Delft University of Technology
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft Institute of Applied Mathematics

Cooperative Locality of Shortened Hamming Codes

(Dutch title: Coöperatieve Localiteit van Verkorte Hamming Codes)

A thesis submitted to the
Delft Institute of Applied Mathematics
in partial fulfillment of the requirements

for the degree

BACHELOR OF SCIENCE
in
APPLIED MATHEMATICS

by

Joep Bom

Delft, Nederland
June 2017

BSc Thesis APPLIED MATHEMATICS

"Cooperative Locality of Shortened Hamming Codes"

(Dutch title: "Coöperatieve Localiteit van Verkorte Hamming Codes"

Joep Bom

Delft University of Technology

Supervisor

Dr.ir. J.H. Weber

Thesis committee

Dr. D.C. Gijswijt Dr. J.A.M. De Groot

June, 2017 Delft

Preface

This bachelor thesis is written as part of the curriculum of bachelor students of Applied Mathematics, at the TU Delft. The first time I learned about coding theory was at the Junior TU-Delft program in 2012; I was intrigued, and took coding theory as subject for my final project (Profielwerkstuk). My interest in the subject grew during my time as a student of Applied Mathematics, where I was able to learn more about linear algebra and coding theory. Therefore it is no surprise that I ended up writing my bachelor thesis on this interesting subject.

My supervisor, J. Weber, had recently written a paper about cooperative locality, which is to be published this month at the IEEE International Symposium on Information Theory. As demand and usage of cloud storage increases, cooperative locality has recently become more important. I feel privileged to be able to research this very recent field of mathematics.

I would like to thank my supervisor, J. Weber, for his guidance and flexibility in the process of writing this thesis. Next, I would like to thank my thesis committee, for reviewing my thesis. Last of all, I would like to thank Eliran, for correcting my English, and helping me through this very busy quarter.

Joep Bom
Delft, June 2017

Abstract

Binary erasure-repairing codes protect information stored on multiple servers by adding parity servers. A characteristic of a code is its cooperative locality; a measure of the amount of servers that need to be accessed to repair erased servers. This report discusses the cooperative locality of Hamming codes and shortened Hamming codes, using the row space of parity-check matrices of these codes. In some cases, an equality for this locality is found, in other cases a bound is given.

Contents

1

Introduction

This report discusses binary erasure-repairing codes and their qualities. In Section 1.1, an introduction to the field of repairing erasures can be found. Section 1.2 discusses some fundamentals of erasure-repairing codes.

1.1. Introduction

Every file on a computer is nothing more than a long row of 0's and 1's, called *bits*. Recently, files are often stored in the cloud; this means that the file is spread over multiple servers, called *data* servers. Due to numerous varying causes, servers can fail and get erased, referred to as an *erasure*. This means part of the file is lost. The field of erasure-repairing codes finds ways to secure servers against erasures. By adding extra servers in a smart way, the bits on an erased server can be retrieved. These ways are called *codes*, and the added servers are called *parity* servers. In this report, it is assumed that all servers contain the same amount of bits. In subsection 1.1.1, 1.1.2 and 1.1.3, three different codes are discussed. Subsection 1.1.4 compares these codes based on three key factors.

1.1.1. Repetition Code

The most trivial code for securing servers against erasures, is the *Repetition code*. This code creates a duplicate of every server, doubling the amount of servers. If a server were to get erased, its data can be retrieved by copying the data of its duplicate server, into the erased server. In that way the servers would return to their original state, repairing the erasure.

Example 1. Assume there are four servers containing data, call these servers S1, S2, S3 and S4. Four parity servers are added, called P1, P2, P3 and P4. Here P1=S1, P2=S2, P3=S3 and P4=S4. If server S3 gets erased, it can be repaired by copying the data of server P3 into S3.

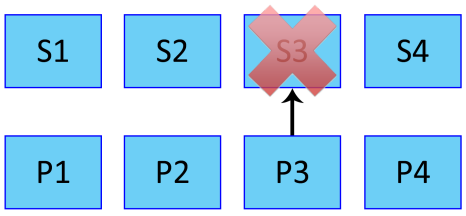

Figure 1.1: Visual representation of the Repetition code.

1.1.2. Parity Code

A different way to secure servers, is to add one parity server in a smart way. This code is called the *Parity code*. The bits in the parity server are chosen in a specific way; the i^{th} bit of the parity server is

a 0, if the sum of the i^{th} bits of the data servers is even. If this sum is uneven, the i^{th} bit in the parity server will be a 1. That way the sum of the i^{th} bits of all (data and parity) servers is always even.

If one server is erased, its data can be repaired bit by bit. The i^{th} bit can be found with the sum of the i^{th} bits of all non-erased servers.

Example 2. Assume there are four data servers: S1 containing 1101, S2 containing 1010, S3 containing 1111 and S4 containing 0000, and one parity server P1. The sum of the first bits is $1 + 1 + 1 + 0 = 3$, which is uneven, therefore the first bit in the parity server P1 is a 1. Repeating this process for the second, third and fourth bit, we find that P1 contains 1000.

Now assume S3 is erased. The sum of the first bits of S1, S2, S4 and P1 is 1+1+1+0=3. So the first bit of S3 had to be a 1. Repeating this process for the second, third and fourth bit, we find that S3 must contain 1111. Thus the erased data can be retrieved.

Figure 1.2: Visual representation of the Parity code.

1.1.3. (7,4)-Hamming Code

The Repetition code and the Parity code can repair one erasure, but if two erasures happen at the same time, these codes can not guarantee that they can be repaired. The (7,4)-Hamming code is a code that can repair two erasures, by adding three parity servers to four data servers. Call the data and parity servers respectively S1, S2, S3, S4, P1, P2 and P3. Let the i^{th} bit in S1 be $s1_i$, and name the bits in the other servers similarly.

The i^{th} bits in the parity servers are again determined by the i^{th} bits in the data servers:

choose $p1_i$ such that $s1_i + s2_i + s4_i + p1_i$ is even
choose $p2_i$ such that $s1_i + s3_i + s4_i + p2_i$ is even
choose $p3_i$ such that $s2_i + s3_i + s4_i + p3_i$ is even

These conditions are visually represented in Figure 1.3. The bits in P1, P2 and P3 are chosen in such a way, that the sum of the bits in every circle is even.

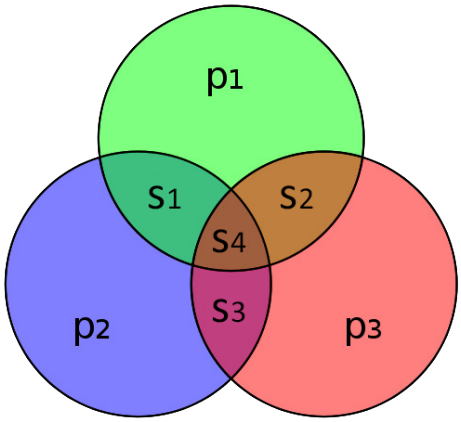

Figure 1.3: Graphical depiction of the (7,4)-Hamming code.

Example 3. Assume there are four data servers: S1 containing 1101, S2 containing 1010, S3 containing 1111 and S4 containing 0000. Then using the conditions above we can determine that P1 contains 0111, P2 contains 0010, and P3 contains 0101.

Now assume S1 and P1 are erased. For all $i \in \{1, 2, 3, 4\}$, the sum $s1_i + s3_i + s4_i + p2_i$ is even, so S1 can be repaired using S3, S4 and P2. Now P1 can be repaired using S1, S2 and S4, since for all $i \in \{1, 2, 3, 4\}$, the sum $s1_i + s2_i + s4_i + p1_i$ is even. We find that S1 contains 1101, and P1 contains 0111.

1.1.4. Key Factors

In subsection 1.1.1, 1.1.2 and 1.1.3, three different erasure-repairing codes are introduced. What makes one code better than another?

There are three key factors, which evaluate and represent the quality of a code:

- Repairability: The amount of simultaneous erasures a code can always repair.
- Information Rate: The amount of data servers divided by the total amount of servers.
  - The fraction of the storage that contains data
- e-Cooperative Locality: The amount of servers accessed to repair e erasures.
  - Closely related to the time it takes to repair e erasures.

Depending on the application, one key factor can be more important than another. If your data needs to be very reliant, repairability is important. If the amount of storage is limited, the information rate is important. If erasures need to be repaired quickly, the cooperative locality is important. In Example 4, 5 and 6, the key factors of our three codes are determined.

Example 4. *Repetition code*

- The Repetition code can repair one erasure, as seen in subsection 1.1.1. If two erasures happen, one in a data server and one in its duplicate parity server, the servers can not be repaired. Therefore, the Repetition code has a repairability of one erasure.
- Since every data server is duplicated, this code has an information rate of $\frac{1}{2}$.
- In order to repair an erasure, only one server needs to be accessed. So the 1-Cooperative Locality of the code is 1.

Example 5. *Parity code*

- The Parity code can repair one erasure, as seen in subsection 1.1.2. If two erasures happen, the servers can not be repaired. Therefore, the Parity code has a repairability of one erasure.
- Assume there are k data servers. Since the Parity code adds one parity server, this code has an information rate of $\frac{k}{k+1}$.
- In order to repair an erasure, all k other servers need to be accessed. So the 1-Cooperative Locality of the code is k.

Example 6. *(7,4)-Hamming code*

- The (7,4)-Hamming code can repair up to two erasures, as seen in subsection 1.1.3. If three erasures happen, they can not always be repaired. Therefore, the (7,4)-Hamming code has a repairability of two erasures.
- Since this code adds three parity servers to four data servers, it has an information rate of $\frac{4}{7}$.
- In order to repair one erasure, the servers in only one of the circles in Figure 1.3 need to be accessed. This means only three servers need to be accessed to repair one erasure. So the 1-Cooperative Locality of the code is 3.
  In order to repair two erasures, the servers in only two of the three circles in Figure 1.3 need to be accessed. This means four servers need to be accessed to repair two erased servers. So the 1-Cooperative Locality of the code is 4.

1.2. Fundamentals

An (n,k)-*code* is a code that secures k data servers, by adding $n-k$ parity servers. So in total there are n servers. Filling our parity servers is called *encoding*. Codes determine these bit by bit. Therefore encoding can be seen as an injective function $f(\mathbf{x}) : (F_2)^k \to (F_2)^n$, where F_2 is the field with elements $\{0,1\}$. Notice that in this field $1+1=0$. $(F_2)^k$ contains all binary vectors of length k. These vectors are called *message words*. The image of function $f(\mathbf{x})$ is called the *code* C. Elements of C are called *codewords*. Notice that $C \subseteq (F_2)^n$, and $|C| = |(F_2)^k| = 2^k$.
The repairability of a code is dependent on the difference between codewords. The more the codewords differ, the more erasures a code can repair.

Definition 1. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in (F_2)^n$. Then the *Hamming weight* of $\mathbf{x}$ is $wt(\mathbf{x}) = |\{i \leq n \mid x_i \neq 0\}|$.

Definition 2. Let $\mathbf{x}, \mathbf{y} \in (F_2)^n$. Then the *Hamming distance* between $\mathbf{x}$ and $\mathbf{y}$ is $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} + \mathbf{y})$.

For a (n, k)-code C, the distances between every pair of codewords can be calculated. The minimum distance between two codewords is called the distance d of a code. If C has distance d, C is called a (n, k, d)-*code*. The amount of erasures a code can always repair, is equal to $d - 1$ [1].

Example 7. *(4,2)-Repetition code*
This code adds two parity servers to two data servers. The possible message words are $(F_2)^2 = \{(00), (01), (10), (11)\}$. The encoding function $f(\mathbf{x})$ projects different message words on different codewords. The two parity servers are duplicates of the data servers, so the codewords are: $f((00)) = (0000)$, $f((01)) = (0101)$, $f((10)) = (1010)$ and $f((11)) = (1111)$.

Notice that the minimum Hamming distance between any of these codewords is 2. Therefore, this code is a $(4, 2, 2)$-code with a repairability of 1 erasure.

1.2.1. Linear Codes

In general, a code might have no structure and the codewords can be quite random. The focus in this report is on an important subclass of codes with a clear structure called *linear codes*. Many of the important and widely used codes, are linear codes.

Definition 3. A subspace C of $(F_2)^n$ is a *linear code*.

From Definition 3 follows that C is a linear code, if and only if any linear combination of codewords is also a codeword. A linear (n, k)-code is called a $[n, k]$-code. If it has distance d, it is called a $[n, k, d]$-code.

Example 8.
The Repetition code, Parity code, and (7,4)-Hamming code are examples of linear codes.

Since a $[n, k]$-code C is a subspace of $(F_2)^n$, a basis for C can be found. The dimension of C is equal to k, so this basis contains k codewords. For linear codes, the encoding function $f(\mathbf{x})$ is a linear map.

Definition 4. Let C be a $[n, k]$-code. The $(k \times n)$ matrix G with a basis for C as rows is called a *generator matrix* for C.

If G is a generator matrix for a code C, then the encoding function is the matrix multiplication $f(\mathbf{u}) = \mathbf{u}G$. Notice that there can be many different bases for a code, hence there can also be many different generator matrices for a code.

Often a code only adds parity servers, while the data servers stay intact. In that case, the generator matrix needs to be of the form $G = (I_k \mid A)$, where I_k is the $(k \times k)$ identity matrix. Such a matrix is called a generator matrix in *standard form*. Every linear code has a unique generator matrix in standard form.

Example 9. *(6,3)-Repetition code*
The Repetition code C_1 with $n = 6$ and $k = 3$ contains $2^3 = 8$ codewords. These codewords are:

$$C = \begin{Bmatrix} (000000), & (001001), & (010010), & (011011), \\ (100100), & (101101), & (110110), & (111111) \end{Bmatrix}$$

A basis for C is $B_1' = \{(001001), (011011), (111111)\}$. With this basis a generator matrix can be constructed:

$$G_1' = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Notice that G_1' is not in standard form.
Another basis for C is $B_1 = \{(100100), (010010), (001001)\}$. With this basis a different generator matrix can be constructed:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Notice that G_1 is in standard form.

Example 10. *(5,4)-Parity code*
The Parity code C_2 with $n = 5$ and $k = 4$ contains $2^4 = 16$ codewords. These codewords are all the words of $(F_2)^5$ with an even weight:

$$C_2 = \begin{Bmatrix} (00000), & (00011), & (00101), & (00110), \\ (01001), & (01010), & (01100), & (01111), \\ (10001), & (10010), & (10100), & (10111), \\ (11000), & (11011), & (11101), & (11110) \end{Bmatrix}$$

A basis for C_2 is $B_2 = \{(10001), (01001), (00101), (00011)\}$. With this basis a generator matrix can be constructed:

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Notice that G_2 is in standard form.

Example 11. *(7,4)-Hamming code*
The (7,4)-Hamming code C_3 with $n = 7$ and $k = 4$ contains $2^4 = 16$ codewords:

$$C_3 = \begin{Bmatrix} (0000000), & (0001111), & (0010011), & (0011100), \\ (0100101), & (0101010), & (0110110), & (0111001), \\ (1000110), & (1001001), & (1010011), & (1011100), \\ (1100011), & (1101100), & (1110000), & (1111111) \end{Bmatrix}$$

A basis for C_3 is $B_3 = \{(1000110), (0100101), (0010011), (0001111)\}$. With this basis a generator matrix can be constructed:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Notice that G_3 is in standard form.

For a linear $[n, k]$-code C, there is an easy way to check whether a given word in $(F_2)^n$ is a codeword or not.

Definition 5. Let C be a $[n, k]$-code. Then a binary $((n - k) \times n)$ matrix H over F_2, such that $\mathbf{x} \in C \Leftrightarrow H\mathbf{x} = \mathbf{0}$, is called a *parity-check matrix* of C.

Since C is a subspace of $(F_2)^n$ with dimension k, such a parity-check matrix H can always be found [2].

If a generator matrix of a code C is of the standard form $G = [I_k \mid A]$, then a parity-check matrix of C is $H = [A^T \mid I_{n-k}]$. Knowing this, parity-check matrices for the codes in Example 9, 10 and 11 can easily be found.

Example 12. *(6,3)-Repetition code*
In Example 9, a standard generator matrix for C_1 was found: $G_1 = [I_3 \mid A]$ with $A = I_3$. Then a parity check matrix for C_1 is:

$$H_1 = [A^T \mid I_3] = [{I_3}^T \mid I_3] = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Example 13. *(5,4)-Parity code*
In Example 10, a standard generator matrix for C_2 was found: $G_2 = [I_4 \mid A]$ with $A = (1111)^T$. Then a parity check matrix for C_2 is:

$$H_2 = [A^T \mid I_1] = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Example 14. *(7,4)-Hamming code*
In Example 11, a standard generator matrix for C_3 was found: $G_3 = [I_4 \mid A]$ with

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Then a parity check matrix for C_3 is:

$$H_3 = [A^T \mid I_3] = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

A code can have many parity-check matrices. Let H be a parity-check matrix of a code C. Then every matrix with a basis for the row space of H as rows, is a parity-check matrix for C. In fact, the rows of every parity-check matrix of C form a basis for the row space of H [2].

1.3. Cooperative Locality

The focus in this report, is finding the cooperative locality of shortened Hamming codes. The cooperative locality of a code is equal to the amount of servers that need to be accessed to repair erasures. In that way, the cooperative locality of a code describes the time it takes to repair erasures. The concept of cooperative locality is introduced by Rawat, Mazumdar, and Vishwanath [3]. In this section, cooperative locality will be properly defined, and ways of determining the cooperative locality of a code will be explored.

Definition 6. Let C be a linear $[n, k, d]$-code. The set $R \in \{1, 2, ..., n\}$ is a *cooperative repair set* for a set E, disjoint from R, if every codeword in C which is zero on R is also zero on E. [3]

Definition 7. A linear-$[n, k, d]$-code C has (r, e)-*cooperative locality*, where $1 \leq e < d$, if every set E of size e has a cooperative repair set of size r or less. [3]

Lemma 1. *Let C be a linear $[n, k, d]$-code. The set $R \subseteq \{1, 2, \dots, n\}$ is a cooperative repair set for the nonempty set $E \subseteq \{1, 2, \dots, n\}$ disjoint from R if and only if there are $|E|$ words $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,n})$, $i \in E$ as rows in a parity-check matrix of C, such that for each $i \in E$, $\mathbf{x}_{i,i} = 1$ and $\mathbf{x}_{i,j} = 0$ for $j \notin R \cup \{i\}$. [4]*

Lemma 1 says, that the cooperative locality of a code can be found by looking at the rows of parity-check matrices of C. Since all parity-check matrices of a code can be found from the row space of one single parity-check matrix, Lemma 1 can be simplified.

Lemma 2. *Let C be a linear $[n, k, d]$-code. The set $R \subseteq \{1, 2, \dots, n\}$ is a cooperative repair set for the nonempty set $E \subseteq \{1, 2, \dots, n\}$ with $|E| < d$ disjoint from R if and only if there are $|E|$ independent words $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,n})$, $i \in E$ in the row space of a parity-check matrix of C, such that for each $i \in E$, $\mathbf{x}_{i,i} = 1$ and $\mathbf{x}_{i,j} = 0$ for $j \notin R \cup \{i\}$.*

Proof. Let H be a parity-check matrix of C. Then a matrix H' of the same size as H is a parity-check matrix of C if and only if H' has the same row space as H. This means that all parity-check matrices of C have $n - k$ independent words as rows, and that all independent sets of $n - k$ words in the row space of H construct a parity-check matrix of C, with these words as rows. Let R be a cooperative repair set of E. Lemma 1 says, that there are $|E|$ words $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,n})$, $i \in E$ as rows in a parity-check matrix of C, such that for each $i \in E$, $\mathbf{x}_{i,i} = 1$ and $\mathbf{x}_{i,j} = 0$ for $j \notin R \cup \{i\}$. Notice that $\{\mathbf{x}_i \mid i \in E\}$ is an independent set of words. Since the row spaces of all parity check matrices of C are equal, $\{\mathbf{x}_i \mid i \in E\} \subseteq \text{Row}(H)$.

Now let $E \subseteq \{1, 2, \dots, n\}$ with $|E|$ independent words $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,n})$, $i \in E$ in the row space of a parity-check matrix H of C, such that for each $i \in E$, $\mathbf{x}_{i,i} = 1$ and $\mathbf{x}_{i,j} = 0$ for $j \notin R \cup \{i\}$.
The Singleton Bound says that $d \leq n - k + 1$ [2]. $d \in \mathbb{Z}$ and $|E| < d$, so $|E| \leq d - 1$. Therefore $|E| \leq d - 1 \leq n - k$.
So $\{\mathbf{x}_i \mid i \in E\}$ is an independent set with $|\{\mathbf{x}_i \mid i \in E\}| \leq n - k$ words. We can extend the set $\{\mathbf{x}_i \mid i \in E\}$, by defining a set $P \subseteq \text{Row}(H)$ of $n - k - |\{\mathbf{x}_i \mid i \in E\}|$ independent words, such that $\{\mathbf{x}_i \mid i \in E\} \cup P$ is a set of $n - k$ independent words in $\text{Row}(H)$.
Then $\{\mathbf{x}_i \mid i \in E\} \cup P$ spans $\text{Row}(H)$, so C has a parity-check matrix with $\{\mathbf{x}_i \mid i \in E\} \cup P$ as rows. With Lemma 1, follows that R is a cooperative repair set for E. □

With Lemma 2, the cooperative locality of the three codes can be determined.

Example 15. *(6,3)-Repetition code*
In Example 12, a parity-check matrix for C_1 was found:

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The non-zero words in the row space of H_1 are:

$$\begin{aligned} \mathbf{h_1} &= (100100) \\ \mathbf{h_2} &= (010010) \\ \mathbf{h_3} &= (001001) \\ \mathbf{h_4} = \mathbf{h_1} + \mathbf{h_2} &= (110110) \\ \mathbf{h_5} = \mathbf{h_1} + \mathbf{h_3} &= (101101) \\ \mathbf{h_6} = \mathbf{h_2} + \mathbf{h_3} &= (011011) \\ \mathbf{h_7} = \mathbf{h_1} + \mathbf{h_2} + \mathbf{h_3} &= (111111) \end{aligned}$$

Let $E = \{3\}$.

According to Lemma 2, if we find a $\mathbf{x}_3 = (x_{3,1}, x_{3,2}, \dots, x_{3,6})$ in this row space of H_1, such that $x_{3,3} = 1$ and choose $R \subseteq \{1, 2, \dots, 6\} \setminus \{3\}$, such that $R = \{j \mid x_{3,j} = 1\}$, then R is a cooperative repair set for E. There are four different words in the row space of H with their third element equal to 1, these are $\mathbf{h}_3$, $\mathbf{h}_5$, $\mathbf{h}_6$, and $\mathbf{h}_7$. Each one of these constructs a cooperative repair set for $E = \{3\}$, containing the positions of the other elements equal to 1 in that word. We find:

$$\begin{aligned} R_3 &= \{6\} \\ R_5 &= \{1, 4, 6\} \\ R_4 &= \{2, 5, 6\} \\ R_5 &= \{1, 2, 4, 5, 6\} \end{aligned}$$

We have found four different cooperative repair sets for $E - \{3\}$, with different sizes. The smallest cooperative repair set for $E = \{3\}$ is R_3, which has size 1.
If we repeat this process for all six sets E of size one, we can determine the $(r, 1)$-cooperative locality of C_1. Notice that, since every column of H_1 has weight ≥ 1, we can find such a word $\mathbf{x}_i$ and thus a cooperative repair set for all E of size 1. Finding these sets can be a very time consuming process, especially if the code becomes bigger.

Observe that since $\mathbf{h}_1$, $\mathbf{h}_2$, $\mathbf{h}_3$ have weight 2 and every column of H has weight ≥ 1. It follows that for all sets E of size 1, a cooperative repair set of size 1 can be found. So C_1 has $(r = 1, e = 1)$-cooperative locality.

Example 16. *(5,4)-Parity code*
In Example 13, a parity-check matrix for C_2 was found:

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The only non-zero word in the row space of H_2, is $\mathbf{h_1} = (11111)$. Choose an $i \in \{1, 2, 3, 4, 5\}$ and let $E = \{i\}$.

According to Lemma 2, if we find a $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,5})$ in this row space of H_2, such that $x_{i,i} = 1$ and choose $R \subseteq \{1, 2, \dots, 5\} \setminus \{i\}$, such that $R = \{j \mid x_{i,j} = 1\}$, then R is a cooperative repair set for E. h_1 is the only non-zero word in the row space of H_2, so there is one cooperative repair set for E possible: $R_i = \{1, 2, \dots, 5\} \setminus \{i\}$. Notice that $|R_i| = 4$. i was chosen randomly, so C_2 has $(r = 4, e = 1)$-cooperative locality.

Example 17. *(7,4)-Hamming Code*
In Example 14, a parity-check matrix for C_3 was found:

$$H_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The non-zero words in the row space of H_1 are:

$$\begin{aligned}
\mathbf{h_1} &= (1101100)\\
\mathbf{h_2} &= (1011010)\\
\mathbf{h_3} &= (0111001)\\
\mathbf{h_4} = \mathbf{h_1} + \mathbf{h_2} &= (0110110)\\
\mathbf{h_5} = \mathbf{h_1} + \mathbf{h_3} &= (1010101)\\
\mathbf{h_6} = \mathbf{h_2} + \mathbf{h_3} &= (1100011)\\
\mathbf{h_7} = \mathbf{h_1} + \mathbf{h_2} + \mathbf{h_3} &= (0001111)
\end{aligned}$$

Choose $i \in \{1, 2, \dots, 7\}$ and let $E = \{i\}$.

According to Lemma 2, if we find a $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \dots, x_{i,7})$ in this row space of H_3, such that $x_{i,i} = 1$ and choose $R \subseteq \{1, 2, \dots, 7\} \backslash \{i\}$, such that $R = \{j \mid x_{i,j} = 1\}$, then R is a cooperative repair set for $E = \{i\}$. Notice that all non-zero words in the row space of H_3 have weight 4 and every column of H_3 has weight ≥ 1. Therefore, for all $i \in \{1, 2, \dots, 7\}$, we can find a cooperative repair set R for $E = \{i\}$ with $|R| = 3$. So C_3 has $(r = 3, e = 1)$-cooperative locality.

Let $E = \{3, 4\}$. According to Lemma 2, if we find $\mathbf{x}_3 = (x_{3,1}, x_{3,2}, \dots, x_{3,7})$ and $\mathbf{x}_4 = (x_{4,1}, x_{4,2}, \dots, x_{4,7}) \neq \mathbf{x}_3$ in the row space of H, such that $x_{3,3} = x_{4,4} = 1$ and $x_{3,4} = x_{4,3} = 0$, and choose $R \subseteq \{1, 2, \dots, 7\} \backslash \{3, 4\}$, such that $R = \{j \mid x_{3,j} = 1 \text{ or } x_{4,j} = 1\}$, then R is a cooperative repair set for $E = \{3, 4\}$. There are two words in the row space of H with their third element equal to 1 and their fourth element equal to 0, $\mathbf{h}_4$ and $\mathbf{h}_5$. There are also two words with their third element equal to 0 and their fourth element equal to 1, these words are $\mathbf{h}_1$ and $\mathbf{h}_7$. Every combination of these words constructs a cooperative repair set for $E = \{3, 4\}$, containing the positions of the other elements equal to 1 in those words. We find:

$$\begin{aligned}
R_{4,1} &= \{1, 2, 5, 6\}\\
R_{4,7} &= \{2, 5, 6, 7\}\\
R_{5,1} &= \{1, 2, 5, 7\}\\
R_{5,7} &= \{1, 5, 6, 7\}
\end{aligned}$$

We have found four different cooperative repair sets for $E\{3, 4\}$, with $|R_{4,1}| = |R_{4,7}| = |R_{5,1}| = |R_{5,7}| = 4$. If we repeat this process for all sets E of size two, we can determine the $(r, e = 2)$-cooperative locality of C_3. This is again a time consuming process.

Observe that all columns of H_3 are different and have weight ≥ 1. Therefore, for all $i_1, i_2 \in \{1, 2, \dots, 7\}$ with $i_1 \neq i_2$, we can find a $\mathbf{x}_{i_1}$ and $\mathbf{x}_{i_2}$ in the row space of H_3, such that $x_{i_1,i_1} = x_{i_2,i_2} = 1$ and $x_{i_1,i_2} = x_{i_2,i_1} = 0$. So for all $i_1, i_2 \in \{1, 2, \dots, 7\}$ with $i_1 \neq i_2$, a cooperative repair set for $E = \{i_1, i_2\}$ exists.

Notice that for every pair of non-zero words $\mathbf{x}_{i_1}, \mathbf{x}_{i_2}$ in the row space of H_3, there is exactly one position j, such that $\mathbf{x}_{i_1,j} = \mathbf{x}_{i_2,j} = 0$. This means that, for all $i_1, i_2 \in \{1, 2, \dots, 7\}$ with $i_1 \neq i_2$, a cooperative repair set R for $E = \{i_1, i_2\}$ must have $|R| = 4$.

So C_3 has $(r = 4, e = 2)$-cooperative locality.

2

Research

This chapter is dedicated to finding the cooperative locality of shortened Hamming codes. In section 2.1 we will define Hamming codes. Section 2.2 explains how a code can be shortened, and what a shortened Hamming code looks like. In section 2.3, the cooperative locality of Hamming codes and shortened Hamming codes will be determined.

2.1. Hamming Codes

In examples 3, 6, 11 and 14, the (7,4)-Hamming code is discussed; this is one example of a Hamming code. Hamming codes form a class of codes, invented by Richard Hamming. For each $m \geq 2$, there is a linear $[2^m - 1, 2^m - 1 - m, 3]$-code called a $(2^m - 1, 2^m - 1 - m)$-Hamming code.

Definition 8. The $Ham(2, m)$ code is a linear $[2^m - 1, 2^m - 1 - m, 3]$-code, generated by the $(2^m - 1 - m \times 2^m - 1)$ generator matrix $G = \left[I_{2^m-1-m} \mid A\right]$, where A is a $(2^m - 1 - m \times m)$ matrix, with all words in $(F_2)^m$ with weight ≥ 2 as rows.

Remark. A parity-check matrix $H : (m \times 2^m - 1)$ of $Ham(2, m)$ is: $H = \left[A^T \mid I_m\right]$. Notice that H contains all non-zero words in $(F_2)^m$ as columns. In fact, all parity-check matrices of $Ham(2, m)$, contain all non-zero words in $(F_2)^m$ as columns.

Example 18. $Ham(2, 2)$ is a $[3, 1, 3]$-code with the following generator matrix and parity-check matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Example 19. $Ham(2, 3)$ is the $(7, 4)$-Hamming code.

2.2. Shortened Hamming Codes

There are multiple possible modifications that alter a code; this report will only discuss shortening codes.

Definition 9. A $[n, k, d]$-code can be shortened by deleting a data server from the encoding process. The resulting code is a $[n - 1, k - 1, d]$-code.

Remark. This is equivalent to deleting a row and it's corresponding data column from the generator matrix, and to deleting a column from the parity-check matrix of the code.

Example 20. We shorten the $Ham(2, 3)$ code C_3. This code has generator matrix:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

To shorten the code, first we delete the second row. Then we get the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

The corresponding data column is the second column, notice it contains only zero's. If we delete this column we get the generator matrix of our shortened code C_3':

$$G_3' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Notice that C_3' is a $[6,3,3]$-code. G_3' is in standard form, so a parity-check matrix can easily be found:

$$H_3' = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Notice that H_3' could have been constructed from the parity-check matrix of C_3 (see example 14), by removing the second column.

Lemma 3. *A s times shortened $Ham(2,m)$ code C is a $[2^m-1-s, 2^m-1-m-s, 3]$ code, with a $((2^m-1-m-s)\times(2^m-1-s))$ generator matrix $G = [I_{2^m-1-m-s} \mid A]$, where A is a $((2^m-1-m-s)\times m)$ matrix, with all but s different words in $(F_2)^m$ with weight ≥ 2 as rows.*
C has a $(m \times (2^m-1-s))$ parity-check matrix $H = [A'^T \mid I_m]$.

Proof. This follows from Definition 8, applying shortening as defined in Definition 9 s times. □

2.3. Cooperative Locality

In Example 17, we found that the $Ham(2,3)$ code has $(r=3, e=1)$-cooperative locality and $(r=4, e=2)$-cooperative locality. In this section, the cooperative locality of Hamming codes and shortened Hamming codes will be researched. First some useful definitions and lemmas are given. In subsection 2.3.1 the cooperative localities of unshortened Hamming codes will be determined. Subsection 2.3.2 will discuss the 1-cooperative locality of shortened Hamming codes, and subsection 2.3.3 the 2-cooperative locality of these codes.

Lemma 4. *Let A be a $(b \times c)$ binary matrix with independent rows and non-zero columns. Pick $s \leq c$ different columns $\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_s}$. If these columns form an independent set, then for all possible words $\mathbf{k} = (k_1, k_2, \ldots, k_s)$ in $(F_2)^s$, there are 2^{b-s} different words $\mathbf{x} = (x_1, x_2, \ldots, x_c)$ in Row(A) with $x_{i_1} = k_1, x_{i_2} = k_2, \ldots, x_{i_s} = k_s$.*

Proof. The rows of A are independent, so $|\text{Row}(A)| = 2^b$. Take $s=1$, and pick a column $\mathbf{i_1}$ of A. Note that $\mathbf{i_1}$ is nonzero. Then exactly half of the words $\mathbf{x} = (x_1, x_2, \ldots, x_c)$ in Row(A) have $x_{i_1} = 0$ (so the other half has $x_{i_1} = 1$). This means there are 2^{b-1} words $\mathbf{x}$ in Row(A), with $x_{i_1} = 1$ and 2^{b-1} words $\mathbf{x}$ in Row(A), with $x_{i_1} = 0$. So the Lemma is true for $s=1$.
Pick $t \leq c-1$ different columns $i_1, i_2, \ldots, i_t$, such that these columns form an independent set. Assume that for all possible words $\mathbf{k} = (k_1, k_2, \ldots, k_t)$ in $(F_2)^t$, there are 2^{b-t} different words $\mathbf{x} = (x_1, x_2, \ldots, x_c)$ in Row(A) with $x_{i_1} = k_1$, $x_{i_2} = k_2, \ldots, x_{i_t} = k_t$. Assume that a column $j \neq \{i_1, i_2, \ldots, i_t\}$ exists, such that the set of all columns $i_1, i_2, \ldots, i_t, j$ is independent. Pick a $\mathbf{k} \in (F_2)^t$. Since the set of columns $i_1, i_2, \ldots, i_t, j$ is independent, exactly half of the words $\mathbf{x} = (x_1, x_2, \ldots, x_c)$ in Row(A) with $x_{i_1} = k_1$, $x_{i_2} = k_2, \ldots, x_{i_t} = k_t$ have $x_p = 0$ (so the other half has $x_p = 1$). So for $\mathbf{k}' = (k_1, k_2, \ldots, k_t, l) \in (F_2)^{t+1}$ and $l \in \{0,1\}$, there are $2^{b-t}/2 = 2^{b-(t+1)}$ different words $\mathbf{x} = (x_1, x_2, \ldots, x_c)$ in Row(A) with $x_{i_1} = k_1$, $x_{i_2} = k_2, \ldots, x_{i_t} = k_t$, $x_p = l$. Since $\mathbf{k}$ was chosen randomly, this is true for all $\mathbf{k}' = (k_1, k_2, \ldots, k_{t+1}) \in (F_2)^{t+1}$. With induction follows that Lemma 4 is true for all $s \leq c$. □

Lemma 4, is a useful tool in finding the $\mathbf{x}_i$'s for Lemma 2 in the row space of a parity-check matrix of a code. In Example 21 the consequences of Lemma 4 are investigated for a parity-check matrix of the $Ham(2,3)$ code.

Example 21.
We take

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

H is a parity check matrix of the $Ham(2,3)$ code. We pick 2 different columns: $i_1 = 1$ and $i_2 = 2$. Since two different words in $(F_2)^m$ are always independent, the set S formed by these two columns is independent:

$$S = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Then Lemma 4 says that for all words $\mathbf{k} = (k_1, k_2)$ in $(F_2)^2$, there are $2^{3-2} = 2$ different words $\mathbf{x} = (x_1, x_2, \dots, x_7)$ in Row(A) with $x_1 = k_1$ and $x_2 = k_2$.
The row space of H contains the following words:

$$\begin{aligned} \mathbf{x}_0 &= (0000000) \\ \mathbf{x}_1 &= (1101100) \\ \mathbf{x}_2 &= (1011010) \\ \mathbf{x}_3 &= (0111001) \\ \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{x}_2 &= (0110110) \\ \mathbf{x}_5 = \mathbf{x}_1 + \mathbf{x}_3 &= (1010101) \\ \mathbf{x}_6 = \mathbf{x}_2 + \mathbf{x}_2 &= (1100011) \\ \mathbf{x}_7 = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 &= (0001111) \end{aligned}$$

The four different words $\mathbf{k} = (k_1, k_2)$ in $(F_2)^2$ are:

$$\begin{aligned} \mathbf{k}_1 &= (00) \\ \mathbf{k}_2 &= (01) \\ \mathbf{k}_3 &= (10) \\ \mathbf{k}_4 &= (11) \end{aligned}$$

Notice that the row space of H has precisely two rows $\mathbf{x}_j$ with $x_{j,1} = k_{1,1} = 0$ and $x_{j,2} = k_{1,2} = 0$, these are $\mathbf{x}_0$ and $\mathbf{x}_7$. In fact, for all $\mathbf{k}$'s, there are two such rows, which is precisely what Lemma 4 says.

Definition 10. Let $\mathbf{a}$ and $\mathbf{b}$ be words in $(F_2)^n$. Then $Z(\mathbf{a}, \mathbf{b}) = \{i \mid a_i = 0 \wedge b_i = 0\} \subseteq \{0, 1, \dots, n\}$.

Lemma 5. *Let $\mathbf{a}$ and $\mathbf{b}$ be words in $(F_2)^n$. Write $wt(\mathbf{a}) = \alpha, wt(\mathbf{b}) = \beta$ and $wt(\mathbf{a} + \mathbf{b}) = \gamma$. Then $|Z(\mathbf{a}, \mathbf{b})| = n - \frac{\alpha+\beta+\gamma}{2}$.*

Proof. Define $A = \{i \mid a_i = 1 \wedge b_i = 1\} \subseteq \{1, 2, \dots, n\}$. For all i, if $(a + b)_i = 1$, then either $a_i = 1$ and $b_i = 0$ or $a_i = 0$ and $b_i = 1$. If $i \in A$, then $(a + b)_i = 0$. From these observations the following formula can be derived: $\alpha + \beta = \gamma + 2 \cdot |A|$. So:

$$|A| = \frac{\alpha + \beta - \gamma}{2}.$$

We know that $|Z(\mathbf{a}, \mathbf{b})| = n - \gamma - |A|$, so:

$$|Z(\mathbf{a}, \mathbf{b})| = n - \gamma - \frac{\alpha + \beta - \gamma}{2} = n - \frac{\alpha + \beta + \gamma}{2}.$$

. □

Example 22. Let $\mathbf{a} = (0, 1, 1, 1, 0, 0, 0, 0, 1)$ and $\mathbf{a} = (1, 1, 1, 0, 1, 0, 0, 1, 0)$. Then $Z(\mathbf{a}, \mathbf{b}) = \{6, 7\}$. We know that $\mathbf{a} + \mathbf{b} = (1, 0, 0, 1, 1, 0, 0, 1, 1)$. So $wt(\mathbf{a}) = 4$, $wt(\mathbf{b}) = 5$ and $wt(\mathbf{a} + \mathbf{b}) = 5$. Lemma 5 says:

$$|Z(\mathbf{a}, \mathbf{b})| = 9 - \frac{4 + 5 + 5}{2} = 2.$$

Lemma 5 can be used as a tool to determine the size of a repair set for two erasures.

2.3.1. Hamming Codes

Theorem 6. *The $Ham(2,m)$ code has $(r = 2^{m-1} - 1, e = 1)$-cooperative locality.*

Proof. $Ham(2,m)$ is a $[2^m - 1, 2^m - 1 - m, 3]$ code, with a parity-check matrix H with as columns all the $2^m - 1$ non-zero words in $(F_2)^m$. Since the columns of H are all $2^m - 1$ non-zero words in $(F_2)^m$, the rows of H all have weight 2^{m-1}.

Pick a $i \in \{1, 2, \dots, 2^m - 1\}$ and let $E = \{i\}$. Pick a row $\mathbf{x} = (x_1, x_2, \dots, x_{2^m-1})$ of H, such that $x_i = 1$. Such an $\mathbf{x}$ exists, since all columns of H are non-zero. Notice that $wt(\mathbf{x}) = 2^{m-1}$. Let $R = \{j \mid x_j = 1\} \subseteq \{1, 2, \dots, 2^m - 1\} \setminus \{i\}$. From Lemma 1 follows that R is a cooperative repair set for E. $wt(\mathbf{x}) = 2^{m-1}$ and $x_i = 1$, so $|R| = 2^{m-1} - 1$.

For an arbitrary E of size 1 a cooperative repair set R can be found with $|R| = 2^{m-1} - 1$. So $Ham(2,m)$ has $(r = 2^{m-1} - 1, e = 1)$-cooperative locality. □

Theorem 7. *The $Ham(2,m)$ code has $(r = 3 \cdot 2^{m-2} - 2, e = 2)$-cooperative locality.*

Proof. $Ham(2,m)$ is a $[2^m - 1, 2^m - 1 - m, 3]$ code, with a parity-check matrix H with as columns all the $2^m - 1$ non-zero words in $(F_2)^m$.

Pick $i_1, i_2 \in \{1, 2, \dots, 2^m - 1\}$ and let $E = \{i_1, i_2\}$. Choose two different rows $\mathbf{x}_{i_1} = (x_{i_1,1}, x_{i_1,2}, \dots, x_{i_1,2^m-1})$ and $\mathbf{x}_{i_2} = (x_{i_2,1}, x_{i_2,2}, \dots, x_{i_2,2^m-1})$ in $\text{Row}(H)$, such that $x_{i_1,i_1} = x_{i_2,i_2} = 1$ and $x_{i_1,i_2} = x_{i_2,i_1} = 0$. These exist, since every column of H is different and nonzero. All non-zero words in $\text{Row}(H)$ have weight 2^{m-1}, so $wt(\mathbf{x}_{i_1}) = wt(\mathbf{x}_{i_2}) = wt(\mathbf{x}_{i_1} + \mathbf{x}_{i_2}) = 2^{m-1}$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \dots, 2^m - 2\} \setminus E$. Lemma 2 says that R is a cooperative repair set for E. Notice that $|R| = 2^m - 1 - |Z(\mathbf{x}_{i_1}, \mathbf{x}_{i_2})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x}_{i_1}, \mathbf{x}_{i_2})| = 2^m - 1 - \frac{2^{m-1} + 2^{m-1} + 2^{m-1}}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2$. So $Ham(2,m)$ has $(r = 3 \cdot 2^{m-2} - 2, e = 2)$-cooperative locality. □

Theorem 8. *The $Ham(2,m)$ code does not have $(r = 2^{m-1} - 2, e = 1)$-cooperative locality.*

Proof. $Ham(2,m)$ is a $[2^m - 1, 2^m - 1 - m, 3]$ code, with a parity-check matrix H with as columns all the $2^m - 1$ non-zero words in $(F_2)^m$. All words in the row space of H have weight 2^{m-1}, so from Lemma 2 follows that every repair set R for E with $|E| = 1$ has $|R| = 2^{m-1} - 1$. So $Ham(2,m)$ does not have $(r = 2^{m-1} - 2, e = 1)$-cooperative locality. □

Theorem 9. *The $Ham(2,m)$ code does not have $e \cdot 2^{m-2} - 3, e = 2)$-cooperative locality.*

Proof. $Ham(2,m)$ is a $[2^m - 1, 2^m - 1 - m, 3]$ code, with a parity-check matrix H with as columns all the $2^m - 1$ non-zero words in $(F_2)^m$. All words in the row space of H have weight 2^{m-1}, so with Lemma 4 we find that for every pair $\mathbf{x}, \mathbf{y} \in Row(H)$, $|Z(\mathbf{x}, \mathbf{y})| = 2^m - 1 - 3 \cdot 2^{m-2}$. From Lemma 2 follows that every repair set R for E with $|E| = 2$ has $|R| = 2^m - 1 - (2^m - 1 - 3 \cdot 2^{m-2}) - 2 = 3 \cdot 2^{m-2} - 2$. So $Ham(2,m)$ does not have $(r = 3 \cdot 2^{m-2} - 3, e = 1)$-cooperative locality. □

From Theorem 6 and 8 can be concluded that the smallest r for which $Ham(2,m)$ has $(r, e = 1)$-cooperative locality is $r = 2^{m-1} - 1$. From Theorem 7 and 9 can be concluded that the smallest r for which $Ham(2,m)$ has $(r, e = 2)$-cooperative locality is $r = 3 \cdot 2^{m-2} - 2$. We find that for Hamming codes, if one server gets erased, roughly half of the servers need to be accessed to repair said server. If two servers get erased, roughly three quarters of the servers need to be accessed.

2.3.2. Shortened Hamming Codes with One Erasure

Theorem 10. *Let $m \geq 3$. A one times shortened Ham(2,m) code has $(r = 2^{m-1} - 2, e = 1)$-cooperative locality.*

Proof. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $p \in \{1, 2, \dots, 2^m - 1\}$. Let H be a parity-check matrix of a $[2^m - 2, 2^m - 2 - m, 3]$ shortened Hamming code C, obtained from H' by removing the p^{th} column. Choose $i \in \{1, 2, \dots, 2^m - 2\}$ and let $E = \{i\}$.

The i^{th} column of H is also a column in H', say the j^{th} column of H', and is not equal to the p^{th} column of H', since every column of H' is different. Therefore the set of these two columns is independent.

Lemma 4 says that for all possible words $\mathbf{k} = (k_1, k_2)$ in $(F_2)^2$, there are 2^{m-2} different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_j = k_1$ and $x'_p = k_2$. Since $(1,1) \in (F_2)^2$, there are $2^{m-2} \geq 1$ different words $\mathbf{x}'$ in Row(H') with $x'_j = 1$ and $x'_p = 1$.

Choose one such $\mathbf{x}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$. $\mathbf{x}'$ constructs a cooperative repair set for E in the following way:

Let $\mathbf{x}$ be the word in Row(H), constructed from $\mathbf{x}'$ by removing the p^{th} element. Let $R = \{j \mid x_j = 1\} \subseteq \{1, 2, \dots, 2^m - 2\} \backslash E$. With Lemma 2 follows that R is a cooperative repair set for E. Since $wt(\mathbf{x}) = 2^{m-1} - 1$, $|R| = 2^{m-1} - 2$, so C has $(r = 2^{m-1} - 2, e = 1)$-cooperative locality. □

Theorem 11. *Let $m \geq 3$. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $2 \leq s \leq m$ different $p_1, p_2, \dots, p_s \in \{1, 2, \dots, 2^m - 1\}$. Call the p_1^{th}, p_2^{th}, $\dots$, p_s^{th} columns of H' respectively $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Let H be a parity-check matrix of a $[2^m - 1 - s, 2^m - 1 - m - s, 3]$ shortened Hamming code C, obtained from H' by removing said columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Then if $\{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ form an independent set, C has $(r = 2^{m-1} - s, e = 1)$-cooperative locality.*

Proof. Assume $\{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ is an independent set. Choose a $i \in \{1, 2, \dots, 2^m - 1 - s\}$ and let $E = \{i\}$. The i^{th} column of H is also a column of H', say the j^{th} column of H'. Call this column $\mathbf{j}$. Notice that $\mathbf{j} \notin \{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$, since all columns of H' are different. Let $S = \{\mathbf{j}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$. We consider the cases.
1.) S is an independent set.
2.) S is a dependent set.

1.) Assume S is an independent set. Notice that this is only possible if $s \leq m-1$. $(1, 1, \dots, 1) \in (F_2)^{s+1}$, from Lemma 4 follows that there are $2^{m-(s+1)} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_j = 1$, and $x'_{p_t} = 1$ for all $t \in \{1, 2, \dots, s\}$. Choose one such $\mathbf{x}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$. $\mathbf{x}'$ constructs a repair set for E in the following way: Let $\mathbf{x}$ be the word in Row(H), constructed from $\mathbf{x}'$ by removing the p_1^{th}, p_2^{th},$\dots$, p_s^{th} elements. Then $wt(\mathbf{x}) = 2^{m-1} - s$, since the removed elements are all ones. Let $R = \{k \mid x_k = 1\} \subseteq \{1, 2, \dots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. We know that $|R| = wt(\mathbf{x}) - 1 = 2^{m-1} - s - 1$.

2.) Assume S is a dependent set. Then $\mathbf{j} = c_{p_1}\mathbf{p_1} + c_{p_2}\mathbf{p_2} + \dots + c_{p_s}\mathbf{p_s}$. Choose one $t \in \{1, 2, \dots, s\}$ with $c_{p_t} = 1$. Then $\mathbf{p_t} = c_{p_1}\mathbf{p_1} + c_{p_2}\mathbf{p_2} + \dots + 0 \cdot \mathbf{p_t} + \dots + c_{p_s}\mathbf{p_s} + \mathbf{j}$. Notice that $S = \{\mathbf{j}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\} \setminus \{\mathbf{p_t}\}$ is an independent set.
$(1, 1, \dots, 1) \in (F_2)^s$, from Lemma 4 follows that there are $2^{m-s} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_j = 1$, and $x'_{p_k} = 1$ for all $k \in \{1, 2, \dots, s\} \setminus \{t\}$.
Choose one such $\mathbf{x}'$. Notice that $x'_{p_t} = 0$ or $x'_{p_t} = 1$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$. $\mathbf{x}'$ constructs a repair set for E in the following way:
Let $\mathbf{x}$ be the word in Row(H), constructed from $\mathbf{x}'$ by removing the p_1^{th}, p_2^{th},$\dots$, p_s^{th} elements. Then $wt(\mathbf{x}) = 2^{m-1} - s$ or $wt(\mathbf{x}) = 2^{m-1} - (s-1)$, depending on the value of x'_{p_t}. Let $R = \{k \mid x_k = 1\} \subseteq \{1, 2, \dots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. We know that $|R| = wt(\mathbf{x}) - 1 = 2^{m-1} - s - 1$ or $|R| = 2^{m-1} - s$. So $|R| \leq 2^{m-1} - s$
In both cases we find a cooperative repair set for E with $R \leq 2^{m-1} - s$, so C has $(r = 2^{m-1} - s, e = 1)$-cooperative locality. □

Theorem 12. *Let $m \geq 3$. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $2 \leq s < 2^m - 1 - m$ different $p_1, p_2, \dots, p_s \in \{1, 2, \dots, 2^m - 1\}$. Call the p_1^{th}, p_2^{th}, $\dots$, p_s^{th} columns of H' respectively $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Let H be a parity-check matrix of a $[2^m - 1 - s, 2^m - 1 - m - s, 3]$ shortened Hamming code C, obtained from H' by removing said columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Then C does not have $(r = 2^{m-1} - s - 1, e = 1)$-cooperative locality.*

Proof. Let $\mathbf{y} = \mathbf{p_1} + \mathbf{p_2}$. Then $\mathbf{y}$ is a column of H', say the y^{th} column.
Consider two options.
1.) $\mathbf{y} \in \{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$, so $\mathbf{y} = \mathbf{p_t}$ for some $t \in \{1, \dots, s\}$.
2.) $\mathbf{y} \notin \{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$.

1.) Choose $i \in \{1, 2, \dots, 2^m - 1 - s\}$ and let $E = \{i\}$. The i^{th} column of H is also a column of H', say the j^{th} column. Choose a $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_j = 1$. Notice that since $\mathbf{y} = \mathbf{p_1} + \mathbf{p_2}$, $x'_y = x'_{p_1} + x'_{p_2}$. So x'_y, x'_{p_1} and x'_{p_2} can not all be ones. Let $\mathbf{x}$ be the word in Row(H),

constructed from $\mathbf{x}'$ by removing the $p_1^{\text{th}}, p_2^{\text{th}}, \ldots, p_s^{\text{th}}$ elements. Notice that then $wt(\mathbf{x}) \geq 2^{m-1} - (s-1)$. Let $R = \{k \mid x_k = 1\} \subseteq \{1, 2, \ldots, 2^m - 1 - s\} \setminus E$, the cooperative repair set constructed from $\mathbf{x}$. Then $|R| \geq 2^{m-1} - (s-1) - 1 = 2^{m-1} - s$. So for all $i \in \{1, 2, \ldots, 2^m - 1 - s\}$, all cooperative repair sets R for $E = \{i\}$ have $|R| \geq 2^{m-1} - s$.

2.) The columns of H' are all nonzero words in $(F_2)^m$, so $\mathbf{y}$ is a column of H', and since $\mathbf{y} \notin \{\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_s}\}$, also a column of H. Choose $i \in \{1, 2, \ldots, 2^m - 1 - s\}$, such that the i^{th} column of H is $\mathbf{y}$, and let $E = \{i\}$. The i^{th} column of H is also a column of H', say the j^{th} column. $\mathbf{y} = \mathbf{p_1} + \mathbf{p_2}$, so for any $\mathbf{x}' \in \text{Row}(H')$, if $x'_j = 1$, then either $x'_{p_1} = 0$ or $x'_{p_2} = 0$. Every cooperative repair set for $E = \{i\}$ is constructed from one of these $\mathbf{x}'$. Choose one such $\mathbf{x}'$. Let $\mathbf{x}$ be the word in $\text{Row}(H)$, constructed from $\mathbf{x}'$ by removing the $p_1^{\text{th}}, p_2^{\text{th}}, \ldots, p_s^{\text{th}}$ elements. Notice that then $wt(\mathbf{x}) \geq 2^{m-1} - (s-1)$. Let $R = \{k \mid x_k = 1\} \subseteq \{1, 2, \ldots, 2^m - 1 - s\} \setminus E$, from Lemma 2 follows that this is a cooperative repair set for E. Then $|R| \geq 2^{m-1} - (s-1) - 1 = 2^{m-1} - s$. For this specific i, all cooperative repair sets R have $|R| \geq 2^{m-1} - s$.

In both cases we can find a $i \in \{1, 2, \ldots, 2^m - 1 - s\}$, such that there is no cooperative repair set R for $E = \{i\}$ with $|R| < 2^{m-1} - s$. So C does not have $(r = 2^{m-1} - s - 1, e = 1)$-cooperative locality. □

Theorem 13. *Let $m \geq 3$. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $2 \leq s \leq m + 1$ different $p_1, p_2, \ldots, p_s \in \{1, 2, \ldots, 2^m - 1\}$. Call the $p_1^{th}, p_2^{th}, \ldots, p_s^{th}$ columns of H' respectively $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_s}$. Let H be a parity-check matrix of a $[2^m - 1 - s, 2^m - 1 - m - s, 3]$ shortened Hamming code C, obtained from H' by removing said columns $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_s}$. Let k be the biggest even number in $\{1, 2, \ldots s - 1\}$. Then if $\{\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_{s-1}}\}$ form an independent set, and $\mathbf{p_s} = \mathbf{p_1} + \mathbf{p_2} + \cdots + \mathbf{p_k}$, C has $(r = 2^{m-1} - s, e = 1)$-cooperative locality.*

Proof. Assume $\{\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_{s-1}}\}$ is an independent set, and $\mathbf{p_s} = \mathbf{p_1} + \mathbf{p_2} + \ldots, \mathbf{p_k}$. Choose a $i \in \{1, 2, \ldots, 2^m - 1 - s\}$ and let $E = \{i\}$. The i^{th} column of H is also a column of H', say the j^{th} column of H'. Call this column $\mathbf{j}$. Notice that $\mathbf{j} \notin \{\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_s}\}$, since all columns of H' are different. Consider the set $S = \{\mathbf{j}, \mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_{s-1}}\}$. There are two different cases.

1.) S is an independent set.

2.) S is a dependent set.

1.) Assume S is an independent set. Notice that this is only possible if $s \leq m - 1$. $(1, 1, \ldots, 1) \in (F_2)^s$, from Lemma 4 follows that there are $2^{m-s} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_{2^m-1})$ in $\text{Row}(H')$ with $x'_j = 1$, and $x'_{p_t} = 1$ for all $t \in \{1, 2, \ldots, s - 1\}$. Choose one such $\mathbf{x}'$. All words in $\text{Row}(H')$ have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$.
$\mathbf{x}'$ constructs a repair set for E in the following way:

Let $\mathbf{x}$ be the word in $\text{Row}(H)$, constructed from $\mathbf{x}'$ by removing the $p_1^{\text{th}}, p_2^{\text{th}}, \ldots, p_s^{\text{th}}$ elements. Then $wt(\mathbf{x}) \leq 2^{m-1} - (s-1)$, since $x'_{p_t} = 1$ for $t \in \{1, 2, \ldots, s-1\}$. Let $R = \{k \mid x_k = 1\} \subseteq \{1, 2, \ldots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. We know that $|R| \leq wt(\mathbf{x}) - 1 = 2^{m-1} - s$.

2.) Assume S is a dependent set. Then $\mathbf{j} = c_{p_1}\mathbf{p_1} + c_{p_2}\mathbf{p_2} + \cdots + c_{p_{s-1}}\mathbf{p_{s-1}}$. Choose one $t \in \{1, 2, \ldots, k\}$ with $c_{p_t} = 1$. Then $\mathbf{p_t} = c_{p_1}\mathbf{p_1} + c_{p_2}\mathbf{p_2} + \cdots + 0 \cdot \mathbf{p_t} + \cdots + c_{p_{s-1}}\mathbf{p_{s-1}} + \mathbf{j}$. Notice that $S = \{\mathbf{j}, \mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_{s-1}}\} \setminus \{\mathbf{p_t}\}$ is an independent set. $(1, 1, \ldots, 1) \in (F_2)^{s-1}$, from Lemma 4 follows that there are $2^{m-(s-1)} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_{2^m-1})$ in $\text{Row}(H')$ with $x'_j = 1$, and $x'_{p_h} = 1$ for all $h \in \{1, 2, \ldots, s - 1\} \setminus \{t\}$.

Choose one such $\mathbf{x}'$. Notice that $x'_{p_t} = 0$ or $x'_{p_t} = 1$. If $x'p_t = 0$, since $\mathbf{p_s} = \mathbf{p_1} + \mathbf{p_2} + \cdots + \mathbf{p_k}$, $t \leq k$, and k is even, $x'p_s = 1$. If $x'p_t = 1$, then $x'p_s = 0$. All words in $\text{Row}(H')$ have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$. $\mathbf{x}'$ constructs a repair set for E in the following way:

Let $\mathbf{x}$ be the word in $\text{Row}(H)$, constructed from $\mathbf{x}'$ by removing the $p_1^{\text{th}}, p_2^{\text{th}}, \ldots, p_s^{\text{th}}$ elements. Then $wt(\mathbf{x}) = 2^{m-1} - (s-1)$. Let $R = \{h \mid x_h = 1\} \subseteq \{1, 2, \ldots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. We know that $|R| = wt(\mathbf{x}) - 1 = 2^{m-1} - (s-1) - 1 = 2^{m-1} - s$.

In both cases we can find a cooperative repair set R for $E = \{i\}$ with $|R| = 2^{m-1} - s$. So C has $(r = 2^{m-1} - s, e = 1)$-cooperative locality. □

With Theorem 10 we found that if $s = 1$, C has $(r = 2^{m-1} - 2, e = 1)$-cooperative locality. With Theorem 12, we found that for all $m > 2$ and $2 \leq s < 2^m - 1 - m$ the s times shortened $Ham(2,m)$ code C does not have $(r, e = 1)$-cooperative locality with $r = 2^{m-1} - s - 1$.

With Theorem 11 we found that if the s deleted columns from the parity-check matrix of the non-shortened $Ham(2,m)$ code form an independent set, C has $(r = 2^{m-1} - s, e = 1)$-cooperative locality. The s deleted columns can only form an independent set if $s \leq m$. Theorem 13 says that if $s - 1$ of the s deleted columns form an independent set, and the last deleted column is a specific linear combination of the first s columns, C also has $(r = 2^{m-1} - s, e = 1)$-cooperative locality. This is only possible if $s \leq m + 1$.

So if $s \leq m+1$, and a $Ham(2,m)$ code is shortened s times in a specific way, the smallest r for which this code has $(r, e = 1)$-cooperative locality is $r = 2^{m-1} - s$. For $m, s \leq 9$, Table A.1 in Appendix A shows the smallest r, for which a s times shortened $Ham(2,m)$ code can have $(r, e = 1)$-cooperative locality. Notice that if a code with (r, e)-cooperative locality is shortened, the locality can only decrease.

2.3.3. Shortened Hamming Codes with Two Erasures

Theorem 14. *Let $m \geq 3$. A one time shortened Ham(2,m) code has $(r = 3 \cdot 2^{m-2} - 3, e = 2)$-cooperative locality.*

Proof. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $p \in \{1, 2, \ldots, 2^m - 1\}$. Let H be a parity-check matrix of a $[2^m - 2, 2^m - 2 - m, 3]$ shortened Hamming code C, obtained from H' by removing the p^{th} column. Call this column $\mathbf{p}$ Choose two different $i_1, i_2 \in \{1, 2, \ldots, 2^m - 2\}$ and let $E = \{i_1, i_2\}$.

The i_1^{th} and i_2^{th} columns of H are also columns in H', say the j_1^{th} and j_2^{th} column of H. Call these columns $\mathbf{j_1}$ and $\mathbf{j_2}$. Notice that $\mathbf{j_1}$ and $\mathbf{j_2}$ are not equal to $\mathbf{p}$, since every column of H' is different. Consider the set $S = \{\mathbf{j_1}, \mathbf{j_2}, \mathbf{p}\}$, containing these three columns. There are two different cases.

1.) S is an independent set.

2.) S is a dependent set.

1.) Assume S is an independent set. $(1,0,1) \in (F_2)^3$, from Lemma 4 follows that there are $2^{m-3} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$, and $x'_p = 1$. Also, since $(0,1,1) \in (F_2)^3$, there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \ldots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$, and $y'_p = 1$.

2.) If S is an dependent set, since it contains 3 elements, $\mathbf{j_1} + \mathbf{j_2} + \mathbf{p} = 0$. The set $\{\mathbf{j_1}, \mathbf{j_2}\}$ is independent, and $(1,0) \in (F_2)^2$, so with Lemma 4 we find that there are $2^{m-2} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$ and $x'_{j_2} = 0$. Notice that then $x'_p = 1$. Also, $(0,1) \in (F_2)^2$, so with Lemma 4 we find that there are $2^{m-2} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \ldots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 1$ and $y'_{j_2} = 0$. Notice that then $y'_p = 1$.

In both cases we find that there exist a $\mathbf{x}'$ and $\mathbf{y}'$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$, $x'_p = 1$, $y'_{j_1} = 0$, $y'_{j_2} = 1$, and $y'_p = 1$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$ and $wt(\mathbf{y}') = 2^{m-1}$. Notice that also $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 1$ and $wt(\mathbf{y}) = 2^{m-1} - 1$, since the removed elements are ones. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1}$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \ldots, 2^m - 2\} \setminus E$. Lemma 2 says that R is a cooperative repair set for E. Notice that $|R| = 2^m - 2 - |Z(\mathbf{x}, \mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 2 - \frac{2^{m-1} - 1 + 2^{m-1} - 1 + 2^{m-1}}{2} = 2^m - 2 - 3 \cdot 2^{m-2} + 1.$$

So $|R| = 2^m - 2 - \left(2^m - 2 - 3 \cdot 2^{m-2} + 1\right) - 2 = 3 \cdot 2^{m-2} - 3$.

So a one time shortened $Ham(2,m)$ code has $(r = 3 \cdot 2^{m-2} - 3, e = 2)$-cooperative locality. □

Theorem 15. *Let $m \geq 3$. A two times shortened $Ham(2,m)$ code has $(r = 3 \cdot 2^{m-2} - 4, e = 2)$-cooperative locality.*

Proof. Let H' be a parity-check matrix of a $[2^m-1, 2^m-1-m, 3]$ Hamming code C'. Choose two different $p_1, p_2 \in \{1, 2, \dots, 2^m-1\}$. Let H be a parity-check matrix of a $[2^m-3, 2^m-3-m, 3]$ shortened Hamming code C, obtained from H' by removing the p_1^{th} and p_2^{th} columns. Choose two different $i_1, i_2 \in \{1, 2, \dots, 2^m-3\}$ and let $E = \{i_1, i_2\}$.

The i_1^{th} and i_2^{th} columns of H are also columns in H', say the j_1^{th} and j_2^{th} column of H', and are not equal to the p_1^{th} or p_2^{th} column of H', since every column of H' is different. Call the p_1^{th}, p_2^{th}, j_1^{th} and j_2^{th} columns of H' respectively $\mathbf{p_1}$, $\mathbf{p_2}$, $\mathbf{j_1}$ and $\mathbf{j_2}$. Consider the set $S = \{\mathbf{p_1}, \mathbf{p_2}, \mathbf{j_1}, \mathbf{j_2}\}$ containing these four columns. There are two different cases.

1.) S is an independent set.

2.) S is a dependent set.

1.) Assume S is an independent set. $(1,0,1,1) \in (F_2)^4$, from Lemma 4 follows that there are $2^{m-4} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$, $x'_{p_1} = 1$ and $x'_{p_2} = 1$. Also, since $(0,1,1,1) \in (F_2)^4$, there are $2^{m-4} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$, $y'_{p_1} = 1$ and $y'_{p_2} = 1$.

Choose one $\mathbf{x}'$ and one $\mathbf{y}'$, such that $x'_{j_1} = 1$, $x'_{j_2} = 0$, $x'_{p_1} = 1$, $x'_{p_2} = 1$, $y'_{j_1} = 0$, $y'_{j_2} = 1$, $y'_{p_1} = 1$ and $y'_{p_2} = 1$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$ and $wt(\mathbf{y}') = 2^{m-1}$. Notice that also $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th} and p_2^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 2$ and $wt(\mathbf{y}) = 2^{m-1} - 2$, since the removed elements are ones. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1}$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \dots, 2^m-3\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 3 - |Z(\mathbf{x}, \mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - \frac{2^{m-1} - 2 + 2^{m-1} - 2 + 2^{m-1}}{2} = 2^m - 3 - 3 \cdot 2^{m-2} + 2.$$

So $|R| = 2^m - 3 - \left(2^m - 3 - 3 \cdot 2^{m-2} + 2\right) - 2 = 3 \cdot 2^{m-2} - 4$.

2.) S is a dependent set with 4 elements. Then either $\{\mathbf{p_1}, \mathbf{j_1}, \mathbf{j_2}\}$, or $\{\mathbf{p_2}, \mathbf{j_1}, \mathbf{j_2}\}$ is an independent set. Assume without loss of generality that $\{\mathbf{p_1}, \mathbf{j_1}, \mathbf{j_2}\}$ is an independent set. Then $\mathbf{p_2}$ is a linear combination of $\mathbf{p_1}, \mathbf{j_1}$ and $\mathbf{j_2}$, write $\mathbf{p_2} = c_{p_1}\mathbf{p_1} + c_{j_1}\mathbf{j_1} + c_{j_2}\mathbf{j_2}$. We consider the four options:

a) $c_{p_1} = 0$, $c_{j_1} = 1$, $c_{j_2} = 1$

b) $c_{p_1} = 1$, $c_{j_1} = 0$, $c_{j_2} = 1$

c) $c_{p_1} = 1$, $c_{j_1} = 1$, $c_{j_2} = 0$

d) $c_{p_1} = 1$, $c_{j_1} = 1$, $c_{j_2} = 1$

a) $(1,0,1) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$ and $x'_{p_1} = 1$. Notice that then $x'_{p_2} = 1$. Also, $(0,1,1) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$ and $y'_{p_1} = 1$. Notice that then $y'_{p_2} = 1$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$, $wt(\mathbf{y}') = 2^{m-1}$ and $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th} and p_2^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 2$ and $wt(\mathbf{y}) = 2^{m-1} - 2$, since the removed elements are ones. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1}$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - \frac{2^{m-1} - 2 + 2^{m-1} - 2 + 2^{m-1}}{2} = 2^m - 3 - 3 \cdot 2^{m-2} + 2.$$

b) $(1,0,1) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$ and $x'_{p_1} = 1$. Notice that then $x'_{p_2} = 1$. Also, $(0,1,0) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$ and $y'_{p_1} = 0$. Notice that then $y'_{p_2} = 1$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$, $wt(\mathbf{y}') = 2^{m-1}$ and $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th} and p_2^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 2$ and $wt(\mathbf{y}) = 2^{m-1} - 1$. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1} - 1$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - \frac{2^{m-1} - 2 + 2^{m-1} - 1 + 2^{m-1} - 1}{2} = 2^m - 3 - 3 \cdot 2^{m-2} + 2.$$

c) $(1,0,0) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$ and $x'_{p_1} = 0$. Notice that then $x'_{p_2} = 1$. Also, $(0,1,1) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$ and $y'_{p_1} = 1$. Notice that then $y'_{p_2} = 1$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$, $wt(\mathbf{y}') = 2^{m-1}$ and $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th} and p_2^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 1$ and $wt(\mathbf{y}) = 2^{m-1} - 2$. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1} - 1$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - \frac{2^{m-1} - 1 + 2^{m-1} - 2 + 2^{m-1} - 1}{2} = 2^m - 3 - 3 \cdot 2^{m-2} + 2.$$

d) $(1,0,0) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$ and $x'_{p_1} = 0$. Notice that then $x'_{p_2} = 1$. Also, $(0,1,1) \in (F_2)^3$, so with Lemma 4 we find that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$ and $y'_{p_1} = 1$. Notice that then $y'_{p_2} = 0$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$, $wt(\mathbf{y}') = 2^{m-1}$ and $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th} and p_2^{th} element. Then $wt(\mathbf{x}) = 2^{m-1} - 1$ and $wt(\mathbf{y}) = 2^{m-1} - 1$. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1} - 2$. Lemma 5 says:

$$|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - \frac{2^{m-1} - 1 + 2^{m-1} - 1 + 2^{m-1} - 2}{2} = 2^m - 3 - 3 \cdot 2^{m-2} + 2.$$

In all four cases we can find a $\mathbf{x}$ and $\mathbf{y}$ in Row(H) with $x_{i_1} = 1$, $x_{i_2} = 0$, $y_{i_1} = 0$, $y_{i_2} = 1$ and $|Z(\mathbf{x}, \mathbf{y})| = 2^m - 3 - 3 \cdot 2^{m-2} + 2$. These $\mathbf{x}$ and $\mathbf{y}$ construct a cooperative repair set for E in the following way:

Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \dots, 2^m - 3\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 3 - |Z(\mathbf{x}, \mathbf{y})| - 2 = 2^m - 3 - \left(2^m - 3 - 3 \cdot 2^{m-2} + 2\right) - 2 = 3 \cdot 2^{m-2} - 4$.

In both cases 1.) and 2.) we can find a cooperative repair set for E with $|R| = 3 \cdot 2^{m-2} - 4$, so a two times shortened $Ham(2, m)$ code has $(r = 3 \cdot 2^{m-2} - 4, e = 2)$-cooperative locality. □

Theorem 16. *Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $3 \leq s \leq m$ different $p_1, p_2, \dots, p_s \in \{1, 2, \dots, 2^m - 1\}$. Call the p_1^{th}, p_2^{th}, $\dots$, p_s^{th} columns of H' respectively $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Let H be a parity-check matrix of a $[2^m - 3, 2^m - 3 - m, 3]$ shortened Hamming code C, obtained from H' by removing said columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Then if $\{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ in an independent set, C has $(r = 3 \cdot 2^{m-2} - 2 - s, e = 2)$-cooperative locality.*

Proof. Assume $\{\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ is an independent set. Choose two different $i_1, i_2 \in \{1, 2, \dots, 2^m - 1 - s\}$ and let $E = \{i_1, i_2\}$. The i_1^{th} and i_2^{th} columns of H are also columns in H', say the j_1^{th} and j_2^{th} column of H'. Call the j_1^{th} and j_2^{th} columns of H' respectively $\mathbf{j_1}$ and $\mathbf{j_2}$. Notice that $\mathbf{j_1}$ and $\mathbf{j_2}$ and are not equal to any of the columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$, since every column of H' is different. Consider the following cases:

1. $\{\mathbf{j_1}, \mathbf{j_2}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ is an independent set.
2. $\{\mathbf{j_1}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ is an independent set and $\{\mathbf{j_2}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ is a dependent set.
3. $\{\mathbf{j_1}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ and $\{\mathbf{j_2}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ are both dependent sets.
   (a) $\mathbf{j_1}$ and $\mathbf{j_2}$ are both linear combinations of an even amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$.
   (b) $\mathbf{j_1}$ and $\mathbf{j_2}$ are both linear combinations of an uneven amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$.

(c) $\mathbf{j_1}$ is a linear combination of an uneven amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$ and $\mathbf{j_2}$ is a linear combination of an even amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$.

Notice that without loss of generality, these cases describe all possible cases.

1.) Notice that $\{\mathbf{j_1}, \mathbf{j_2}, \mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}\}$ can only be an independent set, if $s \leq m-2$. $(1,0,1,1,1,\dots,1) \in (F_2)^{s+2}$, from Lemma 4 follows that there are $2^{m-(s+2)} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$, $x'_{j_2} = 0$, and $x'_{p_t} = 1$ for all $t \in \{1,2,\dots,s\}$. Also, since $(0,1,1,1,1,\dots,1) \in (F_2)^{s+2}$, there are $2^{m-(s+2)} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$, and $y'_{p_t} = 1$ for all $t \in \{1,2,\dots,s\}$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = 2^{m-1}$ and $wt(\mathbf{y}') = 2^{m-1}$. Notice that also $wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Then $wt(\mathbf{x}) = 2^{m-1} - s$ and $wt(\mathbf{y}) = 2^{m-1} - s$, since the removed elements are ones. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1}$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1,2,\dots,2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 1 - s - |Z(\mathbf{x},\mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{2^{m-1} - s + 2^{m-1} - s + 2^{m-1}}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.

2.) $(1,1,1,1,1,\dots,1) \in (F_2)^{s+1}$, so from Lemma 4 follows that there are $2^{m-(s+1)} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{j_1} = 1$ and $x'_{p_t} = 1$ for all $t \in \{1,2,\dots,s\}$. Also, since $(0,1) \in (F_2)^2$, and $\{\mathbf{j_1}, \mathbf{j_2}\}$ is an independent set, there are $2^{m-2} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$ and $y'_{j_2} = 1$.

Choose one such $\mathbf{x}'$ and one such $\mathbf{y}'$. Define $l = |\{p_t \mid y'_{p_t} = 1 \wedge 1 \leq t \leq s\}|$ to be the amount of columns p_t, where $y'_{p_t} = 1$, for $t \in \{1,2,\dots,s\}$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = wt(\mathbf{y}') = wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Then $wt(\mathbf{x}) = 2^{m-1} - s$ and $wt(\mathbf{y}) = 2^{m-1} - l$. Notice that $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1} - s + l$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1,2,\dots,2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 1 - s - |Z(\mathbf{x},\mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{2^{m-1} - s + 2^{m-1} - l + 2^{m-1} - s + l}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.

3.) In this case $\mathbf{j_1} = b_1\mathbf{p_1} + b_2\mathbf{p_2} + \cdots + b_s\mathbf{p_s}$, and $\mathbf{j_2} = c_1\mathbf{p_1} + c_2\mathbf{p_2} + \cdots + c_s\mathbf{p_s}$ with $c_t, b_t \in \{0,1\}$, for all $t \in \{1,2,\dots,s\}$. $\mathbf{j_1} \neq \mathbf{j_2}$, so there is at least one $t_1 \in \{1,2,\dots,s\}$, such that $b_{t_1} \neq c_{t_1}$.

a) Assume without loss of generality that $b_{t_1} = 1$ and $c_{t_1} = 0$. $(0,1,\dots,1) \in (F_2)^s$, so from Lemma 4 follows that there are $2^{m-s} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{p_{t_1}} = 0$ and $x'_{p_t} = 1$ for all $t \in \{1,2,\dots,s\} \setminus \{t_1\}$. Pick one such $\mathbf{x}'$. Notice that $x'_{j_1} = 1$ and $x'j_2 = 0$.

$\mathbf{j_1} + \mathbf{j_2} + \mathbf{p_{t_1}} \neq \mathbf{0}$, since $\mathbf{j_1}$ and $\mathbf{j_2}$ are both linear combinations of an even amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Therefore $\{\mathbf{j_1}, \mathbf{j_2}, \mathbf{p_{t_1}}\}$ is an independent set, and $(0,1,1) \in (F_2)^3$, so from Lemma 4 follows that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$, $y'_{j_2} = 1$ and $y'_{p_{t_1}} = 1$. Pick one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = wt(\mathbf{y}') = wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Let $l = |\{1 \leq k \leq s \mid y'_{p_k} = 1 \wedge k \neq t_1\}|$. Then $wt(\mathbf{x}) = 2^{m-1} - (s-1)$, $wt(\mathbf{y}) = 2^{m-1} - (1+l)$, $wt(\mathbf{x} + \mathbf{y}) = 2^{m-1} - (s-l)$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1,2,\dots,2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 1 - s - |Z(\mathbf{x},\mathbf{y})| - 2$. Lemma 5

says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{2^{m-1} - (s-1) + 2^{m-1} - (1+l) + 2^{m-1} - (s-l)}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.

b) Assume without loss of generality that $b_{t_1} = 1$ and $c_{t_1} = 0$. $(0, 1, \dots, 1) \in (F_2)^s$, so from Lemma 4 follows that there are $2^{m-s} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{p_{t_1}} = 0$ and $x'_{p_t} = 1$ for all $t \in \{1, 2, \dots, s\} \setminus \{t_1\}$. Pick one such $\mathbf{x}'$. Notice that $x'_{j_1} = 0$ and $x'j_2 = 1$.

$\mathbf{j_1} + \mathbf{j_2} + \mathbf{p_{t_1}} \neq \mathbf{0}$, since $\mathbf{j_1}$ and $\mathbf{j_2}$ are both linear combinations of an uneven amount of columns $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_s}$. Therefore $\{\mathbf{j_1}, \mathbf{j_2}, \mathbf{p_{t_1}}\}$ is an independent set, and $(1, 0, 1) \in (F_2)^3$, so from Lemma 4 follows that there are $2^{m-3} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 1$, $y'_{j_2} = 0$ and $y'_{p_{t_1}} = 1$. Pick one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = wt(\mathbf{y}') = wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Let $l = |\{1 \leq k \leq s \mid y'_{p_k} = 1 \wedge k \neq t_1\}|$. Then $wt(\mathbf{x}) = 2^{m-1} - (s-1)$, $wt(\mathbf{y}) = 2^{m-1} - (1+l)$, $wt(\mathbf{x}+\mathbf{y}) = 2^{m-1} - (s-l)$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \dots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 1 - s - |Z(\mathbf{x},\mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{2^{m-1} - (s-1) + 2^{m-1} - (1+l) + 2^{m-1} - (s-l)}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.

c) $(1, 1, \dots, 1) \in (F_2)^s$, so from Lemma 4 follows that there are $2^{m-s)} \geq 1$ different words $\mathbf{x}' = (x'_1, x'_2, \dots, x'_{2^m-1})$ in Row(H') with $x'_{p_t} = 1$ for all $t \in \{1, 2, \dots, s\}$. Pick one such $\mathbf{x}'$. Notice that $x'_{j_1} = 1$ and $x'j_2 = 0$.

$(0, 1) \in (F_2)^2$, and $\{\mathbf{j_1}, \mathbf{j_2}\}$ is an independent set, so from Lemma 4 follows that there are $2^{m-2} \geq 1$ different words $\mathbf{y}' = (y'_1, y'_2, \dots, y'_{2^m-1})$ in Row(H') with $y'_{j_1} = 0$ and $y'_{j_2} = 1$. Pick one such $\mathbf{y}'$. All words in Row(H') have Hamming weight equal to 2^{m-1}, so $wt(\mathbf{x}') = wt(\mathbf{y}') = wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. $\mathbf{x}'$ and $\mathbf{y}'$ construct a cooperative repair set for E in the following way:

Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Let $l = |\{1 \leq k \leq s \mid y'_{p_k} = 1\}|$. Then $wt(\mathbf{x}) = 2^{m-1} - s$, $wt(\mathbf{y}) = 2^{m-1} - l)$, $wt(\mathbf{x}+\mathbf{y}) = 2^{m-1} - (s-l)$. Let $R = \{j \mid x_j = 1 \vee y_j = 1\} \subseteq \{1, 2, \dots, 2^m - 1 - s\} \setminus E$. From Lemma 2 follows that R is a cooperative repair set for E. Observe that $|R| = 2^m - 1 - s - |Z(\mathbf{x},\mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{2^{m-1} - s + 2^{m-1} - l + 2^{m-1} - (s-l)}{2} = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| = 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.

In all cases we can find a cooperative repair set R for E with $|R| = 3 \cdot 2^{m-2} - 2 - s$, so C has $(r = 3 \cdot 2^{m-2} - 2 - s, e = 2)$-cooperative locality. □

Theorem 17. *Let $m \geq 3$. Let H' be a parity-check matrix of a $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code C'. Choose $1 \leq s \leq 2^m - 2 - m$ different $p_1, p_2, \dots, p_s \in \{1, 2, \dots, 2^m - 1\}$. Call the p_1^{th}, p_2^{th}, …, p_s^{th} columns of H' respectively $\mathbf{p_1}$, $\mathbf{p_2}$, …, $\mathbf{p_s}$. Let H be a parity-check matrix of a $[2^m - 1 - s, 2^m - 1 - m - s, 3]$ shortened Hamming code C, obtained from H' by removing said columns $\mathbf{p_1}$, $\mathbf{p_2}$, …, $\mathbf{p_s}$. Then C does not have $(r = 3 \cdot 2^{m-2} - s - 3, e = 2)$-cooperative locality.*

Proof. Pick any $\mathbf{x}', \mathbf{y}' \in$ Row(H'), then $wt(\mathbf{x}') = wt(\mathbf{y}') = wt(\mathbf{x}' + \mathbf{y}') = 2^{m-1}$. Let $\mathbf{x}$ and $\mathbf{y}$ be the words in Row(H) constructed from $\mathbf{x}'$ and $\mathbf{y}'$ by removing the p_1^{th}, p_2^{th},…, p_s^{th} elements. Then $wt(\mathbf{x}) + wt(\mathbf{y}) + wt(\mathbf{x}+\mathbf{y}) \geq 3 \cdot 2^{m-1} - 2s$. Any repair set R generated by $\mathbf{x}$ and $\mathbf{y}$ has $|R| = 2^m - 1 - s - (\mathbf{x},\mathbf{y})| - 2$. Lemma 5 says:

$$|Z(\mathbf{x},\mathbf{y})| = 2^m - 1 - s - \frac{wt(\mathbf{x}) + wt(\mathbf{y}) + wt(\mathbf{x}+\mathbf{x})}{2} \leq 2^m - 1 - s - \frac{3}{2}(2^{m-1} - 2s) = 2^m - 1 - 3 \cdot 2^{m-2}.$$

So $|R| \geq 2^m - 1 - s - \left(2^m - 1 - 3 \cdot 2^{m-2}\right) - 2 = 3 \cdot 2^{m-2} - 2 - s$.
So C does not have $(r = 3 \cdot 2^{m-1} - s - 3, e = 2)$-cooperative locality. □

With Theorem 17, we found that for all $m > 2$ and $3 \leq s < 2^m - 1 - m$ the s times shortened $Ham(2, m)$ code C does not have $(r, e = 2)$-cooperative locality with $r = 3 \cdot 2^{m-2} - 3 - s$.

With Theorem 16 we found that if the s deleted columns of the parity-check matrix of the non-shortened $Ham(2, m)$ code form an independent set, C has $(r = 3 \cdot 2^{m-1} - 2 - s, e = 2)$-cooperative locality. The s deleted columns can only form an independent set if $s \leq m$. With Theorem 14 and 15 we found that this equality also holds for $s = 1$ and $s = 2$.

So if $s \leq m$, and a $Ham(2, m)$ code is shortened s times in a specific way, the smallest r for which this code can have $(r, e = 2)$-cooperative locality is $r = 3 \cdot 2^{m-2} - 2 - s$. For $m, s \leq 9$, Table A.2 in Appendix A shows the smallest r, for which a s times shortened $Ham(2, m)$ code can have $(r, e = 2)$-cooperative locality. Notice that if a code with (r, e)-cooperative locality is shortened, the locality can only decrease.

2.4. Performance Comparison

Table B.1 in Appendix B, shows the information rate of some shortened Hamming codes. This rate is equal to the amount of data servers divided by the total amount of servers. Every time a code is shortened, a data server is deleted, so both the numerator and the denominator decrease by one. Since the numerator is smaller than the denominator, the rate decreases. This means that every time a code is shortened, more storage is needed to store the same amount of data. Notice that when m increases, the information rate of shortened $Ham(2, m)$ codes increases. This means less storage is needed to store the same amount of data.

Table B.2 in Appendix B, shows the repairability divided by the total amount of servers, of some shortened Hamming codes. This fraction is a measure for the reliability of the code. If a code uses more servers, it is more likely to suffer from erasures. Every time a code is shortened, a server is deleted, so this fraction will increase. This means that every time a code is shortened, storage becomes more reliable. Notice that when m increases, this fraction for shortened $Ham(2, m)$ also codes increases. This means that storage becomes less reliable.

Table A.1 and A.2 in Appendix A, show the cooperative localities of some shortened Hamming codes, a measure of the time it takes to repair erasures. Notice that a more shortened code means a lower cooperative locality. This means that shortening a code more often, results in faster repair speeds. Notice that when m increases, the cooperative locality for shortened $Ham(2, m)$ codes increases. This means erasure are repaired more slowly.

If m increases, with a (shortened) $Ham(2, m)$ code, less storage is needed, but the servers are also less reliable and it will take more time to repair erasures. If such a code is shortened more often, more storage is needed, but the servers are also more reliable and erasures can be repaired faster. Which code is the best, depends on which key factor(s) are most important for the situation.

Notice that if a $Ham(2, m)$ code is shortened $s = 2^{m-1} - 1$ times, the resulting code is a $[2^m - 1 - s, 2^m - 1 - m - s, 3] = [2^m - 1 - (2^{m-1} - 1), 2^m - 1 - m - (2^{m-1} - 1), 3] = [2^{m-1}, 2^{m-1} - 1 - (m - 1), 3]$-code. A $Ham(2, m - 1)$ code is a $[2^{m-1} - 1, 2^{m-1} - 1 - (m - 1), 3]$-code. The $Ham(2, m - 1)$ is similar to the shortened $Ham(2, m)$ code, but has an extra parity server. In terms of reliability and information rate, the $Ham(2, m - 1)$ code is better then the shortened $Ham(2, m)$ code. But the cooperative locality of the shortened $Ham(2, m)$ code can be lower than that of the $Ham(2, m - 1)$ code, as example 23 will show.

Example 23. A $s = 2^{4-1} - 1 = 7$ times shortened $Ham(2, 4)$ code C can have a parity-check matrix

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Notice that C is a $[8, 4, 3]$-code.
With the four rows in H, a cooperative repair set for all sets $E \subseteq \{1, 2, \ldots, 8\}$ with $|E| = 1$ can be

found. Therefore, it is easy to see that C has $(r = 2, e = 1)$-cooperative locality. A $Ham(2,3)$ code has $(r = 3, e = 1)$-cooperative locality, so in terms of cooperative locality, the shortened $Ham(2,4)$ code is better then a $Ham(2,3)$ code.

3

Conclusion and Recommendations

3.1. Conclusion

In this report, we researched the cooperative locality of shortened Hamming codes. Shortened Hamming codes can be constructed from Hamming codes, by deleting columns of its parity-check matrix. A s times shortened $Ham(2,m)$ code adds m parity servers to $2^m - m - 1 - s$ data servers, and can repair up to two simultaneous erasures.

First we found that the cooperative locality of a code can be found, by analyzing the Hamming weight of the rows of its parity-check matrices. This is equivalent to analyzing the row space of one parity-check matrix.

Then we found that the smallest r, for which a $Ham(2,m)$ code has $(r, e = 1)$-cooperative locality, is $r = 2^{m-1} - 1$. The smallest r, for which this code has $(r, e = 2)$-cooperative locality, is $r = 3 \cdot 2^{m-2} - 2$. A one time shortened Hamming code has $(r, e = 1)$-cooperative locality with as smallest $r = 2^{m-1} - 2$.

We found that the cooperative locality of a shortened Hamming codes depends on the deleted columns. If the columns of a $s \geq 2$ times shortened $Ham(2,m)$ code are independent, the smallest r, for which a shortened Hamming code has $(r, e = 1)$-cooperative locality, is $r = 2^{m-1} - s$. This is only possible, if $s \leq m$. We also discovered that for $s = m+1$, if the s deleted columns are picked in a specific way, we get the same smallest r.

If the columns of a $s \geq 1$ times shortened $Ham(2,m)$ code are independent, the smallest r, for which a shortened Hamming code has $(r, e = 2)$-cooperative locality, is $r = 3 \cdot 2^{m-2} - 2 - s$. This is only possible if $s \leq m$.

Also, for all $2 \leq s < 2^m - 1 - m - s$, we found that a s times shortened $Ham(2,m)$ code does not have $(r = 2^{m-1} - s - 1, e = 1)$ and $(r = 3 \cdot 2^{m-2} - 3 - s, e = 2)$-cooperative locality.

At last, we compared different shortened Hamming codes, in terms of information rate, reliability and repair speed. We found that for s times shortened $Ham(2,m)$ codes, a higher s results in a lower information rate, more reliability, and higher repair speed. A higher m results in a higher information rate, less reliability, and lower repair speed.

3.2. Recommendations

For a big m, a $Ham(2,m)$ code can be shortened much more often than m times. The bounds on the smallest possible cooperative locality of these many times shortened Hamming codes are not so strong. A possibility for tighter bounds can be researched.

This report only focuses on the cooperative locality of shortened Hamming codes, while leaving other very popular codes out. The cooperative locality of such codes can be researched.

Which code is best, is dependent on the situation. A way to find the best code in a certain situation can be researched.

A

Appendix

Table A.1: Smallest r, for which a s times shortened $Ham(2,m)$ code has $(r, e = 1)$-cooperative locality.

r		m						
		3	4	5	6	7	8	9
s	0	3	7	15	31	63	127	255
	1	2	6	14	30	62	126	254
	2	2	6	14	30	62	126	254
	3	1	5	13	29	61	125	253
	4		4	12	28	60	124	252
	5		3	11	27	59	123	251
	6		$2 \leq r \leq 3$	10	26	58	122	250
	7		$1 \leq r \leq 2$	$9 \leq r \leq 10$	25	57	121	249
	8		$1 \leq r \leq 2$	$8 \leq r \leq 10$	$24 \leq r \leq 25$	56	120	248
	9		$1 \leq r \leq 2$	$7 \leq r \leq 10$	$23 \leq r \leq 25$	$55 \leq r \leq 56$	119	247

Table A.2: Smallest r, for which a s times shortened $Ham(2,m)$ code has $(r, e = 2)$-cooperative locality.

r		m						
		3	4	5	6	7	8	9
s	0	4	10	22	46	94	190	382
	1	3	9	21	45	93	189	381
	2	2	8	20	44	92	188	380
	3	1	7	19	43	91	187	379
	4		6	18	42	90	186	378
	5		$5 \leq r \leq 6$	17	41	89	185	377
	6		$4 \leq r \leq 6$	$16 \leq r \leq 17$	40	88	184	376
	7		$3 \leq r \leq 6$	$15 \leq r \leq 17$	$39 \leq r \leq 40$	87	183	375
	8		$2 \leq r \leq 6$	$14 \leq r \leq 17$	$38 \leq r \leq 40$	$86 \leq r \leq 87$	182	374
	9		$1 \leq r \leq 6$	$13 \leq r \leq 17$	$37 \leq r \leq 40$	$85 \leq r \leq 87$	$181 \leq r \leq 182$	373

B

Appendix

Table B.1: Information rate of a s times shortened $Ham(2, m)$ code.

$\frac{k}{n}$		m						
		3	4	5	6	7	8	9
s	0	0,571	0,733	0,839	0,9048	0,9449	0,96863	0,98239
	1	0,5	0,714	0,833	0,9032	0,9445	0,96850	0,98235
	2	0,4	0,692	0,828	0,9016	0,944	0,96838	0,98232
	3	0,25	0,667	0,821	0,9	0,9435	0,96825	0,98228
	4		0,636	0,815	0,8983	0,9431	0,96813	0,98225
	5		0,6	0,808	0,8966	0,9426	0,968	0,98221
	6		0,556	0,8	0,8947	0,9421	0,96787	0,98218
	7		0,5	0,792	0,8929	0,9417	0,96774	0,98214
	8		0,429	0,783	0,8909	0,9412	0,96761	0,98211
	9		0,333	0,773	0,8889	0,9407	0,96748	0,98207

Table B.2: Repairability divided by total amount of servers of a s times shortened $Ham(2, m)$ code.

$\frac{e}{n} = \frac{2}{n}$		m						
		3	4	5	6	7	8	9
s	0	0,286	0,133	0,06452	0,0317	0,01575	0,00784	0,003914
	1	0,333	0,143	0,0667	0,03226	0,01587	0,00787	0,003922
	2	0,4	0,154	0,0690	0,0328	0,016	0,00791	0,003929
	3		0,167	0,0714	0,0333	0,01613	0,00794	0,003937
	4		0,182	0,0741	0,0339	0,01626	0,00797	0,003945
	5		0,2	0,0769	0,0345	0,01639	0,008	0,003953
	6		0,222	0,08	0,0351	0,01653	0,00803	0,003960
	7		0,25	0,0833	0,0357	0,01667	0,00806	0,003968
	8		0,286	0,0870	0,0364	0,01681	0,00810	0,003976
	9		0,333	0,0909	0,0370	0,01695	0,00813	0,003984

Bibliography

[1] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, *On the locality of codeword symbols,* IEEE Transactions on Information Theory **58**, 6925 (2012).

[2] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall, *Coding Theory and Crypthography: The Essentials* (Marcel Dekker, 2000) pp. 1–74.

[3] A. S. Rawat, A. Mazumdar, and S. Vishwanath, *Cooperative local repair in distributed storage,* EURASIP Journal on Advances in Signal Processing **2015**, 107 (2015).

[4] K. A. S. Abdel-Ghaffar and J. H. Weber, *Bounds for cooperative locality using generalized hamming weights,* (2017), proceedings 2017 IEEE International Symposium on Information Theory, Aachen, Germany, June 25-30, 2017.

[5] J. A. M. De Groot, *TU Delft course: Toegepaste algebra: Codes en cryptosystemen,* (2017), lecture sheets.