THE 2-SELMER GROUP OF A NUMBER FIELD AND HEURISTICS FOR NARROW CLASS GROUPS AND SIGNATURE RANKS OF UNITS

DAVID S. DUMMIT AND JOHN VOIGHT
(APPENDIX WITH RICHARD FOOTE)

ABSTRACT. We investigate in detail a homomorphism which we call the 2-Selmer signature map from the 2-Selmer group of a number field K to a nondegenerate symmetric space, in particular proving the image is a maximal totally isotropic subspace. Applications include precise predictions on the density of fields K with given narrow class group 2-rank and with given unit group signature rank. In addition to theoretical evidence, extensive computations for totally real cubic and quintic fields are presented that match the predictions extremely well. In an appendix with Richard Foote, we classify the maximal totally isotropic subspaces of orthogonal direct sums of two nondegenerate symmetric spaces over perfect fields of characteristic 2 and derive some consequences, including a mass formula for such subspaces.

CONTENTS

1. INTRODUCTION

Let K be a number field of degree $n = [K : \mathbb{Q}] = r_1 + 2r_2$, where r_1, r_2 as usual denote the number of real and complex places of K, respectively. We assume here that $r_1 > 0$, i.e., that K is not totally complex, in order to avoid trivialities. Let C_K denote the class group of K and $E_K = \mathcal{O}_K^*$ the unit group of K.

The purpose of this paper is to closely investigate the 2-Selmer group of K, defined as

$$\mathrm{Sel}_2(K) = \{z \in K^* : (z) = \mathfrak{a}^2 \text{ for some fractional ideal } \mathfrak{a}\}/K^{*2}$$

and a homomorphism

$$\varphi : \mathrm{Sel}_2(K) \to V_\infty \perp V_2,$$

2010 *Mathematics Subject Classification.* 11R29, 11R27, 11R45, 11Y40.

which we call the 2-Selmer signature map, from $\mathrm{Sel}_2(K)$ to an orthogonal direct sum of two nondegenerate symmetric spaces over $\mathbb{F}_2$. The spaces V_∞ and V_2 are constructed from the archimedean and 2-adic completions of K and their nondegenerate symmetric space structures are induced by the quadratic Hilbert symbol. The homomorphism φ is composed of two maps, the first mapping to V_∞ that records signs under the real embeddings of K, and the second to V_2 that keeps track of certain 2-adic congruences up to squares. See Sections 4 and 5 for details.

Our first main result is the following theorem (Theorem 6.1).

Theorem. *The image of the 2-Selmer signature map $\varphi : \mathrm{Sel}_2(K) \to V_\infty \perp V_2$ is a maximal totally isotropic subspace.*

The spaces V_∞ and V_2 have, separately, been studied (see Remark 6.4), however the observation that the image is a *maximal* totally isotropic subspace, which follows from a computation of the relevant dimensions, has been missed in previous work. This observation is crucial, because we can prove (in the Appendix with Richard Foote) a fundamental structure theorem (Theorem A.13) for maximal totally isotropic subspaces of orthogonal direct sums such as $V_\infty \perp V_2$. This structure theorem then allows us to compute the probability that a subspace of $V_\infty \perp V_2$ is isomorphic to a given maximal totally isotropic subspace (Theorem 6.7), which in turn then allows us to give several precise conjectures related to the size of the narrow class group of K and of the group of possible signatures of units of K.

To state these conjectures, first recall that the 2-rank, $\mathrm{rk}_2(A)$, of an abelian group A is the dimension of $A/2A$ as a vector space over $\mathbb{F}_2$. If A is finite, then $\mathrm{rk}_2(A) = \dim A[2]$, where $A[2] = \{x \in A : 2x = 0\}$ is the subgroup of elements of order dividing 2, and if A is an elementary abelian 2-group, we have $\#A = 2^{\mathrm{rk}_2(A)}$.

For nonnegative integers m, define the symbol (the q-Pochhammer symbol $(q^{-1};q^{-1})_{m-1}$)

$$(q)_m = \prod_{i=1}^{m}(1-q^{-i}). \tag{1.1}$$

If K is a number field whose Galois closure has the symmetric group S_n as Galois group we refer to K simply as an 'S_n-field'.

If ρ denotes the 2-rank of C_K and ρ^+ denotes the 2-rank of the narrow class group C_K^+ of K, it is a theorem due to Armitage and Fröhlich (for which we provide two proofs) that $\rho^+ - \rho \le \lfloor r_1/2 \rfloor$. Our first application (Conjecture 7.1) predicts the distribution of the values of $\rho^+ - \rho$.

Conjecture. *As K varies over S_n-fields of odd degree n with signature (r_1, r_2) (counted by absolute discriminant), the density of fields such that $\rho^+ - \rho = k$ for $0 \le k \le \lfloor r_1/2 \rfloor$ is*

$$\frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}}{2^{k(k+r_2)}(2)_k(2)_{k+r_2}(4)_{r_1+r_2-1}(4)_{(r_1-1)/2-k}}\,.$$

If we combine this conjecture with the existing predictions of Malle [M3, Conjecture 2.1, Proposition 2.2] and Adam–Malle [A-M] for the distribution of the values of $\rho = \mathrm{rk}_2 C_K$, we obtain a conjecture on the distribution of the values of ρ^+ (see Conjecture 7.5).

One consequence of Conjecture 7.5 is a prediction for the distribution of the 2-rank of the narrow class group of S_n-fields with a fixed r_2 and odd r_1 tending to infinity (see Corollary 7.9); for totally real S_n-fields of odd degree n tending to infinity we predict the 2-rank ρ^+ of

the narrow class group is given by $(2)_\infty/2^{(\rho^+)^2}(2)^2_{\rho^+}$ (so, for example, approximately 28.879%, 57.758%, 12.835%, 0.524% and 0.005% should have 2-rank 0,1,2,3,4, respectively).

Another consequence of Conjecture 7.5 is the following conjecture (Conjecture 7.24) on the size of the 2-torsion of the narrow class group, which for $n = 3$ is known to be true by a theorem of Bhargava–Varma [B-V] (see also the results of Ho–Shankar–Varma [HSV]).

Conjecture. *The average size of $C_K^+[2]$ is $1 + 2^{-r_2}$ as K varies over S_n-fields of odd degree n with signature (r_1, r_2) (counted by absolute discriminant).*

The next application in Section 7 was the source of our original motivation (arising from certain generalizations of a refined abelian Stark's Conjecture). Every unit in E_K has a sign in each of the r_1 real embeddings of K and the collection of possible signatures of units in K is a subgroup of $\{\pm 1\}^{r_1}$. The rank of this elementary abelian 2-group is an integer s between 1 (since $-1 \in E_K$) and r_1, and is equal to 1 precisely when K has a system of fundamental units that are all totally positive. Attempts to find totally real cubic and quintic fields with a totally positive system of fundamental units suggested that such fields are rare. This contrasts markedly with the real quadratic case, for which, as Harold Stark observed to the second author, a density of 100% have a totally positive fundamental unit, hence unit signature rank 1 (since to have a unit of norm -1 the discriminant cannot be divisible by a prime $p \equiv 3 \bmod 4$). Trying to understand and reconcile these two disparate behaviors led to the question considered here: what is the density of fields K whose units have given signature rank s? In Conjecture 7.31, one of the central results of this paper, we predict the probability that an S_n-field of odd degree n and signature (r_1, r_2) has unit signature rank s for any s with $1 \le s \le r_1$.

A consequence of Conjecture 7.31 is that for totally real S_n-fields of odd degree n, the most common signature rank for the units is not n (indicating all possible signatures occur for the units), but rather $n - 1$ (more precisely, the principal terms in equation (7.32) show that the ratio of corank 1 fields to corank 0 fields is approximately $2 - 1/2^{n-2}$, the ratio of the reciprocals of the orders of the isometry groups $\mathrm{Aut}(S_1)$ and $\mathrm{Aut}(S_0)$, cf. Section 7). After corank 1 followed by corank 0, the next highest predicted densities are corank 2,3, etc., in decreasing order. Although we make no specific conjectures here for fields of even degree, the fact that corank 1 is predicted to be the most common unit signature rank (followed by $0, 2, 3, \dots$) suggests that real quadratic and totally real cubic fields may in fact be demonstrating the same, rather than disparate, behavior regarding the existence of a totally positive system of fundamental units.

Our final conjecture (Conjecture 7.33) in Section 7 is a prediction for the density of S_n-fields of odd degree n whose class group C_K (which is naturally a quotient of the narrow class group C_K^+) is in fact a direct summand of C_K^+.

While we expect the development here will be applicable to other number fields, for the conjectures in Section 7 we restrict to fields K of odd degree n whose Galois closure has the symmetric group S_n as Galois group (see the discussion at the beginning of Section 7).

When $n = 3$ or 5, i.e., when K is a cubic or quintic number field, it is known (cf. [Bha4], [Cohn], [D-H], [Bha2]) that, when ordered by absolute discriminant, a density of 100% of fields of degree n have the symmetric group S_n as Galois group for their Galois closure. As a result, in these cases the conjectures in Section 7 can be stated as densities for all fields (with given signature (r_1, r_2)). For example, in the case of totally real fields we have the following (for other possibilities for (r_1, r_2) and the exact values in these conjectures, see section 7).

Conjecture. *As K varies over all totally real cubic (respectively, all totally real quintic) fields ordered by absolute discriminant:*

(a) *$\rho^+ = \rho$ with density $2/5$, and $\rho^+ = \rho + 1$ with density $3/5$, (respectively, $\rho^+ = \rho$, $\rho^+ = \rho + 1$, and $\rho^+ = \rho + 2$ with densities $16/51$, $30/51$, and $5/51$)*

(b) *the signature rank of the units is 3, 2, and 1 with densities that are approximately 36.3%, 61.8%, and 1.9% (respectively, 5, 4, 3, 2, and 1 with densities that are approximately 30.46%, 58.93%, 10.55%, 0.058%, and 0.000019%), and*

(c) *C_K is a direct summand of C_K^+ with a density that is approximately 94.4% (respectively, 98.2%).*

The small densities predicted for totally real fields that possess a totally positive system of fundamental units—approximately one in every five million for totally real quintic fields, for example—quantifies (conjecturally) the empirical observation that such fields appear to be rare which, as previously mentioned, was the question that motivated this investigation.

It has been conjectured (see Malle, [M4]) that when ordered by absolute discriminant, a density of 100% of fields of degree n have the symmetric group S_n as Galois group for their Galois closure if and only if $n = 2$ or n is an odd prime. If we also grant this conjecture, then each of the conjectures in Section 7 can be stated as densities for all fields (with given signature (r_1, r_2)) of odd prime degree.

In Section 8 we present the results of fairly extensive computations in the case of totally real cubic and quintic fields. The numerical data agrees with the predicted values extremely well (cf. Tables 5 and 6) and provides compelling evidence for the conjectures.

We note there is no apparent function field analogue of our setting because when the prime field has nonzero characteristic, there are no 2-adic places and so the intricate bilinear structure on the direct sum of signature spaces disappears.

Organization. The remainder of this paper is organized as follows.

In Section 2 we set up basic notation, discuss the archimedean signature map, and derive some fundamental rank relations.

In Section 3, we discuss the 2-Selmer group and give an elegant but unpublished proof of the Armitage–Fröhlich theorem due to Hayes, in particular relating the 2-Selmer group with subfields of ray class groups.

In Section 4, we discuss the 2-adic signature map, then define and prove the basic properties of the 2-Selmer signature map.

In section 5, we examine the bilinear space structure provided by the Hilbert symbol.

In Section 6 we prove that the image of the 2-Selmer signature map is a maximal totally isotropic subspace and derive a number of consequences: another proof of the Armitage–Fröhlich theorem, a result of Hayes on the size of the Galois group of the compositum of unramified quadratic extensions of unit type, and fundamental results needed for the conjectures that follow. We close Section 6 with an explicit description of the possible images of the 2-Selmer signature map for fields K of degree up to 5.

Section 7 applies the results on the 2-Selmer signature map from the previous sections to produce the explicit conjectures described above.

We conclude the main body in Section 8 with a description of computations for totally real cubic and quintic fields.

Finally, Appendix A (with Richard Foote) establishes the basic properties of nondegenerate finite dimensional symmetric spaces over perfect fields of characteristic 2, proves a theorem classifying the maximal totally isotropic subspaces of an orthogonal direct sum of two such spaces, and then derives a number of consequences of the classification theorem.

Acknowledgments. The authors would like to thank Evan Dummit, Richard Foote, John Jones, Bjorn Poonen, Peter Stevenhagen, and David P. Roberts for helpful comments, and Michael Novick for some early computations that helped shape the final result. The second author was funded by an NSF CAREER Award (DMS-1151047).

2. The archimedean signature map

We begin with the usual method to keep track of the signs of nonzero elements of K at the real infinite places. Let $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$.

Definition 2.1. The archimedean signature space V_∞ of K is

$$V_\infty = K_{\mathbb{R}}^*/K_{\mathbb{R}}^{*2} \simeq \prod_{\substack{v|\infty \\ v \text{ real}}} \{\pm 1\} = \{\pm 1\}^{r_1}. \tag{2.2}$$

The multiplicative group V_∞ can also be naturally viewed as a vector space over $\mathbb{F}_2$, written additively, and we shall often consider $V_\infty \simeq \mathbb{F}_2^{r_1}$ by identifying $\{\pm 1\}$ with $\mathbb{F}_2$.

Definition 2.3. For $\alpha \in K^*$ and $v : K \hookrightarrow \mathbb{R}$ a real place of K, let $\alpha_v = v(\alpha)$ and define $\operatorname{sgn}(\alpha_v) = \alpha_v/|\alpha_v| \in \{\pm 1\}$. The archimedean signature map of K is the homomorphism

$$\begin{aligned} \operatorname{sgn}_\infty : K^* &\to V_\infty \\ \alpha &\mapsto (\operatorname{sgn}(\alpha_v))_v. \end{aligned} \tag{2.4}$$

The map $\operatorname{sgn}_\infty$ is surjective with kernel K^{*+}, the subgroup of totally positive elements of K^*, which contains the nonzero squares, K^{*2}.

Definition 2.5. The unit signature group of K is the image, $\operatorname{sgn}_\infty(E_K)$, of the units of K under the archimedean signature map. Define the (unit) signature rank of K to be the 2-rank of $\operatorname{sgn}_\infty(E_K)$:

$$\operatorname{sgnrk}(E_K) = \operatorname{rk}_2 \operatorname{sgn}_\infty(E_K).$$

The unit signature group is the subgroup of all signatures of units of K, and the size of this elementary abelian 2-group is a measure of how many signature types of units are possible. Since $-1 \in E_K$ and r_1 is assumed to be nonzero, we have $1 \leq \operatorname{sgnrk}(E_K) \leq r_1$, where the minimum is achieved precisely when K has a system of fundamental units that are all totally positive and the maximum occurs if and only if every possible signature occurs as the signature of some unit of K. For example, a real quadratic field has unit signature rank 1 if and only if the fundamental unit has norm $+1$. Note also that if $r_1 = 1$ then necessarily $\operatorname{sgnrk}(E_K) = 1$.

Relationship to 2-ranks of class groups. We use the following notation:

- I_K, the group of fractional ideals of K;
- $P_K \leq I_K$, the subgroup of principal fractional ideals of K;
- $C_K = I_K/P_K$, the class group of K;
- $P_K^+ \leq P_K$, the subgroup of principal fractional ideals generated by $\alpha \in K^{*+}$; and

- $C_K^+ = I_K/P_K^+$, the narrow (or strict) class group of K.

The fundamental exact sequence relating the usual and the narrow class groups is

$$0 \to P_K/P_K^+ \to C_K^+ \to C_K \to 0. \tag{2.6}$$

The natural map $\alpha \mapsto (\alpha)$ for elements $\alpha \in K^*$ gives an exact sequence

$$1 \to E_K \to K^* \to P_K \to 1,$$

and the image of the subgroup K^{*+} of totally positive elements in P_K is, by definition, P_K^+. This gives the isomorphism

$$P_K/P_K^+ \simeq K^*/E_K K^{*+}, \tag{2.7}$$

so (2.6) may be written

$$0 \to K^*/E_K K^{*+} \to C_K^+ \to C_K \to 0. \tag{2.8}$$

The image of the units E_K under the archimedean signature map $\operatorname{sgn}_\infty$ has full preimage $E_K K^{*+}$, so (2.8) may also be written

$$0 \to \{\pm 1\}^{r_1}/\operatorname{sgn}_\infty(E_K) \to C_K^+ \to C_K \to 0. \tag{2.9}$$

The map on the left is induced by mapping an r_1-tuple of signatures in $\{\pm 1\}^{r_1}$ to the principal ideal (α), where α is any element in K^* with the given signatures.

Definition 2.10. For the groups in the exact sequence (2.8), we define

$$\begin{aligned} \rho &= \operatorname{rk}_2 C_K, \\ \rho^+ &= \operatorname{rk}_2 C_K^+, \\ \rho_\infty &= \operatorname{rk}_2 K^*/E_K K^{*+}. \end{aligned} \tag{2.11}$$

By the Dirichlet unit theorem we have $\operatorname{rk}_2(E_K) = \dim(E_K/E_K^2) = r_1 + r_2$, and by the surjectivity of $\operatorname{sgn}_\infty$ we have $\operatorname{rk}_2(K^*/K^{*+}) = r_1$. Let $E_K^+ = E_K \cap K^{*+}$ denote the group of totally positive units of K. The following diagram is commutative, with exact rows and columns:

$$\begin{array}{ccccc} & & K^* & \longrightarrow & P_K \\ & & \uparrow & & \uparrow \\ E_K & \longrightarrow & E_K K^{*+} & \longrightarrow & P_K^+ \\ \uparrow & & \uparrow & & \\ E_K^+ & \longrightarrow & K^{*+} & & \\ \uparrow & & & & \\ E_K^2 & & & & \end{array} \quad .$$

The row maps in the upper square induce the isomorphism $K^*/E_K K^{*+} \simeq P_K/P_K^+$ in (2.7), and the row maps in the lower square induce the evident isomorphism $E_K/E_K^+ = E_K/(E_K \cap K^{*+}) \simeq E_K K^{*+}/K^{*+}$. Since E_K/E_K^2 and K^*/K^{*+} are elementary abelian 2-groups, these isomorphisms together with the diagram above give various rank relations which we record in the following lemma.

Lemma 2.12. *With notation as above, we have the following rank relations:*

$$\begin{aligned} \mathrm{rk}_2(K^*/E_K K^{*+}) &= \mathrm{rk}_2(P_K/P_K^+) = \rho_\infty, \\ \mathrm{rk}_2(E_K K^{*+}/K^{*+}) &= \mathrm{rk}_2(E_K/E_K^+) = r_1 - \rho_\infty, \\ \mathrm{rk}_2(E_K^+/E_K^2) &= r_2 + \rho_\infty, \ \textit{and} \\ \mathrm{sgnrk}(E_K) &= r_1 - \rho_\infty. \end{aligned} \tag{2.13}$$

Finally, since $P_K/P_K^+ \simeq K^*/E_K K^{*+}$ is an elementary abelian 2-group, from (2.8) it follows that $\rho^+ - \rho$ is the rank of the largest subgroup of P_K/P_K^+ that is a direct summand of C_K^+. We record the following consequence.

Lemma 2.14. *We have $\rho^+ = \rho + \rho_\infty$ if and only if the exact sequence in (2.9) splits.*

3. The 2-Selmer group of a number field

In this section, we investigate a subgroup Z of elements of K^* classically referred to as "singular elements", and their classes modulo squares. As an application we give an unpublished proof due to Hayes of the Armitage–Fröhlich theorem.

Definition 3.1. An element $z \in K^*$ is called a singular element if the principal ideal generated by z is a square, i.e., $(z) = \mathfrak{a}^2$ for some fractional ideal $\mathfrak{a} \in I_K$.

Let Z denote the multiplicative group of all singular elements of K. Since every element in K^{*2} is singular, $Z \supseteq K^{*2}$.

Definition 3.2. The 2-Selmer group of K is $\mathrm{Sel}_2(K) = Z/K^{*2}$.

Remark 3.3. As noted by Lemmermeyer [Le], nonzero field elements whose principal ideals are squares arose in a number of classical problems in algebraic number theory, often involving reciprocity laws. The nomenclature referring to the collection of such elements mod squares as the 2-Selmer group was introduced by Cohen in [Co2] by analogy with the Selmer groups for elliptic curves. We shall use the over-used qualifier *singular* sparingly.

The group $\mathrm{Sel}_2(K)$ is a finite elementary abelian 2-group whose rank can be computed as follows. If $z \in Z$, then $(z) = \mathfrak{a}^2$ for a unique $\mathfrak{a}$, so we have a well-defined homomorphism

$$\begin{aligned} Z &\to C_K \\ z &\mapsto [\mathfrak{a}]; \end{aligned} \tag{3.4}$$

this map surjects onto the subgroup $C_K[2]$ and has kernel $E_K K^{*2}$, giving the isomorphism

$$Z/E_K K^{*2} \simeq C_K[2].$$

Since $E_K K^{*2}/K^{*2} \simeq E_K/E_K^2$ has rank $r_1 + r_2$, and $C_K[2]$ has rank ρ, it follows that the elementary abelian 2-group $\mathrm{Sel}_2(K) = Z/K^{*2}$ has rank

$$\mathrm{rk}_2 \mathrm{Sel}_2(K) = \rho + r_1 + r_2. \tag{3.5}$$

Totally positive singular elements. Let $Z^+ = Z \cap K^{*+} \leq Z$ denote the subgroup of totally positive elements of Z. Then for $z \in Z^+$, the ideal $\mathfrak{a}$ with $(z) = \mathfrak{a}^2$ defines a class of order 2 in the narrow class group C_K^+, and the map $z \mapsto [\mathfrak{a}]$ gives a surjective homomorphism from Z^+ to $C_K^+[2]$. The kernel of this homomorphism is the set of $z \in Z^+$ with $(z) = (\beta)^2$ where $\beta \in K^{*+}$ is totally positive. Then $z = \varepsilon\beta^2$ where ε is a unit, necessarily totally positive, i.e., $\varepsilon \in E_K^+$. This gives the isomorphism

$$Z^+/E_K^+(K^{*+})^2 \simeq C_K^+[2].$$

Under this isomorphism, the image of the subgroup $E_K^+K^{*2}/E_K^+(K^{*+})^2$ consists of those classes $[\mathfrak{a}]$ (of order 2) in C_K^+ represented by an ideal $\mathfrak{a}$ with $\mathfrak{a}^2 = (\varepsilon\alpha^2)$ for some $\varepsilon \in E_K^+$ and $\alpha \in K^*$, i.e., $\mathfrak{a} = (\alpha)$ is a principal ideal. Hence

$$Z^+/E_K^+K^{*2} \simeq C_K^+[2]/(P_K/P_K^+).$$

(Note this is the image of $C_K^+[2]$ in $C_K[2]$ under the natural projection in (2.6).) Since $C_K^+[2]$ is an elementary abelian 2-group of rank ρ^+ and P_K/P_K^+ has rank ρ_∞, this gives

$$\mathrm{rk}_2(Z^+/E_K^+K^{*2}) = \rho^+ - \rho_\infty. \tag{3.6}$$

We have $E_K^+K^{*2}/K^{*2} = E_K^+/(E_K^+ \cap K^{*2}) = E_K^+/E_K^2$, whose rank was computed to be $r_2 + \rho_\infty$ in (2.13). Again, since Z^+/K^{*2} is an elementary abelian 2-group, together these give

$$\mathrm{rk}_2(Z^+/K^{*2}) = \rho^+ + r_2. \tag{3.7}$$

The Armitage–Fröhlich theorem. Let H be the Hilbert class field of K and H^+ the narrow Hilbert class field of K. Then we have $C_K \simeq \mathrm{Gal}(H/K)$ and $C_K^+ \simeq \mathrm{Gal}(H^+/K)$, so (2.6) gives

$$\begin{aligned} \mathrm{rk}_2 \mathrm{Gal}(H/K) &= \rho \\ \mathrm{rk}_2 \mathrm{Gal}(H^+/K) &= \rho^+ \\ \mathrm{rk}_2 \mathrm{Gal}(H^+/H) &= \rho_\infty. \end{aligned} \tag{3.8}$$

Let Q denote the compositum of all quadratic subfields of H (i.e., the compositum of all unramified quadratic extensions of K) and let Q^+ be the compositum of all the quadratic subfields of H^+ (i.e., the compositum of all quadratic extensions of K unramified at finite primes). Then in particular the rank relations (3.8) show

$$\begin{aligned} [Q^+ : K] &= 2^{\rho^+} \\ [Q : K] &= 2^{\rho}. \end{aligned} \tag{3.9}$$

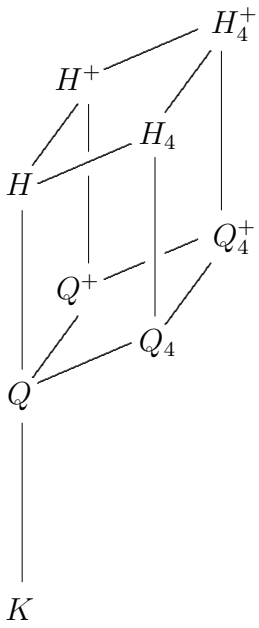
We can also relate Z and Z^+ to class fields and their 2-ranks as a result of the following lemma, the source of interest for these elements classically. Let H_4 denote the ray class field of K of conductor (4) and let H_4^+ denote the ray class field of K of conductor $(4)\infty$, where ∞ denotes the product of all the real infinite places of K.

Lemma 3.10. *Let $z \in K^*$. Then $K(\sqrt{z}) \subseteq H_4^+$ if and only if $z \in Z$, and $K(\sqrt{z}) \subseteq H_4$ if and only if $z \in Z^+$.*

Proof. The first statement of the lemma follows from the conductor-discriminant theorem and the explicit description of the ring of integers in local quadratic extensions (see e.g. Narkiewicz [N, Theorem 5.6, Corollary 5.6]). The second statement follows as a consequence: a subfield, $K(\sqrt{z})$, of H_4^+ is also contained in H_4 if and only if $K(\sqrt{z})$ is unramified over K at all real places, so if and only if z is also totally positive, i.e., $z \in Z^+$. □

Let Q_4^+ be the compositum of the quadratic extensions of K in H_4^+, i.e., the composite of the quadratic extensions of K of conductor dividing $(4)\infty$. Similarly, let $Q_4 \subseteq H_4$ be the compositum of the quadratic extensions of K in H_4, i.e., the composite of the quadratic extensions of K of conductor dividing (4). By the lemma, the elements of Z^+ give the Kummer generators for Q_4 (respectively, the elements of Z give the Kummer generators for Q_4^+); by Kummer theory, equation (3.5) (respectively, (3.7)) gives

$$\begin{aligned} [Q_4^+ : K] &= 2^{\rho+r_1+r_2} \\ [Q_4 : K] &= 2^{\rho^+ + r_2} \ . \end{aligned} \tag{3.11}$$



Combined with (3.9) this gives the degrees:

$$\begin{aligned} [Q_4^+ \colon Q] &= 2^{r_1+r_2} \\ [Q^+ \colon Q] &= 2^{\rho^+ - \rho} \\ [Q_4 \colon Q] &= 2^{\rho^+ + r_2 - \rho} \ . \end{aligned}$$

The fields Q^+ and Q_4 are Galois over Q, with intersection Q, so

$$[Q^+Q_4 \colon Q] = [Q^+ \colon Q][Q_4 \colon Q] = 2^{2\rho^+ - 2\rho + r_2}.$$

Since $Q^+Q_4 \subseteq Q_4^+$, this shows

$$r_1 + r_2 \geq 2\rho^+ - 2\rho + r_2,$$

i.e., $\rho^+ - \rho \leq r_1/2$, a result due to Armitage–Fröhlich [A-F].

Theorem 3.12 (Armitage–Fröhlich)**.** *If ρ (respectively, ρ^+) is the 2-rank of the class group (respectively, narrow class group) of the number field K then*

$$\rho^+ - \rho \leq \lfloor r_1/2 \rfloor,$$

where r_1 is the number of real places of K.

By the exact sequence (2.6), we have $\rho^+ \geq \rho_\infty$, so one consequence is the following corollary, also due to Armitage–Fröhlich.

Corollary 3.13. *We have*

$$\rho \geq \rho_\infty - \lfloor r_1/2 \rfloor = \lceil r_1/2 \rceil - \operatorname{sgnrk}(E_K) = \operatorname{rk}_2(E_K^+/E_K^2) - \lfloor n/2 \rfloor. \tag{3.14}$$

Remark 3.15. Armitage–Fröhlich [A-F] proved, but did not explicitly state, the stronger result $\rho^+ - \rho \leq \lfloor r_1/2 \rfloor$ (Theorem 3.12), explicitly stating only $\rho_\infty - \rho \leq \lfloor r_1/2 \rfloor$ (Corollary 3.13). However, equations (3) and (4) of their paper show that (in their notation)

$$\dim_2(X_2) - \dim_2(\operatorname{Ker}(\rho \cap X_2)) = \dim_2(\rho(X_2)) \leq \lfloor r_1/2 \rfloor$$

which is equivalent to $\rho^+ - \rho \leq \lfloor r_1/2 \rfloor$. The stronger result has occasionally been misattributed as due first to Oriat [O], who provided a different proof of the result.

Remark 3.16. The elegant proof of the Armitage–Fröhlich Theorem presented above is an unpublished proof due to D. Hayes [H]. In section 5 we provide a proof, due to Hayes and Greither-Hayes, which shows the contribution to the class number on the right hand side of (3.14) in Corollary 3.13 is provided by unramified quadratic extensions generated by units (cf. Proposition 6.3).

4. The 2-adic and the 2-Selmer signature maps

In this section, in addition to keeping track of the signs of elements at the real places as in section 2, we also keep track of "2-adic signs".

The 2-adic signature map. Let $\mathcal{O}_{K,2} = \mathcal{O}_K \otimes \mathbb{Z}_2$.

Definition 4.1. The 2-adic signature space of K is

$$V_2 = \mathcal{O}_{K,2}^*/(1+4\mathcal{O}_{K,2})\mathcal{O}_{K,2}^{*2}. \tag{4.2}$$

We say that a finite place v of K is even if it corresponds to a prime dividing (2). Let K_v denote the completion of K at a place v and let $\mathcal{O}_{K,v} \subseteq K_v$ be its valuation ring. Then $\mathcal{O}_{K,2} \simeq \prod_{v \text{ even}} \mathcal{O}_{K,v}$. Let $U_v = \mathcal{O}_v^*$ denote the group of local units in $\mathcal{O}_v$. Then as abelian groups, we have

$$V_2 \simeq \prod_{v|(2)} U_v/(1+4\mathcal{O}_v)U_v^2. \tag{4.3}$$

The idea that signatures of units are related to congruences modulo 4 goes back (at least) to Lagarias [La], and the space V_2 appears explicitly in Hagenmüller [Ha1, Ha2], where one can also find the following proposition.

Proposition 4.4. *The 2-adic signature space V_2 is an elementary abelian 2-group of rank $n = [K:\mathbb{Q}]$.*

Proof. The local factor $U_v/(1+4\mathcal{O}_v)U_v^2$ is the quotient modulo squares of $U_v/(1+4\mathcal{O}_v)$, so is an abelian group of exponent 2, and its rank is the same as the rank of the subgroup $U_v/(1+4\mathcal{O}_v)[2]$ of elements of order dividing 2 in this group. If $u \in U_v$ has $u^2 = 1+4t$ with $t \in \mathcal{O}_v$, then $a = (u-1)/2$ satisfies $a^2 + a - t = 0$, so $a \in \mathcal{O}_v$ and $u = 1+2a$. An easy check shows the map $u \mapsto a$ defines a group isomorphism $U_v/(1+4\mathcal{O}_v)[2] \xrightarrow{\sim} \mathcal{O}_v/2\mathcal{O}_v$, an elementary abelian 2-group of rank equal to the local degree $[K_v:\mathbb{Q}_v]$, from which the proposition follows. □

As in the case of the archimedean signature map, we shall often view $V_2 \simeq \mathbb{F}_2^n$ as a vector space over $\mathbb{F}_2$, written additively.

Let

$$\mathcal{O}_{K,(2)}^* = \{\alpha \in K : v(\alpha) = 0 \text{ for } v \text{ even}\} \tag{4.5}$$

be the units in the localization of $\mathcal{O}_K$ at the set of even primes.

The inclusion $\mathcal{O}_{K,(2)}^* \hookrightarrow \mathcal{O}_{K,2}^*$ followed by the natural projection induces a homomorphism from $\mathcal{O}_{K,2}^*$ to V_2. We can use this homomorphism and the following lemma to define a homomorphism from the group Z of singular elements to the 2-adic signature space V_2.

Lemma 4.6. *Every $\alpha \in Z$ can be written $\alpha = \alpha'\beta^2$ with $\beta \in K^*$ and $\alpha' \in \mathcal{O}_{K,(2)}^*$. The element α' is unique up to $\mathcal{O}_{K,(2)}^{*2}$.*

Proof. If $\alpha \in Z$, then the valuation of α at any finite prime is even; by weak approximation, we can write $\alpha = \alpha'\beta^2$ with $\alpha', \beta \in K^*$ with $\alpha' \in Z$ relatively prime to (2) (i.e., $\alpha' \in U_v$ for all even places v). If also $\alpha = \alpha''\gamma^2$ with $\alpha'', \gamma \in K^*$, and α'' relatively prime to (2), then $(\beta/\gamma)^2 = \alpha'/\alpha''$ shows $\beta/\gamma \in \mathcal{O}_{K,(2)}^*$. Finally, $\alpha'' = \alpha'(\beta/\gamma)^2$ shows $\alpha''\mathcal{O}_{K,(2)}^{*2} = \alpha'\mathcal{O}_{K,(2)}^{*2}$. □

Definition 4.7. The 2-adic signature map is the homomorphism

$$\begin{aligned} \mathrm{sgn}_2 : Z &\to V_2 \\ \alpha &\mapsto \alpha' \end{aligned}$$

given by mapping $z = \alpha'\beta^2$ as in Lemma 4.6 to the image of $\alpha' \in \mathcal{O}^*_{K,(2)}$ in V_2.

Since α' in Lemma 4.6 is unique up to $\mathcal{O}^{*2}_{K,(2)}$, the image of α' in V_2 does not depend on the choice of α', so the 2-adic signature map is well-defined.

By weak approximation, the 2-adic signature map sgn_2 is surjective.

Kernel of the 2-adic signature map. By construction, $\ker \mathrm{sgn}_2$ is the subgroup of Z consisting of the elements congruent to a square modulo 4. An alternate characterization of the elements in $\ker \mathrm{sgn}_2$ comes from the following classical result.

Proposition 4.8. *Let $\alpha_v \in U_v$. Then $K_v(\sqrt{\alpha_v})$ is unramified over K_v if and only if α_v is congruent to a square modulo 4.*

If $z \in Z$ then $\mathrm{sgn}_2(z) = 0$ (viewing V_2 additively) if and only if $K(\sqrt{z})$ is unramified over K at all even primes.

Proof. As in Lemma 3.10, the first statement follows from the formula for the discriminant of a local quadratic extension. For $z \in Z$, $K(\sqrt{z}) = K(\sqrt{\alpha'})$ where $\alpha' \in \mathcal{O}^*_{K,(2)}$ as in Lemma 4.6, so the second statement follows from the first together with the definition of sgn_2. □

In particular, we have the following result determining when the image of -1 is trivial under the 2-adic signature map, showing it conveys arithmetic information about the field K. (The image of -1 under the archimedean signature map being both obvious and never trivial.)

Corollary 4.9. *We have $\mathrm{sgn}_2(-1) = 0$ if and only if $K(\sqrt{-1})$ is unramified at all finite primes of K.*

Proof. The extension $K(\sqrt{-1})$ is automatically unramified at finite primes not dividing (2), so the result follows immediately from the Lemma. □

Corollary 4.10. *If K is a field of odd degree over $\mathbb{Q}$, then $\mathrm{sgn}_2(-1) \neq 0$.*

Proof. Since $n = [K : \mathbb{Q}]$ is odd, at least one of the local field degrees $[K_v : \mathbb{Q}_2]$ for some v dividing (2) must be odd. Since $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$ is ramified it follows that $K_v(\sqrt{-1})$ is a ramified quadratic extension of K_v for this v, so $\mathrm{sgn}_2(-1) \neq 0$ by the Lemma. □

The 2-Selmer signature map. Combining the archimedean and 2-adic signature maps, noting that K^{*2} is in the kernel of both maps, we may define one of the fundamental objects of this paper:

Definition 4.11. The 2-Selmer signature map of K is the map

$$\begin{aligned} \varphi : \mathrm{Sel}_2(K) &\to V_\infty \oplus V_2 \\ \alpha K^{*2} &\mapsto (\mathrm{sgn}_\infty(\alpha), \mathrm{sgn}_2(\alpha)) \end{aligned}$$

for any representative $\alpha \in Z$. Write φ_∞ for the homomorphism sgn_∞, viewed as having image in V_∞ identified as a subgroup of $V_\infty \oplus V_2$, and similarly for φ_2.

The groups $\mathrm{Sel}_2(K)$, V_∞, and V_2 are all multiplicative elementary abelian 2-groups, written additively when viewed as vector spaces over $\mathbb{F}_2$; as $\mathbb{F}_2$-vector spaces, by (3.5), (2.1), and (4.2) we have

$$\begin{aligned} \dim \mathrm{Sel}_2(K) &= \rho + r_1 + r_2, \\ \dim V_\infty &= r_1, \text{ and} \\ \dim V_2 &= n. \end{aligned} \tag{4.12}$$

By Kummer theory, subgroups of K^*/K^{*2} correspond to composita of quadratic extensions of K, and Lemmas 3.10 and 4.8 identify those corresponding to several subgroups related to the 2-Selmer signature map, whose ranks were computed in Section 3. We summarize the results in the following proposition.

Proposition 4.13. *With notation as above, we have the following correspondences of Kummer generators and extensions of K:*

(a) $\mathrm{Sel}_2(K) = Z/K^{*2} \simeq \mathrm{Gal}(Q_4^+/K)$, *where Q_4^+ is the compositum of all quadratic extensions of K of conductor dividing $(4)\infty$;*
(b) $\ker \varphi_\infty = Z^+/K^{*2} \simeq \mathrm{Gal}(Q_4/K)$, *where Q_4 is the compositum of all quadratic extensions of K of conductor dividing (4);*
(c) $\ker \varphi_2 \simeq \mathrm{Gal}(Q^+/K)$, *where Q^+ is the compositum of all quadratic extensions in the narrow Hilbert class field of K; and*
(d) $\ker \varphi \simeq \mathrm{Gal}(Q/K)$, *where Q is the compositum of all quadratic extensions in the Hilbert class field of K.*

In particular,

$$\begin{aligned} \mathrm{rk}_2 \mathrm{Sel}_2(K) &= \rho + r_1 + r_2, \\ \mathrm{rk}_2 \ker \varphi_\infty &= \rho^+ + r_2, \\ \mathrm{rk}_2 \ker \varphi_2 &= \rho^+, \text{ and} \\ \mathrm{rk}_2 \ker \varphi &= \rho. \end{aligned} \tag{4.14}$$

We consider the image of the 2-Selmer signature map φ in Section 6.

5. Nondegenerate symmetric space structures

In this section we show that both the archimedean and 2-adic signature spaces V_∞ and V_2 carry the structure of a finite-dimensional nondegenerate symmetric space over $\mathbb{F}_2$.

The quadratic Hilbert (norm residue) symbol $(\alpha_v, \beta_v)_v$ defines a symmetric nondegenerate pairing on K_v^*/K_v^{*2} for each place v, satisfying $(\alpha_v, \beta_v)_v = +1$ if and only if β_v is a norm from $K_v(\sqrt{\alpha_v})$. In particular, for archimedean v, the symbol is $+1$ unless $K_v \simeq \mathbb{R}$ and both α_v and β_v are negative, in which case the symbol is -1

Suppose that v is an even place of K. If $\alpha_v \in 1 + 4\mathcal{O}_v \subset K_v^*$ then by Lemma 4.8 the field $K_v(\sqrt{\alpha_v})$ is unramified over K_v (possibly equal to K_v if α_v is a square). By class field theory, every unit is a norm from such an unramified abelian extension, so $(\alpha_v, \beta_v)_v = 1$ for every $\beta_v \in U_v$. It follows that the Hilbert symbol induces a symmetric pairing of the quotient $U_v/(1+4\mathcal{O}_v)U_v^2$ with itself, which we again denote simply by $(\alpha_v, \beta_v)_v$. This induced pairing is also nondegenerate: if $\alpha_v \in U_v$ satisfies $(\alpha_v, \beta_v)_v = 1$ for every $\beta_v \in U_v$, then every unit in K_v is a norm from $K_v(\sqrt{\alpha_v})$, which again by class field theory implies $K_v(\sqrt{\alpha_v})/K_v$ is unramified, so α_v is a square modulo 4 (i.e., is trivial in $U_v/(1 + 4\mathcal{O}_v)U_v^2$) by Lemma 4.8.

Taking the product of the Hilbert symbols on K_v^*/K_v^{*2} for the real places and on $U_v/(1+4\mathcal{O}_v)U_v^2$ for the even places then gives nondegenerate symmetric pairings on V_∞ and V_2:

$$\begin{aligned} b_\infty : V_\infty \oplus V_\infty \to \{\pm 1\} \qquad & \text{and} \quad b_2 : V_2 \oplus V_2 \to \{\pm 1\} \\ b_\infty(\alpha,\beta) = \prod_{v \text{ real}} (\alpha_v, \beta_v)_v, \qquad & b_2(\alpha,\beta) = \prod_{v \text{ even}} (\alpha_v, \beta_v)_v. \end{aligned} \tag{5.1}$$

Viewing V_∞ and V_2 as $\mathbb{F}_2$-vector spaces and writing the pairings b_∞ and b_2 additively, both V_∞ and V_2 have the structure of a finite dimensional $\mathbb{F}_2$-vector space equipped with a nondegenerate symmetric bilinear form.

Proposition A.1 in the Appendix classifies the three possible nondegenerate finite dimensional symmetric spaces over $\mathbb{F}_2$ up to isometry: (1) alternating of even dimension, (2) nonalternating of odd dimension, and (3) nonalternating of even dimension. For nonalternating spaces, there is a canonical nonzero element v_{can}: the unique nonisotropic element orthogonal to the alternating subspace when n is odd and the unique nonzero vector in the radical of the alternating subspace when n is even; in both cases v_{can} is the sum of all the elements in any orthonormal basis.

The following proposition determines the isometry type for V_∞ and for V_2.

Proposition 5.2. *If the archimedean signature space V_∞ is equipped with the bilinear form b_∞ and the 2-adic signature space V_2 is equipped with the bilinear form b_2 then the following statements hold:*

(a) *V_∞ is a nondegenerate nonalternating symmetric space over $\mathbb{F}_2$ of dimension r_1 with $\operatorname{sgn}_\infty(-1) = v_{\text{can}} \in V_\infty$.*
(b) *V_2 is a nondegenerate symmetric space over $\mathbb{F}_2$ of dimension n. More precisely,*
  (i) *if $K(\sqrt{-1})$ is ramified over K at some even prime, then V_2 is nonalternating, and $\operatorname{sgn}_2(-1) = v_{\text{can}} \in V_2$, and*
  (ii) *if $K(\sqrt{-1})$ is unramified over K at all finite primes, then V_2 is alternating (so n is even), and $\operatorname{sgn}_2(-1) = 0$.*

Proof. The element $\alpha = (-1, 1, \ldots, 1)$ (written multiplicatively) in V_∞ has $b_\infty(\alpha,\alpha) = -1$, so V_∞ is nonalternating. An element $(\alpha_v)_v$ in V_∞ is isotropic with respect to b_∞ if and only if the number of α_v that are negative is even, and in that case the element is orthogonal to $\operatorname{sgn}_\infty(-1)$. It follows that $\operatorname{sgn}_\infty(-1)$ satisfies the characterizing property of v_{can} both when n is odd and when n is even, proving (a).

For the space V_2, note first that the Hilbert symbol always satisfies $(\alpha_v, -\alpha_v) = 1$ (multiplicatively), hence $(\alpha_v, \alpha_v) = 1$ for all α_v if and only if $(\alpha_v, -1) = 1$ for all α_v. Since the pairing on $U_v/(1+4\mathcal{O}_v)U_v^2$ is nondegenerate, this happens if and only if $-1 \in (1+4\mathcal{O}_v)U_v^2$. Hence $b_2(\alpha,\alpha) = 0$ (additively) for all α if and only if $-1 \in (1+4\mathcal{O}_v)U_v^2$ for every even prime v. In other words, b_2 is alternating if and only if $\operatorname{sgn}_2(-1) = 0$ (additively in $\mathbb{F}_2^n \simeq V_2$), which is equivalent to the statement that $K(\sqrt{-1})$ is unramified over K at all finite primes by Corollary 4.9.

Suppose now that $\operatorname{sgn}_2(-1) \neq 0$, i.e., that V_2 is not alternating. By the product formula for the Hilbert norm residue symbol we have

$$\prod_{v \text{ real}} (-1,-1)_v \prod_{v \text{ even}} (-1,-1)_v \prod_{v \text{ odd}} (-1,-1)_v = 1.$$

For odd primes v, $K_v(\sqrt{-1})$ is unramified over K_v, so -1 is a norm, hence $(-1,-1)_v = 1$ for these primes. If v is a real archimedean place, $(-1,-1)_v = -1$. Hence

$$b_2(\mathrm{sgn}_2(-1), \mathrm{sgn}_2(-1)) = \prod_{v \text{ even}} (-1,-1)_v = (-1)^{r_1} = (-1)^n$$

since $n = r_1 + 2r_2$. It follows that $\mathrm{sgn}_2(-1)$ is isotropic with respect to b_2 if n is even and is nonisotropic if n is odd.

As noted above, the norm residue symbol satisfies $1 = (\alpha_v, -\alpha_v)_v = (\alpha_v, \alpha_v)_v(\alpha_v, -1)_v$ for all α_v. Hence $\mathrm{sgn}_2(-1)$ is orthogonal to every isotropic element of V_2, i.e., is orthogonal to the alternating subspace of V_2. It follows that $\mathrm{sgn}_2(-1)$ satisfies the characterizing property of v_{can} whether n is odd or even, completing the proof. □

All three possible types of nondegenerate space over $\mathbb{F}_2$ in the proposition arise for number fields, in fact all three can occur as a V_2. For any odd degree field K, the space V_2 is necessarily nonalternating of odd dimension. For even degree, we can see both possibilities already in the case $n = 2$ of quadratic fields, as follows. Suppose $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field of discriminant D. By the proposition, V_2 is alternating if and only if $K(\sqrt{-1})$ is unramified over K at all finite primes, which happens if and only if 2 ramifies in K but does not totally ramify in $K(\sqrt{-1})$, i.e., if and only if $D \equiv 4 \pmod 8$.

Remark 5.3. We note the special role played by -1, the generating root of unity in E_K: its image in the symmetric spaces V_∞ and V_2 gives the nonzero canonical element of the space (when there is one) as in Proposition A.1. This is in keeping with the philosophy of Malle [M2] that the second roots of unity should play a role in determining whether 2 is a "good" prime in Cohen-Lenstra type heuristics.

6. The image of the 2-Selmer signature map

Since the form b_∞ is nondegenerate on V_∞ and b_2 is nondegenerate on V_2, the form $b_\infty \perp b_2$ defines a nondegenerate symmetric bilinear form on the orthogonal direct sum of V_∞ and V_2. To emphasize this symmetric space structure on the target space for the 2-Selmer signature map, from now on we write $V_\infty \oplus V_2$ as $V_\infty \perp V_2$.

The following theorem is foundational.

Theorem 6.1. *The image of the* 2*-Selmer signature map*

$$\varphi : \mathrm{Sel}_2(K) \to V = V_\infty \perp V_2$$

is a maximal totally isotropic subspace of $V_\infty \perp V_2$ *and* $\dim(\mathrm{im}\,\varphi \cap V_\infty) = \rho^+ - \rho$.

Proof. If $\alpha, \beta \in Z$ then, by the product formula for the Hilbert norm residue symbol,

$$\prod_{v \text{ real}} (\alpha,\beta)_v \prod_{v \text{ even}} (\alpha,\beta)_v \prod_{v \text{ odd}} (\alpha,\beta)_v = 1.$$

Since the principal ideals generated by the singular elements α, β are squares, locally at all finite primes these elements differ from a square by a unit. Then for all odd finite places v, the field $K_v(\sqrt{\alpha_v})$ is an unramified extension of K_v (possibly trivial), so every unit is a norm. Since β_v differs from a unit by a square, also β_v is a norm, so $(\alpha,\beta)_v = 1$. Therefore

$$\prod_{v \text{ real}} (\alpha,\beta)_v \prod_{v \text{ even}} (\alpha,\beta)_v = 1,$$

which when written additively for the bilinear forms b_∞ and b_2 gives

$$b(\varphi(\alpha),\varphi(\beta)) = b_\infty(\mathrm{sgn}_\infty(\alpha),\mathrm{sgn}_\infty(\beta)) + b_2(\mathrm{sgn}_2(\alpha),\mathrm{sgn}_2(\beta)) = 0.$$

Thus $\varphi(\alpha)$ and $\varphi(\beta)$ are orthogonal with respect to $b = b_\infty \perp b_2$, so $\varphi(\mathrm{Sel}_2(K))$ is a totally isotropic subspace of $V_\infty \perp V_2$.

The dimension of $V_\infty \perp V_2$ is $r_1 + n$. By Proposition 4.13, the dimension of $\mathrm{Sel}_2(K)$ is $\rho + r_1 + r_2$ and the dimension of $\ker\varphi$ is ρ, so $\mathrm{im}\,\varphi$ has dimension $r_1 + r_2 = (r_1+n)/2$, hence $\varphi(\mathrm{Sel}_2(K))$ is a maximal totally isotropic subspace.

Finally, $\mathrm{im}\,\varphi \cap V_\infty$ is $\varphi(\ker\varphi_2)$, hence has dimension $\dim(\ker\varphi_2) - \dim(\ker\varphi) = \rho^+ - \rho$ by (4.14). □

As a corollary of Theorem 6.1, we have a second proof of the theorem of Armitage–Fröhlich (Theorem 3.12).

Corollary 6.2 (The Armitage–Fröhlich Theorem)**.** *We have*

$$\rho^+ - \rho \le \lfloor r_1/2 \rfloor.$$

Proof. Since the image $\varphi(\mathrm{Sel}_2(K))$ is totally isotropic, the image under φ_∞ of the elements in $\ker\varphi_2$ is a totally isotropic subspace of V_∞ with respect to b_∞. As a result, $\varphi_\infty(\ker\varphi_2)$ has dimension at most $\lfloor r_1/2 \rfloor$. The computations in section 3 show the dimension of $\ker\varphi_2$ is ρ^+ and the kernel of φ_∞ on $\ker\varphi_2$ is $\ker\varphi_\infty \cap \ker\varphi_2 = \ker\varphi$, which has dimension ρ. This gives $\rho^+ - \rho \le \lfloor r_1/2 \rfloor$. □

As a second corollary of Theorem 6.1 we prove the following result of Hayes (unpublished) on "unramified quadratic extensions of unit type", namely, unramified quadratic extensions that are generated by square roots of units.

Corollary 6.3. *Let Q_u be the subfield of the Hilbert class field of K given by the compositum of all unramified quadratic extensions of the form $K(\sqrt{\varepsilon})$ for units $\varepsilon \in E_K$. Then*

$$\mathrm{rk}_2\,\mathrm{Gal}(Q_u/K) \ge \mathrm{rk}_2(E_K^+/E_K^2) - \lfloor n/2 \rfloor = \rho_\infty - \lfloor r_1/2 \rfloor.$$

In particular, $\rho \ge \rho_\infty - \lfloor r_1/2 \rfloor$.

Proof. Consider the restriction of φ_∞ and φ_2 to the subgroup $E_K K^{*2}/K^{*2}$ of $\mathrm{Sel}_2(K)$. Then, as before, since $\varphi(\mathrm{Sel}_2(K))$ is totally isotropic, the image under φ_2 of $\ker\varphi_\infty$ (restricted to $E_K K^{*2}/K^{*2}$) is a totally isotropic subspace of V_2 under b_2, hence has dimension at most $\lfloor n/2 \rfloor$. The kernel of φ_∞ on $E_K K^{*2}/K^{*2}$ is the subgroup $E_K^+ K^{*2}/K^{*2}$ and the kernel of φ_2 on these elements is the subgroup $E_{K,4}^+ K^{*2}/K^{*2}$ where $E_{K,4}^+$ are the totally positive units of K that are locally squares mod 4 at the primes above 2. This gives

$$\dim(E_K^+ K^{*2}/K^{*2}) - \dim(E_{K,4}^+ K^{*2}/K^{*2}) \le \lfloor n/2 \rfloor$$

i.e.,

$$\dim(E_K^+/E_K^2) - \dim(E_{K,4}^+/E_K^2) \le \lfloor n/2 \rfloor.$$

It follows from Proposition 4.8 that $\varepsilon \in E_{K,4}^+$ if and only if $K(\sqrt{\varepsilon})$ is an unramified quadratic extension of K. Two units in $E_{K,4}^+$ generate the same quadratic extension if and only if they differ by an element in E_K^2 (equivalently, $E_{K,4}^+ K^{*2}/K^{*2} \simeq E_{K,4}^+/E_K^2$). Hence $\mathrm{rk}_2\,\mathrm{Gal}(Q_u/K) = \dim(E_{K,4}^+ K^{*2}/K^{*2})$ which together with the previous inequality and equation (2.13) gives the first statement of the corollary. Since Q_u is a subfield of the Hilbert

class field of K, $\rho \geq \operatorname{rk}_2 \operatorname{Gal}(Q_u/K)$, which gives the final statement of the corollary and completes the proof. □

Remark 6.4. While essentially equivalent to the elegant proof of Hayes presented in section 3, the proof presented in Corollary 6.2 is perhaps more conceptual and 'explains' the $\lfloor r_1/2 \rfloor$ in the Armitage–Fröhlich Theorem: it is the maximum dimension of a totally isotropic subspace. This proof has its origins in a note by Serre at the end of the original 1967 Armitage–Fröhlich paper [A-F]—in the current notation that note amounts to the statement that $\varphi_\infty(\ker \varphi_2)$ is totally isotropic in V_∞. Serre's note provided an alternate proof of the critical step in the original Armitage–Fröhlich proof. Greither and Hayes in an unpublished paper in the notes of the Centre de Recherches Mathématiques from 1997, [G-H], were perhaps the first to also involve dyadic signatures. They explicitly noted what they termed a 'dual' statement to Serre's, namely that $\varphi_2(\ker \varphi_\infty)$ is totally isotropic in V_2. In the same paper Greither and Hayes note the work of Haggenmüller [Ha1] from 1981/82 providing quadratic extensions of unit type unramified outside finite primes (but possibly ramified at infinite places) and, as previously noted, Haggenmüller explictly uses the space V_2.

Remark 6.5. As remarked earlier, Armitage and Fröhlich [A-F] explicitly give only the inequality $\rho \geq \rho_\infty - \lfloor r_1/2 \rfloor$. In response to a question/conjecture of the current paper's first author (based on computer calculations for totally real cubic fields), Hayes [H] in 1997, and then Greither–Hayes [G-H] using the 'dual' statement noted above, proved Corollary 6.3, which shows that a subgroup of 2-rank at least $\rho_\infty - \lfloor r_1/2 \rfloor$, precisely the contribution to the class group guaranteed by the explicit theorem of Armitage and Fröhlich, is accounted for by totally unramified quadratic extensions of unit type. In fact there are independent elements of order 4 in the narrow Hilbert class group also accounting for a subgroup of this 2-rank in the class group [Du].

As noted in Remark 6.4, the spaces V_∞ and V_2 have, either implicitly or explicitly, been introduced in previous work. The advantage to the current approach, combining the two spaces V_∞ and V_2, is precisely that the image of the 2-Selmer signature map is a *maximal* totally isotropic subspace of $V_\infty \perp V_2$, and Theorem A.13 in the Appendix gives a structure theorem for such subspaces. This allows us to determine the possible images of the 2-Selmer signature map for K by applying the results in the Appendix to $W = V_\infty$ and $W' = V_2$ (so $\dim W = r_1$ and $\dim W' = n = r_1 + 2r_2$ have the same parity). By Proposition 5.2, the space $W = V_\infty$ is always nonalternating (with nonzero canonical element $\operatorname{sgn}_\infty(-1)$), and the same Proposition gives the conditions under which V_2 is one of three possible types. Then applying Corollary A.17 in cases (v), (iv), and (ii), respectively, and using the appropriate formulas in Proposition A.6 gives the following theorem.

Theorem 6.6. *Up to equivalence under the action of* $\operatorname{Aut}(V_\infty) \perp \operatorname{Aut}(V_2)$*, the following is a complete list of the maximal totally isotropic subspaces* S *of* $V_\infty \perp V_2$ *and the orders of their stabilizers,* $\operatorname{Aut}(S)$*, in* $\operatorname{Aut}(V_\infty) \perp \operatorname{Aut}(V_2)$*. Recall the notation* $(q)_m = \prod_{i=1}^{m}(1 - q^{-i})$*.*

(a) *If* n *is odd, then for each* k *with* $0 \leq k \leq \lfloor r_1/2 \rfloor$*, up to equivalence there is a unique maximal totally isotropic subspace* S_k *with* $\dim(S_k \cap V_\infty) = k$*, and*

$$\#\operatorname{Aut}(S_k) = 2^{(r_1+r_2-1)(r_1+r_2)/2+r_2^2+r_2k+k^2}(2)_k(2)_{k+r_2}(4)_{(r_1-1)/2-k} \ .$$

(b) *If* n *is even and* $K(\sqrt{-1})$ *is ramified over* K *at a finite place, then*

(i) *for each k with $0 \le k < r_1/2$, up to equivalence there is a unique maximal totally isotropic subspace $S_{k,1}$ such that $U = S_k \cap V_\infty$ has $\dim U = k$ and $\mathrm{sgn}_\infty(-1) \notin U$, and*

$$\#\mathrm{Aut}(S_{k,1}) = 2^{(r_1+r_2-1)(r_1+r_2)/2+r_2^2+r_2k+k^2}(2)_k(2)_{k+r_2}(4)_{r_1/2-1-k} \ ;$$

(ii) *for each k with $0 < k \le r_1/2$, up to equivalence there is a unique maximal totally isotropic subspace $S_{k,2}$ such that $U = S_k \cap V_\infty$ has $\dim U = k$ and $\mathrm{sgn}_\infty(-1) \in U$, and*

$$\#\mathrm{Aut}(S_{k,2}) = 2^{(r_1+r_2-1)(r_1+r_2)/2+r_2^2+r_2k+k^2+r_1-2k}(2)_{k-1}(2)_{k+r_2-1}(4)_{r_1/2-k} \ .$$

(c) *If n is even and $K(\sqrt{-1})$ is unramified over K at all finite places, then for each k with $0 < k \le r_1/2$, up to equivalence there is a unique maximal totally isotropic subspace S_k with $\dim(S_k \cap V_\infty) = k$, and*

$$\#\mathrm{Aut}(S_k) = 2^{(r_1+r_2-1)(r_1+r_2)/2+r_2^2+r_2k+k^2+r_1+r_2-k}(2)_{k-1}(2)_{k+r_2}(4)_{r_1/2-k} \ .$$

For brevity we state the following result for the case when n is odd since this is the case considered in the applications of the next section; the other two possible cases are very similar.

Theorem 6.7. *Suppose n is odd, and S_k for $0 \le k \le \lfloor r_1/2 \rfloor$ is as in (a) of Theorem 6.6. If S is chosen uniformly randomly from among the maximal totally isotropic subspaces of $V_\infty \perp V_2$, then the probability that S is isomorphic to S_k is*

$$\begin{aligned}\mathrm{Prob}(S \simeq S_k) &= \frac{1}{\#\mathrm{Aut}(S_k)} \Big/ \sum_{i=0}^{\lfloor r_1/2 \rfloor} \frac{1}{\#\mathrm{Aut}(S_i)} \\ &= \frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}}{2^{k(k+r_2)}(2)_k(2)_{k+r_2}(4)_{r_1+r_2-1}(4)_{(r_1-1)/2-k}} \ . \end{aligned} \tag{6.8}$$

Proof. This a restatement of the mass formula in the Appendix (cf. the discussion preceding Corollary A.22), as follows. The total number of maximal totally isotropic subspaces of $V_\infty \perp V_2$ equivalent to S_k is $\#\mathrm{Aut}(V_\infty)\#\mathrm{Aut}(V_2)/\#\mathrm{Aut}(S_k)$ and the total number of all maximal totally isotropic subspaces of $V_\infty \perp V_2$ is the sum of these for $0 \le k \le \lfloor r_1/2 \rfloor$. Then $\mathrm{Prob}(S \simeq S_k)$ is the quotient, which is the right hand side of the first equality in (6.8). Using the values computed in Corollary A.22 for these expressions gives the final equality of the theorem. □

Remark 6.9. The probability in Theorem 6.7 is, not surprisingly, the probability obtained following the Cohen–Lenstra heuristic of assigning a mass of $1/\#\,\mathrm{Aut}(S)$ to each equivalence type (under the action of $\mathrm{Aut}(V_\infty) \perp \mathrm{Aut}(V_2)$) of maximal totally isotropic subspace S.

Examples in low degree. We conclude this section by giving an explicit representative for each of the isometry classes of maximal totally isotropic subspaces S in Theorem 6.6 in the case when K is a totally real field, i.e., $r_2 = 0$, when $n = 2, 3, 4, 5$. Explicit representatives for fields with $r_2 > 0$ can be constructed similarly.

In each example, the spaces S are given by presenting an $n \times 2n$ matrix giving the $2n$ coordinates for n basis elements for S in terms of bases for $W = V_\infty$ and $W' = V_2$ chosen as in Remark A.3: an orthonormal basis for the nonalternating space V_∞ and for V_2 when

it is nonalternating, and a hyperbolic basis for V_2 when it is alternating (which can only occur if n is even). The procedure for finding a basis for S is the one described following Corollary A.22 at the end of the Appendix. Also listed is the order of the subgroup $\mathrm{Aut}(S)$ of isometries in $\mathrm{Aut}(V_\infty) \perp \mathrm{Aut}(V_2)$ that stabilize S.

Example 6.10. $n = 2$. There are two cases:

1. V_2 nonalternating ($K = \mathbb{Q}(\sqrt{D})$, $D > 0$, with discriminant $D \equiv 4 \pmod 8$). Then (orthonormal basis for V_∞ and for V_2)

$$k = 0: \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 2$$

$$k = 1: \quad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 4\ .$$

2. V_2 alternating ($K = \mathbb{Q}(\sqrt{D})$, $D > 0$, with discriminant $D \not\equiv 4 \pmod 8$). Then (orthonormal basis for V_∞ and hyperbolic basis for V_2)

$$k = 1: \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 4\ .$$

Example 6.11. $n = 3$. Then (orthonormal basis for V_∞ and for V_2)

$$k = 0: \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 6$$

$$k = 1: \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 4\ .$$

Example 6.12. $n = 4$. There are two cases:

1. V_2 nonalternating (K a totally real quartic field and $K(\sqrt{-1})$ is ramified over K at some finite (necessarily even) prime). Then (orthonormal basis for V_∞ and for V_2)

$$k = 0: \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 48$$

$$k=1:\quad \begin{pmatrix}1&1&1&1&1&1&1&1\\0&0&0&1&0&0&0&1\\0&0&0&0&1&1&0&0\\1&1&0&0&0&0&0&0\end{pmatrix}\qquad (w_{\mathrm{can}}\notin U,\ w'_{\mathrm{can}}\notin U')\qquad \#\mathrm{Aut}(S)=32$$

$$\begin{pmatrix}0&1&1&0&0&1&1&0\\1&1&0&0&1&1&0&0\\0&0&0&0&1&1&1&1\\1&1&1&1&0&0&0&0\end{pmatrix}\qquad (w_{\mathrm{can}}\in U,\ w'_{\mathrm{can}}\in U')\qquad \#\mathrm{Aut}(S)=384$$

$$k=2:\quad \begin{pmatrix}0&0&0&0&1&1&1&1\\0&0&0&0&1&1&0&0\\1&1&1&1&0&0&0&0\\1&1&0&0&0&0&0&0\end{pmatrix}\qquad \#\mathrm{Aut}(S)=256\ .$$

2. V_2 alternating (K a totally real quartic field and $K(\sqrt{-1})$ is unramified over K at all finite primes). Then (orthonormal basis for V_∞ and hyperbolic basis for V_2)

$$k=1:\quad \begin{pmatrix}1&1&0&0&1&0&0&0\\0&1&1&0&0&1&0&0\\0&0&0&0&0&0&1&0\\1&1&1&1&0&0&0&0\end{pmatrix}\qquad \#\mathrm{Aut}(S)=384$$

$$k=2:\quad \begin{pmatrix}0&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0\\1&1&0&0&0&0&0&0\\0&0&1&1&0&0&0&0\end{pmatrix}\qquad \#\mathrm{Aut}(S)=768\ .$$

Example 6.13. $n=5$. Then (orthonormal basis for V_∞ and for V_2)

$$k=0:\quad \begin{pmatrix}1&1&1&1&1&1&1&1&1&1\\0&0&0&1&1&0&0&0&1&1\\0&0&1&1&0&0&0&1&1&0\\0&1&1&1&1&0&1&1&1&1\\1&1&0&0&0&1&1&0&0&0\end{pmatrix}\qquad \#\mathrm{Aut}(S)=720$$

$$k=1:\quad \begin{pmatrix}1&1&1&1&1&1&1&1&1&1\\0&0&0&1&1&0&0&0&1&1\\0&0&1&1&0&0&0&1&1&0\\0&0&0&0&0&1&1&0&0&0\\1&1&0&0&0&0&0&0&0&0\end{pmatrix}\qquad \#\mathrm{Aut}(S)=384$$

$$k = 2: \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \#\mathrm{Aut}(S) = 2304\ .$$

7. Conjectures on 2-ranks of narrow class groups and unit signature ranks

In this section we apply the results on 2-Selmer signature maps in the previous sections to provide heuristics for the distribution of various numerical invariants of number fields. Among these applications are conjectures related to the distributions for the 2-ranks of narrow class groups and for the signature rank of the units.

For these applications we consider number fields K up to isomorphism, and generally restrict here to fields K satisfying two further assumptions.

The first assumption is that the degree $n = [K : \mathbb{Q}]$ is *odd*. The reasons for this restriction are (at least) twofold: (1) the conjectures involve the 2-ranks of various groups and the prime 2 is generally much more problematic in extensions of even degree, and (2) the possible images of the 2-Selmer signature map for K are simpler to describe when n is odd. Fields of even degree have recently been considered by Breen [Br].

The second assumption is that the Galois closure of K over $\mathbb{Q}$ has the symmetric group S_n as Galois group. When the Galois group G of the Galois closure of K is a proper subgroup of S_n it is expected that it will be necessary to consider additional complications due to the existence of possible G-stable subspaces.

If $\mathscr{K}$ is a collection of number fields (for example, the collection of all number fields with signature (r_1, r_2)), then by the density of the subset satisfying some condition $\mathscr{C}$ (for example, the subset of fields with odd class number) we mean the following: order the fields K in $\mathscr{K}$ by their absolute discriminant $|\mathrm{disc}\, K|$ and set

$$\mathrm{Prob}(\mathscr{C}) = \lim_{X\to\infty} \frac{\#\{K \in \mathscr{K} : |\mathrm{disc}\, K| \le X \text{ and } K \text{ satisfies condition } \mathscr{C}\}}{\#\{K \in \mathscr{K} : |\mathrm{disc}\, K| \le X\}}$$

when this limit exists. In the following, a statement conjecturing "$\mathrm{Prob}(\mathscr{C}) = \alpha$" for a given collection $\mathscr{K}$ will implictly include the necessary statement that the limit required for the left hand side exists.

Recall the notation $(q)_m = \prod_{i=1}^{m}(1 - q^{-i})$.

Conjectures: image of the 2-Selmer signature map. By Theorem 6.1, the image of the 2-Selmer signature map φ for the number field K is a maximal totally isotropic subspace of $V_\infty \perp V_2$, and by Theorem 6.6 this image is uniquely determined up to isomorphism by the integer $k = \dim(\mathrm{im}\,\varphi \cap V_\infty)$. Further, by Theorem 6.1, $\dim(\mathrm{im}\,\varphi \cap V_\infty) = \rho^+ - \rho$ where, as before, ρ^+ is the 2-rank of the narrow class group of K and ρ is the 2-rank of the class group of K.

If we apply the heuristic assumption

(H_1) The image of the 2-Selmer signature map is a uniformly random maximal totally isotropic subspace of $V_\infty \perp V_2$.

then we may apply Theorem 6.7, which computes the distribution of such subspaces of $V_\infty \perp V_2$, and obtain the following conjecture.

Conjecture 7.1. *For the collection of number fields K of odd degree n with signature (r_1, r_2) whose Galois closure has the symmetric group S_n as Galois group, we have*

$$\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ - \mathrm{rk}_2\, C_K = k) = \frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}}{2^{k(k+r_2)}(2)_k(2)_{k+r_2}(4)_{r_1+r_2-1}(4)_{(r_1-1)/2-k}}\ , \tag{7.2}$$

where k is any integer $0 \le k \le \lfloor r_1/2 \rfloor$.

Table 1 gives the values for these predicted densities when $n = 3, 5, 7$ (when $r_1 = 1$, $\dim(\mathrm{im}\,\varphi \cap V_\infty)$ is necessarily 0; also equation (7.2) yields precisely 1 in this case).

(r_1, r_2)	$k=0$	$k=1$	$k=2$	$k=3$
$(3,0)$	$2/5$	$3/5$		
$(1,1)$	1			
$(5,0)$	$16/51$	$30/51$	$5/51$	
$(3,1)$	$2/3$	$1/3$		
$(1,2)$	1			
$(7,0)$	$3584/12155$	$7056/12155$	$1470/12155$	$45/12155$
$(5,1)$	$112/187$	$70/187$	$5/187$	
$(3,2)$	$14/17$	$3/17$		
$(1,3)$	1			

TABLE 1. Conjectured $\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ - \mathrm{rk}_2\, C_K = k)$ for S_n-fields K of degree n and signature (r_1, r_2).

Conjectures: 2-ranks of narrow class groups. Conjecture 7.1 predicts the difference between the 2-rank of the narrow class group, ρ^+, and the 2-rank of the usual class group, ρ, so can be used to predict ρ^+ itself if it is coupled with information about ρ.

Malle [M3, Conjecture 2.1, Proposition 2.2] and Adam–Malle [A-M], based on extensive computations and the analogy to the function field case, have refined the Cohen–Martinet heuristics to give a prediction for $\mathrm{rk}_2\, C_K$. This prediction for K involves in particular the value of an inner product $u = \langle \chi_E, \chi_a \rangle$ of two characters on the Galois group of the Galois closure of K.

If K is a number field of degree n whose Galois closure L has the symmetric group S_n as Galois group, the decomposition group Γ_v of an infinite place in L is generated by an element $\sigma \in S_n$ which is the product of r_2 distinct transpositions. Then Herbrand's theorem (cf. [C-M, Theorem 6.7, p. 62]) shows the character χ_E in [M3] is the character of the representation $-1 + \mathrm{Ind}_{\Gamma_v}^{S_n}(1_{\Gamma_v})$. The augmentation character $\chi_a = \chi_\pi - 1$ in [M3] is the character of the natural linear permutation representation π of S_n on the cosets of $\mathrm{Gal}(L/K)$ (which is defined over $\mathbb{Q}$) less the trivial representation; the value of $\chi_a(\tau)$ for $\tau \in S_n$ is one less than the number of fixed points of τ. The character χ_a is absolutely irreducible on S_n of degree $n-1$ (this follows from the double transitivity of S_n—cf. Exercise 9 in Section 18.3 of

[Du-F]), and has Schur index 1 (since the associated representation is defined over $\mathbb{Q}$). The value of χ_a on an element τ of S_n is one less than the number of fixed points of τ. Then

$$u = \langle \chi_E, \chi_a \rangle_{S_n} = \langle -1 + \mathrm{Ind}_{\Gamma_v}^{S_n}(1_{\Gamma_v}), \chi_a \rangle_{S_n} = \langle \mathrm{Ind}_{\Gamma_v}^{\Gamma}(1_{\Gamma_v}), \chi_a \rangle_{S_n}$$

By Frobenius reciprocity this last inner product is $\langle 1, \chi_a|_{\Gamma_v} \rangle_{\Gamma_v} = (\chi_a(1) + \chi_a(\sigma))/2$, which yields $u = r_1 + r_2 - 1$.

If in addition n is odd, necessarily $r_1 > 0$, so K does not contain a fourth root of unity, and [M3, Conjecture 2.1, Proposition 2.2] is the following.

Conjecture 7.3 (Malle, Adam–Malle)**.** *For the collection of number fields K of odd degree n with signature (r_1, r_2) whose Galois closure has the symmetric group S_n as Galois group, we have*

$$\mathrm{Prob}(\mathrm{rk}_2\, C_K = \rho) = \frac{1}{2^{\rho(r_1+r_2-1)+\rho(\rho+1)/2}(2)_\rho} \frac{(4)_{r_1+r_2-1}(2)_\infty}{(2)_{r_1+r_2-1}(4)_\infty} \tag{7.4}$$

for any nonnegative integer ρ.

If φ is the 2-Selmer signature map for the number field K, then by (4.14) we have $\dim \ker \varphi = \rho$ if and only if $\mathrm{rk}_2\, C_K = \rho$, i.e., $\mathrm{Prob}(\dim \ker \varphi = \rho) = \mathrm{Prob}(\mathrm{rk}_2\, C_K = \rho)$. As a result, we make the following heuristic assumption:

(H_2) The 2-Selmer signature maps φ of number fields K have $\mathrm{Prob}(\dim \ker \varphi = \rho)$ given by the probability distribution in (7.4) of Conjecture 7.3, independent of the distribution of the images in heuristic (H_1).

Under this heuristic assumption, multiplying the probability $\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ - \mathrm{rk}_2\, C_K = k)$ predicted by Conjecture 7.1 with the probability $\mathrm{Prob}(\mathrm{rk}_2\, C_K = \rho^+ - k)$ predicted by Conjecture 7.3 and summing over the appropriate values of k yields the following conjecture.

Conjecture 7.5. *For the collection of number fields K of odd degree n with signature (r_1, r_2) whose Galois closure has the symmetric group S_n as Galois group, we have*

$$\begin{aligned}\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ = \rho^+) &= \sum_{k=0}^{\min(\rho^+, \lfloor r_1/2 \rfloor)} \mathrm{Prob}(\mathrm{rk}_2\, C_K = \rho^+ - k)\ \mathrm{Prob}(\mathrm{rk}_2\, C_K^+ - \mathrm{rk}_2\, C_K = k) \\ &= \frac{(2)_\infty (4)_{(r_1-1)/2} (4)_{(r_1-1)/2+r_2}}{2^{(r_1+r_2-1)\rho^+}(4)_\infty} \sum_{k=0}^{\min(\rho^+, \lfloor r_1/2 \rfloor)} \frac{2^{k(r_1-1-k)-(\rho^+-k)(\rho^+-k+1)/2}}{(2)_k (2)_{k+r_2} (2)_{\rho^+-k} (4)_{(r_1-1)/2-k}}\end{aligned} \tag{7.6}$$

for any nonnegative integer ρ^+.

Remark 7.7. There are other predictions for $\mathrm{Prob}(\mathrm{rk}_2\, C_K = \rho)$: one due to Venkatesh–Ellenberg involving the Schur multiplier [V-E, §2.4], work of Garton [G] accounting for roots of unity, and theorems of Wood in the function field case [Wood] that suggest predictions in the number field case. It is possible that these different perspectives all agree with Conjecture 7.3, but this has not yet been established. If Conjecture 7.3 needs modification, then the conjectures presented here conditional on the distribution of 2-ranks for class groups can be modified accordingly. It would also be of interest to find a "full matrix model", in the style of Venkatesh–Ellenberg [V-E] (inspired by Friedman–Washington [F-W]) that predicts both the image and kernel of the 2-Selmer map directly, without relying on independent conjectures

regarding the 2-rank of the class group. Recent unpublished work of Bartel–Lenstra gives a hopeful indication that such a model might exist.

For the first two values of ρ^+, Conjecture 7.5 gives

$$\operatorname{Prob}(\operatorname{rk}_2 C_K^+ = 0) = \frac{(2)_\infty (4)_{(r_1-1)/2+r_2}}{(4)_\infty (2)_{r_2}}$$

and

$$\operatorname{Prob}(\operatorname{rk}_2 C_K^+ = 1) = \begin{cases} \left(\dfrac{1}{2^{r_2}}\right) \dfrac{(2)_\infty (4)_{r_2}}{(4)_\infty (2)_{r_2}} & \text{if } r_1 = 1 \\ \left(\dfrac{1}{2^{r_1+r_2-1}} + \dfrac{2^{r_1-1}-1}{2^{r_1}(2^{r_2+1}-1)}\right) \dfrac{(2)_\infty (4)_{(r_1-1)/2+r_2}}{(4)_\infty (2)_{r_2}} & \text{if } r_1 > 1\ , \end{cases}$$

with increasingly complicated expressions when $\rho^+ > 1$.

If r_2 is fixed and r_1 tends to infinity, all the terms in (7.6) tend to zero except the term with $k = \rho^+$, so Conjecture 7.5 implies

$$\lim_{r_1\to\infty} \operatorname{Prob}(\operatorname{rk}_2 C_K^+ = \rho^+) = \frac{(2)_\infty}{2^{\rho^+(\rho^++r_2)}(2)_{\rho^+}(2)_{r_2+\rho^+}}\ . \tag{7.8}$$

Taking in particular the values when $r_2 = 0$ gives the following corollary.

Corollary 7.9. *Conjecture 7.5 predicts that among totally real S_n-fields of large odd degree n, the 2-ranks ρ^+ of the narrow class group are distributed as follows: approximately* 28.879% *have 2-rank 0,* 57.758% *have 2-rank 1,* 12.835% *have 2-rank 2,* 0.524% *have 2-rank 3,* 0.005% *have 2-rank 4, etc., according to the values*

$$\frac{(2)_\infty}{2^{(\rho^+)^2}(2)_{\rho^+}^2}\ . \tag{7.10}$$

We next compute the t-power moments of the distribution on the right hand side of (7.6). For fixed (r_1, r_2) with r_1 odd, let

$$\eta(\rho) = \frac{1}{2^{\rho(r_1+r_2-1)+\rho(\rho+1)/2}(2)_\rho} \frac{(4)_{r_1+r_2-1}(2)_\infty}{(2)_{r_1+r_2-1}(4)_\infty}\ , \tag{7.11}$$

$$p(k) = \frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}}{2^{k(k+r_2)}(2)_k(2)_{k+r_2}(4)_{r_1+r_2-1}(4)_{(r_1-1)/2-k}}\ , \text{ and} \tag{7.12}$$

$$\eta^+(\rho^+) = \sum_{k=0}^{\min(\rho^+,\lfloor r_1/2\rfloor)} \eta(\rho^+-k)\, p(k) \tag{7.13}$$

denote the distributions in Conjectures 7.3, 7.1, and 7.5, respectively. We first prove the following combinatorial lemma.

Lemma 7.14. *Suppose m and r_2 are nonnegative integers. If*

$$\tilde{p}(k) = \frac{(q)_{2m+r_2}(q^2)_m(q^2)_{m+r_2}}{q^{k(k+r_2)}(q)_k(q)_{k+r_2}(q^2)_{2m+r_2}(q^2)_{m-k}}, \tag{7.15}$$

(with $(q)_m = \prod_{i=1}^{m}(1-q^{-i})$ *as before) then*

$$\sum_{k=0}^{m} q^k \tilde{p}(k) = \frac{1+q^{-r_2}}{1+q^{-2m-r_2}}. \tag{7.16}$$

Proof. If

$$f_{m,k} = q^{-k(k+r_2-1)} \frac{1+q^{-2m-r_2}}{1+q^{-r_2}} \frac{(q)_{2m+r_2}(q^2)_m(q^2)_{m+r_2}}{(q)_k(q)_{k+r_2}(q^2)_{2m+r_2}(q^2)_{m-k}}$$

then (7.16) is equivalent to

$$\sum_{k=0}^{m} f_{m,k} = 1. \tag{7.17}$$

Since $f_{0,0} = 1$, the sum for $m = 0$ is indeed 1. For $m \geq 1$ and $0 \leq k \leq m$, define

$$\mathrm{cert}_{m,k} = \frac{(q^{2k}-q^{2m})(q^{3+2k}+q^{2m}-q^{1+2m}+q^{1+k+2m}+q^{1+k+2m+r2}+q^{2+2k+2m+r2})}{q^{2k+2m}(q^{2m}-1)(q^{2(m+r_2)}-1)},$$

and set $g_{m,k} = \mathrm{cert}_{m,k} f_{m,k}$. Then a straightforward computation confirms that

$$1 - \frac{f_{m-1,k}}{f_{m,k}} = \mathrm{cert}_{m,k} - \mathrm{cert}_{m,k-1}\frac{f_{m,k-1}}{f_{m,k}}$$

for $1 \leq k \leq m-1$. It follows that

$$f_{m,k} - f_{m-1,k} = g_{m,k} - g_{m,k-1} \tag{7.18}$$

for $1 \leq k \leq m-1$. Defining $f_{m-1,m} = g_{m,-1} = 0$, it is easy to check that (7.18) holds for $0 \leq k \leq m$. Summing (7.18) from $k = 0$ to m, using $f_{m-1,m} = g_{m,-1} = 0$ and noting $g_{m,m} = 0$ (since $\mathrm{cert}_{m,m} = 0$) gives

$$\sum_{k=0}^{m} f_{m,k} - \sum_{k=0}^{m-1} f_{m-1,k} = 0.$$

It follows that the sum on the left hand side in (7.17) is independent of m, hence always equals 1 since the sum is 1 for $m = 0$, which completes the proof. □

Remark 7.19. The factor $\mathrm{cert}_{m,k}$ (for "certificate") in the Lemma determining a Wilf-Zeilberger recurrence (7.18) for $f_{m,k}$ were determined using the software package "qZeil" implementing a q-analogue of the Zeilberger algorithm. The software was graciously provided by Peter Paule at the Research Institute for Symbolic Computation at Johannes Kepler University, Linz, Austria. The method of proof in the Lemma follows Section 4 of the paper [P-R] (see also §2.1 in [R]).

Proposition 7.20. *For* $t \geq 1$, *the* t^{th}*-power moment* $\sum_{\rho^+=0}^{\infty} 2^{t\rho^+}\eta^+(\rho^+)$ *of the probability distribution predicting* $\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ = \rho^+)$ *in Conjecture 7.5 is*

$$\prod_{s=1}^{t}(1+2^{s-r_1-r_2}) \sum_{k=0}^{\lfloor r_1/2 \rfloor} 2^{tk} p(k) \tag{7.21}$$

where $p(k)$ *is given by* (7.12). *For* $t = 1$ *we have*

$$\sum_{\rho^+=0}^{\infty} 2^{\rho^+}\eta^+(\rho^+) = 1 + 2^{-r_2}. \tag{7.22}$$

Proof. By (7.13) we have

$$\begin{aligned}\sum_{\rho^+=0}^{\infty} 2^{t\rho^+}\eta^+(\rho^+) &= \sum_{\rho^+=0}^{\infty} 2^{t\rho^+} \sum_{k=0}^{\min(\rho^+,\lfloor r_1/2\rfloor)} \eta(\rho^+-k)\,p(k) \\ &= \left(\sum_{\rho=0}^{\infty} 2^{t\rho}\eta(u,\rho)\right)\left(\sum_{k=0}^{\lfloor r_1/2\rfloor} 2^{tk}p(k)\right).\end{aligned} \tag{7.23}$$

The first expression is the t^{th}-power moment of $\eta(u,\rho)$, whose value was calculated by Malle [M3, Proposition 2.2] to be

$$\left(\sum_{\rho=0}^{\infty} 2^{t\rho}\eta(u,\rho)\right) = \prod_{s=1}^{t}(1+2^{s-r_1-r_2})$$

which gives the first statement in the proposition. For $t=1$, the first factor in (7.21) is $1+2^{-r_1-r_2-1}$ and the second factor is $(1+2^{-r_2})/(1+2^{-r_1-r_2-1})$ by setting $q=2$ and $m=(r_1-1)/2$ in Lemma 7.14, so their product yields (7.22). □

Table 2 gives approximate values of the probability distribution $\eta^+(\rho^+)$ together with its moments.

(r_1,r_2)	$\rho^+=0$	$\rho^+=1$	$\rho^+=2$	$t=1$	$t=2$	$t=3$	$t=4$
$(3,0)$	0.314567	0.550492	0.124516	2	21/4	39/2	225/2
$(1,1)$	0.629133	0.314567	0.052427	3/2	3	9	45
$(5,0)$	0.294907	0.571382	0.127102	2	81/16	135/8	4995/64
$(3,1)$	0.589813	0.368633	0.039935	3/2	45/16	225/32	405/16
$(1,2)$	0.786417	0.196604	0.016384	5/4	15/8	15/4	45/4
$(7,0)$	0.290298	0.576061	0.128021	2	321/64	519/32	71415/1024
$(5,1)$	0.580597	0.381017	0.037448	3/2	177/64	837/128	21195/1024
$(3,2)$	0.774129	0.214268	0.011376	5/4	117/64	855/256	4185/512
$(1,3)$	0.884719	0.110590	0.004608	9/8	45/32	135/64	135/32

TABLE 2. Conjectured $\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ = \rho^+)$ for S_n-fields K of degree n and signature (r_1,r_2), and the t-power moments of the associated probability distribution.

Combining Conjecture 7.5 that $\mathrm{Prob}(\mathrm{rk}_2\, C_K^+ = \rho^+) = \eta^+(\rho^+)$ with the first moment computation in the previous proposition gives the following conjecture.

Conjecture 7.24. *For the collection of number fields K of odd degree n with signature (r_1,r_2) whose Galois closure has the symmetric group S_n as Galois group, the average size of $C_K^+[2]$ is $1+2^{-r_2}$.*

For cubic fields ($n=3$), this conjecture is a theorem of Bhargava–Varma [B-V]. See also Ho–Shankar–Varma [HSV], who prove related results for the family of number fields arising from binary n-ic forms.

Conjectures: Signature ranks of units. We next consider the signature rank for S_n-fields K of odd degree n. The units of K define a subspace E of $\mathrm{Sel}_2(K)$ of dimension r_1+r_2 that contains the element $(-1)K^{*2}/K^{*2}$ (which is nontrivial: $\sqrt{-1}\notin K^*$ since r_1 is positive). If φ is the 2-Selmer signature map for K then the signature rank of the units of K is the dimension of $\varphi_\infty(E)$, hence is $r_1+r_2-\dim(E\cap\ker\varphi_\infty)$. By equation 4.14, the subspace $\dim\ker\varphi_\infty$ of $\mathrm{Sel}_2(K)$ has dimension $\rho^+ + r_2 = (\rho+k)+r_2$, where $k=\dim(\mathrm{im}\,\varphi\cap V_\infty)$ is determined by the isomorphism type of $\mathrm{im}\,\varphi$ as a maximal totally isotropic subspace of $V_\infty\perp V_2$ and where $\rho=\dim(\ker\varphi)$.

We make the following heuristic assumption:

(H_3) For the collection of fields K of odd degree the subspace of $\mathrm{Sel}_2(K)$ generated by the units of K is distributed as a uniformly random subspace.

With this assumption $\dim(E\cap\ker\varphi_\infty)$ can be determined using the linear algebra computation in the following lemma.

Lemma 7.25. *Let q be any prime power, let X be an $\mathbb{F}_q$-vector space with $\dim X=m$, let $0\neq e\in X$, and let $Y\subseteq X$ be a subspace with $e\notin Y$ and $\dim Y=r$.*

If E is a uniformly random subspace of X with $e\in E$ and $\dim E=t\geq 1$, then

$$\mathrm{Prob}(\dim(E\cap Y)=s')=q^{s'(r+t-m-s')}\frac{(q)_r(q)_{t-1}(q)_{m-1-r}(q)_{m-t}}{(q)_{r-s'}(q)_{s'}(q)_{t-1-s'}(q)_{m-1}(q)_{m+s'-r-t}}$$

for any nonnegative integer s' with $r+t-m\leq s'\leq\min(r,t-1)$.

Proof. Fix the integer s' with $r+t-m\leq s'\leq\min(r,t-1)$. The total number of possible subspaces E satisfying $e\in E$, $\dim E=t$, and $\dim(E\cap Y)=s'$ can be counted by constructing a basis for E, as follows. Start with e, then choose s' linearly independent elements of Y, and finally complete with $t-1-s'$ additional linearly independent elements of X to give a basis of E. This gives a total of

$$\begin{aligned}1\cdot(q^r-1)(q^r-q)\cdots(q^r-q^{s'-1})\cdot(q^m-q^{r+1})\cdots(q^m-q^{r+t-s'-1})\\ =q^{rs'+m(t-1-s')}\frac{(q)_r(q)_{m-1-r}}{(q)_{r-s'}(q)_{m+s'-r-t}}\end{aligned}\tag{7.26}$$

possible bases. A subspace E has

$$1\cdot(q^{s'}-1)\cdots(q^{s'}-q^{s'-1})\cdot(q^t-q^{s'+1})\cdots(q^t-q^{t-1})=q^{s'^2}(q)_{s'}\;q^{t(t-1-s')}(q)_{t-1-s'}\tag{7.27}$$

such bases, and the total number of subspaces of dimension t containing the element e is

$$\frac{(q^m-q)\cdots(q^m-q^{t-1})}{(q^t-q)\cdots(q^t-q^{t-1})}=q^{(m-t)(t-1)}\frac{(q)_{m-1}}{(q)_{m-t}(q)_{t-1}}.\tag{7.28}$$

Then $\mathrm{Prob}(\dim(E\cap Y)=s')$ is obtained by dividing (7.26) by the product of (7.27) and (7.28), which simplifies to give the result stated in the lemma. □

We now apply the lemma with $q=2$, $X=\mathrm{Sel}_2(K)$, $e=(-1)K^{*2}/K^{*2}$, $Y=\ker\varphi_\infty$, and E the subspace generated by the units of K in $\mathrm{Sel}_2(K)$, so $t=r_1+r_2$. Note that since $n=[K:\mathbb{Q}]$ is odd, Corollary 4.10 gives $\mathrm{sgn}_2(-1)\neq 0$, hence $e\notin Y$. Under the assumption that $\dim(\mathrm{im}\,\varphi\cap V_\infty)=k$ and $\dim(\ker\varphi)=\rho$ for the associated 2-Selmer signature map, we have $m=r_1+r_2+\rho$ and $r=\rho+k+r_2$. Taking $s'=r_1+r_2-s$, the lemma then gives an expression for $\mathrm{Prob}(\dim(E\cap\ker\varphi_\infty)=r_1+r_2-s)$ for integers s with $k+r_2\leq(r_1+r_2-s)\leq$

$\min(\rho+k+r_2, r_1+r_2-1)$. Since $\dim(E\cap\ker\varphi_\infty) = r_1+r_2-s$ if and only if $\mathrm{sgnrk}(E_K) = s$, the result of applying the lemma is the conditional probability

$$\begin{aligned}&\mathrm{Prob}\big(\,\mathrm{sgnrk}(E_K) = s \;\big|\; \dim(\mathrm{im}\,\varphi\cap V_\infty) = k \text{ and } \dim(\ker\varphi) = \rho\,\big)\\ &\qquad = 2^{(r_1+r_2-s)(k-r_1+s)}\frac{(2)_{\rho+k+r_2}(2)_{r_1+r_2-1}(2)_{r_1-k-1}(2)_\rho}{(2)_{\rho+k-r_1+s}(2)_{r_1+r_2-s}(2)_{s-1}(2)_{r_1+r_2-1+\rho}(2)_{r_1-s-k}}\,,\end{aligned} \tag{7.29}$$

for integers s with $r_1 - \min(\rho+k, r_1-1) \le s \le r_1 - k$.

The probability that $\dim(\mathrm{im}\,\varphi\cap V_\infty) = k$ is predicted in Conjecture 7.2. Multiplying by the conditional probability in equation (7.29) and summing over the possible values of k gives the predicted probability for the unit signature rank to equal s as K ranges over fields whose class group has 2-rank ρ (recall $\dim(\ker\varphi) = \mathrm{rk}_2\, C_K[2]$):

$$\begin{aligned}&\mathrm{Prob}\big(\,\mathrm{sgnrk}(E_K) = s \;\big|\; \mathrm{rk}_2\, C_K[2] = \rho\,\big) =\\ &\qquad 2^{(r_1+r_2-s)(s-r_1)}\frac{(2)_{r_1+r_2-1}^2(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}(2)_\rho}{(2)_{r_1+r_2-s}(2)_{s-1}(2)_{r_1+r_2-1+\rho}(4)_{r_1+r_2-1}}\;\times\\ &\qquad\left(\sum_{k=\max(0,r_1-s-\rho)}^{\min(r_1-s,(r_1-1)/2)}\frac{2^{k(r_1-s-k)}(2)_{r_1-1-k}(2)_{\rho+k+r_2}}{(2)_{r_1-s-k}(4)_{(r_1-1)/2-k}(2)_k(2)_{k+r_2}(2)_{\rho+k-r_1+s}}\right),\end{aligned} \tag{7.30}$$

for any integer $\rho \ge \max(0, (r_1+1)/2 - s)$ (note that $\rho \ge (r_1+1)/2 - s$ is Corollary 3.13).

The probability that $\dim(\ker\varphi) = \rho$ is predicted in Conjecture 7.3. Multiplying by this probability as well and summing over all the possible values of k and ρ we obtain the following conjecture for the predicted probability of signature rank s.

Conjecture 7.31. *For the collection of number fields K of odd degree n with signature (r_1, r_2) whose Galois closure has the symmetric group S_n as Galois group, we have*

$$\begin{aligned}&\mathrm{Prob}(\mathrm{sgnrk}(E_K) = s) =\\ &\qquad 2^{(r_1+r_2-s)(s-r_1)}\frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}(2)_\infty}{(2)_{r_1+r_2-s}(2)_{s-1}(4)_\infty}\;\times\\ &\qquad\times\left(\sum_{\rho=\max(0,(r_1+1)/2-s)}^{\infty}\frac{1}{2^{\rho(r_1+r_2-1)+\rho(\rho+1)/2}(2)_{r_1+r_2-1+\rho}}\right.\\ &\qquad\qquad\left.\left(\sum_{k=\max(0,r_1-s-\rho)}^{\min(r_1-s,(r_1-1)/2)}\frac{2^{k(r_1-s-k)}(2)_{r_1-1-k}(2)_{\rho+k+r_2}}{(2)_{r_1-s-k}(4)_{(r_1-1)/2-k}(2)_k(2)_{k+r_2}(2)_{\rho+k-r_1+s}}\right)\right)\end{aligned} \tag{7.32}$$

for any integer s with $1 \le s \le r_1$.

Table 3 gives approximate numerical values for the predicted densities in Conjecture 7.31 when $n = 3, 5, 7$ (when $r_1 = 1$ we have $\mathrm{sgnrk}(E_K) = 1$; also equation (7.32) yields precisely 1 for $s = 1$ in this case).

(r_1, r_2)	$s=1$	$s=2$	$s=3$	$s=4$	$s=5$	$s=6$	$s=7$
$(3,0)$	0.019097	0.618304	0.362599				
$(1,1)$	1						
$(5,0)$	$1.9 \cdot 10^{-7}$	0.000582	0.105508	0.589338	0.304572		
$(3,1)$	0.002630	0.346318	0.651052				
$(1,2)$	1						
$(7,0)$	$< 9 \cdot 10^{-16}$	$< 2 \cdot 10^{-10}$	0.000003	0.003921	0.122913	0.580570	0.292593
$(5,1)$	$< 4 \cdot 10^{-9}$	0.000040	0.027980	0.377432	0.594548		
$(3,2)$	0.000346	0.180949	0.818705				
$(1,3)$	1						

TABLE 3. Conjectured probability that the signature rank of the units is s for S_n-fields K of degree n and signature (r_1, r_2)

Conjectures: Class group a direct summand of the narrow class group. As a final application, we conjecture a probability that the fundamental exact sequence (2.6) (equivalently, (2.8) or (2.9)) splits, i.e., that the class group C_K is a direct summand of the narrow class group C_K^+. As noted in Lemma 2.14, the splitting of this sequence is equivalent to $\rho^+ = \rho + \rho_\infty$. Given values for ρ and $k = \rho^+ - \rho$, this is the condition that ρ_∞ is also k.

Since $\mathrm{sgnrk}(E_K) = r_1 - k$ if and only if $\rho_\infty = k$ by (2.13), the conditional probability $\mathrm{Prob}\big(\rho_\infty = k \;\big|\; \dim(\mathrm{im}\,\varphi \cap V_\infty) = k \text{ and } \dim(\ker\varphi) = \rho\big)$ is obtained from (7.29) on setting $s = r_1 - k$. Multiplying by the probability that $\dim(\mathrm{im}\,\varphi \cap V_\infty) = k$ predicted in Conjecture 7.2 and the probability that $\dim(\ker\varphi) = \rho$ predicted in Conjecture 7.3 and summing over the possible values of k and ρ yields the following conjecture.

Conjecture 7.33. *For the collection of number fields K of odd degree n with signature (r_1, r_2) whose Galois closure has the symmetric group S_n as Galois group, we have*

$$\begin{aligned}\mathrm{Prob}(C_K \text{ is a direct summand of } C_K^+) = \\ \frac{(2)_{r_1+r_2-1}(4)_{(r_1-1)/2}(4)_{(r_1-1)/2+r_2}(2)_\infty}{(4)_\infty} \times \\ \times \left(\sum_{\rho=0}^{\infty} \frac{1}{2^{\rho(r_1+r_2-1)+\rho(\rho+1)/2}(2)_{r_1+r_2-1+\rho}(2)_\rho} \right. \\ \left. \left(\sum_{k=0}^{\lfloor r_1/2 \rfloor} \frac{(2)_{\rho+k+r_2}}{2^{k(k+r_2)}(2)_{k+r_2}^2(2)_k(4)_{(r_1-1)/2-k}} \right) \right) .\end{aligned} \tag{7.34}$$

Table 4 gives approximate numerical values for these predicted densities when $n = 3, 5, 7$ (when $r_1 = 1$ we have $\mathrm{sgnrk}(E_K) = 1$ and, by (2.13) or directly, $\rho_\infty = 0$ and $\rho^+ = \rho$; also equation (7.34) yields precisely 1 in this case).

(r_1, r_2)	$\mathrm{Prob}(\rho^+ = \rho + \rho_\infty)$
$(3,0)$	0.943700
$(1,1)$	1
$(5,0)$	0.982241
$(3,1)$	0.981776
$(1,2)$	1
$(7,0)$	0.995315
$(5,1)$	0.994300
$(3,2)$	0.994831
$(1,3)$	1

TABLE 4. Predicted probability that C_K is a direct summand of C_K^+ for S_n-fields K of degree n and signature (r_1, r_2)

Remark 7.35. As in the derivation of equation (7.30), one can give a predicted probability that C_K is a direct summand of C_K^+ just for those fields with $\mathrm{rk}_2\, C_K[2] = \rho$ for any fixed ρ:

$$\mathrm{Prob}\big(C_K \text{ is a direct summand of } C_K^+ \;\big|\; \mathrm{rk}_2\, C_K[2] = \rho\big) = \frac{(2)_{r_1+r_2-1}^2 (4)_{(r_1-1)/2} (4)_{(r_1-1)/2+r_2}}{(4)_{r_1+r_2-1} (2)_{r_1+r_2-1+\rho}} \left(\sum_{k=0}^{\lfloor r_1/2 \rfloor} \frac{(2)_{\rho+k+r_2}}{2^{k(k+r_2)} (2)_{k+r_2}^2 (2)_k (4)_{(r_1-1)/2-k}} \right). \tag{7.36}$$

8. Computations for totally real cubic and quintic fields

In this section, we present the results of some relatively extensive computations for totally real cubic and quintic fields, providing evidence for our conjectures. In these computations, for efficiency we assume class group bounds that are implied by the Generalized Riemann Hypothesis (GRH), so the results are conditional on GRH.

Results. Tables 5 (totally real cubic fields) and 6 (totally real quintic fields) summarize our computations. In each we randomly sampled N fields (typically one million) with discriminants bounded by several different values of X, as indicated in the tables. The procedure for generating the fields differs slightly in the two cases, as described in greater detail later. As noted in the Introduction, because it is known that 100% of totally real cubic (respectively, quintic) number fields have the symmetric group as Galois group for their Galois closure, our conjectures predict densities for *all* totally real cubic (respectively, quintic) fields.

For each discriminant bound X, the corresponding entries in the tables are the following:

- the computed density of fields with given 2-rank ρ of the class group, predicted in Conjecture 7.3,
- the computed density of fields with given 2-rank ρ^+ of the narrow class group, predicted in Conjecture 7.5,
- the density of fields with given $k = \rho^+ - \rho$, the dimension of the intersection of the image of the 2-Selmer signature map with the space V_∞ (cf. Definition 4.11), predicted in 7.1,

- the t^{th}-power moment ($t = 1, 2, 3$) of the distribution of values of ρ and of ρ^+ for the computed fields, cf. Proposition 7.20,
- the density of fields with given signature rank of the units, predicted in Conjecture 7.32 (the indicated exact values 0 are known to hold),
- the density of fields with given signature rank of the units and given 2-rank of the class group ρ (with separate indication $1/\sqrt{N_i}$ of the margin for error, where N_i is the number of fields in the sample having $\rho = i$), cf. equation (7.30), and
- the density of fields for which (2.9) splits, equivalently, C_K is a direct summand of C_K^+, predicted in Conjecture 7.33.

As the data in the two tables shows, the computed densities are in remarkably good agreement with our predictions, in each case convergent apparently monotonically to the expected values. The convergence is relatively slow, which seems to be a characteristic of these sorts of problems and is a phenomenon observed by other authors (and may be an inherent computational difficulty, see [DGK]). It would be possible to extend these computations, and sample with larger X, but already this data we believe is sufficiently compelling.

Remark 8.1. The first totally real cubic fields K with signature ranks $s = 3, 2, 1$ are generated by roots of the following polynomials: (1) $s = 3$, $x^3 - x^2 - 2x + 1$, $\operatorname{disc} K = 49$, (2) $s = 2$, $x^3 - 4x - 1$, $\operatorname{disc} K = 229$, and (3) $s = 1$, $x^3 - 39x - 26$, $\operatorname{disc} K = 13689$.

The first totally real quintic fields K with unit signature rank $s = 4$ and $s = 5$ have been known for some time and the first examples with $s = 2$ and $s = 3$ were computed in the 2006 Master's thesis of Jason Hill (cf. [Hi]), and confirmed by the computations here. These fields are generated by roots of the following polynomials: (1) $s = 5$, $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$, $\operatorname{disc} K = 14641$, (2) $s = 4$, $x^5 - 2x^4 - 3x^3 + 5x^2 + x - 1$, $\operatorname{disc} K = 36497$, (3) $s = 3$, $x^5 - 2x^4 - 6x^3 + 8x^2 + 8x + 1$, $\operatorname{disc} K = 638597$, and (4) $s = 2$, $x^5 - x^4 - 21x^3 - 7x^2 + 68x + 60$, $\operatorname{disc} K = 52315684$.

In addition, Hill found 20 totally real quintic fields with a totally positive system of fundamental units, the first of which (not known to be the first example of such a field) is given by (5) $s = 1$, $x^5 - 2x^4 - 32x^3 + 41x^2 + 220x - 289$, $\operatorname{disc} K = 405673292473$.

Hill's search (the precursor to the one here) was not exhaustive, and yielded roughly one field with a totally positive system of fundamental units for every 10 million totally real quintic fields produced.

Computational matters. We begin with comments related to the computations for totally real cubic fields.

A cubic ring is a commutative ring that is free of rank 3 as a $\mathbb{Z}$-module. By the correspondence of Delone–Faddeev [D-F] (as refined by Gan–Gross–Savin [GGS]), cubic rings are parametrized by $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms, with action twisted by the determinant; see Gross–Lucianovic [G-L]. This parametrization is discriminant-preserving, and unique representatives of the $\mathrm{GL}_2(\mathbb{Z})$-orbits are provided by reduced forms. By work of Davenport–Heilbronn [D-H], maximal orders in cubic fields are in bijection with reduced binary cubic forms satisfying certain congruence conditions. Belabas [Bel] has used these bijections to exhibit a fast algorithm to tabulate cubic fields. Following his method, but with statistical purposes in mind, we instead use this bijection to *sample* binary cubic forms.

		X					
		10^{10}	10^{11}	10^{12}	10^{13}	10^{14}	predicted
N		10^6	10^6	10^6	$0.82 \cdot 10^6$	$0.33 \cdot 10^6$	
$1/\sqrt{N}$		0.001	0.001	0.001	0.001	0.002	
k	0	0.415	0.412	0.408	0.406	0.405	$2/5 = 0.400$
	1	0.585	0.588	0.592	0.594	0.596	$3/5 = 0.600$
sgnrk(E_K)	1	0.015	0.016	0.017	0.017	0.017	0.019
	2	0.604	0.606	0.610	0.612	0.614	0.618
	3	0.382	0.377	0.373	0.370	0.368	0.363
ρ	0	0.821	0.812	0.806	0.800	0.798	0.786
	1	0.169	0.177	0.181	0.186	0.188	0.197
	2	0.010	0.011	0.012	0.013	0.014	0.016
	≥ 3	0.000	0.000	0.000	0.000	0.000	0.001
ρ moments	1	1.199	1.212	1.220	1.228	1.231	1.250
	2	1.661	1.710	1.746	1.779	1.792	1.875
	3	2.867	3.052	3.195	3.331	3.380	3.750
ρ^+	0	0.338	0.333	0.327	0.324	0.322	0.315
	1	0.555	0.554	0.555	0.554	0.553	0.550
	2	0.102	0.107	0.111	0.115	0.117	0.125
	≥ 3	0.005	0.006	0.007	0.008	0.008	0.010
ρ^+ moments	1	1.897	1.921	1.941	1.955	1.963	2.000
	2	4.530	4.690	4.825	4.926	4.968	5.250
	3	14.20	15.23	16.27	17.02	17.19	19.50
splits?	yes	0.952	0.949	0.948	0.946	0.946	0.944
	no	0.048	0.051	0.052	0.053	0.054	0.056
sgnrk(E_K)	1	0.000	0.000	0.000	0.000	0.000	0
(fields with	2	0.588	0.590	0.594	0.596	0.597	0.600
$\rho = 0$)	3	0.412	0.410	0.406	0.405	0.403	0.400
$1/\sqrt{N_0}$		0.001	0.001	0.001	0.001	0.002	
sgnrk(E_K)	1	0.082	0.083	0.085	0.083	0.082	0.086
(fields with	2	0.674	0.678	0.679	0.683	0.686	0.686
$\rho = 1$)	3	0.245	0.240	0.237	0.235	0.232	0.229
$1/\sqrt{N_1}$		0.002	0.002	0.002	0.003	0.004	
sgnrk(E_K)	1	0.120	0.125	0.130	0.132	0.126	0.131
(fields with	2	0.672	0.677	0.675	0.677	0.685	0.686
$\rho = 2$)	3	0.208	0.198	0.196	0.191	0.190	0.183
$1/\sqrt{N_2}$		0.010	0.010	0.010	0.010	0.015	

TABLE 5. Computed data versus predicted for totally real cubic fields.

		D			
		10^9	$10 \cdot 10^9$	$320 \cdot 10^9$	predicted
N		10^6	10^6	10^6	
$1/\sqrt{N}$		0.001	0.001	0.001	
k	0	0.376	0.356	0.333	$16/51 \approx 0.314$
	1	0.566	0.574	0.584	$30/51 \approx 0.588$
	2	0.058	0.070	0.084	$5/51 \approx 0.098$
sgnrk(E_K)	1	0.000	0.000	0.000	$1.9 \cdot 10^{-7}$
	2	0.000	0.000	0.000	0.000582
	3	0.060	0.073	0.089	0.106
	4	0.567	0.576	0.585	0.589
	5	0.372	0.351	0.325	0.305
ρ	0	0.981	0.973	0.958	0.940
	1	0.018	0.027	0.041	0.059
	≥ 2	0.000	0.000	0.000	0.001
ρ moments	1	1.02	1.03	1.04	1.06
	2	1.05	1.08	1.13	1.20
	3	1.13	1.20	1.32	1.49
ρ^+	0	0.368	0.345	0.318	0.295
	1	0.564	0.570	0.574	0.571
	≥ 2	0.068	0.085	0.108	0.134
ρ^+ moments	1	1.77	1.83	1.91	2.00
	2	3.73	4.05	4.50	5.06
	3	9.45	10.9	13.3	16.9
splits?	yes	0.994	0.991	0.987	0.982
	no	0.006	0.009	0.013	0.018
sgnrk(E_K) (fields with $\rho = 0$)	1	0.000	0.000	0.000	0
	2	0.000	0.000	0.000	0
	3	0.059	0.070	0.084	0.098
	4	0.566	0.575	0.584	0.588
	5	0.375	0.354	0.332	0.314
$1/\sqrt{N_0}$		0.001	0.001	0.001	
sgnrk(E_K) (fields with $\rho = 1$)	1	0.000	0.000	0.000	0
	2	0.002	0.004	0.006	0.009
	3	0.150	0.169	0.194	0.221
	4	0.621	0.622	0.614	0.607
	5	0.227	0.205	0.185	0.162
$1/\sqrt{N_0}$		0.007	0.006	0.005	

TABLE 6. Computed data versus predicted for totally real quintic fields.

Let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $a,b,c,d \in \mathbb{Z}$ and let

$$P = b^2 - 3ac, \quad Q = bc - 9ad, \quad R = c^2 - 3bd. \tag{8.2}$$

We say that f is real if $\operatorname{disc} f > 0$, and we suppose that f is real. The binary quadratic form $H(f)(x,y) = Px^2 + Qxy + Ry^2$ is called the Hessian of f. Following Belabas [Bel, Definition 3.2], we say f is Hessian reduced if $|Q| \leq P$ and $P \leq R$, and we say f is reduced if f is Hessian reduced and all of the following further conditions hold:

- $b > 0$ or $d < 0$,
- $Q \neq 0$ or $d < 0$,
- $P \neq Q$ or $b < |3a - b|$, and
- $P \neq R$ or $(a \leq |d|$ and $(a \neq |d|$ or $b < |c|))$.

By [Bel, Corollary 3.3.1] two equivalent real, reduced forms are equal.

Suppose that $f(x,y)$ is irreducible and let $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/(f(x,1))$, so that K is a cubic field. The cubic ring defined by f is the order $R \subseteq K$ with $\mathbb{Z}$-basis $1, a\theta, a\theta^2 + b\theta$. By the work of Davenport–Heilbronn [D-H], the order R fails to be maximal at p if and only if either $p \mid f$ or $f(x,y)$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a form such that $p^2 \mid a$ and $p \mid b$ (see also Belabas [Bel, Corollary 3.3.2]). For a nice self-contained account of the above, see Bhargava–Shankar–Tsimserman [BST, §§2–3].

Using this, we can sample totally real cubic fields. Let $X > 0$ be a height parameter, and sample $a,b \in [0,X] \cap \mathbb{Z}$ and $c,d \in [-X,X] \cap \mathbb{Z}$ uniformly. We keep the corresponding cubic form $f(x,y)$ if it is real, irreducible, reduced, and the corresponding order R is maximal. In this way, we have sampled a uniformly random totally real cubic field K and the discriminant of K is $O(X)$, with an effectively computable constant.

For such fields, we compute (subject to the GRH) using the computer algebra system Magma [BCP] the class group, unit group, narrow class group, and 2-Selmer group [Co2, §5.2.2]. The 2-Selmer signature map φ is then effectively computable, defined by real and 2-adic signatures, the latter of which are given by (efficiently computable) congruences modulo bounded powers of even primes. We also verify the equalities (4.14) and Proposition 5.2 in each case.

Using this procedure, we computed N random totally real cubic fields with height bound $X = 10^m$ and $m = 10, 11, 12, 13, 14$, where N is as indicated. By the central limit theorem, this sampling procedure will converge to the actual distribution (in each case, with fixed X) with error $O(1/\sqrt{N})$ as N increases, so $1/\sqrt{N}$ gives an approximation of the margin of error. While this procedure samples number fields ordered by height and not by discriminant, we expect the same densities for both orderings. In particular this sampling difference should not effect the numerical data presented—the results agree for those ranges of discriminant for which we have complete lists of all cubic fields. The advantage in using the precise bijection of totally real cubic fields (more precisely, with their rings of integers) with certain reduced binary cubic forms is that it is possible to sample such cubic fields with large discriminants. Computing exhaustive lists of all totally real cubic fields up to these discriminant bounds is computationally impractical.

We next turn to the computations for totally real quintic fields.

By work of Bhargava [Bha1, Bha2, Bha3], in principle one should similarly be able to sample quintic fields as we did cubic fields, but such an explicit method has not yet been exhibited. Instead, we simply generated a large table of totally real quintic fields.

For an overview of algorithms for enumeration of number fields, see Cohen [Co2, §9.3]. The computations here are described in Voight [V], where a number of substantial optimizations are made for the case of totally real fields (which have been implemented and are available in SAGE [Sage]). The basic starting point is Hunter's theorem (see [Hu] and the improvement [Co1, Theorem 6.4.2]), which in the case of a totally real quintic field K states that there exists a nonrational algebraic integer $\alpha \in K$ (hence a generator for K over $\mathbb{Q}$) with $\mathrm{Tr}(\alpha) \in \{0, -1, -2\}$ and

$$t_2(\alpha) \le \frac{\mathrm{Tr}(\alpha)^2}{5} + \sqrt{2}\left(\frac{\mathrm{disc}\, K}{5}\right)^{1/4} \tag{8.3}$$

with Minkowski norm $t_2(\alpha) = \sum_{i=1}^{5} {\alpha_i}^2$ given by the sum of squares of the conjugates of α. We let $t_2(K)$ denote the minimum $t_2(\alpha)$ for such a generator α of the field K. Then Hunter's inequality implies

$$\mathrm{disc}\, K \ge \frac{5}{4}(t_2(K) - 4/5)^4 \tag{8.4}$$

and based on preliminary computations, a significantly better lower bound for $\mathrm{disc}\, K$ relative to $t_2(K)$ appears unlikely. This last inequality implies that we can be assured of computing a complete list of totally real quintic fields with discriminant bounded by 10^{10} by computing all polynomials with $t_2 = t \le 299$ (and checking when polynomials generate the same field K). Examining the data for computations for values of $t < 100$ and root discriminant bounded by 40 suggested it requires roughly $5.0(10)^{-13} D^{7/4} (\log D)^3$ seconds to compute all totally real quintic fields up to discriminant D. This estimate indicates a computation of polynomials with $t_2 \le 299$ for fields with a root discriminant bound of 100 would require more than 60 CPU years.

As a result, we compromised and limited the computations to searching all totally real quintic fields with $t_2(K) < 175$, but keeping only those fields with root discriminant bounded by 200. This computation (on a cluster at the Vermont Advanced Computing Center) ran for approximately 329 CPU days and produced 376 508 889 fields.

By (8.4) this yielded a complete list of all totally real quintic fields whose discriminant is at most 1 151 072 334 (root discriminant ≤ 64.89), and in addition yielded a large number of fields with larger discriminant (over 370 million, each with root discriminant at most 200).

As a check on the computations, we first compared our list of fields to the table of totally real fields with disciminant bounded by $2(10^7)$ (root discriminant ≤ 28.8540) computed by the PARI group [P]. The results agree except that there are 5 duplications in the PARI database (which lists 22740 fields):

i	d	f_1	f_2
8590	9262117	$x^5 - 10x^3 + x^2 + 13x - 6$	$x^5 - 26x^3 + 20x^2 + 10x + 1$
13372	13072837	$x^5 + x^4 - 18x^3 - 6x^2 + 28x + 17$	$x^5 + 2x^4 - 17x^3 - 6x^2 + 64x - 40$
15570	14731145	$x^5 + x^4 - 25x^3 - 25x^2 + 2x + 5$	$x^5 + x^4 - 20x^3 - 31x^2 + 23x + 1$
19853	17946025	$x^5 + 2x^4 - 17x^3 - 20x^2 + 10x + 5$	$x^5 + 2x^4 - 20x^3 - 17x^2 + 16x + 13$
20453	18371721	$x^5 - 31x^3 + 60x^2 + 16x + 1$	$x^5 + 2x^4 - 23x^3 - 47x^2 + 129x + 265$

(we list the numbers of the field $i, i+1$ in the PARI database, their common discriminant, and two (primitive) polynomials for the corresponding fields). The corrected total of 22735 fields is the same as the number of fields we computed.

We then compared our data to that of Malle [M1], who has computed all totally real fields with discriminant $\leq 10^9$. He reports that there are 2 341 960 such quintic fields. The number of fields and the collection of field discriminants reported by Malle are both the same as ours with the same discriminant bound.

For a fixed discriminant bound D, the count of fields for given values of $t_2(K)$ appear to be nearly normally distributed, with a mean on the order of $D^{1/4}$, as suggested by (8.3); this in turn suggests a cumulative count of fields should be approximated by an error function $\mathrm{erf}(t)$. A best-fit regression results in an error-function approximation that suggests among the 376 508 889 computed fields we have approximately 99% of totally real quintic fields with root discriminant at most 100, and perhaps a narrow majority of fields with root discriminant at most 200. The sampling in Table 6 was taken for discriminants bounded by 10^9 (for which our list of fields is complete), 10^{10} (root discriminant 100), and $3.2(10)^{11}$ (root discriminant 200), respectively.

Appendix A. Maximal totally isotropic subspaces of orthogonal direct sums over perfect fields of characteristic 2 (with Richard Foote)

Throughout this appendix, $\mathbb{F}$ denotes a perfect field of characteristic 2.

We first classify, up to isometry, the possible nondegenerate finite dimensional symmetric spaces over $\mathbb{F}$, and prove a version of Witt's Theorem for them. We then prove a structure theorem for the maximal totally isotropic subspaces of an orthogonal direct sum of two such spaces and derive a number of consequences. These results will be applied to number fields in Section 6.

Suppose V is a nontrivial n-dimensional vector space over $\mathbb{F}$ equipped with a nondegenerate symmetric bilinear form b. The map $v \mapsto b(v,v)$ from V to $\mathbb{F}$ is an $\mathbb{F}_2$-linear homomorphism and if $b(v,v) = \alpha \neq 0$ then, because $\mathbb{F}$ is perfect, there is a scalar multiple of v of any length β (namely γv where $\gamma^2 = \beta/\alpha$), so $v \mapsto b(v,v)$ is either the trivial map or is surjective. The set

$$V_{\mathrm{alt}} = \{v \in V \mid b(v,v) = 0\}$$

of isotropic elements of V is a canonical subspace, called the *alternating subspace* of V, and is of codimension at most 1.

Let H denote the hyperbolic plane over $\mathbb{F}$.

Proposition A.1. *If b is a nondegenerate symmetric bilinear form on the vector space V of dimension $n \geq 1$ over $\mathbb{F}$, then up to isometry precisely one of the following three cases can occur:*

(1) The form b is alternating, i.e., $V = V_{\mathrm{alt}}$. Then n is even and V is an orthogonal direct sum of $n/2$ hyperbolic planes.

(2) The form b is not alternating. Then there is an orthonormal basis for V and with respect to such a basis the form is the "dot product" on V. The element v_{can} given by the sum of the elements in any orthonormal basis is uniquely defined independent of the choice of orthonormal basis and $V_{\mathrm{alt}} = \langle v_{\mathrm{can}} \rangle^{\perp}$. There are two possible subcases:

(i) If n is odd, then V_{alt} is an orthogonal direct sum of $(n-1)/2$ hyperbolic planes; V is the orthogonal direct sum of V_{alt} and the one-dimensional space $\mathcal{D} = \langle v_{\mathrm{can}} \rangle$. The element v_{can} is the unique element of length 1 in V orthogonal to V_{alt}.

(ii) If n is even, then the form b restricted to the alternating subspace V_{alt} of codimension 1 is degenerate, with radical $\langle v_{\text{can}}\rangle$; V_{alt} is the orthogonal direct sum of $\langle v_{\text{can}}\rangle$ and a (noncanonical) subspace V'_{alt} that is the orthogonal direct sum of $n/2-1$ hyperbolic planes. The nondegenerate space $\mathcal{D} = (V'_{\text{alt}})^{\perp}$ is a two-dimensional space containing $\langle v_{\text{can}}\rangle$ and $\mathcal{D}$ is the direct sum $\langle v_1\rangle \oplus \langle v_{\text{can}}\rangle$ with any element $v_1 \in \mathcal{D}$ with $b(v_1, v_1) = 1$. The space V is the orthogonal direct sum of V'_{alt} and $\mathcal{D}$, so $V = (\langle v_1\rangle \oplus \langle v_{\text{can}}\rangle) \perp H^{n/2-1}$ and $V_{\text{alt}} = \langle v_{\text{can}}\rangle \perp H^{n/2-1}$.

Proof. Suppose first that b is nondegenerate and alternating. For any $0 \neq x \in V$, there is a $y \in V$ with $b(x, y) \neq 0$ since b is nondegenerate. Then the subspace $\langle x, y\rangle$ is a hyperbolic plane H. Since b restricted to $\langle x, y\rangle$ is nondegenerate, $V = \langle x, y\rangle \oplus \langle x, y\rangle^{\perp}$. Then b restricted to $\langle x, y\rangle^{\perp}$ is nondegenerate and alternating, so by induction V is the orthogonal direct sum of hyperbolic planes, which is (1) of the proposition.

Assume now that b is not alternating on V, so the alternating subspace V_{alt} is of codimension 1.

We first prove by induction that V has an orthonormal basis. This is clear if $\dim V = 1$. If $\dim V > 1$, then V contains at least two linearly independent elements of length 1 (for example, any element v_1 of length 1 together with $v_1 + v_0$ for any nonzero $v_0 \in V_{\text{alt}}$). Since $V_{\text{alt}}^{\perp}$ has dimension 1, it follows that there exists an element v in V of length 1 that is not contained in $V_{\text{alt}}^{\perp}$. Then $V = \langle\, v\,\rangle \perp \langle\, v\,\rangle^{\perp}$, and $\langle\, v\,\rangle^{\perp}$ is a subspace of dimension $n-1$ on which b is nondegenerate and nonalternating. By induction, there is an orthonormal basis for $\langle\, v\,\rangle^{\perp}$, which together with v gives an orthonormal basis for V.

Next, if $\{v_1, \ldots, v_n\}$ and $\{v'_1, \ldots, v'_n\}$ are two orthonormal bases for V, then they are related by an $n \times n$ orthogonal matrix $A = (a_{ij})$. Then $(a_{i1} + \cdots + a_{in})^2 = a_{i1}^2 + \cdots + a_{in}^2 = 1$ for any $i = 1, 2, \ldots, n$, so the row sums of A (and similarly, the column sums) are all 1. It follows that $v_1 + \cdots + v_n = v'_1 + \cdots + v'_n$ and so the sum of the elements in any orthonormal basis is the same. Also, if $\{v_1, \ldots, v_n\}$ is an orthonormal basis and $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, then $b(v, v) = \alpha_1^2 + \cdots + \alpha_n^2 = (\alpha_1 + \cdots + \alpha_n)^2 = b(v, v_{\text{can}})^2$. In particular, the elements of V_{alt} are those whose coordinates with respect to any orthonormal basis sum to 0, and $v \in V_{\text{alt}}$ if and only if $b(v, v_{\text{can}}) = 0$, i.e., $V_{\text{alt}} = \langle\, v_{\text{can}}\,\rangle^{\perp}$.

Suppose that n is odd. In this case $\langle\, v_{\text{can}}\,\rangle$ is nondegenerate, hence $V = \langle\, v_{\text{can}}\,\rangle \perp \langle\, v_{\text{can}}\,\rangle^{\perp} = \langle\, v_{\text{can}}\,\rangle \perp V_{\text{alt}}$. Also b restricted to $V_{\text{alt}} = \langle\, v_{\text{can}}\,\rangle^{\perp}$ is nondegenerate, so V_{alt} is the orthogonal direct sum of hyperbolic planes by case 1, which proves (2i).

Suppose that n is even. In this case $v_{\text{can}} \in V_{\text{alt}}$ and since $\langle\, v_{\text{can}}\,\rangle = V_{\text{alt}}^{\perp}$ it follows that b is degenerate on V_{alt} with a 1-dimensional radical: $\operatorname{rad} V_{\text{alt}} = \langle v_{\text{can}}\rangle$. Then b induces a nondegenerate alternating form on $V_{\text{alt}}/\langle v_{\text{can}}\rangle$, which is therefore the orthogonal direct sum of hyperbolic planes by (1). Taking any lift to V_{alt} gives a subspace V'_{alt} that is an orthogonal direct sum $H^{n/2-1}$ of hyperbolic planes. Since b restricts to a nondegenerate form on V'_{alt}, it follows that $(V'_{\text{alt}})^{\perp}$ is a two-dimensional space containing $\langle v_{\text{can}}\rangle$ and the remaining statements for (2ii) in the proposition follow, completing the proof. □

Remark A.2. If Q is a quadratic form with associated bilinear form b, then b is uniquely determined by Q via $b(x, y) = Q(x+y) - Q(x) - Q(y)$ (however, b does not uniquely determine Q, even if b is nondegenerate). Note that if b arises from a quadratic form in characteristic 2, then b must be alternating, so a symmetric bilinear form that is not alternating cannot come from a quadratic form—in particular the bilinear forms in (2) of the proposition do not arise from any quadratic form Q on V.

Remark A.3. We refer to the three 'types' of nondegenerate spaces in Proposition A.1: If V is alternating of dimension $2m$ then $V \simeq H_1 \perp H_2 \perp \cdots \perp H_m$ where $H_i = \langle e_i, f_i \rangle$ is a hyperbolic plane with hyperbolic basis $\{e_i, f_i\}$. If V is nonalternating with orthonormal basis $v_1, \ldots, v_n$ let $m = \lfloor n/2 \rfloor$; for $1 \le i \le m$ let $e_i = v_{2i-1} + v_{2i}$, and let $f_i = v_{2i} + \cdots + v_n$ (n odd) or $f_i = v_{2i} + \cdots + v_{n-1}$ (n even). Then $V \simeq H_1 \perp H_2 \perp \cdots \perp H_{m-1} \perp \mathcal{D}$ where $H_i = \langle e_i, f_i \rangle$ is a hyperbolic plane with hyperbolic basis $\{e_i, f_i\}$ and either (1) $\mathcal{D} = \langle v_{\text{can}} \rangle$ with $b(v_{\text{can}}, v_{\text{can}}) = 1$ if n is odd, or (2) $\mathcal{D} = \langle v_{\text{can}}, v_n \rangle$ with $b(v_{\text{can}}, v_{\text{can}}) = 0$, $b(v_{\text{can}}, v_n) = b(v_n, v_n) = 1$ if n is even.

Witt's Theorem. Since most versions of Witt's Theorem on lifting isometries require an alternating form when the field has characteristic 2 we include the following variant for each of the three nondegenerate symmetric bilinear forms that can occur. When the form b is not alternating, every isometry of V maps the canonical element v_{can} to itself, and the following shows this is the only obstruction to lifting isometries between subspaces.

Proposition A.4 (Witt's Theorem)**.** *Suppose V is a vector space of dimension $n \ge 1$ over a perfect field of characteristic 2 with a nondegenerate symmetric bilinear form b as in Proposition A.1.*

(1) Suppose b is alternating. Then every isometry from a subspace W to a subspace W' extends to an isometry of V.

(2) Suppose b is not alternating. Let v_{can} denote the sum of the elements in any orthonormal basis for V. Assume W and W' are subspaces of V with $W \cap \langle v_{\text{can}} \rangle = W' \cap \langle v_{\text{can}} \rangle$ (i.e., either both W and W' contain v_{can} or neither does). Then every isometry $\sigma : W \to W'$ that maps v_{can} to v_{can} if $v_{\text{can}} \in W, W'$, extends to an isometry of V.

Proof. The statement in (1) is the standard version of Witt's Theorem (cf. [Bour], Theorem 1, §4.3, p. 71).

For (2), suppose first that n is odd. We have $V = \langle v_{\text{can}} \rangle \perp V_{\text{alt}}$, so V_{alt} is subspace of codimension 1 with a nondegenerate alternating form. Now σ restricts to an isometry of the canonical subspaces W_{alt} to W'_{alt}. If W, hence also W', is contained in V_{alt}, then by (1) applied in the latter space, σ extends to an isometry of V_{alt}, and hence to an isometry of V by mapping v_{can} to itself. It remains to consider when W_{alt} is codimension one in W (and likewise for W'). In this case let $w_1, w_2, \ldots, w_d$ be a basis of W chosen so that $w_2, \ldots, w_d$ is a basis of W_{alt}, and let $w'_i = \sigma(w_i)$ for all i.

If $v_{\text{can}} \in W$, then we may choose $w_1 = v_{\text{can}}$ and so $w'_1 = v_{\text{can}}$ as well by hypothesis. As before, $\sigma : W_{\text{alt}} \to W'_{\text{alt}}$ extends to an isometry of V_{alt}, and since $\sigma(v_{\text{can}}) = v_{\text{can}}$, it also extends to an isometry of V.

If $v_{\text{can}} \notin W$, consider the subspaces obtained by replacing w_1 by $w_1 + v_{\text{can}}$ and w'_1 by $w'_1 + v_{\text{can}}$ in the bases for W and W'; these two new subspaces both lie in V_{alt}. Since v_{can} is orthogonal to V_{alt}, the isomorphism defined by mapping $w_1 + v_{\text{can}}$ to $w'_1 + v_{\text{can}}$ and $w_i \mapsto w'_i$ for $2 \le i \le d$ is an isometry of these new subspaces, hence by what has previously been shown extends to an isometry of V. Any isometry of V necessarily fixes v_{can}, hence this isometry maps w_1 to w'_1, i.e., it is an extension of the original σ, completing the proof for n odd.

Suppose now that n is even. Embed V into the $(n+1)$-dimensional space $V_1 = V \oplus \langle v_{n+1} \rangle$, and extend b to V_1 by defining $b(v_{n+1}, v_{n+1}) = 1$ and $b(v, v_{n+1}) = b(v_{n+1}, v) = 0$ for $v \in V$. Then $V_1 = V \perp \langle v_{n+1} \rangle$ and V_1 is a nondegenerate nonalternating space with an orthonormal basis consisting of an orthonormal basis for V together with v_{n+1}. If $v_{1,\text{can}}$ is the canonical

vector for V_1, it follows that $v_{1,\mathrm{can}} = v_{\mathrm{can}} + v_{n+1}$. Let $W_1 = W \perp \langle\, v_{n+1} \,\rangle$ and $W_1' = W' \perp \langle\, v_{n+1} \,\rangle$. Then either both W_1 and W_1' contain $v_{1,\mathrm{can}}$ or neither does. Define $\sigma_1 : W_1 \to W_1'$ by $\sigma_1(w + \alpha v_{n+1}) = \sigma(w) + \alpha v_{n+1}$ for $w \in W$ and $\alpha \in \mathbb{F}$. Then σ_1 is an isometry from W_1 to W_1' that maps $v_{1,\mathrm{can}}$ to $v_{1,\mathrm{can}}$ if $v_{1,\mathrm{can}} \in W_1, W_1'$. By what has already been proved for odd n, σ_1 extends to an isometry $\widetilde{\sigma_1}$ of V_1 that in particular maps v_{n+1} to itself. Since $\langle\, v_{n+1} \,\rangle^{\perp} = V$, the restriction of $\widetilde{\sigma_1}$ to $\langle\, v_{n+1} \,\rangle^{\perp}$ is an isometry of V that extends σ, completing the proof. □

Remark A.5. Not every isometry of subspaces extends to an isometry of V when b is not alternating, as shown by the example $W = \langle v \rangle$ and $W' = \langle v' \rangle$ and the map $\sigma(v) = v'$ where $v = v_{\mathrm{can}}$ and v' is a vector of length 1 other than v_{can} when n is odd (respectively, of length 0 other than v_{can} when n is even).

Orders of Isometry Groups. We give the orders of some isometry groups and subspace stabilizers in the case when $\mathbb{F} = \mathbb{F}_q$ is a finite field of characteristic 2. First consider when V is nondegenerate of dimension $n = 2m$ with an alternating form, or of dimension $n = 2m+1$ with a nonalternating form. In both cases the group of isometries of V is

$$\mathrm{Aut}(V) \simeq \mathrm{Aut}(V_{\mathrm{alt}}) \simeq Sp_{2m}(q).$$

The stabilizer, P_U, of a totally isotropic subspace U of V is a maximal parabolic subgroup, and its structure is well known (and explicitly described in [Wil, Section 3.5.5]). In particular, P_U contains a Borel (2-Sylow) subgroup of $\mathrm{Aut}(V)$, and the odd part of $\#P_U$ is the same as that of its Levi factor, $GL_k(q) \times Sp_{2m-2k}(q)$, where $k = \dim U$.

When V has dimension $n = 2m$ with a nonalternating form, embed V as a subspace of codimension 1 in $V_1 = V \perp \langle\, v_{n+1} \,\rangle$ where v_{n+1} has length 1, and let $v_{1,\mathrm{can}}$ denote the canonical element in V_1. Since $V = \langle\, v_{n+1} \,\rangle^{\perp}$, the isometries of V are the isometries of V_1 that fix v_{n+1}. Now $\mathrm{Aut}(V_1) = \mathrm{Aut}(V_{1,\mathrm{alt}})$, and under this identification the isometries that fix v_{n+1} are those that fix $v_{n+1} + v_{1,\mathrm{can}} \in V_{1,\mathrm{alt}}$. This is the normal subgroup of index $q-1$ in the maximal parabolic subgroup of $\mathrm{Aut}(V_{1,\mathrm{alt}})$ fixing the 1-dimensional space $\langle\, v_{n+1} + v_{1,\mathrm{can}} \,\rangle$. By [Wil], the group of isometries of V is

$$\mathrm{Aut}(V) \simeq E \cdot Sp_{2m-2}(q) \qquad \text{where } E \simeq (\mathbb{F}_q)^{n-1} \text{ as an additive abelian group}$$

(note the slight misstatement in [Wil]: E is abelian, not special, in characteristic 2). The stabilizer of any totally isotropic subspace U of dimension k in V also stabilizes the subspace $U_1 = \langle\, U, v_{\mathrm{can}} \,\rangle$, which has dimension $k_1 = k$ or $k+1$. The stabilizer in $\mathrm{Aut}(V)$ of U_1 is E together with a maximal parabolic subgroup stabilizing a (k_1-1)-dimensional totally isotropic space in $Sp_{2m-2}(q)$, for $1 \le k_1 \le m$. If $v_{\mathrm{can}} \in U$, i.e., $U = U_1$, this gives the order of the stabilizer of U. Otherwise U is a complement to $\langle\, v_{\mathrm{can}} \,\rangle$ in U_1. Since, by Witt's Theorem, all such complements are isometric under the action of the stabilizer of U_1 in V, and since there are q^k of them, the stabilizer of U has index q^k in the stabilizer of U_1.

For our purposes only the orders of these stabilizers will be required and we summarize the results needed in the following proposition. The results of the proposition may also be obtained directly by somewhat tedious but elementary counting arguments (e.g., when V is alternating, completing a basis for U to a hyperbolic basis for V and computing the possible images of the basis elements, etc.). The transitivity statements in the proposition are immediate from Witt's Theorem A.4.

Proposition A.6. *Suppose V is vector space of dimension $n \geq 1$ over the finite field $\mathbb{F}_q$ of characteristic 2 with a nondegenerate symmetric bilinear form b, let $\mathrm{Aut}(V)$ be the group of isometries of V, and for any subspace U of V let $\mathrm{Aut}(V,U)$ be the stabilizer of U in $\mathrm{Aut}(V)$.*

1. *Suppose b is alternating, so $n = 2m$ is even. Then $\mathrm{Aut}(V)$ is transitive on the set of totally isotropic subspaces U of dimension k and for such a U*
$$\#\mathrm{Aut}(V,U) = q^{m^2} \prod_{i=1}^{k} (q^i - 1) \prod_{i=1}^{m-k} (q^{2i} - 1).$$
In particular ($k = 0$), $\#\mathrm{Aut}(V) = q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1)$.
2. *(i) Suppose b is not alternating and $n = 2m + 1$ is odd. Then $\mathrm{Aut}(V)$ is transitive on the set of totally isotropic subspaces U of dimension k and for such a U*
$$\#\mathrm{Aut}(V,U) = q^{m^2} \prod_{i=1}^{k} (q^i - 1) \prod_{i=1}^{m-k} (q^{2i} - 1).$$
In particular ($k = 0$), $\#\mathrm{Aut}(V) = q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1)$.
(ii) Suppose b is not alternating, $n = 2m$ is even, and v_{can} is the unique nonzero element in the radical of the alternating subspace of V. Then
   (a) $\mathrm{Aut}(V)$ is transitive on the set of totally isotropic subspaces U of dimension k with $v_{\mathrm{can}} \in U$ and for such a U
$$\#\mathrm{Aut}(V,U) = q^{m^2} \prod_{i=1}^{k-1} (q^i - 1) \prod_{i=1}^{m-k} (q^{2i} - 1);$$
   (b) $\mathrm{Aut}(V)$ is transitive on the set of totally isotropic subspaces U of dimension k with $v_{\mathrm{can}} \notin U$ and for such a U
$$\#\mathrm{Aut}(V,U) = q^{m^2-k} \prod_{i=1}^{k} (q^i - 1) \prod_{i=1}^{m-k-1} (q^{2i} - 1).$$
In particular (either $k = 1$ in (a) or $k = 0$ in (b)), $\#\mathrm{Aut}(V) = q^{m^2} \prod_{i=1}^{m-1} (q^{2i} - 1)$.

Maximal Totally Isotropic Subspaces of Orthogonal Direct Sums. In this subsection we prove the main result of this appendix, Theorem A.13, describing the structure of the maximal totally isotropic subspaces of an orthogonal direct sum of two nondegenerate symmetric spaces as in Proposition A.1.

For the remainder of this subsection, W is a vector space over $\mathbb{F}$ of dimension $n \geq 1$ with a nondegenerate symmetric bilinear form b, and W' is a vector space over $\mathbb{F}$ of dimension $n' \geq 1$ with a nondegenerate symmetric bilinear form b', where we make the additional assumption that n and n' have the same parity.

The form $B = b \perp b'$ defines a nondegenerate form on the orthogonal direct sum $V = W \perp W'$ of even dimension $n+n'$: $B(w_1 + w_1', w_2 + w_2') = b(w_1, w_2) + b'(w_1', w_2')$. We identify $W = W \perp 0$ as a subspace of V, and similarly for W'.

Suppose S is a maximal totally isotropic subspace of $V = W \perp W'$. Let U denote the totally isotropic subspace $S \cap W$ and similarly let $U' = S \cap W'$. Suppose U has dimension k and let $U^{\perp}$ denote the subspace of elements of W orthogonal to U; similarly suppose U' has dimension k' with orthogonal subspace $(U')^{\perp}$ in W'.

Since U is totally isotropic, $U = \text{rad}\,(U^\perp)$. If $\mathcal{K}$ is any vector space complement for U in $U^\perp$ it follows that $\mathcal{K} \simeq U^\perp/\text{rad}\,(U^\perp)$ is a nondegenerate space whose type is independent of the complement chosen, that $\dim \mathcal{K} = n - 2k$, and that $U^\perp = U \perp \mathcal{K}$. Similarly, for any vector space complement $\mathcal{K}'$ for U' in $(U')^\perp$ we have $(U')^\perp = U' \perp \mathcal{K}'$ and $\mathcal{K}'$ is nondegenerate of dimension $n' - 2k'$ whose type is independent of the complement chosen. Because n and n' have the same parity, the same is true for $\dim \mathcal{K}$ and $\dim \mathcal{K}'$.

The subspace of elements of the full space V that are orthogonal to U is $U \perp \mathcal{K} \perp W'$, with a similar statement for U'. Since S is totally isotropic and contains U and U', S is contained in the intersection of these orthogonal complements, so we obtain

$$U \perp U' \subseteq S \subseteq U \perp \mathcal{K} \perp \mathcal{K}' \perp U'. \tag{A.7}$$

It follows immediately that

$$S = U \perp \widetilde{S} \perp U' \tag{A.8}$$

where $\widetilde{S} = S \cap (\mathcal{K} \perp \mathcal{K}')$.

Since S is maximal totally isotropic in V, $\widetilde{S}$ must be maximal totally isotropic in $\mathcal{K} \perp \mathcal{K}'$. Also $\widetilde{S} \cap \mathcal{K}$ is contained in $S \cap W = U$, so $U \cap \mathcal{K} = 0$ implies $\widetilde{S} \cap \mathcal{K} = 0$ and similarly $\widetilde{S} \cap \mathcal{K}' = 0$.

Lemma A.9. *Suppose $\mathcal{K}$ and $\mathcal{K}'$ are nondegenerate spaces whose dimensions have the same parity and $\widetilde{S}$ is a maximal totally isotropic space of $\mathcal{K} \perp \mathcal{K}'$ that satisfies $\widetilde{S} \cap \mathcal{K} = \widetilde{S} \cap \mathcal{K}' = 0$. Then $\mathcal{K}$ and $\mathcal{K}'$ are isometric, and there is a unique isometry $\tau : \mathcal{K} \to \mathcal{K}'$ such that*

$$\widetilde{S} = \{w + \tau w \mid w \in \mathcal{K}\}.$$

In particular, $\dim \mathcal{K} = \dim \mathcal{K}' = \dim \widetilde{S}$.

Proof. Suppose $\dim \mathcal{K} = a$ and $\dim \mathcal{K}' = b$ where a and b have the same parity. Since $\widetilde{S}$ is a maximal totally isotropic subspace we have $\dim \widetilde{S} = (a+b)/2$. The canonical projection of $\widetilde{S}$ to $\mathcal{K}$ is injective since $\widetilde{S} \cap \mathcal{K} = 0$, so $\dim \widetilde{S} \leq \dim \mathcal{K}$, and similarly for $\mathcal{K}'$, so $\dim \widetilde{S} \leq \min(a, b)$. Together these yield

$$\dim \widetilde{S} = (a + b)/2 \geq \min(a, b) \geq \dim \widetilde{S},$$

which implies that equality holds throughout, and that $a = b$ since a and b have the same parity. Hence $\dim \mathcal{K} = \dim \mathcal{K}' = \dim \widetilde{S}$ and the canonical projections of $\widetilde{S}$ to $\mathcal{K}$ and to $\mathcal{K}'$ are isomorphisms. It follows that for each $w \in \mathcal{K}$ there is a unique $w' \in \mathcal{K}'$ with $w + w' \in \widetilde{S}$. Since $\widetilde{S}$ is a subspace, the resulting map $\tau : \mathcal{K} \to \mathcal{K}'$ mapping w to w' is an isomorphism of vector spaces over $\mathbb{F}$ and $\widetilde{S} = \{w + \tau w \mid w \in \mathcal{K}\}$. Finally, if $s_1 = w_1 + w_1'$ and $s_2 = w_2 + w_2'$ with $w_1, w_2 \in \mathcal{K}$, $w_1', w_2' \in \mathcal{K}'$ are two elements in the totally isotropic space $\widetilde{S}$ then $0 = B(s_1, s_2) = b(w_1, w_2) + b'(w_1', w_2')$. Hence $b(w_1, w_2) = b'(\tau(w_1), \tau(w_2))$ for all $w_1, w_2 \in \mathcal{K}$, i.e., τ is an isometry. □

Since n and n' have the same parity, so do $\dim \mathcal{K} = n - 2k$ and $\dim \mathcal{K}' = n' - 2k'$, hence by the lemma, the complements $\mathcal{K}$ and $\mathcal{K}'$ in (A.7) and (A.8) are isometric. This implies the dimensions of U and U' are related by $n - n' = 2(k - k')$, and that there is a compatibility constraint imposed on U and U' to ensure $\mathcal{K} \simeq U^\perp/\text{rad}\,(U^\perp)$ and $\mathcal{K}' \simeq (U')^\perp/\text{rad}\,((U')^\perp)$ are of the same type.

Remark A.10. As previously noted, the type of the nondegenerate space $\mathcal{K}$ is independent of the vector space complement chosen. Explicitly:

(a) if W is alternating, then $\mathcal{K}$ is alternating,
(b) if W is of odd dimension, then $\mathcal{K}$ is nonalternating of odd dimension, and
(c) if W is nonalternating of even dimension, then $\mathcal{K}$ has even dimension and is alternating if and only if $w_{\text{can}} \in U$.

The reason for (c) is that, since U is always contained in W_{alt}, the even dimensional space $\mathcal{K}$ is contained in W_{alt} if and only if $U^\perp = U \perp \mathcal{K} \subseteq W_{\text{alt}} = \langle\, w_{\text{can}} \,\rangle^\perp$, i.e., $\mathcal{K}$ is alternating if and only if $w_{\text{can}} \in U$. There are similar statements for the spaces U' and $\mathcal{K}'$ in W'.

Definition A.11. The totally isotropic subspaces U of W and U' of W' will be said to have compatible isotropy types if they satisfy the condition that rad $(W_{\text{alt}}) \subseteq U$ if and only if rad $(W'_{\text{alt}}) \subseteq U'$.

Remark A.12. If $W = W'$, the content of the statement that U_1 and U_2 have compatible isotropy types is that, in the case when W is nonalternating of even dimension, either both U_1 and U_2 contain w_{can} or both do not. As such, in the situation $W = W'$ we shall say that the totally isotropic subspaces U_1 and U_2 of W have the *same isotropy type*.

With these preliminaries we have the following structure theorem for maximal totally isotropic subspaces of orthogonal direct sums.

Theorem A.13 (Structure Theorem)**.** *Let S be a maximal totally isotropic subspace of $V = W \perp W'$ as above, with $U = S \cap W$ of dimension k and $U' = S \cap W'$ of dimension k'. Then*

(a) $n - n' = 2(k - k')$,
(b) U and U' have compatible isotropy types,

and $S = U \perp \widetilde{S} \perp U'$ where $\widetilde{S}$ is a diagonal subspace of $\mathcal{K} \perp \mathcal{K}'$:

$$\widetilde{S} = \{w + \tau w \mid w \in \mathcal{K}\}$$

for a unique isometry $\tau : \mathcal{K} \to \mathcal{K}'$ from a vector space complement, $\mathcal{K}$, for U in $U^\perp$ to a vector space complement, $\mathcal{K}'$, for U' in $(U')^\perp$.

Conversely, if U is a totally isotropic subspace of W of dimension k and U' is a totally isotropic subspace of W' of dimension k' satisfying (a) and (b) then there exist precisely $\#\text{Aut}(\mathcal{K})$ maximal totally isotropic subspaces S with $S \cap W = U$ and $S \cap W' = U'$, where $\mathcal{K}$ is any vector space complement for U in $U^\perp$.

Proof. The equality in (a) was noted previously. For (b), if W and W' are both nonalternating of even dimension, then the statement that the isometric subspaces $\mathcal{K}$ and $\mathcal{K}'$ are both alternating or both nonalternating is the statement that $w_{\text{can}} \in U$ if and only if $w'_{\text{can}} \in U'$, i.e., U and U' have compatible isotropy types. The other cases to verify for (b) are checked similarly. The decomposition statement for S follows from (A.8) and Lemma A.9.

For the converse, let $\mathcal{K}$ be any vector space complement to U in the subspace $U^\perp$ and define $\mathcal{K}'$ similarly for U'. Since $\mathcal{K} \simeq U^\perp/\text{rad}\,(U^\perp)$, $\mathcal{K}$ is nondegenerate, as is $\mathcal{K}'$. By (a), $\dim \mathcal{K} = \dim \mathcal{K}'$ and by (b) the spaces have the same type, so there is an isometry $\tau : \mathcal{K} \to \mathcal{K}'$. Then the diagonal subspace $\widetilde{S} = \{w + \tau w \mid w \in \mathcal{K}\}$ is totally isotropic and $S = U \perp \widetilde{S} \perp U'$ is a maximal totally isotropic subspace of V with $S \cap W = U$ and $S \cap W' = U'$.

From the containments in (A.7), the subspaces S correspond bijectively with the totally isotropic diagonal subspaces of the quotient $(U^\perp \perp (U')^\perp)/(U \perp U')$, which is isometric with $\mathcal{K} \perp \mathcal{K}'$ for any complements $\mathcal{K}$ and $\mathcal{K}'$, and, by Lemma A.9 there are $\#\mathrm{Aut}(\mathcal{K})$ such subspaces. □

By Witt's Theorem, the group of isometries $\mathrm{Aut}(W)$ acts transitively on the totally isotropic subspaces U of any fixed dimension k and isotropy type, as does $\mathrm{Aut}(W')$ on the totally isotropic subspaces U' of dimension $k' = k + (n' - n)/2$ of given isotropy type. Fix such a subspace U of W and a compatible U' of W'.

As we have seen, any two vector space complements $\mathcal{K}_1$ and $\mathcal{K}_2$ for U in $U^\perp$ are isometric and any isometry from $\mathcal{K}_1$ to $\mathcal{K}_2$ together with the identity map on U defines an isometry of $U^\perp$ to itself, which can then be extended to an isometry of W by Witt's Theorem. Similarly, there is an isometry of W' that is the identity on U' and extends any given isometry of one complement for U' in $(U')^\perp$ to another. In particular, if $\tilde{S}_1 = \{k + \tau_1(k) \mid k \in \mathcal{K}\}$ and $\tilde{S}_2 = \{k + \tau_2(k) \mid k \in \mathcal{K}\}$ are two diagonal subspaces of $\mathcal{K} \perp \mathcal{K}'$ as in Theorem A.13, then the isometry $\tau_2\tau_1^{-1}$ of $\mathcal{K}'$ can be extended to an isometry σ' of W' that stabilizes (in fact, can be taken to be the identity on) U'. Then $1 \perp \sigma' \in \mathrm{Aut}(W, U) \perp \mathrm{Aut}(W', U')$ is an isometry from $U \perp \tilde{S}_1 \perp U'$ to $U \perp \tilde{S}_2 \perp U'$.

Combined with Theorem A.13 these observations give us the following.

Corollary A.14. *Under the action of* $\mathrm{Aut}(W, U) \perp \mathrm{Aut}(W', U')$ *there is a single orbit of maximal totally isotropic subspaces* S *having* $S \cap W = U$ *and* $S \cap W' = U'$*; this orbit has size* $\#\mathrm{Aut}(\mathcal{K})$ *where* $\mathcal{K}$ *is any vector space complement for* U *in* $U^\perp$*.*

Under the action of the group $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ *there is a single orbit of maximal totally isotropic subspaces* S *in Theorem A.13 having the same* k *(so the same* k'*), the same isotropy type for* U*, and the same (compatible) isotropy type for* U'*.*

Corollary A.15. *If* $\mathbb{F} = \mathbb{F}_q$ *is a finite field of characteristic 2, then the order of the group of isometries in* $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ *that stabilize a maximal totally isotropic subspace* S *as in Theorem A.13 is given by*

$$\#\mathrm{Aut}(S) = \frac{\#\mathrm{Aut}(W, U)\#\mathrm{Aut}(W', U')}{\#\mathrm{Aut}(\mathcal{K})} \tag{A.16}$$

with orders of the isometry groups in (A.16) *given by Proposition A.6 and Remark A.10.*

Proof. Any isometry in $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ that stabilizes S also stabilizes $S \cap W$ and $S \cap W'$, so is an element of the subgroup $\mathrm{Aut}(W, U) \perp \mathrm{Aut}(W', U')$. The index of the stabilizer of S in this latter group is $\#\mathrm{Aut}(\mathcal{K})$ by Corollary A.14, giving (A.16). □

By Theorem A.13 the maximal totally isotropic subspaces S of $W \perp W'$ correspond to compatibly isotropic subspaces U and U' of suitable dimensions, and by Corollary A.14, there is a unique S up to equivalence under $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ if there is one. It remains to make explicit when, given a totally isotropic subspace U of W, there is a subspace U' of W' with a compatible isotropy type.

Without loss, we may assume that $\dim W \leq \dim W'$.

Corollary A.17. *Suppose* $\dim W = n \leq n' = \dim W'$. *For the five possible types for pairs of spaces* W, W', *the compatible isotropy constraint and the number of equivalence classes under* $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ *of maximal totally isotropic subspaces of* $W \perp W'$ *are the following:*

(i) W *alternating,* W' *alternating: no constraint. There is one equivalence class for each* k *with* $0 \leq k \leq n/2$.

(ii) W *nonalternating and* n *even,* W' *alternating:* $w_{\mathrm{can}} \in U$. *There is one equivalence class for each* k *with* $1 \leq k \leq n/2$

(iii) W *alternating,* W' *nonalternating and* n' *even:* $w'_{\mathrm{can}} \in U'$. *If* $n = n'$ *there is one equivalence class for each* k *with* $1 \leq k \leq n/2$. *If* $n < n'$ *there is one equivalence class for each* k *with* $0 \leq k \leq n/2$.

(iv) W *nonalternating and* n *even,* W' *nonalternating and* n' *even:* $w_{\mathrm{can}} \in U$ *if and only if* $w'_{\mathrm{can}} \in U'$. *There is one equivalence class for* $k = 0$, *there are two equivalence classes for each* k *with* $0 < k < n/2$ *(one class with* $w_{\mathrm{can}} \in U$ *and* $w'_{\mathrm{can}} \in U'$ *and one class with* $w_{\mathrm{can}} \notin U$ *and* $w'_{\mathrm{can}} \notin U'$*), and there is one equivalence class with* $k = n/2$.

(v) W *nonalternating and* n *odd,* W' *nonalternating and* n' *odd: no constraint. There is one equivalence class for each* k *with* $0 \leq k \leq (n-1)/2$.

Proof. This is straightforward. For example, the compatibility condition in (ii) is that $w_{\mathrm{can}} \in U$ if and only if $0 \in U'$, i.e., simply that $w_{\mathrm{can}} \in U$, and in this case k must be at least 1 and at most $n/2$ since U is totally isotropic. The remaining cases are similar. □

Remark A.18. The results of Corollary A.17 show there is a 'reciprocity' between the $\mathrm{Aut}(W)$ equivalence class of a totally isotropic subspace U of W and the unique $\mathrm{Aut}(W')$ equivalence class of a compatibly isotropic subspace U' of W'; the subspaces U and U' are 'linked' through a maximal totally isotropic subspace S of $W \perp W'$. Note also that, while Corollary A.17 was stated for $\dim W \leq \dim W'$, this reciprocity is completely symmetric in W and W'.

By the second statement in Corollary A.14, when $\mathbb{F} = \mathbb{F}_q$ is a finite field of characteristic 2 each equivalence class in Corollary A.17 has size

$$\frac{\#\mathrm{Aut}(W)\#\mathrm{Aut}(W')}{\#\mathrm{Aut}(S_i)} \tag{A.19}$$

where S_i is any representative for the equivalence class and $\mathrm{Aut}(S_i)$ is the subgroup of isometries in $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ that stabilize S_i. By Corollary A.15 this expression is

$$\frac{\#\mathrm{Aut}(W)}{\#\mathrm{Aut}(W,U)}\,\#\mathrm{Aut}(\mathcal{K})\,\frac{\#\mathrm{Aut}(W')}{\#\mathrm{Aut}(W',U')} \tag{A.20}$$

for an appropriate U and compatibly isotropic U' and with $\mathcal{K}$ any vector space complement to U in $U^{\perp}$. These equivalence classes partition the set of all maximal totally isotropic subspaces S of $V = W \perp W'$, so the sum of these orders for any of the five cases in Corollary A.17 is the total number of maximal totally isotropic subspaces of $V = W \perp W'$. Since any two maximal totally isotropic subspaces are trivially isometric (by any vector space isomorphism) and since $\mathrm{Aut}(V)$ is transitive on the set of spaces S by Witt's Theorem, this total is $\#\mathrm{Aut}(V)/\#\mathrm{Aut}(V,S)$. This yields a "mass formula" for the action of $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$

on these spaces:

$$\sum_i \frac{1}{\#\mathrm{Aut}(S_i)} = \frac{\#\mathrm{Aut}(V)}{\#\mathrm{Aut}(V,S)\#\mathrm{Aut}(W)\#\mathrm{Aut}(W')} \tag{A.21}$$

where the sum is extended over representatives S_i of the equivalence classes of maximal totally isotropic subspaces of V as in Corollary A.14, and S is any maximal totally isotropic subspace of V.

The following corollary gives the mass formula explicitly in the case where n and n' are odd (so both W and W' are nonalternating); this is the case of particular interest in the applications in Sections 6 and 7 (see Theorem 6.7). The mass formula in the other cases can be handled similarly.

Corollary A.22. *Suppose $\mathbb{F} = \mathbb{F}_q$ is a finite field of characteristic 2 and suppose W and W' are both nonalternating where n, n' are odd, $n \le n'$. For $0 \le k \le \lfloor n/2 \rfloor$ let S_k be a maximal totally isotropic subspace of $V = W \perp W'$ with $k = \dim(S_k \cap W)$ as in Corollary A.17. Then the number of isometries in $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ stabilizing S_k is*

$$\#\mathrm{Aut}(S_k) = q^{(n'-1)^2/4+k(n-k-1)} \prod_{i=1}^{k}(q^i-1) \prod_{i=1}^{k+(n'-n)/2}(q^i-1) \prod_{i=1}^{(n-1)/2-k}(q^{2i}-1) \tag{A.23}$$

and

$$\sum_{k=0}^{(n-1)/2} \frac{1}{\#\mathrm{Aut}(S_k)} = \frac{\prod_{i=1}^{(n+n')/2-1}(q^i+1)}{q^{(n-1)^2/4+(n'-1)^2/4}\prod_{i=1}^{(n-1)/2}(q^{2i}-1)\prod_{i=1}^{(n'-1)/2}(q^{2i}-1).} \tag{A.24}$$

Proof. Let $U = S_k \cap W$ and $U' = S_k \cap W'$ as in Theorem A.13, so that $k = \dim U$ and $k' = \dim U'$ with $n - n' = 2(k - k')$. Since $n = 2m+1$ and $n' = 2m'+1$ are odd, (2)(i) of Proposition A.6 gives

$$\#\mathrm{Aut}(W,U) = q^{m^2}\prod_{i=1}^{k}(q^i-1)\prod_{i=1}^{m-k}(q^{2i}-1), \quad \#\mathrm{Aut}(W',U') = q^{m'^2}\prod_{i=1}^{k'}(q^i-1)\prod_{i=1}^{m'-k'}(q^{2i}-1). \tag{A.25}$$

A vector space complement $\mathcal{K}$ for U in $U^\perp \subseteq W$ has dimension $n - 2k = 2(m-k)+1$ and is nonalternating (cf. Remark A.10), so again by (2)(i) of Proposition A.6 we have

$$\#\mathrm{Aut}(\mathcal{K}) = q^{(m-k)^2}\prod_{i=1}^{m-k}(q^{2i}-1). \tag{A.26}$$

By (A.20), $\#\mathrm{Aut}(S_k)$ is the product of the two orders in (A.25) divided by the order in (A.26), which simplifies to give the first statement in the corollary.

In the case under consideration, $V = W \perp W'$ is nonalternating of even dimension $n+n'$; any maximal totally isotropic S contains v_{can} and has dimension $(n+n')/2$, so by (2)(ii)(a) and (2)(i) of Proposition A.6 we have

$$\#\mathrm{Aut}(V) = q^{(n+n')^2/4}\prod_{i=1}^{(n+n')/2-1}(q^{2i}-1), \qquad \#\mathrm{Aut}(V,S) = q^{(n+n')^2/4}\prod_{i=1}^{(n+n')/2-1}(q^i-1),$$

$$\#\mathrm{Aut}(W) = q^{(n-1)^2/4}\prod_{i=1}^{(n-1)/2}(q^{2i}-1), \qquad \#\mathrm{Aut}(W') = q^{(n'-1)^2/4}\prod_{i=1}^{(n'-1)/2}(q^{2i}-1).$$

Using these orders for the right hand side of (A.21) and simplifying the result gives the second equality of the corollary. □

Finally, we indicate how to construct a representative totally isotropic space S for each of the possible equivalence classes delineated in Corollary A.17. This is straightforward using the explicit descriptions in Remark A.3, as follows.

For each dimension k in Corollary A.17, take a totally isotropic subspace U of dimension k in W: either $U = \langle e_1, e_2, \dots, e_k \rangle$ or $U = \langle e_1, e_2, \dots, e_{k-1}, w_{\text{can}} \rangle$, depending on whether $w_{\text{can}} \in U$ or not, as appropriate. Then one vector space complement $\mathcal{K}$ for U in $U^\perp$ has a basis obtained by taking the basis for W in Remark A.3 and removing the elements $e_1, f_1, \dots, e_k, f_k$ (if $U = \langle e_1, e_2, \dots, e_k \rangle$) or the elements $e_1, f_1, \dots, e_{k-1}, f_{k-1}, w_{\text{can}}, v_n$ (if $U = \langle e_1, e_2, \dots, e_{k-1}, w_{\text{can}} \rangle$).

Similarly take a totally isotropic subspace U' of W' of dimension $k' = k + (n' - n)/2$ (satisfying any compatible isotropy constraint with U required by Corollary A.17) and construct a vector space complement $\mathcal{K}'$ for U' in $(U')^\perp$.

The complements $\mathcal{K}$ and $\mathcal{K}'$ will be isometric vector spaces, and it is elementary to construct an explicit isometry τ since their bases are compatible with the description in Proposition A.1 and Remark A.3. Then τ defines a totally isotropic diagonal $\widetilde{S}$ which together with U and U' gives a maximal totally isotropic subspace S with $S \cap W = U$ and $S \cap W' = U'$.

Remark A.27. The development here considered the case when $\dim W$ and $\dim W'$ have the same parity since this is the situation that arises in the number field applications. When $\dim W$ and $\dim W'$ have opposite parity there are two cases: (1) one of the spaces is alternating, in which case the results follow immediately by applying the results here to the alternating subspace of $W \perp W'$, and (2) both W and W' are nonalternating, and in this case the development here is easily modified. For example, the decomposition (A.8) still holds, the proof of Lemma A.9 shows that $\dim \mathcal{K}$ and $\dim \mathcal{K}'$ differ by one, and if $\dim \mathcal{K}' = \dim \mathcal{K} + 1$, the diagonal subspaces $\widetilde{S}$ of $\mathcal{K} \perp \mathcal{K}'$ correspond to the isometries τ from $\mathcal{K}$ to a nondegenerate subspace $\mathcal{K}'_0$ of codimension 1 in $\mathcal{K}'$. The number of diagonal subspaces is then $\#\text{Aut}(\mathcal{K})$ times the number of possible $\mathcal{K}'_0$, which can easily be computed (e.g., by counting their orthogonal complements). There are similar extensions of the other results. We omit the details.

References

[A-M] Adam, M., Malle, G.: *A class group heuristic based on the distribution of* 1*-eigenspaces in matrix groups*, J. Number Theory **149** (2015), 225–235.

[A-F] Armitage, J.V., Fröhlich, A.: *Class numbers and unit signatures*, Mathematika **14** (1967), 94–98.

[Bel] Belabas, K.: *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237.

[Bha1] Bhargava, M.: *Gauss composition and generalizations*, Algorithmic number theory (ANTS V, Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, 1–8.

[Bha2] Bhargava, M.: *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591.

[Bha3] Bhargava, M.: *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), no. 1, 53–94.

[Bha4] Bhargava, M.: *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[BKLPR] Bhargava, M., Kane, D. M., Lenstra, H.W., Jr., Poonen, B., and Rains, E.: *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275-321.

[BST] Bhargava, M., Shankar, A., and Tsimerman, J.: *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499.

[B-V] Bhargava, M., Varma, I.: *On the mean number of* 2*-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields*, Duke Math. J. **164** (2015), 1911–1933.

[BCP] Bosma, W., Cannon, J., and Playoust, C., *The Magma algebra system. I. The user language.*, J. Symbolic Comput., **24** (3–4), 1997, 235–265.

[Bour] Bourbaki, N.: Éléments de Mathématique, Algèbre, Chapitre 9, Springer-Verlag, 2007.

[Br] Breen, B.: *Class groups and unit groups in* S_n*-fields of even degree*, Dartmouth Ph.D. thesis, forthcoming.

[Co1] Cohen, H.: A Course in Computational Algebraic Number Theory, second corrected printing, GTM 138, Springer-Verlag, 1995.

[Co2] Cohen, H.: Advanced Topics in Computational Number Theory, GTM 193, Springer-Verlag, 2000.

[C-L] Cohen, H. and Lenstra, H.W.: *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, 33–62.

[C-M] Cohen, H. and Martinet, J.: *Étude heuristique des groupes de classes des corps de nombres*, J. reine angew. Math. **404** (1990), 39–76.

[Cohn] H. Cohn, H., *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476-477.

[D-H] Davenport, H. and Heilbronn, H.: *On the density of discriminant of cubic fields. II*, Proc. Roy. Soc. London A **322** (1971), 405–420.

[D-F] Delone, B. N. and Faddeev, D. K.: *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[Du] Dummit, D.S.: *Classes of Order* 4 *in the strict class group of number fields and remarks on unramified quadratic extensions of unit type*, in preparation.

[Du-F] Dummit, D. and Foote, R. : Abstract Algebra, Third Edition, John-Wiley, 2004.

[DGK] Dummit, D., Granville, A. and Kisilevsky, H., *Big biases amongst products of two primes*, Mathematika **62** (2016), 502–507.

[F-W] Friedman, E. and Washington, L. C.: *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, 227–239.

[GGS] Gan, W.-T., Gross, B. H., and Savin, G.: *Fourier coefficients of modular forms on* G_2, Duke Math. J. **115** (2002), 105–169.

[G] Garton, D.: *Random matrices, the Cohen-Lenstra heuristics, and roots of unity*, Algebra & Number Theory **9** (2015), no. 1, 149–171.

[G-H] Greither, C. and Hayes, D.: A note on the theorem of Armitage–Fröhlich, (unpublished). Prepublication 97-8, Collection Mathemématique, Departement de Mathématiques et de Statistique, Université Laval, Quebec, Canada, 1–8.

[G-L] Gross, B. Lucianovic, M. *On cubic rings and quaternion rings*, J. Number Theory **129** (2008), no. 6, 1468–1478.

[H] Hayes, D.: *On the* 2*-ranks of Hilbert Class Fields (Working Paper)*, unpublished.

[Ha1] Haggenmüller, R.: *Signaturen von Einheiten und unverzweigte quadratische Erweiterungen totalreeler Zahlkörper*, Arch. Math. **39** (1982), 312–321.

[Ha2] Haggenmüller, R.: *Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen*, Manuscripta Math. **36** (1981/82), no. 1, 83–103.

[Hi] Hill, J., *On Finding Totally Real Quintic Number Fields of Minimal Signature Group Rank*, M.S. thesis, University of Vermont, 2006.

[HSV] Ho, W., Shankar, A., and Varma, I.: *The mean number of* 2*-torsion elements in class groups of odd degree number fields arising from binary* n*-ic forms*, preprint, June 2, 2016.

[Hu] Hunter, J., *The minimum discriminant of quintic fields*, Proc. Glasgow Math. Assoc. **3** (1957), 57–67.

[La] Lagarias, J.C.: *Signatures and congruences (mod 4) in certain totally real fields*, Jour. für Math. **320** (1980), 1–5.

[Le] Lemmermeyer, F.: *Selmer groups and quadratic reciprocity*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 279–293.

[M1] Malle, G.: *The totally real primitive number fields of discriminant at most* 10^9, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 114–123.

[M2] Malle, G.: *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory 128 (2008), 2823-2835.

[M3] Malle, G.: *On the distribution of class groups of number fields*, Experiment. Math. **19** (2010), no. 4, 465–474.

[M4] Malle, G.: *On the distribution of Galois groups*, J. Number Theory 92 (2002), 315–329.

[N] Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, Second Edition, Springer-Verlag, 1980.

[O] Oriat, B.: *Relation entre les* 2*-groupes de classes d'idéaux au sens ordinaire et restreint de certains corps de nombres*, Bull. Soc. Math. France **104** (1976), 301-307.

[P] PARI group, *Number field tables*, at `ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`.

[P-R] Paule, P., Riese, A.: *A Mathematica q-Analogue of Zeilberger's algorithm based on an algebraically motivated approach to q-hypergeometric telescoping*, in Special Functions, q-Series and Related Topics, M.E.H. Ismail, D.R. Masson, M. Rahman (Eds.), Fields Inst. Commun., vol. 14, American Mathematical Society, Providence, RI (1997), 179–210.

[P-V] Poonen, B. and Rains, E.: *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.

[R] Riese, A.: A Mathematica q-analogue of Zeilberger's algorithm for proving q-hypergeometric identities, diploma thesis, J. Kepler University, Linz, (1995).

[Sage] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 5.2)* (2011), available at `http://www.sagemath.org/`.

[S] Stevenhagen, P.: *The number of real quadratic fields having units of negative norm*, Experiment. Math. **2** (1993), 121–136.

[V-E] Venkatesh, A. and Ellenberg, J. S.: *Statistics of number fields and function fields*, Proceedings of the International Congress of Mathematicians, Vol. II, Hindustan Book Agency, New Delhi, 2010, 383–402.

[V] Voight, J.: *Enumeration of totally real number fields of bounded root discriminant*, Algorithmic number theory (ANTS VIII, Banff, 2008), eds. Alfred van der Poorten and Andreas Stein, Lecture Notes in Comp. Sci., vol. 5011, Springer, Berlin, 2008, 268–281.

[Wil] Wilson, R.: The Finite Simple Groups, Springer-Verlag, 2009.

[Wood] Wood, M. M.: *Nonabelian Cohen-Lenstra moments*, preprint, 2016.

Department of Mathematics, University of Vermont, Lord House, 16 Colchester Ave., Burlington, VT 05405, USA

E-mail address: `dummit@math.uvm.edu`

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: `jvoight@gmail.com`