear turn out to be related to the Stirling numbers of the second kind.
The result about the (torsion) annihilator ideal could only be proved by first obtaining a new lower bound for the 2-adic valuation of all Stirling numbers $S(n, k)$ of the second kind, namely

$$\nu_2(S(n,k)) \geq d(k) - d(n), \quad \text{for} \quad 0 \leq k \leq n$$

where $d(k)$ the sum of the binary digits in the binary representation of k.

2 Stirling numbers of the second kind

2.1 Preliminaries

Let $n \in \mathbb{N}$. The Stirling numbers $S(n, k)$ ($k \in \mathbb{N}$) of the second kind are given by

$$x^n = \sum_{k=0}^{\infty} S(n,k)(x)_k,$$

where $(x)_k = x(x-1)(x-2)\ldots(x-k+1)$ for $k \in \mathbb{N}\setminus\{0\}$ and $(x)_0 = 1$. Actually $S(n, k)$ is the number of ways in which it is possible to partition a set with n elements in k classes.
The Stirling numbers of the second kind can be defined in several ways.

Proposition 2.1.

$$\begin{aligned}
S(n,k) &= \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{k-i}(k-i)^n,\\
S(n,k) &= S(n-1,k-1) + kS(n-1,k)\\
&\qquad \textit{with}\;\; S(n,0) = S(0,k) = 0 \;\; \textit{and} \;\; S(0,0) = 1\\
S(n,k) &= \frac{1}{k!}\sum_{n_1,n_2,\ldots,n_k}\binom{n}{n_1,n_2,\ldots n_k},\\
&\qquad \textit{where } n_1, n_2, \ldots, n_k \textit{ are non-zero and their sum equals } n.
\end{aligned}$$

Proof.
See [1] and [6].

□

2.2 2-adic valuation of Stirling numbers of the second kind

The 2-adic valuation of Stirling numbers of the second kind and other combinatorial numbers has been widely studied, but many problems in this area are still unsolved. We will give a new lower bound for the 2-adic valuation of all Stirling numbers of the second kind.

Denote by $d(n)$ the sum of the digits in the binary representation of n and define the 2-adic valuation function $\nu_2(n)$ for all non-zero integers n by $\nu_2(n) = p$, where $2^p|n$ and $2^{p+1} \nmid n$.
Recall the following properties.

$$\nu_2(n!) = n - d(n) \qquad \text{(Legendre)}$$
$$\nu_2\left(\binom{n}{k}\right) = d(k) + d(n-k) - d(n) \qquad \text{(Kummer)}$$

for all $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.
A new lower bound on the 2-adic valuation of Stirling numbers of the second kind can be obtained as follows.

Theorem 2.2. *Let $n, k \in \mathbb{N}$ and $0 \leq k \leq n$. Then*

$$\nu_2\left(S(n,k)\right) \geq d(k) - d(n).$$

Proof.

By induction on n.

For $n = 0$, $\nu_2(S(0,0)) = \nu_2(1) \geq d(0) - d(0)$.

Assume now that the above inequality is true for all $i < n$. We will prove the theorem for n. Note that for $k = 0$ the result is obviously true.
Let $1 \leq k \leq n$. The Stirling numbers of the second kind satisfy the well-known 'vertical' recurrence relation

$$S(n,k) = \sum_{i=k-1}^{n-1} \binom{n-1}{i} S(i, k-1).$$

Combining this with the 'triangular' recurrence relation

$$S(n,k) = S(n-1,k-1) + kS(n-1,k)$$

we obtain

$$kS(n,k) = \sum_{i=k-1}^{n-1} \binom{n}{i} S(i, k-1).$$

Thus

$$\begin{aligned}
\nu_2(kS(n,k)) &= \nu_2\left(\sum_{i=k-1}^{n-1}\binom{n}{i}S(i,k-1)\right)\\
&\geq \min_{k-1\leq i\leq n-1}\{\nu_2\left(\binom{n}{i}\right)+d(k-1)-d(i)\}\\
&\qquad\qquad\qquad\qquad\text{(by the induction hypothesis)}\\
&= \min_{k-1\leq i\leq n-1}\{d(n-i)+d(k-1)-d(n)\}\\
&\qquad\qquad\qquad\qquad\text{(by the Kummer identity)}\\
&= d(k-1)-d(n)+1.
\end{aligned}$$

So,

$$\begin{aligned}
\nu_2(S(n,k)) &\geq d(k-1)-\nu_2(k)+1-d(n)\\
&= d(k)-d(n).
\end{aligned}$$

□

2.3 Relationship between Stirling numbers of the second kind and quadratic forms

We can evaluate

$$f(X) = c_dX^d + \ldots + c_1X + c_0 \in \mathbb{Z}[X]$$

in classes of quadratic forms $\phi \in W(F)$ by defining

$$f(\phi) = c_d\phi^d \perp \ \ldots \ \perp c_1\phi \perp c_0\langle 1\rangle \ \in W(F)$$

where $c_i\phi = sign(c_i)\underbrace{(\phi \perp \ \ldots \ \perp \phi)}_{|c_i| \text{ times}}$ and $\phi^i = \underbrace{\phi \ \otimes \ \ldots \ \otimes \ \phi}_{i \text{ times}}$.

For arbitrary $k > 0$ and $a_1, a_2, \ldots, a_k \in F^* = F\backslash\{0\}$ denote with $\langle\langle a_1, a_2, \ldots, a_k\rangle\rangle$ the 2^k-dimensional k-fold Pfister form

$$\langle\langle a_1, a_2, \ldots, a_k\rangle\rangle := \langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \langle 1, a_k\rangle.$$

Stirling numbers of the second kind turn up in a natural way by making calculations in the Witt ring.

Proposition 2.3. *Let* $f(X) = c_dX^d + \ldots + c_1X \in \mathbb{Z}[X]$.

Then

$$
\begin{aligned}
f(\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle) = &\left(\sum_{q=1}^{d} 2^{q-1}1!\ S(q,1)c_q\right)(\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle)\\
&\perp \left(\sum_{q=2}^{d} 2^{q-2}2!\ S(q,2)c_q\right)(\perp_{i<j}^{n}\langle\langle a_i, a_j\rangle\rangle)\\
&\perp \ \dots\\
&\perp \left(\sum_{q=n}^{d} 2^{q-n}n!\ S(q,n)c_q\right)\langle\langle a_1,\dots,a_n\rangle\rangle.
\end{aligned}
$$

Proof.

The evaluation of the polynomial $f(X) = c_d X^d + \ldots + c_1 X$ in sums of 1-fold Pfister forms $\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle$ can be written in the following way.

$$
\begin{aligned}
f(\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle) = &A_1(c_1,\dots,c_d)(\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle)\\
&\perp A_2(c_1,\dots,c_d)(\perp_{i<j}^{n}\langle\langle a_i, a_j\rangle\rangle)\\
&\perp \ \dots\\
&\perp A_n(c_1,\dots,c_d)\langle\langle a_1,\dots,a_n\rangle\rangle,
\end{aligned}
$$

where the $A_p(c_1,\dots,c_d)$ are expressions in $c_1,\dots,c_d$ with natural numbers as coefficients, i.e.

$$
A_p(c_1,\dots,c_d) = \sum_{q=1}^{d} \gamma_{p,q} c_q, \quad \text{with} \quad \gamma_{p,q} \in \mathbb{N}.
$$

The natural number $\gamma_{p,q}$ is the coefficient of $\langle\langle a_1,\dots,a_p\rangle\rangle$ in $(\perp_{i=1}^{p}\langle\langle a_i\rangle\rangle)^q$.

For $p \leq q$ we can write

$$
\begin{aligned}
\gamma_{p,q} &= \sum_{q_1,q_2,\dots,q_p\geq 1}^{q_1+q_2+\ldots+q_p=q} \binom{q}{q_1,q_2,\dots,q_p} 2^{q_1-1}2^{q_2-1}\dots\ 2^{q_p-1}\\
&= 2^{q-p} \sum_{q_1,q_2,\dots,q_p\geq 1}^{q_1+q_2+\ldots+q_p=q} \binom{q}{q_1,q_2,\dots,q_p}\\
&= 2^{q-p}p!\,S(q,p).
\end{aligned}
$$

If $p > q$ then clearly no p-fold Pfister form can occur in $(\perp_{i=1}^{p}\langle\langle a_i\rangle\rangle)^q$.
So,

$$
\gamma_{p,q} = \begin{cases} 2^{q-p}p!\,S(q,p) & \text{if} \quad p \leq q,\\ 0 & \text{otherwise.}\end{cases}
$$

Applying this to the coefficients $A_p(c_1,\dots,c_d)$ we obtain

$$\begin{aligned} f(\perp_{i=1}^n \langle\langle a_i\rangle\rangle) = & \left(\sum_{q=1}^{d} 2^{q-1}1!\ S(q,1)c_q\right)(\perp_{i=1}^n \langle\langle a_i\rangle\rangle) \\ & \perp \left(\sum_{q=2}^{d} 2^{q-2}2!\ S(q,2)c_q\right)(\perp_{i<j}^n \langle\langle a_i,a_j\rangle\rangle) \\ & \perp \ \dots \\ & \perp \left(\sum_{q=n}^{d} 2^{q-n}n!\ S(q,n)c_q\right)\langle\langle a_1,\dots,a_n\rangle\rangle. \end{aligned}$$

□

Corollary 2.4. *Let $f(X)=c_dX^d+\ldots+c_1X+c_0\in\mathbb{Z}[X]$ and $\phi \ \simeq\ \langle a_1,a_2,\dots a_n\rangle$ a quadratic form of dimension n. If $f(n):=f(n\langle 1\rangle)=0$ then*

$$\begin{aligned} f(\phi) = & \left(\sum_{q=1}^{d}\sum_{t=q}^{d} 2^{q-1}1!\ S(q,1)\binom{t}{q}(-n)^{t-q}c_t\right)(\perp_{i=1}^n \langle\langle a_i\rangle\rangle) \\ & \perp \left(\sum_{q=2}^{d}\sum_{t=q}^{d} 2^{q-2}2!\ S(q,2)\binom{t}{q}(-n)^{t-q}c_t\right)(\perp_{i<j}^n \langle\langle a_i,a_j\rangle\rangle) \\ & \perp \ \dots \\ & \perp \left(\sum_{q=n}^{d}\sum_{t=q}^{d} 2^{q-n}n!\ S(q,n)\binom{t}{q}(-n)^{t-q}c_t\right)\langle\langle a_1,\dots,a_n\rangle\rangle \end{aligned}$$

Proof.
Note that for all

$$\phi \ \simeq\ \langle a_1,a_2,\dots a_n\rangle$$

we have

$$\phi \ \simeq\ \perp_{i=1}^n \langle\langle a_i\rangle\rangle - n\langle 1\rangle.$$

We can also rewrite $f(X)$ as

$$f(X)=g(X-n)=\sum_{q=1}^{d}\sum_{t=q}^{d}\binom{t}{q}(-n)^{t-q}c_t(X-n)^q.$$

The condition $f(n)=0$ implies that the constant term in $g(Y)$ with $Y=X-n$ vanishes. The result follows from the previous proposition applied to $g(Y)$. □

Lemma 2.5. *Let $f(X)=c_dX^d+\ldots+c_1X\in\mathbb{Z}[X]$. If $f(\perp_{i=1}^k \langle\langle a_{\sigma(i)}\rangle\rangle)=0$, for all $1\le k\le n,\ \sigma\in S_d$ then*

$$\left(\sum_{q=n}^{d} 2^{q-n}n!\ S(q,n)c_q\right)\langle\langle a_{\tau(1)},\dots a_{\tau(n)}\rangle\rangle=0, \quad \textit{for all} \quad \tau\in S_d.$$

Proof.
By induction on n.
For $n = 1$,

$$\begin{aligned}0 &= f(\langle\langle a_i \rangle\rangle)\\ &= c_d \langle\langle a_i \rangle\rangle^d + c_{d-1} \langle\langle a_i \rangle\rangle^{d-1} + \ldots + c_1 \langle\langle a_i \rangle\rangle\\ &= (2^{d-1} c_d + 2^{d-2} c_{d-1} + \ldots + c_1) \langle\langle a_i \rangle\rangle\\ &= \left(\sum_{q=1}^{d} 2^{q-1} 1!\ S(q,1) c_q \right) \langle\langle a_i \rangle\rangle\end{aligned}$$

since $S(q, 1) = 1$ for all $q \geq 1$.
Assume now that the lemma is true for all $i < n$. We will prove the lemma for n.
Let $\sigma \in S_d$.

$$\begin{aligned}0 &= f(\perp_{i=1}^{n} \langle\langle a_{\sigma(i)} \rangle\rangle)\\ &= \left(\sum_{q=1}^{d} 2^{q-1} 1!\ S(q,1) c_q \right) (\perp_{i=1}^{n} \langle\langle a_{\sigma(i)} \rangle\rangle)\\ &\quad \perp \left(\sum_{q=2}^{d} 2^{q-2} 2!\ S(q,2) c_q \right) (\perp_{i<j}^{n} \langle\langle a_{\sigma(i)}, a_{\sigma(j)} \rangle\rangle)\\ &\quad \perp \ldots\\ &\quad \perp \left(\sum_{q=n}^{d} 2^{q-n} n!\ S(q,n) c_q \right) \langle\langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle\rangle\end{aligned}$$

by Proposition 2.3.
Note that for every subset $U \subset \{1, \ldots, d\}$ of $k \leq d$ elements, there exists a permutation $\tau \in S_d$ such that $U = \{\tau(1), \ldots, \tau(k)\}$.
So,

$$\begin{aligned}0 = &\left(\sum_{q=1}^{d} 2^{q-1} 1!\ S(q,1) c_q \right) (\perp_{\tau \in X_1 \subset S_d} \langle\langle a_{\tau(1)} \rangle\rangle)\\ &\perp \left(\sum_{q=2}^{d} 2^{q-2} 2!\ S(q,2) c_q \right) (\perp_{\tau \in X_2 \subset S_d} \langle\langle a_{\tau(1)}, a_{\tau(2)} \rangle\rangle)\\ &\perp \ldots\\ &\perp \left(\sum_{q=n}^{d} 2^{q-n} n!\ S(q,n) c_q \right) \langle\langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle\rangle\\ = &\left(\sum_{q=n}^{d} 2^{q-n} n!\ S(q,n) c_q \right) \langle\langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle\rangle\end{aligned}$$

by the induction hypothesis. ∎

3 Polynomials annihilating the Witt Ring

3.1 Preliminaries

The *fundamental ideal* $I(F)$ of $W(F)$ is the ideal consisting of all even dimensional forms of $W(F)$. Put $I_t(F) := I(F) \cap W_t(F)$.
A field F is called *nonreal* if -1 is a sum of squares in F. The natural number

$$s(F) := min\{n \in \mathbb{N} \,|\, a_1^2 + a_2^2 + \ldots + a_n^2 = -1,\ a_i \in F\}$$

is called the *level* of F.
A field F is called *(formally) real* if -1 is not a sum of squares in F. In this case we define the level $s(F) = \infty$.
It is a well-known fact that $s(F)$ is a power of two, if F is nonreal ([7] or [2]).
The *height* of F is the smallest two-power $h(F) = 2^d$ such that $2^d W_t(F) = 0$.
If no such power exists then $h(F) := \infty$. If F is nonreal then $h(F) = 2s(F)$.

We define the *torsion annihilator ideal* $A_t(F)$ in $\mathbb{Z}[X]$ by

$$A_t(F) = \{f(X) \in \mathbb{Z}[X] \,|\, f(\varphi) = 0 \text{ for all } \varphi \in I_t(F)\}.$$

For F nonreal, define the *full annihilator ideal* $A(F)$ in $\mathbb{Z}[X]$ by

$$A(F) = \{f(X) \in \mathbb{Z}[X] \,|\, f(\varphi) = 0 \text{ for all } \varphi \in W(F)\},$$

the *even annihilator ideal* by

$$A_e(F) = \{f(X) \in \mathbb{Z}[X] \,|\, f(\varphi) = 0 \text{ for all even dimensional } \varphi \in W(F)\}$$

and the *odd annihilator ideal* by

$$A_o(F) = \{f(X) \in \mathbb{Z}[X] \,|\, f(\varphi) = 0 \text{ for all odd dimensional } \varphi \in W(F)\}.$$

In what follows, let $k = k(r)$ be the natural number uniquely determined by $\nu_2((2k-2)!) < r \leq \nu_2((2k)!)$ (see [5]).

We define the ideals

$$\begin{aligned}
J_{e,r} &= (\{2^{r-\nu_2((2i)!)}X^{2i}\}_{0\leq i\leq k-1}) \ + \ (X^{2k}) \\
&= (2^r, 2^{r-1}X^2, 2^{r-3}X^4, ..., 2^{r-\nu_2((2i)!)}X^{2i}, ..., 2^{r-\nu_2((2k-2)!)}X^{2k-2}, X^{2k}), \\
J_{o,r} &= (\{2^{r-\nu_2((2i)!)}(X-1)^{2i}\}_{0\leq i\leq k-1}) \ + \ ((X-1)^{2k}) \\
&= (2^r, 2^{r-1}(X-1)^2, 2^{r-3}(X-1)^4, ..., 2^{r-\nu_2((2i)!)}(X-1)^{2i}, ..., 2^{r-\nu_2((2k-2)!)}(X-1)^{2k-2}, (X-1)^{2k}) \\
&\quad \text{and} \\
J_r &= (\{2^{r-\nu_2((2i)!)}X^{2i}(X-1)^{2i}\}_{0\leq i\leq k-1}) \ + \ (X^{2k}(X-1)^{2k}) \\
&= (2^r, 2^{r-1}X^2(X-1)^2, 2^{r-3}X^4(X-1)^4, ..., \\
&\quad 2^{r-\nu_2((2i)!)}X^{2i}(X-1)^{2i}, ..., 2^{r-\nu_2((2k-2)!)}X^{2k-2}(X-1)^{2k-2}, X^{2k}(X-1)^{2k}).
\end{aligned}$$

Example 3.1.

$$\begin{aligned}
J_{e,1} &= (2, X^2), \\
J_{e,2} &= (4, 2X^2, X^4), \\
J_{e,3} &= (8, 4X^2, X^4), \\
J_{e,4} &= (16, 8X^2, 2X^4, X^6), \\
J_{e,5} &= (32, 16X^2, 4X^4, 2X^6, X^8). \\
J_{e,6} &= (64, 32X^2, 8X^4, 4X^6, X^8).
\end{aligned}$$

3.2 Generators for the full annihilator ideal

Since $\mathbb{Z}[X]$ is noetherian, the ideals $A_e(F), A_o(F), A(F)$ and $A_t(F)$ are finitely generated. Under certain conditions we give a set of generators.
The following lemma is proved in [5]. We will give an alternative proof, using Stirling numbers of the second kind.

Lemma 3.2. *Let F be a field for which $2^r W_t(F) = 0$ then*

$$J_{e,r} \subseteq A_t(F).$$

Proof.
Let $f(X) = 2^{r-\nu_2((2i)!)}X^{2i}$ be one of the generators of $J_{e,r}$ and $\phi \simeq \langle a_1, a_2, \ldots, a_n\rangle$ an arbitrary even dimensional element of $W_t(F)$.
Since n is even, we have $f(n\langle 1\rangle) = 2^{r-\nu_2((2i)!)+2i}\left(\frac{n}{2}\right)^{2i}\langle 1\rangle = 2^{r+d(2i)}\left(\frac{n}{2}\right)^{2i}\langle 1\rangle = 0$.
By Corollary 2.4

$$\begin{aligned}
f(\phi) = &\left(\sum_{q=1}^{d} 2^{q-1}1!\ S(q,1)\binom{2i}{q}(-n)^{2i-q}2^{r-\nu_2((2i)!)}\right)(\perp_{i=1}^{n}\langle\langle a_i\rangle\rangle) \\
\perp &\left(\sum_{q=2}^{d} 2^{q-2}2!\ S(q,2)\binom{2i}{q}(-n)^{2i-q}2^{r-\nu_2((2i)!)}\right)(\perp_{i<j}^{n}\langle\langle a_i, a_j\rangle\rangle) \\
\perp &\ \ldots \\
\perp &\left(\sum_{q=n}^{d} 2^{q-n}n!\ S(q,n)\binom{2i}{q}(-n)^{2i-q}2^{r-\nu_2((2i)!)}\right)\langle\langle a_1, \ldots, a_n\rangle\rangle.
\end{aligned}$$

For all $j \leq q$ we have

$$\begin{aligned}
\nu_2 &\left(2^{q-j} j!\ S(q,j) \binom{2i}{q} (-n)^{2i-q} 2^{r-\nu_2((2i)!)}\right) \\
&= q - j + \nu_2(j!) + \nu_2(S(q,j)) + \nu_2\left(\binom{2i}{q}\right) \\
&\qquad + (2i-q)\nu_2(n) + r - \nu_2((2i)!) \\
&= q - j + j - d(j) + \nu_2(S(q,j)) + d(q) + d(2i-q) - d(2i) \\
&\qquad + (2i-q)\nu_2(n) + r - 2i + d(2i) \\
&\qquad\qquad \text{(by Kummer and Legendre)} \\
&\geq q - d(j) + d(j) - d(q) + d(q) + d(2i-q) \\
&\qquad + (2i-q)\nu_2(n) + r - 2i \\
&\qquad\qquad \text{(by Theorem 2.2)} \\
&\geq q + d(2i-q) + (2i-q) + r - 2i \\
&\qquad\qquad \text{(since } n \text{ is even)} \\
&\geq r
\end{aligned}$$

Since $2^r W_t(F) = 0$ it follows that

$$f(\phi) = 0$$

or equivalently that

$$f(X) \in A_t(F).$$

□

This brings us to the main result of this paper:

Theorem 3.3. *Let F be a field such that $2^r W_t(F) = 0$ and $2^{r-1}(I_t(F))^{2k-1} \neq 0$ with k uniquely determined by $\nu_2((2k-2)!) < r \leq \nu_2((2k)!)$. Then*

$$J_{e,r} = A_t(F).$$

Proof.

Let F be a field such that $2^r W_t(F) = 0$ and $2^{r-1}(I_t(F))^{2k-1} \neq 0$. Let k be the unique natural number such that $\nu_2((2k-2)!) < r \leq \nu_2((2k)!)$.

Since $X^{2k} \in J_{e,r}$ annihilates every even quadratic form, we will have to prove that every polynomial of degree $2k-1$,

$$f(X) = c_{2k-1}X^{2k-1} + ... + c_1 X + c_0, \text{ with } c_i \in \mathbb{Z},$$

annihilating every even quadratic torsion form, lies in $J_{e,r}$.

$I_t(F)$ is generated by the elements $\langle\langle a\rangle\rangle \in I_t(F)$. The condition on the power of the fundamental ideal implies the existence of elements $a_1, \ldots, a_{2k-1} \in F^*$ such that the form $2^{r-1}\langle\langle a_1, \ldots, a_{2k-1}\rangle\rangle$ is not zero.
Fix such elements.

We will evaluate the polynomial $f(X)$ in the even quadratic forms of the form

$$\perp_{i=1}^{n} \langle\langle a_{\sigma(i)}\rangle\rangle$$

where $1 \le n \le 2k-1,\ \sigma \in S_{2k-1}$.

Since $f(0) = c_0\langle 1\rangle$ has to vanish and $2^r W_t(F) = 0$, it follows that $c_0 = b_0 2^r$ for some $b_0 \in \mathbb{Z}$. By Lemma 2.5 we get the following set of equations in the Witt ring:

$$\left(\sum_{q=n}^{2k-1} 2^{q-n} n!\ S(q,n) c_q\right) \langle\langle a_1, \ldots a_n\rangle\rangle = 0,\ 1 \le n \le 2k-1. \tag{1}$$

For $n = 2k-1$, this becomes

$$\begin{aligned} 0 =& (2k-1)!\ S(2k-1, 2k-1) c_{2k-1} \langle\langle a_1, \ldots, a_{2k-1}\rangle\rangle \\ =& (2k-1)!\ c_{2k-1} \langle\langle a_1, \ldots, a_{2k-1}\rangle\rangle. \end{aligned}$$

Since

$$2^{r-1}\langle\langle a_1, \ldots, a_{2k-1}\rangle\rangle \ne 0,$$

and $2^r W_t(F) = 0$ it follows that

$$(2k-1)!\ c_{2k-1} = b_{2k-1} 2^r \quad \text{for some } b_{2k-1} \in \mathbb{Z},$$

and since $\nu_2((2k-1)!) = \nu_2((2k-2)!) < r$ that

$$c_{2k-1} = 2^{r-\nu_2((2k-1)!)} b_{2k-1} \quad \text{for some } b_{2k-1} \in \mathbb{Z}.$$

For $n = 2k-2$, (1) becomes

$$((2k-2)!\ c_{2k-2} + 2(2k-2)!\ S(2k-1, 2k-2) c_{2k-1}) \langle\langle a_1, \ldots, a_{2k-1}\rangle\rangle = 0. \tag{2}$$

The second term $2(2k-2)!S(2k-1,2k-2)c_{2k-1}\langle\langle a_1,\ldots,a_{2k-2}\rangle\rangle$ vanishes since

$$\begin{aligned}
\nu_2(2(2k-2)!\ S(2k-1,2k-2)c_{2k-1}) &= 1+\nu_2((2k-2)!) \\
&\quad +\nu_2(S(2k-1,2k-2))+\nu_2(c_{2k-1}) \\
&= 1+2k-2-d(2k-2) \\
&\quad +\nu_2(S(2k-1,2k-2))+\nu_2(c_{2k-1}) \\
&\qquad\qquad \text{(by Legendre)} \\
&\geq 2k-1-d(2k-2) \\
&\quad +d(2k-2)-d(2k-1)+\nu_2(c_{2k-1}) \\
&\qquad\qquad \text{(by Theorem 2.2)} \\
&\geq 2k-1-d(2k-1)+r-(2k-1)+d(2k-1) \\
&= r
\end{aligned}$$

and $2^r W_t(F) = 0$.

Equation (2) is thus equivalent to

$$(2k-2)!\ c_{2k-2}\langle\langle a_1,\ldots,a_{2k-2}\rangle\rangle = 0$$

and it follows, since $\nu_2((2k-2)!) = \nu_2((2k-1)!) < r$ that

$$c_{2k-2} = 2^{r-\nu_2((2k-2)!)}b_{2k-2} \quad \text{for some } \ b_{2k-2}\in\mathbb{Z}.$$

Using the same technique and observing that

$$\begin{aligned}
\nu_2(2^{q-n}n!\ S(q,n)c_q) &= q-n+\nu_2(n!)+\nu_2(S(q,p))+\nu_2(c_q) \\
&= q-d(n)+\nu_2(S(q,n))+\nu_2(c_q) \\
&\qquad \text{(by Legendre)} \\
&\geq q-d(n)+d(n)-d(q)+r-q+d(q) \\
&\qquad \text{(by Theorem 2.2)} \\
&= r
\end{aligned}$$

for all $n<q$ and that $\nu_2(n!) < r$ for all $1\leq n\leq 2k-1$, the set of equations (1) is equivalent to the set of equations

$$n!\ c_n\langle\langle a_1,\ldots,a_n\rangle\rangle = 0\ ,\ \text{where } n = 1,\ldots,2k-1.$$

The solutions are,

$$c_n = 2^{r-\nu_2(n!)}b_n \quad \text{for some } \ b_n\in\mathbb{Z}.$$

We can thus rewrite,

$$f(X) = c_{2k-1}X^{2k-1}+\ldots+c_1X+c_0$$

as

$$
\begin{aligned}
f(X) &= 2^{r-\nu_2((2k-1)!)}b_{2k-1}X^{2k-1} + 2^{r-\nu_2((2k-2)!)}b_{2k-2}X^{2k-2} + \\
&\quad \ldots + 2^{r-\nu_2((2j+1)!)}b_{2j+1}X^{2j+1} + b_{2j}2^{r-\nu_2((2j)!)}X^{2j} + \ldots + 2^{r-\nu_2(1!)}b_1X + 2^{r-\nu_2(0!)}b_0 \\
&= 2^{r-\nu_2((2k-2)!)}X^{2k-2}(b_{2k-1}X + b_{2k-2}) + \ldots + 2^{r-\nu_2((2j)!)}X^{2j}(b_{2j+1}X + b_{2j}) + \ldots + 2^r(b_1X + b_0)
\end{aligned}
$$

or equivalently,

$$f(X) \in J_{e,r}$$

i.e.

$$A_t(F) \subset J_{e,r}$$

and using the other inclusion of the previous lemma

$$A_t(F) = J_{e,r}.$$

□

Corollary 3.4. *Let F be a nonreal field of finite level $s(F) = 2^{r-1}$ such that $s(F)(I(F))^{2k-1} \neq 0$, where $k = k(r)$ is uniquely determined by $\nu_2((2k-2)!) < r \leq \nu_2((2k)!)$. Then*

$$A(F) = J_r.$$

Proof. Since $s(F) = 2^{r-1}$, we have that $2^r W(F) = 0$. Moreover, if F is a nonreal field, $I_t(F) = I(F)$. The non-vanishing condition on the power of the fundamental ideal implies that

$$A_e(F) = J_{e,r}.$$

If ϕ is an odd-dimensional form in $W(F)$, then $\phi \perp -\langle 1 \rangle$ is an even-dimensional form in $W(F)$. This implies that

$$A_o(F) = J_{o,r}.$$

And finally, since $J_{e,r}$ and $J_{o,r}$ are comaximal ideals, we get

$$A(F) = A_e(F) \cap A_o(F) = J_{e,r} \cap J_{o,r} = J_{e,r} \cdot J_{o,r} = J_r.$$

□

Corollary 3.5. *Let F be a real field of finite height $h(F) = 2^r$ such that $\frac{1}{2}h(F)(W_t(F))^{2k-1} \neq 0$, where $k = k(r)$ is uniquely determined by $\nu_2((2k-2)!) < r \leq \nu_2((2k)!)$. Then*

$$A_t(F) = J_{e,r}.$$

Proof. By the definition of the height $h(F) = 2^r$, we have that $2^r W(F) = 0$. Moreover, if F is a real field, $I_t(F) = W_t(F)$. The non-vanishing condition on the power of the torsion ideal implies that

$$A_t(F) = J_{e,r}.$$

□

Remark 3.6. *In [5], examples are given of non-real fields F satisfying the conditions of Corollary 3.4.*
Examples of real fields of arbitrary height $h(F) = 2^r$ satisfying the conditions of Corollary 3.5 can be found. These results will be published later.

Remark 3.7. *One can show that, for a field F, satisfying $2^r W(F) = 0$, but not satisfying the non-vanishing condition $2^{r-1}(I_t(F))^{2k-1} \neq 0$, the torsion annihilator ideal $A_t(F)$ always differs from $J_{e,r}$.*
A set of generators for the ideal $A_t(F)$ in these cases is, in general, not known.

References

[1] R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics, a foundation for computer science, (Addison Wesley, 1989).

[2] T. Y. Lam, The algebraic theory of quadratic forms, (Reading Mass., 1973).

[3] D. W. Lewis, Annihilating polynomials for quadratic forms, IJMMS **27**, No. 7, 449–455 (2001).

[4] D. W. Lewis, Witt Rings as Integral Rings, Invent. Math. **90**, 631–633 (1987).

[5] V. Ongenae, J. Van Geel, Polynomials Annihilating the Witt Ring, Math. Nachr. **185**, 213–226 (1997).

[6] J. Riordan, Combinatorial Identities, (Krieger, 1979).

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

Stefan De Wannemacker
Department of Mathematics
University College Dublin
Belfield, Dublin
Ireland
e-mail: sdwannem@maths.ucd.ie