SELF–ORTHOGONAL CODES AND THE TOPOLOGY OF SPINOR GROUP

By

Jay A. Wood

IMA Preprint Series # 461

October 1988

SELF-ORTHOGONAL CODES AND THE TOPOLOGY OF SPINOR GROUPS

JAY A. WOOD*

Abstract. Maximal doubly-even self-orthogonal binary linear codes correspond to the maximal elementary abelian 2-groups of the spinor group $\mathrm{Spin}(n)$. We will describe the correspondence and discuss various techniques from the algebraic topology of $\mathrm{Spin}(n)$ which may be useful in studying self-orthogonal codes. In particular, Quillen's results in equivariant cohomology theory coupled with some Morse theory may allow one to address certain questions on the minimum weight of doubly-even self-orthogonal codes.

Key words. self-orthogonal codes, spinor groups, flat connections, equivariant cohomology, Morse theory

AMS(MOS) subject classifications. Primary 94B05, 57R70; Secondary 11T71, 22E40, 53C05, 22E70, 55R40, 57T10

1. Introduction. The purpose of this paper is to offer a new way to view the self-orthogonal binary linear codes—as certain abelian 2-subgroups of the spinor groups $\mathrm{Spin}(n)$—and then to propose some ideas on how the topology of $\mathrm{Spin}(n)$ may be able to answer questions on the minimum weights of self-orthogonal codes.

The reader should be warned of the speculative nature of trying to apply algebraic topology to coding theory. One may only be translating one intractable problem into another intractable problem. Nevertheless, viewing the self-orthogonal codes as subgroups of $\mathrm{Spin}(n)$ offers a fresh perspective on the codes, and the new ideas are interesting and worth a try. The other direction may also be useful: using codes to say something about the topology of $\mathrm{Spin}(n)$.

An outline of the contents of the paper follows. My original interest was in understanding the gauge equivalence classes of flat connections on principal G-bundles over a compact manifold X, where G is a compact Lie group. Such objects arise in the study of the ends of Yang-Mills moduli spaces. Gauge equivalence classes of flat connections are parameterized by homomorphisms from the fundamental group $\pi_1(X)$ of the base manifold X into the structure group G of the bundle, up to conjugation in G, i.e., by the space

$$\mathcal{F} = \mathrm{Hom}(\pi_1(X), G)/\,\mathrm{Ad}(G),$$

where $\mathrm{Ad}(G)$ indicates G acting via the adjoint representation (conjugation). In the special case where $\pi_1(X)$ is abelian, considering only the image subgroups appearing in $\mathcal{F}$ leads

*Department of Mathematics, Bowdoin College, Brunswick, ME, 04011. This research was supported in part by grants from the Faculty Research Committee of Bowdoin College, by NSA Grant Number MDA904-88-H-2026, and by the Institute for Mathematics and its Applications with funds provided by the National Science Foundation. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon. E-mail: jwood@bowdoin.bitnet.

one to the set of conjugacy classes of maximal abelian subgroups of G, where G is a compact Lie group. In Section 2 we discuss these issues in more detail and outline what happens when $G = \mathrm{SU}(n)$, $\mathrm{Sp}(n)$, or $\mathrm{SO}(n)$.

In Section 3 we discuss $G = \mathrm{Spin}(n)$, the universal double covering group of $\mathrm{SO}(n)$. $\mathrm{Spin}(n)$ is described concretely in terms of the Clifford algebra. The maximal abelian subgroups of $\mathrm{Spin}(n)$ have a continuous piece and a discrete piece, and the discrete piece corresponds to a self-orthogonal code. The basic idea is this: View the diagonal matrices in $\mathrm{SO}(n)$ as a binary vector space V. *Question*: When does a subspace W (i.e., a matrix subgroup) of V lift to an abelian subgroup of $\mathrm{Spin}(n)$? *Answer*: Precisely when W is a self-orthogonal code. Moreover, the doubly-even self-orthogonal codes lift to the elementary abelian 2-subgroups of $\mathrm{Spin}(n)$.

The elementary abelian 2-subgroups of $\mathrm{Spin}(n)$ (call them 2-*tori*) are especially important in understanding the $\mathbf{Z}/2$-topology of $\mathrm{Spin}(n)$. After reviewing some topological background in Section 4, we summarize in Section 5 some results of Borel on how the 2-tori in $\mathrm{Spin}(n)$ reflect 2-torsion in the cohomology of $\mathrm{Spin}(n)$ and its classifying space. For example, the existence of inequivalent maximal doubly-even self-orthogonal codes implies the presence of 2-torsion in the cohomology of $\mathrm{Spin}(n)$.

The interaction between 2-tori and cohomology was greatly extended by Quillen in his study of equivariant cohomology theory. In this case, $\mathrm{Spin}(n)$ acts on some space X. Among the results of Quillen which are summarized in Section 6 is the one-to-one correspondence between the minimal prime ideals of the equivariant cohomology ring $H^*_{\mathrm{Spin}(n)}(X; \mathbf{Z}/2)$ and the conjugacy classes of maximal 2-tori in $\mathrm{Spin}(n)$ which have fixed points when acting on X. Already when X is a point (so every 2-torus has a fixed point), the conjugacy classes of maximal 2-tori, i.e., the equivalence classes of maximal doubly-even self-orthogonal codes, are in one-to-one correspondence with the minimal prime ideals of $H^*_{\mathrm{Spin}(n)}(\mathrm{point}; \mathbf{Z}/2) \cong H^*(B\mathrm{Spin}(n); \mathbf{Z}/2)$.

In order to address weight-theoretic questions of codes, one studies the function

$$f = -\mathrm{trace} \circ \pi : \mathrm{Spin}(n) \to \mathbf{R},$$

where π is the double covering map $\pi : \mathrm{Spin}(n) \to \mathrm{SO}(n)$. In Section 7 we view f as a Morse function on $\mathrm{Spin}(n)$ and examine the structure of its critical points.

Finally, in Section 8 we couple Quillen's equivariant cohomology theory for $\mathrm{Spin}(n)$ acting on some space X with the Morse theory of the function f, by letting $X = X_{\alpha,\beta} = \{x \in \mathrm{Spin}(n) \mid \alpha < f(x) < \beta\}$. By varying the values of α and β, the 2-tori which have fixed points on $X_{\alpha,\beta}$ (and hence contribute prime ideals to $H^*_{\mathrm{Spin}(n)}(X_{\alpha,\beta})$) will change. Thus it might be possible to detect the existence of doubly-even self-orthogonal codes of high minimum weight via the prime ideal structure of the equivariant cohomology rings $H^*_{\mathrm{Spin}(n)}(X_{\alpha,\beta})$.

Acknowledgements. We thank Haynes Miller for his continued interest in this work and for suggesting the use of Morse filtrations to study weight problems. We also thank

the Institute for Mathematics and its Applications for its hospitality during the Workshops on Coding Theory and Design Theory, June 1988.

2. Maximal abelian subgroups of compact connected Lie groups. The correspondence between self-orthogonal codes and abelian subgroups of $\mathrm{Spin}(n)$ originated in studying the conjugacy classes of maximal abelian subgroups of compact Lie groups. This in turn stemmed from studying the gauge equivalence classes of flat connections on principal bundles in Yang-Mills theory. This section describes briefly this chain of ideas.

In Simon Donaldson's applications of Yang-Mills theory to the study of the topology of smooth 4-manifolds (see [11] and [13]), the ends of the moduli spaces of self-dual connections on a principal bundle play an important role. If the principal bundle is $P \to X$ with structure group G (a compact, simple Lie group), then the ends of the moduli space turn out to be parameterized by the space of flat connections on P, modulo gauge equivalence.

By making use of the holonomy subgroups associated to the flat connections (see [15, Chapter II]), one can show that the space of flat connections on P, modulo gauge equivalence, is equal to

$$\mathcal{F} = \mathrm{Hom}(\pi_1(X), G)/\,\mathrm{Ad}(G),$$

the space of group homomorphisms from the fundamental group $\pi_1(X)$ of X to the structure group G of the bundle, modulo the adjoint action $\mathrm{Ad}(G)$ of G (G acting by conjugation). For more details, see [27, §2].

To simplify matters somewhat, we assume that $\pi_1(X)$ is abelian, and we consider only the image subgroups of the homomorphisms appearing in $\mathcal{F}$. This leads one to study the space of conjugacy classes of abelian subgroups of G, where G is a compact, simple Lie group. The most important are the conjugacy classes of maximal abelian subgroups of G.

The compact, simple Lie groups up to local isomorphism were classified by Élie Cartan. There are four infinite families of examples:

- (A_n) $\mathrm{SU}(n+1)$: the $(n+1) \times (n+1)$ complex unitary matrices of determinant 1, $n \geq 1$,
- (B_n) $\mathrm{SO}(2n+1)$: the $(2n+1) \times (2n+1)$ real orthogonal matrices of determinant 1, $n \geq 2$,
- (C_n) $\mathrm{Sp}(n)$: the $n \times n$ quaternionic unitary matrices, $n \geq 3$,
- (D_n) $\mathrm{SO}(2n)$: the $2n \times 2n$ real orthogonal matrices of determinant 1, $n \geq 4$,

and five exceptional groups: G_2, F_4, E_6, E_7, and E_8. See, for example, [14, p. 516]. We discuss the conjugacy classes of maximal abelian subgroups in G, for G equaling $\mathrm{SU}(n)$, $\mathrm{Sp}(n)$ or $\mathrm{SO}(n)$. We will not discuss the exceptional groups.

When G equals $\mathrm{SU}(n)$ or $\mathrm{Sp}(n)$, theorems in linear algebra on simultaneous diagonalization of commuting unitary operators imply that every abelian subgroup of G is conjugate to a subgroup of diagonal matrices. Thus there is only one maximal abelian subgroup of G up to conjugation: the subgroup of all diagonal matrices in G. This subgroup is a maximal torus in G (isomorphic to a product of circle groups).

When $G = \mathrm{SO}(n)$, there are theorems in linear algebra on commuting orthogonal operators which say that abelian subgroups of G can be conjugated into a certain normal form consisting of some 2×2 rotation blocks down the main diagonal, supplemented by diagonal elements thereafter. Up to conjugation, the maximal abelian subgroups of $\mathrm{SO}(n)$ are thus of the form

$$T^l \times V(n-2l),$$

where T^l is an l-dimensional torus (the product of l circle groups) in $\mathrm{SO}(2l)$, thought of as l 2×2 rotation blocks down the diagonal, and

$$V(k) = \{\text{diagonal matrices in } \mathrm{SO}(k)\}.$$

The possible values of l are $l = 0, 1, 2, \ldots, [n/2]$, except $l \neq n/2 - 1$, when n is even. ($V(2)$ is not maximal abelian in $\mathrm{SO}(2)$.) $[a]$ denotes the greatest integer $\leq a$.

Example. In $\mathrm{SO}(3)$, the two maximal abelian subgroups, up to conjugation, are:

$$T^1 = \left\{ \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

and

$$V(3) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\}$$
$$\cong \mathbf{Z}/2 \oplus \mathbf{Z}/2.$$

Cartan's classification of the simple, compact Lie groups was only up to local isomorphism. The groups $\mathrm{SU}(n)$ and $\mathrm{Sp}(n)$ are simply-connected, but the special orthogonal groups $\mathrm{SO}(n)$ are not simply-connected. Since $\pi_1(\mathrm{SO}(n)) = \mathbf{Z}/2$, for $n \geq 3$, $\mathrm{SO}(n)$ has a universal covering group which double covers $\mathrm{SO}(n)$. This is the spinor group $\mathrm{Spin}(n)$. We define $\mathrm{Spin}(n)$ more concretely and examine its maximal abelian subgroups in the next section.

3. Abelian subgroups of Spin(n) and self-orthogonal codes. In order to study the conjugacy classes of maximal abelian subgroups of $\mathrm{Spin}(n)$, and how they relate to self-orthogonal codes, we define $\mathrm{Spin}(n)$ by means of the Clifford algebra C_n. The reader may refer to [2] for more details.

On $\mathbf{R}^n$, choose an orthonormal basis $e_1, e_2, \ldots, e_n$. The *Clifford algebra* C_n is the associative algebra with 1 over $\mathbf{R}$ generated by $e_1, e_2, \ldots, e_n$, subject to the relations

$$e_i e_j + e_j e_i = -2\delta_{ij}.$$

$\mathbf{R}^n$ injects linearly into C_n as the linear combinations of $e_1, e_2, \ldots, e_n$. Every non-zero $x \in \mathbf{R}^n$ is a unit in C_n with inverse $x^{-1} = -x/\|x\|^2$. The unit sphere $S^{n-1} \subset \mathbf{R}^n$ also sits inside C_n, and any $x \in S^{n-1}$ is a unit with $x^{-1} = -x$.

DEFINITION. $\mathrm{Spin}(n)$ is defined to be the (multiplicative) subgroup of the group of units of C_n generated by products of an even number of factors from S^{n-1}.

The double covering homomorphism $\pi : \mathrm{Spin}(n) \to \mathrm{SO}(n)$ is defined by using Clifford multiplication: for $x \in \mathrm{Spin}(n)$, $y \in \mathbf{R}^n \subset C_n$, Clifford conjugation

$$\pi_x : y \mapsto xyx^{-1}$$

maps $\mathbf{R}^n \to \mathbf{R}^n$, is orthogonal (since the factors in x are of unit length), and has determinant 1 (x has an even number of factors). Thus $\pi : x \mapsto \pi_x$ maps $\mathrm{Spin}(n) \to \mathrm{SO}(n)$. π is surjective, as follows from the next lemma, and $\ker \pi = \{\pm 1\}$.

For an index set $I = \{i_1 < i_2 < \cdots < i_r\} \subset \{1, 2, \ldots, n\}$, set

$$e_I = e_{i_1} e_{i_2} \cdots e_{i_r},$$

with $e_\emptyset = 1$, by convention. Similarly, let v_I be the diagonal matrix with -1's in diagonal positions $i_1, i_2, \ldots, i_r$, and 1's elsewhere on the diagonal. The next lemma is an easy exercise for the reader.

LEMMA 3.1.

(1) $|I \cup J| = |I| + |J| - 2|I \cap J|$

(2) $e_I^2 = \begin{cases} +1, & \text{if } |I| \equiv 0, 3 \bmod 4 \\ -1, & \text{if } |I| \equiv 1, 2 \bmod 4 \end{cases}$

(3) $e_I e_J = \begin{cases} +e_J e_I, & \text{if } |I||J| + |I \cap J| \text{ is even} \\ -e_J e_I, & \text{if } |I||J| + |I \cap J| \text{ is odd} \end{cases}$

(4) $e_I e_j e_I^{-1} = \begin{cases} +(-1)^{|I|} e_j, & \text{if } j \notin I \\ -(-1)^{|I|} e_j, & \text{if } j \in I \end{cases}$

Recall from Section 2 that $V(n) = \{\text{diagonal matrices in } \mathrm{SO}(n)\}$. Let

$$\tilde{V}(n) = \{\pm e_I \mid |I| \text{ is even } \} \subset \mathrm{Spin}(n).$$

Lemma 3.1 implies that $\tilde{V}(n)$ is a non-abelian subgroup of $\mathrm{Spin}(n)$ and that $\tilde{V}(n) = \pi^{-1}(V(n))$. Clearly, $\pi(e_I) = v_I$. Moreover, $V = V(n)$ and $\tilde{V} = \tilde{V}(n)$ fit into the following exact sequence of groups:

$$1 \to \mathbf{Z}/2 \xrightarrow{i} \tilde{V} \xrightarrow{\pi} V \to 1, \tag{3.2}$$

where $\mathbf{Z}/2 \cong \{\pm 1\} = \ker \pi \subset \tilde{V}$, i is the inclusion, and π is the projection from $\mathrm{Spin}(n)$ to $\mathrm{SO}(n)$, restricted to $\tilde{V}$.

Recall also from Section 2 that, up to conjugation, the maximal abelian subgroups of $\mathrm{SO}(n)$ are of the form

$$B_l = T^l \times V(n-2l),$$

where T^l is an l-dimensional torus in $\mathrm{SO}(2l)$. We now wish to discuss the maximal abelian subgroups of $\mathrm{Spin}(n)$. Let A be a maximal abelian subgroup of $\mathrm{Spin}(n)$, so that $\pi(A)$ is an abelian subgroup of $\mathrm{SO}(n)$. Some conjugate of $\pi(A)$ is contained in a B_l, so that a conjugate of A is contained in $\pi^{-1}(B_l)$. Now

$$\pi^{-1}(B_l) = \tilde{T}^l \cdot \tilde{V}(n-2l),$$

where $\tilde{T}^l$ is an l-dimensional torus in $\mathrm{Spin}(2l)$ which double covers T^l. Because $\tilde{V}$ is non-abelian, $\pi^{-1}(B_l)$ itself cannot be a maximal abelian subgroup of $\mathrm{Spin}(n)$. However, the discussion above leads to the next theorem, a more detailed proof of which is contained in [26, Theorem 5.6].

THEOREM 3.3. *Any maximal abelian subgroup of* $\mathrm{Spin}(n)$ *is conjugate to*

$$\tilde{T}^l \cdot M,$$

for some $l = 0, 1, 2, \ldots, [n/2]$, $(l \neq n/2 - 1$, *when* n *is even), where* $\tilde{T}^l$ *is an* l*-dimensional torus in* $\mathrm{Spin}(2l)$, *and* M *is a maximal abelian subgroup of* $\mathrm{Spin}(n-2l)$ *which is contained in* $\tilde{V}(n-2l)$.

Remark. Two maximal abelian subgroups of $\mathrm{Spin}(n)$ of the form $\tilde{T}^l \cdot M_1$, $\tilde{T}^l \cdot M_2$ are conjugate if and only if M_1 and M_2 are conjugate in $\mathrm{Spin}(n-2l)$ by an element of the normalizer $\tilde{N}$ of $\tilde{V}(n-2l)$ in $\mathrm{Spin}(n-2l)$. See [26, Theorem 5.8].

Thus we see that the study of the conjugacy classes of maximal abelian subgroups of $\mathrm{Spin}(n)$ reduces to the study of the maximal abelian subgroups of $\tilde{V}(k)$, up to the action of the normalizer $\tilde{N}$ of $\tilde{V}(k)$ in $\mathrm{Spin}(k)$.

Because $\tilde{V}$ and V fit into the exact sequence (3.2), the basic question before us is: Which subgroups of V lift to give abelian subgroups of $\tilde{V}$? To answer this question, we follow Quillen [24, §4] in using (3.2) to define two F_2-valued forms. Note that V is an elementary abelian 2-group of rank $n-1$, i.e., an $(n-1)$-dimensional vector space over F_2.

DEFINITION. F_2 is the two element field which we identify with $\mathbf{Z}/2 = \{\pm 1\}$ in the usual way. Define $B : V \times V \to \mathsf{F}_2$ by

$$iB(x,y) = \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1}, \quad \pi\bar{x} = x, \pi\bar{y} = y,$$

and define $Q : V \to \mathsf{F}_2$ by

$$iQ(x) = \bar{x}^2, \quad \pi\bar{x} = x.$$

By using Lemma 3.1, one can prove the following proposition.

PROPOSITION 3.4.

(1) $B : V \times V \to \mathbf{F}_2$ *is a symmetric, bilinear form, and* $B(v_I, v_J) \equiv |I \cap J| \bmod 2$.

(2) $Q : V \to \mathbf{F}_2$ *is a quadratic form, with* $Q(x+y) + Q(x) + Q(y) = B(x,y)$ *and* $Q(v_I) \equiv \frac{1}{2}|I| \bmod 2$.

The matrix subgroups W of V are just the $\mathbf{F}_2$-linear subspaces of V. A subspace W of V is *B-isotropic* (resp. *Q-isotropic*) if B (resp. Q) vanishes identically when restricted to W. Then the definitions of B and Q and the correspondence $W \mapsto \pi^{-1}(W)$ yield the next theorem.

THEOREM 3.5. *Let W be a subgroup of V. Then $\pi^{-1}(W)$ is an abelian subgroup (resp. elementary abelian 2-subgroup) of $\tilde{V}$ if and only if W is B-isotropic (resp. Q-isotropic).*

Finally, we wish to show the relationship between abelian subgroups of $\tilde{V}$ and self-orthogonal codes. Let us recall some definitions from coding theory [17]. Let V' be an n-dimensional vector space over $\mathbf{F}_2$, with a fixed basis. The choice of basis allows one to define a *dot product* "$\cdot$", with values in $\mathbf{F}_2$, in the usual way. A *binary, linear code* is an $\mathbf{F}_2$-subspace W of V'. W is *self-orthogonal* if $W \subset W^\perp$, where

$$W^\perp = \{y \in V' \mid w \cdot y = 0, \text{ for all } w \in W\}.$$

W is *self-dual* if $W = W^\perp$. The *weight* $\mathrm{wt}(x)$ of $x \in V'$ is the number of non-zero coefficients in the expression of x in terms of the fixed basis. Since $\mathrm{wt}(x) \equiv x \cdot x \bmod 2$, every element of a self-orthogonal code has even weight. A self-orthogonal code W is *doubly-even* if every element of W has weight divisible by 4.

Of particular interest in coding theory is the *minimum weight*

$$d(W) = \min\{\mathrm{wt}(x) \mid 0 \neq x \in W\}$$

of a code W. The minimum weight determines the error-correcting capability of the code, as W can correct $< [d(W)/2]$ errors. Finding codes with high minimum weight is an important problem in coding theory, one we return to in Section 8.

Let $V' = V'(n) = \{\text{diagonal matrices in } \mathrm{O}(n)\}$, with basis $v_1, v_2, \ldots, v_n$, where v_i is the diagonal matrix with a -1 at diagonal position i and 1's elsewhere on the diagonal. It is easy to check that the dot product on V', when restricted to the subspace $V \subset V'$, is exactly the bilinear form B of Proposition 3.4. Thus the B-isotropic subspaces are precisely the self-orthogonal codes. Similarly, an element x has weight divisible by 4 if and only if $Q(x) = 0$. In summary, we have:

THEOREM 3.6.

(1) *Abelian subgroups of $\tilde{V}$ which contain -1 are in one-to-one correspondence with B-isotropic subspaces of V, which in turn are in one-to-one correspondence with self-orthogonal codes.*

(2) *Elementary abelian 2-subgroups of $\tilde{V}$ which contain -1 are in one-to-one correspondence with Q-isotropic subspaces of V, which in turn are in one-to-one correspondence with doubly-even self-orthogonal codes.*

Remark. The equivalence relations behave nicely as well. Two abelian subgroups of $\tilde{V}$ are conjugate via an element of the normalizer $\tilde{N}$ of $\tilde{V}$ in $\mathrm{Spin}(n)$ if and only if their corresponding self-orthogonal codes in V are permutation equivalent. For details, see [27, Theorem 4.6].

4. Topological background. Several concepts from algebraic topology are reviewed in this section. The treatment is not exhaustive—only those features needed in later sections are covered. The reader may consult the references for further information.

If X is a topological space and R is a commutative ring, then the *singular cohomology groups* $H^n(X;R)$, $n \geq 0$, fit together to form a graded ring, the *singular cohomology ring*

$$H^*(X;R) = \bigoplus_{n=0}^{\infty} H^n(X;R).$$

The multiplication is given by the cup product

$$\smile : H^m(X;R) \otimes H^n(X;R) \to H^{m+n}(X;R).$$

The multiplication is commutative in the sense of graded rings: if $a \in H^m(X;R)$, $b \in H^n(X;R)$, then $b \smile a = (-1)^{mn} a \smile b$. Any continuous map $f : X \to Y$ induces a ring homomorphism $f^* : H^*(Y;R) \to H^*(X;R)$.

When $R = \mathbf{Z}/p$, p prime, the cohomology ring $H^*(X;\mathbf{Z}/p)$ admits certain cohomology operations, especially the Steenrod reduced power operations $\mathcal{P}^i$. The cases $p = 2$ and p odd behave slightly differently. Since we shall only need the case $p = 2$ in later sections, this is the only case that will be covered.

When $p = 2$, the relevant Steenrod operations are called the *Steenrod squares*, denoted Sq^i. The Steenrod squares have the following four properties [20, pp. 90–91].

(1) For any space X and any two non-negative integers n, i, Sq^i is an additive homomorphism

$$Sq^i : H^n(X;\mathbf{Z}/2) \to H^{n+i}(X;\mathbf{Z}/2).$$

(2) If $f : X \to Y$, then $Sq^i \circ f^* = f^* \circ Sq^i$.

(3) If $a \in H^n(X;\mathbf{Z}/2)$, then $Sq^0(a) = a$, $Sq^n(a) = a \smile a$, and $Sq^i(a) = 0$, for all $i > n$.

(4) (*Cartan formula*) Whenever $a \smile b$ is defined,

$$Sq^k(a \smile b) = \sum_{i+j=k} Sq^i(a) \smile Sq^j(b).$$

The Steenrod squares will play an important role in Quillen's work on equivariant cohomology theory.

In order to explain equivariant cohomology, one needs the concept of the classifying space of a group. Let G be a compact Lie group (not necessarily connected—any finite group works!). Associated to G is a topological space BG, called the *classifying space* of G. BG is the base space of a principal G-bundle $EG \to BG$, where EG is contractible. It is well-known that BG exists, for every G, and is unique up to homotopy [25, §19]. In general, BG is infinite dimensional.

Example 4.1. The exponential map $\mathbf{R} \to S^1$, $x \mapsto e^{2\pi i x}$, is a principal $\mathbf{Z}$-bundle over S^1. Since $\mathbf{R}$ is contractible, $B\mathbf{Z} = S^1$.

Example 4.2. The standard projection $S^n \to \mathbf{R}P^n$ is a principal $\mathbf{Z}/2$-bundle over the real projective space $\mathbf{R}P^n$. Alas, S^n is not contractible. Taking the limit as $n \to \infty$ leads to the principal $\mathbf{Z}/2$-bundle $S^\infty \to \mathbf{R}P^\infty$, and S^∞ is contractible. Thus $B\mathbf{Z}/2 = \mathbf{R}P^\infty$.

Example 4.3. Similar arguments for the projections $S^{2n+1} \to \mathbf{C}P^n$ and $S^{4n+3} \to \mathbf{H}P^n$ give that

$$B\mathrm{U}(1) = B\mathrm{SO}(2) = BS^1 = \mathbf{C}P^\infty$$

and

$$B\mathrm{Sp}(1) = B\mathrm{SU}(2) = BS^3 = \mathbf{H}P^\infty.$$

Example 4.4. Using the projection from Stiefel manifolds to Grassmann manifolds, plus taking limits, implies that

(1) $B\mathrm{O}(n) = Gr(n, \mathbf{R}^\infty)$, the Grassmannian of unoriented n-planes in $\mathbf{R}^\infty$.

(2) $B\mathrm{SO}(n) = \widetilde{Gr}(n, \mathbf{R}^\infty)$, the Grassmannian of oriented n-planes in $\mathbf{R}^\infty$.

(3) $B\mathrm{U}(n) = Gr(n, \mathbf{C}^\infty)$, the Grassmannian of complex n-planes in $\mathbf{C}^\infty$.

(4) $B\mathrm{Sp}(n) = Gr(n, \mathbf{H}^\infty)$, the Grassmannian of quaternionic n-planes in $\mathbf{H}^\infty$.

For details, see [20, pp. 145, 163].

The importance of the classifying spaces is that they classify principal G-bundles. Denote by ξ_G the principal G-bundle $EG \to BG$ in the definition of BG. To every map $f : X \to BG$, one can define the *pull-back* of ξ_G, denoted $f^*(\xi_G)$, which is a principal G-bundle over X. The basic fact is that all principal G-bundles on X occur in this way [25, §19].

THEOREM 4.5. *The homotopy classes $[X, BG]$ of maps $f : X \to BG$ are in one-to-one correspondence with isomorphism classes of principal G-bundles on X, via $f \mapsto f^*(\xi_G)$.*

One use of this theorem is to assign cohomology classes to principal G-bundles on X. If ξ is a principal G-bundle on X, then $\xi = f^*(\xi_G)$, for some $f : X \to BG$. Then $f^*(H^*(BG; R)) \subset H^*(X; R)$ is the *characteristic subring* associated to ξ, which is very

important in the study of bundles ξ. This is the theory of characteristic classes of bundles; see [20].

Now suppose that a compact Lie group G acts on a space X on the left. The constructions that follow are due originally to Borel (see, for example, [3, Chapter 4]). In the principal G-bundle $EG \to BG$, G acts on the total space EG on the right. The space $EG \times_G X$ is the space of equivalence classes of pairs of points $(e, x) \in EG \times X$, where $(e, x) \sim (e', x')$ if there exists $g \in G$ such that $e' = eg$ and $x' = g^{-1}x$. The bundle $EG \times_G X \to BG$ is the *associated bundle* (to $EG \to BG$) with typical fiber X. The *equivariant cohomology ring* of X with respect to its G-action is defined by

$$H^*_G(X) = H^*(EG \times_G X).$$

If X is a point, then $EG \times_G \mathrm{pt} = BG$, so that $H^*_G(\mathrm{pt}) = H^*(BG)$. Equivariant cohomology will play a prominent role in later sections.

Remark. When G is a finite group, the equivariant cohomology $H^*_G(\mathrm{pt}) = H^*(BG)$ is equal to the group cohomology of G [16, Theorem 11.5].

5. Results of Borel on p-torsion. We review some early results of Borel which relate the behavior of the elementary abelian p-subgroups of a compact, connected Lie group G to various properties of the cohomology of G and its classifying space.

DEFINITIONS. For convenience of notation, an elementary abelian p-group will be called a *p-torus*. A p-torus A is isomorphic to a product of r copies of $\mathbf{Z}/p$, where r is the *rank* of A. If G is a compact, connected Lie group, the *p-rank* of G, denoted $r_p(G)$, is the maximum of the ranks of p-tori which are subgroups of G. The *rank* $l(G)$ of G is the dimension of a maximal torus (product of circle groups) of G.

If T is a maximal torus of G, a compact, connected Lie group, then the subgroup ${}_pT$ of T consisting of points of order p is a p-torus. This shows that $r_p(G) \geq l(G)$, for all primes p. One should not expect equality to hold, as the next example illustrates.

Example 5.1. Let $G = \mathrm{SO}(n)$. The rank $l(\mathrm{SO}(n)) = [n/2]$. $V(n)$, the subgroup of all diagonal matrices in $\mathrm{SO}(n)$, is a 2-torus of maximal rank $r_2(\mathrm{SO}(n)) = n - 1$.

There are some general results relating $r_p(G)$ and $l(G)$:

PROPOSITION 5.2.

(1) (BOREL AND SERRE, [6, PROPOSITION 6])

$$l(G) \leq r_p(G) \leq \begin{cases} 2\,l(G), & \text{if } p = 2, \\ (3/2)\,l(G), & \text{if } p \text{ is an odd prime,} \end{cases}$$

and $l(G) = r_p(G)$, if p does not divide the order of the Weyl group of G.

(2) (BOREL, [5]) *$l(G) = r_p(G)$, for p an odd prime.*

There are two more results of Borel related to p-tori which we wish to discuss. The first result relates torsion in the cohomology groups to p-tori which are not contained in maximal tori.

THEOREM 5.3 (BOREL, [4, THEOREM 4.5]). *Let G be a compact, connected Lie group, and let p be a prime. BG is the classifying space of G. The following conditions are equivalent.*

(1) *$H^*(G;\mathbf{Z})$ has no p-torsion.*

(2) *$H^*(BG;\mathbf{Z})$ has no p-torsion.*

(3) *Every p-torus is contained in a maximal torus.*

(4) *Every p-torus of rank ≤ 3 is contained in a maximal torus.*

The second result lists the p-torsion that occurs amongst the simple compact Lie groups (see the list in Section 2).

THEOREM 5.4 (BOREL, [4, THEOREM 2.5]). *Suppose that G is a compact, connected, simply-connected, simple Lie group, and that p is prime. Then $H^*(G;\mathbf{Z})$ has p-torsion in exactly the following cases:*

$$p = 2 : G = \mathrm{Spin}(n), n \geq 7; G_2, F_4, E_6, E_7, E_8;$$
$$p = 3 : G = F_4, E_6, E_7, E_8;$$
$$p = 5 : G = E_8.$$

Discussion. Theorem 5.3 says that $H^*(G;\mathbf{Z})$ has p-torsion if and only if there exists a p-torus which is not contained in a maximal torus. There are two basic ways in which this can occur. First, one might have $r_p(G) > l(G)$: rank reasons alone would preclude a p-torus of maximal rank from being contained in a maximal torus. By Borel's result in Proposition 5.2, this case will only occur when $p = 2$. Example 5.1 shows that $r_2(G) > l(G)$, for $G = \mathrm{SO}(n)$, $n \geq 3$.

For $G = \mathrm{Spin}(n)$, one can show that the 2-rank of $\mathrm{Spin}(n)$ behaves as follows. See [24, Table 6.2 ($r_2 = n - h$)] or [26, Theorem 3.18].

PROPOSITION 5.5.

$$r_2(\mathrm{Spin}(n)) = \begin{cases} [n/2]+1, & \text{if } n \equiv 0,1,7 \bmod 8, \\ [n/2], & \text{if } n \equiv 2,3,4,5,6 \bmod 8. \end{cases}$$

Since $l(\mathrm{Spin}(n)) = [n/2]$, we see that $r_2 > l$, when $n \equiv 0,1,7 \bmod 8$. This accounts for 2-torsion in $H^*(\mathrm{Spin}(n);\mathbf{Z})$, $n = 7,8,9$, for example.

The second way for a p-torus not to be contained in a maximal torus (when $r_p = l$) is for there to exist at least two distinct conjugacy classes of maximal p-tori. One conjugacy class which always exists is the conjugacy class of the p-torus ${}_pT$ of order p points on a

maximal torus. Thus there exists a p-torus not contained in a maximal torus if and only if its conjugacy class is distinct from that of ${}_pT$. Whenever G has p-torsion, p odd, it follows that G has non-conjugate maximal p-tori.

When $G = \mathrm{Spin}(n)$, $n \geq 7$ and $n \equiv 2,3,4,5,6 \bmod 8$, the presence of 2-torsion in $H^*(\mathrm{Spin}(n); \mathbf{Z})$ implies the existence of non-conjugate maximal 2-tori, i.e., inequivalent maximal doubly-even self-orthogonal codes. This explains why inequivalent maximal doubly-even codes begin to appear at $n = 10$.

In the next section p-tori are related to the prime ideal structure of equivariant cohomology rings.

6. Results of Quillen on equivariant cohomology. We now outline some results of Quillen [23] which relate the collection of p-tori in a compact Lie group G to the prime ideal structure of $H^*(BG; \mathbf{Z}/p)$. If G acts on some space X, it is the p-tori together with information about their fixed point sets on X which is related to prime ideals in the equivariant cohomology ring $H^*_G(X; \mathbf{Z}/p)$. We borrow shamelessly from [23] and the reader should see Quillen's paper for the full story.

Throughout this section G will be a compact Lie group (not necessarily connected), and X will be a compact topological space on which G acts. Let p be a fixed prime. A will denote a p-torus in G, and all cohomology will be with $\mathbf{Z}/p$-coefficients. We assume in addition that $H^*(X)$ is finite dimensional. This implies that the fixed point set

$$X^A = \{x \in X \mid ax = x, \text{ for all } a \in A\}$$

has only finitely many connected components [23, Corollary 4.3].

From the p-tori in G and their fixed point sets, we build a category $\mathcal{A}(G, X)$. The objects of $\mathcal{A}(G, X)$ are all pairs (A, c), where A is a p-torus in G and c is a connected component of X^A. A morphism

$$\theta : (A, c) \to (A', c')$$

in $\mathcal{A}(G, X)$ is a triple $((A, c), (A', c'), \bar{\theta})$, where $\bar{\theta}$ is a homomorphism $\bar{\theta} : A \to A'$ of the form $\bar{\theta}(a) = gag^{-1}$, for some $g \in G$ which has the properties that $gAg^{-1} \subset A'$ and $gc \supset c'$. Composition of morphisms is just composition of the corresponding homomorphisms of p-tori.

For any $(A, c) \in \mathcal{A}(G, X)$, every map from $(A, \mathrm{pt}) \to (G, X)$ consisting of the inclusion homomorphism $A \subset G$ and any map taking the one-point space to the component c, induces a homomorphism

$$(A, c)^* : H^*_G(X) \to H^*_A \tag{6.1}$$

on equivariant cohomology. (We denote $H^*_A(\mathrm{pt})$ simply by H^*_A.) If $\theta : (A,c) \to (A',c')$ is any morphism in $\mathcal{A}(G,X)$, then $\theta^*(A',c')^* = (A,c)^*$. The family (6.1) of homomorphisms then defines a homomorphism

$$H^*_G(X) \longrightarrow \operatorname*{proj\,lim}_{(A,c)\in\mathcal{A}(G,X)} H^*_A$$

to the projective limit. The main theorem of Quillen is

THEOREM 6.2 (QUILLEN, [23, THEOREM 6.2, (8.5)]). *The homomorphism*

$$h : H^*_G(X) \longrightarrow \operatorname*{proj\,lim}_{(A,c)\in\mathcal{A}(G,X)} H^*_A$$

is an F-isomorphism. That is, every element in $\ker h$ *is nilpotent, and, for any* $y \in \operatorname{proj\,lim} H^*_A$, $y^{p^n} \in \operatorname{image}(h)$, *for some* n.

Remark. Speaking loosely, h being an F-isomorphism means that h is an isomorphism "modulo nilpotents." The condition on the image of h is that $\operatorname{coker} h$ consists of nilpotent elements which are killed by a pth power.

Theorem 6.2 has several consequences which will be of use in later sections. Since our main interest is the case of 2-tori in $\mathrm{Spin}(n)$, it will simplify the exposition to assume $p = 2$ from here on. The reader may consult [23] for the changes necessary for the p odd case.

Remember from Section 4 that any cohomology ring $H^*(X;R)$ is commutative in the graded sense: $b \smile a = (-1)^{mn} a \smile b$, for $a \in H^m(X;R)$, $b \in H^n(X;R)$. When $R = \mathbf{Z}/2$, $-1 = 1$, so that $H^*(X;\mathbf{Z}/2)$ is also commutative in the usual sense. The machinery of commutative algebra, e.g., prime ideals, can be applied to $H^*(X;\mathbf{Z}/2)$.

A 2-torus A of rank r can be viewed as an r-dimensional vector space over $\mathbf{Z}/2$. As such, it has a dual vector space denoted $A^\sharp$. There is a canonical isomorphism $H^1_A \cong A^\sharp$ from which one can prove that $H^*_A \cong S(A^\sharp)$, where $S(A^\sharp)$ is the symmetric algebra on $A^\sharp$.

Because $S(A^\sharp)$ is a polynomial ring, the kernel $\wp_{A,c}$ of the homomorphism $(A,c)^* : H^*_G(X) \to H^*_A$ of (6.1) is a prime ideal in $H^*_G(X)$. One can characterize the prime ideals of $H^*_G(X)$ which are of the form $\wp_{A,c}$. Remember that the Steenrod squaring operations were defined in Section 4.

THEOREM 6.3 (QUILLEN, [23, THEOREM 12.1]). *A prime ideal of* $H^*_G(X)$ *is of the form* $\wp_{A,c}$ *for some pair* (A,c) *if and only if it is homogeneous and stable under the Steenrod squaring operations* Sq^i, $i \geq 0$.

Further relations among the $\wp$'s are summarized in the next theorem of Quillen.

THEOREM 6.4 (QUILLEN, [23, PROPOSITION 11.2]).

(1) *One has* $\wp_{A,c} \supset \wp_{A',c'}$ *if and only if there is a morphism* $(A,c) \to (A',c')$; *in particular* $\wp_{A,c} = \wp_{A',c'}$ *if and only if* (A,c) *and* (A',c') *are isomorphic.*

(2) *There is a one-to-one correspondence between conjugacy classes of maximal pairs* (A, c) *and minimal prime ideals of* $H_G^*(X)$ *given by associating to* (A, c) *the prime ideal* $\wp_{A,c}$.

Remark. Theorems 6.3 and 6.4 show that there is an order-reversing correspondence between the category $\mathcal{A}(G, X)$ and the category of homogeneous, Sq^i-stable, prime ideals of $H_G^*(X)$. When $X = \text{pt}$, $\mathcal{A}(G, X)$ is just the category of 2-tori in G, while $H_G^*(\text{pt}) = H^*(BG)$ is the cohomology of the classifying space of G. When $G = \text{Spin}(n)$, more details on this correspondence, plus examples, can be found in [26, §5].

One final consequence of Quillen's main theorem relates the Krull dimension of H_G^* to the 2-rank of G.

THEOREM 6.5 (QUILLEN, [23, THEOREM 7.7, COROLLARY 7.8]). *The Krull dimension of* $H_G^*(X)$ *equals the maximum rank of a 2-torus* A *of* G *such that* $X^A \neq \emptyset$. *In particular, when* $X = pt$, *the Krull dimension of* H_G^* *equals* $r_2(G)$, *the maximum rank of a 2-torus of* G.

Looking ahead, the basic strategy in Section 8 will be to find actions of $G = \text{Spin}(n)$ on various X such that the minimum weight $d(A)$ of a 2-torus A affects whether or not X^A is empty. It is only when $X^A \neq \emptyset$ that (A, c) can contribute a prime ideal to $H_G^*(X)$.

By examining the Morse theory of the trace functional on $\text{Spin}(n)$, various candidates arise for $\text{Spin}(n)$-actions with weight-theoretic importance. This is the topic we start in the next section.

7. Morse theory on Spin(n). In its broadest sense, Morse theory relates the topology of a manifold to the behavior of the critical points of a function on the manifold. Morse's original formulation of the theory, where the critical points are isolated, is expounded in [19]. Bott's generalization of the theory to non-isolated critical points appears in [7] and [8]. The main features of Morse theory are summarized in this section, drawing heavily on the cogent account of Atiyah and Bott [1, §1]. Then the Morse theory of the trace functional on $\text{Spin}(n)$ is examined.

Throughout this section, let X be a smooth, compact manifold, and let $f : X \to \mathbf{R}$ be a smooth function on X. A point $x \in X$ is a *critical point* of f if the differential df of f vanishes at x. (In local coordinates on X, all the partial derivatives of f vanish at x.) At a critical point x, the *Hessian* $H_x f$ is a well-defined symmetric bilinear form on the tangent space $T_x X$ of X at x. (In local coordinates, $H_x f$ is represented by the matrix of second-order partial derivatives of f at x.) The critical point x is *non-degenerate* if $H_x f$ is non-degenerate, and the *index* $\lambda_x(f)$ of f at a non-degenerate critical point x is the number of negative eigenvalues in a diagonalization of $H_x f$.

If $f : X \to \mathbf{R}$ has only non-degenerate critical points, define the *Morse counting series*

$M_t(f)$ by

$$M_t(f) = \sum_{x \text{ critical}} t^{\lambda_x(f)},$$

where the sum is over the (finite number of) critical points of f.

Information about the topology of X, in particular its cohomology, can be summarized in the Poincaré series of X. If K is any field, the *Poincaré series* of X relative to K is defined as

$$P_t(X;K) = \sum_i t^i \dim H^i(X;K).$$

One of the fundamental results in Morse theory is the relationship between the Morse counting series and the Poincaré series. The relationship is called the Morse inequalities.

THEOREM 7.1 (MORSE INEQUALITIES). *There exists a polynomial $R(t)$ with non-negative coefficients such that*

$$M_t(f) - P_t(X;K) = (1+t)R(t).$$

In particular, the coefficients of $M_t(f)$ dominate those of $P_t(X;K)$, and $M_{-1}(f) = P_{-1}(X) = \chi(X)$, the Euler number of X.

Remark. The Morse inequalities follow from the main structure theorem of Morse theory, which tells how the sub-level sets $X_a = \{x \in X \mid f(x) \leq a\}$ relate. More precisely, X_a is homotopy equivalent to X_b if there are no critical values of f between a and b. Also, X_b is obtained from X_a by attaching a λ-cell, if there is one critical point x of index λ in $X_b - X_a$. Thus the information on non-degenerate critical points and indices describes the handlebody structure of X.

In many examples of functions $f : X \to \mathbb{R}$ (in particular, the trace functional on a Lie group), the critical points of f are not isolated, hence degenerate. Although the Morse theory above does not apply in this situation, Bott has a generalization of Morse theory which often does apply.

Let $Y \subset X$ be a connected submanifold of X. We say that Y is a *non-degenerate critical manifold* for f if $df \equiv 0$ on Y and $H_Y f$ is non-degenerate on the normal bundle $\nu(Y)$ of Y. A function $f : X \to \mathbb{R}$ is called *non-degenerate* if its set of critical points is a union of non-degenerate critical manifolds. To emphasize, at every point $y \in Y$, the Hessian $H_y f$ at y vanishes when restricted to the tangent space $T_y Y$ to Y at y (because $df \equiv 0$ on Y). The non-degeneracy condition is that $H_y f$ is non-degenerate when restricted to a normal space $\nu_y(Y)$ to Y at y.

By putting a Riemannian metric on the normal bundle $\nu(Y)$, $H_Y f$ can be thought of as a non-degenerate self-adjoint operator $\nu(Y) \to \nu(Y)$. It then defines an orthogonal splitting $\nu(Y) = \nu^+(Y) \oplus \nu^-(Y)$ into spaces spanned by the positive and negative eigenvectors,

respectively. The *index* λ_Y of Y as a critical manifold of f is defined to be the fiber dimension of $\nu^-(Y)$ (a constant, since Y is connected). To avoid technical difficulties, we assume the negative normal bundle $\nu^-(Y)$ is orientable.

The generalization of the Morse counting series for non-degenerate f is defined as

$$M_t(f) = \sum_{Y \text{ critical}} t^{\lambda_Y} P_t(Y),$$

where the summation is over all the non-degenerate critical manifolds Y of f, and where a coefficient field K has been fixed. Once again, the Morse inequalities are true.

THEOREM 7.2 (MORSE-BOTT INEQUALITIES). *If f is a non-degenerate function on X, then*

$$M_t(f) - P_t(X) = (1+t)R(t),$$

where $R(t)$ is a polynomial with non-negative coefficients.

We next wish to examine the Morse theory of the trace functional on $X = \mathrm{Spin}(n)$. More specifically, let $f : \mathrm{Spin}(n) \to \mathbf{R}$ be $f = -\mathrm{tr} \circ \pi$, where $\pi : \mathrm{Spin}(n) \to \mathrm{SO}(n)$ is the standard projection of Section 3, and tr is the trace. If $x \in \mathrm{Spin}(n)$ actually belongs to $\tilde{V}(n)$, so that $\pi(x)$ is a diagonal matrix, then $f(x)$ equals the number of -1's minus the number of $+1$'s on the diagonal in $\pi(x)$. Viewing x as a binary code word, we see that $f(x) = 2\,\mathrm{wt}(x) - n$, where $\mathrm{wt}(x)$ is the weight of x (Section 3). Since questions concerning the weights of code words are of crucial importance in coding theory, f is a natural function to investigate.

The Morse theory of the trace functional on the classical matrix groups has been studied by Frankel [12]. (We learned of this work from Haynes Miller and his paper [18], which generalizes Frankel's results.) Much of Frankel's work on $\mathrm{SO}(n)$ carries over directly to the case of $\mathrm{Spin}(n)$. In succeeding paragraphs, we follow closely Frankel's line of argument.

We fix a bi-invariant Riemannian metric on $\mathrm{Spin}(n)$, and use the metric to identify the differential df of f with the gradient vector field $\mathrm{grad}\, f$. We need to review a few facts about maximal tori in compact, connected Lie groups. A *torus* in G is a subgroup of G which is isomorphic to a product of circle groups. A *maximal torus* in G is a torus in G which is contained in no larger torus in G. Maximal tori play an important role in the study of compact, connected Lie groups. The basic properties of maximal tori are summarized next. See [9, p. 159].

THEOREM 7.3 (MAXIMAL TORUS THEOREM). *Let G be a compact, connected Lie group. Then every element of G is contained in a maximal torus, and any two maximal tori in G are conjugate.*

We fix a choice of maximal torus $\tilde{T}$ in $\mathrm{Spin}(n)$ as follows. Let $k = [n/2]$, so that $n = 2k$ or $n = 2k+1$, if n is even or odd, respectively. In terms of Clifford algebra multiplication

from Section 3,

$$\tilde{T} = \left\{ \prod_{j=1}^{k} (\cos 2\pi t_j - e_{2j-1}e_{2j} \sin 2\pi t_j) \mid t_j \in \mathbf{R}/\mathbf{Z} \right\} \tag{7.4}$$

is a maximal torus of $\mathrm{Spin}(n)$ which double covers the standard maximal torus T of $\mathrm{SO}(n)$. Explicitly, T is of the form

$$T = \left\{ \begin{pmatrix} R(\theta_1) & & & \\ & \ddots & & \\ & & R(\theta_k) & \\ & & & (1) \end{pmatrix} \right\},$$

where

$$R(\theta) = \begin{pmatrix} \cos 2\pi\theta & -\sin 2\pi\theta \\ \sin 2\pi\theta & \cos 2\pi\theta \end{pmatrix}, \quad \theta \in \mathbf{R}/\mathbf{Z},$$

and the 1 appears only if $n = 2k+1$ is odd. Denote the element $R(\theta_1) \times \cdots \times R(\theta_k) \in T$ by $(\theta_1, \ldots, \theta_k)$. The double covering map $\tilde{T} \to T$ sends

$$\prod_{j=1}^{k} (\cos 2\pi t_j - e_{2j-1}e_{2j} \sin 2\pi t_j) \mapsto (2t_1, \ldots, 2t_k).$$

(The reader should be aware of the conventions used for factors of 2π—the mapping doubles the angles.)

For any point $x \in \mathrm{Spin}(n)$, let $M_x = \{gxg^{-1} \mid g \in \mathrm{Spin}(n)\}$ be the space of conjugates of x. It is well-known that M_x is an embedding of the homogeneous space $\mathrm{Spin}(n)/C(x)$, where $C(x) = \{g \in \mathrm{Spin}(n) \mid gxg^{-1} = x\}$ is the *centralizer* of x in $\mathrm{Spin}(n)$. Because the trace is a class function, we have $f(gxg^{-1}) = f(x)$, for all $g, x \in \mathrm{Spin}(n)$. It will be useful to know the center of $\mathrm{Spin}(n)$. See [26, Remark 1.4].

PROPOSITION 7.5. *The center of* $\mathrm{Spin}(2k+1)$ *is* $\{\pm 1\}$. *The center of* $\mathrm{Spin}(2k)$ *is* $\{\pm 1, \pm e_1 e_2 \cdots e_{2k}\}$, *which is isomorphic to* $\mathbf{Z}/2 \oplus \mathbf{Z}/2$ *when* k *is even and isomorphic to* $\mathbf{Z}/4$ *when* k *is odd.*

To examine the critical points of f, note that if $\operatorname{grad} f = 0$ at x, then $\operatorname{grad} f = 0$ at gxg^{-1}, for any $g \in \mathrm{Spin}(n)$. This holds because f is a class function. Consequently, if x is a critical point, the conjugacy class M_x of x is a critical manifold. As mentioned above, x is contained in some maximal torus, so x is conjugate to some element h in the fixed maximal torus $\tilde{T}$. Thus the critical set of f on $\mathrm{Spin}(n)$ consists of the conjugates of the critical points of f which lie on $\tilde{T}$. Frankel [12, Lemma 1] has shown that $\operatorname{grad} f$ is tangent to $\tilde{T}$ at each point $h \in \tilde{T}$, so that the critical points of f (as a function on $\mathrm{Spin}(n)$) which

lie on $\tilde{T}$ are the same as the critical points of f restricted to $\tilde{T}$ (as a function on $\tilde{T}$). This reduces the problem of finding the critical points of f on $\mathrm{Spin}(n)$ to finding the critical points of f on $\tilde{T}$.

To determine the critical points of f on $\tilde{T}$, we use a slightly different parameterization of $\tilde{T}$. The problem with (7.4) is that the mapping $\mathbf{R}^k/\mathbf{Z}^k \to \tilde{T}$ sending

$$(t_1, \dots, t_k) \mapsto \prod_{j=1}^{k} (\cos 2\pi t_j - e_{2j-1}e_{2j} \sin 2\pi t_j)$$

is not injective. (Let one $t = 1/2$, the rest 0; the result is always $-1 \in \tilde{T}$.) To remedy this, we follow Bröcker and tom Dieck [9, p. 174]. There is an isomorphism $\beta : \mathbf{R}^k/\mathbf{Z}^k \to \tilde{T}$ sending $(\zeta_1, \dots, \zeta_k) \mapsto \beta_1\beta_2 \cdots \beta_k$, $\zeta_\nu \in \mathbf{R}/\mathbf{Z}$, where

$$\beta_1 = \cos 2\pi\zeta_1 - e_1e_2 \sin 2\pi\zeta_1,$$

and

$$\beta_j = (\cos \pi\zeta_j + e_1e_2 \sin \pi\zeta_j)(\cos \pi\zeta_j - e_{2j-1}e_{2j} \sin \pi\zeta_j), \quad j > 1.$$

Simplifying the product $\beta_1\beta_2 \cdots \beta_k$, we have

(7.6)

$$\begin{aligned}\beta_1\beta_2 \cdots \beta_k = {} & (\cos \pi(2\zeta_1 - \zeta_2 - \cdots - \zeta_k) - e_1e_2 \sin \pi(2\zeta_1 - \zeta_2 - \cdots - \zeta_k)) \\ & \times \prod_{j=2}^{k} (\cos \pi\zeta_j - e_{2j-1}e_{2j} \sin \pi\zeta_j).\end{aligned}$$

Thus we see that $\pi(\beta_1\beta_2 \cdots \beta_k) = (2\zeta_1 - \zeta_2 - \cdots - \zeta_k, \zeta_2, \dots, \zeta_k) \in T$. (Beware the 2π-conventions!) Computing the trace we have

$$f(\zeta_1, \dots, \zeta_k) \equiv -2 \cos 2\pi(2\zeta_1 - \zeta_2 - \cdots - \zeta_k) - 2\sum_{j=2}^{k} \cos 2\pi\zeta_j \bmod 1.$$

At critical points we see that $\sin 2\pi(2\zeta_1 - \zeta_2 - \cdots - \zeta_k) = \sin 2\pi\zeta_j = 0$, $j > 1$ ($\zeta_\nu \in \mathbf{R}/\mathbf{Z}$). Then $\zeta_j \equiv 0, 1/2 \bmod 1$ ($j > 1$), and $2\zeta_1 - \zeta_2 - \cdots - \zeta_k \equiv 0, 1/2 \bmod 1$, also. In (7.6), this implies that $\beta_1\beta_2 \cdots \beta_k$ is $\pm$ a product of pairs of the form $e_{2j-1}e_{2j}$, for various j. More precisely, write

$$\beta_1\beta_2 \cdots \beta_k = \pm \prod_{j \in J} e_{2j-1}e_{2j},$$

where $J \subset \{1, 2, \dots, k\}$.

In general, any two elements σ of the form $\pm \prod_{j \in J} e_{2j-1}e_{2j}$ will be conjugate if their index sets J have the same number of elements. (For example, $-\sigma$ is conjugate to σ, in

general.) There are some exceptions. When $J = \emptyset$, $\sigma = 1$ and $-\sigma = -1$ are not conjugate, since they are central in $\mathrm{Spin}(n)$. Also, when $n = 2k$ is even, and $J = \{1, 2, \ldots, k\}$, then $\sigma = e_1 e_2 \cdots e_n$ and $-\sigma = -e_1 e_2 \cdots e_n$ are not conjugate, because they too are central. Since M_σ is connected, each M_σ passes through all the conjugates of σ. Thus to discuss the critical manifolds of f, we need only take one σ from each conjugacy class. Hence we may assume that σ has the form $\pm\sigma_0 = \pm 1$ ($J = \emptyset$) or, for $j = 1, 2, \ldots, k$,

$$\sigma_j = \prod_{q=1}^{j} e_{2q-1} e_{2q}.$$

When $n = 2k$ is even, we need both $\pm e_1 e_2 \cdots e_n$.

The critical submanifolds $M_j = M_{\sigma_j}$ are homogeneous spaces of the form $\mathrm{Spin}(n)/C(\sigma_j)$, where C denotes the centralizer. Both ± 1 are in the center of $\mathrm{Spin}(n)$, so $C(\pm 1) = \mathrm{Spin}(n)$ and both $+M_0 = \{+1\}$ and $-M_0 = \{-1\}$ are one point critical manifolds. When $n = 2k$ is even, $\pm e_1 e_2 \cdots e_n$ are both central, so $M_k = \{e_1 e_2 \cdots e_n\}$ and $-M_k = \{-e_1 e_2 \cdots e_n\}$ are also single points. In the general case, $C(\sigma_j) = \mathrm{Spin}(2j) \times \mathrm{Spin}(n-2j)$, so that $M_j = \mathrm{Spin}(n)/(\mathrm{Spin}(2j) \times \mathrm{Spin}(n-2j))$ is isomorphic to $\mathrm{SO}(n)/(\mathrm{SO}(2j) \times \mathrm{SO}(n-2j)) \cong \widetilde{Gr}(2j, \mathbf{R}^n)$, the Grassmannian of oriented $2j$-planes in $\mathbf{R}^n$. Summarizing, we have

THEOREM 7.7. *The function $f = -\operatorname{tr} \circ \pi$ on $\mathrm{Spin}(n)$ has critical manifolds as follows.*

$n = 2k+1$: $\{+1\}$, $\{-1\}$ *and* $\widetilde{Gr}(2j, \mathbf{R}^{2k+1})$, $j = 1, 2, \ldots, k$.

$n = 2k$: $\{+1\}$, $\{-1\}$, $\{e_1 e_2 \cdots e_{2k}\}$, $\{-e_1 e_2 \cdots e_{2k}\}$, *and* $\widetilde{Gr}(2j, \mathbf{R}^{2k})$, $j = 1, 2, \ldots, k-1$.

Remark. The critical values of $f = -\operatorname{tr} \circ \pi$, i.e., the values of f at its critical manifolds, are: $f(\pm 1) = -n$, $f(\widetilde{Gr}(2j, \mathbf{R}^n)) = 4j - n$. When $n = 2k$ is even, $f(\pm e_1 e_2 \cdots e_n) = n$. The critical points ± 1 are global minima; the critical points $\pm e_1 e_2 \cdots e_n$ ($n = 2k$) are global maxima. When $n = 2k+1$, $\widetilde{Gr}(2k, \mathbf{R}^{2k+1})$ consists of global maxima.

The arguments dealing with the non-degeneracy of the critical manifolds and their indices are technical, and we choose not to include them here. Basically they follow Frankel's method of attack and yield the following result.

THEOREM 7.8. *The critical manifolds of $f = -\operatorname{tr} \circ \pi$ on $\mathrm{Spin}(n)$ are all non-degenerate. Their indices are:*

$$\lambda(\{+1\}) = \lambda(\{-1\}) = 0,$$
$$\lambda(\widetilde{Gr}(2j, \mathbf{R}^n)) = j(2j-1),$$
$$\lambda(\{e_1 e_2 \cdots e_n\}) = \lambda(\{-e_1 e_2 \cdots e_n\}) = k(2k-1) = \dim \mathrm{Spin}(n), \quad \text{when } n = 2k.$$

In addition, all the negative normal bundles $\nu^-(M_\sigma)$ are orientable.

In summary, the function $f = -\operatorname{tr} \circ \pi$ on $\mathrm{Spin}(n)$ is related to the weight properties of codes. It also is a non-degenerate Morse function on $\mathrm{Spin}(n)$, whose critical manifolds are

well-known spaces. In the next section we describe a program for detecting doubly-even codes of high minimum weight by using both the Morse theory and equivariant cohomology.

8. Detection of maximal 2-tori with high minimum weight. Armed with several topological tools from preceding sections, we wish to address a coding theory question: How can one detect the existence of maximal doubly-even self-orthogonal codes with high minimum weight? We offer one approach to a solution in this section.

The basic tool is Theorem 6.4, which, given an action of $\mathrm{Spin}(n)$ on X, establishes a one-to-one correspondence of conjugacy classes of maximal pairs (A, c) of 2-tori A and components of their fixed point sets with minimal prime ideals of $H^*_{\mathrm{Spin}(n)}(X)$. Already when $X =$ point, maximal 2-tori in $\mathrm{Spin}(n)$, i.e., maximal doubly-even self-orthogonal codes, are in one-to-one correspondence with minimal prime ideals in $H^*_{\mathrm{Spin}(n)} \cong H^*(B\mathrm{Spin}(n))$. Quillen [24, Theorem 6.5] has determined the ring structure of $H^*(B\mathrm{Spin}(n))$, but to determine the minimal prime ideals seems too general and too hard a problem to carry out at this time. (It is equivalent to classifying the maximal doubly-even self-orthogonal codes. This has been done for $n \leq 32$ by Conway, Pless, and Sloane [21], [22], and [10]. It is well-near impossible for $n = 40$ [10, pp. 52–53].) See [26, §5] for other details.

Part of the problem with taking $X =$ point is that $H^*(B\mathrm{Spin}(n))$ might provide too much information: we are getting information about all the doubly-even codes with no special emphasis being placed on those of high minimum weight. It is for this reason that we bring the trace functional $f = -\operatorname{tr} \circ \pi$ on $\mathrm{Spin}(n)$ into play, since $f(x) = 2\,\mathrm{wt}(x) - n$. We use f to define special spaces X on which $\mathrm{Spin}(n)$ can act.

Remember that $\mathrm{Spin}(n)$ acts on itself by conjugation and that f is a class function: $f(gxg^{-1}) = f(x)$, for all $g, x \in \mathrm{Spin}(n)$. Thus any subspace of $\mathrm{Spin}(n)$ of the form

$$X_{\alpha,\beta} = \{x \in \mathrm{Spin}(n) \mid \alpha < f(x) < \beta\} \quad (\alpha < \beta)$$

inherits a $\mathrm{Spin}(n)$ action. One can understand the topology of $X_{\alpha,\beta}$ by using Morse theory—as in Section 7. Only those critical manifolds with critical values between α and β will contribute to the Morse-Bott inequalities for $X_{\alpha,\beta}$.

If one uses $X_{\alpha,\beta}$ as the space on which $\mathrm{Spin}(n)$ acts, minimal prime ideals of $H^*_{\mathrm{Spin}(n)}(X_{\alpha,\beta})$ correspond to maximal 2-tori A such that ${X_{\alpha,\beta}}^A \neq \emptyset$, i.e., only those maximal 2-tori A which have fixed points on $X_{\alpha,\beta}$. What are the fixed points of A on $X_{\alpha,\beta}$? The fixed points of A on $\mathrm{Spin}(n)$ itself are just the centralizer

$$C(A) = \{x \in \mathrm{Spin}(n) \mid axa^{-1} = x, \text{ for all } a \in A\}$$

of A in $\mathrm{Spin}(n)$. Thus ${X_{\alpha,\beta}}^A = C(A) \cap X_{\alpha,\beta}$, i.e., those elements of the centralizer of A whose "weights" are restricted by the inequalities $\alpha < f(x) < \beta$.

For the rest of the section, let us assume that $n \equiv 0, 1, 7 \bmod 8$. In these cases, maximal 2-tori are also maximal abelian subgroups of $\mathrm{Spin}(n)$ ([26, Theorem 3.20]), i.e., $C(A) = A$.

Then ${X_{\alpha,\beta}}^A = A \cap X_{\alpha,\beta}$. Remember that $f(\pm 1) = -n$ and that ± 1 are always in the center of $\mathrm{Spin}(n)$, hence in any $C(A)$. If α is chosen so that $\alpha \geq -n$, then $\pm 1 \notin X_{\alpha,\beta}$. Now fix an integer $d > 0$ and suppose that β is chosen so that $\beta \leq 2d - n$. If A is any maximal 2-torus whose minimum weight

$$d(A) = \min\{\mathrm{wt}(x) \mid \pm 1 \neq x \in A\}$$

satisfies $d \leq d(A)$, then ${X_{\alpha,\beta}}^A = \emptyset$. Such a maximal 2-torus makes no contribution to the prime ideals in $H^*_{\mathrm{Spin}(n)}(X_{\alpha,\beta})$. We summarize.

THEOREM 8.1. *Assume $n \equiv 0, 1, 7 \bmod 8$, and $d > 0$. A maximal 2-torus A of $\mathrm{Spin}(n)$ has fixed points on $X_{-n,2d-n}$ if and only if the minimum weight $d(A) < d$. In particular, only those maximal 2-tori A with minimum weight $d(A) < d$ contribute prime ideals to $H^*_{\mathrm{Spin}(n)}(X_{-n,2d-n})$.*

Once the principle behind Theorem 8.1 is understood, there are several directions to explore. One can now vary the values of α and β, for example. If $\alpha < -n$, then $\pm 1 \in X_{\alpha,\beta}$, so that every maximal 2-torus A has ${X_{\alpha,\beta}}^A \neq \emptyset$. Thus all maximal 2-tori contribute prime ideals to $H^*_{\mathrm{Spin}(n)}(X_{-n-\epsilon,2d-n})$, while only those with $d(A) < d$ contribute to $H^*_{\mathrm{Spin}(n)}(X_{-n,2d-n})$.

Similar reasoning applies when one varies β. Maximal 2-tori A with $d(A) = d$ do not contribute prime ideals to $H^*_{\mathrm{Spin}(n)}(X_{-n,2d-n})$, but they do contribute prime ideals to $H^*_{\mathrm{Spin}(n)}(X_{-n,2d-n+\epsilon})$. By step-wise increasing β, one gets contributions from maximal 2-tori of increasingly higher minimum weight. The problem then is to understand precisely how the prime ideals of $H^*_{\mathrm{Spin}(n)}(X_{-n,\beta})$ change as β varies from $2d-n$ to $2d-n+\epsilon$. This should allow one to detect maximal 2-tori A with $d(A) = d$.

The stategy of changing β and seeing how cohomology changes is precisely the idea behind the fundamental structure theorem of Morse theory (see Remark following Theorem 7.1), only now it is being applied in the context of equivariant cohomology theory. The author is continuing to pursue these methods, and ideas of Atiyah and Bott [1, §1] may be of use.

Concluding Remarks. My goal in this paper has been to outline in some depth the interrelationships between coding theory and the topology of $\mathrm{Spin}(n)$. I hope I have succeeded in showing that equivariant Morse theory may be of use in detecting the existence of maximal doubly-even codes of high minimum weight. There is more work to be done, and I hope the reader agrees that it is worth the effort.

REFERENCES

[1] Michael F. Atiyah and Raoul Bott, *The Yang-Mills equations over Riemann surfaces*, Philosophical Transactions of the Royal Society of London, A 308 (1982), pp. 523–615.

[2] Michael F. Atiyah, Raoul Bott and Arnold Shapiro, *Clifford Modules*, Topology, 3(Supp 1) (1964), pp. 3–38.

[3] Armand Borel, *Seminar on Transformation Groups*, Annals of Mathematics Studies 46, Princeton University Press, Princeton, N. J., 1960.

[4] ————, *Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tôhoku Mathematical Journal, 13 (1961), pp. 216–240.

[5] ————, *On the p-rank of compact connected Lie groups*, preprint 1987.

[6] Armand Borel and Jean-Pierre Serre, *Sur certains sous-groupes des groupes de Lie compacts*, Commentarii Mathematici Helvetici, 27 (1953), pp. 128–139.

[7] Raoul Bott, *Nondegenerate critical manifolds*, Annals of Mathematics, 60 (1954), pp. 248–261.

[8] ————, *The stable homotopy of the classical groups*, Annals of Mathematics, 70 (1959), pp. 313–337.

[9] Theodor Bröcker and Tammo tom Dieck, *Representations of Compact Lie Groups*, Graduate Texts in Mathematics 98, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1985.

[10] John H. Conway and Vera Pless, *On the enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A, 28 (1980), pp. 26–53.

[11] Simon K. Donaldson, *An application of gauge theory to the topology of 4-manifolds*, Journal of Differential Geometry, 18 (1983), pp. 279–315.

[12] Theodore Frankel, *Critical submanifolds of the classical groups and Stiefel manifolds*, in *Differential and Combinatorial Topology: A Symposium in Honor of Marston Morse*, Stewart S. Cairns, editor, Princeton University Press, Princeton, N. J., 1965, pp. 37–53.

[13] Daniel S. Freed and Karen K. Uhlenbeck, *Instantons and Four-Manifolds*, Mathematical Sciences Research Institute Publications 1, Springer-Verlag, New York, Heidelberg, Berlin, 1984.

[14] Sigurdur Helgason, *Differential Geometry, Lie Groups, and Symmetric Spaces*, Pure and Applied Mathematics 80, Academic Press, New York, San Francisco, London, 1978.

[15] Shoshichi Kobayashi and Katsumi Nomizu, *Foundations of Differential Geometry*, Interscience Tracts in Pure and Applied Mathematics 15, Interscience Publishers, New York, London, Sydney, 1963/1969.

[16] Saunders MacLane, *Homology*, Grundlehren der mathematischen Wissenschaften 114, Springer-Verlag, Berlin, Göttingen, Heidelberg, 1963.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library 16, North-Holland, Amsterdam, New York, Oxford, 1978.

[18] Haynes Miller, *Stable splittings of Stiefel manifolds*, Topology, 24 (1985), pp. 411–419.

[19] John W. Milnor, *Morse Theory*, Annals of Mathematics Studies 51, Princeton University Press, Princeton, N. J., 1969.

[20] John W. Milnor and James D. Stasheff, *Characteristic Classes*, Annals of Mathematics Studies 76, Princeton University Press, Princeton, N. J., 1974.

[21] Vera Pless, *A classification of self-orthogonal codes over $GF(2)$*, Discrete Mathematics, 3 (1972), pp. 209–246.

[22] Vera Pless and N. J. A. Sloane, *On the classification and enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A, 18 (1975), pp. 313–335.

[23] Daniel Quillen, *The spectrum of an equivariant cohomology ring I,II*, Annals of Mathematics, 94 (1971), pp. 549–602.

[24] ————, *The mod 2 cohomology rings of extra-special 2-groups and the spinor groups*, Mathematische Annalen, 194 (1971), pp. 197–212.

[25] Norman Steenrod, *The Topology of Fibre Bundles*, Princeton University Press, Princeton, N. J., 1951.

[26] Jay A. Wood, *Spinor groups and algebraic coding theory*, Journal of Combinatorial Theory, Series A (to appear).

[27] ————, *Flat connections, spinor groups and error-correcting codes*, submitted to the Proceedings of the 1988 Northwestern International Conference on Algebraic Topology.