ILLINOIS JOURNAL OF MATHEMATICS
Volume 33, Number 1, Spring 1989

THE 4-CLASS RANKS OF QUADRATIC EXTENSIONS OF CERTAIN IMAGINARY QUADRATIC FIELDS

BY

FRANK GERTH III

1. Introduction and statement of main result

Let K be a quadratic extension of the field of rational numbers $\mathbf{Q}$. Let C_K be the 2-class group of K in the narrow sense. Then it is a classical result that rank $C_K = t - 1$, where t is the number of primes that ramify in $K/\mathbf{Q}$. Let R_K be the 4-class rank of K in the narrow sense; i.e.,

$$R_K = \operatorname{rank} C_K^2 = \dim_{\mathbf{F}_2}\left(C_K^2/C_K^4\right).$$

Here $\mathbf{F}_2$ is the finite field with two elements, and C_K^2/C_K^4 is an elementary abelian 2-group which we are viewing as a vector space over $\mathbf{F}_2$. In [6] we have presented results which specify how likely it is for $R_K = 0, 1, 2, \ldots,$ both for imaginary quadratic extensions of $\mathbf{Q}$ and for real quadratic extensions of $\mathbf{Q}$.

Suppose now we replace the base field $\mathbf{Q}$ by an imaginary quadratic field F whose class number is odd, and suppose K is a quadratic extension of F. We let C_K denote the 2-class group of K. Then rank $C_K = t - 1 - \beta$, where t is the number of primes that ramify in K/F, and $\beta = 0$ or 1. (See Equation 3.5 for more details.) We let R_K denote the 4-class rank of K, and we ask the following question: how likely is $R_K = 0, 1, 2, \ldots$? Since the 2-class groups of both F and $\mathbf{Q}$ are trivial, and since the groups of units in the rings of integers of F and $\mathbf{Q}$ are finite cyclic groups, there is a reasonable expectation that the 4-class ranks of quadratic extensions of F will exhibit a behavior similar to the 4-class ranks of quadratic extensions of $\mathbf{Q}$.

To make the situation more precise, we introduce some notation. We let $\mathcal{O}_F$ denote the ring of integers of F. For a nonzero ideal I of $\mathcal{O}_F$, we let $N(I)$ denote the absolute norm of I. Equivalently $N(I) = [\mathcal{O}_F\colon I]$. For a quadratic extension K of F, we let $D_{K/F}$ denote the relative discriminant. For each

Received February 2, 1987.

positive integer t, each nonnegative integer j, and each positive real number x, we define

$$A_t = \{\text{quadratic extensions } K \text{ of } F \text{ with exactly } t \text{ primes of } F \text{ ramified in } K\}, \tag{1.1}$$

$$A_{t;x} = \{K \in A_t\colon N(D_{K/F}) \le x\}, \tag{1.2}$$

$$A_{t,j;x} = \{K \in A_{t;x}\colon R_K = j\}. \tag{1.3}$$

We then define the density $d_{t,j}$ by

$$d_{t,j} = \lim_{x\to\infty} \frac{|A_{t,j;x}|}{|A_{t;x}|} \tag{1.4}$$

where $|S|$ denotes the cardinality of a set S, and we define the limit density $d_{\infty,j}$ by

$$d_{\infty,j} = \lim_{t\to\infty} d_{t,j}. \tag{1.5}$$

Our main result is the following theorem.

THEOREM 1.1. *Let F be an imaginary quadratic field with odd class number, and let K be a quadratic extension of F. Let R_K be the 4-class rank of K, and let $N(D_{K/F})$ be the absolute norm of the relative discriminant of K/F. Let j be a nonnegative integer, and let the density $d_{\infty,j}$ be defined by* (1.5). (*Also see* (1.1) *through* (1.4).)

(i) *If $F \neq \mathbf{Q}(\sqrt{-1})$, then*

$$d_{\infty,j} = \frac{2^{-j(j+1)}\prod_{k=1}^{\infty}(1-2^{-k})}{\left[\prod_{k=1}^{j}(1-2^{-k})\right]\left[\prod_{k=1}^{j+1}(1-2^{-k})\right]} \quad \textit{for } j = 0,1,2,\ldots.$$

In particular,

$$d_{\infty,0} = .577576,\ d_{\infty,1} = .385051,\ d_{\infty,2} = .036672,\ d_{\infty,3} = .000699.$$

(ii) *If $F = \mathbf{Q}(\sqrt{-1})$, then*

$$d_{\infty,j} = \frac{2^{-j(j+3)/2}}{\left[\prod_{k=2}^{\infty}(1+2^{-k})\right]\left[\prod_{k=1}^{j}(1-2^{-k})\right]} \quad \textit{for } j = 0,1,2,\ldots.$$

In particular,

$$d_{\infty,0} = .629134,\ d_{\infty,1} = .314567,\ d_{\infty,2} = .052428,\ d_{\infty,3} = .003745.$$

Remark. The formula for $d_{\infty,j}$ when $F \neq \mathbf{Q}(\sqrt{-1})$ is the same formula that occurs when one considers real quadratic extensions K of $\mathbf{Q}$ (cf. (1.6) and Theorem 5.11 in [6]). When $F = \mathbf{Q}(\sqrt{-1})$, the formula for $d_{\infty,j}$ is the same general type of formula that occurs when one considers the 3-part of the principal genus in cyclic cubic extensions of $\mathbf{Q}(\zeta)$, where ζ is a primitive cube root of unity (cf. [8], Corollary 3.2).

Remark. A recent paper of Cohen and Martinet [5] presents numerical heuristics for class groups of number fields, extending earlier conjectures of Cohen and Lenstra [4]. Now in our Theorem 1.1, the Galois closure of K is typically an extension of $\mathbf{Q}$ of degree 8 with dihedral Galois group. Thus our extension K/F corresponds to the extension K/k on p. 133 in [5]. Although Cohen and Martinet exclude the 2-class group (C_K in our notation) from their heuristics in case (6.1) on p. 133 in [5], it is interesting to observe that our formula in Theorem 1.1(i) is the formula one would expect if the Cohen-Martinet heuristics were extended to the calculation of the rank of C_K^2. So although the Cohen-Martinet heuristics would not apply to C_K because the rank of C_K must be large if many primes ramify in K/F, it is possible that the Cohen-Martinet heuristics could be extended to C_K^2 when the imaginary quadratic field F has odd class number and $F \neq \mathbf{Q}(\sqrt{-1})$. The calculation of the rank of C_K^2 when $F = \mathbf{Q}(\sqrt{-1})$ is different essentially because $\mathbf{Q}(\sqrt{-1})$ contains a fourth root of unity (compare Case 4 with Cases 1, 2, and 3 in the next section).

2. Preliminary results

Let notation be the same as in Section 1. Since we are assuming F is an imaginary quadratic field with odd class number, then $F = \mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$, or $\mathbf{Q}(\sqrt{-p})$, where p is a rational prime with $p \equiv 3 \pmod 4$. Let α be a nonunit in $\mathcal{O}_F$. We shall specify a particular method for choosing a generator for the principal ideal $\alpha\mathcal{O}_F$. In our subsequent applications, $\alpha\mathcal{O}_F$ will be some odd power of a prime ideal that does not lie above the rational prime 2.

Case 1. $F = \mathbf{Q}(\sqrt{-p})$ with $p \equiv 7 \pmod 8$. Then 2 splits in $\mathcal{O}_F$; i.e., $2\mathcal{O}_F = \mathcal{L}_1\mathcal{L}_2$, where $\mathcal{L}_1$ and $\mathcal{L}_2$ are distinct prime ideals in $\mathcal{O}_F$. For $\alpha \notin \mathcal{L}_1$, we have $\alpha \equiv \pm 1 \pmod{\mathcal{L}_1^2}$. We let $\beta = \pm\alpha$ so that $\beta \equiv 1 \pmod{\mathcal{L}_1^2}$. Then $\beta\mathcal{O}_F = \alpha\mathcal{O}_F$, and β is the generator that we shall use in subsequent applications.

Case 2. $F = \mathbf{Q}(\sqrt{-p})$ with $p \equiv 3 \pmod 8$. Then $2\mathbf{Q}_F$ is a prime ideal, and $\mathcal{O}_F/2\mathcal{O}_F$ is the finite field with four elements. We let $\zeta \in \mathcal{O}_F$ so that the images of 0, 1, ζ, and ζ^2 in $\mathcal{O}_F/2\mathcal{O}_F$ are the four distinct elements of $\mathcal{O}_F/2\mathcal{O}_F$. For $\alpha \notin 2\mathcal{O}_F$, we have $\alpha^3 \equiv 1 + 2c_1 \pmod{4\mathcal{O}_F}$, where $c_1 = 0, 1, \zeta$, or ζ^2. We let $\beta = \pm\alpha^3$ so that $\beta \equiv 1 + 2d_1 \pmod{4\mathcal{O}_F}$ with $d_1 = 0$ or ζ. In this case we are actually specifying a certain generator β for the ideal $\alpha^3\mathcal{O}_F$ rather than $\alpha\mathcal{O}_F$.

Case 3. $F = \mathbf{Q}(\sqrt{-2})$. For $\alpha \notin \sqrt{-2}\,\mathcal{O}_F$, we have

$$\alpha \equiv 1 + c_1\sqrt{-2} + c_2(\sqrt{-2})^2 + c_3(\sqrt{-2})^3 \pmod{4\mathcal{O}_F}$$

with $c_j = 0$ or 1 for $1 \le j \le 3$. Alternatively we note that

$$\alpha \equiv \pm(1 + \sqrt{-2})^j \pmod{4\mathcal{O}_F}$$

with $j = 0, 1, 2$, or 3. We choose $\beta = \pm\alpha$ so that

$$\beta \equiv (1 + \sqrt{-2})^j \pmod{4\mathcal{O}_F}$$

with $j = 0, 1, 2$, or 3.

Case 4. $F = \mathbf{Q}(\sqrt{-1})$. We let $i = \sqrt{-1}$, and we note that $1 + i$ is a prime element of $\mathcal{O}_F$ dividing 2. For $\alpha \notin (1 + i)\mathcal{O}_F$,

$$\alpha \equiv 1 + c_1(1 + i) + c_2(1 + i)^2 + c_3(1 + i)^3 \pmod{4\mathcal{O}_F}$$

with $c_j = 0$ or 1 for $1 \le j \le 3$. Alternately we note that

$$\alpha \equiv i^k\bigl(1 + (1 + i)^3\bigr)^l \pmod{4\mathcal{O}_F}$$

with $k = 0, 1, 2$, or 3 and $l = 0$ or 1. We choose $\beta = i^m\alpha$ with $m = 0, 1, 2$, or 3 such that

$$\beta \equiv \bigl(1 + (1 + i)^3\bigr)^l \pmod{4\mathcal{O}_F}$$

with $l = 0$ or 1.

We now describe some properties of Hilbert symbols and power residue symbols (cf. [2], Chapter 12, and [3], pp. 348–354). Let F be an imaginary quadratic field of the form specified above. For nonzero elements a and b of $\mathcal{O}_F$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we define the Hilbert symbol $(a, b)_\mathfrak{p} \in \{\pm 1\}$ by

$$(a, K/F)_\mathfrak{p}\sqrt{b} = (a, b)_\mathfrak{p}\sqrt{b}$$

where $K = F(\sqrt{b})$ and $(a, K/F)_{\not p}$ is the norm residue symbol. We suppose $a\mathcal{O}_F = \not p_1^{j_1}$ and $b\mathcal{O}_F = \not p_2^{j_2}$, where $\not p_1$ and $\not p_2$ are distinct prime ideals of $\mathcal{O}_F$ that do not lie above 2, and j_1 and j_2 are positive odd integers. In the following discussion we assume a and b have the same form as β in cases 1 through 4 above. Our goal is to indicate the relationship between $(a, b)_{\not p_1}$ and $(a, b)_{\not p_2}$ in the four cases. In each case we start with the product formula $\prod_{\not p}(a, b)_{\not p} = 1$, and we note that $(a, b)_{\not p} = 1$ for all $\not p$ not lying above 2 and different from $\not p_1$ and $\not p_2$.

Case 1. We start with $(a, b)_{\not p_1}(a, b)_{\not p_2}(a, b)_{\mathcal{L}_1}(a, b)_{\mathcal{L}_2} = 1$. By assumption $a \equiv b \equiv 1 \pmod{\mathcal{L}_1^2}$. So $(a, b)_{\mathcal{L}_1} = 1$. Also $(a, b)_{\mathcal{L}_2} = 1$ unless $a \equiv b \equiv -1$ $(\mathrm{mod}\ \mathcal{L}_2^2)$. So

$$(2.1) \qquad (a, b)_{\not p_1} = \varepsilon_1 (a, b)_{\not p_2}$$

with

$$(2.2) \qquad \varepsilon_1 = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{\mathcal{L}_2^2} \text{ or } b \equiv 1 \pmod{\mathcal{L}_2^2} \\ -1 & \text{if } a \equiv b \equiv -1 \pmod{\mathcal{L}_2^2}. \end{cases}$$

Case 2. We start with $(a, b)_{\not p_1}(a, b)_{\not p_2}(a, b)_{(2)} = 1$. Now $(a, b)_{(2)} = 1$ if $a \equiv 1 \pmod{4\mathcal{O}_F}$ or $b \equiv 1 \pmod{4\mathcal{O}_F}$. Otherwise $a \equiv b \equiv 1 + 2\zeta \pmod{4\mathcal{O}_F}$. In general

$$(a, a)_{(2)}(-1, a)_{(2)} = (-a, a)_{(2)} = 1.$$

So $(a, a)_{(2)} = (-1, a)_{(2)}$. The product formula $(-1, a)_{(2)}(-1, a)_{\not p_1} = 1$ implies $(-1, a)_{(2)} = (-1, a)_{\not p_1}$. Now $(-1, a)_{\not p_1} = (-1)^{(Na-1)/2} = -1$ since

$$Na \equiv (1 + 2\zeta)(1 + 2\zeta^2) \equiv -1 \pmod{4\mathcal{O}_F}.$$

Hence when $a \equiv b \equiv 1 + 2\zeta \pmod{4\mathcal{O}_F}$, we have

$$(a, b)_{(2)} = (a, a)_{(2)} = (-1, a)_{(2)} = (-1, a)_{\not p_1} = -1.$$

So

$$(2.3) \qquad (a, b)_{\not p_1} = \varepsilon_2 (a, b)_{\not p_2}$$

with

$$(2.4) \qquad \varepsilon_2 = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{4\mathcal{O}_F} \text{ or } b \equiv 1 \pmod{4\mathcal{O}_F} \\ -1 & \text{if } a \equiv b \equiv 1 + 2\zeta \pmod{4\mathcal{O}_F}. \end{cases}$$

Case 3. We start with $(a, b)_{\not p_1}(a, b)_{\not p_2}(a, b)_{(\sqrt{-2})} = 1$. Since

$$a \equiv (1 + \sqrt{-2})^{j_a} \pmod{4\mathcal{O}_F} \quad \text{with } j_a = 0, 1, 2, \text{or } 3,$$

and since

$$b \equiv (1 + \sqrt{-2})^{j_b} \pmod{4\mathcal{O}_F} \quad \text{with } j_b = 0, 1, 2, \text{ or } 3,$$

then $(a, b)_{(\sqrt{-2})} = (1 + \sqrt{-2},\ 1 + \sqrt{-2})^{j_a j_b}_{(\sqrt{-2})}$. If either j_a or j_b is even, then $(a, b)_{(\sqrt{-2})} = 1$. So suppose j_a and j_b are odd. Then by the procedures used in case 2,

$$\begin{aligned}(1 + \sqrt{-2}, 1 + \sqrt{-2})^{j_a j_b}_{(\sqrt{-2})} &= (a, a)_{(\sqrt{-2})} = (-1, a)_{(\sqrt{-2})} \\ &= (-1, a)_{\not{p}_1} = -1.\end{aligned}$$

So with

$$a \equiv (1 + \sqrt{-2})^{j_a} \pmod{4\mathcal{O}_F} \quad \text{with } j_a = 0, 1, 2, \text{ or } 3,$$

and with

$$b \equiv (1 + \sqrt{-2})^{j_b} \pmod{4\mathcal{O}_F} \quad \text{with } j_b = 0, 1, 2, \text{ or } 3,$$

we have

$$(a, b)_{\not{p}_1} = \varepsilon_3 (a, b)_{\not{p}_2} \tag{2.5}$$

with

$$\varepsilon_3 = \begin{cases} 1 & \text{if } j_a \text{ or } j_b \text{ is even} \\ -1 & \text{if both } j_a \text{ and } j_b \text{ are odd.} \end{cases} \tag{2.6}$$

Case 4. We start with $(a, b)_{\not{p}_1}(a, b)_{\not{p}_2}(a, b)_{(1+i)} = 1$. We recall that

$$a \equiv \left(1 + (1 + i)^3\right)^{l_a} \pmod{4\mathcal{O}_F} \quad \text{with } l_a = 0 \text{ or } 1,$$

and

$$b \equiv \left(1 + (1 + i)^3\right)^{l_b} \pmod{4\mathcal{O}_F} \quad \text{with } l_b = 0 \text{ or } 1.$$

If $l_a = 0$ or $l_b = 0$, then clearly $(a, b)_{(1+i)} = 1$. So suppose $l_a = 1$ and $l_b = 1$. Then

$$(a, b)_{(1+i)} = (a, a)_{(1+i)} = (-1, a)_{(1+i)} = (i^2, a)_{(1+i)} = 1.$$

So $(a, b)_{(1+i)} = 1$ even when $l_a = l_b = 1$. Hence

$$(a, b)_{\not{p}_1} = (a, b)_{\not{p}_2}. \tag{2.7}$$

In Cases 1 through 4, we note that $(a, b)_{\mathfrak{p}_1} = (b/\mathfrak{p}_1)$, where $(b/\mathfrak{p}_1)$ is the quadratic residue symbol which satisfies

$$(b/\mathfrak{p}_1) = \begin{cases} 1 & \text{if } \mathfrak{p}_1 \text{ splits in } F(\sqrt{b})/F \\ -1 & \text{if } \mathfrak{p}_1 \text{ is inert in } F(\sqrt{b})/F. \end{cases}$$

Similarly $(a, b)_{\mathfrak{p}_2} = (a/\mathfrak{p}_2)$. Then (2.1)–(2.7) are the quadratic reciprocity laws for the fields F considered in Cases 1 through 4. We note that the form of the quadratic reciprocity law for the fields F in Cases 1, 2, and 3 is analogous to the form of the quadratic reciprocity law for $\mathbf{Q}$. In Case 4, however, the quadratic reciprocity law has the simpler form given by (2.7).

3. Proof of the theorem

Let notation be the same as in Sections 1 and 2. Since the proof of Theorem 1.1 uses many of the ideas used in [6], we shall indicate in this section the appropriate modifications of the arguments in [6] and refer the reader to [6] for more details. First we note that the absolute norm of the relative discriminant of a quadratic extension K of F has the form

$$N(D_{K/F}) = 2^e N(\mathfrak{p}_1 \dots \mathfrak{p}_g)$$

where the integer $e \geq 0$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ are distinct prime ideals of F that do not lie above 2. If exactly t primes of F ramify in K, then $g = t$ if $e = 0$, and $g = t - 1$ if $e > 0$. Since

$$|\{2^e N(\mathfrak{p}_1 \dots \mathfrak{p}_{t-1}) \leq x\}| = o|\{N(\mathfrak{p}_1 \dots \mathfrak{p}_t) \leq x\}| \quad \text{as } x \to \infty,$$

it suffices to consider the fields K with

$$D_{K/F} = \mathfrak{p}_1 \dots \mathfrak{p}_t \tag{3.1}$$

when calculating $d_{t,j}$ in Equation 1.4. Now let h denote the class number of F. Then for $1 \leq j \leq t$, $\mathfrak{p}_j^h$ is a principal ideal in $\mathcal{O}_F$. We let a_j be the generator of $\mathfrak{p}_j^h$ chosen by the rules specified in Cases 1 through 4 in Section 2. (Actually in Case 2, a_j is a generator of $\mathfrak{p}_j^{3h}$.) Then we see that $K = F(\sqrt{\mu})$ with

$$\mu = a_1 \dots a_t. \tag{3.2}$$

In Cases 1, 2, and 3, we let M_K be the $(t-1) \times (t+1)$ matrix with entries in the finite field $\mathbf{F}_2$ specified as follows:

$$M_K = [m_{jk}], \qquad m_{jk} \in \mathbf{F}_2, \qquad 1 \leq j \leq t-1, \qquad 0 \leq k \leq t, \tag{3.3}$$

where

$$(3.4)\qquad (-1)^{m_{jk}} = \begin{cases} (-1,\mu)_{\mathfrak{p}_j} & \text{for } 1 \le j \le t-1 \text{ and } k = 0 \\ (a_k,\mu)_{\mathfrak{p}_j} & \text{for } 1 \le j \le t-1 \text{ and } 1 \le k \le t. \end{cases}$$

If σ is a generator of $\mathrm{Gal}(K/F)$, we note that $C_K^{1-\sigma} = C_K^2$. Then using the results in Section 1 of [9], we see that the 2-class rank of K is given by

$$(3.5)\qquad r_K = t - 1 - \operatorname{rank}[\text{column } 0 \text{ of } M_K],$$

and the 4-class rank of K is given by

$$(3.6)\qquad R_K = t - 1 - \operatorname{rank} M_K$$

except perhaps when each $a_k \equiv 1 \pmod{4\mathcal{O}_F}$ for $1 \le k \le t$. If each $a_k \equiv 1 \pmod{4\mathcal{O}_F}$, then $\mathcal{P}_1^h, \dots, \mathcal{P}_t^h$ may not generate all of ${}_2C_K$, where $\mathcal{P}_1, \dots, \mathcal{P}_t$ are the prime ideals in the ring of integers of K above $\mathfrak{p}_1, \dots, \mathfrak{p}_t$, and where ${}_2C_K$ is the subgroup of C_K generated by the elements of order 2 in C_K. Hence we might need another column in our matrix M_K in Equation 3.3, corresponding to another generator for ${}_2C_K$. However the probability that $a_k \equiv 1 \pmod{4\mathcal{O}_F}$ for all k with $1 \le k \le t$ goes to zero as $t \to \infty$. So when we compute $d_{\infty,j}$ in (1.5), the possible error will go to zero. So it suffices to use M_K specified by (3.3) and (3.4) when we compute R_K in (3.6).

Now from (3.2), $\mu = a_1 \dots a_t$, and from properties of Hilbert symbols, $(-\mu,\mu)_{\mathfrak{p}_j} = 1$ for each j. So from (3.4) we see that the sum of the entries in each row of M_K is zero. So we may discard any column of M_K without changing the rank. Since the quadratic reciprocity law in F in cases 1, 2, and 3 (see (2.1)–(2.6)) has the same form as the quadratic reciprocity law in $\mathbf{Q}$, then we see that by discarding a column from M_K (which does not change the rank) and by rearranging the rows and columns, we get the same type of matrix as the matrix $\overline{M}$ in Equation 5.7 of [6]. We can now follow the same procedures used in Section 5 of [6] to get the same limit density given by Theorem 5.11. This is precisely the limit density that we have specified in Theorem 1.1 of this paper when $F \ne \mathbf{Q}(\sqrt{-1})$.

For Case 4, we define M_K by (3.3) and (3.4) except with $(\sqrt{-1},\mu)_{\mathfrak{p}_j}$ replacing $(-1,\mu)_{\mathfrak{p}_j}$ in (3.4). Since the quadratic reciprocity law in Case 4 is given by (2.7), we get the following matrix $\overline{M}_K$ instead of the matrix $\overline{M}$ of Equation 5.7 of [6]:

$$(3.7)\qquad \overline{M}_K = \left[\begin{array}{c:c} H_{l-1} & \\ & M \\ O_{t-l} & \end{array}\right]$$

where $H_{l-1} \in \mathbf{F}_2^{l-1}$ is the vector with each component equal to 1; O_{t-l} is the zero vector in $\mathbf{F}_2^{t-l}$; and M is a $(t-1) \times (t-1)$ symmetric matrix with entries in $\mathbf{F}_2$. We now must determine the appropriate Markov process that arises from the above matrices.

Let k and n be positive integers with $k \leq n$. Let M_1 be an $n \times (n+1)$ matrix of the form

$$M_1 = [J \quad A] \tag{3.8}$$

where J is a vector in $\mathbf{F}_2^n$ with exactly k components equal to 1, and A is an $n \times n$ symmetric matrix with entries in $\mathbf{F}_2$. Let

$$M_2 = \begin{bmatrix} J & A & B \\ 1 & B^T & d \end{bmatrix} \tag{3.9}$$

where $B \in \mathbf{F}_2^n$, B^T is the transpose of B, and $d \in \mathbf{F}_2$.

LEMMA 3.1. *Let M_1 and M_2 be specified by* (3.8) *and* (3.9). *Suppose* rank $M_1 = r$. *Of all possible M_2,*

(i) $2^{n+1} - 2^{r+1}$ *have* rank $M_2 = r + 2$;
(ii) $3 \cdot 2^{r-1}$ *have* rank $M_2 = r + 1$;
(iii) 2^{r-1} *have* rank $M_2 = r$.

Proof. Let $c(M_1)$ denote the column space of M_1. Then rank $M_2 = r + 2$ if and only if $B \notin c(M_1)$. Since rank $M_1 = r$, then there are $2^n - 2^r$ choices for $B \notin c(M_1)$. Since d can be arbitrary, then there are two choices for d. Thus there are $2^{n+1} - 2^{r+1}$ matrices M_2 with rank $M_2 = r + 2$. So (i) is proved. Now suppose rank $M_2 = r$. Let

$$S_1 = \{V \in \mathbf{F}_2^n \colon V^TJ = 1\} \quad \text{and} \quad S_0 = \{V \in \mathbf{F}_2^n \colon V^TJ = 0\}.$$

Then $S_1 = V_1 + S_0$ for a fixed $V_1 \in S_1$. Now if rank $M_2 = r$, then $B^T = V^TA$ for some $V \in S_1$. Write $V = V_1 + V_2$ with $V_2 \in S_0$. Then $B^T = V_1^TA + V_2^TA$, and the number of possible vectors B equals $|\{V_2^TA\colon V_2 \in S_0\}|$. Since $V_2^T[J \quad A] = [0 \quad V_2^TA]$, then

$$\dim_{\mathbf{F}_2}\{V_2^T[J \quad A]\colon V_2 \in S_0\} = \dim_{\mathbf{F}_2}\{V_2^TA\colon V_2 \in S_0\}.$$

Since $\operatorname{rank}[J \quad A] = r$ and $\dim_{\mathbf{F}_2} S_0 = n - 1$, then

$$\dim_{\mathbf{F}_2}\{V_2^T[J \quad A]\colon V_2 \in S_0\} = r \quad \text{or} \quad r - 1.$$

Since the first entry in some row of $[J \quad A]$ is 1, but the first entry in each $V_2^T[J \quad A]$ is 0, then

$$\dim_{\mathbf{F}_2}\{V_2^T[J \quad A]\colon V_2 \in S_0\} = r - 1.$$

So the number of possible vectors B is 2^{r-1}. If $V \in S_1$ and $V^TA = B^T$, we also need $d = V^TB$. If $W \in S_1$ such that $W^TA = B^T$, then $W = V + V_0$ for some $V_0 \in S_0$, and $0 = W^TA - V^TA = V_0^TA$. Then

$$W^TB = V^TB + V_0^TB = V^TB + V_0^T(AV) = V^TB.$$

So for each B, the element d is uniquely determined. So the number of matrices M_2 with rank $M_2 = r$ is 2^{r-1}. So (iii) is proved. Finally (ii) is proved by subtracting the numbers in (i) and (iii) from 2^{n+1}.

Remark. Lemma 3.1 is also true if the last entry in the first column of M_2 is 0 instead of 1. Note that Lemma 3.1 is valid for each choice of k, $1 \leq k \leq n$, where k represents the number of components of J equal to 1.

To get the transition matrix of the associated Markov process, we divide each term in (i) through (iii) of Lemma 3.1 by 2^{n+1} (recall that 2^{n+1} is the sum of the terms in (i) through (iii) of Lemma 3.1), and we let $t = n + 1$, $j = n - \operatorname{rank} M_1$, and $l = n + 1 - \operatorname{rank} M_2$. Then we have the following Markov process in Case 4, which is used in place of Markov process D' in Appendix III of [6]:

The Markov process has states $y_{t,j}$ with $t = 2, 3, 4, \ldots$, and $j = 0, 1, 2, \ldots$. Let

$$Y_t = (y_{t,0}, y_{t,1}, y_{t,2}, \ldots).$$

Then $Y_{t+1} = Y_tQ$, where

$$Q = [q_{jl}] \quad \text{with } j = 0, 1, 2, \ldots; \qquad l = 0, 1, 2, \ldots;$$

$$q_{jl} = \begin{cases} 1 - 2^{-j} & \text{if } l = j - 1 \\ 3 \cdot 2^{-j-2} & \text{if } l = j \\ 2^{-j-2} & \text{if } l = j + 1 \\ 0 & \text{otherwise.} \end{cases}$$

We let $Y = (y_0, y_1, y_2, \ldots)$ denote $\lim_{t \to \infty} Y_t$, which is the invariant probability vector for the Markov process. Then $d_{\infty, j} = y_j$ for $j = 0, 1, 2, \ldots$, and hence we need to calculate y_j for each j. We can apply Lemma 1.5 of [7] to get

$$y_j = \frac{2^{-j-1}}{1 - 2^{-j}} y_{j-1} \quad \text{for } j = 1, 2, 3, \ldots. \tag{3.10}$$

Using the recurrence relation (3.10) and the fact that $\Sigma_{j=0}^{\infty} y_j = 1$, we get

$$Y = \omega^{-1}\left(1, \frac{2^{-2}}{2^{-1}}, \ldots, \prod_{k=1}^{j} \frac{2^{-k-1}}{1-2^{-k}}, \ldots\right) \tag{3.11}$$

or equivalently

$$Y = \omega^{-1}\left(1, 2^{-1}, \ldots, \frac{2^{-j(j+3)/2}}{\prod_{k=1}^{j}(1-2^{-k})}, \ldots\right) \tag{3.12}$$

where

$$\omega = 1 + \sum_{j=1}^{\infty} \frac{2^{-j(j+3)/2}}{\prod_{k=1}^{j}(1-2^{-k})}. \tag{3.13}$$

By Corollary 2.2 in [1],

$$\omega = \prod_{j=0}^{\infty}(1+2^{-2-j}) = \prod_{j=2}^{\infty}(1+2^{-j}). \tag{3.14}$$

Since $d_{\infty,j} = y_j$ for $j = 0, 1, 2, \ldots$, then the formula for $d_{\infty,j}$ in part (ii) of Theorem 1.1 follows from Equations 3.12 and 3.14.

References

1. G. Andrews, *The theory of partitions*, Addison-Wesley, Reading, Mass., 1976.
2. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1967.
3. J. Cassels and A. Fröhlich, *Algebraic number theory*, Thompson Book Co., Washington, D.C., 1967.
4. H. Cohen and H. Lenstra, *Heuristics on class groups of number fields*, Springer Lecture Notes in Mathematics, No. 1068, Springer-Verlag, N.Y., 1984, pp. 33–62.
5. H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics*, Math. Comp., vol. 48 (1987), 123–137.
6. F. Gerth, *The 4-class ranks of quadratic fields*, Invent. Math. vol. 77 (1984), pp. 489–515.
7. ______, *Limit probabilities for coranks of matrices over $GF(q)$*, Linear and Multilinear Algebra, vol. 19 (1986), pp. 79–93.
8. ______, *Densities for 3-class ranks in certain cubic extensions*, to appear.
9. F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Körper*, J. Number Theory, vol. 4 (1972), pp. 144–156.

The University of Texas at Austin
Austin, Texas