*Homology, Homotopy and Applications, vol. 14(2), 2012, pp.189–196*

# EVERY BINARY SELF-DUAL CODE ARISES FROM HILBERT SYMBOLS

TED CHINBURG AND YING ZHANG

(*communicated by Charles A. Weibel*)

*Abstract*

In this paper we construct binary self-dual codes using the étale cohomology of $\mu_2$ on the spectra of rings of $S$-integers of global fields. We will show that up to equivalence, all self-dual codes of length at least 4 arise from Hilbert pairings on rings of $S$-integers of $\mathbb{Q}$. This is an arithmetic counterpart of a result of Kreck and Puppe, who used cobordism theory to show that all self-dual codes arise from Poincaré duality on real three manifolds.

## 1. Introduction

Recently, M. Kreck and V. Puppe [**4**] gave a topological construction of all self-dual codes using the cohomology of three-manifolds. A self-dual code is a triple $(W, V, E)$ in which $W$ is a vector space of finite even dimension over $\mathbb{F}_2$, $V$ is a subspace of $W$, $E$ is an ordered basis $\{e_i\}_{i=1}^{2n}$ of $W$ and $V$ is its own orthogonal complement with respect to the bilinear form $\langle\ ,\ \rangle\colon W \times W \to \mathbb{F}_2$ defined by

$$\Big\langle \sum_{i=1}^{2n} a_i e_i, \sum_{i=1}^{2n} b_i e_i \Big\rangle = \sum_{i=1}^{2n} a_i b_i.$$

This implies that $V$ has dimension $n$. In the following we will call the pair $(W, E)$ together with the form $\langle\ ,\ \rangle$ a Euclidean space over $\mathbb{F}_2$, and $E$ is an orthonormal basis for $\langle\ ,\ \rangle$. Another self-dual code $(W', V', E')$ is defined to be equivalent to $(W, V, E)$ if there is a bijection between $E$ and $E'$ which when extended to an $\mathbb{F}_2$-linear isomorphism $W \to W'$ carries $V$ to $V'$.

The object of this note is to give a construction of self-dual codes which exploits the analogy between three-manifolds and the spectra of rings of $S$-integers of global fields.

Let $K$ be a global field of characteristic different from 2. If $K$ is a function field, let $X$ be a smooth projective curve with function field $K$. If $K$ is a number field, let $\mathcal{O}_K$ be the ring of integers of $K$ and let $X = \operatorname{Spec} \mathcal{O}_K$. Suppose $v$ is a place of $K$ and that $\mathcal{F}$ is a sheaf on the small étale site of $\operatorname{Spec} K_v$, where $K_v$ is the completion of $K$ at $v$. We define the reduced étale cohomology group $H^r_{\mathrm{et}}(K_v, \mathcal{F})$ to be the usual étale

Ted Chinburg was partially supported by NSF grant DMS-1100355.
Received May 8, 2012, revised September 4, 2012; published on November 28, 2012.
2000 Mathematics Subject Classification: 14G50; 14F20, 94B05, 11T71.
Key words and phrases: binary self-dual code, $S$-integer, étale cohomology.
Article available at `http://intlpress.com/HHA/v14/n2/a11` and `doi:10.4310/HHA.2012.v14.n2.a11`

cohomology group unless $v$ is real, in which case we let $H^r_{\mathrm{et}}(K_v, \mathcal{F}) := H^r_T(\mathbb{Z}/2, \mathcal{F})$ be the $r^{\mathrm{th}}$ Tate cohomology of the $\mathrm{Gal}(\overline{K_v}/K_v) \cong \mathbb{Z}/2$ module associated to $\mathcal{F}$. When $K$ is a number field, we let $H^r_c(\mathrm{Spec}\, \mathcal{O}_K, \mathcal{F})$ be the cohomology group with compact support defined by Milne [**5**, Section 2, p. 165].

Let $S$ be a finite non-empty set of places of $K$ which contains all the archimedean places and all places of residue characteristic 2. Let $U$ be the open complement of $S$ in $X$. We have a long exact sequence

$$\cdots H^r_c(U, \mathcal{F}) \to H^r_{\mathrm{et}}(U, \mathcal{F}) \to \oplus_{v \in S} H^r_{\mathrm{et}}(K_v, i_v^* \mathcal{F}) \xrightarrow{\delta_r} H^{r+1}_c(U, \mathcal{F}) \cdots , \qquad (1)$$

where $i_v \colon \mathrm{Spec}\, K_v \to X$ is the canonical morphism. We show the following result in Section 2:

**Theorem 1.1.** *The image of the restriction homomorphism*

$$\Phi \colon H^1_{\mathrm{et}}(U, \mu_2) \to \oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)$$

*is its own orthogonal complement with respect to the non-degenerate bilinear product*

$$\left(\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)\right) \times \left(\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)\right) \to \oplus_{v \in S} H^2_{\mathrm{et}}(K_v, \mu_2) \xrightarrow{\delta_2} H^3_c(U, \mu_2) \cong \mathbb{F}_2, \qquad (2)$$

*which is the composition of the natural cup product pairing with the boundary map of (1) for $r = 2$.*

Therefore, if there is an orthonormal basis $E$ for the bilinear product (2) such that $\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)$ is Euclidean with respect to $E$, then image($\Phi$) becomes a self-dual code by definition. This matter is addressed by the following result, which is also proved in Section 2:

**Theorem 1.2.** *If $v \in S$ is complex, then $H^i_{\mathrm{et}}(K_v, \mu_2) = 0$ for all $i \geqslant 1$. Otherwise, there is a Euclidean basis for the cup product pairing*

$$H^1_{\mathrm{et}}(K_v, \mu_2) \times H^1_{\mathrm{et}}(K_v, \mu_2) \to H^2_{\mathrm{et}}(K_v, \mu_2) \cong \mathbb{F}_2$$

*if and and only if $-1$ is not a square in $K_v$.*

*Remark 1.3.* If $v$ is not complex, then $-1$ is not a square in $K_v$ when (i) $v$ is real, or (ii) $v$ is non-archimedean and the order of the residue field of $v$ is congruent to 3 mod 4, or (iii) $v$ is non-archimedean of even residue characteristic and $-1 \notin (K_v^*)^2$.

**Corollary 1.4.** *If every non-complex place $v$ of $S$ satisfies one of conditions (i)–(iii) of Remark 1.3, then the union of the Euclidean bases produced by Theorem 1.2 gives a Euclidean basis for the bilinear product space $\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)$ which is the orthogonal sum of the $H^1_{\mathrm{et}}(K_v, \mu_2)$. With respect to this basis the image of $\Phi$ in Theorem 1.1 is a self-dual code. This is the case, in particular, if $K = \mathbb{Q}$ and every odd finite place $v$ in $S$ has residue field order congruent to 3 mod 4.*

Suppose $E$ is a basis for a finite dimensional space $W$ over $\mathbb{F}_2$ and that $\langle\ ,\ \rangle$ is the associated Euclidean bilinear form. Let $n = \dim_{\mathbb{F}_2}(W)$. The orthogonal group $O(n)$ is defined to be the group of linear transformations of $W$ which respect $\langle\ ,\ \rangle$. The group $O(n)$ equals the group of permutations of the basis $E$ if and only if $n \leqslant 3$.

Therefore, when $\dim(H^1_{\text{et}}(K_v, \mu_2)) \leqslant 3$ for all $v \in S$, the above orthonormal basis for $H^1_{\text{et}}(K_v, \mu_2)$ is unique up to permutations. In fact, $\dim(H^1_{\text{et}}(K_v, \mu_2)) > 3$ if and only if $K_v$ is a non-trivial extension of $\mathbb{Q}_2$, see [**6**, Proposition 5.7, Chap. II].

Our second main result is the following arithmetic analogue of Proposition 2 of [**4**]:

**Theorem 1.5.** *Up to equivalence, all self-dual codes of length at least* 4 *arise from the construction in Corollary 1.4 when* $K = \mathbb{Q}$. *In fact, each such code arises up to equivalence from infinitely many different subsets* $S$ *of the places of* $K = \mathbb{Q}$.

To conclude this introduction, we give a more explicit description of the codes produced by Corollary 1.4 under the hypothesis that $\text{Pic}(U)$ has odd order. This hypothesis is simply that the ring $O_{K,S}$ of $S$-integers of $K$ has class group of odd order. In this case, $H^1_{\text{et}}(U, \mu_2)$ is isomorphic to $O^*_{K,S}/(O^*_{K,S})^2$. The group $H^1_{\text{et}}(K_v, \mu_2)$ is isomorphic to $K^*_v/(K^*_v)^2$. The pairing

$$H^1_{\text{et}}(K_v, \mu_2) \times H^1_{\text{et}}(K_v, \mu_2) \to H^2_{\text{et}}(K_v, \mu_2) \subset \mathbb{F}_2$$

is the Hilbert pairing

$$K^*_v/(K^*_v)^2 \times K^*_v/(K^*_v)^2 \to \{\pm 1\} \cong \mathbb{F}_2 \tag{3}$$

(see [**7**, Chap. XIV]). The code space

$$\Phi(O^*_{K,S}/(O^*_{K,S})^2) \subset \oplus_{v \in S} K^*_v/(K^*_v)^2$$

is simply the subgroup which is the diagonal image of $O^*_{K,S}$ under the natural homomorphism induced by the inclusion of $K$ into $K_v$ for $v \in S$. When each non-complex $v$ satisfies one of the conditions in Remark 1.3, $K^*_v/(K^*_v)^2$ has a Euclidean basis. The Euclidean structure of the vector space $\oplus_{v \in S} K^*_v/(K^*_v)^2$ comes from the orthogonal sum of the structures from each of the Hilbert pairings (3).

When $K = \mathbb{Q}$ and $S = \{\infty, 2, p_1, \ldots, p_n\}$ for some positive primes $p_i \equiv 3 \bmod 4$, the group $O^*_{K,S}$ is the group $\langle -1, 2, p_1, \ldots, p_n \rangle$. The Hilbert pairings in (3) are easily described in this case (see Section 3). For example, when $S = \{\infty, 2, 3, 7\}$, one generates the Hamming code $e_8$. When

$$S = \{\infty, 2, 7, 19, 31, 131, 179, 367, 883, 1223, 1307, 39079\},$$

one gets the Golay code $g_{24}$.

In the course of proving Theorem 1.5 in Section 3, we give a new parametrization of self-dual codes via matrices consisting of $1 \times 2$ blocks which have certain properties ("boxed matrices"). The theorem is proved by showing that all self-dual codes are equivalent to codes which have boxed descriptions. This has consequences to the description of unimodular lattices, in view of the connection between such lattices and self-dual codes proved in [**3**].

It would be very interesting to see if boxed matrix descriptions of codes are also useful in the topological context considered by Kreck and Puppe, e.g., in trying to construct explicitly the three manifolds giving rise to self-dual codes. At present, the construction of these manifolds is indirect and proceeds by showing that certain elements of cobordism groups are trivial. It would also be interesting if one could see the proof of Theorem 1.5 for $K = \mathbb{Q}$ as a kind of explicit cobordism calculation concerning the étale "surfaces" $\text{Spec}(K_v)$ inside the étale "three-manifold" $\text{Spec}(\mathbb{Z})$.

## 2. Etale cohomology over ring of integers

*Proof of Theorem 1.1.* We will first prove Theorem 1.1, whose notations we now assume.

Artin-Verdier duality (cf. [**5**, Section II.3]) shows that

$$H^r_{\mathrm{et}}(U, \mu_2(-1)) \times H^{3-r}_c(U, \mu_2) \to H^3_c(U, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z} \tag{4}$$

is a perfect duality of $\mathbb{F}_2$ vector spaces. Here $\mu_2(-1) := \mathcal{H}om(\mu_2, \mathbb{G}_m)$ is canonically isomorphic to $\mu_2$. In the following we will not distinguish between these two sheaves.

For ease of notation, we denote $A = H^1_{\mathrm{et}}(U, \mu_2)$, $B = \oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)$ and $C = H^2_c(U, \mu_2)$. The pairing $B \times B \to \mathbb{F}_2$, which is the sum of the Hilbert symbols at $v$ for $v \in S$, is a perfect pairing by local class field theory. This identifies the dual $\check{B} = \mathrm{Hom}_{\mathbb{F}_2}(B, \mathbb{F}_2)$ of $B$ with $B$. By (4) we have perfect pairing $A \times C \to \mathbb{F}_2$, which identifies $\check{A}$ with $C$. From (1) for $r = 1$ we have an exact sequence

$$A \xrightarrow{\Phi} B \xrightarrow{\Psi} C.$$

Here the above pairings identify $\Psi \colon B = \check{B} \to C = \check{A}$ with the dual $\check{\Phi}$ of $\Phi$. Hence

$$\dim(\mathrm{coker}(\Phi)) = \dim(\ker(\check{\Phi})) = \dim(\ker(\Psi)) = \dim(\mathrm{image}(\Phi)),$$

where the last equality follows from the above exact sequence. Thus $\dim(\mathrm{image}(\Phi)) = \frac{1}{2}\dim(B)$, so all we now must show is that $\mathrm{image}(\Phi)$ is self-annihilating. This is true for the following reasons: The pairing $B \times B \to \mathbb{F}_2$ is given by the composition of the natural cup product pairing

$$\left(\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)\right) \times \left(\oplus_{v \in S} H^1_{\mathrm{et}}(K_v, \mu_2)\right) \to \left(\oplus_{v \in S} H^2_{\mathrm{et}}(K_v, \mu_2)\right)$$

with the boundary homomorphism

$$\oplus_{v \in S} H^2_{\mathrm{et}}(K_v, \mu_2) \xrightarrow{\delta_2} H^3_c(U, \mu_2) \cong \mathbb{F}_2.$$

The pairing of two elements in the image of $A \to B$ is 0 because the cup product of such elements in $H^2_{\mathrm{et}}(U, \mu_2)$ has trivial image under the composition of homomorphisms

$$H^2_{\mathrm{et}}(U, \mu_2) \to \oplus_{v \in S} H^2_{\mathrm{et}}(K_v, \mu_2) \xrightarrow{\delta_2} H^3_c(U, \mu_2)$$

in (1) when $r = 2$. This completes the proof. □

*Proof of Theorem 1.2.* We now prove Theorem 1.2. A non-trivial vector space $W$ over $\mathbb{F}_2$ equipped with any non-degenerate bilinear product $\langle\ ,\ \rangle$ has a Euclidean basis if and only if there is an $x \in W$ such that $\langle x, x \rangle = 1$ is non-trivial in $\mathbb{F}_2$. This is easy to prove when $W$ has dimension less than or equal to 3, and the general case follows by induction on dimension.

Suppose now that $v$ is not a complex place. The pairing

$$H^1_{\mathrm{et}}(K_v, \mu_2) \times H^1_{\mathrm{et}}(K_v, \mu_2) \to H^2_{\mathrm{et}}(K_v, \mu_2) \cong \mathbb{F}_2$$

is the Hilbert pairing

$$(\ ,\ )_v \colon K_v^*/(K_v^*)^2 \times K_v^*/(K_v^*)^2 \to \{\pm 1\} \cong \mathbb{F}_2.$$

This pairing has a Euclidean basis if and only if there is an element $\alpha \in K_v^*/(K_v^*)^2$ such that $(\alpha, \alpha)_v = -1 \in \pm 1$. Here $(\alpha, \alpha)_v = (\alpha, -\alpha)_v \cdot (\alpha, -1)_v = (\alpha, -1)_v$. By the

definition of the Hilbert pairing,

$$(\alpha, -1)_v = \sigma(\sqrt{-1})/\sqrt{-1}$$

where $\sigma \in \mathrm{Gal}(K_v(\sqrt{-1})/K_v) = G$ is the image of $\alpha$ under the Artin map $\sigma\colon K_v^* \to G$. Hence there exists $\alpha$ with $(\alpha, -1)_v = -1$ if and only if $K_v(\sqrt{-1})$ is a non-trivial extension of $K_v$. This completes the proof of Theorem 1.2. □

To conclude this section we make a few comments concerning the comparison of the above construction with that of Proposition 2 of [**4**]. The code space considered by Kreck and Puppe is the image of the natural homomorphism

$$H^1(W, \mathbb{F}_2) \to H^1(\partial W, \mathbb{F}_2) = \oplus_{i=1}^{2n} H^1(\mathbb{R}P^2, \mathbb{F}_2)$$

in which $W$ is a three-manifold with boundary $\partial W$ the disjoint union of $2n$ copies of $\mathbb{R}P^2$. Each $\mathbb{R}P^2$ is the boundary of a three-orbifold which is the quotient of a three-dimensional ball $B^3$ by the antipodal involution which fixes the center of $B^3$. In the arithmetic context, the role of $\mathbb{R}P^2$ is played by $\mathrm{Spec}(K_v)$, which has étale cohomological dimension 2 when $v$ is finite. The fixed loci of the involution should be compared to the spectrum of the residue field $\mathrm{Spec}(k(v))$. However, when $k(v)$ is the residue field of a finite place, $\mathrm{Spec}(k(v))$ has étale cohomological dimension 1 rather than 0. So a better topological counterpart would make $\partial W$ a finite disjoint union of connected smooth surfaces $S_i$, each of which is the boundary of a three orbifold which is the quotient of a neighborhood of a circle by an involution which fixes the circle. Klein bottles and two-dimensional tori could be realized as boundaries of such three orbifolds. When $S_i$ is a Klein bottle, $H^1(S_i, \mathbb{F}_2)$ is two-dimensional and the cup product $H^1(S_i, \mathbb{F}_2) \times H^1(S_i, \mathbb{F}_2) \to H^2(S_i, \mathbb{F}_2) \cong \mathbb{F}_2$ has a Euclidean structure. Thus a Klein bottle is analogous to $\mathrm{Spec}(K_v)$ when $\#k(v) \equiv 3 \bmod 4$. A two-dimensional torus is analogous to $\mathrm{Spec}(K_v)$ when $\#k(v) \equiv 1 \bmod 4$, since in this case the cup product pairing on $H^1$ does not have a Euclidean structure.

## 3. Hilbert symbol codes over $\mathbb{Q}$

Let $S$ be a finite set of places of $\mathbb{Q}$ consisting of the infinite place $\infty$, the place determined by the prime 2, and the places determined by a finite set $p_1, \ldots, p_{n-2}$ of distinct positive prime numbers which are congruent to 3 mod 4. The $S$-units $\mathbb{Z}_S^*$ of $\mathbb{Z}$ are then the subgroup $\langle -1, 2, p_1, \ldots, p_{n-2}\rangle$ of $\mathbb{Q}^*$ generated by $-1, 2, p_1, \ldots, p_{n-2}$. Recall that for each place $v_p \in S$ we have a Hilbert symbol pairing

$$(\ ,\ )_{v_p}\colon \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \to \mathbb{F}_2.$$

Write the $\mathbb{F}_2$ vector space $W_p$ additively for the multiplicative group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. The space $W = \oplus_{v_p \in S} W_p$ is a finite dimensional vector space over $\mathbb{F}_2$, and we have a non-degenerate pairing $(\ ,\ )\colon W \times W \to \mathbb{F}_2$ defined by $(\ ,\ ) = \sum_{v_p \in S}(\ ,\ )_{v_p}$. Now we specify an explicit basis for each $W_p$ with respect to which the pairing $W \times W \to \mathbb{F}_2$ is Euclidean.

For an odd prime $p$ congruent to 3 mod 4, $-1$ is a non-square in $\mathbb{Q}_p^*$. We choose the representatives $\{-p, p\}$ in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ for the $\mathbb{F}_2$ basis for $W_p$. For $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ we use the representatives $\{-2, -10, -5\}$. For $\mathbb{R}^*/(\mathbb{R}^*)^2$ we use $-1$. It is an easy calculation to show that under this basis the Hilbert symbol pairing on $W$ is Euclidean; cf. [**8**, p. 23].

Note that when $p$ is odd, a rational integer $l$ which is prime to $p$ is not a square in $\mathbb{Q}_p^*$ if and only if $l$ is a non-square mod $p$, and in this case the vector in $W_p$ corresponding to $l$ is $(1,1)$. If $l$ is a square in $\mathbb{Q}_p^*$, then the corresponding vector is $(0,0)$.

The image of $\Phi(\mathbb{Z}_S^*)$ in $W$ gives us a generator matrix $M$ of a linear code $V$ in $W$ which has the form indicated in Table 1. In this table there are three entries under $W_2$ because $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is a three-dimensional vector space over $\mathbb{F}_2$. The entries for a given row under $W_2$ are the coefficients of the corresponding generator of $\mathbb{Z}_S^*$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ relative to the ordered basis $\{-2,-10,-5\}$. Under the chosen basis,

Table 1: A boxed code

| $S$-units \ places | $W_{p_1}$ $\{-p_1,p_1\}$ | $W_{p_2}$ $\{-p_2,p_2\}$ | $\cdots$ | $W_2$ $\{-2,-10,-5\}$ | | $W_{\mathbb{R}}$ $\{-1\}$ |
|---|---|---|---|---|---|---|
| $p_1$ | 01 | 00/11 | | 00/11 | 1 | 0 |
| $p_2$ | 11/00 | 01 | | | 1 | 0 |
| $\vdots$ | $\vdots$ | | $\ddots$ | | $\vdots$ | $\vdots$ |
| 2 | 11/00 | | | 01 | 1 | 0 |
| $-1$ | 11 | 11 | $\cdots$ | 11 | 1 | 1 |

Theorem 1.1 guarantees that $V$ is a self-dual code in $W$. This can also be seen more directly in this special case by observing from Table 1 that $M$ has rank $n$ and that $V$ is self-annihilating by quadratic reciprocity.

We will view the $n \times 2n$ binary matrix $M$ in Table 1 as an $n \times n$ block matrix $\tilde{M}$, where each block is a pair of elements $(a_{2i}, a_{2i+1})$. The matrix $\tilde{M}$ has the following properties:

(1) The bottom row of $\tilde{M}$ has all entries equal to (11).

(2) All entries of the last column of $\tilde{M}$ equal the (10) pair except for the (11) in the final row.

(3) The diagonal elements of $\tilde{M}$ are all (01) except for the final diagonal entry, which is equal to (11).

(4) All other pairs in $\tilde{M}$ are either (00) or (11), which we will call *identical pairs*.

We say that a block matrix having properties (1)–(4) is *half-boxed*. We will say that $\tilde{M}$ is *boxed* if the following is also true:

(5) For all $n-1 \geqslant i > j \geqslant 1$, $b_{ij} + b_{ji} = (11)$.

It follows from quadratic reciprocity that a Hilbert code $V$ gives a boxed generator matrix $\tilde{M}$. On the other hand, we can view the generator matrix of an arbitrary self-dual code $V'$ as an $n \times n$ matrix $\tilde{M}'$ whose entries are $1 \times 2$ blocks. The following lemma is an easy observation:

**Lemma 3.1.** *If $\tilde{M}'$ is half-boxed, and its row vectors are orthogonal to each other, then condition (5) is automatically satisfied, i.e., $\tilde{M}'$ is boxed.*

*Proof of Theorem 1.5.* Every vector in a self-dual code $V$ must have even weight, i.e., an even number of 1's, since every vector has trivial product with itself. It follows

that $V$ must contain the vector $m_1$ having all entries equal to 1, since this vector is orthogonal to all vectors of even weight. Suppose now that $M$ is the generator matrix for a self-dual code $V$ of length $2n$ and that the last row of $M$ is $m_1$. Observe that elementary row operations to $M$ correspond to a change of basis for the code $V$. Column permutations send $M$ to a generator matrix for a code equivalent to $V$. We will show by induction on $n$ that after applying a sequence of invertible linear row operations and permutations of columns to $M$, one can make the associated block matrix $\tilde{M}$ half-boxed. We will in fact show that we can do this without ever adding another row to the final row $m_1$ of $M$. This will prove the theorem, since the above operations lead to codes equivalent to $V$ by definition.

For $n = 2$ our claim is obvious. We now suppose that $n > 2$ and that $M$ is the generator matrix for a self-dual code $V$ of length $2n$ and that the last row of $M$ is $m_1$. As $\operatorname{rank}(M) = n$, the first row of $M$ is neither all-zero $00\cdots0$ nor all-one $11\cdots1$. Therefore we can permute the columns of $M$ to make the pair on the upper-left corner of $\tilde{M}$ equal (01). We view $\tilde{M}$ as having four blocks: Here $w$ is a column block-vector

Table 2: Block form of $\tilde{M}$

| | |
|---|---|
| 01 | $u$ |
| $w$ | $M'$ |

of length $n-1$, and $u$ is a row block-vector of the same length. By adding the first row of $\tilde{M}$ to the $j$-th row if necessary, $2 \leqslant j < n$, we can assume that $w$ consists only of identical pairs. Now $M'$ represents the generator matrix of a self-dual code of length $2n-2$ which has all 1's in the final row. By our induction hypothesis, we can do column permutations and row operations on $M'$ such that $\tilde{M}'$ is in half-boxed form, where the bottom row of $M'$ remains all 1's. We perform these same operations on the original matrix $M$. This leads to a column block-vector $w$ in $\tilde{M}$ which still consists of identical pairs, and the bottom row of $\tilde{M}$ remains $m_1$.

Consider the first $(n-2)$ pairs in $u$. We have now arranged that the diagonal entries of $\tilde{M}'$ are all of the form (01) except for the diagonal entry in the bottom row, and the entries of $\tilde{M}'$, which are not in the last row or column are identical pairs. Therefore we can add to the first row of $\tilde{M}$ rows numbered 2 through $n-1$ in such a way that all block entries of $u$, except for the last block, become identical pairs. After these operations the upper-left corner of $M$ is either 01 or 10, since these operations amounts to adding certain identical pairs in $w$ to 01. Since the weight of the first row is even, the last pair of $u$ should be either 01 or 10. By adding the bottom row to the first row if necessary, we can assume the last pair of $u$ is 10. Finally, if the upper-left corner of $M$ is 10, we permute the first two columns of $M$ to make it 01. Now the associated block matrix $\tilde{M}$ is in half-boxed form. Therefore $\tilde{M}$ is in fact boxed by Lemma 3.1.

To complete the proof, we now need to show that every boxed matrix $\tilde{M}$ can be realized by the Hilbert code associated to some set $S = \{2, \infty, p_1, \ldots, p_{n-2}\}$. To specify the $p_i$ we begin by requiring their classes in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \times \mathbb{R}^*/(\mathbb{R}^*)^2$ to be as in the last two block columns of $\tilde{M}$. This can be done with $p_i$ congruent to 3 mod 4. We now choose the $p_i$ to lie in residue classes mod $p_j$ for $1 \leqslant j < i \leqslant n-2$ such that

the class of $p_i$ in $\mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2$ is given by the entry $b_{ij}$ of $\tilde{M}$. Since there is a unique boxed matrix which has these entries, and the block matrices associated to Hilbert codes are boxed, we have now realized $\tilde{M}$ by a Hilbert code. By the equidistribution of prime numbers in congruence classes, each self-dual code can be realized by this construction with infinite many distinct sets of places $S$. □

*Remark 3.2.* Suppose we specify arbitrary identical pairs for the entries $b_{ij}$ in a block matrix $\tilde{M}$ as $i$ and $j$ range over pairs for which $1 \leqslant i < j \leqslant n-1$. Then $\tilde{M}$ can be completed in a unique way to a boxed matrix. This gives a new non-recursive way of writing down self-dual codes of a given length. For some known recursive algorithms, see [**1**] and [**2**].

*Remark 3.3.* Consider the case $K = \mathbb{F}_q(T)$, where $q$ is a prime power and $q \equiv 3$ mod 4, $T$ is a parameter. $X = \mathbb{P}^1_{\mathbb{F}_q}$. $S = \{\frac{1}{T}, g_1(T), \ldots, g_{n-1}(T)\}$ where each $g_i(T)$ is a monic irreducible polynomial in $\mathbb{F}_q[T]$ of odd degree. Denote $W := \oplus_{v \in S} K_v^*/(K_v^*)^2$. Then upon a suitable choice of basis, the Hilbert symbol pairing $W \times W \to \mathbb{F}_2$ is also Euclidean, and the diagonal image of $\Phi\colon \mathcal{O}_U^*/(\mathcal{O}_U^*)^2 = \langle -1, g_1(T), \ldots, g_{n-1}(T)\rangle$ in $W$ is also given by a boxed matrix.

## References


[**1**] R. T. Bilous and G.H.J. Van Rees, An enumeration of binary self-dual codes of length 32, *Designs, Codes and Cryptography* **26** (2002), no. 1-3, 61–68.

[**2**] S. Bouyuklieva and I. Bouyukliev, An algorithm for classification of binary self-dual codes, `arXiv:1106.5930`, June (2011).

[**3**] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, *J. Math. Soc. Japan* **43** (1991), no. 1, 67–87.

[**4**] M. Matthias and V. Puppe, Involutions on 3-manifolds and self-dual, binary codes, *Homology, Homotopy and Applications* **10** (2008), no. 2, 139–148.

[**5**] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge Publishing, Charleston, SC, 2006.

[**6**] J. Neukirch, *Algebraic number theory*, Grundlehren Math. Wiss. **332**, Springer-Verlag, New York, 1999.

[**7**] J.-P. Serre, *Corps locaux*, 3rd ed. Hermann, Paris, 1968.

[**8**] J.-P. Serre, *A course in arithmetic*, Grad. Texts in Math. **7**, Springer-Verlag, New York, 1973.



Ted Chinburg `ted@math.upenn.edu`

Department of Mathematics, University of Pennsylvania, 209 S. 33rd St., Philadelphia, PA 19104-6395

Ying Zhang `yinzhang@sas.upenn.edu`

Department of Mathematics, University of Pennsylvania, 209 S. 33rd St., Philadelphia, PA 19104-6395