Theoretical Mathematics & Applications, vol. 6, no. 1, 2016, 151-161
ISSN: 1792- 9687 (print), 1792-9709 (online)
Scienpress Ltd, 2016

A New Theory of Error Correction Coding

Louis M. Houston[1]

Abstract

We have derived a new theory of error correction coding. For a given rate, R, we can construct a codeword with greater error correction than that predicted by the traditional theoretical limit. The maximum improvement is 33%. The new theory incorporates the concept of an analytic message or a message with a non-zero level of predictability. We show that error correction is based on both redundancy and predictability and we focus on a special case in which the message is a digital root 9 number.

Mathematics Subject Classification: 94A16; 94A24

Keywords: error correction; coding theory; codeword; code rate; digital root

1 Introduction

Error correction coding [1] is the means whereby errors that may be introduced into digital data as a result of transmission through a communication

[1] Louisiana Accelerator Center, University of Louisiana at Lafayette, LA, U.S.A.
E-mail:houston@louisiana.edu

Article Info: *Received:* June 15, 2015. *Revised:* July 25, 2015.
Published online : January 5, 2016.

channel [2] can be corrected based upon received data. Alternatively, error correction may be used to correct data that has deteriorated in storage.

The idea behind error correcting codes is conceptually simple: add redundancy [3] to the information so that even if the resulting data gets corrupted, e.g. packets get corrupted during routing or the DVD gets some scratches, the original information can still be recovered. Error-correcting codes are one of the glories of the information age: They are what guarantees the accurate transmission of digital information over the airwaves or through copper wire, even in the presence of corrupting influences that represent noise.

Error correction coding is referred to as coding theory [4]. Coding theory, sometimes called algebraic coding theory, deals with the design of error correcting codes. It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra [5]. It has connections with other areas of discrete mathematics, especially number theory [6] and the theory of experimental designs [7].

Error correction coding is essentially based on a repetition scheme. The disadvantage of the repetition scheme is that it multiplies the number of bits transmitted by a factor that may prove unacceptably high. In 1948, Claude Shannon, working at Bell Laboratories in the USA, inaugurated the whole subject of coding theory by showing that it was possible to encode messages in such a way that the number of extra bits transmitted was as small as possible [7]. Unfortunately, his proof did not give any explicit recipes for these optimal codes. It was two years later that Richard Hamming, also at Bell Labs, began studying explicit error correcting codes with information transmission rates more efficient than simple repetition [8]. His first attempt produced a code in which four data bits were followed by three check bits that allowed not only the detection, but the correction of a single error. The repetition code would require nine check bits to achieve this.

The value of error correction codes for information transmission, both on

Earth and from space, was immediately apparent, and a wide variety of codes were constructed that achieved both economy of transmission and error correction capacity.

A code C is given by an encoding map of the form: $C : \sum^k \to \sum^n (\text{for integers } k < n)$

which encodes a sequence of k symbols (the message) from $\sum$ into a larger sequence of n symbols (the codeword) [9].

The rate of C is the ratio $R = k/n$ [10]. Note that R exactly captures the amount of information contained per bit of a codeword.

The question of interest is as follows: given a code C of rate R, what is the maximum fraction of errors, ρ [11], that can be tolerated by C? Now as every codeword has k symbols of information, it is intuitive that in the worst case at least k symbols of a codeword should be uncorrupted to have any hope of recovering the original information. In other words, we can only have $\rho \le (n-k)/k = 1-R$, irrespective of the computational power of the decoder. Therefore, $\rho = 1-R$ is accepted as the theoretical limit of error correction [12].

Current error correction theory treats messages as purely random [13], but in this paper we demonstrate that the more general theory must also incorporate messages with some level of predictability that we refer to as analytic messages. By including both redundancy and predictability into error correction, we can show that the theoretical limit for error correction is, in fact, incorrect and that the true limit is actually greater.

In this paper, we derive the new theoretical error correction limit and focus on a special case that involves messages that consist of digital root 9 numbers [14].

2 Theory

2.1 The essential elements of the theory

A code C is defined as the mapping:

$$C:\sum^{k}\to\sum^{n}, k\le n,\quad k,n\in\mathbb{Z}^{+}, \tag{1}$$

$\sum$ is the alphabet.

The length of the message is k and the length of the codeword is *n*. In the traditional theory, $k<n$, but in the new theory, $k\le n$.

We define an analytic message as a message that contains predictable symbols.

We define α as the number of predictable symbols in the message. We define β as the rule for predicting symbols in the message. We define μ as the mass of the message.

(For a completely random message, $\alpha=0$ and $\beta=\varnothing$.) The code rate is

$$R=\frac{k}{n}. \tag{2}$$

The mass is

$$\mu=\frac{k}{\alpha+1}|\Sigma|. \tag{3}$$

The mass is a measure of the complexity of the message. The mass generally increases with the length of the message. A completely analytic message can still have mass. However, in general, the more predictable a message, the less is its mass.

The theoretical limit for the fractional error tolerance, $\tilde{\rho}$ is

$$\tilde{\rho}=1-R+\frac{\alpha}{n}. \tag{4}$$

Observe that for purely random messages, $\tilde{\rho}\to\rho$ consistent with the traditional theory.

It is clear that error correction improves as predictability increases, but also note

that as predictability increases, mass (i.e. complexity) decreases.

Let us consider a simple case that demonstrates the relative error correction performance limits of a random message and an analytic message. Without loss of generality, let the alphabet, $\sum$ consist of base 10 digits. Suppose that a random message is 22 and the codeword is 2222, so that $k = 2$ and $n = 4$. In this case $\alpha = 0$ and $\beta = \varnothing$. The error correction limit is $1 - R = 1 - 2/4 = 1/2$. Now consider a case for which $\beta =$ "the digits of the message are sequential". In this case the message is predictable such that $\alpha = k - 1$. Let the message be 12 and the codeword be 1212. Once again, $k = 2$ and $n = 4$. The error correction limit is $1 - R + 1/4 = 1 - 2/4 + 1/4 = 3/4$. The logic of this increase in error correction is simple. In the random message case, we need at least two digits to recover the message. In the analytic case, if we only had one digit and β, we could recover the entire message. However, observe that the mass of the random message is $\mu = 20$, while the mass of the analytic message is $\mu = 10$. Therefore, the random message has twice the complexity of the analytic message.

2.2 Four major messages types

There are four major message types.

The completely analytic message (i.e. completely predictable):

$$\alpha = k. \tag{5}$$

The message that has k-1 predictable digits:

$$\alpha = k - 1. \tag{6}$$

The message that has one predictable digit:

$$\alpha = 1. \tag{7}$$

The random message:

$$\alpha = 0. \tag{8}$$

It is clear to see that for the completely analytic message (5), there is complete

error correction: $\tilde{\rho} = 1 - R + k/n = 1$.

For (6), we have $\tilde{\rho} = 1 - R + (k-1)/n = (n-1)/n$.

For (7), we have $\tilde{\rho} = 1 - R + 1/n = (n-k+1)/n$.

For (8), we have $\tilde{\rho} \to \rho = 1 - R = (n-k)/n$.

The mass of a completely analytic message is

$$\mu = \frac{k}{k+1}|\Sigma|. \tag{9}$$

We see that $\mu \in [(1/2)|\Sigma|, |\Sigma|)$.

The mass of a message with $k-1$ predictable digits is

$$\mu = |\Sigma|. \tag{10}$$

The mass of a message with one predictable digit is

$$\mu = \frac{k}{2}|\Sigma|. \tag{11}$$

The mass of a random message is

$$\mu = k|\Sigma|. \tag{12}$$

It is interesting to compare the random message with the message that has one predictable digit. Given the same alphabet size, if the message that has one predictable digit is twice as long as the random message, then they have the same mass. This normalizes the complexity so that we can compare the error correction. As stated earlier, we can write the error correction of the random message as

$$\tilde{\rho}_{\alpha=0} = \frac{(n-k)}{n}. \tag{13}$$

For the message that has one predictable digit, the error correction becomes

$$\tilde{\rho}_{\alpha=1} = \frac{(2n-2k+1)}{2n} = \frac{(n-k+1/2)}{n} = \frac{(n-k)}{n} + \frac{1}{2n}$$

or

$$\tilde{\rho}_{\alpha=1} = \tilde{\rho}_{\alpha=0} + \frac{1}{2n}. \tag{14}$$

Note that in this case, the rates are identical. If $k=1$ and $n=2$,

$$\tilde{\rho}_{\alpha=1}=\frac{1}{2}+\frac{1}{4}=\frac{3}{4}. \tag{15}$$

The error correction improvement is

$100\%(1-\tilde{\rho}_{\alpha=0}/\tilde{\rho}_{\alpha=1})=100\%(1-0.5/0.75)=33\%$

3 The Case of Digital Root Nine Messages

3.1 The digital root nine theorem

Based on a mathematical theorem, all numbers $\frac{9m}{2^n}$ or $\frac{9m}{5^n}$, where m and n are positive integers have a digital root of 9. A digital root is the single digit result of successive digit sums [14]. For example, the digital root of 225 is 9 or the digital root of 3.14 is 8. A digital root 9 number is an analytic message with $\alpha=1$. The rule is: $\beta=$"the digital root of the message is 9". The theorem is as follows.

Theorem I. $dr\left(\frac{9m}{2^n}\right)=dr\left(\frac{9m}{5^n}\right)=9$, $m\in\mathbb{Z}^+$, $n\in\mathbb{Z}^+\cup\{0\}$.

Proof. The digits $\{a_j\}$ of an arbitrary positive number x are given by the equation:

$$a_j=\left\lfloor\frac{x}{10^{j-1}}\right\rfloor-10\left\lfloor\frac{x}{10^j}\right\rfloor.$$

Therefore, we can perform the digit sum as follows:

$$\sum_j a_j=\sum_j\left(\left\lfloor\frac{x}{10^{j-1}}\right\rfloor-10\left\lfloor\frac{x}{10^j}\right\rfloor\right).$$

Let $j=-\ell$ to $+\ell$.

$$\sum_j a_j = \left\lfloor \frac{x}{10^{-\ell-1}} \right\rfloor - 10\left\lfloor \frac{x}{10^{-\ell}} \right\rfloor + \left\lfloor \frac{x}{10^{-\ell}} \right\rfloor - 10\left\lfloor \frac{x}{10^{-\ell+1}} \right\rfloor + \ldots$$

$$\sum_j a_j = \left\lfloor 10^{\ell+1}x \right\rfloor - 9\left\lfloor 10^{\ell}x \right\rfloor - 9\left\lfloor 10^{\ell-1}x \right\rfloor - 9\left\lfloor 10^{\ell-2}x \right\rfloor - \ldots$$

Let $x = 9y$.

$$\sum_j a_j = \left\lfloor 10^{\ell+1}(9y) \right\rfloor - 9\left\lfloor 10^{\ell}(9y) \right\rfloor - 9\left\lfloor 10^{\ell-1}(9y) \right\rfloor - 9\left\lfloor 10^{\ell-2}(9y) \right\rfloor - \ldots$$

Let $10^{\ell+1}(9y) \in \mathbb{Z}^+$.

$$\sum_j a_j = 10^{\ell+1}(9y) - 9\left\lfloor 10^{\ell}(9y) \right\rfloor - 9\left\lfloor 10^{\ell-1}(9y) \right\rfloor - 9\left\lfloor 10^{\ell-2}(9y) \right\rfloor - \ldots$$

$$\sum_j a_j = 9\left[10^{\ell+1}y - \left\lfloor 10^{\ell}(9y) \right\rfloor - \left\lfloor 10^{\ell-1}(9y) \right\rfloor - \left\lfloor 10^{\ell-2}(9y) \right\rfloor - \ldots \right].$$

$\therefore dr\left(\sum_j a_j \right) = 9$, since the digital root of 9*b*, where *b* is a positive integer, is 9.

Let $y = \frac{m}{2^n}$ *or* $\frac{m}{5^n}$. Since 2 and 5 are factors of 10, $dr\left(\frac{9m}{2^n} \right) = dr\left(\frac{9m}{5^n} \right) = 9$. □

3.2 A demonstration of error recovery for a digital root nine number

A combination of digital root 9 numbers is also a digital root 9 number.

Given the number $\frac{9m}{2^n}$, $10^n\left(\frac{9m}{2^n} \right)$ is a digital root 9 integer.

Suppose we want to generate a digital root 9 number that has 16 digits. We find a combination of

$10^5\left(\frac{9(563)}{2^5} \right)$ and $10^5\left(\frac{9(933)}{2^5} \right)$

= 15834375 and 26240625.

We then replace all occurrences of 9 with 0. This essentially makes the number

base 9.

This 16 digit digital root 9 number becomes $D = 1583437526240625$.

After long storage, we retrieve the number and find

$$D = \ 158\text{x}4375\ 26240625, \tag{16}$$

where x is a corrupted digit. Observe that D is a codeword for which $k = n$, so there is no redundancy.

To recover x, we simply use the equation:

$$dr(D) = D - 9\left\lfloor \frac{D-1}{9} \right\rfloor \tag{17}$$

to calculate the digital root of D while varying x from 0 to 8 until

$$dr(D) = 9. \tag{18}$$

We find that $x = 3$.

[In the above equation, $\lfloor\ \rfloor$ represents the greatest integer function]. In this case, for the error correction of *D*, we have demonstrated that $\tilde{\rho}_{\alpha=1} = 1 - R + 1/n = (n-k+1)/n$ which, in this case, is $\tilde{\rho}_{\alpha=1} = 1/n = 1/16$.

4 Conclusion

The traditional error correction coding theory is based, essentially, on the redundancy of the message and has neglected the impact of message predictability on error correction. When predictability is included in the theory, in the form of analytic messages, the error correction can be significantly improved. That is, the theoretical limit for error correction is significantly increased for analytic messages in comparison to random messages. Current error correction methods have come near to the traditional theoretical limit, but with the new theory and analytic messages such as digital root 9 messages, error correction codes can reach a new level of performance that outstrips the old theoretical limit.

Acknowledgements. The author greatly appreciates the important observation of Paul Walton.

References

[1] C. Berrou and A. Glaviuex, Near Optimum Error Correcting and Decoding: Turbo Codes, *IEEE Trans. Comm.*, **44**(10), (1996), 1261-1271.

[2] C.E. Shannon, A Mathematical Theory of Communication, *Bell System Technical Journal*, **27**, (1948), 379-423 & 623-656.

[3] B. Auffarth, M. Lopez-Sanchez and J. Cerquides, Comparison of Redundancy and Relevance Measures for Feature Selection in Tissue Classification of CT Images, *Advances in Data Mining. Applications and Theoretical Aspects*, (2010), 248-262.

[4] B. Alexander, At the Dawn of the Theory of Codes, *Math. Intel*., **15**, (1993), 20-26.

[5] O.F. Humphreys and M.Y. Prest, *Numbers, Groups and Codes*, New York, Cambridge University Press, 1990.

[6] G. E. Andrews, *Number Theory*, New York, Dover, 1994.

[7] C.S. Peirce, Note on the Theory of the Economy of Research, *Coast Survey Report*, 197-201, (1876).

[8] T.K. Moon, *Error Correction Coding*. New Jersey, John Wiley & Sons, 2005.

[9] R. Bose and D. Ray-Chaudhuri, On a Class of Error-Correcting Binary Codes, *Inf. And Control*, **3**, (1960), 68-79.

[10] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, 2003.

[11] C. Berrou, A. Glaviuex and P. Thitimajshima, Near-Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes, in Proc. 1993 *IEEE*

International Conference on Communications, Geneva, Switzerland, (1993), 1064-1070.

[12] V. Guruswami and P. Indyk, Linear-time encodable/decodable codes with near-optimal rate, *IEEE Trans. on Info. Theory*, **51**(10), (2005), 3393-3400.

[13] M. Santha, U.V. Vazirani, Generating quasi-random sequences from slightly-random sources, *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, University of California, (1984), 434-440.

[14] F.M. Hall, *An Introduction into Abstract Algebra*, 2nd edition, CUP Archive, 101, 1980.