British Journal of Mathematics & Computer Science
2014_BJMCS_8887

SCIENCEDOMAIN *international*
www.sciencedomain.org

About Euclidean Codes in Rings

K. Abdelmoumen*[1] , H. Ben-azza[2] , M. Najmeddine[3]

[1] *Faculty of Science and Technology Fez, Morocco*
[2] *Moulay Ismaïl University, Ensam-Meknès, Morocco*
[3] *Moulay Ismaïl University, Ensam-Meknès, Morocco.*

Original research papers

Received: XX December 20XX
Accepted: XX December 20XX
Online Ready: XX December 20XX

Abstract

In this paper, we construct codes over rings which have a Euclidean division, in the commutative and non commutative cases. Such construction generalizes Reed-Solomon codes. We exemplify the construction for Gaussian integers and Lipschitz quaternions.

Keywords: Coding theory, Euclidean rings, Gaussian integers, quaternions

1 Introduction

In this paper, we construct error-correcting codes over rings equipped with a Euclidean division algorithm. The method of encoding a message is similar to techniques introduced in [8] and [11], or by using the Chinese remainder theorem (see [16]). As an important example, consider the Reed-Solomon codes viewed as a Euclidean code following [16]. Let k be a fixed nonnegative integer, and the ring $A = \mathbb{F}_q[X]$ of polynomials with indeterminate X over the Galois field $\mathbb{F}_q$. The set of messages is $A_k = \{f \in \mathbb{F}_q[X] : deg(f) < k\}$. Let $x_1, ..., x_n$ be distinct elements of $\mathbb{F}_q$. Then the encoding is given by the evaluation

$$\begin{array}{cccl} ev & : & A_k & \longrightarrow & \Pi_{i=1}^{n} A/\langle X - x_i\rangle \\ & & f & \longmapsto & (f \text{ mod } \langle X - x_1\rangle, ..., f \text{ mod } \langle X - x_n\rangle) \end{array} \tag{1.1}$$

In Section 2, we present a construction based on Euclidean commutative rings and estimate its Hamming distance, after giving many properties of Euclidean rings. This is a kind of generalization of the Reed-Solomon code (1.1). We illustrate the construction by the Gaussian integers. The resulting codes are necessarily non linear and heterogeneous. Section 3 presents the analogue construction for Lipschitz quaternions, a typical case of non commutative rings. Section 4 concludes with research perspectives.

**Tel : +212664344767*
**Corresponding author: E-mail: abkhalid9@gmail.com*

For basics on coding theory, refer to [17], and background on algebraic number theory consult [14, 2].

2 Codes over Euclidean Commutative Rings

Definition 2.1. A commutative domain A is said Euclidean if there exists a mapping $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ called a Euclidean algorithm such that

(i) For all a and b in $A \setminus \{0\}$, $\quad \varphi(a) \leq \varphi(ab)$;

(ii) For all a, b in $A \setminus \{0\}$, there exist q and r in A such that $a = bq + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$, (Euclidean division).

Note that if a and b are associate in the Euclidean ring A, i.e., there exits a unit $u \in A$ such that $a = ub$, with Euclidean algorithm φ, then $\varphi(a) = \varphi(b)$. Note also that the condition (i) of the definition may be removed by a result of Motzkin (see [15, 1] for more details).

Example 2.1.

1. *The ring $\mathbb{Z}$ of integers is Euclidean. Indeed, $\varphi(z) = |z|$ is a Euclidean algorithm over $\mathbb{Z}$.*
2. *Let $\mathbb{K}$ be commutative ring, then the polynomial ring $\mathbb{K}[X]$ is Euclidean with the Euclidean algorithm defined by $\varphi(P(X)) := deg(P(X))$ if $P(X)$ is nonzero, and $deg(P(X)) = -\infty$ else.*
3. *The Gaussian ring $\mathbb{Z}[i] = \{a + ib : (a, b) \in \mathbb{Z}^2\}$ is Euclidean with for all $z = a + ib$, $\varphi(z) = |z|^2 = z\overline{z} = a^2 + b^2$.*
4. *We give examples of Euclidean rings related to number fields (cf. [2]).*
   Let $A_1 = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ (resp. $A_2 = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$) with the algorithm $x + y\sqrt{m} \mapsto |x^2 - my^2|$ (resp. $x + y(\frac{1+\sqrt{m}}{2}) \mapsto |x^2 + xy + \frac{1}{4}(1-m)y^2|$), where m is a squarefree integer.
   - *If $m < 0$, then A_1 is Euclidean if and only if $m = -1$ or $m = -2$.*
   - *If $m > 0$ with $m \equiv 2, 3(\ mod\ 4)$, then A_1 is Euclidean if and only if $m \in \{2, 3, 6, 7, 11, 19, 57\}$.*
   - *If $m > 0$ with $m \equiv 1(\ mod\ 4)$, then A_2 is Euclidean if and only if $m \in \{5, 13, 17, 21, 29, 33, 37, 41, 73\}$.*
   - *If $m < 0$ with $m \equiv 1(\ mod\ 4)$, then A_2 is Euclidean if and only if $m \in \{-3, -7, -11\}$.*

Remark 2.1 ([7]). Let A be a commutative integral ring , which is not a field, with the Euclidean algorithm φ, then $\varphi(A)$ is isomorphic to (as an ordered set) $\mathbb{N}$.

Remark 2.2. In general, we do not have uniqueness for the pair (q, r) in (ii) of the definition. For example, let $A = \mathbb{Z}$ and $\varphi(z) = |z|$. We have $11 = 2 \times 5 + 1$ and $11 = 3 \times 5 + (-4)$. For $A = \mathbb{Z}[i]$, there exists one to four pairs (q, r) of $\mathbb{Z}[i]$.

The following theorem shows that if A is a commutative integral domain with a surjective Euclidean algorithm, for which the uniqueness of Euclidean division holds, then A is either a field or a polynomial ring over a commutative ring.

Theorem 2.2 ([7]). *Let A be a commutative domain with a Euclidean algorithm φ such that $\varphi(A \setminus \{0\}) = \mathbb{N}$. Then the following properties are equivalent.*

- *The Euclidean division is unique. i.e., for all $a \in A$ and all $b \in A \setminus \{0\}$, there exist q , r unique in A such that $a = bq + r$ and $\varphi(r) < \varphi(b)$.*
- *The ring A contains a sub-field K, and there exists $X \in A$ such that the family $(X^n)_{n \geq 0}$ is a basis of the K-vector space A : A is a polynomial ring over the K. Furthermore the Euclidean algorithm φ is defined by $\varphi(P(X)) = deg(P(X))$.*

Let A be an integral commutative ring and φ a Euclidean algorithm over A. Consider the following two properties:

Property 1. For all a and b in $A \setminus \{0\}$, $\quad \varphi(a+b) \leq \varphi(a) + \varphi(b)$.

Property 2. For all a and b in $A \setminus \{0\}$, $\quad \varphi(a+b) \leq \max(\varphi(a), \varphi(b))$.

Note that property 2 implies property 1.

Remark 2.3. If φ verifies the property 2, then the Euclidean division is unique.

Proof. Suppose that for a and $b \neq 0$ in A, there exist q_1, r_1 and q_2, r_2 in A such that $a = bq_1 + r_1 = bq_2 + r_2$ and $\varphi(r_1) < \varphi(b)$, $\varphi(r_2) < \varphi(b)$, with $q_1 \neq q_2$ and $r_1 \neq r_2$. From $b(q_2 - q_1) = r_1 - r_2$ and $q_2 - q_1 \neq 0$, we obtain $\varphi(r_1 - r_2) \geq \varphi(b)$. Then $\varphi(b) \leq \max(\varphi(r_1), \varphi(r_2)) < \varphi(b)$, a contradiction. □

Let(A, φ) be a Euclidean ring, $n \geq 2$ and n, k in $\mathbb{N}$.

Let $I_1 = \langle \alpha_1 \rangle, \ldots, I_n = \langle \alpha_n \rangle$ be distinct prime ideals, different from A verifying the hypothesis

$$\forall J \subset \{1, ..., n\}, \quad \varphi(\prod_{i \in J} \alpha_i) \geq |J|, \tag{2.1}$$

and the α_i for $i = 1, ..., n$ does not divide 2 in A , with $2 = 2.1_A = 1_A + 1_A$.

For the purpose of the construction of codes over Euclidean rings, we introduce the following defintion, and we do not need property 1 to hold for all the elements of A.

Definition 2.2. A subset $S \subset A$ is said to be φ-stable if :

$$\forall x \neq y \in S, \begin{cases} -x \in S \\ \varphi(x+y) \leq \varphi(x) + \varphi(y) \end{cases}$$

Let S be a φ-stable subset. We set $\quad A_k = \{a \in A : \varphi(a) < k\} \cap S \quad$ and define the encoding mapping (evaluation) by

$$\begin{array}{cccc} ev & : & A_k & \longrightarrow & G = A/I_1 \times \cdots \times A/I_n \\ & & x & \longmapsto & ev(x) = (x + I_1, \ldots, x + I_n) \end{array}$$

Note that since A is supposed Euclidean, it is principal , and consequently it is a Dedekind ring. It follows that A/I_i is a field of finite cardinality and G is a finite group.

Proposition 2.1. *If $2k \leq n$, then ev is injective.*

Proof. Let x and y in A_k such that $ev(x) = ev(y)$. Then $x - y \in I_i$ and α_i divides $x - y$, for all $1 \leq i \leq n$. So, $\alpha = \prod_{i=1}^{n} \alpha_i$ divides $x - y$. There exists $b \in A$ such that $x - y = b\alpha$. If we suppose that $b \neq 0$, then $\varphi(x - y) \geq \varphi(\alpha)$. We have $x, y \in S$. If $x \neq -y$, then

$$\varphi(x - y) \leq \varphi(x) + \varphi(-y) = \varphi(x) + \varphi(y) < 2k.$$

The hypothesis (2.1) implies that $n \leq \varphi(\alpha)$. Hence, $2k \leq n \leq \varphi(x - y) < 2k$. A contradiction.

If $x = -y$ then $2x \in I_i$, and α_i divides $2x$ for all $1 \leq i \leq n$. As α_i does not divide 2 in A, α_i divides x.

So, $\alpha = \prod_{i=1}^{n} \alpha_i$ divides x. Therefore $k \leq n \leq \varphi(x) < k$. A contradiction.

Then $b = 0$ and $x = y$. We conclude that ev is injective. □

Let n , k in $\mathbb{N}$ such that $2k \leq n$. For $x = (x_1, ..., x_n), y = (y_1, ..., y_n)$ in G, their Hamming distance is $d(x, y) = \text{card}\{i : x_i \neq y_i\}$.

Definition 2.3. The set $\mathcal{C}_k = ev(A_k) = \{(x + I_1, \ldots, x + I_n) : x \in A_k\}$ is called a *Euclidean code* of size n and rate k over A. We denote by d the minimum Hamming distance of the code $\mathcal{C}_k$ which is $\min\{d(x, y) : x, y \in \mathcal{C}_k \text{ et } x \neq y\}$. We say that $\mathcal{C}_k$ is an $[n, k, d]-$ code over A.

Proposition 2.2. *$\mathcal{C}_k$ is an $[n, k, d]-$code of minimum Hamming distance d over A such that $d \geq n + 1 - 2k$.*

Proof. Let x and y be distinct elements of A_k, and $J = \{i \in \{1, \ldots, n\} : x + I_i = y + I_i\}$. Then $\prod_{i \in J} \alpha_i$ divides $x - y$. Thus $\varphi(x - y) \geq \varphi(\prod_{i \in J} \alpha_i) \geq |J|$. We have $x, y \in S$. If $x \neq -y$, then $\varphi(x - y) \leq \varphi(x) + \varphi(-y) = \varphi(x) + \varphi(y) < 2k$. Thus $|J| < 2k$. Therefore $d(ev(x), ev(y)) \geq n-2k+1$. If $x = -y$, a similar reasoning to that of the previous proposition shows that $|J| \leq \varphi(x) < k$, and in this
case we have $d \geq n + 1 - k \geq n + 1 - 2k$. □

Example 2.3. *Consider the Gaussian ring $\mathbb{Z}[i]$ which is mentioned in example 2.1* (3).
Recall the following result [5]:
A Gaussian integer $z \in \mathbb{Z}[i]$ is prime if and only if one of the three following cases holds:

(i) $N(z) = 2$ *(in this case z is associate to $1 + i$; that is , $z \in \{1 + i, -1 - i, -1 + i, 1 - i\}$);*

(ii) $N(z) = p$, *where p is prime in $\mathbb{Z}$ and $p \equiv 1($ mod $4)$;*

(iii) *z is associate to q where q is prime in $\mathbb{Z}$ and $q \equiv 3($ mod $4)$.*

We take $n = 12$, $k = 5$ and $\alpha_1 = 3; \alpha_2 = 7; \alpha_3 = 2 + 5i; \alpha_4 = 2 - 5i; \alpha_5 = 1 + 6i; \alpha_6 = 1 - 6i;$ $\alpha_7 = 2 + i; \alpha_8 = 1 + 2i; \alpha_9 = 2 + 3i; \alpha_{10} = 3 + 2i; \alpha_{11} = 1 + 4i; \alpha_{12} = 1 - 4i.$
Let $S = \{0, \pm 1, \pm 2i\}$. We have $A_k = \{z \in \mathbb{Z}[i] : \varphi(z) < 5\} \cap S = S.$

The computations are simple but tedious, therefore we have used the computer algebra system Maple to verify the calculations [10]. The procedure `div_euclidean` determines representatives of the classes modulo $\alpha_m, m = 1, ..., 11,$ for each element of A_k. For more details on this division see an appendix in [9]. Note that the function `round` of a real number returns the closest integer to this real, and for a complex number z the returned value is $round(Re(z)) + i * round(Im(z))$.

```
>  div_euclidean:=proc(a::complex,b::complex):
      a-b*round(a/b);
      end:
>L:=[3,7,2+5*I,2-5*I,1+6*I,1-6*I,2+I,1+2*I,2+3*I,3+2*I,1+4*I,1-4*I]:
> ev:=z->[seq(div_euclidienne(z,k), k in L)]:
> C_k:=map(ev,{0,-1,1,-2*I,2*I});
  C_k := {[-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1],[0,0,0,0,0,0,0,0,0,0,0,0],
  [1,1,1,1,1,1,1,1,1,1,1,1],[-I,2I,2I,2I,2I,2I,1,-1,2I,2I,2I,2I],
  [I,-2I,-2I,-2I,-2I,-2I,-1,1,-2I,-2I,-2I,-2I]}
> with(combinat,choose):
> # Procedure with parameters the code C and its length n which return the minimum distance of C:
  dist_Min:=proc(C,n)
local P,d,j,l,pair,x,y,d_H,L1,L2;
P:=choose(C,2); d:=n;
for j from 1 to nops(P) do;
pair:=op(j,P);x:=op(1,pair);y:=op(2,pair);d_H:=0;
for l from 1 to n do;
 L1:=op(l,x);L2:=op(l,y);
```

```
 if L1<>L2 then d_H:=d_H+1 fi;
 od;
 if d_H<d then d:=d_H fi;
 od;
 return d;
end:
> dist_Min(C_k,12);

                                    11
```

The minimum distance of the code C_k is $d = 11$ and verifies $d \geq n - 2k + 1 = 3$.

Using the same idea of the proof of the above proposition, we obtain the following proposition:

Proposition 2.3. *Suppose that φ verifies the **property 2** and that $k \leq n$. Then $\mathcal{C}_k$ is an $[n, k, d]-$code of minimum Hamming distance d over A such that $d \geq n + 1 - k$.*

Example 2.4 (Reed-Solomon Codes)**.** *Let k be a nonnegative integer, and $A = \mathbb{F}_q[X]$ with $q = p^s$ is a prime power. Set $A_k = \{f \in \mathbb{F}_q[X] : deg(f) < k\}$. Let $x_1, ..., x_n$ be distinct elements of $\mathbb{F}_q$, and $I_i = \langle X - x_i \rangle$. We have $\varphi = deg$. The ring (A, φ) verifies **property 2**. The encoding map*

$$\begin{array}{cccc} ev & : & A_k & \longrightarrow & \Pi_{i=1}^{n} A/I_i \\ & & f & \longmapsto & (f \text{ mod } \langle X - x_1 \rangle, ..., f \text{ mod } \langle X - x_n \rangle) \end{array}$$

$\mathcal{C}_k = ev(A_k)$ is the Reed-Solomon code of length n, dimension k and the minimum distance d verifies $d \geq n + 1 - k$. As we work in the case of linear codes over finite fields, by applying the Singleton bound, we find again that $\mathcal{C}_k$ is a MDS code.

3 Codes over Quaternion Integers

In this section, we treat the similar notions to section 2, by defining codes over quaternions. There are two basic classical versions of quaternion integers, those of Lipschitz denoted by $\mathbb{L}$ and those of Hurwitz. We will illustrate the construction for Lipschitz quaternions (for nice introductions, see [5, 4, 6]). Note that similar results will hold for the Hurwitz quaternions formed by adjoining $\frac{1}{2}(1 + i + j + k)$ to $\mathbb{L}$ resulting in an integral domain in which every one-sided ideal is principal .

We denote by $\mathbb{L} = \{A = x_0 + x_1 i + x_2 j + x_3 k :$ the x_i in $\mathbb{Z}\}$ the noncommutative ring of quaternion integers of Lipschitz, where 1 is the multiplicative unit and $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$. The integers $x_i, i = 0, 1, 2, 3$ are called the components of A. The conjugate of a quaternion A is $\overline{A} = x_0 - x_1 i - x_2 j - x_3 k$, and its norm is $N(A) = A\overline{A} = \sum_{i=0}^{3} x_i^2$. For $A, B \in \mathbb{L}$, we have $N(AB) = N(A)N(B)$. A quaternion is said primitive if the greatest common divisor of its components is 1. We note that for all $A \in \mathbb{L}$, we may write $A = \text{gcd}(A) \cdot A'$ where A' is primitive and $gcd(A) = gcd(x_0, x_1, x_2, x_3) \in \mathbb{Z}$. We denote by $\mathbb{L}_P$ the set of primitive quaternions.

The unit group of $\mathbb{L}$ is $U = \{\pm 1, \pm i, \pm j, \pm k\}$. The multiplication by an element of U does not change the norm.

We recall that a quaternion is prime if and only if its norm is a prime in $\mathbb{Z}$. We must note that a prime in $\mathbb{Z}$ is always a product of a prime and its conjugate in $\mathbb{L}$ (another formulation of Lagrange's theorem : every prime integer in $\mathbb{Z}$ is a sum of four squares).

Definition 3.1. A subset $S \subset \mathbb{L}_P$ is said to be N-stable if :

$$\forall A \neq A' \in S, \begin{cases} -A \in S \\ N(A + A') \leq N(A) + N(A') \end{cases}$$

We note that $\mathbb{L}$ admits a left Euclidean division as shown by the following theorem

Theorem 3.1 ([6, 5])**.**
For all $\alpha, \beta \in \mathbb{L}$ with β an odd quaternion , there exist $\delta, \gamma \in \mathbb{L}$ such that

$$\alpha = \gamma\beta + \delta \text{ with } N(\delta) < N(\beta).$$

Proof. We set $m = N(\beta) = \beta\overline{\beta}$ an odd integer and $\sigma = \alpha\overline{\beta} = s_0 + s_1 i + s_2 j + s_3 k$. Since m is an odd nonnegative integer, there exists a (unique) $r_i \in \mathbb{Z}$ such that

$$|s_i - r_i m| < \frac{m}{2} \quad \text{i.e. } |\frac{s_i}{m} - r_i| < \frac{1}{2} \text{ for } i = 0, ..., 3 \quad (r_i \text{ is the closest integer to } \frac{s_i}{m})$$

We let $\gamma = r_0 + r_1 i + r_2 j + r_3 k$. Hence, $N(\sigma - \gamma m) = \sum_i (s_i - r_i m)^2 < m^2$. Then we have

$$N(\sigma - \gamma m) = N(\alpha\overline{\beta} - \gamma\beta\overline{\beta}) = N(\alpha - \gamma\beta)N(\overline{\beta}) < m^2 = N(\beta)N(\overline{\beta}).$$

The remainder is $\delta = \alpha - \gamma\beta$ and we have $N(\delta) < N(\beta)$. □

Remark 3.1. This algorithmic proof gives the calculation of δ which we denote by α mod β. It is this remainder that is used in the construction of codes over $\mathbb{L}$.

Example 3.2. *By using the package `Quaternions` of Maple, we write a procedure which returns a remainder of the left Euclidean division of q_1 by q_2 with q_2 odd.*

```
> with(Quaternions):
> # First we define a procedure that returns the norm
     of a quaternion
> N:=proc(A):
   return A*conjugate(A);
  end:
> # Then, we define a procedure that returns
   a remainder of the left Euclidean division of two quaternions
> div_Quaternions:= proc(Q1,Q2):: Quaternions;
      round(Q1*conjugate(Q2)/N(Q2)):
      return Q1-%*Q2;
   end:
```

We apply the procedure `div_Quaternions` to the quaternions

$$q_1 = 1 - 3i + 7j + 4k \text{ and } q_2 = 1 - 2i + j + 5k$$

```
> q1 := Quaternions( 1, -3, 7, 4 ); q2 := Quaternion( 1, -2, 1, 5 );
                      q1 := 1 - 3 I + 7 J + 4 K
                       q2 := 1 - 2 I + J + 5 K
> N(q2);
                                  31
>  div_Quaternions(q1,q2);
                                2 + J
> N(%);
                                  5
```

Now, we proceed to the construction of codes over $\mathbb{L}$ similarly to Section 2.

Let n and k be in $\mathbb{N}$ such that $n \geq 2$. Let $\alpha_1, ..., \alpha_n$ be prime quaternions of $\mathbb{L}$ of distinct norms strictly greater than 2 such that

$$\forall J \subset \{1, ..., n\}, \quad N(\prod_{i \in J} \alpha_i) \geq |J|. \tag{3.1}$$

Consider an $N-$stable subset S of $\mathbb{L}_P$ and put $A_k = \{A \in \mathbb{L}_P : N(A) < k\}$, and let $S_k = S \cap A_k$ be the primitive quaternions to be encoded by

$$\begin{array}{cccc} ev & : & S_k & \longrightarrow & \Pi_{i=1}^n \mathbb{L}/\langle \alpha_i \rangle \\ & & A & \longmapsto & (A \text{ mod } \alpha_1, ..., A \text{ mod } \alpha_n) \end{array} \tag{3.2}$$

In the construction (3.2), we use the algorithm mentioned in the remark (3.1).

Theorem 3.3 ([3]). *Let $A \in \mathbb{L}_P$ be a primitive quaternion, with the norm $N(A) = p_1 ... p_n$ decomposed into a product of primes. Then there exist prime quaternions $P_1, ..., P_n$ such that $A = P_1 \cdots P_n$ and $N(P_i) = p_i$ for $i = 1, ..., n$.*

Proposition 3.1. *If $2k \leq n$, then ev is injective. Thus we obtain a code denoted by C_k.*

Proof. Suppose that $2k \leq n$, and for distinct A, A' in S_k we have $ev(A) = ev(A')$. Then α_i divides $A - A'$, and $N(\alpha_i) = p_i$ divides $N(A - A')$ for $i = 1, ..., n$. We deduce that $\prod_{i=1}^{n} p_i$ divides $N(A - A')$.

We set $N(A - A') = \prod_{i=1}^{n} p_i \prod_{j=1}^{m} q_j$, with the q_j primes in $\mathbb{Z}$.

By the theorem (3.3), there exist prime quaternions $P_1, ..., P_n, Q_1, ..., Q_m$ such that $A - A' = \prod_{i=1}^{n} P_i \prod_{j=1}^{m} Q_j$, with $N(P_i) = p_i$ and $N(Q_j) = q_j$. Then $N(A - A') = N(\prod_{i=1}^{n} P_i) N(\prod_{j=1}^{m} Q_j)$. As $N(\prod_{i=1}^{n} P_i) = N(\prod_{i=1}^{n} \alpha_i) \geq n$ (by (3.1)), we have that $N(A - A') \geq n$. If $A \neq -A'$, then $n \leq N(A - A') = N(A + (-A')) \leq N(A) + N(A') < 2k$. A contradiction.

If $A = -A'$, then $N(A - A') = N(2A) = 4N(A)$, and since the integers $N(\alpha_i)$ are odd primes and divide $4N(A)$, we see that $N(\alpha_i)$ divides $N(A)$. A similar reasoning shows that $N(A) \geq n$. We get a contradiction with the fact that $N(A) < k$. □

Proposition 3.2. *If $2k \leq n$, then C_k is an $[n, k, d]$-code of minimum Hamming distance d such that $d \geq n + 1 - 2k$.*

Proof. Let A and A' be distinct in S_k.

We consider $J = \{i \in \{1, ..., n\} : A \text{ mod } \alpha_i = A' \text{ mod } \alpha_i\}$. Then α_i divides $A - A'$ for $i \in J$, and so $N(\alpha_i) = p_i$ divides $N(A - A')$ for $i \in J$. Thus $\prod_{i \in J} p_i = N(\prod_{i \in J} \alpha_i)$ divides $N(A - A')$. By using hypothesis (3.1), $|J| \leq N(A - A')$. If $A \neq -A'$, then $N(A - A') \leq N(A) + N(A') < 2k$, and we obtain the result. If $A = A'$, a similar reasoning to that of the previous proposition shows that $|J| \leq N(A) < k$, and in this case we have $d \geq n + 1 - k \geq n + 1 - 2k$. □

Example 3.4. *We take $n = 8$, $k = 3$, and we consider the following prime quaternions :*

$\alpha_1 = 1 + i + j; \alpha_2 = 1 + 2i; \alpha_3 = 1 + i + j + 2k; \alpha_4 = 1 + 3i + j; \alpha_5 = 2i - 3k; \alpha_6 = 2 + 2j + 3k$ *;*

$\alpha_7 = 1 + i + 4j + k; \alpha_8 = 1 + 2i + 3j + 3k.$

Let $S = \{0, \pm(1 + i), \pm(j + k)\}$ be an N-stable set and $S_k = A_k \cap S = S$.

By using the package `Quaternions`, we determine the code words of C_k.

The procedures `div_Quaternions` and `dist_Min` defined above are used also.

```
>L:=[Quaternion(1,1,1,0),Quaternion(1,2,0,0),Quaternion(1,1,1,2),Quaternion(1,3,1,0),
Quaternion(0,2,0,-3),Quaternion(2,0,2,3),Quaternion(1,1,4,1),Quaternion(1,2,3,3)]:
S_k:={Quaternion(0,0,0,0),Quaternion(1,1,0,0),Quaternion(-1,-1,0,0),Quaternion(0,0,1,1),
       Quaternion(0,0,-1,-1)}:
> ev:=z->[seq(div_Quaternions(z,k), k in L)]:
> C_k:=map(ev,S_k);
   C_k := {[0,0,0,0,0,0,0,0],[I,-J,J+K,J+K,J+K,J+K,J+K,J+K],
   [J,I,-1-I,-1-I,-1-I,-1-I,-1-I,-1-I],[-I,J,-J-K,-J-K,-J-K,-J-K,-J-K,-J-K],
   [-J,-I,1+I,1+I,1+I,1+I,1+I,1+I]}
> dist_Min(C_k,8);
                                  8
```

The minimum distance of the code C_k is $d = 8$ verifying $d \geq n - 2k + 1$.

Remark 3.2. It was shown by Martínez et all. [13] that for any non zero $A \in \mathbb{L}$ the cardinality of $\mathbb{L}/\mathbb{L}A$ (viewed as a group) is $N(A)^2$, and we can deduce from corollary 22 in [13] that image of the encoding ev is included in the additive group $\prod_{i=1}^{n}(\mathbb{Z}/N(\alpha_i)\mathbb{Z} \times \mathbb{Z}/N(\alpha_i)\mathbb{Z})$ since the α_i are supposed primes in (3.2). See also [4] for related concepts.

4 Conclusion

This note mainly uses Euclidean algorithm to construct codes with typical examples : Gaussian integers and Quaternion integers. Some questions and further investigations are as follows.

1. What could be said about orders (see [14]) as message spaces, not necessarily maximal orders which are rings of integers, concerning constructions from algebraic number field ?
2. Other metrics which are studied in [9, 13] may be used in the context of the present work.
3. The decoding question may be approached, for example, by using the framework sketched by Sudan in [16] or by the concept of key equation used in [12].

References

[1] Agargun, A-G. and Fletcher, C-R. Euclidean rings. Turk. J. Math., 19: (1995), pp. 291–299.

[2] Alaca, S. and Williams, K-S. Introductory algebraic number theory. Cambridge U. Pr, (2004).

[3] Benneton, G. Sur l'arithmtique des quaternions et des biquaternions. Annales scientifiques de l'école Normale Suprieure, Sr. 3, 60 (1943), pp. 173–214.

[4] Chatters, A-W. Isomorphic subrings of matrix rings over the integer quaternions. Communications in Algebra , vol. 23, no. 2, (1995), pp. 783–802 .

[5] Davidoff,G., Sarnak, P. and Alain Valette. Elementary Number Theory, Group Theory and Ramanujan Graphs. Cambridge University Press, (2003).

[6] Dickson, L-E. Arithmetic of quaternions. Proc. London Math. Soc., (2) 20 (1920), pp. 225–232.

[7] Fresnel, J. Anneaux. Hermann Editor, Paris, (2001).

[8] Guruswami, V. Constructions of Codes from Number Fields. ECCC Technical Report TR01-002, January (2001).

[9] Huber, K. Codes Over Gaussian Integers. IEEE. Trans. Inform. Vol. 40, NO. 1, January (1994). pp. 207–216.

[10] Kilima, R-E., Sigmon, N. and Stitzinger, E. Applications of abstract algebra with Maple. CRC Press LLC, (1999).

[11] Lenstra, H-W. Codes from algebraic number fields. In : M. Hazewinkel, J.K. Lenstra, L.G.L.T. Meertens (eds), Mathematics and computer sciences II, Fundamental contributions in the Netherlands since 1945, CWI Monograph 4, pp. 95-104, North-Holland, Amsterdam, (1986).

[12] Li, W., Sidorenko, V. and Nielsen, J-S-R. On decoding Interleaved Chinese Remainder codes. Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July (2013), pp. 7-12.

[13] Martínez, C., Beivide, R. and Gabidulin, E-M. Perfect codes from Cayley graphs over Lipschitz integers. IEEE Trans. Inf. Theory, vol. 55, no. 8, (2009), pp. 3552-3562.

[14] Neukirch, J. Algebraic number theory. Springer, (1999).

[15] Samuel, P. About euclidean rings. J. Algebra, 19: (1971), pp.282–301.

[16] Sudan, M. Ideal error-correcting : Unifying algebraic and number-theoretic algorithms. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science Volume 2227, (2001), pp 36-45

[17] van Lint, J-H. Introduction to coding theory. volume 86 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, third edition, (1999).