Perfect 1-error-correcting Lipschitz weight codes

OLOF HEDEN\textsuperscript{1,*} AND MURAT GÜZELTEPE\textsuperscript{2}

\textsuperscript{1} Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden
\textsuperscript{2} Department of Mathematics, Sakarya University, TR-54187 Sakarya, Turkey

Received May 10, 2015; accepted October 27, 2015

Abstract. Let $\pi$ be a Lipschitz prime and $p = \pi \pi^\ast$. Perfect 1-error-correcting codes in $H(\mathbb{Z})_\pi$ are constructed for every prime number $p \equiv 1(\text{mod } 4)$. This completes a result of the authors in an earlier work, Perfect Mannheim, Lipschitz and Hurwitz weight codes, (Math. Commun. \textbf{19}(2014), 253–276), where a construction is given in the case $p \equiv 3(\text{mod } 4)$.

AMS subject classifications: 94B60
Key words: perfect codes

1. Introduction

Lipschitz weight codes were introduced by Martinez et al. in [3, 4]. Shortly, consider the ring of quaternions over the integers

$$H(\mathbb{Z}) = \{a_0 + a_1e_1 + a_2e_2 + a_3e_3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\},$$

where

$$e_1^2 = e_2^2 = e_3^2 = -1,$$

and

$$e_1e_2 = -e_2e_1 = e_3, \quad e_2e_3 = -e_3e_2 = e_1, \quad e_3e_1 = -e_1e_3 = e_2.$$  \hfill (1)

A Lipschitz prime is an element $\pi = a_0 + a_1e_1 + a_2e_2 + a_3e_3$ in $H(\mathbb{Z})$ such that $p = \pi \pi^\ast = (a_0 + a_1e_1 + a_2e_2 + a_3e_3)(a_0 - a_1e_1 - a_2e_2 - a_3e_3) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ is an odd prime number. The integer $N(\pi) = \pi \pi^\ast$ is called the norm of $\pi$.

The elements in the left ideal

$$\langle \pi \rangle = \{\lambda \pi \mid \lambda \in H(\mathbb{Z})\}$$

constitute a normal subgroup of the additive group of the ring $H(\mathbb{Z})$. The set of cosets to $\langle \pi \rangle$ in $H(\mathbb{Z})$ constitute an Abelian group denoted as below:

$$H = H(\mathbb{Z})_\pi = H(\mathbb{Z})/\langle \pi \rangle.$$
In [3], it is proved that the size of $H(\mathbb{Z})_{\pi}$ is equal to $p^2$.

Let
\[ \mathcal{E} = \{ \pm 1, \pm e_1, \pm e_2, \pm e_3 \}, \]
and let $\mathcal{E}_{\pi}$ denote the family of cosets to $\langle \pi \rangle$ containing the elements of $\mathcal{E}$. We define the \textit{distance} between the words $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ in the direct product $H(\mathbb{Z})^n_{\pi}$ of $n$ copies of $H(\mathbb{Z})_{\pi}$,
\[ d((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)) = 1, \]
if there is a $j \in [n]$ and an $\epsilon \in \mathcal{E}_{\pi}$ such that $\beta_j = \alpha_j + \epsilon$ and $\beta_i = \alpha_i$, for $i \neq j$.

A \textit{perfect} 1-error-correcting Lipschitz weight code of length $n$ is a subset $C$ of the direct product $H(n)$ of $n$ copies of the group $H$, such that every element in $C \setminus H^n$ is at distance one from exactly one word of $C$.

In [1], perfect 1-error-correcting Lipschitz weight codes in $H(n)_{\pi}$ are constructed for every Lipschitz prime $\pi$ such that $p = \pi \pi' \equiv 3 \pmod{4}$, for $p > 3$. The purpose of this paper is to extend this result to the case $p \equiv 1 \pmod{4}$.

\section{Notation}

The coset $a + \langle \pi \rangle$ to the left ideal $\langle \pi \rangle$ in the ring $H(\mathbb{Z})$ is denoted by $\overline{a}$.\footnote{To simplify reading of the text, one of the reviewers suggested a change of the notation used in “Part One” [1] of this study.}

It is important for our results that the Abelian group $H(\mathbb{Z})_{\pi}$, consisting of the cosets to the left ideal $\langle \pi \rangle$, is a left module over the ring $H(\mathbb{Z})$, see [1]. We remind that, as a left module over $H(\mathbb{Z})$, the left distributive rule holds in $H(\mathbb{Z})_{\pi}$, that is,
\[ \lambda(\overline{a} + \overline{b}) = \lambda \overline{a} + \lambda \overline{b}, \]
is true for every $\lambda \in H(\mathbb{Z})$ and $\overline{a}, \overline{b} \in H(\mathbb{Z})_{\pi}$.

For example, with $\pi = 2 - 3e_2$, we get that $13e_i = e_i(2 + 3e_2)(2 - 3e_2) \in \langle \pi \rangle$, for $i = 1, 2, 3$, and that $\overline{e_3} = 3\overline{e_1}$, as
\[ 4e_1(2 - 3e_2) \in \langle \pi \rangle \implies 8e_1 - 12e_3 \in \langle \pi \rangle \implies -12e_3 \in -8e_1 + \langle \pi \rangle. \]

Also used in an example below is the fact that
\[ (2 + 2e_3)\overline{e_3} = -2e_3 + 2 = \overline{2} - 2\overline{e_3} = \overline{2} - 10e_1 = \overline{2} + 3\overline{e_1} = \overline{2} + 3\overline{e_1}, \tag{3} \]
and that
\[ \overline{0} = e_1 \overline{0} = e_1(8\overline{e_1} - 12\overline{e_3}) = -\overline{8} + 12\overline{e_2} = \overline{5} - \overline{e_2}, \]
that is, $\overline{e_3} = \overline{5}$.

Finally, we let $\mathcal{E}_0$ and $\mathcal{E}_1$ denote the following sets
\[ \mathcal{E}_0 = \{ \pm 1, \pm \overline{e_1} \}, \quad \mathcal{E}_1 = \{ \pm \overline{e_2}, \pm \overline{e_3} \}. \]
3. Preliminaries

Throughout this paper we are only concerned with the case when \( p = \pi^* \equiv 1 \pmod{4} \) is a prime number. It then follows from the Christmas theorem of Fermat that \( p \) is the sum of two squares. Henceforth, we consider the case when \( \pi = a_0 + a_2 e_2 \), whereby \( a_0^2 + a_2^2 = \frac{1}{p} \) is equal to a prime number \( p \).

We note that \( p \in \langle \pi \rangle \), as \( p = \pi^* \pi \). Thus, \( \mathbf{y} = \mathbf{u} \in H(\mathbf{Z})_\pi \), and elements in \( H(\mathbf{Z})_\pi \) can be described as 4-tuples \( x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 \), where we may assume that \( x_i \in \mathbb{Z}_p \) for \( i = 0, 1, 2, 3 \). The element \( 0 = a_0 + a_2 e_2 \) is equal to \( \mathbf{u} \in H(\mathbf{Z})_\pi \). Hence, if we let \( \mathbf{i} \) denote the element \(-a_0/a_2 \) in the finite field \( \mathbb{Z}_p \), then \(-\mathbf{i} + e_2 = \mathbf{u} \in H(\mathbf{Z})_\pi \), and furthermore, as \( \mathbf{u} = e_1(x_0 + x_2 e_2) = x_0 e_1 + x_2 e_3 \), we get that
\[
\mathbf{i} e_1 - e_3 = \mathbf{0}.
\]

Hence, with this notation,
\[
x + ye_3 = x + iye_1, \quad xe_1 + ye_2 = i y + xe_1,
\]
and
\[
x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 = x_0 + i x_2 + (x_1 + i x_3) e_1,
\]
and, trivially, in \( \mathbb{Z}_p \) we have
\[
i^2 = -1. \tag{6}
\]

We say that a selection of coset representatives \( \overline{H} = \overline{H(\mathbf{Z})}_\pi \) to \( \langle \pi \rangle \) in \( H(\mathbf{Z})_\pi \) is a \textit{complete selection of coset representatives} if no two elements of \( \overline{H(\mathbf{Z})}_\pi \) are congruent modulo \( \pi \), and if all cosets to \( \langle \pi \rangle \) are represented in \( \overline{H(\mathbf{Z})}_\pi \), that is,
\[
|\overline{H(\mathbf{Z})}_\pi| = |H(\mathbf{Z})_\pi|.
\]

As in [1], we say that the set \( \overline{H} \) is \( \mathcal{E} \)-homogeneous if
\[
\overline{h} \epsilon = \overline{h'} \epsilon \implies \overline{h} = \overline{h'}
\]
for every \( \epsilon \in \mathcal{E}_\pi \) and \( \overline{h}, \overline{h}' \in \overline{H} \). In [1], the following proposition is proved:

**Proposition 1.** Let \( \pi = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \) be a Lipschitz prime with \( p = \pi^* \pi \).
Then, for any two distinct elements \( e_i \) and \( e_j \) in \( \{ e_0 = 1, e_1, e_2, e_3 \} \) such that \( p \) does not divide \( a_i^2 + a_j^2 \), it is true that
\[
C_{i,j} = \{ x, e_i + x e_j : x, e_j \in \mathbb{Z}_p \}
\]

is a complete selection of coset representatives to \( \langle \pi \rangle \) in \( H(\mathbf{Z})_\pi \). Furthermore, \( C_{i,j} \) is \( \mathcal{E} \)-homogeneous.

A code \( C \) is a \textit{group code} if it is a subgroup of \( H^n \), or equivalently, as \( H^n \) is a finite group,
\[
c, c' \in C \implies c - c' \in C.
\]
We say that a group code \( C \) in \( H^n \) is an \textit{(n, k)}-code if the size of \( C \) is equal to \(|H|^k\).

A more general version of the next theorem is proved in [1].
Theorem 1. Let \( H \) and \( \mathcal{E}_\pi \) be constituted as above, and let \( \overline{1} \) be a complete selection of coset representatives to \( \langle \pi \rangle \). Assume that the norm of \( \pi \) is an odd prime number. Let \( n = (|H| - 1)/(|\mathcal{E}_\pi|) \). If \( g_1 = 1, g_2, \ldots, g_n \) are elements in \( \overline{1} \), satisfying the following three conditions:

(i) \( |g_i \mathcal{E}_\pi| = |\mathcal{E}_\pi|, \) for \( i = 2, 3, \ldots, n; \)

(ii) \( g_i \mathcal{E}_\pi \cap g_j \mathcal{E}_\pi = \emptyset, \) for \( i \neq j; \)

(iii) \( H \setminus \{0\} = \mathcal{E}_\pi \cup g_2 \mathcal{E}_\pi \cup \ldots \cup g_n \mathcal{E}_\pi; \)

then the null-space \( C \) of the matrix

\[
H = \left( \begin{array}{c} 1 \\ g_2 \\ \vdots \\ g_n \end{array} \right)
\]

is a perfect 1-error-correcting group \((n, n-1)\)-code in \( H^n \).

Indeed, the code \( C \) is defined by the elements \( g_i, \) for \( i \in [n], \) and may not be altered by a change of these elements. It follows from the results in [2] that it suffices that these elements have the above properties and belong to some ring \( \mathcal{R} \) such that \( H \) is a left module over \( \mathcal{R} \). For the sake of convenience in relation to the presentation of our result, instead of \( H(\mathbb{Z}) \) we consider the ring

\[
H(\mathbb{Z}_p) = \{a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}_p\},
\]

where \( e_1, e_2 \) and \( e_3 \) have the properties described in Eq. (1) and Eq. (2), and where \( p = \pi \pi^* \). It follows from Proposition 1 that the Abelian group \( H(\mathbb{Z}_p) \) is isomorphic to the Abelian group formed by the cosets to the left ideal \( \langle \pi \rangle \) in the ring \( H(\mathbb{Z}_p) \).

Thus, in order to prove the existence of a perfect 1-error-correcting Lipschitz weight code of length \( n \), it suffices to prove the existence of a partition of the space as indicated in the theorem, where \( g_i, \) for \( i \in [n], \) belongs to \( H(\mathbb{Z}_p) \). In fact, such partitions are constructed in Section 5 for the cases considered in this paper.

4. Some lemmas

Throughout this section, when not stated otherwise, \( \pi = a_0 + a_2 e_2, \) where \( a_0^2 + a_2^2 \) is equal to a prime number \( p \equiv 1(\text{mod} \ 4), \) although some of the lemmas are true for every Lipschitz prime \( \pi \).

Let \( D(a + be_1) \) denote the set

\[
D(a + be_1) = \{ \pm(a \pm be_1) \} \cup \{ \pm(b \pm ae_1) \} \cup \{ \pm(i a \pm ib e_1) \} \cup \{ \pm(i b \pm ia e_1) \}. \tag{7}
\]

Let \( \mathcal{Q} \) denote the following subgroup of the multiplicative group \( \mathbb{Z}_p^* \) of the finite field \( \mathbb{Z}_p: \)

\[
\mathcal{Q} = \{1, -1, i, -i\}.
\]

The first lemma is an immediate consequence of the fact that \( \mathcal{Q} \) is a subgroup of \( \mathbb{Z}_p^* \).

Lemma 1. If \( x + ye_1 \in D(a + be_1) \), then \( D(x + ye_1) = D(a + be_1) \).
Corollary 1. There is a sequence $a_i + b_i e_1$, $i = 1, 2, \ldots, s$, of elements in $H(\mathbb{Z})_\pi$ such that the sets $\mathcal{D}(a_i + b_i e_1)$ partitions $H(\mathbb{Z})_\pi$, that is,

$$H(\mathbb{Z})_\pi \setminus \{0\} = \bigcup_{i=1}^{s} \mathcal{D}(a_i + b_i e_1),$$

and

$$i \neq j \implies \mathcal{D}(a_i + b_i e_1) \cap \mathcal{D}(a_j + b_j e_1) = \emptyset.$$

**Proof.** The corollary follows from the fact that from Lemma 1 we may deduce that every non-zero element $x + ye_1$ of $H(\mathbb{Z})_\pi$ belongs to exactly one of the sets $\mathcal{D}(a + be_1)$.

**Lemma 2.** For any element $a, b \in \mathbb{Z}_p$,

$$|\mathcal{D}(a + be_1)| = \begin{cases} 8, & \text{if } ab(a^2 + b^2)(a^2 - b^2) = 0, \\ 16, & \text{otherwise.} \end{cases}$$

**Proof.** We consider the case $a^2 + b^2 = 0$, that is, when $b = ia$ or $b = -ia$. The other cases are treated similarly. From the definition in Eq. (7), we get that

$$\mathcal{D}(a + iae_1) = \mathcal{D}(a - iae_1) = \{ \pm(a \pm iae_1) \} \cup \{ \pm(ia \pm a e_1) \}. $$

As $i \neq \pm 1$ and $a \neq 0$, this is a set consisting of eight distinct elements.

**Lemma 3.** For any element $a, b \in \mathbb{Z}_p$,

$$\mathcal{D}(a + be_1) = \begin{cases} a\mathcal{E}_\pi, & \text{if } b = 0, \\ b\mathcal{E}_\pi, & \text{if } a = 0, \\ (a + ae_3)\mathcal{E}_\pi, & \text{if } a^2 + b^2 = 0, \\ (a + ae_1)\mathcal{E}_\pi, & \text{if } a^2 - b^2 = 0, \\ (a + be_1)\mathcal{E}_\pi \cup (b + ae_1)\mathcal{E}_\pi, & \text{if } ab(a^2 + b^2)(a^2 - b^2) \neq 0. \end{cases}$$

**Proof.** As in the proof of the previous lemma, we just treat the case $a^2 + b^2 = 0$, and here just when $b = ia$. We consider products to the left of the elements in $\mathcal{E}_\pi$ with elements $a + ae_3$, where $a \in \mathbb{Z}_p \setminus \{0\}$. For instance, we get

$$(a + ae_3)e_2 = ia - ae_1 = b - ae_1 \in \mathcal{D}(a + be_1),$$

e tc.

We close this section with the following observation: Let $d_1, d_2, \ldots, d_{(p-1)/4}$ be a family of coset representatives to $\mathcal{Q}$ in $\mathbb{Z}_p$. The following easily verified relations are useful when deriving partitions of the set $H(\mathbb{Z})_\pi$ into cosets of $\mathcal{E}_\pi$:

$$\bigcup_{a \in \mathbb{Z}_p \setminus \{0\}} \mathcal{D}(a + iae_1) = \bigcup_{i=1}^{(p-1)/4} (d_i + d_i e_3)\mathcal{E}_\pi. \quad (8)$$
5. Construction of necessary partitions

**Theorem 2.** For every prime number $p$ with $p \equiv 1 \pmod{4}$ there is a Lipschitz prime $\pi$, with $\pi^4 = p$, and a sequence of $t = (p^2 - 1)/8$ elements $g_1, \ldots, g_t$ of $H(\mathbb{Z}_p)$ such that

$$H(\mathbb{Z}_p) \setminus \{0\} = g_1E_\pi \cup \ldots \cup g_tE_\pi,$$

$$i \neq j \implies g_iE_\pi \cap g_jE_\pi,$$

and $|g_iE_\pi| = |E_\pi|$, for $i = 1, \ldots, t$ and $j \neq i$.

**Proof.** The theorem follows immediately from Corollary 1, Lemma 2 and Lemma 3, as for every element $g \in H(\mathbb{Z}_p)$,

$$|gE_\pi| \leq |E_\pi| = 8.$$

\[ \square \]

In order to be able to apply Theorem 1 we note that the set

$$\{a + be_1 \mid C_{0,1} \mid p \not| a^2 + b^2\} \cup \{a \pm ae_3 \mid C_{0,3} \mid p \not| a \in \mathbb{Z}_p\},$$

forms a complete set of coset representatives to $\langle \pi \rangle$ in $H(\mathbb{Z}_p)$.

We illustrate the construction described in the proof above in the next example.

**Example 1.** Let $\pi = 2 - 3e_2$. Then $p = 13$, $i = 2/3 = 5$, $e_2 = 5$ and $e_3 = 5e_1$, see Section 2 and Section 3.

The group $Q = \{\pm 1, \pm 5\}$ has for example the coset representatives $d_1 = 1$, $d_2 = 2$, and $d_3 = 4$ in the multiplicative group of the field $\mathbb{Z}_{13}$. To form the partition of the set $H(\mathbb{Z}_p)$ into left cosets of $E_\pi$, we begin by using equations (8), (9) and (10) letting

$$g_i = d_i + d_ie_1, \quad g_{3+i} = d_i + d_ie_1, \quad g_{6+i} = d_i,$$

for $i = 1, 2, 3$. This provides nine of the $(p^2 - 1)/|E_\pi| = (13^2 - 1)/8 = 21$ requested left cosets $g_iE_\pi$ to $E_\pi$.

The remaining cosets to $E_\pi$ are formed recursively using Lemma 1 and the case $ab(a^2 + b^2)(a^2 - b^2) \neq 0$ of Lemma 3. We obtain “the next two cosets $g_{2(k+1)}E_\pi$ and $g_{2(k+1)+1}E_\pi$” by first choosing an element $a + be_1$ such that

$$a + be_1 \not\in g_1E_\pi \cup g_2E_\pi \cup \ldots \cup g_{2k+1}E_\pi,$$

(where we assume that $k \geq 4$). We then let $g_{2k+2} = a + be_1$ and $g_{2k+3} = b + ae_1$. When this procedure terminates, we have obtained the requested partition of $H(\mathbb{Z}_\pi)$. 

\[ \square \]
For example, we may let
\[ g_{10} = 1 + 2e_1, g_{11} = 2 + e_1, g_{12} = 1 + 3e_1, g_{13} = 3 + e_1, g_{14} = 1 + 4e_1, g_{15} = 4 + e_1, g_{16} = 1 + 6e_1, g_{17} = 6 + e_1, g_{18} = 2 + 4e_1, g_{19} = 4 + 2e_1, g_{20} = 2 + 6e_1, g_{21} = 6 + 2e_1. \]

The element \( \mathbf{T} \) of \( H(Z)_\pi \) belongs to the coset \( d_1E_\pi \). For the error-correcting procedure we may thus form the matrix
\[
H = \begin{bmatrix}
1 & 1 + e_3 & 2 + 2e_3 & 2 + e_1 & 2 + e_1 & 1 + 3e_1 & 3 + e_1 & \cdots
\end{bmatrix}.
\]

The perfect 1-error-correcting code \( C \) is the null space in \( H(Z)_\pi \) of \( H \), the number of words of \( C \) is \(|C| = 169^{20}\). If, after a transmission, the word \( x_1, x_2, \ldots, x_{21} \) is received by giving the syndrome
\[
H \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{21} \end{bmatrix} = \begin{bmatrix} 2 + 3e_1 \end{bmatrix},
\]
then the error \( \epsilon = -e_3 \) has appeared in the third coordinate position as from Section 2
\[
2 + 3e_1 = (2 + 2e_1)(-e_3).
\]

From the theorem above and Theorem 1, we immediately get the following corollary:

**Corollary 2.** To every prime number \( p \) such that \( p \equiv 1 \pmod{4} \) there is a Lipschitz prime \( \pi \) of norm \( N(\pi) = p \) such that there exists a perfect 1-error-correcting Lipschitz weight code in \( H(Z)_\pi^n \), where \( n = (p^2 - 1)/8 \).

Thus, combining with the results of [1], we get

**Theorem 3.** To every prime number \( p > 3 \) there is a Lipschitz prime \( \pi \) of norm \( N(\pi) = p \) such that there exists a perfect 1-error-correcting Lipschitz weight code in \( H(Z)_\pi^n \), where \( n = (p^2 - 1)/8 \).

A final remark is that the crucial part in our construction of perfect 1-error-correcting Lipschitz weight codes is the derivation of a partition of \( H(Z)_\pi \) into left cosets of \( E_\pi \). As soon as this problem is solved, we can easily extend the construction with parity-check matrices, like in Theorem 4 in “Part One” of this study [1], in order to obtain codes of other lengths and sizes. Thus we now know, cf. Section 5.2 of [1], that for every prime number \( p > 3 \) there is a perfect 1-error-correcting Lipschitz weight code \( C \) of length \( n = (p^2l - 1)/8 \) and size \(|C| = p^{2k} \), where \( k = (p^2l - 1)/8 - l \), and \( l \) is any non-negative integer.

**Acknowledgement**

We are grateful to one of the reviewers who encouraged us to write a more clear presentation.

\(^1\)The case \( p = 3 \) is out of any general interest.
References