Generators and relations for $W_q(K)$ in characteristic 2

Jón Kr. Arason

RH-18-2006

Science Institute
University of Iceland
Dunhaga 3, IS 107 Reykjavík

jka@hi.is

December 2006

The purpose of this note is to prove the following theorem describing the Witt group $W_q(K)$ of quadratic forms over a field K of characteristic 2 in terms of generators and relations.

Theorem: $W_q(K)$ is generated by the $[a,b]$, $a,b \in K$, such that $[a,b]$ is biadditive as a function of a and b and such that

(I) $[a, br^2] = [ar^2, b]$ for all $a, b, r \in K$.

(II) $[a, ar^2 + r] = 0$ for all $a, r \in K$.

In [Arason] there was given a presentation of $W_q(K)$ as a module over the Witt ring $W(K)$ of symmetric bilinear forms over K. This was used in [Kato] to give a presentation of $W_q(K)$ that can be seen to be essentially equivalent to the one in the theorem. Here we give a direct elementary proof.

In this note K always is a field of characteristic 2. We shall assume that the reader is familiar with the basic facts about quadratic forms over such a field. These can be found in [Scharlau], Chapter 1.6 and Chapter 9.4, and (with some proofs missing) in [SBF], Appendix 1, and also in [Baeza]. All the relevant facts are already in the fundamental paper [Arf].

We shall, however, need some more elementary facts about such forms. For a lack of suitable references we shall start by gathering some. The proofs needed are easy but included for completeness. As usual, for elements a and b in K the quadratic form on K^2, $(x,y) \mapsto ax^2 + xy + by^2$, is denoted by $[a,b]$. In particular, $[0,0]$ is the hyperbolic plane. But, obviously, every $[a,0]$ and every $[0,b]$ is isomorphic to the hyperbolic plane. (For example, $ax^2 + xy = uv$, where $u = x$ and $v = ax + y$.) We shall use $\cong$ to denote isomorphism of quadratic form but $\sim$ for Witt equivalence.

Fact 1: For any r in K we have

$$[ar^2, b] \cong [a, br^2]$$

Proof: If $r = 0$ both sides are isomorphic to the hyperbolic plane. If $r \neq 0$ then $ar^2x^2 + xy + by^2 = au^2 + uv + br^2v^2$, where $u = rx$ and $v = r^{-1}y$.

Fact 2: For any r in K we have

$$[a,b] \cong [a, ar^2 + r + b]$$

Proof: Writing $x = u + rv$ and $y = v$ we have $ax^2 + xy + by^2 = au^2 + uv + (ar^2 + r + b)v^2$.

Fact 3: Assume that $[a,b] \cong [c,d]$. Then there is an r in K such that

$$[a,b] \cong [cr^2,b] \cong [c,br^2] \cong [c,d]$$

Proof: The hypotesis implies that there are s and t in K, not both equal 0, such that $b = cs^2 + st + dt^2$.

If $t \neq 0$ we take $r = t^{-1}$ and get $br^2 = c(sr)^2 + (sr) + d$. If $t = 0$ we take $r = ds^{-1}$ and get $br^2 = cd^2 + d + d$. In both cases the third isomorphism therefore follows from Fact 2. The second one holds by Fact 1 and the first one then follows from the hypothesis.

Fact 4: We have

$$[a,b] \oplus [a,c] \sim [a,b+c]$$

Proof: Writing $x = x_1 + u$ and $v = y + v_1$ we get $ax^2 + xy + bx^2 + au^2 + uv + cv^2 = ax_1^2 + x_1y + (b+c)y^2 + uv_1 + cv_1^2$. This shows that $[a,b] \oplus [a,c] \cong [a,b+c] \oplus [0,c]$. As $[0,c]$ is hyperbolic the result follows.

We now turn to the proof of the theorem. For that we let N be the subgroup of $K \otimes K := K \otimes_{\mathbf{Z}} K$ generated by all elements of the form
(I) $a \otimes br^2 - ar^2 \otimes b$ for $a, b, r \in K$.
(II) $a \otimes (ar^2 + r)$ for $a, r \in K$.
We then let $M = (K \otimes K)/N$.

For $a, b \in K$ we denote by $\lfloor a, b \rfloor$ the class of $a \otimes b$ in M. We then can rewrite (I) and (II) as
(I) $\lfloor a, br^2 \rfloor = \lfloor ar^2, b \rfloor$ for all $a, b, r \in K$.
(II) $\lfloor a, ar^2 + r \rfloor = 0$ for all $a, r \in K$.
We refer to these equations as relations of type (I) and type (II), respectively.
Remark: As $\mathrm{char}(K) = 2$, K is in fact a vector space over $\mathbf{F}_2$ and hence $K \otimes K$ can also be interpreted as $K \otimes_{\mathbf{F}_2} K$. In particular, M is a 2-torsion group. Let $K_0 = \{\, x^2 \mid x \in K \,\}$, which is a subfield of K. The relations of type (I) then simply mean that the natural projection $K \otimes K \to M$ factors through $K \otimes_{K_0} K$. So M can also be described as the quotient of $K \otimes_{K_0} K$ by the subgroup generated by all $a \otimes_{K_0} (ar^2 + r)$ with $a, r \in K$.
Remark: In some applications it seems nicer to use relations of the type $\lfloor a, br^2 \rfloor = \lfloor b, ar^2 \rfloor$ instead of relations of type (I). (Also that gives an easier proof of the symmetry of $\lfloor a, b \rfloor$.)

It is well know (cf. [Arf]) that $W_q(K)$ is additively generated by the $[a,b] \in W_q(K)$. (We shall, as is common, use the notation $[a,b]$ also for the class in $W_q(K)$ of the form $[a,b]$. The correct meaning will hopefully be clear from the context.) From Fact 4 above (and the symmetry of $[a,b]$) it follows that $[a,b]$ is biadditive as a function of a and b. From Fact 1 and Fact 2 above it follows that $[a,br^2]=[ar^2,b]$ and $[a,ar^2+r]=0$ for every $a,b,r\in K$. We therefore have a group epimorphism $M\to W_q(K)$ mapping each generator $\lfloor a,b\rfloor$ of M to $[a,b]$ in $W_q(K)$. We call it the canonical morphism $M\to W_q(K)$.

Step 1: $\lfloor a,b\rfloor=\lfloor b,a\rfloor$ for every $a,b\in K$.

Proof: By letting $a=c$ and $r=1$ in relations of type (II), we get that $\lfloor c,c+1\rfloor=0$, i.e., $\lfloor c,c\rfloor=\lfloor c,1\rfloor$ for every $c\in K$. In particular, $\lfloor a+b,a+b\rfloor=\lfloor a+b,1\rfloor=\lfloor a,1\rfloor+\lfloor b,1\rfloor$. But we also get that $\lfloor a+b,a+b\rfloor=\lfloor a,a\rfloor+\lfloor a,b\rfloor+\lfloor b,a\rfloor+\lfloor b,b\rfloor=\lfloor a,1\rfloor+\lfloor a,b\rfloor+\lfloor b,a\rfloor+\lfloor b,1\rfloor$. Comparing these two expressions for $\lfloor a+b,a+b\rfloor$, we see that $\lfloor a,b\rfloor+\lfloor b,a\rfloor=0$, i.e., that $\lfloor a,b\rfloor=\lfloor b,a\rfloor$.

Step 2: If $[a,b]$ is isotropic then $\lfloor a,b\rfloor=0$.

Proof: By hypothesis, there are $r,s\in K$, not both 0, such that $ar^2+rs+bs^2=0$. If $a=0$ then, of course, $\lfloor a,b\rfloor=0$. So we may assume that $a\neq 0$. But then $s\neq 0$ and we may, because of the homogenity of the equation, assume that $s=1$. Then we have $ar^2+r+b=0$, i.e., $b=ar^2+r$, so $\lfloor a,b\rfloor=0$ by the relations of type (II).

Step 3: If $[a,b]\cong[c,d]$ then $\lfloor a,b\rfloor=\lfloor c,d\rfloor$.

Proof: Because of Fact 3, relations of type (I) and Step 1 we may assume that $c=a$. But, by the Cancellation Theorem for quadratic forms over K (cf. [Arf]), $[a,b]\cong[a,d]$ implies that $[a,b-d]$ is hyperbolic. By Step 2 we then get $\lfloor a,b-d\rfloor=0$, hence $\lfloor a,b\rfloor=\lfloor a,d\rfloor$.

Step 4: The canonical morphism $M\to W_q(K)$ is an isomorphism.

Proof: We only have to show that this morphism is injective. To do that we have to show that if $\bigoplus_i[a_i,b_i]$ is hyperbolic then $\sum_i\lfloor a_i,b_i\rfloor=0$ in M. By induction on the number of summands, it suffices to show that if $\bigoplus_{i=1}^n[a_i,b_i]$ is isotropic then there are $c_1,\dots,c_{n-1},d_1,\dots,d_{n-1}\in K$ such that $\sum_{i=1}^n\lfloor a_i,b_i\rfloor=\sum_{i=1}^{n-1}\lfloor c_i,d_i\rfloor$ in M. The case $n=1$ is given by Step 2, so we assume $n>1$. By the induction assumption, we may assume that all the $[a_i,b_i]$ are anisotropic. Then there are c_i, each c_i a value of $[a_i,b_i]$, not all $c_i=0$, such that $c_1+\cdots+c_n=0$. By the induction assumption, we may assume that all $c_i\neq 0$. Then $[a_i,b_i]=[c_i,d_i]$ for some $d_i\in K$, hence $\lfloor a_i,b_i\rfloor=\lfloor c_i,d_i\rfloor$ by Step 3. To complete the proof it therefore suffices to show that $\lfloor c_{n-1},d_{n-1}\rfloor+\lfloor c_n,d_n\rfloor=\lfloor c_{n-1}+c_n,d'_{n-1}\rfloor+\lfloor c'_n,d'_n\rfloor$ for some $d'_{n-1},c'_n,d'_n\in$

K. But we have in general, by the biadditivity of the symbol $\lfloor a,b \rfloor$, that $\lfloor a+a', b\rfloor + \lfloor a', b+b'\rfloor = \lfloor a,b\rfloor + \lfloor a',b\rfloor + \lfloor a',b\rfloor + \lfloor a',b'\rfloor = \lfloor a,b\rfloor + \lfloor a',b'\rfloor$. In particular, $\lfloor c_{n-1}+c_n, d_{n-1}\rfloor + \lfloor c_n, d_{n-1}+d_n\rfloor = \lfloor c_{n-1}, d_{n-1}\rfloor + \lfloor c_n, d_n\rfloor$.

This concludes the proof of the theorem. We now shall give some consequences.

Let $W(K)$ be the Witt ring of symmetric bilinear forms over K and let $I(K)$ be the fundamental ideal of $W(K)$. Then $W_q(K)$ is a $W(K)$-module in a natural way. In particular, we have the subgroups $I^nW_q(K) := I(K)^nW_q(K)$ of $W_q(K)$. (For this, see [Scharlau], [SBF], or [Baeza].)

Recall that $\wp(K)$ is the additive subgroup $\{\, r^2+r \mid r \in K \,\}$ of K. The Arf invariant $\Delta : W_q(K) \to K/\wp(K)$ is an epimorphism that maps the generator $[a,b]$ to $ab + \wp(K)$. It is well known that its kernel equals $IW_q(K)$.

Clearly, by $d + \wp(K) \mapsto [1,d]$ there is given a right inverse to the Arf invariant. It follows that $W_q(K)$ is the direct sum of the subgroup $\{\,[1,d] \mid d \in K\,\}$ and $IW_q(K)$. In particular, $IW_q(K)$ is isomorphic to the quotient of $W_q(K)$ by this subgroup.

If $a \neq 0$ then $\langle a\rangle[1,d] = [a, \frac{d}{a}]$ in $W_q(K)$. It follows that $\langle 1,a\rangle[1,d] = [1,d] + [a,\frac{d}{a}]$. Writing $d = ab$ the right hand side becomes $[1,ab] + [a,b]$. As this equals 0 if $a = 0$, we conclude that $IW_q(K)$ is generated by the $[[a,b]] := [1,ab] + [a,b]$ with $a,b \in K$. Using our representation of $W_q(K)$ above and that $IW_q(K)$ is isomorphic to the quotient of $W_q(K)$ described above, we get the following representation of $IW_q(K)$.

Corollary 1: $IW_q(K)$ is generated by the $[[a,b]]$, $a,b \in K$, such that $[[a,b]]$ is biadditive as a function of a and b and such that

(0) $[[1,a]] = 0$ for all $a \in K$.

(I) $[[a,br^2]] = [[ar^2,b]]$ for all $a,b,r \in K$.

(II) $[[a,ar^2+r]] = 0$ for all $a,r \in K$.

If $a,b \neq 0$ then we get as above that $\langle 1,a\rangle\langle 1,b\rangle[1,d] = [1,d] + [a,\frac{d}{a}] + [b,\frac{d}{b}] + [ab,\frac{d}{ab}]$. Writing $d = abc$, the right hand side becomes $[1,abc] + [a,bc] + [b,ac] + [ab,c]$. Denoting this by $[[a,b,c]]$, and noting that this is trivial if $a = 0$ or $b = 0$, we see that $I^2W_q(K)$ is generated by the $[[a,b,c]]$ with $a,b,c \in K$.

As $[1,abc] + [1,abc] = 0$, we can write $[[a,b,c]] = [[a,bc]] + [[b,ac]] + [[ab,c]]$. Denoting by $((a,b))$ the class of $[[a,b]]$ in $IW_q(K)/I^2W_q(K)$, we get the following representation of this quotient.

Corollary 2: $IW_q(K)/I^2W_q(K)$ is generated by the $((a,b))$, $a,b \in K$, such that $((a,b))$ is biadditive as a function of a and b and such that

(0) $((1,a)) = 0$ for all $a \in K$.

(I) $((a,br^2)) = ((ar^2,b))$ for all $a,b,r \in K$.

(II) $((a,ar^2+r)) = 0$ for all $a,r \in K$.

(III) $((a,bc)) + ((b,ac)) + ((ab,c)) = 0$ for all $a,b,c \in K$.

It is well known that $IW_q(K)/I^2(K)W_q(K)$ is isomorphic to $\mathrm{Br}_2(K)$, the 2-torsion part of the Brauer group of K. Under this isomorphism $((a,b))$ corresponds to the class of the Clifford algebra of $[a,b]$. In particular, Corollary 2 gives a presentation of $\mathrm{Br}_2(K)$ by generators and relations.

Acknowledgements:

The original draft for this note was written during a two month visit to the University of Talca, Chile, in the year 2002. The author wishes to express his thanks for the hospitality he enjoyed during this visit.

References:

[Arason] J.K. Arason: Wittring and Galoiscohomologie bei Charakteristik 2. J. Reine Angew. Math. *307/308*, 247–256 (1979).

[Arf] C. Arf: Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I). J. Reine Angew. Math. *183*, 148–167 (1941).

[Baeza] R. Baeza: Quadratic forms over semilocal rings. Lecture notes in mathematics 655. Berlin, Heidelberg, New York: Springer 1978.

[Kato] K. Kato: Symmetric bilinear forms, quadratic forms and Milnor K-theory in characteristic two. Invent. Math. *66*, 493–510 (1982).

[SBF] J. Milnor; D. Husemoller: Symmetric bilinear forms. Berlin, Heidelberg, New York: Springer 1973.

[Scharlau] W. Scharlau: Quadratic and hermitian forms. Berlin, Heidelberg, New York: Springer 1985.