

KATHOLIEKE
UNIVERSITEIT
LEUVEN

SYMMETRIC CODES OVER RINGS

André Barbé Fritz von Haeseler

SCD/SISTA report nr. 02-126
September 2002

TOEGEPASTE WETENSCHAPPEN
Departement Elektrotechniek (ESAT-SCD/SISTA)
Kasteelpark Arenberg, 10
B3001 Leuven /Heverlee - Belgium

Symmetric codes over rings*

André Barbé, Fritz von Haeseler

Departement Elektrotechniek (ESAT-SISTA/COSIC)
Kasteelpark Arenberg 10
B 3001 Leuven
{Andre.Barbe,fvanhaes}@esat.kuleuven.ac.be

Abstract

Shannon suggested to investigate a binary multiplying channel and asked for a maximal uniquely decodable symmetric code. Motivated by his example, we define such a code, called Shannon set, for an arbitrary ring. We investigate the Shannon sets for the rings $\mathbb{F}_q^{n\times n}$, $n \in \mathbb{N}$, and the rings $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$ for $m \in \mathbb{N}$.

AMS classification: 94A
Keywords: zero-error information theory, two way communication

1 Introduction

In 1961, Shannon [3] formulated the following problem. Two terminals, $T1$ and $T2$, wish to communicate over a binary multiplicative channel. To this end, they choose a code, i.e., a set $\mathbf{X} \subseteq \{0,1\}^n$, which is also the set of input vectors to the channel. If $\underline{x}, \underline{y} \in \mathbf{X}$ are input vectors, then the output vector is given by $\underline{z} = (z_i)_{i=1,\ldots,n} = (x_i y_i)_{i=1,\ldots,n}$ (the usual product of natural numbers). Each terminal should be able to determine uniquely the vector transmitted by the other terminal on the basis of its own vector and the output vector. Since both terminals are using the same set $\mathbf{X}$, the set is called a symmetric code.

Shannon's question was to determine the possible sets $\mathbf{X}$ and to find a set with highest possible cardinality. A set $\mathbf{X}$ with this property is called uniquely decodable. This problem and its generalizations have been studied by several authors, see e.g., [1, 4] for more references.

We can reformulate Shannon's question in a ring theoretic setting by considering $\{0,1\}^n$ as the ring $\mathcal{R} = \mathbb{Z}_2^n$, i.e., the n-fold product of the ring $\mathbb{Z}_2 = \mathbb{Z}/(2\mathbb{Z})$. Then Shannon's problem comes down to finding a subset $\mathbf{X} \subset \mathcal{R}$ such that for all given x, $y \in \mathbf{X}$ the knowledge of x and xy allows to find $y \in \mathbf{X}$ uniquely, or, vice versa, a knowledge of y and xy allows to determine $x \in \mathbf{X}$ uniquely. This subset $\mathbf{X}$ is then said to have the unique decoding property.

In this paper we study Shannon's question for arbitrary rings $\mathcal{R}$. We introduce the notion of a Shannon set of a ring $\mathcal{R}$ as a subset with unique decoding property which has maximal cardinality. The cardinality of a Shannon set is called the Shannon number of the ring.

After some preliminary definitions and some general observation we will study the rings $\mathbb{F}_q^{n\times n}$, i.e., the ring of $n \times n$-matrices with entries in the finite field $\mathbb{F}_q$ of charcteristic

*This note is an extended version of a paper presented at the 23-rd Symposium on Information Theory in the Benelux, Louvain-la-Neuve, Belgium, May 29–31,2002

p, where $q = p^\alpha$ is the number of elements of $\mathbb{F}_q$ and p is a prime number. We shall prove that the set of invertible matrices is the only Shannon set of the ring $\mathbb{F}_q^{n\times n}$.

We shall also study the ring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, i.e., the set of integers modulo m with addition and multiplication modulo m. We shall show that the Shannon number of $\mathbb{Z}/(m)$ is equal to $\phi(m)$, where ϕ is Euler's totient function. However, contrary to the case of the ring $\mathbb{F}_q^{n\times n}$, there may be several Shannon sets. The Table 1, provides a complete list.

Properties of m	Number of Shannon sets
$\gcd(m,6) = 1$	1
$m = 2m'$ and $\gcd(m',6) = 1$	$2^{\phi(m')}$
$m = 4m'$ and $\gcd(m',2) = 1$	$2^{\phi(m')} + 1$
$m = 2^\alpha m'$, $\alpha \geq 3$ and $\gcd(m',6) = 1$	1
$m = 3^\beta m'$, $\beta \geq 1$ and $\gcd(m',6) = 1$	1
$m = 6m'$ and $\gcd(m',6) = 1$	$2^{2\phi(m')+1} - 2^{\phi(m')}$
$m = 2 \cdot 3^\beta m'$, $\beta \geq 2$ and $\gcd(m',6) = 1$	$2^{3^\beta \phi(m')}$
$m = 2^\alpha 3^\beta m'$, $\alpha \geq 3$, $\beta \geq 1$ and $\gcd(m',6) = 1$	1

Table 1: The number of different Shannon sets for the ring $\mathbb{Z}_m$

2 Shannon sets of a ring

From now on $\mathcal{R}$ denotes a ring with 1 and 0. For $r \in \mathcal{R}$ and a subset $A \subset \mathcal{R}$ we write rA as abbreviation for the set $\{ra \mid a \in A\}$. The cardinality of A is denoted as $|A|$. For $s \in \mathcal{R}$ we define $l_s : \mathcal{R} \to \mathcal{R}$ and $r_s : \mathcal{R} \to \mathcal{R}$ as

$$l_s(t) = st \text{ and } r_s(t) = ts,$$

respectively.

Definition 2.1 *A subset $\mathbf{X}$ of $\mathcal{R}$ has the* unique decoding property *if for every $s \in \mathbf{X}$ the maps $l_s : \mathbf{X} \to \mathcal{R}$ and $r_s : \mathbf{X} \to \mathcal{R}$ are injective, respectively.*

In case of a finite ring $\mathcal{R}$ one has the obvious

Lemma 2.2 *Let $\mathcal{R}$ be a finite ring. A subset $\mathbf{X}$ of $\mathcal{R}$ has the* unique decoding property *if and only if $|r\mathbf{X}| = |\mathbf{X}r| = |\mathbf{X}|$ holds for all $r \in \mathbf{X}$.*

In case that $\mathcal{R}$ is commutative then it is sufficient to consider either l_s or r_s. If furthermore, $\mathcal{R}$ is finite, then a subset $\mathbf{X}$ of $\mathcal{R}$ has the unique decoding property if $|x\mathbf{X}| = |\mathbf{X}|$ for all $x \in \mathbf{X}$.

Note that the problem of finding a subset $\mathbf{X}$ satisfying the requirements of Definition 2.1 is equivalent to Shannon's problem mentioned in the introduction. Indeed, if terminal T1 knows $x \in \mathbf{X}$ and $xy \in \mathcal{R}$, then, due to the fact that $l_x : \mathbf{X} \to \mathcal{R}$ is injective, it can uniquely determine $y \in bfX$. The same holds for terminal T2 and its knowledge of $y \in \mathbf{X}$ and $xy \in \mathcal{R}$.

The set of all subsets of $\mathcal{R}$ having the unique decoding property is denoted $\mathcal{U}(\mathcal{R})$. If $x \in \mathcal{R}$, then $\{x\} \in \mathcal{U}(\mathcal{R})$. Without proof we state some elementary properties.

Lemma 2.3

- *If $\mathbf{X} \in \mathcal{U}(\mathcal{R})$, then any subset of $\mathbf{X}$ has the unique decoding property.*
- *If $\mathbf{X}_1$, $\mathbf{X}_2 \in \mathcal{U}(\mathcal{R})$, then $\mathbf{X}_1 \cap \mathbf{X}_2 \in \mathcal{U}(\mathcal{R})$.*

- *If $\mathcal{R}_1$ and $\mathcal{R}_2$ are rings then $\mathcal{U}(\mathcal{R}_1) \times \mathcal{U}(\mathcal{R}_2) \subset \mathcal{U}(\mathcal{R}_1 \times \mathcal{R}_2)$.*

The relation $\subset$ defines a partial order on $\mathcal{U}(\mathcal{R})$. It is therefore meaningful to speak of maximal elements of $\mathcal{U}(\mathcal{R})$. In the case of a finite ring certain maximal elements in $\mathcal{U}(\mathcal{R})$ are special.

Definition 2.4 *Let $\mathcal{R}$ be a finite ring. The set $\mathbf{X} \in \mathcal{U}(\mathcal{R})$ is called a* Shannon set *of the finite ring $\mathcal{R}$ if*

$$|\mathbf{X}| = \max\{|Y| \mid Y \in \mathcal{U}(\mathcal{R})\}.$$

The cardinality $|\mathbf{X}|$ of a Shannon set is called the Shannon number *of the ring $\mathcal{R}$ and is denoted as $\chi(\mathcal{R})$.*

In particular, Shannon sets of $\mathcal{R}$ are maximal in $\mathcal{U}(\mathcal{R})$. On the other hand, of course, not every maximal element of $\mathcal{U}(\mathcal{R})$ is a Shannon set. E.g. the set $\{0\}$ is a set with the unique decomposition property and $\{0\}$ is maximal in $\mathcal{U}(\mathcal{R})$.

The following lemma provides a lower bound for the Shannon number of a ring.

Lemma 2.5 *If $\mathcal{R}^\star$ denotes the set of units of the finite ring $\mathcal{R}$, then $\chi(\mathcal{R}) \geq |\mathcal{R}^*|$.*

The proof is obvious. As the ring $(\mathbb{Z}_2)^n$ shows, this estimate can be very poor. In fact, we have only one unit and large sets with the unique decoding property, see e.g. [4]. If a finite commutative ring with 0 and 1 has large Shannon sets, then it is already a field, as shown by

Theorem 2.6 *Let $\mathcal{R}$ be a finite commutative ring with 0 and 1. The ring $\mathcal{R}$ is a field if and only if $\chi(\mathcal{R}) = |\mathcal{R}| - 1$.*

Proof: If $\mathcal{R}$ is a field then the assertion is obviously true.

If $\chi(\mathcal{R}) = |\mathcal{R}| - 1$, then for any $r \neq 0$ the map $l_r : \mathcal{R} \setminus \{0\} \to \mathcal{R}$, $x \mapsto rx$, is injective. Now suppose that there exist $r, s \in \mathcal{R} \setminus \{0\}$ such that $rs = 0$. We compute $r(s+1) = rs + r = r \cdot 1$ and conclude that due to the injectivity property of l_r it follows that either $s + 1 = 0$ or $s + 1 = 1$. If $s + 1 = 0$, then it follows that $r = 0$ and if $s + 1 = 1$, then it follows that $s = 0$; this is a contradiction to our assumption. Therefore any map l_r restricted to $\mathcal{R} \setminus \{0\}$ is injective with image $\mathcal{R} \setminus \{0\}$, thus $\mathcal{R}$ is a field.

■

We conclude the section with some examples.

1. For $m \geq 2$ we define a ringstructure on $\{0, \ldots, m-1\}$ by using the addition mod m and the multiplication is given by $rs = 0$ for all r, s. The thus defined ring has Shannon number 1. Any $r \neq 0$ defines a Shannon set $\{r\}$.

2. For $m \geq 2$ we define a ringstructure on $\{0, \ldots, m-1\}$ by using the addition mod m and the multiplication is given by $0r = r0 = 0$ for all r and $r1 = 1r = r$ and $rs = 0$ for all other possibilities. The thus defined ring has Shannon number 2 and any two different elements r, s in $\{1, \ldots, m-1\}$ define a Shannon set $\{r, s\}$.

3. If $\mathcal{R} = \mathbb{Z}_2^3$, then a Shannon set is given by $\{(0,1,1), (1,0,1), (1,1,0)\}$.

4. Let $\mathcal{R} = \mathbb{Z}$, the ring of integers, then the set $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ has the unique decoding property. Moreover, $\mathbb{Z}^*$ is maximal in the sense that every set $\mathbf{X} \in \mathcal{U}(\mathbb{Z})$, $X \neq \{0\}$, is a subset of $\mathbb{Z}^*$. This observation generalizes to every integral domain, i.e., a commutative ring $\mathcal{R}$ without zero divisors.

5. Let $\mathcal{R} = \mathbb{Z}^{n\times n}$, $n \geq 1$, the ring of $(n \times n)$-matrices with entries in $\mathbb{Z}$. Then

$$\mathbf{X} = \{A \mid \det A \neq 0,\ A \in \mathbb{Z}^{n\times n}\}$$

belongs to $\mathcal{U}(\mathbb{Z}^{n\times n})$. Furthermore, $\mathbf{X}$ is maximal in $\mathcal{U}(\mathbb{Z}^{n\times n})$.

3 Shannon sets of the ring $\mathbb{F}_q^{n\times n}$

In this section, we study the ring of matrices over a finite field of characteristic p, where p is a prime number. We will show that for rings of this type there exists only one Shannon set.

Theorem 3.1 *Let $\mathcal{R} = \mathbb{F}_q^{n\times n}$ be the ring of $n \times n$-matrices with entries in the field F_q of characteristic p. The set $Gl(n, \mathbb{F})$ of invertible matrices is the only Shannon set of $\mathbb{F}_q^{n\times n}$.*

Proof: The set $Gl(n, \mathbb{F}_q)$ of invertible $n\times n$-matrices has the unique decoding property. The cardinality of $Gl(n, \mathbb{F}_q)$ is given by $\prod_{j=0}^{n-1}(q^n - q^j)$. Now suppose that $\mathbf{X} \in \mathcal{U}(\mathbb{F}_q^{n\times n})$ is such that $|\mathbf{X}| > |Gl(n, \mathbb{F}_q)|$. Then $\mathbf{X}$ contains at least one matrix A such that $A \notin Gl(n, \mathbb{F}_q)$. If we consider A as a linear map from the $\mathbb{F}_q$-vectorspace $\mathbb{F}_q^n$ to itself, then $A\left(\mathbb{F}_q^n\right)$ is an at most $(n-1)$–dimensional subspace of $\mathbb{F}_q^n$. This gives that the cardinality of the set $A\mathbb{F}_q^{n\times n} = \{AB \mid B \in \mathbb{F}_q^{n\times n}\}$ is smaller than or equal to $q^{n(n-1)}$. On the other hand, $A \in \mathbf{X}$ and therefore $|A\mathbf{X}| = |\mathbf{X}|$. This yields $|Gl(n, \mathbb{F}_q)| = \prod_{j=0}^{n-1}(q^n - q^j) < |\mathbf{X}| = |A\mathbf{X}| \leq q^{n(n-1)}$, which is a contradiction.

Therefore, no element of $\mathcal{U}(\mathbb{F}_q^{n\times n})$ has a cardinality larger than $Gl(n, \mathbb{F}_q)$. As the above arguments show, a Shannon set does not contain a non-invertible matrix. This shows that $Gl(n, \mathbb{F}_q)$ is the only Shannon set.

■

As a consequence we note

Corollary 3.2

$$\chi\left(\mathbb{F}_q^{n\times n}\right) = \prod_{j=0}^{n-1}(q^n - q^j).$$

4 Shannon sets of the ring $\mathbb{Z}_m$

In this section we study the residue class rings $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$, where m is a natural number. Theorem 4.2 shows that the Shannon number of the ring $\mathbb{Z}_m$ is equal to the cardinality of the set of units $\mathbb{Z}_m^*$. Moreover, we provide the proofs for the results listed in Table 1.

We begin with an auxiliary Lemma and some notations.

Lemma 4.1 *If $1 < p_2 < p_3 < \ldots < p_L$ are natural numbers, then*

$$\prod_{j=2}^{L} \frac{p_j}{p_j - 1} \leq p_L,$$

where equality holds if and only if $j = p_j$ for all $j = 2, \ldots, L$.

The simple proof is omitted.

The function $\phi : \mathbb{N} \to \mathbb{N}$ defined as $\phi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right)$, where the product runs over all prime numbers p that divide m, is called *Euler's totient function*, see [2]. $\phi(m)$ is equal to the number of units in the ring $\mathbb{Z}_m$. Moreover, ϕ has the following two properties

- For all prime numbers and all $\alpha \in \mathbb{N} \setminus \{0\}$ one has

$$\phi(p^\alpha) = p^{\alpha-1}\phi(p).$$

- If m_1 and m_2 are relatively prime, i.e., $\gcd(m_1, m_2) = 1$, then

$$\phi(m_1 m_2) = \phi(m_1)\phi(m_2).$$

If d is a divisor of m, then the set $Z_m(d)$ denotes the set $\{l \in \mathbb{Z}_m \mid \gcd(l, m) = d\}$, and we have

$$|Z_m(d)| = \phi\left(\frac{m}{d}\right).$$

Moreover, for two divisors d_1 and d_2 of m we have that $d_1 Z_m(d_2) = Z_m(\gcd(d_1 d_2, m))$. The collection of sets $Z_m(d)$, d divides m, forms a partition of $\mathbb{Z}_m$, i.e., $\mathbb{Z}_m = \cup_{d|m} Z_m(d)$ and every $x \in \mathbb{Z}_m$ is containded in a unique $Z_m(d)$.

Moreover, as a consequence of Lemma 4.1, we have the following inequality

$$\frac{m}{\phi(m)} = \prod_{p|m} \frac{p}{p-1} \leq p_L, \tag{1}$$

where p_L is the largest prime divisor of m.

Theorem 4.2 *If $\mathcal{R} = \mathbb{Z}_m$, then the set of units $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$ is a Shannon set.*

Proof: We suppose that $\mathbf{X}$ is a Shannon set such that $|\mathbf{X}| > \phi(m) = |\mathbb{Z}_m^*|$ an show that this leads to a contradiction. We begin with two auxiliary results.

1. If $d_1 = 1 < d_2 < \ldots < d_M$ are the divisors of m such that $d_j < \frac{m}{\phi(m)}$ for all $j = 1, \ldots, M$, then

$$\mathbf{X} \subseteq \bigcup_{j=1}^{M} Z_m(d_j).$$

Proof: Suppose $x \in \mathbf{X}$ and $x \in Z_m(d)$ where $d \geq \frac{m}{\phi(m)}$, then, due to our assumption on $|\mathbf{X}| > \phi(m)$ and the fact that $\mathbf{X}$ is a Shannon set, we have

$$\phi(m) < |\mathbf{X}| = |x\mathbf{X}| \leq |d\mathbb{Z}_m| = \frac{m}{d} \leq \phi(m),$$

which is a contradiction.

2. If d is a proper divisor of m, i.e., $d > 1$, such that $d < \frac{m}{\phi(m)}$, then $\mathbf{X} \cap Z_m(d) = \emptyset$.

Proof: Let d be the largest proper divisor of m such that $Z_m(d) \cap \mathbf{X} \neq \emptyset$ and let $d_1 = 1 < d_2 < \ldots < d_{K-1} < d_K = d$ be all divisors of m less than or equal to d_K. By 1., it follows that $d_K < \frac{m}{\phi(m)}$. If $m^* = \mathrm{lcm}(d_1, \ldots, d_K)$ denotes the least common multiple of d_1, ..., d_K, then we can write

$$m = m^* \prod_{i=1}^{L} p_i^{\beta_i} m',$$

where $p_1 < \ldots < p_L$ are the prime divisors of m^* and the prime divisors of m' are all greater than d_K.

By 1. we have that

$$\mathbf{X} \subseteq Z_m(d_1) \cup \ldots \cup Z_m(d_K).$$

Let $y \in \mathbf{X} \cap Z_m(d)$. Since $\mathbf{X}$ is a Shannon set of cardinality greater than $\phi(m)$, it follows that

$$\phi(m) < |\mathbf{X}| = |y\mathbf{X}| \leq |d_K \left(Z_m(d_1) \cup \ldots \cup Z_m(d_K)\right)|,$$

which implies

$$\phi(m) < \left| \bigcup_{j=1}^{K} Z_m(\gcd(d_K d_j, m)) \right| = \left| \bigcup_{j=1}^{K} Z_m\left(d_K \gcd\left(d_j, \frac{m^*}{d_K} \prod_{i=1}^{L} p_i^{\beta_i} m' \right) \right) \right|.$$

This can be estimated by

$$\phi(m) < \left| \bigcup_{j=1}^{K} Z_m\left(d_K \gcd\left(d_j, \frac{m^*}{d_K} \prod_{i=1}^{L} p_i^{\beta_i} m' \right) \right) \right| \leq \left| \bigcup_{\delta} Z_m(d_K \delta) \right|,$$

where δ runs over the divisors of $\frac{m^*}{d_K} \prod_{i=1}^{L} p_i^{\beta_i}$. Using Euler's totient function ϕ, we obtain the inequality

$$\phi(m) < \left| \bigcup_{\delta} Z_m(d_K \delta) \right| = \sum_{\delta} \phi\left(\frac{m}{d_K \delta} \right) = \phi(m') \sum_{\delta} \phi\left(\frac{m^* \prod_{i=1}^{L} p_i^{\beta_i}}{d_K \delta} \right).$$

Since the sum is over all divisors of $\frac{m^*}{d_K} \prod_{i=1}^{L} p_i^{\beta_i}$, we obtain the inequality

$$\phi(m) < \phi(m') \frac{m^*}{d_K} \prod_{i=1}^{L} p_i^{\beta_i}.$$

With $\phi(m) = \phi\left(m^* \prod_{i=1}^{L} p_i^{\beta_i} m' \right) = \phi\left(m^* \prod_{i=1}^{L} p_i^{\beta_i} \right) \phi(m')$ and the fact that

$$\phi\left(m^* \prod_{i=1}^{L} p_i^{\beta_i} \right) = m^* \prod_{i=1}^{L} p_i^{\beta_i} \prod_{i=1}^{L} \left(1 - \frac{1}{p_i} \right) = \phi(m^*) \prod_{i=1}^{L} p_i^{\beta_i}$$

we obtain the final inequality

$$\phi(m^*) < \frac{m^*}{d_K},$$

or, $d_K < \frac{m^*}{\phi(m^*)}$. Since $p_1 < \ldots < p_L$ are the prime divisors of m^* there exists a $j_0 \in \{1, \ldots, K\}$ such that $d_{j_0} = p_L \leq d_K$ and thus we have, see 1,

$$p_L \leq d_K < \frac{m^*}{\phi(m^*)} = \prod_{j=1}^{L} \frac{p_j}{p_j - 1}$$

which is a contradiction to Lemma 4.1. Therefore we can conclude that no proper divisor d of m exists such that $\mathbf{X} \cap Z_m(d) \neq \emptyset$. This proves the second auxiliary result.

We are now prepared to finish the proof of Theorem 4.2. By 1., we have $\mathbf{X} \subseteq Z_m(d_1) \cup \ldots \cup Z_m(d_M)$, where d_M is the largest divisor less than $m/\phi(m)$. By 2., it follows that $\mathbf{X} \subseteq Z_m(1)$, which contradicts our assumption $|\mathbf{X}| > \phi(m)$. This completes the proof of Theorem 4.2.

■

Theorem 4.3 *If* $\gcd(m, 6) = 1$, *then* $\mathbb{Z}_m^*$ *is the unique Shannon set of the ring* $\mathbb{Z}_m$.

Proof: If $\mathbf{X}$ is a Shannon set different from $\mathbb{Z}_m^*$, then there exists a largest non-trivial divisor d of m such that $\mathbf{X} \cap Z_m(d) \neq \emptyset$. Due to the above observations in 1. from the previous proof, d has to satisfy $d \leq \frac{m}{\phi(m)}$. Following the arguments given in 2. of the proof of Theorem 4.2, d also satisfies

$$d \leq \frac{m^*}{\phi(m^*)},$$

where m^* is the lowest common multiple of all divisors of m which are less than or equal to d. If $p_2 < \ldots < p_L$ denote the prime divisors of m^*, then we have that

$$p_L \leq d \leq \frac{m^*}{\phi(m^*)} = \prod_{j=2}^{L} \frac{p_j}{p_j - 1}. \tag{2}$$

Since $\gcd(m, 6) = 1$, we have $4 < p_2 < \ldots < p_L$ and Lemma 4.1 implies

$$\prod_{j=2}^{L} \frac{p_j}{p_j - 1} < p_L,$$

which contradicts inequality 2.

■

The proof of Theorem 4.3 gives a hint how to construct Shannon sets $\mathbf{X} \subset \mathbb{Z}_m$ such that $\mathbf{X} \neq Z_m(1)$. If $\mathbf{X}$ is a Shannon set and d a maximal divisor of m such that $\mathbf{X} \cap Z_m(d) \neq \emptyset$, then our above considerations yield the inequalities

$$\frac{m^*}{\phi(m^*)} \leq p_L \leq d \leq \frac{m^*}{\phi(m^*)},$$

where $m^* = \operatorname{lcm}(d_1, \ldots, d_K = d)$ and $p_1 < \ldots < p_L$ are the prime divisors of m^*. It follows that $p_L = m^*/\phi(m^*)$ and, due to Inequality 1, it follows that the prime divisors of m^* may be either $p_1 = 2$ or $p_1 = 2 < p_2 = 3$. This implies that $\mathbf{X} \cap Z_m(d) \neq \emptyset$ is only possible for $d = 2, 3$.

For natural numbers m such that $\gcd(m, 6) \neq 1$ the existence of a unique Shannon set depends on divisibility properties of m w.r.t. 2 and 3.

Theorem 4.4 *Let $m = 2^\alpha 3^\beta m'$ such that $\alpha, \beta \in \mathbb{N}$ and $\gcd(m', 6) = 1$.*

1. *If $\alpha = 0$ and $\beta \geq 1$, then $Z_m(1)$ is the only Shannon set of $\mathbb{Z}_m$.*
2. *If $\alpha \geq 3$ and $\beta \geq 0$, then $Z_m(1)$ is the only Shannon set of $\mathbb{Z}_m$.*

Proof: *1.* A Shannon set $\mathbf{X}$ different from $Z_m(1)$ satisfies $\mathbf{X} \cap Z_m(3) \neq \emptyset$. In particular $\mathbf{X} \subset Z_m(1) \cup Z_m(3)$.

For $\beta = 1$ and for $x \in \mathbf{X} \cap Z_m(3)$ we have the inequality

$$\phi(m) = \phi(3m') = |x\mathbf{X}| \leq |x(Z_m(1) \cup Z_m(3))| = |Z_m(3)|.$$

By the elementary properties of ϕ one obtains $\phi(3m') = 2\phi(m') \leq \phi(m')$; a contradiction.

For $\beta \geq 2$, i.e., $m = 3^\beta m'$, the assumption $x \in \mathbf{X} \cap Z_m(3)$ leads to the inequality

$$\phi(m) = |x\mathbf{X}| \leq |x(Z_m(1) \cup Z_m(3))| \leq |Z_m(3) \cup Z_m(9)|,$$

which gives $\phi(3^\beta m') \leq \phi(3^{\beta-1} m') + \phi(3^{\beta-2} m')$. This yields

$$\phi(3^\beta) \leq \phi(3^{\beta-1}) + \phi(3^{\beta-2}),$$

which is equivalent to

$$3^2\phi(3^{\beta-2}) \leq 3\phi(3^{\beta-2} + \phi(3^{\beta-2}).$$

This leads to the contradiction $9 \leq 3+1$.

2. We start with $\beta = 0$, i.e., $m = 2^\alpha m'$, $\alpha \geq 3$. If $\mathbf{X}$ is a Shannon set such that $x \in \mathbf{X} \cap Z_m(2)$, then, by similar arguments as in *1.*, we obtain the inequality

$$\phi(2^\alpha) \leq \phi(2^{\alpha-1}) + \phi(2^{\alpha-2})$$

which gives $4 \leq 3$; a contradiction.

For $\beta = 1$, i.e., $m = 2^\alpha 3m'$, a Shannon set $\mathbf{X}$ different from $Z_m(1)$ satisfies $\mathbf{X} \cap (Z_m(2) \cup Z_m(3)) \neq \emptyset$. Suppose there exist a $x \in \mathbf{X} \cap Z_m(3)$, then we have $\phi(m) = |\mathbf{X}| = |x\mathbf{X}| \leq |Z_m(3) \cup Z_m(6)|$, which gives the inequality

$$\phi(2^\alpha\, 3) \leq \phi(2^\alpha) + \phi(2^{\alpha-1}),$$

which yields $4 \leq 3$; a contradiction. Thus we conclude that $\mathbf{X}$ satisfies $\mathbf{X} \cap Z_m(3) \neq \emptyset$.

For $x \in \mathbf{X} \cap Z_m(2)$ we obtain $x\mathbf{X} \subset Z_m(2) \cup Z_m(4)$, which yields the estimate

$$\phi(2^\alpha\, 3) \leq \phi(2^{\alpha-1}\, 3) + \phi(2^{\alpha-2}\, 3)$$

being not true for all $\alpha \geq 3$.

Finally, we consider $\beta \geq 2$, i.e., $m = 2^\alpha\, 3^\beta m'$. Then the assumption $x \in \mathbf{X} \cap Z_m(3)$ leads to the inequality

$$\phi(2^\alpha\, 3^\beta) \leq \phi(2^\alpha\, 3^{\beta-1}) + \phi(2^{\alpha-1}\, 3^{\beta-1}) + \phi(2^\alpha\, 3^{\beta-2})$$

which is equivalent to $6 \leq 3 + \frac{\phi(3^{\beta-2})}{3^{\beta-2}} \leq 4$; a contradiction. The assumption $x \in \mathbf{X} \cap Z_m(2)$ leads again to a contradiction.

■

In the remaining cases, i.e, $m = 2m'$, $\gcd(m', 2) = 1$ and $m = 4m'$, $\gcd(m', 2) = 1$, there exists more than one Shannon set.

Theorem 4.5 *For a natural number of the form $m = 2^\alpha m'$, where $\alpha = 1, 2$ and $\gcd(m', 2) = 1$ the following holds.*

1. *If $\alpha = 1$, and $m = 2 \cdot 3^\beta m'$, where $\gcd(6, m') = 1$ and $\beta \neq 1$, then there exist $2^{\phi(3^\beta m')}$ different Shannon sets of $\mathbb{Z}_m$.*
2. *If $\alpha = 1$ and $m = 6m'$, where $\gcd(m', 6) = 1$, then there exist $2^{2\phi(m')+1} - 2^{\phi(m')}$ different Shannon sets of $\mathbb{Z}_m$.*
3. *If $\alpha = 2$, then there exist $2^{\phi(m')} + 1$ different Shannon sets of $\mathbb{Z}_m$.*

Proof. *1.*a) We begin with the case $\beta = 0$, i.e., $m = 2m'$. By the arguments given in the proof of Theorem 4.3, a Shannon set $\mathbf{X}$ has to be a subset of $Z_m(1) \cup Z_m(2)$ and we write

$$\mathbf{X} = \mathbf{X}(1) \cup \mathbf{X}(2),$$

where $\mathbf{X}(i) = \mathbf{X} \cap Z_m(i)$, for $i = 1, 2$. Note that $|Z_m(2)| = |Z_m(1)| = \phi(m)$. Moreover, since $2Z_m(2) = Z_m(2)$, it follows that $Z_m(2)$ has the unique decoding property. Since the cardinality of $Z_m(2)$ equals the cardinality of $Z_m(1)$, it follows that $Z_m(2)$ is a Shannon set. Finally we note that the map $Z_m(2) \ni x \mapsto x + m' \in Z_m(1)$ is bijective.

Let $\mathbf{X}$ be a Shannon set and let $x \in \mathbf{X}(2)$. Since $\mathbf{X}$ is a Shannon set it follows that $x^2 \in x\mathbf{X}$. On the other hand, one has that $x(x+m') = x^2$ and $x+m'$ being an element of $Z_m(1)$ is therefore not an element of $\mathbf{X}(1)$. Thus we see that $\mathbf{X}(1) = Z_m(1) \setminus (\mathbf{X}(2)+m')$ and $\mathbf{X} = (Z_m(1) \setminus (\mathbf{X}(2)+m')) \cup \mathbf{X}(2)$.

On the other hand, if $\mathbf{Y}$ is any subset of $Z_m(2)$, then $(Z_m(1) \setminus (\mathbf{Y}+m') \cup \mathbf{Y}$ is a Shannon set. So there are $2^{|Z_m(2)|}$ Shannon sets for $\beta = 0$.

b) Now suppose that $m = 2 \cdot 3^\beta m'$, where $\beta \geq 2$. A Shannon set $\mathbf{X}$ is a subset of $Z_m(1) \cup Z_m(2) \cup Z_m(3)$ and we write

$$\mathbf{X} = \mathbf{X}(1) \cup \mathbf{X}(2) \cup \mathbf{X}(3),$$

where $\mathbf{X}(i) = \mathbf{X} \cap Z(i)$, $i = 1, 2, 3$.

If $x \in \mathbf{X}(3)$, then it follows that $\phi(m) = |x\mathbf{X}| \leq |Z_m(3) \cup Z_m(6) \cup Z_m(9)|$. We therefore obtain the inequality

$$\phi(2 \cdot 3^\beta m') \leq \phi(2 \cdot 3^{\beta-1} m') + \phi(3^{\beta-1} m') + \phi(2 \cdot 3^{\beta-2} m')$$

which is impossible. This shows that $\mathbf{X} \subset Z_m(1) \cup Z_m(2)$ and an application of the same arguments as above gives the desired result.

2. For $m = 6m'$, where $\gcd(m', 6) = 1$, we have the following facts

- $Z_m(1) = Z_m(2) + 3m'$.
- $Z_m(1) = (Z_m(3) + 2m') \cup (Z_m(3) + 4m')$ and $(Z_m(3) + 2m') \cap (Z_m(3) + 4m') = \emptyset$.
- $|Z_m(1)| = |Z_m(2)| = 2\phi(m')$ and $|Z_m(3)| = \phi(m')$.

As before, we have $\mathbf{X} = \mathbf{X}(1) \cup \mathbf{X}(2) \cup \mathbf{X}(3)$. If $\mathbf{X}(3) = \emptyset$, then the arguments of *1.*a) for $\beta = 0$ apply and since $m = 2(3m')$, we count $2^{\phi(3m')} = 2^{2\phi(m')}$ Shannon sets.

If $x \in \mathbf{X}(3)$, then $\mathbf{X}(1)$ does not contain $x + 2m'$ and $x + 4m'$, since $x^2 = x(x + 2m') = x(x + 4m')$. Moreover, if $x' \in \mathbf{X}(1)$, then there exists $\zeta \in Z_m(3)$ such that either $x' = \zeta + 2m'$ or $x' = \zeta + 4m'$. On the other hand, for $x \in \mathbf{X}(3)$ we have that $xx' = x(\zeta + 2m') = x(\zeta + 4m')$. I.e., if $x' = \zeta + 2m' \in \mathbf{X}(1)$, then $\zeta + 4m' \notin \mathbf{X}(1)$ and vice versa. We conclude that $|\mathbf{X}(1)| \leq \phi(m') - |\mathbf{X}(3)|$. On the other hand, we have that

$$|\mathbf{X}| = 2\phi(m') = |\mathbf{X}(1)| + |\mathbf{X}(2)| + |\mathbf{X}(3)| \leq \phi(m') + |\mathbf{X}(2)|\,.$$

Therefore $|\mathbf{X}(2)| \geq \phi(m')$.

If $x' \in Z_m(2)$, then either $x' + 2m' \in Z_m(2)$ or $x' + 4m' \in Z_m(2)$. In any case it follows for $x \in \mathbf{X}(3)$ and $x' \in \mathbf{X}(2)$ that either $xx' = x(x' + 2m')$ or $xx' = x(x' + 4m')$. Therefore $|\mathbf{X}(2)| \leq \phi(m')$. By our above inequality, it follows that $|\mathbf{X}(2)| = \phi(m')$.

Finally, if $x' \in \mathbf{X}(2)$, then $x' + 3m' \notin \mathbf{X}(1)$, otherwise $x'x' = x'(x' + 3m')$. This gives that

$$\mathbf{X}(1) = Z_m(1) \setminus \left((\mathbf{X}(2) + 3m') \cup (\mathbf{X}(3) + 2m') \cup (\mathbf{X}(3) + 4m')\right).$$

On the other hand, for a given non-empty subset $\mathbf{Y}(3)$ of $Z(3)$ and a subset $\mathbf{Y}(2) \subset Z(2)$ such that $|\mathbf{Y}(2)| = \phi(m')$ and such that for given $x_1, x_2 \in \mathbf{X}(2)$ with $x_1 \not\equiv x_2 \bmod 2m'$, we define $\mathbf{Y}(1)$ as in the above formula (replace $\mathbf{X}$ by $\mathbf{Y}$). Then $\mathbf{Y}(1) \cup \mathbf{Y}(2) \cup \mathbf{Y}(3)$ is a Shannon set.

This gives $2^{\phi(m')}(2^{\phi(m')} - 1)$ Shannon sets if $\mathbf{X}(3) \neq \emptyset$, plus the number of Shannon sets in case $\mathbf{X}(3) = \emptyset$, which gives a total of $2^{2\phi(m')+1} - 2^{\phi(m')}$ Shannon sets.

3. Let $m = 4 \cdot 3^\beta m'$, where $\gcd(m', 6) = 1$. As a first step we consider the case $\beta = 0$, i.e., $m = 4m'$. We have that $|\mathbf{X(1)}| = 2\,|\mathbf{X(2)}| = 2\,|\mathbf{X(4)}|$. Moreover, since the map

$Z_m(2) \ni x \mapsto 2x \in Z_m(4)$ is bijective, it follows that $Z_m(2)$ has the unique decoding property. The map $Z_m(1) \ni x \mapsto x + 2m' \in Z_m(1)$ is bijective.

If $\mathbf{X} = \mathbf{X}(1) \cup \mathbf{X}(2)$ is a Shannon set such that $\mathbf{X}(2) \neq \emptyset$, then $x \in \mathbf{X}(1)$ implies $x + 2m' \notin \mathbf{X}(1)$; otherwise we would have for $y \in \mathbf{X}(2)$: $yx = y(x + 2m')$. This shows that $|\mathbf{X}(1)| \leq \phi(m')$. Since $\mathbf{X}$ is a Shannon set, it follows that $|\mathbf{X}(2)| = \phi(m')$, i.e., $\mathbf{X}(2) = Z_m(2)$, and $|\mathbf{X}(1)| = \phi(m')$. Note that $\mathbf{X}(1)$ is such that $(\mathbf{X}(1) + 2m') \cap \mathbf{X}(1) = \emptyset$.

Let $\mathbf{Y} \subset Z_m(1)$ be such that $(\mathbf{Y} + 2m') \cap \mathbf{Y} = \emptyset$, then $\mathbf{Y} \cup Z_m(2)$ is a Shannon set. This gives $2^{\phi(m')}$ Shannon sets. Since $Z_m(1)$ is also a Shannon set, the assertion follows.

As a next step we consider $m = 12m'$, where $\gcd(m', 6) = 1$. A Shannon set $\mathbf{X}$ is a subset of $Z_m(1) \cup Z_m(2) \cup Z_m(3)$. If we assume that there exists $x \in \mathbf{X}(3)$, then we arrive at the inequality $\phi(12) \leq \phi(4) + \phi(2)$, a contradiction. Thus we conclude that $\mathbf{X} \subset Z_m(1) \cup Z_m(2)$ and apply the arguments for the case $m = 4m'$.

The case $m = 4 \cdot 3^\beta$ for $\beta \geq 2$ is treated in a similar way. The assumption $\mathbf{X}(3) \neq \emptyset$ leads to a contradiction. Thus $\mathbf{X} \subset Z_m(1) \cup Z_m(2)$ and we can use the same arguments as in *1.* for $\beta = 0$.

■

Acknowledgments This research was supported by the Concerted Action Project GOA-Mefisto of the Flemisch Community, by the FWO (Fund for Scientific Research Flanders) projects G.0080.01 and by the Belgian Program on Interuniversity Attraction Poles of the Belgian Prime Minister's Office for Science Technology and Culture (IAP V-22).

References

[1] R. Ahlswede, N. Cai, Z. Zhang. On Interactive Communication, IEEE Trans. Inform. Th., Vol. 43., No. 1, Jan. 1997, 22–37.

[2] G.H. Hardy, E.M. Wright. *An Introduction to the Theory of Numbers*, 5th edition, Oxford Clarendon Press, 1979.

[3] C.E. Shannon. Two-way communication channels, Proc. 4th Berkeley Symp. Math. Stat. and Prob., 1961, 611–644.

[4] L. Tolhuizen. New rate pairs in the zero-error capacity region of the binary multiplying channel without feedback, IEEE Trans. Inform. Th. Vol. 46, No. 3, 2000, 1043–1046.