Gauss Sums in Algebra and Topology

Laurence R. Taylor

We consider Gauss sums associated to functions $T \to \mathbf{R}/\mathbf{Z}$ which satisfy some sort of "quadratic" property and investigate their elementary properties. These properties and a Gauss sum formula from the nineteenth century due to Dirichlet enable us to give elementary proofs of many standard results. We derive the Milgram Gauss sum formula computing the signature mod 8 of a non–singular bilinear form over $\mathbf{Q}$ and its generalization to non–even lattices. We generalize formulae of Brown on the signature mod 8 of non–singular integral forms and a generalization of it due to Kirby and Melvin. These results follow with no additional analysis and require no results on Witt groups. Assuming a bit of algebraic topology, we reprove a theorem of Morita's computing the signature mod 8 of an oriented Poincaré duality space from the Pontryagin square without using Bockstein spectral sequences. Since we work with forms which may be singular, we also obtain a version of Morita's theorem for Poincaré spaces with boundary. We apply our results to the bilinear form $Sq^1 x \cup y$ on $H^1(M; \mathbf{Z}/2\mathbf{Z})$ of an orientable 3–manifold and also derive Levine's formula for the Arf invariant of a knot.

Introduction.

Gauss sums have a long and venerable history. A general version has a finite set T, a function $\psi: T \to \mathbf{R}/\mathbf{Z}$ and the associated Gauss sum

$$G(\psi) = \sum_{t \in T} e^{2\pi i \psi(t)} \ .$$

Even more general notions would replace T by a measure space and the finite sum by an integral. The Gauss sum problem is to evaluate $G(\psi)$ with the first examples going back to Gauss [**6** ,Art.356].

In the generality of a function on a finite set, it is difficult to say very much useful except that the problem can be divided into a magnitude and a phase. We can consider the magnitude or norm, $N(\psi) = |G(\psi)|$, and when $N(\psi) \neq 0$, define the phase $\beta(\psi) \in \mathbf{R}/\mathbf{Z}$ by

$$G(\psi) = N(\psi) \cdot e^{2\pi i \beta(\psi)} \ .$$

Here are two general constructions. Given ψ_i on T_i, $i = 1, 2$, define the *orthogonal* sum $\psi_1 \perp \psi_2: T_1 \times T_2 \to \mathbf{R}/\mathbf{Z}$ by $(\psi_1 \perp \psi_2)(x_1, x_2) = \psi_1(x_1) + \psi_2(x_2)$. Check that

$$G(\psi_1 \perp \psi_2) = G(\psi_1) \cdot G(\psi_2) \ . \tag{1.1}$$

For the second construction, observe $\mathbf{Z}$ acts on the functions by $(a \cdot \psi)(x) = a \cdot \psi(x)$ for $a \in \mathbf{Z}$. For $a = -1$,

$$G(-\psi) = \overline{G(\psi)} \ . \tag{1.2}$$

Partially supported by the N.S.F.

We review and extend some examples for which the magnitude and phase can be calculated and apply these results to some problems in algebra and topology. Our main interest is the case where T is a finite abelian group and ψ has some sort of "quadratic" property, which we now review. A function $\psi\colon T \to \mathbf{Q}/\mathbf{Z}$ is called a *quadratic function* provided

1.3) $\psi(ax) = a^2\psi(x)$ for all integers a and all $x \in T$

1.4) $b(x,y) = \psi(x+y) - \psi(x) - \psi(y)\colon T \times T \to \mathbf{Q}/\mathbf{Z}$ defines a bilinear form.

We call ψ a *quadratic enhancement* of b and b the *associated bilinear form* to ψ. If ψ just satisfies 1.4), we say ψ is an *enhancement* of b. Condition 1.4) is equivalent to the condition

1.5) $\psi(x_1+x_2+x_3) = \psi(x_1+x_2) + \psi(x_1+x_3) + \psi(x_2+x_3) - \big(\psi(x_1) + \psi(x_2) + \psi(x_3)\big)$

for all $x_i \in T$. Any function $\psi\colon T \to \mathbf{R}/\mathbf{Z}$ satisfying 1.5) will be called an *enhancement*. It is an enhancement of the *associated bilinear form*, b_ψ, defined by 1.4). Note that the associated bilinear form for an enhancement is symmetric. The set of functions from T to $\mathbf{R}/\mathbf{Z}$ is a group and the set of enhancements is a subgroup. The orthogonal sum of enhancements is an enhancement and the $\mathbf{Z}$ action takes enhancements to enhancements.

Any symmetric bilinear form has enhancements. Given $b\colon T \times T \to \mathbf{Q}/\mathbf{Z}$ define $\mathcal{W}(b)$ to be $T \oplus \mathbf{Q}/\mathbf{Z}$ with group structure $(t_1, r_1) + (t_2, r_2) = \big(t_1 + t_2, r_1 + r_2 - b(t_1, t_2)\big)$. It is straightforward to check that $\mathcal{W}(b)$ is an abelian group and that $\iota\colon \mathbf{Q}/\mathbf{Z} \to \mathcal{W}(b)$ defined by $\iota(r) = (0, r)$ is an injective homomorphism. Since $\mathbf{Q}/\mathbf{Z}$ is divisible, ι has a section, $\Psi\colon \mathcal{W}(b) \to \mathbf{Q}/\mathbf{Z}$. Define $\psi(t) = \Psi(t, 0)$ and check that ψ is an enhancement of b. Conversely, given an enhancement of b, define $\Psi(t, m) = \psi(t) + m$ and check that it is a section, so the set of enhancements of b corresponds bijectively to the set of sections of ι. Let $\Gamma(b)$ denote the space of sections of ι or equivalently the space of enhancements of b.

The set $\Gamma(b)$ is acted on by the group of homomorphisms, $T^* = \mathrm{Hom}(T, \mathbf{Q}/\mathbf{Z})$: given one enhancement of b, say ψ, and $h \in T^*$ define ψ_h by $\psi_h(t) = \psi(t) + h(t)$ and check that ψ_h is an enhancement of b. If ψ_1 and ψ_2 are enhancements of b, check that $\psi_1 - \psi_2 \in T^*$. Pick an element $\psi \in \Gamma(b)$ and define $T^* \to \Gamma(b)$ using the action on ψ: this function is a bijection.

A homomorphism, $h\colon T_1 \to T_2$ is an *isometry* between two enhancements provided $\psi_2\big(h(x)\big) = \psi_1(x)$: if h is an isomorphism we say ψ_1 and ψ_2 are *isometric*, written $\psi_1 \cong \psi_2$. The map h is an isometry in the usual sense between the associated bilinear forms. As an example, if $a \in Z$ is relatively prime to $|T|$ then multiplication by a on T gives an isometry between $a^2 \cdot \psi$ and ψ if ψ is quadratic.

Any enhancement satisfies $\psi(0) = 0$ and $b(x,x) = \psi(x) + \psi(-x)$ (compute $b(x,-x)$ using bilinearity). Bilinearity also shows that $\psi = \perp_p \psi_p$, where ψ_p denotes ψ restricted to the p–torsion subgroup Induction shows that $\psi(ax) = \frac{a^2+a}{2} \cdot \psi(x) + \frac{a^2-a}{2} \cdot \psi(-x)$. Furthermore, $\psi^q\colon T \to \mathbf{Q}/\mathbf{Z}$ defined by $\psi^q(x) = \psi(x) - \psi(-x)$ is a homomorphism and ψ is quadratic if and only if ψ^q is identically 0.

If $ax = 0$ then $a \cdot b(x,x) = a \cdot \psi^q(x) = 0$, so $a\psi(x) \pm a\psi(-x) = 0$ and $2a\psi(x) = 0$. Hence, for any enhancement, $\psi(T) \subset \mathbf{Q}/\mathbf{Z}$. If a is odd, $a \cdot \psi(x) = -a \cdot \psi(-x)$ and $\psi(ax) = 0$ together imply $a\psi(x) = 0$. It follows that ψ_p takes values in $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$.

Remark 1.6: The action of T^* on enhancements has the following effect. Check that $(\psi_h)^q = \psi^q + 2h$ so if ψ is quadratic, ψ_h is also quadratic if and only if h takes values in $\mathbf{Z}/2\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$. Since ψ^q vanishes on elements of order 2, there exits a homomorphism such that $\psi^q = 2h$ and then ψ_{-h} is quadratic.

If $K \subset T$ is a subgroup, define $K^\perp = \{t \in T \mid b_\psi(t,k) = 0 \ \forall\ k \in K\}$. We call ψ and b_ψ *non–singular* provided $T^\perp = \{0\}$. Note $(T_1 \perp T_2)^\perp = T_1^\perp \oplus T_2^\perp$. If K satisfies $\psi|_K = 0$, then $K \subset K^\perp$ and ψ induces a well–defined function

$$\psi_{K^\perp/K}\colon K^\perp/K \to \mathbf{Q}/\mathbf{Z}\ .$$

Any bilinear form b defines an adjoint homomorphism $Ad(b)\colon T \to \mathrm{Hom}(T, \mathbf{Q}/\mathbf{Z})$ and $T^\perp$ is the kernel of $Ad(b)$. This means that non–singular forms have the property that for any $h \in T^*$ there exists a unique $c \in T$ such that $h(t) = b(t,c)$ for all $t \in T$. In the singular case, given any $h \in T^*$ with $h|_{T^\perp}$ trivial, there exist $c \in T$, not unique, such that $h(t) = b(t,c)$ for all $t \in T$. For $x \in T/T^\perp$ we use the notation ψ_x to denote the enhancement $\psi_x(t) = \psi(t) + b(x_1, t)$ for all $t \in T$, where $x_1 \in T$ maps to x. Check that ψ_x is independent of the choice of x_1.

For any enhancement, ψ restricted to $T^\perp$ is a homomorphism: denote it by ψ^s. We say ψ is *tame* provided ψ^s is trivial. If ψ is tame then it induces a non–singular form on $T/T^\perp$, which we denote by ψ^{red} The orthogonal sum of two tame enhancements is tame. If ψ is tame, so is $a \cdot \psi$ for any $a \in \mathbf{Z}$ which is relatively prime to $|T|$. If ψ is quadratic ψ^s takes values in $\mathbf{Z}/2\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ and if $2x \in T^\perp$, $\psi^s(2x) = 0$.

Remark 1.7: If ψ is tame, ψ_h is tame if and only if h vanishes on $T^\perp$. Since $\mathbf{Q}/\mathbf{Z}$ is injective there is always an extension h of ψ^s to all of T and for any such h, ψ_{-h} is tame. If ψ is tame the function $x \in T/T^\perp \mapsto \psi_x$ defines a bijection between $T/T^\perp$ and the tame enhancements of b.

Remark 1.8: For any abelian group T and $n \in \mathbf{Z}$, let ${}_nT = \big\{x \in T \mid nx = 0\big\}$ and let $n \cdot T = \big\{x \in T \mid x = ny\big\}$. If ψ is tame and quadratic the function $x \in {}_2(T/T^\perp) \mapsto \psi_x$ defines a bijection between ${}_2(T/T^\perp)$ and the tame quadratic enhancements of b.

Theorem 1.9. *Every symmetric bilinear form b has a tame quadratic enhancement.*

Proof: We have seen b has enhancements. Using (1.7) construct a tame one ψ_t. Pass to ${\psi_t}^{red}$ and use (1.6) to construct a quadratic $\hat{\psi}\colon T/T^\perp \to \mathbf{Q}/\mathbf{Z}$ and check that the composition $\psi\colon T \to T/T^\perp \xrightarrow{\hat{\psi}} \mathbf{Q}/\mathbf{Z}$ is a tame quadratic enhancement of b. ∎

For subgroups $K \subset T$ with $\psi|_K = 0$, the Gauss sums for ψ and $\psi_{K^\perp/K}$ are related. This has been noticed before, [**2**], [**3**], [**11**], [**12**], [**14**] and many others, but apparently only for non–singular quadratic functions.

Theorem 1.10. *Let $\psi\colon T \to \mathbf{R}/\mathbf{Z}$ be an enhancement and suppose $\psi|_K = 0$ for some subgroup K. Then*

$$G(\psi) = |K| \cdot G(\psi|_{K^\perp/K})\ .$$

We emphasize that neither tame nor quadratic is assumed. The proof is standard. Pick coset representatives α_i for $T/K^\perp$ and γ_j for $K^\perp/K$ and let κ_k run over the elements of K. Then every element of T can be written uniquely as $\alpha_i+\gamma_j+\kappa_k$ and $\psi(\alpha_i+\gamma_j+\kappa_k) = b(\alpha_i,\gamma_j)+b(\alpha_i,\kappa_k)+\psi(\alpha_i)+\psi(\gamma_j)$. If we fix α_i and γ_j and sum over κ_k then the only term which depends on κ_k is $b(\alpha_i,\kappa_k)$ which is a homomorphism. Hence the sum is 0 if $b(\alpha_i,\kappa_k)$ is non–zero for some κ_k. But by definition of $K^\perp$, $b(\alpha_i,\kappa_k)$ is non–trivial except for the α_i in the 0 coset, say α_0, and in this case the sum is just $|K|\cdot e^{2\pi i\psi(\alpha_0+\gamma_j)}$. ∎

We say that ψ and $\psi|_{K^\perp/K}$ as in (1.10) are *W–equivalent*. Turn W–equivalent into an equivalence relation in the usual manner.

A standard observation permits us to evaluate the magnitude of $G(\psi)$.

Corollary 1.11. *Let ψ be an enhancement. If ψ is not tame then $N(\psi)=0$ and if ψ is tame then $N(\psi)=\sqrt{|T^\perp|\cdot|T|}$.*

Proof: If ψ is not tame then there is a $c\in T^\perp$ such that $\psi(c)\neq 0$ and $\psi(t+c)=\psi(t)+\psi(c)$ for all $t\in T$. Since $\sum_{t\in T}e^{2\pi i\psi(t)}=\sum_{t\in T}e^{2\pi i\psi(t+c)}$ because the sums are over the same elements, just in a different order, one sees $G(\psi)=e^{2\pi i\psi(c)}\cdot G(\psi)$. It follows that $N(\psi)=0$.

If ψ is tame, check that the evident inclusion $\Delta\colon T\subset T\perp T/T^\perp$ with enhancement $\psi\perp-\psi^{red}$ satisfies $\big(\Delta(T)\big)^\perp=\Delta(T)$ and $\psi\perp-\psi^{red}$ restricted to $\Delta(T)$ vanishes so $G(\psi\perp-\psi^{red})=|T|$. But $G(\psi\perp-\psi^{red})=G(\psi)\cdot G(-\psi^{red})$; $G(\psi)=|T^\perp|\cdot G(\psi^{red})$; and $G(-\psi^{red})=\overline{G(\psi^{red})}$ so $|G(\psi\perp-\psi^{red})|=|T^\perp|\cdot N(\psi^{red})^2$. ∎

Remark 1.12: Note that if ψ_1 is W–equivalent to ψ_2 then either both are not tame (because $N(\psi_1)=N(\psi_2)=0$) or $\beta(\psi_1)=\beta(\psi_2)$.

We can evaluate $\beta(\psi_h)$ in terms of $\beta(\psi)$ if both are tame.

Proposition 1.13. *Suppose ψ is an enhancement and tame and that $h\colon T\to\mathbf{Q}/\mathbf{Z}$ is a homomorphism. Then ψ_h is tame if and only if $h(T^\perp)=0$. If q_h is tame let $c\in T/T^\perp$ be the unique element corresponding to h, so $\psi_h=\psi_c$. The value of $\psi(c_1)\in\mathbf{Q}/\mathbf{Z}$ is the same for all elements reducing to c, so let us denote that common value by $\psi(c)$. Then*

$$\beta(\psi_h)=\beta(\psi)-\psi(c).$$

Proof: Just note $\psi_h(t)=\psi(t+c_1)-\psi(c_1)$ for all $t\in T$. ∎

Remark 1.14: We check that a potentially interesting function is in fact nothing new. Let ψ be a tame enhancement and define a new function

$$\Delta_\beta\colon T/T^\perp\to\mathbf{R}/\mathbf{Z}$$

by $\Delta_\beta(x)=\beta(\psi)-\beta(\psi_x)$ for all $x\in T/T^\perp$. Then (1.13) says $\Delta_\beta=\psi^{red}$. In example (3.3) below we encounter the construction Δ_β and it is nice to be able to identify it.

It follows from a beautiful argument due to Frank Connolly, [**4** , p.393], that, in the quadratic case, $\psi \perp \psi \perp \psi \perp \psi$ is isometric to $-\psi \perp -\psi \perp -\psi \perp -\psi$. It follows that for any tame, quadratic enhancement, $\beta(\psi) \in \mathbf{Z}/8\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ and it then follows from (1.13) that $\beta(\psi) \in \mathbf{Q}/\mathbf{Z}$ for any tame enhancement.

Connolly's result can be made more precise: let T_p denote the p–torsion subgroup of T and let $\psi_p = \psi|_{T_p}$. As usual, it suffices to understand ψ_p.

Lemma 1.15. *Assume ψ_p is a quadratic enhancement. If $p \equiv 1 \bmod 4$, $\psi_p \cong -\psi_p$; if $p \equiv 3 \bmod 4$, $\psi_p \perp \psi_p \cong -\psi_p \perp -\psi_p$; $\psi_2 \perp \psi_2 \perp \psi_2 \perp \psi_2 \cong -\psi_2 \perp -\psi_2 \perp -\psi_2 \perp -\psi_2$.*

Here is a version of Connolly's argument. Over the p–adic integers, $\hat{\mathbf{Z}}_p$, the equation $x^2 = a$ has a solution if and only if it has a solution mod p if p is odd or mod 8 if $p = 2$. A direct proof is easy or use Hensel's lemma. We will show how to find $x_i \in \hat{\mathbf{Z}}_p$ such that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = -1$ and with $x_3 = x_4 = 0$ if $p \equiv 3 \bmod 4$ and with $x_2 = x_3 = x_4 = 0$ if $p \equiv 1 \bmod 4$. Assuming this done, Connolly's matrix $M = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ x_3 & -x_4 & -x_1 & x_2 \\ x_4 & x_3 & -x_2 & -x_1 \end{bmatrix}$ corresponds to an evident linear map from $T_p \oplus T_p \oplus T_p \oplus T_p$ to itself. Check $M \cdot M^T = (x_1^2 + x_2^2 + x_3^2 + x_4^2)I$ so M defines an isomorphism which can be checked to be an isometry between $\psi_p \perp \psi_p \perp \psi_p \perp \psi_p$ and $-\psi_p \perp -\psi_p \perp -\psi_p \perp -\psi_p$. If $x_3 = x_4 = 0$ or $x_2 = x_3 = x_4 = 0$ the evident square submatrix gives the required isometry.

To find the x_i, observe $x_1^2 = -1 - x_2^2 - x_3^2 - x_4^2$ has a solution mod 8 ($x_2 = x_3 = 1$, $x_4 = 2$) and hence in $\hat{\mathbf{Z}}_2$. If $p \equiv 1 \bmod 4$, -1 is a quadratic residue mod p so $x_1^2 = -1$ has a solution in $\hat{\mathbf{Z}}_p$. For the case $p \equiv 3 \bmod 4$, recall -1 is not a quadratic residue. Note that $-1 - x_2^2$ takes on $\frac{p+1}{2}$ distinct values mod p, all of which are prime to p. Since there are only $\frac{p-1}{2}$ quadratic residues prime to p the equation $x_1^2 = -1 - x_2^2$ has a solution in $\hat{\mathbf{Z}}_p$. ∎

Brown [**2**] studied the case in which T is a $\mathbf{Z}/2\mathbf{Z}$ vector space. Any enhancement on a $\mathbf{Z}/2\mathbf{Z}$ vector space is quadratic and Brown's functions were assumed non–singular, although tame would have sufficed for many of his results. For example, Brown gave a different argument for $\beta(\psi) \in \mathbf{Z}/8\mathbf{Z}$. An element $\omega \in T$ is *characteristic* provided $b(x,x) = b(\omega,x)$ for all $x \in T$. Brown's argument is to observe that characteristic elements exist and then $\psi_\omega = -\psi$. By (Proposition 1.13), if ψ is tame, $\beta(\psi) = \psi(\omega) + \beta(\psi_\omega) \in \mathbf{Q}/\mathbf{Z}$, so

$$2\beta(\psi) = \psi(\omega) \in \mathbf{Z}/4\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z} \ .$$

This not only shows $\beta(\psi)$ has order 8 but computes it mod 4 as $\psi(\omega)$.

For later use, recall the Gauss sum formulae of Dirichlet [**5**] that we require.

Theorem 1.16. *If $m > 0$ then*

$$\sum_{s=0}^{m-1} e^{2\pi i s^2/m} = \begin{cases} (1+i)\sqrt{m} & m \equiv 0 \ mod\ 4 \\ \sqrt{m} & m \equiv 1 \ mod\ 4 \\ 0 & m \equiv 2 \ mod\ 4 \\ i\sqrt{m} & m \equiv 3 \ mod\ 4 \end{cases}$$

Some elementary Galois theory allows us to extend (1.2) by restricting attention to a prime at a time. Let $\psi: T \to \mathbf{Q}/\mathbf{Z}$ be a quadratic function on a finite p–group of order p^r. Now not only can we multiply ψ by integers but also by p–adic integers. Let $a \in \hat{\mathbf{Z}}_p$ be prime to p (equivalently a is a unit in $\hat{\mathbf{Z}}_p$, written $a \in \hat{\mathbf{Z}}_p^*$). If $s \in \hat{\mathbf{Z}}_p^*$ then multiplication by s on T gives an isometry between then $\beta(a \cdot \psi) = \beta((a \cdot s^2) \cdot \psi)$. As we saw in the proof of Lemma 1.15 $\hat{\mathbf{Z}}_p^*/(\hat{\mathbf{Z}}_p^*)^2 = \mathbf{Z}/2\mathbf{Z}$ if p is odd and $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ if $p = 2$. The quadratic non–residues generate the group for p odd, and ± 1, ± 3 map onto the group for $p = 2$. Finally define $\ell_p(\ ): \hat{\mathbf{Z}}_p^* \to \{0, 1\} = \mathbf{Z}/2\mathbf{Z}$ by $\ell_p(u) = 1$ if u is a quadratic non–residue and 0 otherwise and by $\ell_2(u) = 1$ if $u \equiv \pm 3 \bmod 8$ and 0 otherwise.

We can now work out the formula for $\beta(a \cdot \psi)$ when a is prime to p. (For $p^i \cdot \psi$ see (2.14) and (2.17)).

Theorem 1.17. *Let T be a p group with a tame quadratic enhancement ψ and let $a \in \hat{\mathbf{Z}}_p^*$. Let $|T/T^{\perp}| = p^e$. Then for p odd*

$$\beta(a \cdot \psi) = \beta(\psi) + \frac{\ell_p(a) \cdot e}{2} \tag{1.17$_p$}$$

and for $p = 2$

$$\beta(a \cdot \psi) = a \cdot \beta(\psi) + \frac{\ell_2(a) \cdot e}{2} \tag{1.17$_2$}$$

Proof: It suffices to do the non–singular case since we can work with ψ^{red}. Let ζ be a primitive p^r root of unity where p^r annihilates $\psi(t)$ for all $t \in T$. Let $\omega = e^{\frac{2\pi i}{8}}$.

Using Lemma 1.15 we see

$$G(\psi) = p^{\frac{e}{2}} \omega^{\sigma} \tag{1.18}$$

where $\beta(\psi) = \frac{\sigma}{8}$. The result is immediate for quadratic residues, so let $\eta \in \hat{\mathbf{Z}}_p^*$ be a quadratic non–residue,

Now the left hand side of (1.18) lies in $\mathbf{Q}[\zeta]$ and hence so must the right. The p–adic units $\hat{\mathbf{Z}}_p^*$ map onto the Galois group of $\mathbf{Q}[\zeta]$ over $\mathbf{Q}$. The map sends $a \in \hat{\mathbf{Z}}_p^*$ to ζ^a (which makes sense since $\zeta^{p^r} = 1$ for some r). Let us denote the corresponding Galois automorphism by $\gamma_a: \zeta \mapsto \zeta^a$. For p odd, $\mathbf{Q}[\zeta] \cap \mathbf{Q}[\omega] = \mathbf{Q}$, so ± 1 are the only powers of ω in $\mathbf{Q}[\zeta]$.

For $p \equiv 1 \bmod 4$ Dirichlet (1.16) shows $\sqrt{p} \in \mathbf{Q}[\zeta]$ and one can check that $\gamma_\eta(\sqrt{p}) = -\sqrt{p}$. If e is even, then the right hand side of (1.18) must be an integer, so $\beta(\eta \cdot \psi) = \beta(\psi)$. If e is odd, then the right hand side of (1.18) must be $\sqrt{p}$ times an integer, so $\beta(\eta \cdot \psi) = \beta(\psi) + \frac{1}{2}$. Additionally $\beta(\psi)$ is either 0 or $\frac{1}{2}$. Note both cases are covered by the formula $(1.17)_p$.

For $p \equiv 3 \bmod 4$ Dirichlet (1.16) shows $i\sqrt{p} \in \mathbf{Q}[\zeta]$ and $\gamma_\eta(\sqrt{p}i) = -\sqrt{p}i$. If e is even, then the right hand side of (1.18) must again be an integer, so $\beta(\eta \cdot \psi) = \beta(\psi)$. If e is odd, then the right hand side of (1.18) must be $\sqrt{p}i$ times an integer, so $\beta(\eta \cdot \psi) = \beta(\psi) + \frac{1}{2}$ again and $(1.17)_p$ holds in this case too. Additionally $p \equiv 3 \bmod 4$, $\beta(\psi) = \pm\frac{1}{4}$ if e is odd and 0 or $\frac{1}{2}$ if e is even.

For $p = 2$, there are three multiplications to be worked out. Which class an integer a belongs to can be determined by reducing a mod 8. The numbers are -1 and ± 3 mod 8. The affect of -1 we know: $\beta(-\psi) = -\beta(\psi)$. The wrinkle when we multiply by ± 3 is that these Galois actions send $\sqrt{2}$ to $-\sqrt{2}$. If e is even then this does not matter and $\beta(\eta \cdot \psi) = \eta \cdot \beta(\psi)$ When e is odd we get $\beta(\eta \cdot \psi) = \eta \cdot \beta(\psi) + \frac{1}{2}$. So for $p = 2$ $(1.18)_2$ holds. ∎

Remark 1.19: The restriction in (1.17) that ψ is quadratic is useful in the proof. We leave as an exercise the formula in general. Let T be a p group with a tame enhancement ψ and let $a \in \hat{\mathbf{Z}}_p^*$. Let $|T/T^\perp| = p^e$. Pick a $c \in T/T^\perp$ so that ψ_c is quadratic.

$$\beta(a \cdot \psi) = \begin{cases} \beta(\psi) + (a^2 - 1) \cdot \psi(c) + \frac{\ell_p(\det B)}{8} & \text{if } p \text{ is odd} \\ a \cdot \beta(\psi) + (a^2 - 1) \cdot \psi(c) + \frac{\ell_2(\det B)}{8} & \text{if } p = 2 \end{cases} .$$

Some algebra applications.

Application: Given a symmetric bilinear form B on a rational vector space, V, define $Q: V \to \mathbf{Q}$ by $Q(v) = \frac{B(v,v)}{2}$. Call a lattice *integral* if $B(v_1, v_2) \in \mathbf{Z}$ for all $v_1,\ v_2 \in L$. Pick a lattice $L \subset V$ such that $Q(x)$ is integral for all $x \in L$. Define $L^\# = \{v \in V \mid B(v, \ell) \in \mathbf{Z}\ \forall\ \ell \in L\}$ and check that L integral implies $L \subset L^\#$. If B is non–singular, that is $\det B \neq 0$, check that $L^\#/L$ is finite. Check that Q induces a non–singular quadratic function $\psi_L: L^\#/L \to \mathbf{Q}/\mathbf{Z}$ which enhances the symmetric bilinear form $b_L: L^\#/L \times L^\#/L \to \mathbf{Q}/\mathbf{Z}$ induced by B. The Milgram Gauss Sum Formula [**11**] says

$$\beta(\psi_L) = \frac{\sigma(B)}{8} \ , \qquad (2.1)$$

where $\sigma(B)$ denotes the signature of B.

We prove the formula using some straightforward manipulations and Dirichlet's Gauss sum formula. The basic outline, except for the appeal to Dirichlet, is in Milnor and Husemoller [**12**] who attribute it to Knebusch. A proof for $\det B$ odd was given earlier by Blij in [**1**].

Proof: Call a lattice L *acceptable* if $Q(x) \in \mathbf{Z}$ for all $x \in L$. If L_1 and L_2 are acceptable lattices, so is $L_1 \cap L_2$. To show all acceptable lattices give the same answer, it suffices to show $\beta(\psi_{L_2}) = \beta(\psi_{L_1})$ under the additional assumption that $L_1 \subset L_2$, and hence $L_1 \subset L_2 \subset L_2^\# \subset L_1^\#$. Let $T = L_1^\#/L_1$ and apply Theorem 1.10 to $K = L_2/L_1 \subset T$. Check $K^\perp = L_2^\#/L_1$ so $K^\perp/K = L_2^\#/L_2$.

Over $\mathbf{Q}$, B can be diagonalized and there are acceptable diagonal lattices, so it suffices to show $\beta(\langle 2m\rangle) = \frac{1}{8}$ if $m > 0$. Now $G(\langle 2m\rangle) = \sum_{s=0}^{2m-1} e^{2\pi i \frac{s^2}{4m}}$. Dirichlet (1.16) in case $4m$ says $\sum_{s=0}^{4m-1} e^{2\pi i \frac{s^2}{4m}} = (1+i)\sqrt{4m}$. Since $(s+2m)^2 = s^2$ mod $4m$, $(1+i)\sqrt{4m} = 2 \cdot G(\langle 2m\rangle)$ and the result follows. ∎

Application: Suppose as above that B is a non–singular bilinear form on a rational vector space V and L is an integral lattice with $L^{\#}$ defined as in (2.1). Check B still induces a symmetric, bilinear form b_L on $L^{\#}/L$ which is still non–singular. To apply the Milgram Gauss sum formula to $L^{\#}/L$ we need additionally that $B(v,v) \in 2\mathbf{Z}$ for all $v \in L$. If L does not satisfy this condition we can proceed as follows. There exists a *characteristic element* $\bar{\omega} \in L$: i.e. $B(v,v) \equiv B(\bar{\omega}, v) \bmod 2$ for all $v \in L$. The element $\bar{\omega}$ is not unique but pick one. Then set $Q(x) = \frac{B(x,x)-B(\bar{\omega},x)}{2}$ for all $x \in L^{\#}$. Check that Q induces a quadratic function $\psi_{\bar{\omega}}\colon L^{\#}/L \to \mathbf{Q}/\mathbf{Z}$ and that ψ_L enhances b_L. Then

$$\beta(\psi_{\bar{\omega}}) = \frac{\sigma(B)}{8} - \frac{B(\bar{\omega},\bar{\omega})}{8} \in \mathbf{Q}/\mathbf{Z}\ . \tag{2.2}$$

Proof: Let $L_1 = 2L \subset L$. Check that the function Q defined above induces a function $\psi_{L_1}\colon L_1^{\#}/L_1 \to \mathbf{Q}/\mathbf{Z}$ which is an enhancement of b_{L_1}. The function ψ_{L_1} is almost certainly not quadratic, but just as in the proof of (2.1) prove that $\beta(\psi_{\bar{\omega}}) = \beta(\psi_{L_1})$. Note $\psi_{L_1} + B(?, \bar{\omega}/2) = \psi$ on $L_1^{\#}/L_1$ where ψ is the quadratic function induced by $\frac{B(x,x)}{2}$ on $L_1^{\#}/L_1$. Use (2.1) to calculate $\beta(\psi) = \frac{\sigma(B)}{8}$ and use Proposition 1.13 to deduce that $\beta(\psi_{\bar{\omega}}) = \beta(\psi) - \psi(\bar{\omega}/2) = \beta(\psi) - \frac{B(\bar{\omega},\bar{\omega})}{8}$. ∎

Remark 2.3: From (2.2), it follows that for $\det B = \pm 1$, $\sigma(B) \equiv B(\bar{\omega},\bar{\omega}) \bmod 8$.

If $\det B$ is odd, then $\bar{\omega}$ is unique up to sums with elements of the form $2x$. A classical argument shows $B(\bar{\omega},\bar{\omega}) \equiv B(\bar{\omega}+2x, \bar{\omega}+2x) \bmod 8$ and one checks that $\psi_{\bar{\omega}}$ does not depend on the choice of $\bar{\omega}$ either. For $\det B$ odd (2.2) is a result of Blij [**1**]. The general case appears in [**3**].

If $\det B$ is even however, there are different choices for $\bar{\omega}$ which give different enhancements and different values of $B(\bar{\omega},\bar{\omega})$. Indeed, it is a theorem of Brumfiel&Morgan [**3**] and Wall [**16**] that any quadratic enhancement of a non–singular symmetric bilinear form can be obtained as ψ_L for an appropriate B and $\bar{\omega}$.

We next turn to Brown [**2**] for other ways to obtain quadratic functions. Given a symmetric bilinear form, $B\colon V \times V \to \mathbf{Z}$, define

$$\psi_B\colon V \otimes \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$$

by $\psi_B(x) = \dfrac{B(x,x)}{4}$. This function is quadratic with associated bilinear form

$$B_2\colon (V \otimes \mathbf{Z}/2\mathbf{Z}) \times (V \otimes \mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z}$$

obtained by reducing B mod 2. There is an obvious generalization: let $V_m = V \otimes \mathbf{Z}/m\mathbf{Z}$ and define

$$\psi_{B,m}\colon V_m \to \mathbf{Z}/2m\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$$

with $\psi_{B,m}(x) = \dfrac{B(x,x)}{2m}$. In order for $\psi_{B,m}$ to be defined on V_m it is necessary and sufficient that m be even. This quadratic enhancement, even for $m = 2$, need not be tame. It is non–singular if and only if $\det B$ is relatively prime to m. A further generalization is to recall that for any quadratic $\psi: T \to \mathbf{Q}/\mathbf{Z}$ the function $B \otimes \psi: V \otimes T \to \mathbf{Q}/\mathbf{Z}$ defined by $(B \otimes \psi)\big(v \otimes x\big) = B(v,v)\psi(x)$ is also quadratic [**12** ,p.111]. (One should also check that it really is defined. Note that the formula for $B = \langle 1 \rangle$ implies that ψ is quadratic so the formula does not work for non–quadratic enhancements.) If m is even, let $\mathbf{1}_m: \mathbf{Z}/m\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ be defined by $\mathbf{1}_m(1) = \frac{1}{2m}$. Then $B \otimes \mathbf{1}_m = \psi_{B,m}$ so this generalizes Brown's construction.

Application: If B is a symmetric bilinear form over $\mathbf{Z}$ with determinant ± 1 and if ψ is tame quadratic, then

$$\beta(B \otimes \psi) = \sigma(B) \cdot \beta(\psi) \in \mathbf{Q}/\mathbf{Z} \ . \tag{2.4}$$

Proof: As Brown remarks, Theorem 1.10 shows that $\beta(B \otimes \psi)$ only depends on the Witt class of B. Now the Witt ring of $\mathbf{Z}$ is infinite cyclic generated by the form $\langle 1 \rangle$. But $\langle 1 \rangle \otimes \psi = \psi$. ∎

Remark 2.5: Since for positive even m, $\beta(\mathbf{1}_m) = \frac{1}{8}$, we get Brown's theorem, $\beta(\psi_{B,2}) = \frac{\sigma(B)}{8}$. The calculation at the end of the proof of (2.1) can be rephrased as $\beta(\mathbf{1}_m) = \frac{1}{8}$.

Remark 2.6: If m is odd, define $\mathbf{1}_m: \mathbf{Z}/m\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ by $\mathbf{1}_m(1) = \frac{1}{m}$. If $m > 0$ and $m \equiv 1$ mod 4, $\beta(\mathbf{1}_m) = 0$ and if $m > 0$, $m \equiv 3$ mod 4, $\beta(\mathbf{1}_m) = \frac{1}{4}$. These equations follow immediately from (1.16).

We give another proof of (2.4) that bypasses the Witt ring calculation and uses only the Gram–Schmidt process. We require some preliminaries.

Given ψ, fix a positive integer m so that all the values of ψ applied to elements of T lie in $\mathbf{Z}/m\mathbf{Z}$. When computing $\beta(B \otimes \psi)$ any two integer matrices which are the same mod m clearly yield the same result. We can also split ψ into its p–primary pieces and work with one prime at a time since $(B \otimes \psi)_p = B \otimes \psi_p$. At a fixed prime we can even take B to be a matrix over the p–adic integers.

If A and B are matrices over $\hat{\mathbf{Z}}_p$ such that there is a matrix M with $\det M$ prime to p such that $A = M^{tr} B M$, then the forms induced by A and B are isometric and we say the matrices are *similar*. Note that if A and B are similar, $\det A = \det B \cdot s^2$ for some $s \in \hat{\mathbf{Z}}_p^*$. Call any matrix over $\hat{\mathbf{Z}}_2$ of the form $H_{m_1,m_2} = \begin{pmatrix} 2m_1 & u \\ u & 2m_2 \end{pmatrix}$ with $u \in \hat{\mathbf{Z}}_2^*$ *mod2–hyperbolic*. Call any form which is an orthogonal sum of rank one forms and mod2–hyperbolics *reduced*. A form which is an orthogonal sum of rank one forms will be called *diagonal*.

The usual Gram–Schmidt process can be applied over $\hat{\mathbf{Z}}_p$ to yield the following algorithm for finding a reduced matrix similar to B. See [**12** ,p.6] for a similar result. If there is a diagonal entry α in B generated by x with α relatively prime to p, the Gram–Schmidt formula requires us to divide by $B(x,x)$ which is possible since $B(x,x) \in \hat{\mathbf{Z}}_p^*$. Continue until B is similar to $D \perp B'$ where D is diagonal and the diagonal entries of B' are all divisible by p. Suppose there are a pair of basis elements e, f in B' with $B'(e,f) \in \hat{\mathbf{Z}}_p^*$. If p is odd, replace e, f by $e+f$, $e-f$, note that $B'(e+f, e+f) \in \hat{\mathbf{Z}}_p^*$, and keep going. If $p = 2$, this does not work and a slightly more complicated formula shows that one can orthogonally split off the mod2–hyperbolic $H_{\frac{B(e,e)}{2}, \frac{B(f,f)}{2}}$. For all p one can continue until we have $C_0 \perp B_1$ where C_0 is reduced with $\det C_0 \in \hat{\mathbf{Z}}_p^*$ and every entry in the matrix for B_1 is divisible by p. Divide these entries by p and keep going. Eventually we get that B is similar to an orthogonal sum

$$C_0 \perp pC_1 \perp \cdots \perp p^w C_w \tag{2.7}$$

where each C_i is reduced with $\det C_i$ prime to p. Note that the ranks of the C_i are determined by the abelian group structure of the cokernel of $B\colon \hat{\mathbf{Z}}_p^r \to \hat{\mathbf{Z}}_p^r$.

For $\det A \in \hat{\mathbf{Z}}_p^*$ define a mod 8 integer $\sigma_p(A)$ by

$$\sigma_p(A) \equiv \left\{ \begin{array}{ll} \text{rank } A & \text{if } p \text{ is odd} \\ N_1 - N_{-1} + 3N_3 - 3N_{-3} & \text{if } p = 2 \end{array} \right\} \mod 8$$

and

$$\sigma'_p(A) \equiv \left\{ \begin{array}{ll} \sigma_p(A) + 1 \cdot \ell_p(\det A) & p \equiv 1 \mod 4 \\ \sigma_p(A) + 2 \cdot \ell_p(\det A) & p \equiv 3 \mod 4 \\ \sigma_p(A) + 4 \cdot \ell_p(\det A) & p = 2 \end{array} \right\} \mod 8$$

where N_i is the number of diagonal entries congruent to i mod 8 in any reduced matrix similar to A. It is not obvious that $\sigma_p(A)$ is well–defined for $p = 2$ but this is checked in the proof of the next result.

Proposition 2.8. *For each p and $\psi\colon T \to \mathbf{Q}/\mathbf{Z}$ with ψ tame and quadratic, T a p–group with $|T/T^\perp| = p^e$, and B a symmetric integral form over $\hat{\mathbf{Z}}_p$ with $\det B \in \hat{\mathbf{Z}}_p^*$,*

$$\beta(B \otimes \psi) = \sigma_p(B) \cdot \beta(\psi) + \frac{\ell_p(\det B) \cdot e}{2} \ .$$

Proof: We may pass to ψ^{red} so without loss of generality assume ψ is non–singular. Note $B \otimes \psi$ is also non–singular. We start by proving the formula assuming that that B is reduced and we have defined $\sigma_p(B)$ using B as our reduced form if $p = 2$. The desired formula is additive for orthogonal sum so it suffices to prove the result for $\langle a \rangle$ plus the mod2–hyperbolics if $p = 2$.

Since $a \cdot \psi = \langle a \rangle \otimes \psi$ the formula for rank one forms is just a restatement of the formula in Theorem 1.17.

Next let H_{m_1,m_2} be a mod2–hyperbolic with basis e and f. Let $\langle -1 \rangle$ be a rank one form with basis x. The two elements $x_1 = x + e$ and $x_2 = u \cdot x + f$ are orthogonal and generate orthogonal summands $\langle 2m_1-1\rangle$ and $\langle 2m_2-u^2\rangle$ respectively. Hence $\langle -1\rangle \perp H_{m_1,m_2}$ and $\langle 2m_1-1\rangle \perp \langle 2m_2-1\rangle \perp \langle a_3\rangle$ are isometric for some a_3. Checking determinants shows $a_3 \equiv 1-2m_1-2m_2 \bmod 8$. Hence

$$-\beta(\psi)+\beta(H\otimes\psi) = \big(2m_1-1+2m_2-u^2+a_3\big)\cdot\beta(\psi)+\frac{\ell_2((2m_1-1)\cdot(2m_2-1)\cdot a_3)\cdot e}{2}$$

since $u^2\equiv 1 \bmod 8$ it follows that $\beta(H\otimes\psi)=\frac{\ell_2(\det H)\cdot e}{2}$, verifying the required formula.

If B and C are similar, then $\ell_p(\det B)=\ell_p(\det C)$ and $\beta(B\otimes\psi)=\beta(C\otimes\psi)$. So $\sigma_p(B)=\sigma_p(C)$ for odd primes, finishing the proof in this case. We turn to the case $p=2$ where all we need to show is that if C_1 and C_2 are each similar to B, then $\sigma_2(C_1)=\sigma_2(C_2)$. Compute $\beta(B\otimes\mathbf{1}_4)=\beta(C_i\otimes\mathbf{1}_4)=\frac{\sigma_2(C_i)}{8}$, so $\sigma_2(C_1)\equiv\sigma_2(C_2) \bmod 8$. ∎

Remark: Here is another description of $\sigma_2(A)$ when A is symmetric with $\det A\in\hat{\mathbf{Z}}_2^*$. Recall that if $\bar\omega$ is characteristic element for the form A, then $A(\bar\omega,\bar\omega)$ is well–defined mod 8, see (2.3).

(2.9) $$\sigma_2(A)\equiv A(\bar\omega,\bar\omega) \mod 8\ .$$

To see this, note that it is immediate if A is reduced and then note that $A(\bar\omega,\bar\omega)$ mod 8 is independent of the basis. If we define $\rho_4(a)=0$ if $a\equiv 1 \bmod 4$ and 1 otherwise for any $a\in\hat{\mathbf{Z}}_2^*$, then

$(2.10)_2$ $$\operatorname{rank} A\equiv A(\bar\omega,\bar\omega)+2\cdot\rho_4(\det A) \mod 4$$

Compare this with the result that for any symmetric A over the reals with $\det A\neq 0$,

$(2.10)_\infty$ $$\operatorname{rank} A\equiv \sigma(A)+2\cdot\rho_\infty(\det A) \mod 4$$

where $\rho_\infty(a)=0$ if $a>0$ and 1 if $a<0$.

We can now prove (2.4) directly from 2.8. It suffices to prove (2.4) a prime at a time. For $p\equiv 1 \bmod 4$, $\beta(\psi)$ is a multiple of $\frac{1}{2}$ and $\ell_p(-1)=0$. Since $\operatorname{rank} B\equiv\sigma(B)$ mod 2, (2.4) holds. For $p\equiv 3 \bmod 4$, $\beta(\psi)$ is $\pm\frac{1}{4}$ if e is odd and a multiple of $\frac{1}{2}$ if e is even. Since $\ell_p(-1)=1$ $(2.10)_\infty$ shows that (2.4) holds. When $p=2$, (2.3) and (2.9) show that $\sigma_2(B)=\sigma(B)$. Since $\ell_2(-1)=0$ we are done. ∎

The same proof also establishes the following.

Remark 2.11: If $\psi\colon T\to\mathbf{Q}/\mathbf{Z}$ is a tame quadratic function and if B is any symmetric form over $\mathbf{Z}$ with $\det B$ relatively prime to $2\cdot|T/T^\perp|$ then $\beta(B\otimes\psi)=\sigma_2(B)\cdot\beta(\psi)$ provided we have that $\rho_4(\det B)=\ell_p(\det B)$ for every prime p such that $|(T/T^\perp)_p|\equiv 3 \bmod 4$ and $\ell_p(\det B)=0$ for every $p\equiv 1 \bmod 4$ and for $p=2$. One case that works is if $\det B=\pm\, s^2$ for $s\in\mathbf{Z}$ relatively prime to $2\cdot|T/T^\perp|$.

Kirby and Melvin [**7**] wanted a simple formula for $\beta(B \otimes \mathbf{1}_2)$. If B is similar to $C_0 \perp 2C_1 \perp \cdots$ then $B \otimes \mathbf{1}_2$ is isometric to $C_0 \otimes \mathbf{1}_2 \perp C_1 \otimes (2 \cdot \mathbf{1}_2) \perp \mathbf{0}$ where $\mathbf{0}$ denotes a trivial quadratic function of the appropriate rank. Now $2 \cdot \mathbf{1}_2$ is not tame so $B \otimes \mathbf{1}_2$ is tame if and only of C_1 is a sum of mod2–hyperbolics and then $\beta(B \otimes \psi) = \frac{\sigma_2'(C_0)}{8}$, so we want a simple way to check if C_1 has any diagonal terms and if there are none to compute $\sigma_2'(C_0)$.

If A is any 2–adic matrix with $\det A \in \hat{\mathbf{Z}}_2^*$ compute $\sigma_2'(A)$as follows. Let A be similar to a reduced matrix C and let n_1 (resp. n_3) denote the number of diagonal elements of C congruent to 1 (resp. 3) mod 4. Let ϵ_H denote the number of mod2–hyperbolics of C congruent mod 4 to $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Then

$$\sigma_2'(A) \equiv n_1 - n_3 + 4 \cdot \epsilon_H \qquad \text{mod } 8 \ ,$$

since $n_1 = N_1 + N_{-3}$, $n_3 = N_3 + N_{-1}$ and $\ell_2(\det C) \equiv N_3 + N_{-3} + \epsilon_H$ mod 2.

We say B is mod 2 reduced if there is a basis, $\{x_1, \cdots, x_r, e_1, f_1, \cdots, e_s, f_s, z_1, \cdots, z_t\}$ such that $B(x_i, x_i)$, $1 \le i \le r$, and $B(e_i, f_i)$, $1 \le i \le s$ are odd and all other pairings are even. What this means is that mod 2 B looks like an orthogonal sum of rank one forms with odd entries and some hyperbolics and a trivial form of some rank. If we apply the Gram–Schmidt process to this basis in the given order, we get a reduced form C with a basis $\{x_1', \cdots, x_r', e_1', f_1', \cdots, e_s', f_s', z_1', \cdots, z_t'\}$ where $x_i' = x_i + 2 \cdot \alpha_i$; $e_i' = e_i + 2 \cdot \beta_i$; $f_i' = f_i + 2 \cdot \gamma_i$; $z_i' = z_i + 2 \cdot \delta_i$. This means that all the diagonal elements for B are congruent mod 4 to the corresponding diagonal elements for C and hence

Theorem. *If B is mod 2 reduced, $B \otimes \mathbf{1}_2$ is tame if and only if none of its diagonal entries are congruent to 2 mod 4. If $B \otimes \mathbf{1}_2$ is tame then*

$$\beta(B \otimes \mathbf{1}_2) = \frac{n_1 - n_3 + 4 \cdot \epsilon_H}{8} \tag{2.12}$$

where n_1 (resp. n_3) is the number of diagonal entries of B congruent to 1 (resp. 3) mod 4 and ϵ_H is the number of $\{e_i, f_i\}$ with both $B(e_i, e_i)$ and $B(f_i, f_i)$ congruent to 2 mod 4. Further note

$$4 \cdot \epsilon_H \equiv \sum_{i=1}^{s} B(e_i, e_i) \cdot B(f_i, f_i) \quad \text{mod } 8 \ . \tag{2.13}$$

Finally note that if the diagonal entries of B_1 and B_2 are congruent mod 4 and the off–diagonal entries are congruent mod 2, then all squares are congruent mod 4 and hence $\beta(B_1 \otimes \mathbf{1}_2) = \beta(B_2 \otimes \mathbf{1}_2)$. Kirby&Melvin's algorithm [**7** ,p. 522] is to apply the Gram–Schmidt process mod 4 to B until a mod 2 reduced form B' is obtained. Then B and B' are congruent mod 4 and B' is mod 2 reduced so $\beta(B \otimes \mathbf{1}_2)$ can be computed from the diagonal entries of B'. Kirby and Melvin further add $\langle 1 \rangle \perp \langle -1 \rangle$'s and use them to get rid of all hyperbolics so they get (2.12) with $\epsilon_H = 0$.

In [**14**] we employed a slightly different variant of the Gram–Schmidt process to classify arbitrary non–singular quadratic functions on a p group. Theorem 3.5 (p.268) of [**14**] asserts that any non–singular ψ_p on a finite abelian p group is an orthogonal sum

$$\psi_p = R_1 \otimes \mathbf{1}_p \perp \cdots \perp R_k \otimes \mathbf{1}_{p^k} \tag{2.14}$$

where each R_i is reduced and has $\det R_i \in \hat{\mathbf{Z}}_p^*$. Furthermore, rank R_i depends only on T.

Recall

$$\beta(R_s \otimes \mathbf{1}_{p^s}) = \begin{cases} \dfrac{\sigma'_p(R_s)}{8} & p = 2 \text{ and } s \text{ odd} \\ \dfrac{\sigma_p(R_s)}{8} & p = 2 \text{ and } s \text{ even} \\ \dfrac{\ell_p(R_s)}{2} & p \equiv 1 \bmod 4 \text{ and } s \text{ odd} \\ 0 & p \equiv 1 \bmod 4 \text{ and } s \text{ even} \\ \dfrac{\sigma'_p(R_s)}{4} & p \equiv 3 \bmod 4 \text{ and } s \text{ odd} \\ 0 & p \equiv 3 \bmod 4 \text{ and } s \text{ even} \end{cases}$$

An immediate remark is

Theorem 2.15. *If ψ is tame,*

$$4 \cdot \beta(\psi) = \frac{\dim_{\mathbf{Z}/2\mathbf{Z}}\Big((T/T^{\perp}) \otimes \mathbf{Z}/2\mathbf{Z}\Big)}{2}$$

If T is a $\mathbf{Z}/2\mathbf{Z}$ vector space this is a result of Brown's [**2**] and for ψ non–singular the result is in [**14**].

Remark 2.16: Brown [**2**] defined a product of two quadratic functions on $\mathbf{Z}/2\mathbf{Z}$ vector spaces. We see no hope for defining a product in general, but given two quadratic functions on $\mathbf{Z}/p\mathbf{Z}$ vector spaces, say $\psi_1 = R \otimes \mathbf{1}_p$ and $q_2 = S \otimes \mathbf{1}_p$, define $\psi_1 \bullet \psi_2$ to be $(R \otimes S) \otimes \mathbf{1}_p$. Check that this product is well defined. It clearly is commutative and it is not hard to verify that if $\beta(\psi_i) = \frac{\alpha_i}{8}$ then $\beta(\psi_1 \bullet \psi_2) = \frac{\alpha_1 \cdot \alpha_2}{8}$. When $p = 2$ this is Brown's product and Brown's theorem.

Given a form B and a quadratic enhancement ψ we can work out $(B \otimes \psi)_p$ by finding a matrix similar to one as in (2.7) and a quadratic enhancement ψ_p decomposed as in (2.14), it is clear that $(B \otimes \psi)_p$ is an orthogonal sum of terms of the form $(C_i \otimes R_j) \otimes (p^i \cdot \mathbf{1}_{p^j})$. Hence, to describe $B \otimes \psi$ or even just $p^i \cdot \psi_p$ it suffices to describe $p^i \cdot \mathbf{1}_{p^r}$. Let $T = \mathbf{Z}/p^r\mathbf{Z}$ denote the domain of $p^i \cdot \mathbf{1}_{p^r}$. This form has $T^{\perp} = p^{r-i}T$. If p is odd $p^i \cdot \mathbf{1}_{p^r}$ is tame and $\left(p^i \cdot \mathbf{1}_{p^r}\right)^{red} = \mathbf{1}_{p^{r-i}}$. (Or trivial if $i \geq r$). If $p = 2$ this still works *except* if $r = i$. The form $2^r \cdot \mathbf{1}_{2^r}$ is not tame, although $H_{m,n} \otimes (2^r \cdot \mathbf{1}_{2^r}) = 2^r \cdot (H_{m,n} \otimes \mathbf{1}_{2^r})$ is trivial, therefore tame. Hence $2^i \cdot \psi_2$ is tame if and only if R_i has no diagonal summands. If $p^i \cdot \psi_p$ is tame, we have

$$(p^i \cdot \psi_p)^{red} = R_{i+1} \otimes \mathbf{1}_p \perp \cdots \perp R_k \otimes \mathbf{1}_{p^{k-i}} \tag{2.17}$$

and $\beta(p^i \cdot \psi_p)$ can be worked out from knowledge of the $\sigma_p(R_i)$ and the $\ell_p(\det R_i)$.

Remark 2.18: Note for p odd, each $\sigma_p(R_i)$ and each $\ell_p(\det R_i)$ is an invariant of the isotropy class of ψ_p. For a matrix B similar to $C_0 \perp \cdots \perp p^w C_w$, each $\sigma_p(C_i)$ and each $\ell_p(\det C_i)$ is an invariant of B. For $p = 2$ the invariance fails. The form $\mathbf{1}_4 \perp \mathbf{1}_2$ is isometric to $\langle 3\rangle \otimes \mathbf{1}_4 \perp \langle 3\rangle \otimes \mathbf{1}_2$: the matrices $\langle 1\rangle \perp 2 \cdot \langle 1\rangle$ and $\langle 3\rangle \perp 2 \cdot \langle 3\rangle$ are similar. One can still choose the R_j and the C_i and work out $(C_i \otimes R_j)(p^i \cdot \mathbf{1}_{p^j})$. Check that $\sigma_p(A_1 \otimes A_2) = \sigma_p(A_1) \cdot \sigma_p(A_2)$ and $\ell_p(\det(A_1 \otimes A_2)) = \ell_p(\det A_1) + \ell_p(\det A_2) \bmod 2$ so once the R_j and C_i are known, the calculation is straightforward.

Topology applications.

Application 3.1: (A theorem of Morita [**13**]) Let X be a $4k$ dimensional, oriented, connected Poincaré duality space without boundary. The Pontryagin square

$$\mathcal{P}\colon H^{2k}(X; \mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/4\mathbf{Z}$$

is a quadratic enhancement of the cup product pairing $H^{2k}(X; \mathbf{Z}/2\mathbf{Z}) \times H^{2k}(X; \mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z}$. Brown conjectured and Morita proved that

$$\beta(\mathcal{P}) = \frac{\sigma(X)}{8} \in \mathbf{Q}/\mathbf{Z}$$

where $\sigma(X)$ denotes the signature of X.

For the proof, let B denote the bilinear form on $H^{2k}(X; \mathbf{Z})/torsion$ induced by cup product. We use an observation of Massey's to show $\mathcal{P}$ is W–equivalent to $B \otimes \mathbf{1}_2$ and then Remark 2.5 completes the proof.

Let K denote the image of the torsion in $H^{2k}(X; \mathbf{Z})$ in $H^{2k}(X; \mathbf{Z}) \otimes \mathbf{Z}/2\mathbf{Z}$. An observation of Massey [**10**] which he claims was well–known at the time says that, in our notation,

$$K^{\perp}/K = \big(H^{2k}(X; \mathbf{Z})/torsion\big) \otimes \mathbf{Z}/2\mathbf{Z}\ .$$

Recall that on $H^{2k}(X; \mathbf{Z}) \otimes \mathbf{Z}/2\mathbf{Z} \subset H^{2k}(X; \mathbf{Z}/2\mathbf{Z})$ the Pontryagin square is just the cup product square reduced mod 4. This shows that $\mathcal{P}$ vanishes on K and that the enhancement induced by $\mathcal{P}$ on $K^{\perp}/K$ is just $B \otimes \mathbf{1}_2$. ∎

Application 3.2: Let X be a $4k$ dimensional, oriented, connected Poincaré duality space with boundary. The Pontryagin square

$$\mathcal{P}\colon H^{2k}(X, \partial X; \mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/4\mathbf{Z}$$

is still a quadratic enhancement of the cup product pairing. If $H^{2k}(\partial X;\mathbf{Z})$ is torsion free, then

$$\beta(\mathcal{P}) = \frac{\sigma(X)}{8} \in \mathbf{Q}/\mathbf{Z}$$

Several differences arise in the bounded case. The first is that the cup product pairing has an annihilator: if $T = H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})$, $T^\perp$ is the image of $H^{2k-1}(\partial X;\mathbf{Z}/2\mathbf{Z})$ in $H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})$. A theorem of Thomas [**15**] calculates that the compositions

$$\begin{array}{lll} H^{2k-1}(\partial X;\mathbf{Z}/2\mathbf{Z}) & \to H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z}) \xrightarrow{\mathcal{P}} H^{4k}(X,\partial X;\mathbf{Z}/4\mathbf{Z}) = & \mathbf{Z}/4\mathbf{Z} \\ H^{2k-1}(\partial X;\mathbf{Z}/2\mathbf{Z}) & \xrightarrow{\quad x\cup Sq^1x \quad} H^{4k-1}(\partial X;\mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z} \subset & \mathbf{Z}/4\mathbf{Z} \end{array}$$

are equal. Note that if $H^{2k}(\partial X;\mathbf{Z})$ is torsion–free, $Sq^1x = 0$ so $\mathcal{P}$ is tame in this case. (But not in general: any oriented boundary for an RP^{2k-1} is going to have $\mathcal{P}$ not tame.) We can identify $T/T^\perp$ with the image of $H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})$ in $H^{2k}(X;\mathbf{Z}/2\mathbf{Z})$.

The cup product pairing on $H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})$ comes from a bilinear pairing

$$\lambda\colon H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})\otimes H^{2k}(X;\mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z}$$

whose adjoint is an isomorphism. With respect to λ there is a straightforward generalization of Massey's observation: if $A \subset H^{2k}(X;\mathbf{Z}/2\mathbf{Z})$ denotes the image of the torsion subgroup of $H^{2k}(X;\mathbf{Z})$ in $H^{2k}(X;\mathbf{Z}/2\mathbf{Z})$, then $A^\perp \subset H^{2k}(X,\partial X;\mathbf{Z}/2\mathbf{Z})$ is the image of $H^{2k}(X,\partial X;\mathbf{Z})$.

We would like to relate the enhancement $\mathcal{P}$ to the mod 2 reduction of the integral form. If $H^{2k}(\partial X;\mathbf{Z})$ has 2–torsion much can still go wrong. For example, embed $S^2 \subset CP^2$ so that the fundamental class hits twice a generator and write $CP^2 = P \cup E$, where E is the total space of the normal bundle of the embedding and P is the complement. Then $H^2(P,\partial P;\mathbf{Z}/2\mathbf{Z}) = \mathbf{Z}/2\mathbf{Z}$ and the $\mathcal{P}(x) = \pm 1/4$ but $H^2(P,\partial P;\mathbf{Z}) = 0$. Another phenomenon occurs on $X = (RP^3 - \mathring{D}^3)\times[0,1]$: here the boundary is $RP^3\# RP^3$ so $\mathcal{P}$ is not tame, but $H^2(X,\partial X;\mathbf{Z}) = 0$.

If there is no 2–torsion in $H^{2k}(\partial X;\mathbf{Z})$ then we can make some progress. The image of $H^{2k}(X,\partial X;\mathbf{Z})$ in $H^{2k}(X;\mathbf{Z})/torsion$ has a non–singular bilinear pairing and we let B_X be a matrix for it. It follows from the no 2–torsion condition and the generalization of Massey's observation that $\mathcal{P}$ and ψ_{B_X} are W–equivalent, just as in 3.1.

As we saw above one can not usually relate ψ_{B_X} to the signature of B_X *unless* $\det B_X = \pm 1$. But since $H^{2k}(\partial X;\mathbf{Z})$ is torsion–free, $\det B = \pm 1$. ∎

The function $x \cup Sq^1x$ arises in other contexts. It is the squaring homomorphism associated to the bilinear form

$$R\colon H^k(M;\mathbf{Z}/2\mathbf{Z}) \times H^k(M,\mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z}$$

defined by $R(x,y) = \langle Sq^1x \cup y, [M]\rangle$ on any oriented $2k+1$ dimensional manifold. The form R is symmetric.

Let M^3 be a closed 3 manifold with a fixed Spin structure. In [**8** ,p.209], we showed how to quadratically enhance the linking form ℓ on the torsion subgroup of $H^2(M;\mathbf{Z})$. Let ψ denote this enhancement. We further showed that $\beta(\psi)$ is just Rochlin's μ–invariant of M mod 8. Spin structures on M are acted on by $H^1(M;\mathbf{Z}/2\mathbf{Z})$. For $x \in H^1(M;\mathbf{Z}/2\mathbf{Z})$, define $\hat{\mu}(x)$ to be the difference of the μ invariant for M with its given Spin structure minus the μ invariant for M with Spin structure obtained by acting via x, all reduced mod 8. We showed that $\hat{\mu}$ is a quadratic enhancement of R. (See the remark after formula 4.9, p.213 [**8**]).

Now in general R is singular: in fact $R^\perp$ is precisely the kernel of Sq^1. We see that the image of $H^1(M;\mathbf{Z})$ in $H^1(M;\mathbf{Z}/2\mathbf{Z})$ acts trivially on the quadratic enhancement on ℓ so we get an action of $H^1(M;\mathbf{Z}/2\mathbf{Z})/H^1(M;\mathbf{Z})$ on this set. This group is identified via the integral Bockstein δ with ${}_2H^2(M;\mathbf{Z})$ and R naturally induces a bilinear form on ${}_2H^2(M;\mathbf{Z})$: the enhancement $\hat{\mu}$ also extends to ${}_2H^2(M;\mathbf{Z})$.

In (1.8) we remarked that ${}_2H^2(M;\mathbf{Z})$ acts on the quadratic enhancements of the linking form, and a comparison of (1.14) and the enhancement $\hat{\mu}$ shows that $\hat{\mu}(x) = \Delta_\beta(\delta x)$ for any $x \in H^1(M;\mathbf{Z}/2\mathbf{Z})$. So the quadratic enhancement on R is just the quadratic enhancement of the linking form restricted to ${}_2H^2(M;\mathbf{Z})$.

Application 3.3: If the torsion subgroup of $H_1(M^3;\mathbf{Z})$ is a $\mathbf{Z}/2\mathbf{Z}$ vector space, then the μ invariant mod 8 is $\beta(\hat{\mu})$ since $\hat{\mu} = \psi$. In general, $\hat{\mu}$ is tame unless ${}_4(H^2(M^3;\mathbf{Z}))$ contains an x with $\ell(x,x) = \pm\frac{1}{4}$, in which case $\hat{\mu}$ is not tame: e.g. the lens spaces $L(4,\pm 1)$. For the lens space $L(8,1)$, $\beta(\psi) = \frac{1}{8}$ but $\hat{\mu}$ is trivial on ${}_2H^2(L(8,1);\mathbf{Z})$.

Knot theory provides a natural source of examples of mod2–hyperbolics.

Application 3.4: Given a symmetric integral matrix B with even diagonal entries we can find matrices S such that $B = S + S^{tr}$. The form $S(x,y) = x^{tr}Sy$ symmetrizes to B and if we define $\psi\colon V \otimes \mathbf{Z}/2\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$ by $\psi(x) = \frac{x^{tr}Sx}{2}$ then $\psi = B \otimes \mathbf{1}_2$. If $\det B$ is odd, it follows that ψ is tame and that $\beta(\psi) = \beta(\psi_{B,2}) = \frac{\ell_2(\det B)}{2}$. It further follows that $\det(S - S^{tr}) \in \hat{\mathbf{Z}}_2^*$ so over $\hat{\mathbf{Z}}_2$ there is a symplectic basis $\{e_1, f_1, \cdots, e_s, f_s\}$. Using that same basis for B makes B mod2–hyperbolic so $\beta(\psi) = \displaystyle\sum_{i=1}^{s} \frac{S(e_i,e_i)\cdot S(f_i,f_i)}{2}$.

If S is a Seifert matrix for a knot $\kappa\colon S^{4k-3} \subset S^{4k-1}$, then there is an integral symplectic basis for $S - S^{tr}$ and $\displaystyle\sum_{i=1}^{s} \frac{S(e_i,e_i)\cdot S(f_i,f_i)}{2}$ is the usual definition of the Arf invariant of the knot, $\mathrm{Arf}(\kappa)$. Moreover, $\det B = \Delta_\kappa(-1)$ is the value of the Alexander polynomial of the knot evaluated at -1 and the formula $\mathrm{Arf}(\kappa) = \frac{\ell_2(\Delta_\kappa(-1))}{2}$ is Levine's theorem [**9** ,p.544].

References.

[**1**] F. van der Blij, *An invariant of quadratic forms mod 8*, Indag. Math. **21** (1959) 291-293.

[**2**] E. H. Brown, *Generalizations of the Kervaire invariant*, Ann. of Math. **95** (1972) 368-383.

[**3**] G. W. Brumfiel and J. W. Morgan, *Quadratic functions, the index modulo 8, and a* $\mathbf{Z}/4\mathbf{Z}$*–Hirzebruch formula*, Topology **12** (1973) 105-122.

[**4**] F. X. Connolly, *Linking numbers and surgery*, Topology **12** (1973) 389-409.

[**5**] P. G. L. Dirichlet, "Vorlesungen über Zahlentheorie", F. Vieweg und Sohn, Braunschweig (1871).

[**6**] C. F. Gauss, "Disquistiones Arithmeticae", Fleisher, Leipzig (1801).

[**7**] R. Kirby and P. Melvin, *The* 3*–manifold invariants of Witten and Reshetikin–Turaev for* $sl(2, C)$, Invent. Math. **105** (1991) 473-545.

[**8**] R. C. Kirby and L. R. Taylor, *Pin structures on low–dimensional manifolds*, "Geometry of Low–Dimensional Manifolds: 2", London Math. Soc. Lecture Note Series **151**, Cambridge University Press, Cambridge (1990) 177-242.

[**9**] J. Levine, *Polynomial invariants of knots*, Ann. of Math. **84** (1966) 537-554.

[**10**] W. S. Massey, *On the Stiefel–Whitney classes of a manifold*, Proc. Amer. Math. Soc. **13** (1962) 938-942.

[**11**] R. J. Milgram, *Surgery with coefficients*, Ann. of Math. **100** (1974) 194-248.

[**12**] J. Milnor and D. Husemoller, "Symmetric Bilinear Forms", Ergebnisse der Math. **73**, Springer–Verlag, New York (1973).

[**13**] S. Morita, *On the Pontrjagin square and the signature*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **18** (1971) 405-414.

[**14**] L. R. Taylor, *Relative Rochlin invariants*, Topology and its App. **18** (1984) 259-280.

[**15**] E. Thomas, *The suspension of the generalized Pontryagin cohomology operation*, Pacific J. Math. **9** (1959) 897-911.

[**16**] C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1963) 281-298.

taylor.2@nd.edu
Department of Mathematics University of Notre Dame Notre Dame, IN 46556