Chapter 1

Introduction

1.1 Layman's Summary

A great deal of human effort has been exerted throughout history to communicate messages quickly and reliably over long distances. For example, the Roman empire constructed a communications network based on smoke signals which ranged more than 4,500 kilometers. In 1794, the first mechanical optical telegraph used a network of signal flags mounted on towers to transmit messages across Europe. Commercial electrical telegraph service began in 1844 when Morse sent a message from Washington D.C. to Baltimore. Today, multiple digital and analog communications networks encircle the earth and provide telephone, internet, and television services.

In general, all communications systems such as these must make compromises between speed and reliability. For example, telegraph operators are more prone to error when they receive messages which are sent very rapidly. The noise level also increases with the length of the telegraph wire, degrading the reliability of the system. In 1948, Claude Shannon made this concept mathematically precise, and the field of *information theory* was born. One of his main results, the channel coding theorem, says that there is a fundamental limit on the rate that information can be transmitted reliably through a noisy medium [4].

To explain his result properly, we assume that some *sender* would like to transmit a *message* through a noisy medium (i.e., the *channel*) to a *receiver*. For simplicity, we assume the message is a sequence of *bits* (1's and 0's). While the sender may repeatedly transmit one message bit per channel use, uncertainty in the transmission due to noise may cause errors in

the received message. The reliability of the received message can, of course, be improved by sending the same bit many times and allowing the receiver to choose the most probable bit value. For example, if each message bit is transmitted q times, then the *rate* of transmission, which is the number of message bits transmitted per channel use, is said to be $1/q$. Shannon proved the remarkable result that, by using clever encoding and decoding, information can be transmitted reliably at any rate less than a fundamental limit known as the *channel capacity*. Furthermore, he proved that no system can transmit information reliably at rates above the channel capacity.

For example, consider a channel which erases every other bit. This means that the input sequence, 10110010, is mapped to the output sequence, $1?1?0?1?$. Clearly, one message bit can be transmitted reliably for every two channel uses by sending each message bit twice in a row. This establishes that reliable transmission is possible at rate $1/2$. Since the capacity of this channel also equals $1/2$, we know that reliable communication is impossible at any higher rate. The field of *channel coding* focuses on practical methods of encoding and decoding which achieve reliable communication at rates close to capacity. For most channels, the problem of designing effective codes is quite difficult.

For a long time, it was speculated that no relatively simple coding system could approach capacity. These speculations were based on the fact that the first 40 years of research had produced no such system. A major breakthrough occurred in 1993, when Berrou, Glavieux, and Thitimajshima introduced *turbo codes* [1]. Turbo codes shattered these myths by providing performance very close to capacity with only moderate complexity. The trick behind turbo codes was encoding the same data with two simple encoders and then decoding with two simple decoders working together cooperatively. In particular, the turbo decoder works by passing the output of one decoder to the input of the other decoder in a circular fashion. The name, turbo codes, is derived mainly from the similarity between the decoder structure and a turbo charged engine. This type of decoding, now referred to as *iterative decoding*, was actually invented in the 1960s by Gallager, but was ahead of its time and essentially forgotten [3].

The advent of turbo codes has also sparked new interest in the field of information theory. This has led, in turn, to some very exciting research in the past ten years. For one, the renewed interest in coding theory led to the rediscovery of Gallager codes. Variations of these codes have been shown to nearly achieve the channel capacity of channels whose outputs are independent of each other. Much of the work in this dissertation was directly or indirectly motivated by turbo codes. Chapters 2 and 3 deal with a variation of turbo codes known as

Convolutional Accumulate-m codes. These codes have some very interesting properties and are analyzed in detail. Chapter 4 focuses on a simple method of estimating the channel capacity for a class of time-varying channels, known as finite state channels. Before the work presented here, the capacity of these channels could not be estimated easily. Chapter 5 explains the application of a powerful linear code to a simple finite state channel. Using a combined iterative decoding strategy for the channel and the code, we provide a concise analysis of the decoder behavior. This analysis of the decoder allows us to algebraically construct codes whose iterative decoding performance is extremely close the theoretical limit.

The applications of this research include improving the efficiency of communication systems by either increasing data rates or noise tolerance. Either change brings the system closer to the fundamental limit defined by Shannon. For example, a hard disk drive can be thought of as a communications system which transmits data forward in time (i.e., data is written at one time and read at another). In this sense, techniques described in Chapter 4 may eventually be leveraged to increase the storage density of hard disk drives. This research can also be applied to reduce the complexity of encoding/decoding circuits while leaving the coding performance unchanged. In particular, the codes described in Chapters 2 and 3 operate fairly close to the fundamental limit and are very simple to encode and decode.

1.2 Outline of Dissertation

This dissertation consists of an introduction and four self-contained chapters. The chapters cover a fairly wide range of topics including Chapter 2's straightforward analysis of the serial concatenation of rate-1 codes, Chapter 3's thorough analysis of Convolutional Accumulate-m codes, Chapter 4's exposition on the capacity of finite state channels, and Chapter 5's sizable discussion of the joint iterative decoding of codes and channels with memory.

In Chapters 2 and 3, we consider a new class of simple codes with good performance near the Shannon limit. This inquiry was motivated initially by the Repeat Accumulate (RA) codes of Divsalar, Jin, and McEliece [2], which are perhaps the simplest turbo-like codes. These codes are encoded by repeating each message bit q times, randomly reordering all of these repeated message bits, and then computing the modulo-2 cumulative sum of the entire sequence. Although incredibly simple, their performance under iterative turbo-like decoding is very good.

From a coding perspective, an RA code consists of a repeat code followed by a inter-

leaver (which reorders the bits) and a rate-1 code (i.e., the modulo-2 cumulative sum). In Chapter 2, we investigate the performance of more general coding systems based on interleavers and rate-1 codes. In particular, we consider the serial concatenation, through random interleavers, of an arbitrary binary linear outer code and a cascade of m identical rate-1 binary linear inner codes. Our analysis shows that the maximum likelihood decoding performance of these codes, for large enough m, is extremely good. Simulation results are also provided for a practical configuration of these codes known as Convolutional Accumulate-m (CA^m) codes. CA^m codes are a novel generalization of RA codes formed by using a terminated convolutional code as the outer code and a cascade of m interleaved rate-1 "accumulate" codes as the inner code. The practical performance of CA^m codes using iterative decoding is similar, but generally slightly inferior, to that of turbo codes. In terms of complexity, these codes may still have some advantages.

In Chapter 3, we perform a rigorous analysis of asymptotically long CA^m codes for finite m. We prove a coding theorem for these codes which states that, if the outer code has minimum distance $d \geq 2$, and the Bhattacharyya channel parameter, z, is less than some threshold z^*, then the probability of word error is $O(n^\nu)$, where n is the block length and ν is determined solely by m and d. The minimum distance of these codes is also analyzed in some detail. Finally, the performance of asymptotically long CA^m codes under iterative decoding is analyzed via density evolution.

In Chapter 4, we consider the capacity of the set of time-varying channels known as finite state channels (FSCs). A FSC is a discrete time channel whose output distribution depends both on the channel input and the underlying channel state. This allows the channel output to depend implicitly on previous inputs and outputs via the channel state. We provide a simple Monte Carlo method of estimating the achievable information rates of any FSC, and focus on the problem of estimating the capacity of FSCs with intersymbol-interference. This approach is general enough to allow the mutual information rate to be maximized over Markov input distributions of increasing length, and thus estimate a sequence of non-decreasing lower bounds on capacity. Finally, exact information rates are derived analytically for a very simple channel known as the dicode erasure channel.

In Chapter 5, we consider the joint iterative decoding of irregular low-density parity-check (LDPC) codes and channels with memory. We start by introducing a new class of erasure channels with memory, known as generalized erasure channels (GECs). For these channels, we derive a single parameter recursion for density evolution of the joint iterative decoder. This al-

lows us to give necessary and sufficient conditions for decoder convergence and to algebraically construct sequences of LDPC degree distributions which appear to approach the symmetric information rate of the channel. Finally, we discuss the construction of arbitrary GECs and some implications for more general channels.

Bibliography

[1] C. Berrou, A. Glavieux, and P. Thitimajshima. Near Shannon limit error-correcting coding and decoding: Turbo-codes. In *Proc. IEEE Int. Conf. Commun.*, volume 2, pages 1064–1070, Geneva, Switzerland, May 1993. IEEE.

[2] D. Divsalar, H. Jin, and R. J. McEliece. Coding theorems for "turbo–like" codes. In *Proc. 36th Annual Allerton Conf. on Commun., Control, and Comp.*, pages 201–210, Monticello, IL, USA, Sept. 1998.

[3] R. G. Gallager. Low-density parity-check codes. Research Monograph 21, The M.I.T. Press, Cambridge, MA, USA, 1963.

[4] C. E. Shannon. A mathematical theory of communication. *The Bell Syst. Techn. J.*, 27:379–423, 623–656, July / Oct. 1948.