Canad. J. Math. Vol. **57** (1), 2005 pp. 180–203

On the Size of the Wild Set

Marius Somodi

Abstract. To every pair of algebraic number fields with isomorphic Witt rings one can associate a number, called the *minimum number of wild primes*. Earlier investigations have established lower bounds for this number. In this paper an analysis is presented that expresses the minimum number of wild primes in terms of the number of wild dyadic primes. This formula not only gives immediate upper bounds, but can be considered to be an exact formula for the minimum number of wild primes.

1 Introduction

The abstract theory of symmetric bilinear forms over fields took a major turn in 1937 when Witt constructed a new object, today known as the *Witt ring*. As this object can be associated to any field, number theorists have been interested in understanding the Witt ring of number fields. To describe explicitly the Witt ring of an arbitrary number field is a difficult problem. Another problem in algebraic theory of quadratic forms and number theory is to describe the situation when two number fields have isomorphic Witt rings (in this case the number fields are called *Witt equivalent*). In 1994, R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland ([6]) solved this problem. They proved that two number fields are Witt equivalent if and only if there is a *reciprocity equivalence* between the fields. Later the terminology changed and *reciprocity equivalence* has been renamed *Hilbert symbol equivalence*. A Hilbert symbol equivalence between two number fields K and L is a pair of maps (t, T), where

$$t\colon K^*/K^{*2} \to L^*/L^{*2}$$

is a group isomorphism and

$$T\colon \Omega_K \to \Omega_L$$

is a bijection between the sets of (finite and infinite) primes of K and L respectively, such that the Hilbert symbols are preserved:

$$(a, b)_P = (t(a), t(b))_{TP}, \quad a, b \in K^*/K^{*2}, \quad P \in \Omega_K.$$

In 1991, K. Szymiczek proved that there is a Hilbert symbol equivalence between two number fields if and only if the two number fields have the same level, the same number of real embeddings, and there is a bijection between the dyadic primes of the two fields so that the corresponding dyadic completions have the same level and degree over $\mathbb{Q}_2$ (see [7]).

Received by the editors January 7, 2002; revised March 4, 2003.
AMS subject classification: 11E12, 11E81, 19F15, 11R29.

Constructing a Hilbert symbol equivalence between Witt equivalent number fields is not an easy problem. Since one wants to define maps between infinite sets, in the absence of a systematic method this is an infinite task. In [6] the authors reduced this problem to the problem of constructing a finite object involving finitely many primes. They called this object a *small equivalence*. So far, small equivalence is the only tool employed to construct Hilbert symbol equivalences. The interested reader is referred to [6] for details.

Whenever a Hilbert symbol equivalence (t, T) between two number fields is considered, a partition of the set of prime ideals can be constructed: a prime ideal P is called *tame* for (t, T) if

$$\operatorname{ord}_P(a) \equiv \operatorname{ord}_{TP}(t(a)) \pmod 2$$

for any square class a, and *wild* if it is not tame; the partition consists of the set of tame primes and the set of wild primes. In [6] it is shown that any small equivalence can be extended to a Hilbert symbol equivalence by adding only tame primes. One consequence is that between Witt equivalent number fields one can always construct Hilbert symbol equivalences that have finitely many wild primes. P. E. Conner posed the question: how small can the set of wild primes be? In [2] the following lower bounds for the minimum number of wild primes are given in terms of the 2-ranks of the S-ideal class groups:

Proposition 1 *Let (t, T) be a Hilbert symbol equivalence between number fields K and L with finite wild set $W = Wild(K, L)$. Let S be any finite subset of primes of K containing all infinite primes. Then:*

$$|rk_2(C_K(S)) - rk_2(C_L(TS))| \leq |W \setminus S|$$

and

$$|rk_2(C_K^+(S)) - rk_2(C_L^+(TS))| \leq |W \setminus S|.$$

In the next section, we introduce the concept of a *correspondence*. Intuitively, a correspondence is what remains from a Hilbert symbol equivalence (t, T) if we drop the global square-class map t completely, and restrict the map T to a bijection between finite sets containing all the infinite and all the dyadic primes of both fields. In this paper we will show that any correspondence between two Hilbert symbol equivalent number fields can be extended to a small equivalence (and then to a Hilbert symbol equivalence). We also present a method of extending a correspondence to a Hilbert symbol equivalence with a minimum number of wild primes among all Hilbert symbol equivalences that extend it. In particular, we present a formula that expresses the minimum number of wild primes in *any* Hilbert symbol equivalence between the two fields in terms of the number of dyadic wild primes:

Theorem 2 *Let K and L be Witt equivalent number fields, and let S be a finite set that contains all infinite and dyadic primes in K. Any correspondence $\mathcal{C}$ defined on S can be* *extended to a Hilbert symbol equivalence between K and L that has a wild set of size equal to*

$$\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(TS))|,$$

where $W = W(\mathcal{C}) \subseteq S$ *is the set of wild primes of* $\mathcal{C}$ *and* $\delta = \delta(\mathcal{C})$ *is a non-negative integer called the defect of the correspondence. Moreover, any other extension of* $\mathcal{C}$ *to a Hilbert symbol equivalence between K and L has a wild set of size not less than* $\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(TS))|$.

In particular, if one wants to construct a Hilbert symbol equivalence with a minimum number of wild primes then one has to consider all (finitely many) correspondences that can be defined on the set of infinite and dyadic primes, and determine for each one of them the number of wild dyadic primes ($|W|$) and the defect (δ). When the sum of these two numbers is minimum, then any particular correspondence for which this minimum is achieved can be extended to a Hilbert symbol equivalence with a minimum number of wild primes. This number is $\delta + |W| + |rk_2(C_K(D)) - rk_2(C_L(D'))|$, where D and D' are the sets of dyadic primes in K and L respectively.

The formula that we present gives the exact minimum number of wild primes. However, computing explicitly this number for arbitrary number fields might be difficult. Upper and lower bounds for the minimum number of wild primes might be useful. Here they are:

Corollary 3 *Let* $W = Wild(K, L)$ *be a minimum wild set for two Witt equivalent number fields K and L. Let D and* D' *be the sets of dyadic primes in K and L respectively, r and s be the number of real embeddings and pairs of complex embeddings respectively of K. Then*

$$|rk_2C_K(D) - rk_2C_L(D')| \leq |W| \leq |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

We present a method of extending a correspondence to a small equivalence by adding a minimum number of wild primes. The construction involves two steps. If at least one of the fields has an even S-class number, then as a first step we add primes to the correspondence until both class numbers become odd. To accomplish this, we follow a procedure inspired by Czogala's work [3]. Then we proceed to the second step, where we employ J. Carpenter's method [1] of extending to a small equivalence the particular type of correspondence (which she called *suitable*) that gives odd S-class numbers for both fields. We also prove that this method produces at the end the minimum number of wild primes.

2 Preliminary Results

From now on, K and L will denote two algebraic number fields that are Witt equivalent.

As before we will denote by r the number of real embeddings of K, and by s the number of pairs of complex embeddings of K.

We denote by Ω_K the set of all primes (finite or infinite) of K, by Ω_L the set of all primes of L, and let

$$S = \{P_1, P_2, \dots, P_m\} \subset \Omega_K$$

be a finite set of primes of K that contains all infinite and dyadic primes.

By O_K^* we denote the group of units of the ring of integers O_K. If the set S is defined as above, we denote by $O_K(S)$ the ring of S-integers of O_K. More precisely,

$$O_K(S) = \{x \in K : \mathrm{ord}_P(x) \geq 0, \quad P \notin S\}.$$

The units of the ring of S-integers form a multiplicative group $O_K^*(S)$.

We denote by C_K the ideal class group of K, and by $\rho = rk_2(C_K)$ its 2-rank. Recall that the 2-rank of a finite abelian group G is the dimension of the quotient G/G^2 as an $\mathbb{F}_2$-vector space. Equivalently, the 2-rank of G is r, where $|G/G^2| = 2^r$. Yet another way to describe r is as follows: the 2-rank is the number of cyclic factors of 2-power order appearing in the cyclic decomposition of a 2-Sylow subgroup of G.

Let $C_K(S)$ be the S-class group of K: $C_K(S) = C_K/H_K(S)$, where $H_K(S)$ is the subgroup of C_K generated by the classes of ideals in S. We will denote by $\theta(S)$ the 2-rank of $H_K(S)$. Observe that $\theta(S)$ is the dimension over $\mathbb{F}_2$ of the subspace of C_K/C_K^2 generated by the cosets of ideal classes of primes in S and $rk_2(C_K(S)) = \rho - \theta(S)$. We may assume that the primes in S are numbered so that $[P_1], \dots, [P_{\theta(S)}]$ are linearly independent in C_K/C_K^2.

The following notations will be used (some of these notations generalize objects defined in [3]):

$$K_0(S) = \{x \in K^* : \mathrm{ord}_P(x) \equiv 0 \pmod 2, \quad P \in \Omega_K \setminus S\},$$

$$K_{sq}(S) = \{x \in K_0(S) : \ x \text{ is a local square at } P, \quad P \in S\},$$

$$U_K(S) = \{\bar{x} \in K^*/K^{*2} : \ x \in O_K^*(S)\},$$

$$E_K(S) = \{\bar{x} \in K^*/K^{*2} : \ x \in K_0(S)\},$$

$$G_K(S) = \prod_{P \in S} K_P^*/K_P^{*2}.$$

The following inclusions hold:

$$K^{*2} \subset K_{sq}(S) \subset K_0(S).$$

We will denote by $C_{K,2}(S)$ the subgroup of $C_K(S)$ which consists of all elements in $C_K(S)$ of order 1 or 2. The image of an ideal I of K in any of the above ideal class groups will be denoted by $[I]$.

Lemma 4

1. *$U_K(S)$ is a subgroup of $E_K(S)$.*
2. *$U_K(S)$ is an elementary 2-group of order $2^{|S|}$. Hence $rk_2(U_K(S)) = |S|$.*
3. *There is an exact sequence:*

$$1 \to U_K(S) \to E_K(S) \to C_{K,2}(S) \to 1.$$

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

Proof 1. Obvious.

2. By Dirichlet's unit theorem:

$$O_K^*(S) \simeq W_K(S) \times \mathbb{Z}^{|S|-1}$$

where $W_K(S)$ is a cyclic group of finite even order. Then

$$|O_K^*(S)/O_K^*(S)^2| = 2^{|S|},$$

and the claim follows from the observation that $O_K^*(S)/O_K^*(S)^2 \simeq U_K(S)$.

3. Let $\bar{x} \in E_K(S)$. Then a representative x can be chosen with:

$$xO_K = Q_1^{2\alpha_1} Q_2^{2\alpha_2} \cdots Q_r^{2\alpha_r} I,$$

where $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$, I a product of ideals in S, and $Q_1, \dots, Q_r$ outside S. Define a map:

$$\Psi_S \colon E_K(S) \to C_{K,2}(S)$$

by

$$\Psi_S(\bar{x}) = [Q_1]^{\alpha_1}[Q_2]^{\alpha_2} \cdots [Q_r]^{\alpha_r}.$$

Clearly, Ψ_S is a well-defined map, and a group homomorphism. Moreover,

$$\operatorname{Ker}(\Psi_S) = U_K(S), \quad \operatorname{Im}(\Psi_S) \le C_{K,2}(S).$$

To see that Ψ_S is in fact surjective, note that if $[Q_1]^{\alpha_1}[Q_2]^{\alpha_2} \cdots [Q_r]^{\alpha_r} \in C_{K,2}(S)$ then

$$([Q_1]^{\alpha_1}[Q_2]^{\alpha_2} \cdots [Q_r]^{\alpha_r})^2 = 1$$

in $C_K(S)$, hence one can find $x \in K$ such that

$$xO_K = Q_1^{2\alpha_1} Q_2^{2\alpha_2} \cdots Q_r^{2\alpha_r} I,$$

where I is a product of ideals in S, which means that $\bar{x} \in E_K(S)$. ■

Corollary 5 $rk_2(E_K(S)) = |S| + rk_2(C_K(S))$.

Proof The equality follows directly from Lemma 4 (parts 2 and 3) and the fact that $rk_2(C_{K,2}(S)) = rk_2(C_K(S))$. ■

Let S be a finite set of primes of K containing the infinite and dyadic primes, and P be a prime outside S. Denote by $cl_S(P)$ the class of P in $C_K(S)/C_K(S)^2$. Let $S_1 = S \cup \{P\}$.

Lemma 6

1. $E_K(S) \le E_K(S_1)$.
2. $E_K(S) = E_K(S_1)$ *if and only if* $cl_S(P) \neq 1$.

3. $[E_K(S_1) : E_K(S)] = 2$ *if and only if* $cl_S(P) = 1$. *In this case, if we define*

$$\Phi\colon E_K(S_1) \to \mathbb{Z}/2\mathbb{Z}$$

by $\Phi(\bar{x}) = \mathrm{ord}_P(x) \pmod 2$, *there is a short exact sequence:*

$$1 \to E_K(S) \to E_K(S_1) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Proof 1. Obvious.
2, 3. Note that $cl_S(P) = 1$ if and only if there exists $x^* \in K$ such that

$$P = x^* Q_1^{2\alpha_1} Q_2^{2\alpha_2} \cdots Q_j^{2\alpha_j} P_1^{\beta_1} \cdots P_l^{\beta_l}.$$

This is equivalent to the existence of an element $\bar{x}^* \in E_K(S_1)$ such that $\mathrm{ord}_P(\bar{x}^*) \equiv 1 \pmod 2$. But this means that there exists an element $x^* \in K$ which is a local uniformizer at P, and such that $\bar{x}^* \in E_K(S_1)$. In other words, $cl_S(P) = 1$ if and only if $E_K(S_1) \setminus E_K(S)$ is non-empty.

On the other hand, it follows from Corollary 5 that $[E_K(S_1) : E_K(S)] \leq 2$, since $|S_1| = |S| + 1$ and $rk_2(C_K(S_1)) \leq rk_2(C_K(S))$. Consequently, $cl_S(P) = 1$ if and only if $[E_K(S_1) : E_K(S)] = 2$. The sequence is exact: Φ is well-defined, the kernel of Φ consists of those elements of $E_K(S_1)$ that are local units at P, *i.e.*, they are in $E_K(S)$, and Φ is onto $\mathbb{Z}/2\mathbb{Z}$ because it maps the element x^* to 1. ■

Lemma 7

1. $rk_2(C_K(S_1)) = rk_2(C_K(S))$ *if and only if* $cl_S(P) = 1$.
2. $rk_2(C_K(S_1)) = rk_2(C_K(S)) - 1$ *if and only if* $cl_S(P) \neq 1$.

Proof The results are direct consequences of Lemma 6 and Corollary 5. ■

Definition 8 *Let F be an algebraic number field. A finite subset S of* Ω_F *is called decent if S contains all infinite and all dyadic primes of F.*

Definition 9 *A system* $(S, S', T, (t_P)_{P\in S})$ *consisting of:*

1. *a pair of decent sets:* $S \subset \Omega_K$ *and* $S' \subset \Omega_L$*;*
2. *a bijection* $T : S \to S'$*;*
3. *for any prime* $P \in S$ *an isomorphism,* $t_P\colon K_P^*/K_P^{*2} \to L_{TP}^*/L_{TP}^{*2}$ *such that*

$$(a, b)_P = (t_P(a), t_P(b))_{TP},\ \forall a, b \in K_P^*/K_P^{*2},$$

is called a correspondence between K and L.

Remark 10 If $(S, S', T, (t_P)_{P\in S})$ is a correspondence between K and L then the map

$$t_S = \prod_{P\in S} t_P$$

is a group isomorphism $t_S\colon G_K(S) \to G_L(S')$.

Define now the map

$$\nu_S = \nu_K(S) \colon E_K(S) \to G_K(S)$$

by

$$\nu_S(\bar{x}) = (x_{P_1}, x_{P_2}, \dots, x_{P_m}) = (x)_S,$$

where, for any $P \in S$, x_P denotes the image of the global square class $\bar{x}$ in K_P^*/K_P^{*2}. This map is well-defined. Let $\omega_K(S)$ be the image of ν_S.

Before we continue our investigation, we will introduce a notation and present without proofs two results that will be used:

If $x \in K^*$ and P is a finite prime in K we define the following symbol:

$$\left(\frac{x}{P}\right) = \begin{cases} 1, & \text{if } x \text{ is a local square at } P; \\ -1, & \text{otherwise.} \end{cases}$$

Theorem 11 ([4, Theorem 169]) *Let $\mu_1, \mu_2, \dots, \mu_m$ be integers in K such that a product of powers $\mu_1^{x_1} \cdots \mu_m^{x_m}$ is the square of a number in K only if all exponents $x_1, \dots, x_m$ are even. Let $c_1, \dots, c_m$ be arbitrary values ± 1. Then there are infinitely many prime ideals P in K which satisfy the m conditions*

$$\left(\frac{\mu_1}{P}\right) = c_1, \dots, \left(\frac{\mu_m}{P}\right) = c_m.$$

Corollary 12 ([3]) *Suppose $b_1, \dots, b_l \in K_{sq}(S)$ map to linearly independent elements in $K_{sq}(S)/K^{*2}$ and let $R_1, \dots, R_l$ be primes outside S, in K, such that*

$$\left(\frac{b_i}{R_i}\right) = -1, \left(\frac{b_j}{R_i}\right) = 1, \quad \forall\, i \neq j \in \{1, \dots, l\}.$$

Then the classes $[P_1], \dots, [P_{\theta(S)}], [R_1], \dots, [R_l]$ are linearly independent in C_K/C_K^2.

Lemma 13

1. $rk_2(\operatorname{Ker}(\nu_S)) = rk_2(C_K(S))$.
2. $rk_2(\omega_K(S)) = |S|$.

Proof Regard $G_K(S)$ as an $\mathbb{F}_2$-inner product space, with the inner product B defined as the product of Hilbert symbols:

$$B((x)_S, (y)_S) = \prod_{P \in S} (x_P, y_P)_P.$$

According to [1], $rk_2(G_K(S)) = 2|S|$. Note that $\omega_K(S)$ is a totally isotropic subspace of $G_K(S)$. To prove this, we see that for any prime $P \notin S$, any elements $\bar{x}$, $\bar{y}$ in $E_K(S)$ map to local units at P, so the Hilbert symbol satisfies $(x, y)_P = 1$. Then

$$1 = \prod_{P \in \Omega_K} (x, y)_P = B((x)_S, (y)_S) \cdot 1 = B((x)_S, (y)_S).$$

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

According to [5, Corollary 4.4],

$$rk_2(\omega_K(S)) \leq \frac{1}{2} \cdot rk_2(G_K(S)) = |S|.$$

Now $E_K(S)$ can be regarded as an $\mathbb{F}_2$-vector space, and $\mathrm{Ker}(\nu_S)$ is a subspace of $E_K(S)$. Fix $\{\bar{x}_1, \dots, \bar{x}_q\}$ an $\mathbb{F}_2$-base for $\mathrm{Ker}(\nu_S)$. If we use repeatedly Theorem 11, we can find primes $Q_1, \dots, Q_q$ outside S such that $\bar{x}_i$ is a local square at Q_j, $\forall j \neq i$, and $\bar{x}_i$ is a local non-square unit at Q_i, $\forall i \in \{1, \dots, q\}$. If the ideal classes of Q_i were linearly dependent in C_K/C_K^2 then we would get a relation of the form

$$xO_K = Q_1 \cdots Q_l J^2$$

for some $x \in K$ (after renumbering the ideals if necessary). But then x is a local uniformizer at Q_1 and x_1 is a local non-square unit at Q_1, hence $(x, x_1)_{Q_1} = -1$. On the other hand, $(x, x_1)_Q = 1$ for all $Q \neq Q_1$, as when $Q \notin \{Q_2, \dots, Q_l\}$, both x and x_1 are local units at Q, and when $Q = Q_i$ for some $i \neq 1$, x_1 is a local square at Q. This contradicts Hilbert's reciprocity law. Hence $[Q_1], \dots, [Q_q]$ are linearly independent in $C_K(S)/C_K(S)^2$, which implies:

$$rk_2(\mathrm{Ker}(\nu_S)) \leq rk_2(C_K(S)).$$

Finally,

$$|S| + rk_2(C_K(S)) = rk_2(E_K(S)) = rk_2(\mathrm{Ker}(\nu_S)) + rk_2(\omega_K(S)) \leq rk_2(C_K(S)) + |S|$$

which proves both parts of the lemma. ∎

Corollary 14

1. $\dim_{\mathbb{F}_2}(K_0(S)/K_{sq}(S)) = |S|$.
2. $\dim_{\mathbb{F}_2}(K_{sq}(S)/K^{*2}) = rk_2(C_K(S))$.

Proof 1. Note that $K_0(S)/K^{*2} = E_K(S)$ and $K_{sq}(S)/K^{*2} = \mathrm{Ker}(\nu_S)$. Then $\omega_K(S) \simeq K_0(S)/K_{sq}(S)$, and the equality follows from Lemma 13 part 2.

2. This follows from Lemma 13, part 1. ∎

If $(S, S', T, (t_P)_{P\in S})$ is a correspondence, define

$$H_S = \{(x)_S \in \omega_K(S) : t_S((x)_S) \in \omega_L(S')\}$$

and

$$H_{S'} = \{(x)_{S'} \in \omega_L(S') : t_{S'}^{-1}((x)_{S'}) \in \omega_K(S)\}.$$

Observe that H_S is a subgroup of $\omega_K(S)$ and $H_{S'}$ is a subgroup of $\omega_L(S')$.

Definition 15 *If $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ is a correspondence, we define the defect of $\mathcal{C}$ to be the number $\delta = \delta_{\mathcal{C}}$ given by*

$$\delta_{\mathcal{C}} = rk_2(\omega_K(S)/H_S).$$

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

Then $\delta = rk_2(\omega_K(S)) - rk_2(H_S)$ and thus, according to Lemma 13,

$$\delta = |S| - rk_2(H_S).$$

Let us note that since t_S induces a group isomorphism between H_S and $H_{S'}$, the defect of the correspondence can be also expressed as

$$\delta = rk_2(\omega_L(S')/H_{S'}).$$

The remaining part of this section will be devoted to the study of the defect's behavior under extensions of correspondences. We shall prove now that no matter how we extend (tamely or wildly) the correspondence $\mathcal{C}$ to another correspondence $\mathcal{C}_1$ by adding a pair of primes (P_{m+1}, P'_{m+1}), the defect decreases by at most 1. Let $S_1 = S \cup \{P_{m+1}\}$ and $S'_1 = S' \cup \{P'_{m+1}\}$. Let $\mathcal{C}_1 = (S_1, S'_1, T', (t_P)_{P \in S'})$ be a correspondence that extends $\mathcal{C}$. Denote by δ_1 the defect of $\mathcal{C}_1$.

Proposition 16 *Suppose that we extend (tamely or wildly) a correspondence $\mathcal{C} = (S, S', T, (t_P)_{P \in S})$ of defect δ by adding a pair of primes (P_{m+1}, P'_{m+1}). Then the defect δ_1 of the new correspondence satisfies the inequality:*

$$\delta_1 \geq \delta - 1.$$

Proof First define:

$$F_S = \{(x)_{S_1} \in H_{S_1} : x_{P_{m+1}} = 1\}$$

and

$$F_{S'} = \{(y)_{S'_1} \in H_{S'_1} : y_{P'_{m+1}} = 1\}.$$

Since $(1)_{S_1} \in F_S$, F_S and $F_{S'}$ are non-empty, F_S is a subgroup of H_{S_1} and $F_{S'}$ is a subgroup of $H_{S'_1}$. The last component of any element in H_{S_1} identifies the coset of F_S to which the element belongs. Since there are at most four such cosets, it follows that $|H_{S_1}/F_S| \leq 4$. In fact $|H_{S_1}/F_S| = 1, 2$, or 4, and in all cases $0 \leq rk_2(H_{S_1}/F_S) \leq 2$ or

$$0 \leq rk_2(H_{S_1}) - rk_2(F_S) \leq 2.$$

Claim: The map $\zeta\colon F_S \to H_S$, defined by $\zeta((x)_{S_1}) = (x)_S$, is a well-defined and injective homomorphism.

Once we check well-definedness, then the injectivity is clear. We have to check first that the map is well-defined. Let $(x)_{S_1} \in F_S$ and pick $\bar{x} \in E_K(S_1)$ such that $\nu_{S_1}(\bar{x}) = (x)_{S_1}$. Let x be a representative in K for $\bar{x}$. $x_{P_{m+1}} = 1$ implies that $\bar{x} \in E_K(S)$. Now $t_{P_{m+1}}(1) = 1$, so that

$$t_{S_1}(x_{P_1}, \dots, x_{P_m}, 1) = (t_{P_1}(x_{P_1}), \dots, t_{P_m}(x_{P_m}), 1) \in \omega_L(S'_1).$$

Hence there exists an element $\bar{y} \in E_L(S'_1)$ such that

$$\nu_{S'_1}(\bar{y}) = (t_{P_1}(x_{P_1}), \dots, t_{P_m}(x_{P_m}), 1).$$

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

As before, any representative in L of $\bar{y}$ will be a local square at P'_{m+1} and this implies that, in fact, $\bar{y} \in E_L(S')$. Since $\nu_{S'_1}(\bar{y}) = t_S(\nu_S(\bar{x}))$, we deduce that $(x)_S \in H_S$, so the map ζ is well-defined, and the claim is proved.

Then $rk_2(F_S) \le rk_2(H_S)$ and since $0 \le rk_2(H_{S_1}) - rk_2(F_S) \le 2$, it follows that

$$rk_2(H_{S_1}) - rk_2(H_S) \le 2$$

and thus

$$\begin{aligned}\delta_1 &= rk_2(\omega_K(S_1)) - rk_2(H_{S_1}) = |S_1| - rk_2(H_{S_1}) \\ &= |S| + 1 - rk_2(H_{S_1}) \ge |S| + 1 - rk_2(H_S) - 2 = \delta - 1.\end{aligned}$$

Thus $\delta_1 \ge \delta - 1$. ■

Lemma 17 *Suppose that we extend wildly a correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ of defect δ by adding a pair of primes (P_{m+1}, P'_{m+1}) such that $[P_{m+1}]$ is a square in $C_K(S)$ and $[P'_{m+1}]$ is not a square in $C_L(S')$. Then the defect δ_1 of the new correspondence satisfies the inequality:*

$$\delta_1 \ge \delta.$$

Proof Let $S_1 = S \cup \{P_{m+1}\}$ and $S'_1 = S' \cup \{P'_{m+1}\}$. Since $[P'_{m+1}]$ is not a square in $C_L(S')$ and $[P_{m+1}]$ is a square in $C_K(S)$, we have

$$E_L(S') = E_L(S'_1), \quad E_K(S_1) = E_K(S) \cup \bar{x}_0 E_K(S),$$

for $\bar{x}_0 \in E_K(S_1)$ with $(x_0)_{P_{m+1}} = \pi$, a local uniformizer. If $(y)_{S'_1} \in H_{S'_1}$ then $y_{P'_{m+1}} = 1$ or u', hence $H_{S'_1} = F_{S'}$ or $[H_{S'_1} : F_{S'}] = 2$. We have seen in the proof of Proposition 16 that the map $\zeta\colon F_{S'} \to H_{S'}$, defined by $\zeta((y)_{S'_1}) = (y)_{S'}$, is an injective homomorphism. It follows that

$$rk_2(H_{S'_1}) \le rk_2(F_{S'}) + 1 \le rk_2(H_{S'}) + 1$$

and thus

$$\delta_1 = |S| + 1 - rk_2(H_{S'_1}) \ge |S| - rk_2(H_{S'}) = \delta. \quad ■$$

Proposition 18 *Suppose that we extend tamely a correspondence*

$$\mathcal{C} = (S, S', T, (t_P)_{P\in S})$$

of defect δ by adding a pair of primes (P_{m+1}, P'_{m+1}). Then the defect δ_1 of the new correspondence satisfies the inequality:

$$\delta_1 \ge \delta.$$

Moreover, if $[P_{m+1}]$ is not a square in $C_K(S)$ and $[P'_{m+1}]$ is a square in $C_L(S')$, then $\delta_1 > \delta$.

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

Proof We will consider two cases:

Case 1 At least one of $[P_{m+1}]$ and $[P'_{m+1}]$ is not a square in the corresponding ideal S-class group.

Case 2 Both $[P_{m+1}]$ and $[P'_{m+1}]$ are squares in the corresponding ideal S-class groups.

Suppose we are in Case 1 and let us say that $[P_{m+1}]$ is not a square in $C_K(S)$. Then, by Lemma 6, we get $E_K(S_1) = E_K(S)$, so any element $(x)_{S_1} \in H_{S_1}$ has $x_{P_{m+1}}$ a unit.

By hypothesis, P_{m+1} is tame so $t_{P_{m+1}}(x_{P_{m+1}})$ is a unit. Choose $\bar{y} \in E_L(S')$ such that $\nu_{S'_1}(\bar{y}) = (t_P(x_P))_{P\in S_1}$. Then $\nu_{S'}(\bar{y}) = t_S(\nu_S(\bar{x}))$, so $(x)_S \in H_S$. Consequently the map $\lambda_S \colon H_{S_1} \to H_S$ defined by $\lambda_S((x)_{S_1}) = (x)_S$ is well defined. Moreover, there is a short exact sequence:

$$1 \to \operatorname{Ker}(\lambda_S) \to H_{S_1} \to \operatorname{Im}(\lambda_S) \to 1 \tag{1}$$

hence

$$rk_2(H_{S_1}) = rk_2(\operatorname{Ker}(\lambda_S)) + rk_2(\operatorname{Im}(\lambda_S)). \tag{2}$$

Then

$$\delta_1 = |S| + 1 - rk_2(\operatorname{Ker}(\lambda_S)) - rk_2(\operatorname{Im}(\lambda_S)). \tag{3}$$

We need to study the properties of the map λ_S. They are presented in Lemma 19 below. According to (3), if λ_S is injective then

$$\delta_1 = |S| + 1 - rk_2(\operatorname{Im}(\lambda_S)) \geq |S| + 1 - rk_2(H_S) = \delta + 1 > \delta.$$

Thus $\delta_1 \geq \delta$.

On the other hand, if λ_S is not injective, then by Lemma 19 it is surjective and according to (3)

$$\delta_1 = |S| + 1 - 1 - rk_2(H_S) = \delta,$$

so $\delta_1 \geq \delta$ in this case as well.

Let us consider now the situation when $[P_{m+1}]$ is not a square in $C_K(S)$ and $[P'_{m+1}]$ is a square in $C_L(S')$. We claim that in this case the map λ_S must be injective. Indeed, if λ_S were not injective, we would find $((1)_S, z) \in \operatorname{Ker}(\lambda_S)$, with $z \neq 1$. Since $[P_{m+1}]$ is not a square in $C_K(S)$, by Lemma 6 it follows that $E_K(S_1) = E_K(S)$, so $z = u$, the square class of a non-square unit at P_{m+1}. Since $((1)_S, u) \in H_{S_1}$ and $t_{P_{m+1}}$ is tame, we can find $\bar{y} \in E_L(S'_1)$ such that $\nu_{S'_1}(\bar{y}) = t_{S_1}\big(((1)_S, u)\big) = ((1)_{S'}, u')$, where u' is a local non-square unit at P'_{m+1}. On the other hand, since $[P'_{m+1}]$ is a square in $C_L(S')$ we can find an element $\bar{z} \in E_L(S'_1) \setminus E_L(S')$. Thus $z_{P'_{m+1}} = \pi$ is a local uniformizer at P'_{m+1}. By construction we get $(\bar{y}, \bar{z})_{P'} = 1$ for all $P' \in S'$ (where $\bar{y}$ is a local square) and for all $P' \notin S'_1$ (where both $\bar{y}$ and $\bar{z}$ are local units), while $(\bar{y}, \bar{z})_{P'_{m+1}} = -1$, and these equalities contradict Hilbert's reciprocity law. So necessarily λ_S is injective, and we have seen that in this situation $\delta_1 > \delta$. This completes the study of the first case and also proves the second part of the proposition.

Suppose now that we are in Case 2, so both $[P_{m+1}]$ and $[P'_{m+1}]$ are squares in the corresponding ideal S-class groups. Then, by Lemma 6, we get:

$$E_K(S_1) = E_K(S) \cup \bar{x}_0 E_K(S)$$

for some $\bar{x}_0 \in E_K(S_1) \setminus E_K(S)$, and

$$E_L(S'_1) = E_L(S') \cup \bar{y}_0 E_L(S')$$

for some $\bar{y}_0 \in E_L(S'_1) \setminus E_L(S')$.

Since $\bar{x}_0 \in E_K(S_1) \setminus E_K(S)$, $(x_0)_{P_{m+1}}$ is a uniformizer, and $(y_0)_{P'_{m+1}}$ is a uniformizer as $\bar{y}_0 \in E_L(S'_1) \setminus E_L(S')$. Define the following set, which is a subgroup of H_{S_1}:

$$J_S = \{(x)_{S_1} \in H_{S_1} : x_{P_{m+1}} \text{ is a unit}\}.$$

Claim: If $(x)_{S_1} \in J_S$ then $(x)_S \in H_S$.

In order to prove the claim, observe that by the definition of H_{S_1} we can find $\bar{y} \in E_L(S'_1)$ such that

$$(y)_S = t_S((x)_S),\ y_{P'_{m+1}} = t_{P_{m+1}}(x_{P_{m+1}}).$$

By hypothesis P_{m+1} is tame, so $y_{P_{m+1}}$ is a unit. Then $\bar{y} \in E_L(S')$ and since $\bar{x} \in E_K(S)$, it follows that $(x)_S \in H_S$, and this proves the claim.

Then the map $\lambda_S \colon J_S \to H_S$ defined by $\lambda_S((x)_{S_1}) = (x)_S$ is a well defined group homomorphism.

Now we will consider two subcases:

Subcase 2.1 There exists an element $(x^*)_{S_1} \in H_{S_1}$ such that $x^*_{P_{m+1}}$ is the square class of a uniformizer. Since P_{m+1} is tame, one can find an element $(y^*)_{S'_1} \in H_{S'_1}$ such that $y^*_{P'_{m+1}}$ is the square class of a uniformizer (and $t_{P_{m+1}}(x^*_{m+1}) = y^*_{m+1}$). Without loss of generality we can replace $\bar{x}_0$ by $\bar{x}^*$ and $\bar{y}_0$ by $\bar{y}^*$.

Then $H_{S_1} = J_S \cup (x^*)_{S_1} J_S$ so

$$rk_2(H_{S_1}) = rk_2(J_S) + 1. \tag{4}$$

Claim: λ_S is injective. Indeed, if $(1, \ldots, 1, a) \in \mathrm{Ker}(\lambda_S)$ and $(1, \ldots, 1, a) \neq (1, \ldots, 1, 1)$ then a is the square class of a non-square unit. Pick $\bar{a} \in E_K(S_1)$ such that $\nu_{S_1}(\bar{a}) = (1, \ldots, 1,\ a)$. Then $(\bar{a}, \bar{x}^*)_P = 1$ for all $P \neq P_{m+1}$ and $(\bar{a}, \bar{x}^*)_{P_{m+1}} = -1$, and that contradicts Hilbert's reciprocity law.

Since λ_S is injective, $rk_2(J_S) \leq rk_2(H_S)$ and if we use (4) we get:

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) = |S| + 1 - rk_2(J_S) - 1 \geq |S| - rk_2(H_S) = \delta,$$

which proves the inequality.

Subcase 2.2 There are no elements $(x)_{S_1} \in H_{S_1}$ such that $x_{P_{m+1}}$ is a uniformizer. Then, $J_S = H_{S_1}$.

If λ_S is injective then

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) \geq |S| + 1 - rk_2(H_S) \geq \delta + 1,$$

so the inequality $\delta_1 \geq \delta$ holds.

If λ_S is not injective, then pick $\bar{a} \in E_K(S_1)$ with $\nu_{S_1}(\bar{a}) = (1, \dots, 1, u) \in J_S$. We claim that in this situation λ_S is surjective. Indeed, if $(x)_S \in H_S$, let $\bar{x} \in E_K(S)$ and $\bar{y} \in E_L(S')$ such that $\nu_S(\bar{x}) = (x)_S$ and $\nu_{S'}(\bar{y}) = t_S((x)_S)$. Since $E_K(S) \subset E_K(S_1)$, $\bar{x} \in E_K(S_1)$. If $x_{P_{m+1}} \neq y_{P'_{m+1}}$ then $x_{P_{m+1}} u = y_{P'_{m+1}}$ and thus $\bar{x}\bar{a} \in E_K(S_1)$ and $\nu_{S_1}(\bar{x}\bar{a}) \in J_S$ is such that $\lambda_S(\nu_{S_1}(\bar{x}\bar{a})) = (x)_S$. So λ_S is surjective. Since λ_S is surjective we get $rk_2(J_S) = rk_2(H_S) + rk_2(\mathrm{Ker}(\lambda_S))$. Thus, since λ_S is not injective, $\mathrm{Ker}(\lambda_S)$ is a cyclic group with two elements (generated by $(1, \dots, 1, u)$) hence $rk_2(J_S) = rk_2(H_S) + 1$. We get:

$$\delta_1 = |S| + 1 - rk_2(H_{S_1}) = |S| + 1 - rk_2(J_S) = |S| + 1 - rk_2(H_S) - 1 = \delta$$

which proves the inequality $\delta_1 \geq \delta$. ■

Lemma 19 *Suppose that one extends tamely a correspondence (C) by adding a pair of primes (P_{m+1}, P'_{m+1}) such that $[P_{m+1}]$ is not a square in the corresponding ideal S-class group. Let $\lambda_S \colon H_{S_1} \to H_S$ be the projection map $\lambda_S((x)_{S_1}) = (x)_S$.*

1. *If λ_S is not injective then $\mathrm{Ker}(\lambda_S) \simeq C_2$, hence $rk_2(\mathrm{Ker}(\lambda_S)) = 1$.*
2. *If λ_S is not surjective then $[H_S : \mathrm{Im}(\lambda_S)] = 2$.*
3. *If λ_S is not injective then it is surjective.*

Proof 1. By Lemma 6, $E_K(S_1) = E_K(S)$ and consequently if $(x)_{S_1} \in \mathrm{Ker}(\lambda_S)$ and $(x)_S = (1)_S$, then $x_{P_{m+1}} \in \{1, u\}$. This implies

$$\mathrm{Ker}(\lambda_S) = \{(1, \dots, 1, 1),\ (1, \dots, 1, u)\} \simeq C_2.$$

2. Suppose that λ_S is not surjective, and let $(x_0)_S \in H_S \setminus Im(\lambda_S)$. Then one of the following two situations occurs:

(a) any element $\bar{x} \in E_K(S_1) = E_K(S)$ with $\nu_S(\bar{x}) = (x_0)_S$ has $x_{P_{m+1}} = 1$ and any element $\bar{y} \in E_L(S')$ with $\nu_{S'}(\bar{y}) = t_S((x_0)_S)$ has $y_{P'_{m+1}} = u'$, or
(b) any element $\bar{x} \in E_K(S_1) = E_K(S)$ with $\nu_S(\bar{x}) = (x_0)_S$ has $x_{P_{m+1}} = u$ and any element $\bar{y} \in E_L(S')$ with $\nu_{S'}(\bar{y}) = t_S((x_0)_S)$ has $y_{P'_{m+1}} = 1$.

We will give the details in case (a); case (b) follows by symmetry. Let $(z)_S \in H_S \setminus \mathrm{Im}(\lambda_S)$. Since $(z)_S \in H_S$, one can find $\bar{z} \in E_K(S)$ such that $\nu_S(\bar{z}) = (z)_S$ and one can find $\bar{w} \in E_L(S')$ such that $\nu_{S'}(\bar{w}) = t_S((z)_S)$. Without loss of generality, suppose that $w_{P'_{m+1}} = u$ and $z_{P_{m+1}} = 1$. Since $x_{P_{m+1}} = 1$ and $y_{P'_{m+1}} = u'$, we get $\bar{x}\bar{z} \in E_K(S)$, $\bar{y}\bar{w} \in E_L(S')$, and

$$(xz)_S = (x)_S(z)_S \in H_S,$$
$$(yw)_{S'} = (y)_{S'}(w)_{S'} = t_S((x)_S)t_S((z)_S) = t_S((xz)_S),$$

and

$$(xz)_{P_{m+1}} = 1, \ (yw)_{P'_{m+1}} = 1.$$

This means: $(x)_S(z)_S \in \operatorname{Im}(\lambda_S)$ or $(z)_S \in (x^{-1})_S \operatorname{Im}(\lambda_S)$. Thus $[H_S : \operatorname{Im}(\lambda_S)] = 2$.

3. Suppose that λ_S is non-injective. It is to be shown that λ_S is surjective. By hypothesis, λ_S is non-injective, so one can find $\bar{x}_0 \in E_K(S_1) = E_K(S)$ such that $\nu_{S_1}(\bar{x}_0) = (1, \dots, 1, u)$.

If λ_S were non-surjective, we would have to consider the two cases (a) and (b) from the proof of part 2. Let us say, for instance, that we are in case (a). For such $\bar{x} \in E_K(S_1)$ and $\bar{y} \in E_L(S')$ with $x_{P_{m+1}} = 1$ and $y_{P_{m+1}} = u'$, consider $\bar{x} \cdot \bar{x}_0$. Then

$$\nu_{S_1}(\bar{x} \cdot \bar{x}_0) = ((x)_S, u)$$

so that

$$\lambda_S((x \cdot x_0)_{S_1}) = (x)_S$$

which means that λ_S would be in fact surjective, a contradiction. ■

Corollary 20 *Let $\mathcal{C}_1$ be a correspondence that extends $\mathcal{C}$. Then $\delta_{\mathcal{C}_1} + |W(\mathcal{C}_1)| \geq \delta_{\mathcal{C}} + |W(\mathcal{C})|$.*

Proof If $\mathcal{C}_1$ differs from $\mathcal{C}$ by one pair of primes, then Proposition 16 and Proposition 18 show that if one extends $\mathcal{C}$ tamely, then its defect will not decrease and the wild set is unchanged, while if one extends $\mathcal{C}$ wildly, its defect may decrease by at most 1 and the size of the wild set will increase by 1. If $\mathcal{C}_1$ differs from $\mathcal{C}$ by more than one pair of primes, an argument by induction can be used. ■

3 The Main Results

3.1 Suitable Correspondences

Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a correspondence between K and L such that the S-class number of K and the S'-class number of L are odd. We will call such a correspondence *suitable*. In this section we will use the construction presented in [1] to extend a suitable correspondence to a small equivalence in a way guaranteed to minimize the number of additional wild primes introduced in the small equivalence.

First we wish to relate the defect of a correspondence to another invariant, $d_{S,S'}$, called the *obstruction* in J. Carpenter's paper [1]. In that paper, suitable correspondences $(S, S', T, (t_P)_{P\in S})$ are studied. The author notationally suppresses the maps T

and $(t_P)_{P\in S}$ and refers to such a correspondence as a *suitable pair* (S, S'). J. Carpenter defines the obstruction of a suitable pair (S, S') in the following way:

$$d_{S,S'} = \dim_{\mathbb{F}_2}(U_K(S)/\bar{H}_S),$$

where

$$\bar{H}_S = \{x \in U_K(S) : t_S(i_S(x)) \in i_{S'}(U_L(S'))\}.$$

In the above formula, i_S denotes the restriction of the map ν_S to $U_K(S)$.

Proposition 21 *If $\mathcal{C}$ is any suitable correspondence, then its defect and obstruction coincide.*

Proof In [1] it is proved that, when the class number $h_K(S)$ is odd, i_S is a group monomorphism, and thus

$$rk_2(i_S\big(U_K(S))\big) = rk_2(U_K(S)) = |S|.$$

This observation combined with Lemma 13 shows that

$$rk_2(i_S(U_K(S))) = rk_2(\omega_K(S)).$$

On the other hand,

$$i_S(U_K(S)) = \nu_S(U_K(S)) \subseteq \nu_S(E_K(S)) = \omega_K(S)$$

which imply $i_S(U_K(S)) = \omega_K(S)$. Similarly: $i_{S'}(U_L(S')) = \omega_L(S')$. Note that if $x \in \bar{H}_S$ then $\nu_S(x) = i_S(x)$ is such that $t_S(i_S(x)) \in i_{S'}(U_L(S')) = \omega_L(S')$, which implies that $i_S(x) \in H_S$. Hence $i_S(\bar{H}_S) \subseteq H_S$.

On the other hand, if $(x)_S \in H_S$ then $(x)_S \in \omega_K(S) = i_S(U_K(S))$ which means that actually $(x)_S \in i_S(\bar{H}_S)$. These observations prove that $i_S(\bar{H}_S) = H_S$.

Now since the groups involved in the definition of the obstruction are finite and have exponent equal to 2, then based on the above equality we get:

$$\begin{aligned} d_{S,S'} &= rk_2(U_K(S)/\bar{H}_S) = rk_2(U_K(S)) - rk_2(\bar{H}_S) \\ &= rk_2(i_S(U_K(S))) - rk_2(i_S(\bar{H}_S)) = rk_2(\omega_K(S)) - rk_2(H_S) = \delta. \end{aligned}$$ ∎

Lemma 22 ([1]) *Given a suitable correspondence involving (S, S') with $d_{S,S'} > 0$, there exist primes $P_{m+1} \in \Omega_K \setminus S$ and $P'_{m+1} \in \Omega_L \setminus S'$ such that $(S_1 = S \cup \{P_{m+1}\}, S'_1 = S' \cup \{P'_{m+1}\})$ is also a suitable pair and $d_{S_1,S'_1} < d_{S,S'}$.*

A consequence of the above "obstruction-killing lemma" is the fact that any suitable correspondence $\mathcal{C} = (S, S', (t_P)_{P\in S}, T)$ between K and L can be extended to a small equivalence between K and L. Since any small equivalence can be extended to a Hilbert symbol equivalence between K and L which is tame outside the sets that define the small equivalence ([6]), it follows that the only wild primes in K (if any), outside S, of the Hilbert symbol equivalence constructed in this way are among the primes that are adjoined by the procedure described in the proof of the obstruction-killing lemma. We recall here that J. Carpenter's procedure presented in [1] shows that:

- all the primes adjoined to S are wild;
- the number of such primes does not exceed $d_{S,S'}$.

Carpenter's analysis [1] allows the possibility that the number of additional such primes could be less than δ. The following proposition shows that the minimum number of primes that must be added to a suitable correspondence in order to obtain a small equivalence between the two fields is equal to the defect.

Proposition 23 *Any suitable correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ between K and L can be extended to a small equivalence between K and L by adding exactly δ wild primes.*

Proof Let W' be the set of wild primes added to S by the obstruction-killing procedure. We know that $|W'| \le \delta$.

In order to prove the other inequality, it is enough to show that by adding a pair of primes to an existing suitable correspondence like in the obstruction killing procedure, the defect decreases by at most 1. In the obstruction killing procedure one adds a pair of primes (P_{m+1}, P'_{m+1}) (*i.e.,* $T(P_{m+1}) = P'_{m+1}$) such that the classes in the corresponding ideal S-class groups are squares and defines the local map $t_{P_{m+1}}$ wildly. It is also shown that the defect decreases by at least 1 for the choice of the pair (P_{m+1}, P'_{m+1}). Proposition 16 shows that in this case the defect decreases by at most 1. Consequently, in Carpenter's construction the defect decreases by exactly one.

So, in order to make the defect 0 (*i.e.,* to obtain a small equivalence between K and L) we need to add exactly δ pairs of wild primes. ■

Proposition 23 shows that if the obstruction killing technique is applied to extend a suitable correspondence to a small equivalence then, at each step, the size of the wild set increases by 1 while the defect decreases by 1. At the end of the procedure we obtain a small equivalence with $|W(\mathcal{C})| + \delta_{\mathcal{C}}$ wild primes, where $W(\mathcal{C})$ denotes the wild set of the given correspondence. Corollary 20 shows that this is optimum in terms of the number of wild primes.

Now any Hilbert symbol equivalence $\mathcal{H}$ with a finite wild set contains a small equivalence that has the same set of wild primes. For instance, the small equivalence consists of: all infinite and dyadic primes; non-dyadic primes that represent the generators of the 2-Sylow subgroup of the ideal class groups; the wild primes of $\mathcal{H}$; other non-dyadic primes that make the defect equal to 0. Hence any Hilbert symbol equivalence that has a finite wild set can be regarded as the tame extension of a small equivalence.

Now suppose that $\mathcal{H}$ is a Hilbert symbol equivalence with a finite wild set that extends a suitable correspondence $\mathcal{C}$. Then $\mathcal{H}$ contains a small equivalence that has the same wild set. If this small equivalence contains $\mathcal{C}$ then, by the above argument, it has at least $|W(\mathcal{C})| + \delta_{\mathcal{C}}$ wild primes, and so does $\mathcal{H}$. If the small equivalence does not contain $\mathcal{C}$, define a larger small equivalence as the union of $\mathcal{C}$ with the above small equivalence. With the same argument, this larger small equivalence contains $\mathcal{C}$, so it has at least $|W(\mathcal{C})| + \delta_{\mathcal{C}}$ wild primes. This is also contained in $\mathcal{H}$, and it has the same wild set as $\mathcal{H}$. Consequently, $\mathcal{H}$ has at least $|W(\mathcal{C})| + \delta_{\mathcal{C}}$ wild primes.

We summarize these remarks:

Corollary 24 *Any suitable correspondence $\mathcal{C}$ between two algebraic number fields K and L can be extended to a Hilbert symbol equivalence that has $|W(\mathcal{C})| + \delta(\mathcal{C})$ wild primes. This is the minimum number of wild primes that any Hilbert symbol equivalence extending $\mathcal{C}$ can have.*

3.2 Non-Suitable Correspondences

Some of the results presented in this section are generalizations of A. Czogala's results from [3].

Definition 25 *A correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ is called non-suitable if at least one of the numbers $h_K(S) = |C_K(S)|$ and $h_L(S') = |C_L(S')|$ is even.*

Following closely some constructions from [3], we will present a method to extend a non-suitable correspondence to a suitable correspondence. This method minimizes the number of wild primes added to the correspondence.

Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a non-suitable correspondence and let

$$[P_1], \dots, [P_{\theta(S)}]$$

be the representatives of the cosets of primes in S that are linearly independent in C_K/C_K^2.

Let $\{a_1, \dots, a_h\}$ (with $h = |S|$ according to Corollary 14) be an $\mathbb{F}_2$-base for $K_0(S)/K_{sq}(S)$, and $b_1, \dots, b_l$ (with $l = rk_2(C_K(S))$) be an $\mathbb{F}_2$-base of $K_{sq}(S)/K^{*2}$. When constructing these bases pick $b_1 = -1$, if $-1 \in K_{sq}(S) \setminus K^2$, or $a_1 = -1$, if $-1 \in K_0(S) \setminus K_{sq}(S)$.

Similarly, let $\{a'_1, \dots, a'_{h'}\}$ (with $h' = |S'| = |S| = h$) be an $\mathbb{F}_2$-base for $L_0(S')/L_{sq}(S')$, and $b'_1, \dots, b'_{l'}$ (with $l' = rk_2(C_L(S'))$) be an $\mathbb{F}_2$-base of $L_{sq}(S')/L^{*2}$. As before, when constructing these bases pick $b'_1 = -1$, if $-1 \in L_{sq}(S') \setminus L^2$, or $a'_1 = -1$, if $-1 \in L_0(S') \setminus L_{sq}(S')$.

Lemma 26 *Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a correspondence. Then for every $P \in S$, $t_P(-1) = -1$.*

Proof Fix $P \in S$. For every $x \in K_P^*/K_P^{*2}$ we get:

$$(x, -1)_P = (x, x)_P = (t_P(x), t_P(x))_{TP} = (t_P(x), -1)_{TP}.$$

On the other hand,

$$(x, -1)_P = (t_P(x), t_P(-1))_{TP}.$$

Since t_P is surjective, we get $(y, -1)_{TP} = (y, t_P(-1))_{TP}$ for all y, and this ends the proof. ∎

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

Now since K and L are Witt equivalent, $-1 \in K^2$ if and only if $-1 \in L^2$. On the other hand, based on the previous lemma, for any P in S, -1 is a local square at P if and only if -1 is a local square at TP (as $t_P(-1) = -1$). In particular, $-1 \in K_{sq}(S)$ if and only if $-1 \in L_{sq}(S')$. Hence $b_1 = -1$ if and only if $b'_1 = -1$, and $a_1 = -1$ if and only if $a'_1 = -1$.

Without loss of generality we will assume that $l \le l'$.

Use Theorem 11 to pick primes $R_1, \dots, R_l$ outside S, in K, such that

$$\left(\frac{b_i}{R_i}\right) = -1, \quad i \in \{1, \dots, l\},$$

$$\left(\frac{b_j}{R_i}\right) = 1, \quad j \ne i \in \{1, \dots, l\},$$

$$\left(\frac{a_j}{R_i}\right) = 1, \quad j \in \{1, \dots, m\}, \quad i \in \{1, \dots, l\}.$$

Similarly, pick primes $R'_1, \dots, R'_{l'}$ outside S', in L, such that

$$\left(\frac{b'_i}{R'_i}\right) = -1, \quad i \in \{1, \dots, l'\},$$

$$\left(\frac{b'_j}{R'_i}\right) = 1, \quad j \ne i \in \{1, \dots, l'\},$$

$$\left(\frac{a'_j}{R'_i}\right) = 1, \quad j \in \{1, \dots, m'\}, \quad i \in \{1, \dots, l'\}.$$

It follows that for any $i \in \{1, \dots, l\}$, -1 is a local square at R_i iff -1 is a local square at R'_i. Indeed, if $-1 \in K^2$, then $-1 \in L^2$; so -1 is a local square at all the primes R_i, and -1 is a square at all the primes R'_i. If $b_1 = -1$, then necessarily $b'_1 = -1$, and the claim follows from the construction of the primes R_i, and R'_i, respectively. Finally, if $a_1 = -1$, then $a'_1 = -1$ and the claim follows from the same construction.

We will add to (S, S') the pair (R_1, R'_1), and define the local isomorphism

$$t_{R_1} \colon (K^*_{R_1})/(K^*_{R_1})^2 \to (L^*_{R'_1})/(L^*_{R'_1})^2$$

by $1 \to 1$, $b_1 \to b'_1$, and arbitrarily on the remaining classes. Note that this local isomorphism is tame, for b_1 and b'_1 are both local non-square units at R_1 and R'_1, respectively (by construction).

We claim that $[R_1]$ is not a square in $C_K(S)$: indeed, if $[R_1]$ were a square then there would be an equality

$$xO_K = R_1 I^2 P_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

and then

$$(x, b_1)_{R_1} = -1, \quad (x, b_1)_{P_i} = 1, \quad \forall i \in \{1, \dots, |S|\}$$

as b_1 is a local square at every $P \in S$, and

$$(x, b_1)_Q = 1, \quad Q \notin S \cup \{R_1\}$$

as both x and b_1 are local units at primes different from R_1 and outside S. The above equalities contradict Hilbert's reciprocity law.

Since we extend the correspondence by adding a tame prime, R_1, and $[R_1]$ is not a square in the corresponding ideal S-class group, we can use the construction presented in Case 1 of the proof of Proposition 18: we can define the projection map $\lambda_S\colon H_{S\cup\{R_1\}} \to H_S$. Note that $(1) \neq (b_1)_{S_1} \in \operatorname{Ker}(\lambda_S)$ because b_1 is a local square at all primes in S and it is a local non-square at R_1. Hence λ_S is non-injective and, by Lemma 19, it is surjective. The proof of Proposition 18 shows that in this case $\delta_1 = \delta$.

To sum up: we extend the correspondence tamely and both the wild set and the defect remain unchanged.

Now continue to add pairs (R_i, R_i') to the correspondence and define tame local maps as above. During this process the wild set and the defect are unchanged, which is optimum in terms of the number of wild primes (see Corollary 20).

Let us suppose now that after we add all possible pairs: $(R_1, R_1'), \dots, (R_l, R_l')$ the S'-class number is still even. Corollary 14 and Corollary 12 show that

$$\{[P_1], \dots, [P_{\theta(S)}], [R_1], \dots, [R_l]\}$$

is a base for C_K/C_K^2. So if $S^* = S \cup \{R_1, \dots, R_l\}$ then $h_K(S^*)$ is odd.

Our assumption is that $l \leq l'$. In fact we have $l < l'$, for if $l = l'$ then, as above, the S'^*-class number of L would be odd.

In this situation we will consider other primes in K to pair with the remaining primes $R_{l+1}', \dots, R_{l'}'$. We will use the following result (a proof of this result can be found in [6]):

Lemma 27 *If S is a finite set of primes in K such that $h_K(S)$ is odd and for each $P \in S$ we fix $x_P \in K_P^*/K_P^{*2}$, then there are infinitely many primes Q with the property that there is an $x \in K^*$ such that:*

$$x \equiv x_P, \quad P \in S;$$
$$\operatorname{ord}_Q(x) = 1;$$
$$\operatorname{ord}_P(x) = 0, \quad P \notin S \cup \{Q\}.$$

We use Lemma 27 to obtain primes $R_{l+1}, \dots, R_{l'}$ and elements $b_{l+1}, \dots, b_{l'}$ in K^* such that

$$b_{l+i} = 1 \text{ in } K_P^*/K_P^{*2},\ \forall P \in S \cup \{R_1, \dots, R_{l+i-1}\};$$
$$b_{l+i} = \pi \text{ in } K_{R_{l+i}}^*/K_{R_{l+i}}^{*2};$$
$$\operatorname{ord}_P(b_{l+i}) = 0, \quad P \notin S \cup \{R_1, \dots, R_{l+i}\}.$$

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

It is helpful to observe that -1 is a local square at all primes $R_{l+1}, \dots, R_{l'}$ for otherwise one contradicts Hilbert's reciprocity law. We already know that -1 is a local square at all primes $R'_{l+1}, \dots, R'_{l'}$. Then we have the liberty to define wild local maps at these primes.

So we will add (R_{l+1}, R'_{l+1}) to $(S^* = S \cup \{R_1, \dots, R_l\}, (S')^* = S' \cup \{R'_1, \dots, R'_l\})$, define $T(R_{l+1}) = R'_{l+1}$, and define the local map $t_{R_{l+1}}$ wildly:

$$1 \to 1,\ u \to \pi',\ \pi \to u',\ u\pi \to u'\pi'.$$

Note that b'_{l+1} is a local non-square unit at R'_{l+1}, and b_{l+1} is a local uniformizer at R_{l+1}. Our goal is to show that the defect is preserved by this construction.

Let $S_1^* = S^* \cup \{R_{l+1}\}$, and $(S')_1^* = (S')^* \cup \{R'_{l+1}\}$.

Claim 1: Any element $\bar{x} \in E_K(S^*)$ which maps to an element in H_{S^*} has $x_{R_{l+1}} = 1$.

In order to prove the claim, let $\bar{x} \in E_K(S^*)$ be such that $(x)_{S^*} \in H_{S^*}$. Since $\bar{x} \in E_K(S^*)$, we find $x_{R_{l+1}} = 1$ or u, the local non-square unit at R_{l+1}. Let us show that we cannot have $x_{R_{l+1}} = u$. If $x_{R_{l+1}} = u$ then

$$\begin{aligned}\prod_{P \in \Omega_K} (x, b_{l+1})_P &= \prod_{P \in S^*} (x, b_{l+1})_P \cdot (x, b_{l+1})_{R_{l+1}} \cdot \prod_{P \notin S_1^*} (x, b_{l+1})_P \\ &= \prod_{P \in S^*} (x, 1)_P \cdot (u, \pi)_{R_{l+1}} \cdot \prod_{P \notin S_1^*} (x, b_{l+1})_P = 1 \cdot (-1) \cdot 1 = -1,\end{aligned}$$

which contradicts Hilbert's reciprocity law. This concludes the proof of the claim.

Claim 2: Any $\bar{x} \in E_K(S^*)$ that has $x_{R_{l+1}} = 1$ maps to an element in $H_{S_1^*}$.

Indeed, if all elements $\bar{y} \in E_L((S')^*)$ such that

$$t_{S^*}(\nu_{S^*}(\bar{x})) = \nu_{(S')^*}(\bar{y})$$

have $y_{R'_{l+1}} = u'$ (the square class of the non-square unit), then let us multiply any such $\bar{y}$ by b'_{l+1}. Note that $\bar{y}b'_{l+1} \in E_L((S')^*) = E_L((S')_1^*)$, and

$$\nu_{(S')^*}(\bar{y}b'_{l+1}) = \nu_{(S')^*}(\bar{y}) = t_{S^*}(\nu_{S^*}(\bar{x})),$$

which means that $\bar{y}b'_{l+1}$ has all the properties of $\bar{y}$ except that its local component at R'_{l+1} is 1. This is a contradiction. Consequently $x_{S_1^*} \in H_{S_1^*}$ and the claim is proved.

Now let $F_{S_1^*} = \{(x) \in H_{S_1^*} : x_{R_{l+1}} = 1\}$. We can define a map $H_{S^*} \to F_{S^*}$ in the following way: for $(x)_{S^*} \in H_{S^*}$ choose $\bar{x} \in E_K(S^*)$ such that $\nu_{S^*}(\bar{x}) = (x)_{S^*}$; Claim 1 guarantees that $x_{R_{l+1}} = 1$, while Claim 2 ensures that $\nu_{S_1^*}(\bar{x}) = ((x)_{S^*}, 1)$. So we can define the map by sending $(x)_{S^*}$ to $((x)_{S^*}, 1)$. This is a well defined group homomorphism.

Claim 3: This map is an isomorphism.

In order to prove the claim, note that this map is injective. To prove surjectivity, fix $((x)_{S^*}, 1) \in F_{S^*}$ and choose $\bar{x} \in E_K(S_1^*)$ such that $\nu_{S_1^*}(\bar{x}) = ((x)_{S^*}, 1)$. Since $\bar{x} \in E_K(S_1^*)$ and $x_{R_{l+1}} = 1$, it follows that $\bar{x} \in E_K(S^*)$. On the other hand, since

https://doi.org/10.4153/CJM-2005-008-6 Published online by Cambridge University Press

$((x)_{S^*}, 1) \in H_{S_1^*}$, we can find $\bar{y} \in E_L(S_1'^*)$ such that $y_{R'_{l+1}} = 1$ (so $\bar{y} \in E_L(S'^*)$) and $t_{S^*}((x)_{S^*}) = (y)_{S'^*}$. But then $(x)_{S^*} \in H_{S^*}$ maps to $((x)_{S^*}, 1)$, so the map is surjective.

Note that $[R_{l+1}]$ has odd order in $C_K(S^*)$, hence it is a square (we have seen that $\operatorname{ord}(C_K(S^*))$ is odd for the 2-rank of $C_K(S^*)$ is equal to 0). On the other hand, $[R'_{l+1}]$ is not a square in $C_L((S')^*)$ because, according to Corollary 12,

$$[P'_1], \dots, [P'_{\theta(S')}], [R'_1], \dots, [R'_l], [R'_{l+1}]$$

are linearly independent in C_L/C_L^2. Then $E_L((S')^*) = E_L((S')_1^*)$ (see Lemma 6). Note that $(b_{l+1})_{S_1^*} = (1, \dots, 1, \pi) \in H_{S_1^*}$ (by construction). Consequently, we can write

$$H_{S_1^*} = F_{S^*} \cup (b_{l+1})_{S_1^*} F_{S^*},$$

where $F_{S_1^*} = \{(x) \in H_{S_1^*} : x_{R_{l+1}} = 1\}$. Thus $[H_{S_1^*} : F_{S^*}] = 2$.

If we combine the last equality with Claim 3, we get $rk_2(H_{S_1^*}) = rk_2(H_{S^*}) + 1$. Then:

$$\delta_{S_1^*} = |S^*| + 1 - rk_2(H_{S_1^*}) = |S^*| + 1 - rk_2(H_{S^*}) - 1 = \delta_{S^*}.$$

So the defect is preserved, which is the best one can get when for exactly one of the primes in the pair (R_{l+1} in this case) the class in the ideal S^*-class group is a square (see Lemma 17). Note that the ideal class of any prime outside S^* is a square in $C_K(S^*)$, so the procedure described above is optimal in terms of defect. It does increase the size of the wild set but, according to Proposition 18, since $[R_{l+1}]$ is a square in $C_K(S^*)$ and $[R'_{l+1}]$ is not a square in $C_L(S'^*)$, extending tamely the correspondence will result in increasing the defect. So overall there would be no benefit.

The result that we proved can be stated in the following way:

Proposition 28 *Let $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ be a non-suitable correspondence. Then $\mathcal{C}$ can be extended to a suitable correspondence $\mathcal{C}'$ that has the same defect and such that*

$$|W(\mathcal{C}')| = |W(\mathcal{C})| + |rk_2(C_L(S')) - rk_2(C_K(S))|.$$

Proof The procedure of obtaining $\mathcal{C}'$ has been presented above. We have seen that the defect is preserved, and the number of wild primes added to the correspondence equals $|rk_2(C_L(S')) - rk_2(C_K(S))|$. ∎

Theorem 29 *Any correspondence $\mathcal{C} = (S, S', T, (t_P)_{P\in S})$ between two number fields K and L, of defect δ and wild set W, can be extended to a Hilbert symbol equivalence between K and L that has*

$$\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(S'))|$$

wild primes. Moreover, any other extension of $\mathcal{C}$ to a Hilbert symbol equivalence between K and L has a wild set of size no less than $\delta + |W| + |rk_2(C_K(S)) - rk_2(C_L(S'))|$.

Proof The first part follows from Proposition 23 and Proposition 28.

For the second part, here are the details. When extending a non-suitable correspondence to a suitable one, we consider the pairs $(R_1, R'_1), \dots, (R_l, R'_l)$, where $\{[R_i] : i = 1, \dots, l\}$ is an $\mathbb{F}_2$-base for $C_K(S)/C_K(S)^2$, and $\{[R'_i] : i = 1, \dots, l'\}$ is an $\mathbb{F}_2$-base for $C_L(S')/C_L(S')^2$. For each one of these pairs the defect is unchanged, and so is the wild set (as the local maps are tame). According to Corollary 20, this construction is optimal. As long as $rk_2(C_L(S'^*))$ is still even, the remaining classes $\{[R'_i] : i = l+1, \dots, l'\}$ are not squares in $C_L(S'^*)$. Moreover, any remaining prime P will be a square in $C_K(S^*)$. So we have to find a pair P for R_{l+1}. No matter how we choose P, Proposition 18 shows that if the local map is tame then the defect increases, while Lemma 17 shows that if the local map is wild, the defect does not decrease but the size of the wild set increases by 1. In either situation, the sum of the defect and the size of the wild set increases by at least 1. In our construction, the sum increases at each step by exactly 1, which is optimal. Note that one cannot obtain a suitable correspondence by using a smaller number of primes, as a correspondence is suitable precisely when both $C_K(S^*)/C_K(S^*)^2$ and $C_L(S'^*)/C_L(S'^*)^2$ are trivial, so we need to have in S^* and S'^*, respectively, all the elements in the two bases. ■

In many situations, computing the defect of a correspondence may be difficult. It might be interesting to find bounds for the minimum number of wild primes in Hilbert symbol equivalences between two number fields. If D is the set of dyadic primes in K and S consists of D and the infinite primes, then we obtain directly:

Corollary 30 *Let $W = \mathrm{Wild}(K, L)$ be a minimum set of wild primes of Witt equivalent number fields K and L. Then:*

$$|rk_2C_K(D) - rk_2C_L(TD)| \le |W \setminus D| \le |rk_2C_K(D) - rk_2C_L(TD)| + |D| + r + s.$$

The above corollary gives bounds for the number of non-dyadic primes in a minimum wild set. In particular, when K and L are Witt equivalent non-real number fields of degree n, this number exceeds the difference in 2-ranks of the ideal D-class groups by at most $5n/2$ (the number of complex places is $n/2$ and the number of dyadic primes is at most n). The splitting of 2 in K affects strongly this deviation, because if in addition 2 stays inert in K then the number of wild non-dyadic primes in the minimum wild set exceeds the difference in 2-ranks of the ideal D-class groups by at most $n/2 + 2$.

From the above corollary we obtain directly:

Corollary 31 *Let $W = \mathrm{Wild}(K, L)$ be a minimum wild set for two Witt equivalent number fields K and L. Let D and D' be the sets of dyadic primes in K and L, respectively. Then:*

$$|rk_2C_K(D) - rk_2C_L(D')| \le |W| \le |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

Finally, if we combine this result with Proposition 1 we obtain:

Proposition 32 *If K and L are Witt equivalent number fields then*

$$|rk_2^+C_K(D) - rk_2^+C_L(D')| \le |rk_2C_K(D) - rk_2C_L(D')| + 2|D| + r + s.$$

3.3 Example

Let d_1 and d_2 be two square-free positive integers such that $d_1 \equiv 3 \pmod 8$ and $d_2 \equiv 3 \pmod 8$, and define $K = \mathbb{Q}(\sqrt{-d_1})$ and $L = \mathbb{Q}(\sqrt{-d_2})$. According to [3], these two number fields are Witt equivalent. The discriminants of K and L are $-d_1$ and $-d_2$, respectively. Since the discriminants are congruent to $5 \pmod 8$, the rational prime 2 is inert in both fields: $2O_K = P$, $2O_L = P'$, with $f(P|2) = f(P'|2) = 2$. Then the completions K_P and $L_{P'}$ are unramified quadratic extensions of $\mathbb{Q}_2$. $\mathbb{Q}_2$ has a unique unramified quadratic extension: $\mathbb{Q}_2(\sqrt{-3})$ (see [8, Proposition 6-5-5]), hence $K_P = L_{P'} = \mathbb{Q}_2(\sqrt{-3})$, which means that K_P^*/K_P^{*2} and $L_{P'}^*/L_{P'}^{*2}$ are the same.

Let $S = \{P, P_\infty\}$ and $S' = \{P', P'_\infty\}$, where P_∞ and P'_∞ are the infinite complex primes in K and L respectively. For this choice, $G_K(S) = K_P^*/K_P^{*2}$ and $G_L(S') = L_{P'}^*/L_{P'}^{*2}$ which are canonically identified ("equal") by the identity map. Let T be the map that sends P_∞ to P'_∞ and P to P', and define $t_P\colon K_P^*/K_P^{*2} \to L_{P'}^*/L_{P'}^{*2}$ to be the identity map.

Therefore we have an example of a simple correspondence $\mathcal{C} = (S, S', T, (\mathrm{id}, \mathrm{id}))$.

Since the local map is the identity, the correspondence has no wild primes.

We wish to show next that the defect of this correspondence equals 0. To show that, observe that $\bar{1}$, $-\bar{1}$, and $\bar{2}$ are distinct linearly independent classes in K_P^*/K_P^{*2} and in fact $\bar{1}, -\bar{1}, \bar{2} \in \omega_K(S)(= \mathrm{Im}(\nu_S))$. But remember that $rk_2(\omega_K(S)) = |S| = 2$, and thus $\{-\bar{1}, \bar{2}\}$ is an $\mathbb{F}_2$-base for $\omega_K(S)$. Similarly one can show that $\{-\bar{1}, \bar{2}\}$ is an $\mathbb{F}_2$-base for $\omega_L(S')$, and hence $\omega_K(S) = \omega_L(S')$ which implies that the defect equals 0.

For $\mathcal{C}$, the number of wild primes is 0, the defect is equal to 0, so this correspondence can be extended to a Hilbert symbol equivalence that has $|rk_2(C_K(S)) - rk_2(C_L(S'))|$ wild primes. This is the minimum number of wild primes that *any* Hilbert symbol equivalence can have. Since in the ideal class groups both $P = 2O_K$ and $P' = 2O_L$ are trivial, $C_K(S) = C_K$ and $C_L(S') = C_L$. Thus the minimum number of wild primes is $|rk_2(C_K) - rk_2(C_L)|$. But according to Gauss, the 2-rank of C_K is $k - 1$, where k is the number of distinct prime divisors of $-d_1$, and the 2-rank of C_L is $l - 1$, where l is the number of distinct prime divisors of $-d_2$. By choosing $d_1 = 3$ we have $rk_2(C_K) = 0$, and by choosing $d_2 = 3p_1 \cdots p_N$, with $p_1, p_2, \ldots, p_N$ distinct rational primes congruent to 1 mod 8, it follows directly that for any non-negative integer N there are pairs of (quadratic) Witt equivalent number fields for which the minimum number of wild primes is equal to N. On the other hand, by choosing $k = l$, one can construct infinitely many pairs of tamely equivalent number fields with no wild primes.

Acknowledgment The author wishes to express his gratitude to Robert Perlis and P. E. Conner for their valuable comments and suggestions, and to the referee for simplifying the proof of Corollary 14.

References

[1] J. Carpenter, *Finiteness theorems for forms over global fields*. Math. Z. **209**(1992), 153–166.

[2] P. E. Conner, R. Perlis and K. Szymiczek *Wild sets and* 2*-ranks of class groups*. Acta Arith. **79**(1997), 83–91.

[3] A. Czogala, *On reciprocity equivalence of quadratic number fields*. Acta Arith. **58**(1991), 29–46.

[4] E. Hecke, *Lectures on the Theory of Algebraic Numbers*. Graduate Texts in Mathematics, 77, Springer-Verlag, New York, 1981.
[5] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*. W.A. Benjamin, Reading, MA, 1973.
[6] R. Perlis, K. Szymiczek, P. E. Conner and R. Litherland, *Matching Witts with global fields*. Contemp. Math. **155**(1994), 365–387.
[7] K. Szymiczek, *Witt equivalence of global fields*. Comm. Algebra **19**(1991), 1125–1149.
[8] E. Weiss, *Algebraic Number Theory*. Dover Publications, Mineola, NY, 1998.

Department of Mathematics
University of Northern Iowa
Cedar Falls, IA 50614
U.S.A.
e-mail: somodi@math.uni.edu