Hamming Codes as Error-Reducing Codes

William Rurik Arya Mazumdar

***Abstract*—Hamming codes are the first nontrivial family of error-correcting codes that can correct one error in a block of binary symbols. In this paper we extend the notion of *error-correction* to *error-reduction* and present several decoding methods with the goal of improving the error-reducing capabilities of Hamming codes. First, the error-reducing properties of Hamming codes with standard decoding are demonstrated and explored. We show a lower bound on the average number of errors present in a decoded message when two errors are introduced by the channel for general Hamming codes. Other decoding algorithms are investigated experimentally, and it is found that these algorithms improve the error reduction capabilities of Hamming codes beyond the aforementioned lower bound of standard decoding.**

I. Introduction

Error-correcting codes are used in a variety of communication systems for the purpose of identifying and correcting errors in a transmitted message. This paper focuses on *binary linear* codes. In this case, the messages are encoded in blocks of bits, called codewords, and any modulo-2 linear combination of codewords is also a codeword. A linear code has a generator matrix, that encodes the message (a binary vector) at the transmitting side of a communication channel by multiplying itself with the message. Therefore a binary linear code is just an $\mathbb{F}_2$-linear subspace. A linear block code also has a parity-check matrix, that is a generator matrix of the null-space of the code and helps decode the message at the receiver. A code has a limit in the number of errors that it is capable of correcting (given by $\lfloor \frac{d-1}{2} \rfloor$, where d is the minimum pairwise Hamming distance between words of the code). When this limit is exceeded, undefined behavior occurs when attempting to apply error correction to the erroneous vector. This motivates the exploration and construction of new models that attempt to reduce the number of errors in the received vector upon decoding.

In this paper we investigate the concept of an *error-reducing code*. The term was first used by Spielman in [7], where the concept was defined, but used only as a way to achieve low-complexity error-correcting codes, not as an object of independent interest. In [3], [4], error-reducing codes were central - and it was shown that such codes are equivalent to a combinatorial version of joint-source-channel coding. This line of work has been further extended in [1], [5].

We study the error-reducing properties of Hamming codes, a family of codes that correct one error with optimal redundancy. Our main contribution is to show a lower bound on the average number of errors remaining in the decoded message with *standard decoding* (defined in Section II-A) while two errors are introduced by an adversary. We also show that this lower bound is achievable for Hamming codes. However, standard decoding is not the best decoding method for the purpose of error reduction. We explore several other potential decoding methods for Hamming codes, and experimentally show that it is possible to beat the standard decoding lower bound on average number of errors.

This is in particular noteworthy, because Hamming codes are *perfect codes*, implying that any more than 1 error will certainly result in an incorrect decoding. Since for every possible error vector containing two errors the number of errors in the decoded message is not same, it makes sense to choose the average number of errors in the decoded message as a natural performance metric.

We begin this discussion by presenting some definitions and a simple example of the encoding procedure and the error-correcting properties of the Hamming code (section II). We then demonstrate how these properties can be used to reduce the number of errors in a vector that contains two errors (section III). This demonstration is followed by several algorithms that attempt to maximize the reduction in errors along with an analysis of the performance and scalability of each algorithm (section IV).

II. Hamming codes with standard decoding

Hamming codes are a class of linear block codes that were discovered back in 1950 [2]. A Hamming code can correct one error by adding m, a positive integer, bits to a binary message vector of length $2^m - m - 1$ to produce a codeword of length $2^m - 1$. When multiple errors are introduced into a codeword, there is no guarantee of correct recovery of messages. We show that in that situation as well, it can be possible for a Hamming code to reduce the number of errors contained in that codeword in the decoded message.

It is necessary to introduce some of the basic concepts from error-correcting codes. The material of this section can be found in any standard textbook of coding theory. Our point is to emphasize, via the example at the end of the section, that error reduction is possible in Hamming codes.

Let $x \in \mathbb{F}_2^n$. The *Hamming weight* of x, $w(x)$, is defined as the number of non-zero entries in x. For the case of binary vectors, this is equivalent to the number of 1s in the vector. Further, the *Hamming distance* between the two words $x, y \in \mathbb{F}_2^n$, $d(x, y)$, is the number of coordinates in which the two

William Rurik is with the Department of ECE, University of Minnesota - Minneapolis, email: rurik003@umn.edu. Arya Mazumdar is with the College of Information and Computer Science, University of Massachusetts at Amherst, email: arya@cs.umass.edu, and was with University of Minnesota. This research is supported by an NSF REU (Research Experience for Undergraduates) award NSF 1535566 (a supplement to NSF CCF 1318093).

978-1-5090-1090-5/16/$31.00 ©2016 IEEE

words differ. Two vectors will have a Hamming distance of 0 *if and only if* they are equal.

Let $\mathcal{C}$ denote the set of codewords obtained from encoding a set 2^k binary message vectors of length k (i.e., $\mathbb{F}_2^k$). A code is referred to as a *block code* if the messages are encoded in blocks of a given length (i.e., $\mathcal{C} \subseteq \mathbb{F}_2^n$ for some n). A *linear block code* is a block code that has the property that any $\mathbb{F}_2$-linear combination of codewords in $\mathcal{C}$ is also a codeword. Let $M = \mathbb{F}_2^k$ be a set of binary message vectors of dimension $k = 2^m - m - 1, m \geq 3$, an integer. An $[n, k, 3]$-*Hamming code* is a linear block code that maps a message in M to a unique codeword of length n, where $n = 2^m - 1$. Furthermore, any two of the codewords have a minimum Hamming distance of 3. The $[7, 4, 3]$-Hamming code is the first Hamming code, where $m = 3$. The reason the code is able to correct a single error is because the minimum distance is 3, i.e., a non-zero codeword must have a minimum Hamming weight of 3. Further definitions and concepts relating to Hamming codes and linear block codes can be found in [6, Chapter 2].

A. Standard decoding for Hamming codes

Recall the definitions of the generator and parity-check matrices from the introduction. The $[7, 4, 3]$-Hamming code has generator matrix G and parity check matrix H, given below respectively:

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

Let us look at an example to understand the standard decoding for Hamming codes. Suppose that the message to be sent is $x = (0101)$. This message will be encoded as $G^T \times x = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T = y$ (say).

Now suppose that an error represented by a vector $e = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}^T$ is added to the codeword y. We have, $y + e = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}^T$.

Once this erroneous codeword has been received, the location of the error can be found by multiplying it with the parity-check matrix. This is the standard decoding process for the $[7, 4, 3]$-Hamming code. We have $H \times (y + e) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^T$. It can be seen that the computed column matrix matches with column four of the parity check matrix H. Once this bit has been flipped, it can be seen that this matches the codeword $[1010101]^T$, corresponding to the message (0101), so the error has been corrected.

B. Error reduction with $[7, 4, 3]$-Hamming codes

In the case of 2 errors, the parity check matrix is unable to accurately correct either of the errors. For example, in the context of $[7, 4, 3]$-Hamming code, consider $e = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}^T; y = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T$, where e is the error vector with errors in two locations (columns 1 and 4). Now multiplying H with $y + e$ we get $H \times (y + e)^T = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^T$. So column 5 is the newly corrected column. After correcting what is perceived to be the error, the received codeword becomes 0011001. This corresponds to a message of (0001) since $\begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \times G = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}^T$. So the message (0101) was sent, but (0001) was decoded. The received message has a single error in it. However, two errors were introduced in the simulated communication channel. This means that the number of errors was reduced from the codeword to the decoded message. The goal now becomes finding an effective construction that is able to reproduce this result for other cases.

III. Error-reduction limits of standard decoding

The example above demonstrated a favorable result of standard decoding with the $[7, 4, 3]$-Hamming code by effectively reducing the number of errors in the received message. However, there are cases in which the number of errors in the message at the receiver remains stagnant or even increases. This section will begin with the presentation of our initial results along with some strategies for finding a good generator matrix. We will then prove that the matrix we found is the optimal generator matrix for the $[7, 4, 3]$-Hamming code with standard decoding in terms of the mean number of errors in the received message for every possible error vector.

A. Basic facts for standard decoding

The first pair of matrices that we investigated were the generator and parity check matrices that are labeled in (1). The encoding and decoding methods introduced in section II-A were followed for every possible combination of messages and error vectors. Since we used the $[7, 4, 3]$-Hamming code with two errors introduced, there are $2^4 \cdot \binom{7}{2} = 16 \cdot 21 = 336$ possible combinations of codewords and error vectors for the case in which two errors are introduced (since each message maps to exactly one codeword). The results for standard decoding with two or more errors are included in Table I.

Out of all 336 combinations, the average number of errors found in the decoded message was $\frac{13}{7}$ or about 1.8571 implying an average reduction of $\frac{1}{7}$. Interestingly, It was seen that the remaining errors do not depend on the initial message.

Lemma 1. *Suppose one or more errors are introduced into a codeword for a Hamming code of any order with standard decoding. Let q be the column of the parity-check matrix that is determined to be erroneous (i.e., q is the product of the parity check matrix and the erroneous codeword). q is independent of the initial message to be sent.*

This fact is obvious because $q = H \times (y + e) = H \times y + H \times e = H \times e$ depends on H and e and not on y. We are now able to prove the following proposition.

Proposition 2. *The number of errors in the decoded message (standard decoding) is independent of the transmitted message.*

Proof: It was shown in lemma 1 that the column labeled as erroneous only depends on the error vector. Let r be the received word, r' be the received codeword after correction is applied, and f be the vector that is added to

achieve the operation of applying correction. As before, y represents the original codeword being transmitted and e is the error vector added in the communication channel. We have, $r = y + e; \quad r' = y + e + f$. Now let $\widetilde{e} = e + f$. We have:

$$r' = y + \widetilde{e} \implies \widetilde{e} = r' - y. \tag{2}$$

Since $\widetilde{e}$ can be expressed as a linear combination of two codewords, it must also be a codeword as Hamming codes are linear. This means that $\widetilde{e}$ must have a corresponding message vector. Let m be the transmitted message, w be the final decoded message, and $\widetilde{m}$ be the message corresponding to $\widetilde{e}$. We write (2) as, $w^T \times G = m^T \times G + \widetilde{m}^T \times G \implies w^T \times G = (m + \widetilde{m})^T \times G$, where G is the generator matrix. Since the mapping from messages to codewords is one-to-one, $w = m + \widetilde{m}$. Therefore, the number of errors found in the decoded message is given by the Hamming weight of $\widetilde{m}$, which is shown to depend on the error vector e, the generator matrix G, and the vector that applies correction f. Since lemma 1 establishes that f is independent of the message being transmitted, $\widetilde{m}$, and therefore the resulting number of errors in the decoded message given by $w(\widetilde{m})$, is also independent of the message being transmitted. ■

The fact that the number of errors in the decoded message for a given generator matrix is independent of the message being sent from the transmitter means that only the $\binom{7}{2} = 21$ possible error vectors need to be considered when assessing the error reduction performance of a given Hamming code, when the channel introduces 2 errors. While the column labeled as erroneous has dependence on the parity check matrix and the error vector, the design of the generator matrix is what ultimately influences the reduction in errors. In the next section we will present the best possible generator matrix in respect to the average number of errors in the decoded message for the $[7, 4, 3]$-Hamming code with standard decoding.

B. A lower bound for the $[7, 4, 3]$-Hamming code with standard decoding

We were able to reduce the number of errors in the set of codewords to an average of 1.8571 - but this is not the fundamental limits of standard decoding with the $[7, 4, 3]$-Hamming code. Starting with the generator matrix from (1), if we replace the second row with the modulo-2 sum of the first two rows, we get the following generator matrix.

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{3}$$

For this generator matrix, the results for standard decoding with two or more errors present is summarized in the third column of Table I. When this generator matrix is used along with the parity check matrix that is labeled in (1), the average number of errors found in the decoded message for all error vectors becomes $\frac{12}{7}$ or about 1.7143. While this improvement is relatively small, this Hamming code reaches the maximum level of error reduction that is theoretically possible for the $[7, 4, 3]$-Hamming code with standard decoding. This means that for any $[7, 4, 3]$-Hamming code with two errors, the error reducing capabilities of standard decoding is limited to an average of 1.7143 errors across all possible error vectors.

As a consequence of proposition 2 we may assume that (0000) is the message to be transmitted for simplicity. In order to prove that 1.7143 is the lower bound for the average number of errors found in the set of decoded messages, we will make use of the following lemmas.

Lemma 3. *Consider a $[n = 2^m - 1, 2^m - 1 - m, 3]$-Hamming code with standard decoding. If the received vector y has two errors present, then the index of the column labeled as erroneous by multiplying the parity check matrix with y will always correspond to a 0 on the error vector.*

Proof: Suppose that the index of the column labeled as erroneous by multiply the parity check matrix with y correspond to a 1 in the error vector. Then, for the all-zero message, the corrected codeword will have a Hamming weight of 1, in the presence of two errors. This implies the existence of a codeword with a Hamming weight of 1. ■

Lemma 4. *Let E be the set of all binary vectors with two ones. Suppose that a single 0 in every member of E is replaced with a 1 to obtain E', such set of minimum size. Then $|E'| = \frac{|E|}{3}$.*

Proof: It must first be noted that before any operation is applied, E has a cardinality of $\binom{n}{2}$. If the goal is to reduce the cardinality of E, then we want to map as many members of E as possible to a single vector with a Hamming weight of 3. Now, three different weight-two vectors can be obtained by changing a single coordinate of a weight-3 vector. Hence the statement is proved. It should be noted that this is the total number of codewords that will have a weight of 3. ■

Lemma 5. *Suppose we want to map a message with a Hamming weight of 2 to a codeword with a Hamming weight of 3, then the generator matrix used for the encoding must contain at least one row r, such that $w(r) \geq 4$.*

Proof: Suppose that all rows of the generator matrix have a weight of 3. The process of mapping a message of weight 2 to a codeword with a weight of 3 is the same as taking the modulo-2 sum of two rows within the generator matrix. Let a, b be any two rows of the generator matrix. Note that, $d(a, b) > 2$. Hence $d(a, b) = 4$ or 6. In both the two cases we do not get a codeword of weight 3 as $a + b$. ■

Lemma 6. *Consider an $[n, k, 3]$ Hamming code. Let t be the number of rows in the generator matrix with a Hamming weight of 3. If all other rows have a Hamming weight of 4, then the maximum number of messages with a Hamming weight of 2 that can be mapped to codewords of Hamming weight 3 is $(k - t) \times t$.*

Proof: According to lemma 5, a weight-2 message will generate a weight-3 codeword only when the two rows (of the generator matrix) being added are of weights 3 and 4. Since, there are only t rows within the generator matrix with

a Hamming weight of 3, this combination can happen in at most $(k-t)\times t$ different ways. ∎

The above lemma implies that, for a $[7,4,3]$ Hamming code, if one row of the generator matrix has a weight 4, and all other rows have weight 3, then at most 3 messages with a weight of 2 can be mapped to codewords with a weight of 3. This brings us to the following claim.

Theorem 7. *Consider a $[7,4,3]$-Hamming code $\mathcal{C}$ and let E be the set of all unique error vectors of length 7 and weight 2. Let t be the average number of errors found after standard decoding in the decoded message at the receiver for all possible modulo-2 sums of each member of E with each member of $\mathcal{C}$. If the Hamming code is designed to minimize t using the standard decoder, then $t=\frac{12}{7}$.*

Proof: Because of proposition 2, we can assume that the transmitted message is (0000). Applying lemmas 3 and 4, it can be seen that E can be collapsed to a set of seven unique vectors, call this set E'. The vectors in E' must be codewords in order for standard decoding to work. Since it is not possible to fully correct two errors with a Hamming code using standard decoding (since only one correction is made), the number of errors found in the resulting decoded message will never be zero. This means that the optimal Hamming code will map the seven messages with the lowest possible distance from the original message to the set of seven unique codewords in E'. There are only four messages with a distance of 1 from the message 0000 (those being $0001, 0010, 0100$, and 1000), meaning that the remaining three codewords in E' must correspond to messages that are a Hamming distance of two from the original message. In order for every message with a distance of one from 0000 to be mapped to a vector in E', each row of the generator matrix must have a weight of 3. However, lemmas 5 and 6 show that in order for a message with a weight of 2 to map to a vector in E', the generator matrix must have at least one row that does not have a weight of 3 (otherwise the average number of remaining errors is at least $1\cdot\frac{4}{7}+3\cdot\frac{3}{7}=\frac{13}{7}$). In this case, only 3 messages with a distance of 1 and only three messages with a distance of 2 from 0000 can be mapped to codewords in E'. This means that a seventh message with a distance of 3 from the original message must be mapped to a codeword in E' in order to avoid altering another row of the generator matrix. This gives an average Hamming distance of $1\cdot\frac{3}{7}+2\cdot\frac{3}{7}+3\cdot\frac{1}{7}=\frac{12}{7}$ from the original message 0000, giving the same results that were observed from the generator matrix in (3). ∎

While this theorem is limited to the case of the $[7,4,3]$-Hamming code with two errors, we can extend it to higher order Hamming codes as well - as in the next subsection. However, finding a bound for the case in which three errors are introduced becomes complicated as this allows for codewords to be changed into other codewords by the error vector.

C. Extension to general Hamming Codes

Here we generalize the result of the previous section to general Hamming codes. Our main result is the following.

Theorem 8. *Consider an $[n=2^m-1, k=2^m-1-m, d=3]$ Hamming code $\mathcal{C}$ for $m\geq 4$, and $E=\{e\in\mathbb{F}_2^n : w(e)=2\}$. Find the minimum $\ell\in\mathbb{Z}$, $0\leq\ell\leq\lfloor\frac{k}{2}\rfloor$, such that*

$$k-\ell+\ell(k-\ell)\geq\frac{1}{3}\binom{n}{2}. \tag{4}$$

Then a lower bound for the average (over all codewords in $\mathcal{C}$ and all errors in E) number of errors in a message after standard decoding is $2-\frac{k-\ell}{\frac{1}{3}\binom{n}{2}}$.

We need the following lemma to prove this.

Lemma 9. *For every $m\geq 4$, there is an $\ell\in\mathbb{Z}$, $0\leq\ell\leq\lfloor\frac{k}{2}\rfloor$ such that $k-\ell+\ell(k-\ell)\geq\frac{1}{3}\binom{n}{2}$. Recall that $k=2^m-m-1$ and $n=2^m-1$.*

Proof: If k is odd choose $\ell=\frac{k-1}{2}$ and if k is even, choose $\ell=\frac{k}{2}$. For $m\geq 4$, these value of ℓ satisfy the claim (some details omitted). ∎

Now we are ready to prove theorem 8.

Proof of Theorem 8: Again, we can assume that the sent message is all 0. Let M be the set of messages that map onto codewords of weight 3. It is necessary to minimize the average weight of the message vectors in M. All messages of Hamming weight 1 in M must have the codewords as rows in the generator matrix. Since, from lemma 4, $|M|=\frac{1}{3}\binom{n}{2}>k$, it will be necessary to map messages of weight 2 or more onto codewords of weight 3. However, if every row of the generator matrix has a weight of 3, then, by lemma 5 all of the remaining codewords of weight 3 will have corresponding messages with a weight of 3 or higher. So, M will consist of messages with weights of 1 and 3 or higher. Lemma 6 states that removing ℓ rows of weight 3 from the generator matrix and replacing them with codewords of weight 4 will remove ℓ messages of weight 1 from M and will add up to $\ell\times(k-\ell)$ new messages of weight 2; meaning that up to $\ell\times(k-\ell)-\ell$ messages with a Hamming weight of 3 or higher will be removed from M. In other words, if M still has members with a weight of 3 or greater, then replacing a row of weight 3 within the generator matrix with a row of weight 4 should either reduce or maintain the average Hamming weight of the members of M. When M has no members left with a Hamming weight of 3 or higher (such an M exists as a result of lemma 9), this condition is exactly equivalent to the condition stated in (4). Once M consists solely of messages with a weight of 1 or 2, then the average Hamming weight of the members of M will be $\frac{k-\ell+2(\frac{1}{3}\binom{n}{2}-k-\ell)}{\frac{1}{3}\binom{n}{2}}$. Note that M should have $k-\ell$ members of Hamming weight 1 and the remaining members ($\frac{1}{3}\binom{n}{2}-k-\ell$ of them) will have a weight of 2. Here it can be seen that increasing ℓ beyond the minimum that satisfies the condition in (4) must necessarily increase the average Hamming weight as a message of weight 1 in M will be replaced with a message of weight 2. Since the chosen generator matrix will correspond to an ℓ that minimizes the average weight of the members of M, it must be optimal. ∎

Extending the result of Thm. 8 to three or more errors presents a number of difficulties. The primary challenge is that

Number of errors introduced	Average number of errors in decoded message				
	Standard decoding	Optimized standard decoding	Minimum of sums decoding	Minimum of maximums decoding	Majority bit decoding
2	1.8571	1.7143	1.4286	1.4643	1.2857
3	2.2000	2.1714	1.8571	1.7714	1.7857
4[1]	1.9429	1.8286	2.1429	2.0571	2.1429

TABLE I
RESULTS FOR $[7, 4, 3]$-HAMMING CODE WITH DIFFERENT DECODING METHODS

it can no longer be assumed that the codeword being added to the erroneous vector as a part of the standard decoding process has a weight of 3. This would require a new definition for the set M in Theorem 8.

IV. OTHER DECODING METHODS

Though Hamming codes with standard decoding were found to be limited by theorems 7, 8, other decoding methods have shown more favorable results. Several decoding algorithms were experimentally tested, giving a best-case result of having $\frac{9}{7}$ or 1.2857 errors in the received message. However, there is an increased computational cost of employing such algorithms, substituting a matrix multiplication for several search operations within larger sets. Furthermore, these algorithms do not guarantee independence of the residual errors on the transmitted codeword (i.e., proposition 2 is not valid). For all of these algorithms, it should be assumed that the encoding procedure is unchanged and that the generator matrix in (1) was used for the encoding process. In all of the decoders below, the first step consists of determining all codewords that are a distance of less than or equal to the number of errors introduced from the erroneous vector. The messages corresponding to these codewords were collected into a list L.

A. Minimum of sums decoding

For every message, x, the sum of the Hamming distances between x and all $y \in L$ was taken. The decoded message would then be the message x that minimizes this norm.

As the results show, this decoding method provides a slight improvement to standard decoding, albeit with an increased cost in computational complexity. It should be noted that this decoding method was the only tested method that was found to have results that are independent of the transmitted codeword in this specific experiment for the $[7, 4, 3]$ code.

B. Minimum of maximums decoding

The minimum of maximums decoding algorithm finds all Hamming distances between each message and every member of L. Then, for every message, x, the maximum distance between x and every member in L is included in a list. The message that corresponds to the minimum of this list of distances is chosen as the decoded message. Though this algorithm was an improvement from previous results for the cases in which three or four errors were introduced, the number of errors increased when two errors were present.

[1]Choosing any codeword will reduce errors for the four error case, so this row does not indicate proper scaling in the number of errors introduced.

C. Majority bit decoding

The majority bit decoding algorithm observes each bit for every message in L. Let $L = \{y^1, y^2, \ldots, y^l\}, l = |L|$, and let y_i^j denote the coordinate i of the message y^j. Also let n denote the length of the messages y. For each $j \in \{1, \ldots, k\}$, if $\sum_{i=1}^{l} y_j^i > \frac{l}{2}$, then entry j of the decoded message is 1; otherwise it is 0. This algorithm gave the best reduction for two errors, but this is not uniformly distributed across messages.

The results of all the above algorithms for the $[7, 4, 3]$-Hamming code are shown in Table I.

V. CONCLUSION

In this paper we initiate the study of the error-reducing property for classical families of error-correcting codes. It was found that the error reduction capabilities of Hamming codes are limited when standard decoding is used, inviting the study of other decoding methods. Several other decoding algorithms were implemented for Hamming codes and found to be more effective for reducing errors than standard decoding. For these algorithms, it is important to consider the tradeoff between the consistency of the algorithm across messages and the error reduction performance of the algorithm.

It would be useful to extend the bound presented in Theorem 8 to an arbitrary number of errors. It is also of interest to explore other decoding methods to provide a greater level of error reduction with low complexity. Future work should address the best possible reduction that can be achieved as no lower bound is known in general. Finally, it will be of interest to compute the error-reducing properties of other well-known families of codes such as BCH codes.

REFERENCES

[1] W. Gao and Y. Polyanskiy . *On the bit error rate of repeated error-correcting codes*. Information Sciences and Systems Proceedings (CISS), 2014 Conference on. 2014.

[2] R. W. Hamming. *Error detecting and error correcting codes*. Bell System technical journal, vol. 29, no. 2, pp. 147–160, 1950.

[3] Y. Kochman, A. Mazumdar, and Y. Polyanskiy. *Results on combinatorial joint source-channel coding*. Information Theory Workshop, 2012.

[4] Y. Kochman, A. Mazumdar, and Y. Polyanskiy. *The adversarial joint source-channel problem*. Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on. IEEE, 2012.

[5] A. Mazumdar and A. S. Rawat. *On Adversarial Joint Source Channel Coding*. Information Theory Proceedings (ISIT), 2015 IEEE International Symposium on. IEEE, 2015.

[6] R. Roth. *Introduction to Coding Theory*. Cambridge, NY, 2006.

[7] D.A. Spielman. *Linear-time encodable and decodable error-correcting codes*. Proceedings of the twenty-seventh annual ACM symposium on Theory of computing. ACM, 1995.