Efficient Error Reduction Techniques by Hamming Code In Transmission Channel

Raviraju Balappa D[1*], Gautam Kumar Rajput[2]

[1*]Research Scholar Sunrise University Alwar Rajasthan, Email: ravirajd33@gmail.Com
[2]Associate Professor, Sunrise University Alwar Rajasthan, Email:gautam.rjpt@gmail.Com
*Corresponding author

Received: 12.04.2024 Revised : 16.05.2024 Accepted: 24.05.2024

ABSTRACT
In the current information era, reliable digital communication is crucial, and this requires designing codes that can be reliably decoded over noisy transmission channels. Error-Correcting Codes (ECC) is essentially employed in a range of communication systems to detect and fix problems in a message that has been transferred, which is usually rather important. In particular, a number of decoding techniques for error reduction and correction remain difficult to implement in transmission channels. This study presents a novel approach to code generation that utilizes hamming codes for error reduction and error correction. Here, the error is checked using panty bits in hamming code (linear code), and the error position in a codeword is identified using a hamming code parity check matrix in syndrome coding. After error detection, next step is to use standard decoding with parity check matrix to reduce the error. Experimental research on alternative decoding algorithms generally indicates that these approaches improve the Hamming is the codes' ability to minimize errors above and beyond the bottom bound of essentially standard decoding that was previously established.

Keywords: Hamming code, syndrome decoding, standard decoding, hamming distance.

1. INTRODUCTION

Many of the inventions in our past would never have been as efficient without ECC [1,2]. For example, consider NASA's Mariner 9 program, whose goal was to send images back from Mars and whose error tolerance was ensured by Reed-Muller codes As an outcome, the original driving force was the necessity for error correction in communications and calculations, which was recently a difficult task [4]. A variety of communication systems employ one of the ECC to detect and fix errors in a message that has been conveyed [5]. We explore the idea of an ECC in this work. Spielman coined the name and defined for it, but he only used it to describe a technique for creating low-complexity errorreducing codes—not as a stand-alone notion [6]. These codes have been described as being similar to a form of joint-source-channel coding [7] and ECCs have a significant part to play. In this study, we are interested in assessing the best redundancy in Hamming codes, a particular kind of code that is used to correct single-bit errors. Our foremostinvolvement is to provide a lower assurance on the usualquantity of faults that remain after applying standard decoding techniques, especially when an opponent injects two errors [8]. Further, we prove that Hamming codes are capable of achieving this lower bound. However, such decoding methods are not the most efficient as far as minimizing errors is concerned [9]. We discuss several decoding techniques for Hamming codes &display that it is feasible to achieve more than the traditional lower bound of the average number of decoding errors using experimental analysis. This is especially so since Hamming codes are perfect codes, incorrect decoding will always occur if there is more than one error present [10, 11]. When assessing the success of decoded communications, it is reasonable to use the number of errors in the decoded message as the measure of success since the total number of faults is dependent on any potential error vector containing two errors [13]. Codeword is a block of bits and any linear combination of these codewords is also a codeword when modulo-2 arithmetic is used [14]. In a linear code, a generator matrix is used to encode the message (a binary vector) at the sender's end by appending it with the message. Also, the parity-check matrix which forms the basis of the null space of the code is used in the decoding process of the message at the receiver side. The number of errors that can be corrected by a code is at most $\lfloor (d - 1) / 2 \rfloor$ where d is the minimum Hamming distance between the codewords [15]. Erroneous vectors cannot be corrected when this limit is exceeded, leading to ambiguous behaviour. This drives research and development of new models aimed at minimizing the number of mistakes in the received vector during decoding. Less correction for errors has been produced

by ECC approaches such as Reeder Solomon codes, algebraic-geometric codes, as well as linear codes, which were previously developed. As a result, the suggested approach clarifies how the aforementioned Hamming code checks for errors using parity bits. It is suggested to use syndrome decoding to pinpoint the error's location. This kind of linear code is used to decode a hamming code to locate errors in a vector and reduce the error using standard decoding. The suggested model beats other current decoding strategies like least sums decoding and minimum of maxima decoding by using normal decoding of the Hamming code to reduce error in the code. The suggested techniques have the best capacity to reduce errors.

2. LITERATURE REVIEW

Pereira, F.R.F. et al., et al., 2021 [16] suggested algebraic geometry (AG) codes toward building numerous relations of QUENTA codes with Euclidean as well as Hermitian designs. The maximal entanglement is present also the quantum Singleton fault is the same as either zero or one in two of the created families. By comparing with the codes of the other families, we show that the rate of our codes is higher than the corresponding quantum Gilbert Varshamov bound. Lastly, by adopting asymptotically excellent towers of linear complementary double numbers, improved asymptotically families of QUENTA codes with minimal coupling are created. Besides, an elementary contrasted through quantum Gilbert-Varshamov bound suggests that our method can be used producing an asymptotically huge family of QUENTA codes that go above this limit.

Bordage, S. et al.'s 2020 analysis of closeness testing to codes for AG was published in [17]. A code for AG $C = C(X, P, D)$ across an algebraic curve X denotes matrix interplanetary connected toward assessments scheduled $P \subseteq X$ denotesroles in Riemann-Roch space $L_x(D)$. AG codes are a good choice for statistical proof structures, even if there are ineffective proximity tests available for them. We identify suitable requirements to build efficient Oracle Proof of Proximity (IOPP) methods designed on behalf of AG codes. The method is based on decomposition from the space of Riemann-Roch of every invariant divisor scheduled a curve inside numerous explicit Riemann-Roch spaces preceding the quotient curve. The proposed method offers enough information about AG code C such that C's proximity checking issue can be reduced to address have issue with membership for a much smaller code C.

In 2021, Bartoli, D. et al. [18] looked into the building of quantum numbers using codes of self-orthogonal algebraic geometry. Our method is based on two foundations: Certain unusual characteristics of the algebraic curves underneath, which we call Swiss curves, and the CSS construction. As it happens, a family of the most popular algebraic curves having a large number of rational points is called the Swiss curve family. Instances of this include the Abd´on-Bezerra-Quoos maximum curve, GK curves, altered GK curves, as well as castle curves. We provide applications of our technique to these curves. We expand upon a previous structure by Moyano-Fernández, Hernando, McGuire, and Monserrat.

The method for identifying faults and subsequently fixing them needs to be developed by Kumar, S. et al., (2020) [20] to provide effective communication and provide services in FSO. In this study, we have concentrated on using Reed Solomon (RS) codes to identify and fix maximum received errors done the finite Galois field (GF). The Bit Error Rate (BER), no of mistakes rectified, also Geometric Path Losses in relation to link distance for the proposed FSO system with and without the employ of RS codes are assessed. The model was created using the Modified Gamma-Gamma approach. With the maximum allowable correction of error 399 mistakes for the link distance in the sent message spanning 500m toward 5km, the geometric route sufferers have decreased from -8.76dB to -28.04dB.

Garcia-Herrero et al. [21] examined this decoding algorithm in 2020 and discovered that, in contrast to other effective solutions, it uses majority logic approaches to utilize the identical parity check matrix form without requiring calculation of Galois Field inversions, divisions, or logarithms. For the same message length, the resulting architectures allow for an increase in the Galois Field's order while maintaining comparable area and latency outcomes. Finally, By reducing the delay in decoding to two clock cycles, the lag can be improved by up to five times while sacrificing the critical route, thanks to 3-phasethe decoder's process: syndrome, magnitude estimate, as well as popular logic. The suggested decoder can achieve a minimum 44% reduction in the area when dealing with codes that have a high Galois Field order, or GF (2^8).

Tang, Y.J. et al., [22] presented two strategies in 2021 to address the shortcomings of the techniques that were previously in use. In the initial method, several finite field buildings are investigated in an effort toward additional minimizing the numeral of "1s" in matrix bit of Cauchy ground; also a novel examining technique is created toward identifying the matrices by fewest "1s." The form of parity check matrix Vandermonde matrix joined to an individuality matrix is used in the second method to construct RS

codes. This allows the inverse erasure columns multiplied by. The two suggested methods improve the encoding throughput aimed at 4-erasure-correcting RS codes over GF (28), on average, by 40% and 15% more than previous research based on the Cauchy matrix as well as Vander monde matrix by RM change, correspondingly, intended for a variety of codeword lengths. Furthermore, there is a notable improvement in the decoding throughput as well.

2.1 Research gap

In a research study employing decoding algorithms, including algebraic codes, Reeder Solomon codes, linear codes, etc., the best-case result was 1.6857 mistakes in the received message, which is extremely higher. Nevertheless, using such techniques comes with a higher processing expense since they essentially replace several searches inside of bigger sets with a matrix multiplication, which is rather significant. Moreover, it was believed that the remaining mistakes in the sent codeword were algorithms that did not provide individuality or attractiveness. As a result, the recommended approaches below provide superior error-reducing capabilities when utilizing Hamming codes.

3. PROPOSED METHODOLOGY

ERR is an essential part of systems for electronic communication. Due to improvements in computational capacity, higher-level error-correcting codes can now be used in real-world systems. This suggested method explains the usage of Hamming code for standard decoding to minimize error code as well as error detection and correction during information transfer and storage. Hammering codes are binary codes that can identify and correct single-bit errors. Syndrome decoding is a method that uses a Hamming code's parity-check matrix to identify flaws in a codeword. Reducing the code error while transferring the most information possible without using redundancy is how standard decoding is designed. The recommended strategy outperformed other decoding techniques, lowering the error from 1.765 to 1.652.

3.1 Codes, encoding and decoding

In this instance, F denotes a set of finite also think of it as an alphabet. Adjust optimistic numerals k, n with $k \le n$. Let $R \subset F^k$ as well as $D \subset F^n$ also refer to them accordingly as a source and a code. An encoding rule μ denotes a bijective mapping as of $R \text{ to } D$ also [25] rule of decoding λ denotes a set of mapping $D^{'}$ by $D \subset D'' \subset F^n$ toward D. An information transmission system is illustrated in the material below.

$$R \xrightarrow{e} D \longrightarrow D^{'} \xrightarrow{\delta} C \xrightarrow{\varepsilon^{-1}} R \qquad (1)$$

A transmitter drives the source's symbol $x \in R$ via the channel in the direction of a receiver. The receiver will receive an inaccurate symbol if an error is brought about by noise on the channel. Consequently, one interprets the sign by using an encoder x codeword inside $\omega = \varepsilon(x) \in D$. As of the received word $\omega^{'} \in D$ a decoded word is induced by a decoder $\omega^{n'} = \gamma(\omega^{'}) \in D$, At last, the recipient receives the sign $x^{n'} = \varepsilon^{-1}(\omega^{n})$. Below is the simple e.g., as

$$F = R = \{0,1\}, \quad D = \{(0,0,0),(1,1,1)\}, \quad D^{'} = F^3 \qquad (2)$$

In this scenario, let's say that 0 is sent, encoded as (0, 0, 0), and that the word that is received is (0, 0, 1). By majority vote, the decoder determines that (0, 0, 0) is sent and sends 0 to the recipient. Error-correcting codes were created with the aforementioned objective in mind.

3.2 Hamming code

It is a class of quadratic codes of error-correcting. It can be used to both detect and rectify one- and two-bit mistakes without disclosing untreated problems. Mathematically speaking, binary linear codes are a subset of Hamming codes. Aimed at every number $r \ge 2$ a codeword with a block of dimension exists $n = 2^r - 1$ as measurement of communication $k = 2^r - r - 1$. Therefore, the amount of hamming codes is the highest that can be achieved for codes with a minimum distance of three (that is, a minimum of three-bit transfers required to travel between a single message to another) and a block length $2^r - 1$.

3.2.1 Decoding of hamming codes

Syndrome decoding is a useful technique in decoding linear block codes. Here, in terms of decoding single-bit errors, namely given that subsequent semantics:

If there is a 0 or 1 error in the received word, the decoder will give back the accurate transmission communication. If the message received contains greater than 0 otherwise 1 mistake, the decoder might or might not provide the correct message (i.e., we make no guarantees) [23]. The following technique can be simply expanded to handle block codes that correct more errors and to allow machine learning (ML) decoding (i.e., send the message back associated with a codeword that has the fewest Hamming length toward the word that was received).

The main concept is to make use of the code's linearity. First, we demonstrate the method and then move through its broad aspects. Examine the Hamming code (7, 4) for which the generator matrix G is given by Equation (3). Beginning with G, the parity equations can be stated in the same way.

$$G=\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \quad (3)$$

$$P_1 = D_1 + D_2 + D_4$$
$$P_2 = D_1 + D_3 + D_4 \quad (4)$$
$$P_3 = D_2 + D_3 + D_4$$

Since arithmetic is finished F_2 to write these eqns, move $P^{'}s$ toward the similarsideways as that which is parallel to the $D^{'}s$ (In modulo-2 arithmetic, the sign of the a-and a+ is the same).

$$D_1 + D_2 + D_4 + P_1 = 0$$
$$D_1 + D_3 + D_4 + P_2 = 0 \quad (5)$$
$$D_2 + D_3 + D_4 + P_3 = 0$$

Such equations are n-k in number. Using a parity check matrix, H may state the following formulae in vector form in the following order:

$$H.\left[D_1 D_2 \ldots\ldots D_k P_1 P_2 \ldots\ldots P_{n-k}\right]^T = 0 \quad (6)$$

H is two matrices stacked horizontally, also known as concatenation: A^T, where A denotes sub-matrix of an identity matrix's coding encoder.

$$G = I_{k\times k} \| A \text{ and } I_{(n-k)\times(n-k)} \quad (7)$$

$$H = A^T \left| I_{(n-k)\times(n-k)} \right. \quad (8)$$

H denotes the quality that any legitimate c code words (signify by $1\times n$ matrix).

$$H.c^T = 0 \quad (9)$$

T

herefore, aimed at some letter get back r lacking mistakes, $H.r^T = 0$.

Let's say a term is received r consumes few mistakes in it. r can remain described as $c+e$, where c is a legitimate codeword as well as e denotes sector of mistake, denoted as $1\times n$ a matrix. Aimed at instance r,

$$H.r^T = H.(c+e)^T = 0 + H.e^T \quad (10)$$

If r consists of all zeroes and e at most one-bit mistake if there is at most one. In this instance, $n+1$ each of these numbers $H.e^T; n$ may represent precisely a single-bit mistake; additionally, these single values would represent a no-error scenario $H.e^T = 0$.These $n+1$ potential carriers as well as the specific symptoms. The syndrome associated with every error is pre-computed by syndrome decoding. Considering that the code is organized systematically, each codeword has the form

$D_1D_2.....D_kP_1P_2...P_{n-k}$. If $e=100$ after that syndrome $H.e^T$ denotes outcome once initial information bit, D_1 denotes error. Generally, speaking if an element $i\ of\ e is\ 1$ also another fundamentals are 0, the outcoming syndrome $H.e^T$ fits the scenario where bit i denotes codeword is wrong [24]. Assuming that there is only a single-bit error, we are concerned with saving the symptoms in the event that one of the initial k basics of e is 1.

If $H.r^T$ is not the only zero, and if it doesn't correspond with any saved pattern, The decryptor determines that perhaps whichever parity bit is erroneous or that there were several mistakes. Here, the received word strength only contains the initial k bits of the message. This method offers the ML decoding in the event that a parity bit is erroneous, then it might not be the best approximation when many faults are present.

Anything more intricate than simply sending the decoded message is the first k bits of the text that was received may usually be avoided because single-error correction is frequently used in situations where there is little chance of multiple-bit errors. The two chapters that come before it provides the basic techniques for syndrome decoding for solitary bit defects and produce an ML approximation of given communication in the instance where one bit or zero faults impact the codeword.

Modifying numerous mistakes: Since this decoding concept applies to the many mistake scenario, expanding this syndrome is not difficult. Let's say we want to fix every pattern of $\leq t$ errors. In this instance, pre-compute additional syndromes, which correspond to $0,1,2.....t$ little mistakes. The decoder needs to keep all of these. A total of syndromes need to be pre-computed and stored.

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+.....\binom{n}{t} \qquad (11)$$

In the event that one of these syndromes corresponds, the receiver flips those bits, giving the coded message again via its initial of k bits of the codeword. It then knows precisely which bit mistake sequence caused the syndrome. With this technique, the decoder must type $O(n^t)$ syndrome contrasts, then every contrast of this kind entailed contrasting dual $n-k$ bit-strings through every further.

An instance: To comprehend the processes involved in decoding and encoding a comprehensive instance could be helpful. Think about (7,4) Hamming code. The G code aimed at this linear block is given in eqn (7). Assuming some k=4-bit communication m, the encoder creates a $n=7-bit$ codeword, c throughen larging $m.G.(m\ is\ a\ 1\times k\ matrix, G\ is\ a\ k\times n\ matrix$ as well as c is a $1\times n$ matrix.

The parity check matrix, H aimed at this code can be acquired by using eqn (12)

$$H=\left(\begin{array}{ccc|ccc} 1&1&0&1&1&0&0\\ 1&0&1&1&0&1&0\\ 0&1&1&1&0&0&1 \end{array}\right) \qquad (12)$$

Assume c is transmitted across the television network and obtained via decoder as r. Aimed at correctness, assume c=10100001 and r=1110001 (mistake in the subsequent bit).

The decoder has pre-computed the associated syndromes for every potential single-bit mistake. (In actuality, it only wants toward pre-compute k of these, since everyone represents a mistake in the major k-bitlocations of the codeword.) Here, k = 4 signs of importance described by:

$$\begin{aligned} &H.[1000000]^T=[110]^T\\ &H.[0100000]^T=[101]^T\\ &H.[0010000]^T=[011]^T\\ &H.[0001000]^T=[111]^T \end{aligned} \qquad (13)$$

To sum up, it should come as no surprise that the syndrome aimed at single-bit mistakes in a single of the parity bits is:

$$H.[0000100]^T = [100]^T$$
$$H.[0000010]^T = [010]^T \quad (14)$$
$$H.[0000001]^T = [001]^T$$

To fix single-bit mistakes, the decoder follows these steps. Compute $c^{'} = H.r^T$ For this instance $c^{'} = [101]^T$

If $c^{'}$ is 0, after that send back the initial k bits of r by way of communication. In this instance $c^{'}$ isn't 0.

If $c^{'}$ is not0, afterward contrast $c^{'}$ through n pre-calculated syndromes, $H.e_i$, where $.e_i = [00.....1.....0]$ is a $1 \times n$ matrix by 1 in location I also 0 universally different.

If the error matrix matches what was carried out in the preceding phase e_l then there is a mistake at bit location "in the received word. Turn the bit, then put the first one back k components of r (keep in mind that we only want to carry out this check for the initial k error vectors since it is enough to merely save just one of those because only one of those may need to be flipped k syndromes of single error as well as not n.

In this occasion, a condition $H.[0100000]^T = [101]^T$ which equals $.c^{'} = H.r^T$. As a result, the interpreter performs an ML decoding of the transmitted message via flipping the extra bit & returning the first k=4 bits of r. The returned estimate of the communication in this instance is.

The initial k bits of r must be returned if there is no connection. Even while it's not always ML decoding when ma y bit errors happen, it's still a very excellent estimate if the bit error probability is low.It is unlikely that the BER of a packet composed of multiple of these coded blocks will be sufficiently reduced in this case to make full-fledged ML decoding worthwhile.

3.3 Error reducing of standard coding

Hamming code effectively by lowering the number of mistakes in the message that was received. On the other hand, there are times when a message is sent that has a growing or unceasing amount of errors in it. In this section, we will first go over our preliminary findings and offer some advice on how to choose a high-quality generator matrix. We'll after showing the matrix that was discovered is the most effective matrix aimed at creating [7; 4; 3].-Hamming code by standard decoding for every potential vector of error, as determined by the message's average amount of mistakes that were received.

3.3.1 Hamming codes with standard coding

Remember the definitions from the introduction aimed at parity-check then generator matrices. It consumes generator matrix G and also parity check matrix H, in the under neatheqn:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}; \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad (15)$$

To further grasp the typical decoding for Hamming codes, let's examine one example. Assume that the communication that has to exist is conveyed via $y = (0101)$. This communication will be decoded as $G^T \times y = [1\,0\,1\,0\,1\,0\,1]^T = x(say)$.

Let's currently imagine that a vector indicates an error. $\delta = [0\,0\,0\,1\,0\,0\,0]^T$ Is additional toward codeword x. We have, $x + \delta = [1\,0\,1\,1\,1\,0\,1]^T$.

After receiving this incorrect codeword, the location of the error can be determined by multiplying the parity check matrix. The procedure of standard decoding by [7; 4; 3]-Hamming code. We have

$H \times (x+\delta) = [1\ 0\ 0]^T$: It can be observed that column four of the parity check matrix also resulting a column matrix match. H. It is evident that this matches the codeword after that portion was reversed. $[101010]^T$,consistent with the communication (0101) , so the error has been corrected.

3.3.2 Error reduction by[7, 4, 3] Hamming codes

When there are two inaccuracies, none of the faults can be accurately corrected by the parity check matrix. Aimed at instance, within the framework of [7; 4; 3]-Hamming code, consider $\delta = [1\ 0\ 0\ 1\ 0\ 0\ 0]^T$; $x = [1\ 0\ 1\ 0\ 1\ 0\ 1]^T$ where δ denotes error vector containing mistakes in dual places (columns 1 as well as 4). Currently multiplying H by $y+\delta$ get $H \times (x+\delta)^T = [1\ 0\ 1]^T$: Thus column 5 is the freshly modified column. Once the perceived fault has been fixed, the codeword that was received becomes 0011001. This resembles a communication of (0001) since $G = [0\ 0\ 1\ 1\ 0\ 0\ 1]^T$: Consequently, although (0101) remained transmitted, (0001) remained decoded. There is a single error in the message that was received. Nevertheless, the simulated communication route contained two mistakes. This indicates that there were fewer mistakes in the decoded message than in the codeword. Now, the task is to identify a workable construction that can replicate this outcome in different scenarios.

3.3.3 Basic facts for standard decoding

Here, [7; 4; 3] utilizedHamming code that contains two newly created mistakes 24 · 7 2 = 16 · 21 = 334 code words and error vector combinations that could be used in the event that two mistakes are introduced (because each message corresponds to a single codeword).

Lemma 1: Assume that codeword by a Hamming code of every command by conventional decoding has one or more faults in it. Let q denote the parity-check matrix column (i.e., the produce of erroneous codeword also parity check matrix) that is found to remain mistaken. Q doesn't depend on the first message that needs to be referred.

This is a clear reality since $q = H \times (x+\delta) = H \times x + H \times \delta = H \times \delta$ depends on H *and* δ and not on x .

Proposition 2: It is not reliant on the communication that was sent on the quantity of mistakes in the decoded message (standard decryption).

Proof: Lemma 1 demonstrated that the incorrect column is solely based on the vector of errors. Given r denotes the message that was received, $r^{'}$ denotes transmitted code word afterward alteration also f denotes the vector that is applied to do the corrective procedure. As previously $y\ \delta$ symbolizes the source codeword being sent as well as δ denotes mistake vector that was included in message frequency. It contains $r = x+\delta$; $r^{'} = x+\delta+f$ .Currently allow $\bar{\delta} = \delta + f$.

$$r^{'} = x+\bar{\delta} \Rightarrow \bar{\delta} = r^{'} - y \qquad (16)$$

Meanwhile $\bar{\delta}$ able to articulate by way of a linear combination of dual code words, given that hamming codes are linear, it has to have a code word. A lower bound aimed at [7; 4; 3]-Hamming code via standard decoding

We succeeded in bringing the total numeral of mistakes in codeword set down to an average of 1.652 yet, these are not the essential restrictions of conventional decoding using [7; 4; 3]-Hamming code. Using the generator matrix after (1) as a starting point, we can create the subsequent producer vector by substituting the second row containing the prior two rows' modulo-2 total.

$$G = \begin{bmatrix} 1\,1\,1\,0\,0\,0\,0 \\ 0\,1\,1\,1\,1\,0\ \ 0 \\ 0\,1\,0\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,0\,1 \end{bmatrix} \qquad (17)$$

The conventional decoding of [7,4,3] hamming codes results in a median number of mistakes of 1.652 in the resulting message for all dimensions.

Lemma 2: consider a $\left[n=2^n-1,2^n-1-n,3\right]$. Use conventional coding with hamming code. The column indexas incorrect through the parity check matrix's multiplication marked by y will always match a zero on the error vector in the event that the received vector x contains two errors.

Proof: Assume that the parity check matrix multiplied by y corresponds toward 1 in the error vector aimed at the column index classified by way of inaccurate. In the event of two mistakes, the rectified codeword because the message that is completely zero will have a Hamming weight of 1. This suggests that Codeword by a Hamming weight of one exists.

Lemma 3: Let's say we wish to map a communication with a weight of2toward a weighted codeword that three. In this instance, the generator matrix that is employed to encrypt the communication must include a minimum of one row r, such that $\beta(r)\succ 4$.

Proof: Assume that the generator matrix's row weights are all three. Mapping a weight 2 communication to a weight three codeword involves calculating the modulo-2 sum of the generator matrix's two rows. Let a,b denotes one 2 generator matrix rows. Take note of that, $d(a,b)\succ 2$. Henceforth $d(a,b)=4 or\ 6$. In the two cases, no codeword of weight three is given as $a+b$.

Lemma 4:Study $\left[n,k,3\right]$ Hamming code. Let t represents rows numeral that have a Hamming weight equal to three in the generator matrix. The extremenumeral of communications with a mappable weight of two to codewords in a weight of 2 if the weights in every other row add up to 4 3 is $(k-t)\times t$.

Proof: Lemma 4 states that only when the generator matrix's two rows being added have weights of 3 and 4 can a weight-2 communication produce a weight-3 codeword. Given that the generator matrix only contains rows by a Hamming weight of 3, this arrangement is able to occur in the most $(k-t)\times t$ dissimilar behaviors.

The aforementioned lemma suggests that [7; 4; 3] Hamming code, a maximum of threeCode words weighting three can be translated to messages with a weight of two, provided a generator matrix single row has a strength of 4 while entirely the remaining rows possess a weight of 3. This leads us toward the assertion that follows.

Theorem 7: Suppose we have [7; 4; 3]-Hamming code. Let t be the collection of every distinct error vector with weight 2 as well as length 7. Assume, that t denotes the mean numeral of mistakes discovered in the decoded message at the recipient following normal decoding for all conceivable sums of each element in E divided by each element in C, modulo 2.In the event that the standard decoder is intended to minimize the Hamming code, then 1.652.

Proof: We can presume that the transmitted message is (0000) as a result of proposition 2. Lemmas 2 and 3 showed that E collapses toward seven set distinct vectors, which we will refer to as E0. To enable conventional decoding, the vectors in E0 have to be code words. The no of faults identified in the decoded message will not ever be zero because normal decoding can never entirely repair dual mistakes with a Hamming code (because only one repair is produced). This indicates that seven distinct set code words in E0 will be mapped to the 7 communications by the smallest separation from the source message by best Hamming code. The three additional code words in E0 must match communications that are two Hamming distances apart from the initial message since there are only four messages (0001, 0010, 0100, and 1000) that are at an interval of one from the message 0000. For any message that is one distance away as of 0000 toward a map toward a vector within E0, every row weight in the generator matrix needs to be three. Nevertheless, lemmas 5 and 6 demonstrate that the generator matrix needs to contain at least one row without a weight of 3 an important message that bears two has toward translate toward a vector in E0 (otherwise, the average number of remaining mistakes is (1 · 4 /7 + 3 · 3/7 = 13/7). In this instance, code words in E0 can only be translated to three messages at an interval of one and three at a distance of two from 0000. This indicates that to prevent changing, the generator matrix another row, a seventh message that is three distances away from the initial message needs to be mapped to a codeword in E0. This results in a Hamming distance average of 1 · 3/7 + 2 · 4/7 + 3 · 1/7 = 13/7 as of initial message 0000, producing identical outcomes to those shown in (3)'s generator matrix.

This theory can be extended toward greater order Hamming codes, as shown in the following subset, even though it is only applicable toward [7; 4; 3]-Hamming code by two mistakes. Finding a bound, however, becomes more difficult in the case of three mistakes added, since this permits the error vector to transform codewords into other codewords.

Extension toward overall Hamming Codes

Theorem-8: Assuming a $\left[n=2^n-1, k=2^n-1-n, d=3\right]$ Hamming code c for $n\geq 4$, also $E=\left\{\delta\in F_2^n : \beta(\delta)=21\right\}$.

Discover the least $l\in Z, 0\leq l\leq\left[1/2\right]$, such that

$$k-l+l(k-l)\geq 1/3(n/2) \quad (18)$$

Next, a lower bound on the mean (more than any code words in c also entirely errors in E) noof mistakes in a communication afterward standard decoding is $2-\frac{k-l}{1/3(n/2)}$.

To show this, we must use the equation that follows.

Lemma 5: Aimed atall $n\geq 4$, there is a $l\in Z, 0\leq l\leq\left[k/2\right]$ such that $k-l+l(k-l)\geq 1/3(n/2)$.recall that $k=2^n-n-1 \ and \ n=2^n-1$.

Proof: If k is odd pick $l=\frac{k-1}{2}$ also if k is even, select $l=\frac{k}{2}$.For $n\geq 4$,these values l gratify the claim.

Proof of theorem 8: Once more, we can presume that the entire conducted message is 0. Assume M denotes a collection of messages that correspond to weight 3 codewords. The communication vectors' average weight must be reduced N. Every communication of Hamming weight 1 in N the code words needs to be included in the generator matrix as rows. Considering that the lemma 3 $|N|=1/3(n/2>k$. It required toward map weight two otherwise additional messages onto weight three codewords. Conversely, in case the generator matrix's weight is 3 in each row, then, from lemma 4 there will be related correspondence bearing a three or higher for each of the remaining weighted code words three. So, N will include messages with weights between one and three otherwise may be higher. Lemma 4 claims that “messages by M that are classified as 1 be removed" by "removing weight 3 rows from the generator matrix and swapping them out with weight 4 code words." This will enhance equal to $l(k-l)$ novel communication of weight 2; significance up to $l(k-l)$ messages in M that have a Hamming weight of three or more will be deleted. Stated otherwise, if M still contains members with weights of three or higher, then the members of M's average Hamming weight should either decrease or remain the same when a row of weight three is substituted by a row of weight four in the generator matrix. When M is left with no members that have a Hamming weight of three or more (which it does because of lemma 9), this condition is precisely the same as the one in (4). Once N comprises only messages with weights of 1 otherwise 2, in which case the average Hamming weight of the participants in N will be $\frac{k-l+2(1/3(n/2)-k-l)}{1/3(n/2)}$.Take note of that N must contain $k-l$ hamming weight members 1 also the residual members $(1/3(n/2)-k-l \ of \ \ them)$ will weigh two pounds.. Here, it is evident that growing l over the lowest value that satisfies the requirements (18) inevitably needs to rise typically using weight as a metaphor for weight one in N shall be substituted with a weight two message. Given that the selected generator matrix will match and l that reduce members' regular weight N, it must be optimal. There are several challenges with extending Theorem 8's result to three or more faults. The main issue is that the weight of the codeword that is added to the incorrect vector during the usual decoding procedure can no longer be expected to be 3. This would necessitate revising Theorem 8's definition of the set M.

Table 1. Hamming code with various decoding techniques

Introduced no. of. Errors	Average no. of mistakes in decoded message				
	Standard Decoding	Optimized Standard decoding	Min of Sums decoding	Min of Maximum decoding	Majority Bit decoding

4	1.9581	1.8524	1.5296	1.5641	1.2958
5	2.3000	2.1562	1.8671	1.7785	1.7957
6	1.9530	1.8325	2.1539	2.0654	2.1539

A comparison of suggested and current decoding methods is provided in Table 1. Presenting no. of errors are 4, 5, and 6. The location of the fault is found via syndrome decoding, and the error is reduced by regular decoding. The suggested decoding strategies achieve reduced error in a delivered message as contrasted with alternative decoding methods already in use.

4.CONCLUSION

In conclusion, substantial progress in ECC has been made possible by hamming code. The simplest code to use when examining a signal's transmitted message error is the hamming code. It was found that using traditional decoding severely limits the error reduction capabilities of Hamming codes; this finding motivates further study into alternate decoding methods. By employing typical decoding techniques, syndrome decoding decreases the error by 1.652 and makes it easy to locate the fault employing the Hamming code of parity-check matrix. Generally, one should encompass the bound from Theorem 8 toward an arbitrary no of errors. In order to reduce errors to a greater extent while maintaining a low level of complexity, also, it is intriguing to look into recommended decoding methods in particular, which is really important.

REFERENCE

[1] I . Banafaa, M., Pepeoélu, Ö., Shayea, 1., Alhammadi, A., Shamsan, Z., Razaz, M.A., Alsagabi, M. and Al-Sowayan, S., 2024. A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. IEEE Access.

[2] Wang, S., Mitchell, J. and Piech, C., 2024, March. A large scale RCT on effective error messages in CSI, In Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. I (pp. 1395-1401).

[3] Koktas, E. and Basar, E., 2024. Communications for the planet mars: Past, present, and future. IEEE Aerospace and Electronic Systems Magazine.

[4] Zhong, X., Sham, C.W., Ma, s.L., Chou, H.F., Mostaani, A., vu, T.X. and Chatzinotas, S., 2024. Joint source-channel coding system for 6G communication: Design, prototype and future directions. IEEE Access.

[5] Sokolovskyi, V., Zharikov, E. and Telenyk, S., 2024. DEVELOPMENT OF THEMETHOD OF DETECTING AND CORRECTING DATA TRANSMISSION ERRORS IN IOT SYSTEMS FOR MONITORING THE STATE OF OBJECTS. Eastern-European Journal of Enterprise Technologies.

[6] Upadhyay, R.R., Hamming Codes: Error Reducing Techniques, 2020.

[7] Ez-Zazi, 1., Arioua, M. and El Oualkadi, A., 2020. Adaptive Joint Lossy Source-Channel Coding for Multihop 10T Networks. Wireless Communications and Mobile Computing, 2020(1), p.2127467.

[8] Chlaab, A.K., Flayyih, W.N. and Rokhani, F.z., 2020. Reliability analysis of multibit error correcting coding and comparison to hamming product code for on-chip interconnect. Journal of Engineering, 26(6), pp.94-106.

[9] Duffy, K.R., An, W. and Médard, M., 2022. Ordered reliability bits guessing random additive noise decoding. IEEE Transactions on Signal Processing, 70, pp.4528-4542.

[10] Ravi, G.S., Baker, J.M., Fayyazi, A., Lin, S.F., Javadi-Abhari, A., Pedram, M. and Chong, F.T., 2023, January. Better than worst-case decoding for quantum error correction. In Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operatmg Systems, Volume 2 (pp. 88-102).

[11] Abbe, E., Shpilka, A. and Ye, M., 2020. Reed—Muller codes: Theory and algorithms .IEEE Transactions on Information Theory, 67(6), pp.3251-3277.

[12] Engelberg, S. and Keren, 0., 2024, May. Hardening Bus-Encoders with Power-Aware Single Error Correcting Codes. In 2024 IEEE European Test Symposium (ETS) (pp. 1-4).IEEE.

[13] Shen, L., wu, Y., xu, Y., You, X., Gao, X. and Zhang, W., 2024. GLDPC-PC Codes: Channel Coding Towards 6G Communications. arXiv preprint arXiv:2404.14828.

[14] Heng, Z., Li, X. , Wu, Y. and Wang, Q., 2024. Two families of linear codes with desirable properties from some functions over finite fields. IEEE Transactions on Information Theory.

[15] Sasidharan, B., Viterbo, E. and Dau, S.H., 2024. A Family of Low-Complexity Binary Codes with Constant Hamming Weights. arXiv preprint arXiv:2401.16647.

[16] Pereira, F.R.F., Pellikaan, R., La Guardia, G.G. and De Assis, F.M., 2021. Entanglementassisted quantum codes from algebraic geometry codes. IEEE Transactions on Information Theory, 67(11), pp. 7110-7120.

[17] Bordage, S., Lhotel, M., Nardi, J. and Randriam, H., 2020. Interactive oracle proofs of proximity to algebraic geometry codes. arXiv preprint arXiv:2011.04295.
[18] Bartoli, D., Montanucci, M. and Zini, G., 2021. On certain self-orthogonal AG codes with applications to quantum error-correcting codes. Designs, Codes and Cryptography, 89, pp.1221-1239.
[19] Chen, Z., Ye, M. and Barg, A., 2020. Enabling optimal access and error correction for the repair of Reed Solomon codes. IEEE Transactions on Information Theory, 66(12), pp.7439-7456.
[20] Kumar, S., 2020, August. Impact of Reed Solomon forward error correction code in enhancing performance of free space optical communication link. In Laser Communication and Propagation through the Atmosphere and Oceans IX (Vol. 11506, pp. 25-32). SPIE.
[21] Garcia-Herrero, F., Sånchez-Maciån, A., San-Isidro, M., Aranda, L.A. and Maestro, J.A., 2020. Efficient majority-logic Reed-Solomon decoders for single symbol correction.IEEE Transactions on Device and Materials Reliability, 20(2), pp.390-394.
[22] Tang, Y.J. and Zhang, X., 2021. Fast en/decoding of Reed-Solomon codes for failure recovery. IEEE Transactions on Computers, 71(3), pp. 724-735.
[23] Xiong, L., Han, X., Yang, C.N. and Zhang, X., 2023. Reversible data hiding in shared images based on syndrome decoding and homomorphism. IEEE Transactions on Cloud Computing, 11(3), pp.3085-3098.
[24] Etinski, S., 2023. Generalized syndrome decoding problem and its application to postquantum cryptography (Doctoral dissertation, Université Paris Cité).
[25] Zhang, Y., Zhao, H., cao, K., Zhou, L., Wang, Z., Liu, Y. and Wei, J., 2024. A highly reliable encoding and decoding communication framework based on semantic information. Digital Communications and Networks, 10(3), pp.509-518.