

QUADRATIC FORMS AND THE BIRMAN-CRAGGS HOMOMORPHISMS

BY

DENNIS JOHNSON¹

ABSTRACT. Let \mathcal{M}_g be the mapping class group of a genus g orientable surface M , and \mathcal{G}_g the subgroup of those maps acting trivially on the homology group $H_1(M, \mathbb{Z})$. Birman and Craggs produced homomorphisms from \mathcal{G}_g to \mathbb{Z}_2 via the Rochlin invariant and raised the question of enumerating them; in this paper we answer their question. It is shown that the homomorphisms are closely related to the quadratic forms on $H_1(M, \mathbb{Z}_2)$ which induce the intersection form; in fact, they are in 1-1 correspondence with those quadratic forms of Arf invariant zero. Furthermore, the methods give a description of the quotient of \mathcal{G}_g by the intersection of the kernels of all these homomorphisms. It is a \mathbb{Z}_2 -vector space isomorphic to a certain space of cubic polynomials over $H_1(M, \mathbb{Z}_2)$. The dimension is then computed and found to be $\binom{2g}{3} + \binom{2g}{2}$. These results are also extended to the case of a surface with one boundary component, and in this situation the linear relations among the various homomorphisms are also determined.

1. Introduction. Let M_g be an orientable surface of genus g , \mathcal{M}_g its mapping class group and \mathcal{G}_g the subgroup of those classes acting trivially on $H_1(M_g, \mathbb{Z})$. In [BC], Birman and Craggs produced homomorphisms from \mathcal{G}_g to \mathbb{Z}_2 derived from the Rochlin invariant. Roughly, each $f \in \mathcal{G}_g$ is used to produce a homology 3-sphere, and its Rochlin invariant is the value of (one of) the homomorphism(s) on f . The method in which these homomorphisms were produced leaves it unclear when two of them are equal, as well as how many there are. In this paper we give a canonical form for the homomorphisms, showing that they are in 1-1 correspondence with quadratic forms on $H_1(M_g, \mathbb{Z}_2)$ which induce the intersection form and have zero Arf invariant; this is the content of Theorem 2. This result allows us to show that the number of these homomorphisms is $2^{g-1}(2^g + 1)$ (Theorem 3). Also raised in [BC] is the problem of finding the intersection \mathcal{C} of the kernels of all the homomorphisms, and some explicit representation of \mathcal{G}/\mathcal{C} ; this is answered in Theorem 4. \mathcal{G}/\mathcal{C} is a finite dimensional vector space over \mathbb{Z}_2 and it is thus of some interest to know its dimension, so we give this in Theorem 5. We also give the analogous results of these theorems for the case of a surface with one boundary component, and in this situation determine the linear relations among the homomorphisms.

Received by the editors October 5, 1978 and, in revised form, August 21, 1979.

AMS (MOS) subject classifications (1970). Primary 57A10, 57A05, 55A99.

¹This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract NAS 7-100, sponsored by National Aeronautics and Space Administration.

© 1980 American Mathematical Society
0002-9947/80/0000-0412/\$06.00

I am particularly indebted to Joan Birman for many valuable and stimulating discussions concerning these matters. Also my thanks to Robert McEliece for showing me the material on Boolean algebra, without which I could not have proved Theorem 7.

2. Notation and preliminaries. In this paper, all manifolds will be assumed compact, orientable and *oriented*.

Let M_g be a closed surface of genus $g \geq 2$. We shall use the following notations and abbreviations:

SCC means "simple closed curve".

H_1 means $H_1(M_g, Z_2)$; likewise H^1 .

The above groups have the standard bilinear forms, which are *symplectic* (that is $x \cdot x = 0$); these forms establish self-dualities on H_1 and H^1 . We shall always think of H^1 as the dual of H_1 and the pairing between $x \in H_1$ and $\alpha \in H^1$ will be denoted by either $\langle \alpha, x \rangle$ or $\alpha(x)$. The symplectic automorphism group of H_1 will be denoted by Sp; it is a finite group isomorphic to $Sp(g, Z_2)$. A basis $a_1, \dots, a_g, b_1, \dots, b_g$ for H_1 is *symplectic* if $a_i \cdot a_j = b_i \cdot b_j = 0$ and $a_i \cdot b_j = \delta_{ij}$. If $g \in Sp$, then g^* will denote the dual automorphism of H^1 , with standard law $(gh)^* = h^*g^*$.

\mathfrak{N}_g is the mapping class group (of orientation preserving homeomorphisms) of M_g ; we shall frequently confuse a homeomorphism of M_g with its mapping class in \mathfrak{N}_g . The homology functor gives us a map from \mathfrak{N}_g onto the group Sp, and its kernel we denote by \mathfrak{I}_g . It is the group of mapping classes acting trivially on homology.

3. Quadratic forms on H_1 . By an *Sp-quadratic form*, or simply *Sp-form*, on the symplectic space H_1 we shall mean a function $\omega: H_1 \rightarrow Z_2$ such that

$$\omega(a + b) = \omega(a) + \omega(b) + a \cdot b. \tag{1}$$

Thus, an Sp-form is just one whose associated bilinear form is the existing symplectic form on H_1 . Putting $b = 0$, we find $\omega(0) = 0$. Also, if e_i is any basis for H_1 , we see that an Sp-form is completely determined by its values on the basis. In fact, iterating the formula (1) gives us

$$\omega\left(\sum_{i=1}^{2g} \alpha_i e_i\right) = \sum_{i=1}^{2g} \alpha_i \omega(e_i) + \sum_{i < j} \alpha_i \alpha_j (e_i \cdot e_j). \tag{2}$$

On the other hand, it is easy to see that if $\omega(e_i)$ are arbitrarily specified, then the above formula defines an Sp-form on H_1 . We may state this as

LEMMA 1. *An Sp-quadratic form is determined by its values on a basis. Conversely, these values may be chosen arbitrarily to define an Sp-form by formula (2).*

LEMMA 2. *Let ω_1, ω_2 be two Sp-quadratic forms on H_1 ; then $\omega_1 - \omega_2$ is a homomorphism $H_1 \rightarrow Z_2$. Conversely, if ω is an Sp-form and $\theta: H_1 \rightarrow Z_2$ is a homomorphism then the function $\omega + \theta$ is also an Sp-form.*

PROOF.

$$\begin{aligned} (\omega_1 - \omega_2)(a + b) &= \omega_1(a + b) - \omega_2(a + b) \\ &= \omega_1(a) + \omega_1(b) + a \cdot b - \omega_2(a) - \omega_2(b) - a \cdot b \\ &= (\omega_1 - \omega_2)(a) + (\omega_1 - \omega_2)(b) \end{aligned}$$

showing $\omega_1 - \omega_2$ to be a homomorphism. Conversely,

$$\begin{aligned} (\omega + \theta)(a + b) &= \omega(a + b) + \theta(a + b) \\ &= \omega(a) + \omega(b) + a \cdot b + \theta(a) + \theta(b) \\ &= (\omega + \theta)(a) + (\omega + \theta)(b) + a \cdot b, \end{aligned}$$

showing $\omega + \theta$ to be Sp-quadratic.

Let L be an abelian group. By an *affine space* over L we mean a transitive, free L -space, that is, a set K equipped with an "addition" $+: L \times K \rightarrow K$ satisfying:

- (a) $\lambda_1 + (\lambda_2 + k) = (\lambda_1 + \lambda_2) + k$, for $\lambda_i \in L, k \in K$.
- (b) Given any k_1, k_2 in K , there exists a *unique* λ in L such that $k_2 = \lambda + k_1$.

Thus K is practically like L , but with the distinction that it lacks a natural base point. (L is known as the translation group of K .)

Since the homomorphisms $H_1 \rightarrow Z_2$ are just the elements of H^1 , we see easily using the above lemma that the set Ω of all Sp-forms on H_1 has the natural structure of an affine space over H^1 . If $f \in \text{Sp}$, then f^* acts on H^1 in the usual adjoint way: $(f^*\alpha)(x) = \alpha(fx)$. This adjoint action extends to any function on H_1 , and it is easily seen that if ω is Sp-quadratic, then so is $f^*\omega$. This action of Sp on Ω emphasizes the distinction between Ω and its translation group H^1 : whereas Sp fixes 0 in H^1 , it is not hard to see that (for $g \geq 2$) no ω is fixed by all $f \in \text{Sp}$. We define the *orthogonal group* O_ω of ω to be the subgroup of Sp which does fix ω ; $O_\omega = \{f \in \text{Sp} | \omega(fa) = \omega(a) \text{ for all } a \in H_1\}$.

4. Polynomial functions on Ω . Let V be a vector space over a field F and U an affine space over V . A function $f: U \rightarrow F$ is called *linear* if there is a linear functional $g: V \rightarrow F$, necessarily unique, such that $f(v + u) = g(v) + f(u)$, all $u \in U, v \in V$. This definition implies that if f is linear and c is any constant, then $f + c$ is linear. Also, the linear functions clearly form a vector space $L(U)$ over F . Note that f is determined by choosing $g \in V^*$ and the value of f at some fixed point u_0 of U , which implies that $\dim L(U) = \dim V + 1$. $L(U)$ contains the constant functions as a natural one-dimensional subspace. A *polynomial function* on U is the obvious: sums of products of linear ones.

Consider now the case $U = \Omega, V = H^1$. For a in H_1 we get a function $\bar{a}: \Omega \rightarrow Z_2$ given by $\bar{a}(\omega) = \omega(a)$. Since for $\theta \in H^1$ we get $\bar{a}(\omega + \theta) = \omega(a) + \theta(a) = \bar{a}(\omega) + \langle \theta, a \rangle$, \bar{a} is linear with associated linear functional $\langle -, a \rangle$ on H^1 . This linear functional will be denoted simply by a , in accordance with the canonical duality between H_1 and H^1 .

LEMMA 3. *If e_i is a basis for H_1 , then the constant function 1 and \bar{e}_i form a basis for $L(\Omega)$.*

PROOF. Let $\omega \in \Omega$ be defined by $\omega(e_i) = 0$, that is, $\bar{e}_i(\omega) = 0$, as in Lemma 1. For any $\omega' \in \Omega$ and $f \in L(\Omega)$, we have $f(\omega') = f(\omega) + g(\omega' - \omega)$ where g is the associated linear functional on H^1 . Putting $f(\omega) = \alpha$ and

$$g = \sum_{i=1}^{2g} \alpha_i e_i,$$

we get

$$\begin{aligned} (\alpha \cdot 1 + \sum \alpha_i \bar{e}_i)(\omega') &= \alpha + \sum \alpha_i \bar{e}_i(\omega') = (\text{since } \omega(e_i) = 0) \\ \alpha + \sum \alpha_i (\omega'(e_i) - \omega(e_i)) &= \alpha + \sum \alpha_i \langle \omega' - \omega, e_i \rangle = f(\omega) + g(\omega' - \omega) = f(\omega'). \end{aligned}$$

Thus every element f of $L(\Omega)$ is a linear combination of the $2g + 1$ elements $1, \bar{e}_i$. Since $\dim L(\Omega) = 2g + 1$, these elements form a basis.

LEMMA 4. If $a, b \in H_1$ then $\overline{(a + b)} = \bar{a} + \bar{b} + a \cdot b$.

PROOF. $\overline{(a + b)}(\omega) = \omega(a + b) = \omega(a) + \omega(b) + a \cdot b = (\bar{a} + \bar{b} + a \cdot b)(\omega)$. We may iterate this relation to get

COROLLARY.

$$\overline{\sum_i a_i} = \sum_i \bar{a}_i + \sum_{i < j} a_i \cdot a_j.$$

These laws make precise the manner in which the function from H_1 to $L(\Omega)$ given by $a \rightarrow \bar{a}$ fails to be a homomorphism.

Our field here is Z_2 , so we need to say something about polynomials of degree > 2 . We are really only interested in polynomials as functions on Ω —that is, we take the standpoint that “a function is determined by its values”. Since f^2 and f take exactly the same values, we permit ourselves the reduction of f^2 to f in any expression—precisely, we are dividing out a true polynomial ring by the ideal generated by all $(f^2 - f)$. The fact that $1, \bar{e}_i$ form a basis for linear functions allows any polynomial to be written as a sum of monomials in the \bar{e}_i 's, and the reduction enables us to restrict to *square free monomials*. Such polynomials are known as *Boolean polynomials*; the sum of two such is another, and the product is (after reduction) also Boolean. We shall denote by B_r the space of all Boolean polynomials of degree $\leq r$.

The group Sp acts on a function $f: \Omega \rightarrow Z_2$ in the obvious way, namely, adjoint to its action on Ω . In other words, for $h \in Sp$ and $\omega \in \Omega$, $h(f)(\omega) = f(h^*\omega)$. Suppose in particular that $f = \bar{a}$ for some $a \in H_1$; then we have $h(\bar{a})(\omega) = \bar{a}(h^*\omega) = (h^*\omega)(a) = \omega(ha) = \overline{(ha)}(\omega)$, that is, $h(\bar{a}) = \overline{(ha)}$. More generally, for a polynomial $P(\bar{e}_i)$, we get $hP(\bar{e}_i) = P(\overline{he_i})$.

Now on Ω we find a quadratic Boolean function of particular interest, namely

$$\alpha = \sum_{i=1}^g \bar{a}_i \bar{b}_i,$$

where a_i, b_i is a symplectic basis of H_1 ; this is the *Arf invariant*. Arf (see [A]) showed the following:

- (a) α is invariant under the action of Sp on B_2 .
- (b) ω, ω' are in the same orbit of Sp iff $\alpha(\omega) = \alpha(\omega')$.

We define $\Psi \subset \Omega$ to be the set of all ω having zero Arf invariant. These forms arise naturally in connection with Heegaard splittings of Z_2 -homology spheres, as we see in the next section.

5. Heegaard imbedding and induced quadratic forms. Let M be a genus g surface and W a 3-manifold (assumed oriented!). An imbedding $h: M \rightarrow W$ will be called a *Heegaard imbedding* if $M' = h(M)$ is a Heegaard surface in W . M' thus splits W into two handlebodies A and B . The orientations in M and W define a *positive normal direction* along M' , and we shall make convention that A is on this positive side of M' : A is the *positive handlebody*.

We now restrict W to be a Z_2 -homology sphere. Then we recall Seifert's *linking form* λ on $H_1(M', Z_2)$: for $a, b \in H_1(M', Z_2)$, $\lambda(a, b)$ is defined to be the mod 2 linking of a and b^+ , where b^+ is got by pushing b off of M' in the positive normal direction. Then λ is a bilinear form, and the *self-linking form* ω on $H_1(M', Z_2)$ is given by $\omega(a) = \lambda(a, a)$. ω is an Sp -quadratic form on $H_1(M', Z_2)$ and it may be pulled back to $H_1 = H_1(M, Z_2)$ by means of the imbedding h . We denote the resulting Sp -form by ω_h to indicate its dependence on the imbedding, and call it the *form induced by h* .

Let HA be the kernel of the map $H_1 \rightarrow H_1(A, Z_2)$ induced by the "inclusion" $M \xrightarrow{h} M' \subset A$, and HB the kernel corresponding to handlebody B . The fact that W is a Z_2 -homology sphere implies the following facts:

- (a) H_1 is the direct sum of HA and HB .
- (b) HA and HB are (maximal) isotropic subspaces of H_1 , that is, e.g., $a_1 \cdot a_2 = 0$ for any $a_1, a_2 \in HA$.
- (c) HA and HB are dually paired by the intersection form on H_1 , and so the latter has an Sp -basis a_i, b_i with $a_i \in HA, b_i \in HB$.

Furthermore, given any such basis, the a_i 's may be represented by disjoint SCC's α_i in M such that $h(\alpha_i)$ bound disjoint discs in A (thus, A cut along these discs becomes a 3-ball); likewise for the b_i 's and B . But this implies that $\omega_h(a_i) = \omega_h(b_i) = 0$, and hence that $\alpha(\omega_h) = 0$. Conversely, suppose W has a Heegaard surface of genus g , and let ω be any form of zero Arf invariant. Let $h_0: M \rightarrow W$ be some Heegaard imbedding of M with induced form ω_0 . Since $\omega_0 \in \Psi$ also, we know by Arf's theorems that there is a $v \in \text{Sp}$ with $v^*(\omega_0) = \omega$; further, v is actually the induced homomorphism of some homeomorphism $f: M \rightarrow M$. Putting $h = h_0f$, we have h a Heegaard imbedding with induced form $\omega_h = f^*(\omega_0) = v^*(\omega_0) = \omega$. We have shown

LEMMA 5. *If W is a Z_2 -homology sphere of Heegaard genus $< g$, then the Sp -quadratic form ω on H_1 is induced by some Heegaard imbedding of M into W iff $\alpha(\omega) = 0$, i.e., iff $\omega \in \Psi$.*

6. Splitting along a Heegaard surface and the Rochlin invariant. Let $h: M \rightarrow S^3$ be a Heegaard imbedding, and suppose we are given an element k of $\mathcal{G} (= \mathcal{G}(M))$. We

form a 3-manifold $M(h, k)$ as follows: split S^3 along $h(M)$ into the two handlebodies A and B (recall that A is the positive handlebody). They have the common boundary $h(M)$, and we reglue A to B along this boundary by the map k ; more precisely: x in $h(M) = \partial B$ glued to $hkh^{-1}(x)$ in $h(M) = \partial A$. The condition $k \in \mathcal{G}$ implies that $M(h, k)$ is a homology 3-sphere, and so we may define its Rochlin invariant $\mu(h, k) \in \mathbb{Z}_2$. In what follows we will show how $\mu(h, k)$ is related to the Birman-Craggs homomorphisms; to begin with, we recall the definitions and results of their paper [BC].

We start with an oriented genus g handlebody V_g and an oppositely oriented copy of it, written $-V_g$. Given any map f in the mapping class group \mathfrak{N} of $M = \partial V_g$, we create a 3-manifold $W(f)$ by identifying x in $M = \partial V_g$ with $f(x)$ in $M = \partial(-V_g)$. Suppose now that $h_1, h_2 \in \mathfrak{N}$ are such that $W(h_1h_2)$ is a \mathbb{Z}_2 -homology sphere; then so is $W(h_1kh_2)$ for any $k \in \mathcal{G}$, and the difference of the μ -invariants of these two manifolds (which are rational numbers mod 1) is defined

$$\rho_{h_1, h_2}(k) = \mu(W(h_1kh_2)) - \mu(W(h_1h_2)).$$

It is, for each such pair h_i , a homomorphic function of $k \in \mathcal{G}$. These are the Birman-Craggs homomorphisms (in [BC] the values of ρ lie in $\{0, \frac{1}{2}\} \text{ mod } 1$; we shall multiply everywhere by 2 to make the values lie in $\{0, 1\} \text{ mod } 2$, i.e., \mathbb{Z}_2).

In the proof of Theorem 8 of [BC] we find the following two formulas:

$$\rho_{h_2, h_1}(k) = \rho_{1, h_2h_1}(h_2kh_2^{-1})$$

and, putting $h = h_2h_1$,

$$\rho_{1, h}(k) = \rho_{1, f_2f_1}(k) = \rho_{1, s}(f_2^{-1}kf_2),$$

where s is a single fixed map such that $W(s) = S^3$ and the f_i 's are suitably chosen maps depending on h . These two formulas show that every Birman-Craggs homomorphism ρ is of the form

$$\rho(k) = \rho_{1, s}(fkf^{-1}) \text{ for some } f \in \mathfrak{N}.$$

We note that by definition we have

$$\rho_{1, s}(k) = \mu(W(ks)) - \mu(W(s)) = \mu(W(ks)), \text{ since } W(s) = S^3.$$

Let now h_0 be the imbedding $M \xrightarrow{\text{incl}} V_g \xrightarrow{\text{incl}} W(s) = S^3$; h_0 is a Heegaard imbedding, and it is easy to see that the manifold $M(h_0, k)$ is just $W(ks)$. Thus we have

$$\rho_{1, s}(k) = \mu(M(h_0, k)) = \mu(h_0, k).$$

LEMMA 6. $M(hf, k) = M(h, fkf^{-1})$ for $f \in \mathfrak{N}$, $k \in \mathcal{G}$ and h a Heegaard imbedding of M into S^3 .

PROOF. Note that this is meaningful, since $hf: M \rightarrow S^3$ is also a Heegaard imbedding (same image!). The equality follows from the fact that both manifolds are defined by gluing x to $hfkf^{-1}h^{-1}(x)$.

COROLLARY. $\mu(hf, k) = \mu(h, fkf^{-1})$.

LEMMA 7. Every Birman-Craggs homomorphism ρ is of the form $\rho(k) = \mu(h, k)$ for some Heegaard imbedding $h: M \rightarrow S^3$. Conversely, for any Heegaard imbedding h , $\mu(h, -): \mathcal{G} \rightarrow Z_2$ is a Birman-Craggs homomorphism.

PROOF. To prove the first statement, let $\rho(k)$ be given by $\rho_{1,x}(fkf^{-1})$. Then we have $\rho(k) = \mu(h_0, fkf^{-1}) = \mu(h_0f, k)$ by the above corollary. This proves the statement, since h_0f is a Heegaard imbedding.

To prove the converse, we will show that $\mu(h, k) = \mu(h_0, fkf^{-1}) = \rho_{1,x}(fkf^{-1})$ for some $f \in \mathcal{N}$. Now there exists by Waldhausen's results (see [W]) a homeomorphism $H: S^3 \rightarrow S^3$ such that $Hh(M) = h_0(M)$. Further, H may be chosen to be orientation preserving on S^3 and also to take the positive handlebody of $h(M)$ to that of $h_0(M)$ —that is, to be orientation preserving from $h(M)$ to $h_0(M)$. Hence there is a map $f \in \mathcal{N}$ such that $Hh = h_0f$.

Now clearly $M(Hh, k)$ is homeomorphic to $M(h, k)$, so we get $\mu(h, k) = \mu(Hh, k) = \mu(h_0f, k) = \mu(h_0, fkf^{-1})$. Q.E.D.

This lemma tells us that the distinct Birman-Craggs homomorphisms are in 1-1 correspondence with the distinct functions of the type $\mu(h, -)$.

7. Computing $\mu(h, k)$. In this section we will compute $\mu(h, k)$ for given h, k . Since for fixed h , $\mu(h, k)$ is homomorphic in k , it suffices to determine its value for generators of \mathcal{G} . We shall thus compute $\mu(h, k)$ when k is a Powell generator (see [P]). These are of two types:

Type I. If γ is a bounding simple closed curve (BSCC) in M , then T_γ , the twist on γ , is in \mathcal{G} .

Type II. $T_{\gamma_1}T_{\gamma_2}^{-1}$, where γ_1, γ_2 are disjoint, homologous SCC's in M , with γ_i not homologous to zero, is also in \mathcal{G} . Powell shows in [P] that the totality of Types I and II maps generates \mathcal{G} .

To begin with, let us attack the conceptually simpler case when M is already contained in S^3 (h being thus the inclusion); we write $M(\text{incl}, k)$ and $\mu(\text{incl}, k)$ simply as $M(k), \mu(k)$. If ω is the mod 2 self-linking form of M , then we have

LEMMA 8a. Let γ be a BSCC in M bounding the subsurface $S \subset M$, and let A_i, B_i ($i = 1, \dots, \text{genus}(S)$) be a symplectic basis for $H_1(S)$. Then

$$\mu(T_\gamma) = \sum_{i=1}^{\text{gen}(S)} \omega(A_i)\omega(B_i).$$

PROOF. The results of [GA, Theorem 4] (see also [G, Theorem 2]) show that $M(T_\gamma)$ is got by doing surgery on the curve $\gamma \subset M \subset S^3$ and that $\mu(T_\gamma)$ is the Arf invariant $\alpha(\gamma)$ of γ in S^3 . The Arf invariant of a knot is defined to be the Arf invariant of the self-linking form of any Seifert surface spanning the knot, and this does not depend on the choice of surface. In particular, we may choose it to be $S \subset M$, and then the self-linking form is just ω restricted to $H_1(S)$, whence the lemma follows.

LEMMA 8b. Let $f = T_{\gamma_1}T_{\gamma_2}^{-1}$ be a Type II generator; then $\omega(\gamma_1) = 1$ implies that $\mu(f) = 0$.

PROOF. We consider the link $L = \gamma_1 \cup \gamma_2$ in S^3 , and suppose that they link m times. Since γ_1 and γ_2 are disjoint, the linking number $L(\gamma_1, \gamma_2)$ is the same as $L(\gamma_1, \gamma_2^+)$ where $\gamma_2^+ = \gamma_2$ pushed normally up off M , and this is congruent to $\lambda(\gamma_1, \gamma_2) \pmod 2$, where λ is the mod 2 linking form of M in S^3 . Since γ_1 and γ_2 are homologous, we have $\lambda(\gamma_1, \gamma_2) = \lambda(\gamma_1, \gamma_1) = \omega(\gamma_1) \pmod 2$.

In our case, $\omega(\gamma_1) = 1 \pmod 2$, so we have $m \equiv 1 \pmod 2$, i.e., m is odd.

It is now easily verifiable that the manifold $M(f)$ is the same as the 3-manifold got by doing surgery on the link L with framing $m + 1$ on γ_1 and $m - 1$ on γ_2 , and that this bounds the surgery 4-manifold with quadratic form on H_2 having the matrix

$$\begin{pmatrix} m + 1 & m \\ m & m - 1 \end{pmatrix}.$$

$M(f)$ is a homology sphere, and since m is odd, the above form is even; its signature is zero, and so we get $\mu(M(f)) = 0$. Q.E.D.

This lemma is essentially due to Craggs, as proved in the original manuscript of [BC] (deleted from the published version).

Finally we must consider generators of Type II for which $\omega(\gamma_1) = 0$, that is, $L(\gamma_1, \gamma_2) = m$ is even; say $= 2k$. Let γ_1, γ_2 bound the surface $S \subset M$; abstractly, S looks like Figure 1.

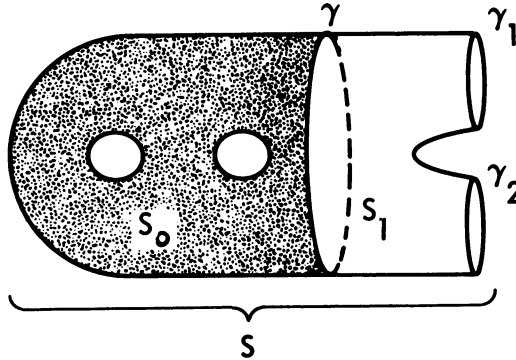


FIGURE 1

We choose a γ as shown in the figure (i.e., γ bounds a surface S_0 in S , and $\gamma \cup \gamma_1 \cup \gamma_2$ bounds a piece S_1 of genus zero in S). Clearly $H_1(S, Z_2) = H_1(S_0, Z_2) \oplus V$, where V is generated by γ_1 . We may choose a symplectic basis for $H_1(S_0, Z_2)$, say A_i, B_i , and then we have $\alpha(\gamma) = \sum_{i=1}^{g(S_0)} \omega(A_i)\omega(B_i)$ by definition.

LEMMA 8c. Let $f = T_{\gamma_1} T_{\gamma_2}^{-1}$ be a generator of Type II, with $\omega(\gamma_i) = 0$ and $\gamma_1 \cup \gamma_2$ bounding $S \subset M$. Then if γ, S_0, A_i, B_i are chosen as above, we have

$$\mu(f) = \alpha(\gamma) = \sum_{i=1}^{g(S_0)} \omega(A_i)\omega(B_i).$$

REMARK. This formula shows that $\alpha(\gamma)$ actually does not depend on the choice of γ .

PROOF. The proof is long and will be divided into a number of sections.

(A) Let X be a closed 4-manifold and $K \subset X$ a “characteristic surface” of X , i.e., differentiably imbedded surface (orientable) whose homology class mod 2 is dual to the second Stiefel-Whitney class w_2 of X . (This is equivalent to the algebraic condition $x \cdot x \equiv K \cdot x \pmod 2$ for all $x \in H_2(X, \mathbb{Z}_2)$.)

If σ_X is the signature of the intersection form on $H_2(X)$, then we have $\sigma_X - K \cdot K$ is divisible by 8, and $(\sigma_X - K \cdot K)/8 \equiv \alpha(K) \pmod 2$ where $\alpha(K)$ is the “Arf invariant” of $K \subset X$, suitably defined (see e.g., [FK]). References for these facts may be found in [FK], or [MH, pp. 24–25].

If W is a 4-manifold with boundary $\partial W = V$ a homology 3-sphere and characteristic surface $K \subset W$, then we get $(\sigma_W - K \cdot K)/8$ is still integral, but the connection with $\alpha(K)$ must now read

$$\frac{\sigma_W - K \cdot K}{8} + \mu(V) \equiv \alpha(K) \pmod 2.$$

(See for example [G, Section 4.2 and Theorem 1].)

(B) Consider now the link of two components $L = \gamma_1 \cup \gamma_2$ in S^3 ; γ_1, γ_2 link evenly, say $2k$. We do a surgery with framing $2k + 1$ on γ_1 and $2k - 1$ on γ_2 . The surgery manifold W is got by attaching 2-handles to tubular neighborhoods of γ_1, γ_2 in $S^3 = \partial D^4$. As in the proof of Lemma 8b, we see that $V = \partial W$ is the same as $M(f)$, where $f = T_{\gamma_1} T_{\gamma_2}^{-1}$.

Let D_i be the 2-disc core of these 2-handles, so that $\partial D_i = \gamma_i$, and let $C_i =$ cone over γ_i in D^4 , so that $\partial C_i = -\gamma_i$. The homology classes of $E_i = C_i + D_i$ form a basis for $H_2(W)$; the intersection form in terms of this basis is

$$\begin{pmatrix} 2k + 1 & 2k \\ 2k & 2k - 1 \end{pmatrix}.$$

Its signature is zero; furthermore, $E_2 - E_1$ is a *characteristic class*, since from this matrix we easily deduce that

$$x \cdot (E_2 - E_1) \equiv x \cdot x \pmod 2 \text{ for } x = E_1 \text{ or } E_2.$$

(C) Let now $\gamma_1 \cup \gamma_2$ bound S in M ; S acquires an orientation from M , and we orient γ_i so as to have $\partial S = \gamma_1 - \gamma_2$. Then

$$\partial(S - D_1 + D_2) = \gamma_1 - \gamma_2 - \gamma_1 + \gamma_2 = 0,$$

so $S - D_1 + D_2$ is an oriented (smoothable) surface K in W . Furthermore, $\partial(S + C_1 - C_2) = 0$ also, and $S + C_1 - C_2$ is actually a cycle in D^4 , and so bounds.

Hence K is homologous to $S - D_1 + D_2 - (S + C_1 - C_2) = -(D_1 + C_1) + (D_2 + C_2) = E_2 - E_1$; i.e., K is a *characteristic surface* for W . Note that

$$\begin{aligned} K \cdot K &= (E_2 - E_1) \cdot (E_2 - E_1) = E_2 \cdot E_2 - 2E_2 \cdot E_1 + E_1 \cdot E_1 \\ &= 2k - 1 - 4k + 2k + 1 = 0 \end{aligned}$$

and hence $(\sigma_W - K \cdot K)/8 = 0$.

We have thus

$$\mu(f) = \mu(V) = \alpha(K).$$

(D) Since $K = S \cup$ discs D_i , S carries all the homology of K . Now let γ be, as in Figure 1, a SCC in S such that $\gamma_1 \cup \gamma_2 \cup \gamma$ bounds a genus zero piece S_1 of S , and γ bounds (on its other side) S_0 in S . Then in K , $S_1 \cup D_1 \cup D_2$ is a disc D , and so $H_1(S_0) \cong H_1(K)$.

Thus the Arf invariant of K is just that of S_0 , and since $S_0 \subset S^3$, $\alpha(S_0)$ is defined in the usual way as the Arf invariant of its self-linking form, which is equal to $\alpha(\gamma)$ by definition. This shows also that the number $\alpha(S_0) = \alpha(\gamma)$ does not depend on the choice of γ , since $\alpha(S_0) = \alpha(K)$, and $\alpha(K)$ is independent of such choice. By (C), we have $\mu(f) = \alpha(\gamma)$ for any choice of γ . This concludes the proof.

The above three lemmas give us the value of $\mu(h, k)$ when h is an inclusion. Suppose now that h is an arbitrary Heegaard imbedding; if $\gamma \subset M$ is a BSCC, then $h(\gamma)$ is a BSCC in $h(M)$ and $M(h, T_\gamma)$ is clearly the same as $M(\text{incl}, T_{h(\gamma)})$. Further, if γ bounds S in M and A_i, B_i is a symplectic basis for $H_1(S)$, then $h(A_i), h(B_i)$ is likewise for $h(S) \subset h(M)$, and hence we get

$$\mu(h, T_\gamma) = \mu(\text{incl}, T_{h(\gamma)}) = \sum_i \omega(hA_i)\omega(hB_i),$$

where ω is the linking form on $h(M)$. But the induced form ω_h on M by definition satisfies $\omega_h(x) = \omega(hx)$, and hence we have

$$\mu(h, T_\gamma) = \sum_i \omega_h(A_i)\omega_h(B_i).$$

This argument may also be applied to the results of Lemmas 8b–c to give, finally

THEOREM 1. *Let $h: M \rightarrow S^3$ be a Heegaard imbedding with induced form ω_h on M . Then for Powell generators T_γ and $T_{\gamma_1}T_{\gamma_2}^{-1}$ we have:*

- (a) $\mu(h, T_\gamma) = \sum_{i=1}^{g(S)} \omega_h(A_i)\omega_h(B_i)$, where A_i, B_i is a symplectic basis of the homology of a surface $S \subset M$ which γ bounds.
- (b) $\mu(h, T_{\gamma_1}T_{\gamma_2}^{-1}) = 0$ if $\omega_h(\gamma_1) = 1$.
- (c) $\mu(h, T_{\gamma_1}T_{\gamma_2}^{-1}) = \sum_{i=1}^{g(S_0)} \omega_h(A_i)\omega_h(B_i)$ for A_i, B_i a symplectic basis of the homology of a surface S_0 chosen as in Lemma 8c.

COROLLARY 1. $\mu(h, k)$ depends only on ω_h and k .

This corollary enables us to write simply $\mu(\omega, k)$ for the Rochlin invariant of any $M(h, k)$ for which $\omega_h = \omega$. Lemma 5 tells us then that $\mu(\omega, k)$ is defined for any $\omega \in \Psi$ and $k \in \mathcal{G}$. We also have the following:

COROLLARY 2. $\mu(\omega, fkf^{-1}) = \mu(f^*(\omega), k)$ for $\omega \in \Psi, f \in \mathfrak{N}, k \in \mathcal{G}$.

PROOF. Let $h: M \rightarrow S^3$ induce ω , so that hf induces $f^*(\omega)$. Then by the corollary to Lemma 6,

$$\mu(\omega, fkf^{-1}) = \mu(h, fkf^{-1}) = \mu(hf, k) = \mu(f^*(\omega), k). \quad \text{Q.E.D.}$$

8. Enumerating the Birman-Craggs homomorphisms. We introduce now the notation $\rho_\omega(k) = \mu(\omega, k)$ for $\omega \in \Psi$, paralleling the notation of [BC]. As we saw in Lemma 7, these functions $\rho_\omega: \mathcal{G} \rightarrow \mathbb{Z}_2$ comprise the totality of Birman-Craggs homomorphisms. Our next goal is to show that these homomorphisms are actually distinct.

LEMMA 9. Let ω be an Sp-quadratic form on H_1 . Then given any nonzero $a \in H_1$, there is an element $b \in H_1$ such that $a \cdot b = 1$ and $\omega(b) = 1$.

PROOF. Choose b_0 so that $a \cdot b_0 = 1$. If $\omega(b_0) = 1$ we are done; otherwise, proceed as follows. Using our continued assumption that the genus is > 2 , we can extend the partial symplectic basis a, b_0 to a larger one $a, b_0; c, d$, where $(a$ or $b_0) \cdot (c$ or $d) = 0$ and $c \cdot d = 1$. Now there is a linear combination of c, d for which $\omega = 1$; for if $\omega(c) = \omega(d) = 0$, then $\omega(c + d) = 0 + 0 + c \cdot d = 1$. Let e be such a linear combination and put $b = b_0 + e$. We have then $a \cdot b = a \cdot b_0 + a \cdot e = 1 + 0 = 1$, and $\omega(b) = \omega(b_0) + \omega(e) + b_0 \cdot e = 0 + 1 + 0 = 1$. Q.E.D.

LEMMA 10. If $\omega, \omega' \in \Psi$ are distinct, then $\rho_\omega \neq \rho_{\omega'}$.

PROOF. Since $\omega \neq \omega'$, there is an $a \in H_1$ such that $\omega(a) \neq \omega'(a)$; let us assume for example that $\omega(a) = 1$ and $\omega'(a) = 0$. By the previous lemma we choose b such that $a \cdot b = 1, \omega(b) = 1$. The mod 2 homology classes a, b may be represented by SCC's α, β of M which intersect geometrically once (transversely). Let S be a regular neighborhood of $\alpha \cup \beta$ and put $\gamma = \partial S$; then γ is a BSCC in M , bounding S , and $H_1(S)$ has symplectic basis a, b . Applying Theorem 1 we get

$$\begin{aligned} \rho_\omega(T_\gamma) &= \omega(a)\omega(b) = 1 \cdot 1 = 1, \quad \text{but} \\ \rho_{\omega'}(T_\gamma) &= \omega'(a)\omega'(b) = 0 \cdot \omega'(b) = 0. \quad \text{Q.E.D.} \end{aligned}$$

Combining now Lemmas 7 and 10 we get

THEOREM 2. The set of homomorphisms ρ_ω ($\omega \in \Psi$) is the set of distinct Birman-Craggs homomorphisms. The Birman-Craggs homomorphisms are thus in natural 1-1 correspondence with the quadratic forms on H_1 which induce the intersection form there and have Arf invariant zero.

COROLLARY. Each ρ_ω is surjective. If $f \in \mathfrak{N}$ is in the orthogonal group of ω , i.e., $f^*(\omega) = \omega$, then $\rho_\omega(fkf^{-1}) = \rho_\omega(k)$.

PROOF. The first statement was proved in [BC, Theorem 8]; the second follows immediately from Corollary 2 of Theorem 1.

Using Theorem 2, we may now enumerate the homomorphisms; we need simply count the elements of Ψ . Although this is a well-known result, we reproduce the argument here. (We wish to thank the referee for considerably simplifying our original argument.)

By Lemma 1, $|\Omega_g|$ (the number of elements in Ω_g) is 2^{2g} . Starting with a symplectic basis a_i, b_i ($i = 1, \dots, g$), we have $\omega \in \Psi$ iff

$$\sum_{i=1}^g \omega(a_i)\omega(b_i) = 0 = \sum_{i=1}^{g-1} \omega(a_i)\omega(b_i) + \omega(a_g)\omega(b_g).$$

The RHS is zero iff:

- (a) the sum is zero and $\omega(a_g)\omega(b_g) = 0$; or
- (b) the sum is one and $\omega(a_g)\omega(b_g) = 1$.

Now (a) is equivalent to $\omega|(\text{subspace } a_i, b_i, i < g)$ is in Ψ_{g-1} and $\omega(a_g)\omega(b_g) = 0$. There are three choices of $\omega(a_g), \omega(b_g)$ satisfying the latter condition, and $|\Psi_{g-1}|$

satisfying the former. Thus (a) occurs $3|\Psi_{g-1}|$ times. Likewise (b) occurs $|\Omega_{g-1}| - |\Psi_{g-1}|$ times, since there is only one solution to $\omega(a_g)\omega(b_g) = 1$, and

$$\sum_{i=1}^{g-1} \omega(a_i)\omega(b_i) = 1 \quad \text{iff } \omega(\text{subspace}) \text{ is in } \Omega_{g-1} - \Psi_{g-1}.$$

Hence we get

$$|\Psi_g| = |\Omega_{g-1}| + 2|\Psi_{g-1}| = 2|\Psi_{g-1}| + 2^{2g-2}.$$

Now $\Psi_0 = 1$, and so we see that $|\Psi_g| = 2^{2g-1} + 2^{g-1}$ satisfies the recursion and initial conditions and so must be the correct value. We have then

THEOREM 3. *The number of distinct Birman-Craggs homomorphisms in genus g is $2^{g-1}(2^g + 1)$.*

9. The space of Birman-Craggs homomorphisms. In [BC, Section 4] we find defined (using our present notation) the following subgroup of \mathcal{G} :

$$\mathcal{C} = \bigcap_{\omega \in \Psi} \text{Ker } \rho_\omega.$$

The problem of finding \mathcal{C} more explicitly, and computing its index in \mathcal{G} (which is finite) is also mentioned in [BC]. We note that \mathcal{G}/\mathcal{C} is a finite group in which every element has order 2, since $\rho_\omega(k^2) = 2\rho_\omega(k) = 0$ for all ω, k , i.e., $k^2 \in \mathcal{C}$. Thus \mathcal{G}/\mathcal{C} is a Z_2 -vector space U of finite dimension, and the homomorphisms ρ_ω all factor through U and in fact span its dual space U^* . We thus call U^* *the space of Birman-Craggs homomorphisms*. The dimension of U^* is possibly less than the number of the homomorphisms ρ_ω , so we are led to ask:

- (a) What is the dimension of U^* (i.e., U)?
- (b) Can we find all linear relations among the generators ρ_ω of U^* ?

In order to attack these problems, we introduce the following. For $k \in \mathcal{G}$, let $\sigma_k: \Psi \rightarrow Z_2$ be defined by $\sigma_k(\omega) = \mu(\omega, k)$; σ is thus a sort of dual version of ρ : $\rho_\omega(k) = \mu(\omega, k) = \sigma_k(\omega)$. Now by definition of $\mathcal{C} = \bigcap_{\omega \in \Psi} \text{Ker } \rho_\omega = \{k \in \mathcal{G} \mid \sigma_k(\omega) = 0, \text{ all } \omega \in \Psi\}$, we have $\sigma_k = 0$ iff $k \in \mathcal{C}$. Furthermore,

$$\sigma_{k_1 k_2}(\omega) = \rho_\omega(k_1 k_2) = \rho_\omega(k_1) + \rho_\omega(k_2) = \sigma_{k_1}(\omega) + \sigma_{k_2}(\omega),$$

and thus

LEMMA 11. *σ is a homomorphism from \mathcal{G} to the vector space of functions $\Psi \rightarrow Z_2$, with kernel \mathcal{C} ; σ can thus be thought of as a 1-1 homomorphism of U into this function space.*

To determine the image of U in this function space it suffices to look at the generators of \mathcal{G} . To this end, we apply Lemmas 8a–c.

Case 1. Let $k = T_\gamma$, γ a BSCC bounding $S \subset M$ with symplectic basis A_i, B_i . The formula $\rho_\omega(k) = \sum_{i=1}^{g(S)} \omega(A_i)\omega(B_i)$ of Lemma 8a may be rewritten in the notation of §4 as

$$\sigma_k(\omega) = \sum_{i=1}^{g(S)} \bar{A}_i(\omega)\bar{B}_i(\omega);$$

in other words, we have

LEMMA 12a. *If $k = T_\gamma$ with γ a bounding SCC, bounding $S \subset M$, and $H_1(S)$ having symplectic basis A_i, B_i ($i = 1, \dots, \text{genus}(S)$) then the function σ_k on Ψ is the restriction to it of the Boolean quadratic*

$$\sum_{i=1}^{g(S)} \overline{A_i B_i}.$$

We define \mathfrak{T} to be the subgroup \mathcal{G} generated by all such T_γ ; \mathfrak{T} is normal in \mathfrak{N} . The above lemma shows that σ maps \mathfrak{T} into the vector space of Boolean quadratic functions on Ψ . (For $g = 2$, $\mathcal{G} = \mathfrak{T}$, see [P].)

Case 2. Let $k = T_{\gamma_1} T_{\gamma_2}^{-1}$, and let S_0 , chosen as in Lemma 8c, have symplectic basis A_i, B_i , let also C be the homology class of the γ_i 's. The results of Lemmas 8b–c were

- (a) If $\omega(C) = 1$, then $\rho_\omega(k) = 0$.
- (b) If $\omega(C) = 0$, then $\rho_\omega(k) = \sum_{i=1}^{g(S_0)} \omega(A_i)\omega(B_i)$.

We may write these two results together in the form

$$\rho_\omega(k) = \left(\sum_i \omega(A_i)\omega(B_i) \right) (\omega(C) + 1)$$

or as in the following:

LEMMA 12b. *If $k = T_{\gamma_1} T_{\gamma_2}^{-1}$ then σ_k on Ψ is the restriction to it of the Boolean cubic*

$$\left(\sum_{i=1}^{g(S_0)} \overline{A_i B_i} \right) (\overline{C} + 1).$$

In Lemma 12a, we chose S to be one of the two pieces which γ bounds in M . This choice should not influence the function σ_k , which depends on γ alone. To see this, let S' be the other piece, with Sp-basis A'_j, B'_j . Then $A_i, A'_j; B_i, B'_j$ form a complete Sp-basis for all of H_1 ; hence $\sum_i \overline{A_i B_i} + \sum_j \overline{A'_j B'_j} = \alpha = 0$ on Ψ . In other words, $\sum_i \overline{A_i B_i} = \sum_j \overline{A'_j B'_j}$ on Ψ , as desired. In the situation of Lemma 12b, a complete basis is formed by $A_i, A'_j, C; B_i, B'_j, D$ for some appropriate class D , and now we get $\sum_i \overline{A_i B_i} + \sum_j \overline{A'_j B'_j} + \overline{CD} = 0$ on Ψ . Multiplying by $\overline{C} + 1$ and noting that $\overline{CD}(\overline{C} + 1) = 0$, we get the equality of the two functions $(\sum_i \overline{A_i B_i})(\overline{C} + 1)$ and $(\sum_j \overline{A'_j B'_j})(\overline{C} + 1)$ on Ψ .

Since \mathcal{G} is generated by the maps of Lemmas 12a and 12b we see that σ maps U into the vector space of Boolean cubic functions on Ψ . We shall next find the images $\sigma(\mathfrak{T})$ and $\sigma(\mathcal{G}) = \sigma(U)$ in this space.

LEMMA 13. *If $f \in \mathfrak{N}$, $k \in \mathcal{G}$, then the cubic $\sigma_{fkf^{-1}}$ is equal to $f(\sigma_k)$, where f acts on cubic polynomials in the usual way (i.e., adjoint to its action on Ω).*

PROOF. $\sigma_{fkf^{-1}}(\omega) = \mu(\omega, f k f^{-1}) =$ (by Corollary 2 to Theorem 1) $\mu(f^*(\omega), k) = \sigma_k(f^*(\omega)) = f(\sigma_k)(\omega)$.

This lemma tells us that $\sigma: U \rightarrow$ cubic functions on Ψ is not only a homomorphism, but actually an Sp-module map: for U has a natural Sp-module structure

defined by conjugation of \mathfrak{M} on \mathcal{G} . Thus $\text{Im } \sigma$ will be an Sp -submodule of the cubic function space, and this fact will enable us to show easily that σ is surjective. The same applies to $\sigma(\mathfrak{T})$ —that is, the image T of \mathfrak{T} in $U = \mathcal{G}/\mathcal{C}$ is an Sp -submodule of U by virtue of the normality of \mathfrak{T} in \mathfrak{M} , and $\sigma(T)$ is a submodule of the quadratic functions on Ψ . Again we will find σ to be surjective.

To begin with then, we choose an Sp -basis a_i, b_i for H_1 . If γ is the boundary of a regular neighborhood of $\alpha_1 \cup \beta_1$, α_1 and β_1 being SCC's intersecting once (transversely) and representing the classes a_1, b_1 , then T_γ is in \mathfrak{T} and by Lemma 12a we have $\sigma_{T_\gamma} = \bar{a}_1\bar{b}_1$ is in $\sigma(\mathfrak{T})$. Consider then the symplectic map $a_1 \rightarrow a_1 + b_1 - b_2, a_2 \rightarrow a_2 - b_1 + b_2$ (basis elements not mentioned are assumed fixed; note also the assumption $g \geq 2$). Applying this to $\bar{a}_1\bar{b}_1$, we get

$$(\overline{a_1 + b_1 - b_2})\bar{b}_1 = (\bar{a}_1 + \bar{b}_1 + \bar{b}_2 + 1)\bar{b}_1 = \bar{a}_1\bar{b}_1 + \bar{b}_1\bar{b}_2 \in \sigma(\mathfrak{T})$$

and hence $\bar{b}_1\bar{b}_2 \in \sigma(\mathfrak{T})$ also. By applying to these two quadratics the Sp maps of the types

- (a) $a_1 \rightarrow b_1, b_1 \rightarrow -a_1,$
- (b) $a_1 \leftrightarrow a_i, b_1 \leftrightarrow b_i,$

we see easily that all quadratic monomials in the basis elements \bar{a}_i, \bar{b}_i also lie in $\sigma(\mathfrak{T})$.

Next, apply $b_1 \rightarrow a_1 + b_1$ to $\bar{b}_1\bar{b}_2$ and get $(\overline{a_1 + b_1})\bar{b}_2 = (\bar{a}_1 + \bar{b}_1 + 1)\bar{b}_2 = \bar{a}_1\bar{b}_2 + \bar{b}_1\bar{b}_2 + \bar{b}_2 \in \sigma(\mathfrak{T})$. The first two terms are in $\sigma(\mathfrak{T})$, so $\bar{b}_2 \in \sigma(\mathfrak{T})$ also. Using (a) and (b) again puts all linear monomials in $\sigma(\mathfrak{T})$. Finally we apply $b_1 \rightarrow a_1 + b_1$ to \bar{b}_1 to get $\bar{a}_1 + \bar{b}_1 + 1$, and find that the constant function $1 \in \sigma(\mathfrak{T})$ too. We have now shown that $\sigma(\mathfrak{T})$ is the space of all Boolean quadratics on Ψ .

To get the cubics, we begin with $\bar{a}_1\bar{b}_1(\bar{b}_2 + 1) = \bar{a}_1\bar{b}_1\bar{b}_2 + \bar{a}_1\bar{b}_1$. This is in $\sigma(\mathcal{G})$ —by Lemma 12b, it is just the image of $T_{b_2}T_{b_2}^{-1}$ with b_2, b_2' as in Figure 2.

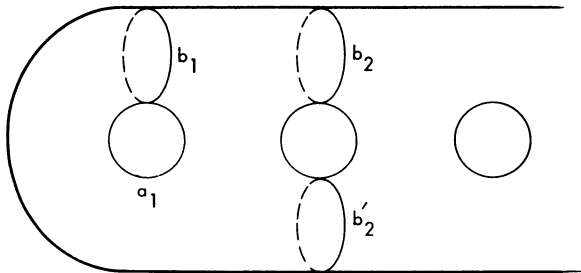


FIGURE 2

Since we already have all quadratics, $\bar{a}_1\bar{b}_1\bar{b}_2 \in \sigma(\mathcal{G})$. Now we apply to it the map $a_1 \rightarrow a_1 + b_1 - b_2, a_2 \rightarrow a_2 - b_1 + b_2$ (note the assumption here that $g \geq 3$) and we get $\bar{a}_1\bar{b}_1\bar{b}_2 + \bar{b}_1\bar{b}_2\bar{b}_3$, showing $\bar{b}_1\bar{b}_2\bar{b}_3 \in \sigma(\mathcal{G})$. The application of transformations (a), (b) to these two cubics gives us all cubic monomials. This finishes the proof of

THEOREM 4. *For $g \geq 3$, the map σ is an isomorphism from $U = \mathcal{G}/\mathcal{C}$ to the space of Boolean cubic functions on Ψ . For $g \geq 2$, the image T of \mathfrak{T} in U is isomorphic via σ to the space of Boolean quadratics on Ψ .*

It remains for us to compute the dimensions of T, U over Z_2 . The dimension of all Boolean cubics on the affine space Ω is, since $\dim \Omega = 2g$, just

$$\sum_{i=0}^3 \binom{2g}{i};$$

there are $\binom{2g}{3}$ cubic monomials, $\binom{2g}{2}$ quadratics, etc. $\dim U$ is less than this, however, by virtue of the fact that the restriction map: functions on $\Omega \rightarrow$ functions on Ψ , has nontrivial kernel; for example, the Arf invariant α is a quadratic function on Ω which is zero on Ψ . We need the dimension of this kernel, the dimension of all cubics which are zero on Ψ .

LEMMA 14. *If f is quadratic on Ω and zero on Ψ , then $f = \lambda\alpha$ for some constant λ ; if f is cubic and the genus is ≥ 3 then $f = \lambda\alpha$ for some linear function λ (using Boolean multiplication).*

PROOF. Choose an Sp-basis a_i, b_i and express f in terms of the basis \bar{a}_i, \bar{b}_i ; it may then be separated into a sum $f = K + Q + L + C$, where K is the pure cubic part, Q the pure quadratic, L the linear and C the constant. The proof proceeds by examining the value of f on certain specific forms $\omega \in \Psi$. By Lemma 1, these ω 's may be specified by giving their values on the basis; we shall do this by giving just those basis elements for which $\omega = 1$.

To begin with, we let $\omega = 0$ on all basis elements; since all nonconstant monomials evaluate to zero on this ω , we have $f(\omega) = C$. Hence, $C = 0$. Next, let $\omega = 1$ on a_i alone; $\omega \in \Psi$ and $f(\omega)$ is clearly just the coefficient of \bar{a}_i in f , which must then be 0. This is true for all a_i , and likewise all b_i , and thus we get $L = 0$.

Turning to the quadratic monomials $\bar{e}_1\bar{e}_2$, first look at those for which $e_1 \cdot e_2 = 0$, e.g., $e_1 = a_i, e_2 = b_j$ ($i \neq j$). We will show its coefficient is zero. (The proof for other monomials with $e_1 \cdot e_2 = 0$, namely $\bar{a}_i\bar{a}_j$ or $\bar{b}_i\bar{b}_j$, is parallel.) But let $\omega = 1$ on a_i and b_j ; again we get $\omega \in \Psi$ and $f(\omega)$ is just the coefficient of $\bar{a}_i\bar{b}_j$. We have now shown that Q must be of the form $\sum_i \lambda_i \bar{a}_i\bar{b}_i$ for some constants λ_i . If f is quadratic (i.e., $K = 0$) then using the form $\omega \in \Psi$ which is 1 on a_i, b_i, a_j, b_j ($i \neq j$) we find easily that $f(\omega) = \lambda_i + \lambda_j$, and conclude that $\lambda_i = \lambda_j$ for all i, j . In other words, $f = Q = \lambda \sum_i \bar{a}_i\bar{b}_i = \lambda\alpha$ for some constant λ . This proves the first statement.

Suppose finally that $f = K + Q, K \neq 0$. We know that $Q = \sum_i \lambda_i \bar{a}_i\bar{b}_i$; but the quadratic part of $(\sum_i \lambda_i \bar{a}_i)\alpha$ is precisely the same. Hence $f - (\sum_i \lambda_i \bar{a}_i)\alpha$ is a pure cubic, still zero on Ψ , and is clearly of the form $\lambda\alpha$ for λ linear iff f is; we may thus assume f to be a pure cubic. If we examine the monomials $\bar{e}_1\bar{e}_2\bar{e}_3$ for which $e_i \cdot e_j = 0, i, j = 1, 2$ or 3 , we find as in the quadratic case that they must have zero coefficient: simply apply f to the $\omega \in \Psi$ which is 1 on e_1, e_2, e_3 . Thus the only terms possible in f are those of the form $\bar{a}_i\bar{b}_i\bar{a}_k$ and $\bar{a}_i\bar{b}_i\bar{b}_k$ ($i \neq k$); let their coefficients be α_{ik} and β_{ik} respectively. Let again $\omega \in \Psi$ be 1 on a_i, b_i, a_j, b_j , and $\omega' \in \Psi$ be 1 on b_k in addition (i, j, k distinct; note that we are using the hypothesis that $g \geq 3$ here). Then we get

$$0 = f(\omega') = \alpha_{ij} + \beta_{ij} + \beta_{ik} + \alpha_{ji} + \beta_{ji} + \beta_{jk}$$

and

$$0 = f(\omega) = \alpha_{ij} + \beta_{ij} + \alpha_{ji} + \beta_{ji}.$$

Subtracting, we get $\beta_{ik} + \beta_{jk} = 0$, thus $\beta_{ik} = \beta_{jk}$ is independent of i, j , and we may simply write it as β_k ; likewise define α_k . Then the equation for $f(\omega) = 0$ may be rewritten $\alpha_i + \beta_i = \alpha_j + \beta_j$ for all i, j . Call this value r ; we put

$$L = \sum_{k=1}^g (\alpha_k \bar{a}_k + \beta_k \bar{b}_k)$$

and get

$$L\alpha = \sum_{k \neq i} (\alpha_k \bar{a}_i \bar{b}_i \bar{a}_k + \beta_k \bar{a}_i \bar{b}_i \bar{b}_k) + \sum_k (\alpha_k + \beta_k) \bar{a}_k \bar{b}_k = f + r\alpha.$$

Hence $f = (L - r)\alpha$. Q.E.D.

LEMMA 15. *If λ is linear and $\lambda\alpha = 0$ (Boolean multiplication) then $\lambda = 0$.*

PROOF. Let $\lambda = \sum_i (\alpha_i \bar{a}_i + \beta_i \bar{b}_i) + \gamma$. The coefficient of $\bar{a}_1 \bar{b}_1 \bar{a}_j$ ($j > 1$) in $\lambda\alpha$ is α_j , so $\alpha_j = 0$. Likewise $\beta_j = 0$ ($j > 1$), and looking at $\bar{a}_2 \bar{b}_2 \bar{a}_1$ and $\bar{a}_2 \bar{b}_2 \bar{b}_1$ shows us that $\alpha_1 = \beta_1 = 0$ also. Hence $\lambda = \gamma$ is constant, and so clearly is zero.

Recalling that B_r is the space of Boolean polynomials of degree $< r$ on Ω , the two previous lemmas give us the following two exact sequences:

$$0 \rightarrow B_1 \xrightarrow{\text{mult by } \alpha} B_3 \rightarrow \text{cubic functions on } \Psi \rightarrow 0,$$

$$0 \rightarrow B_0 (= \text{constants}) \xrightarrow{\text{mult by } \alpha} B_2 \rightarrow \text{quadratic functions on } \Psi \rightarrow 0.$$

By virtue of the isomorphisms of U and T respectively with the right ends of these sequences, we get

THEOREM 5. *For $g \geq 3$, $\dim U = \binom{2g}{3} + \binom{2g}{2} = \frac{1}{3}g(4g^2 - 1)$; for $g \geq 2$, $\dim T = \binom{2g}{2} + \binom{2g}{1} = g(2g + 1)$.*

PROOF. The dimension of B_r is

$$\sum_{i=0}^r \binom{2g}{i}. \quad \text{Q.E.D.}$$

Note that (as previously remarked) $\mathcal{G} = \mathcal{T}$ when $g = 2$ and hence $U = T$. The above formulas for $\dim U$ and $\dim T$ agree when $g = 2$, so the first formula is actually valid for all $g \geq 2$.

It is not known if \mathcal{G} is finitely generated. We have, however, the following

COROLLARY. *\mathcal{G} is generated by not less than $g(4g^2 - 1)/3$ of its elements.*

PROOF. Follows from the same statement for its quotient U .

10. The case of an open surface. We investigate now how the previous material can be extended to the case of a surface with one boundary component, loosely referred to hereafter as "an open surface". Let $M = M_{g,1}$ be such a surface of genus g , and $\mathcal{G}_{g,1}$ its mapping class group of homeomorphisms acting trivially on $H_1(M, Z)$. Let $\partial M = B(\simeq S^1)$, and choose an imbedding v of M into a closed

surface M' of genus $g' > g$. Then $v(B)$ separates M' into two pieces $v(M)$ and M'' . The homeomorphisms of M in \mathcal{G} are by definition restricted to be the identity on B , so we may "extend" any such homeomorphism f to a homeomorphism \bar{f} on M' by putting $\bar{f} = vf v^{-1}$ for points of $v(M)$ and $\bar{f} = 1$ for points of M'' . In this way we get a homomorphism $v^*: \mathcal{G}_{g,1} \rightarrow \mathcal{G}_g$.

The imbedding v also induces a natural splitting of $H_1(M')$ into $H_1(M) \oplus H_1(M'')$ (we have identified M with $v(M)$ here; also, Z_2 coefficients are assumed). This splitting is *symplectic*, that is, it splits the intersection form also: $x \cdot x'' = 0$, $x \in H_1(M)$, $x'' \in H_1(M'')$. We may thus choose a symplectic basis $a_i, a_j''; b_i, b_j''$ with $a_i, b_i \in H_1(M)$, etc. If now ω' is any Sp-form on $H_1(M')$ then its restrictions to $H_1(M), H_1(M'')$ are Sp-forms ω, ω'' respectively, and these give a direct sum decomposition $\omega' = \omega \oplus \omega''$. This is true since $\omega'(x + x'') = \omega'(x) + \omega'(x'') + x \cdot x'' = \omega(x) + \omega''(x'')$. Conversely, any two Sp-forms, ω, ω'' on $H_1(M), H_1(M'')$ define an Sp-form ω' on $H_1(M')$ by means of this equation.

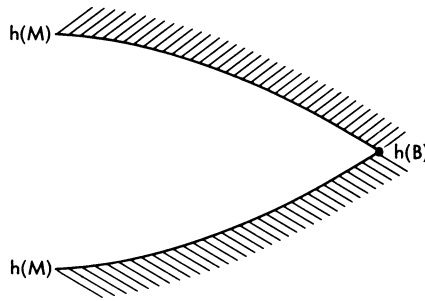


FIGURE 3

A *Heegaard imbedding* of M into W is an imbedding $h: M \rightarrow W$ such that $h(M)$ is contained in some Heegaard surface M' of W . Suppose now h is a Heegaard imbedding of M into S^3 with $h(M)$ contained in M' . Given $k \in \mathcal{G}_{g,1}(M)$ we split S^3 along $h(M)$ as in Figure 3 and reglue by the map k , to be precise, x in the "lower" face glued to $hkh^{-1}(x)$ in the "upper" face. A homology sphere $M(h, k)$ results, and again we define $\mu(h, k)$ to be its Rochlin invariant. Note that $M(h, k)$ is the same as $M(\bar{h}, \bar{k})$ where \bar{h} is the imbedding of M' into S^3 (i.e., the inclusion map) and \bar{k} is the extension of k to M' as previously defined. Thus $\mu(h, k) = \mu(\bar{h}, \bar{k})$. The latter depends only on $\omega_{\bar{h}}$ by Theorem 1, and $\omega_{\bar{h}}$ splits into ω_h on M and ω'' on M'' . Here ω_h is, as for a closed surface, just the self-linking form induced on M by the imbedding h .

Let us look at $\sigma_{\bar{k}}$; since \bar{k} is the extension of k on M , it can be expressed as a product of basic generators in M , and as such it will be a polynomial involving only the basis elements \bar{a}_i, \bar{b}_i ; the \bar{a}_j'', \bar{b}_j'' will not appear. (Again we are identifying M with $v(M)$.) Applying this $\sigma_{\bar{k}}$ to $\omega_{\bar{h}}$ then, we see that its value $\mu(h, k)$ depends only on $\bar{a}_i(\omega_{\bar{h}}) = \omega_{\bar{h}}(a_i) = \omega_h(a_i)$ and, likewise, $\omega_h(b_i)$. In other words, we have proved the analogue of Corollary 1 of Theorem 1 for open surfaces.

COROLLARY 1'. For open surfaces $\mu(h, k)$ depends only on ω_h and k .

We introduce the notation $\mu(\omega, k)$ for open surfaces as well.

It should be noted that, unlike the case for a closed surface, the induced quadratic form ω_h may not have Arf invariant zero, and $\mu(\omega, k)$ will be defined for any ω which is induced by some Heegaard imbedding of M . To see that every $\omega \in \Omega_M$ is so induced it suffices to show that for some $M' \supset M$, M' closed, ω extends to a form ω' on M' which is in $\Psi_{M'}$: for then ω' will be induced by some Heegaard imbedding of M' , which restricted to M induces ω .

LEMMA 16. If $M \subset M'$, M' closed and of genus $g' > g$, then any Sp-form $\omega \in \Omega_M$ extends to an Sp-form $\omega' \in \Psi_{M'}$.

PROOF. Let $a_i, a_j''; b_i, b_j''$ ($i = 1, \dots, g; j = g + 1, \dots, g'$) be a split basis for $H_1(M')$. Define $\omega' = \omega$ on $a_i, b_i, \omega'(a_{g+1}'') = \omega'(b_{g+1}'') = \alpha(\omega)$, and $\omega' = 0$ on the remaining basis elements. Then ω' extends ω and $\alpha(\omega') = 0$ by construction. Q.E.D.

We have now shown that $\mu(\omega, k)$ is defined for all $\omega \in \Omega_M$ and $k \in \mathcal{G}_M$, and hence we may define $\sigma_k: \Omega_M \rightarrow Z_2$ by $\sigma_k(\omega) = \mu(\omega, k)$. This function is a polynomial function with the same expression (e.g., $\overline{AB}(\overline{C} + 1)$) on the generators, but there is a difference: the only Boolean polynomial which is zero on all of Ω_M is the zero polynomial. The arguments leading to Theorem 4 apply then directly to prove the following

THEOREM 6. If M is a surface with one boundary component we have an isomorphism $\sigma: U = \mathcal{G}/\mathcal{C} \rightarrow B_3$, the space of Boolean cubics on Ω ;

$$\dim U = \sum_{i=0}^3 \binom{2g}{i}.$$

The image of $\overline{\mathcal{T}}$ is B_2 , of dimension

$$\sum_{i=0}^2 \binom{2g}{i}.$$

Both these results now hold whenever $g \geq 2$.

When $g = 1$, \mathcal{G} is infinite cyclic and generated by a twist on the boundary curve; it is easy to see that $U = T = Z_2$ in this case.

11. Linear relations among the ρ 's. For an open surface, $\rho_\omega(k) = \mu(\omega, k)$ is defined for all $\omega \in \Omega$ and is a homomorphism of \mathcal{G} to Z_2 . These extra homomorphisms² give us a simpler and more symmetric description of the vector space U^* . Just as pointed out in §9, the ρ_ω ($\omega \in \Omega$) generate U^* , and we can ask then for the linear relations connecting them. Any such linear relation can be written $\sum_{\omega \in \Omega} \alpha_\omega \rho_\omega = 0$ ($\alpha_\omega \in Z_2$). Or, if $S \subset \Omega$ is the subset of Ω for which the coefficients

²It should be noted that the new homomorphisms (with $\alpha(\omega) = 1$) are also surjective. This follows from the fact that for $k =$ the twist on the boundary, $\rho_\omega(k) = \alpha(\omega)$.

α_S are 1, we may write this relation as $\sum_{\omega \in S} \rho_\omega = 0$. Our problem is then to find such subsets S .

Theorem 6 tells us that we may think of U as the space of Boolean cubic polynomials on Ω . Thus a relation S is a subset of Ω such that $\sum_{\omega \in S} \rho_\omega(k) = \sum_{\omega \in S} \sigma_k(\omega) = 0$ for all k , that is, $\sum_{\omega \in S} f(\omega) = 0$ for all Boolean cubics f . Now this is a situation well treated by classical results in Boolean algebra. We give a brief description of the results we need here (see [MS] for an explication in the language of coding theory).

(1) Let W be an affine space over Z_2 and $P(W)$ its *space of subsets*, that is, $P(W)$ is the set of subsets of W , with addition of sets defined by addition of their characteristic functions. (The characteristic function of a subset $S \subset W$ is the function $F_S: W \rightarrow Z_2$ given by $F_S(w) = 1$ iff $w \in S$. This addition of subsets may also be described as the "exclusive or" operation: for $S, T \subset W$, $S + T = (S \cup T) - (S \cap T)$.)

(2) Since W is an affine space, we may talk about its n -dimensional affine subspaces. These subspaces, considered as elements of $P(W)$, generate a *subspace of $P(W)$* called the *n -plane subsets of W* , which we denote by Q_n .

(3) Let, as before, B_n be the space of Boolean polynomials of degree $\leq n$ on W ; if $d = \dim W$, then $B = B_d$ is the space of all Boolean polynomials on W . We have then a natural pairing $P(W) \otimes B \rightarrow Z_2$ given by $\langle S, f \rangle = \sum_{w \in S} f(w)$.

(4) The classical results tell us the following: the above pairing is a *dual* pairing, and furthermore $Q_{n+1} = B_n^\perp$, that is, $\sum_{w \in S} f(w) = 0$ for all f of degree $\leq n$ precisely when S is an $(n + 1)$ -plane set.

We may now apply these results to our special case. Since our relations are those S which satisfy $\sum_{w \in S} f(w) = 0$ for all $f \in B_3$, i.e., $S \in B_3^\perp$, we obtain

THEOREM 7. *For a surface with one boundary component, the relations among the totality of ρ 's are given by the 4-plane subsets of Ω . In particular, a generating set of relations is given by those of the form $\sum_{\omega \in S} \rho_\omega = 0$, where $S \subset \Omega$ is a 4-dimensional affine subspace of Ω .*

We can see how this theorem works by a simple example. For $g = 2$, Ω is 4-dimensional and so there is only *one* relation among the ρ_ω 's, namely $\sum_{\omega \in \Omega} \rho_\omega = 0$. Since $|\Omega| = 16$, we have sixteen ρ_ω 's and one relation, giving $\dim U^* = 15$. This is consistent with $\dim B_3 = \sum_{i=0}^3 \binom{4}{i} = 15$.

REFERENCES

- [A] C. Arf, *Untersuchungen über Quadratische Formen in Körpern der Charakteristik 2*, J. Reine Angew. Math. **183** (1941), 148–167.
 [BC] J. Birman and R. Craggs, *The μ -invariant of 3-manifolds and certain structural properties of the group of homeomorphisms of a closed, oriented 2-manifold*, Trans. Amer. Math. Soc. **237** (1978), 283–309.
 [FK] Michael Freedman and Robion Kirby, *A geometric proof of Rochlin's Theorem*, Proc. Sympos. Pure Math., vol. 32, part 2, Amer. Math. Soc., Providence, R. I., 1978, pp. 85–97.
 [GA] F. Gonzalez-Acuña, *Dehn's construction on knots*, Bol. Soc. Mat. Mexicana **15** (1970), 58–79.
 [G] C. McA. Gordon, *Knots, homology spheres, and contractible 4-manifolds*, Topology **14** (1975), 151–172.

[MH] Dale Husemoller and John Milnor, *Symmetric bilinear forms*, *Ergebnisse der Math. und ihrer Grenzgebiete*, vol. 73, Springer-Verlag, New York, 1973.

[MS] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, vol. 2, American Elsevier, New York, 1977. (See Chapter 13, Sections 2–5, particularly Theorems 4, 8, 12.)

[P] J. Powell, *Two theorems on the mapping group of surfaces*, *Proc. Amer. Math. Soc.* **68** (1978), 347–350.

[W] F. Waldhausen, *Heegaard-Zerlegungen der 3-Sphäre*, *Topology* **7** (1968), 195–203.

JET PROPULSION LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91125

Current address: 15 San Mateo Road, Berkeley, California 94707