Error Correcting Codes & Probability Propagation

David J.C. MacKay
Department of Physics, Cavendish laboratory, University of Cambridge

http://wol.ra.phy.cam.ac.uk/mackay/

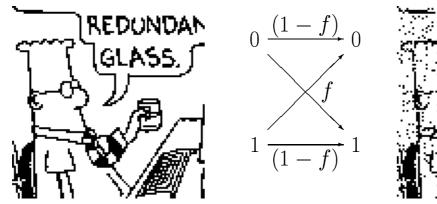
The central problem of information theory:

To achieve reliable communication over an unreliable channel.

Unreliable channels include satellite links, telephone lines, disc drives.

An idealized noisy channel:

Binary symmetric channel, noise level f = 7.5%





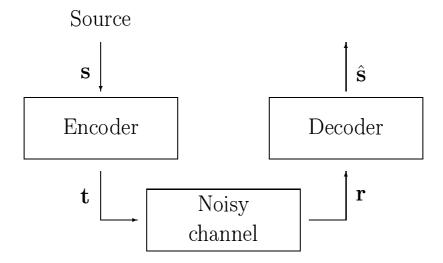
7.5% of bits are flipped

[Source image Copyright@1997 United Feature Syndicate, Inc., used with permission.]

How to achieve reliable communication?

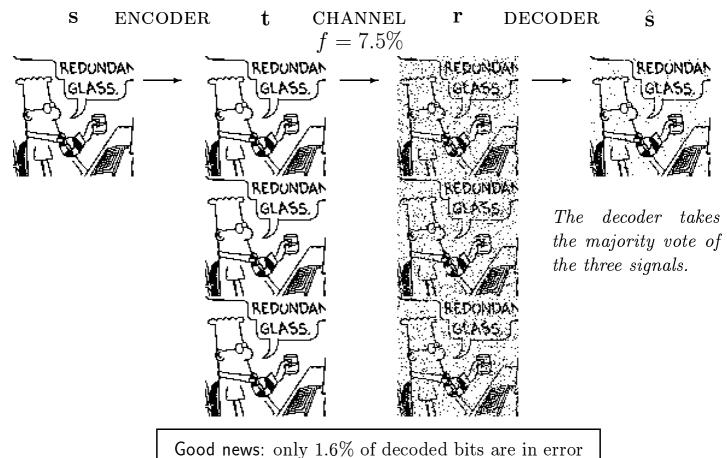
We would like to achieve virtually error-free communication. e.g., an error probability of $\sim 10^{-15}$ per bit.

The 'system' solution for achieving reliable communication



The encoding system introduces redundancy in some systematic way into the transmitted vector \mathbf{t} . The decoding system makes use of this known redundancy to deduce, given the received vector \mathbf{r} , what the noise introduced by the channel and the original source vector probably were.

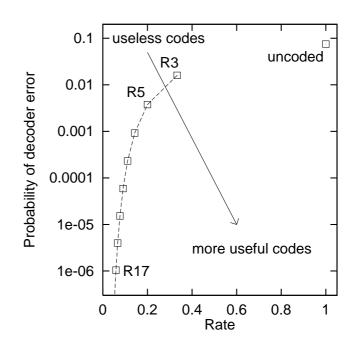
A simple encoder: add redundancy by repetition



1.070 of deceded 5165 are in error

Bad news: rate of communication reduced to 1/3

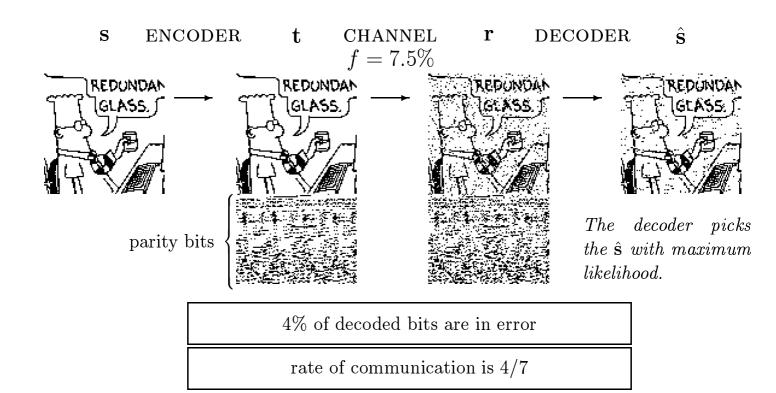
We can further reduce the error probability by repeating more times. With 17 repetitions ('R17'), the error probability is reduced to 10^{-6} . But the rate has fallen to 1/17.



A more complex encoder: The (7,4) Hamming code

Every four source bits are protected with three parity bits.

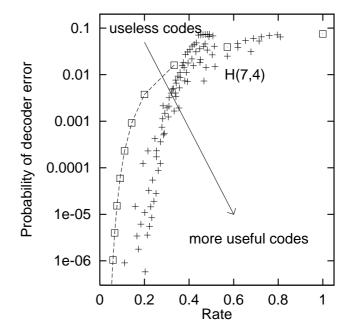
| \mathbf{s} | \mathbf{t} | \mathbf{s} | \mathbf{t} | \mathbf{s} | \mathbf{t} | \mathbf{s} | ${f t}$ | |
|--------------|--------------|--------------|--------------|--------------|--------------|--------------|----------|--|
| 0000 | 0000 000 | 0100 | 0100 110 | 1000 | 1000 101 | 1100 | 1100 011 | |
| 0001 | 0001 011 | 0101 | 0101 101 | 1001 | 1001 110 | 1101 | 1101 000 | |
| 0010 | 0010 111 | 0110 | 0110 001 | 1010 | 1010 010 | 1110 | 1110 100 | |
| 0011 | 0011 100 | 0111 | 0111 010 | 1011 | 1011 001 | 1111 | 1111 111 | |



In theory, what could the best codes achieve?

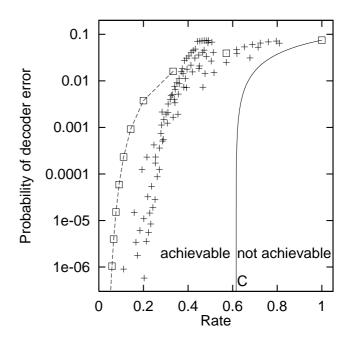
We would like small error probability and large rate.

The repetition codes, the Hamming (7,4) code, and related textbook codes (+) perform as shown here.



One might guess that the error probability can only be made very small by making the rate very small.

However, in 1948 Shannon proved the remarkable result that, for any given channel, the boundary between achievable and nonachievable points meets the R axis at a non-zero value R = C.



The practical challenge is to create error-correcting codes that get close to what Shannon proved is possible.

Low density parity check codes

Our codes are defined in terms of a very sparse matrix, \mathbf{H} , e.g.,

which is known to the encoder and decoder.

The encoding method and the decoding problem

We use encodings, \mathbf{t} which satisfy $\mathbf{H}\mathbf{t} = 0 \pmod{2}$. These consist of a source message \mathbf{s} followed by appropriately chosen parity checks. The received vector is $\mathbf{r} = \mathbf{t} + \mathbf{n} \pmod{2}$, where \mathbf{n} is the noise. The receiver knows \mathbf{H} and can compute $\mathbf{z} = \mathbf{H}\mathbf{r} = \mathbf{H}\mathbf{t} + \mathbf{H}\mathbf{n} = \mathbf{H}\mathbf{n}$. The decoding problem is then to find the sparsest vector \mathbf{x} satisfying the equation

$$\mathbf{H}\mathbf{x} = \mathbf{z} \pmod{2}$$
,

this \mathbf{x} being the best guess for \mathbf{n} . If we can find \mathbf{n} , we can find \mathbf{t} , and from that the original message.

 \mathbf{H} is very sparse, and the \mathbf{x} we are trying to find is sparse, so this problem doesn't sound intractable.

History

These codes were first studied in 1962 by Gallager, but were then generally forgotten by the coding theory community.

Theoretical result:

Low density parity check codes, in spite of their simple construction, are very good codes, given an optimal decoder.

Practical results:

We have developed two decoding strategies.

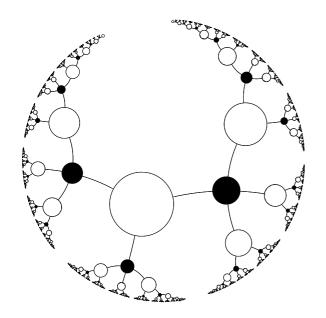
- 1: Mean field methods inspired by statistical physics and neural networks
- 2: Iterative probabilistic decoding from artificial intelligence. This is the better of the two methods.

Iterative probabilistic decoding

We attempt to solve the decoding problem

$$\mathbf{H}\mathbf{x} = \mathbf{z} \pmod{2}$$

by a message-passing algorithm called *probability propagation*. The components of \mathbf{x} and \mathbf{z} can be thought of as nodes in a graph whose edges are defined by the 1s in \mathbf{H} .



White nodes represent bits, x_l ; black nodes represent checks, z_m ; each edge corresponds to a 1 in \mathbf{H} .

On each iteration, a probability ratio is propagated along each edge in the graph, and each node x_l updates its probability that it should actually be in state 1.

If the graph were *cycle-free* then this probability propagation algorithm would generate the correct answer.

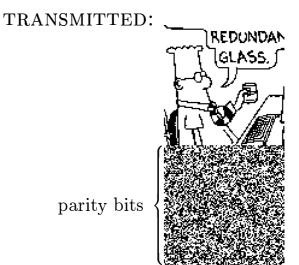
It is not cycle-free, but the algorithm still performs extremely well.

THE ENCODER

We demonstrate a large code that encodes K=10000 source bits into N=20000 transmitted bits.

Each parity bit depends on about 5000 source bits.

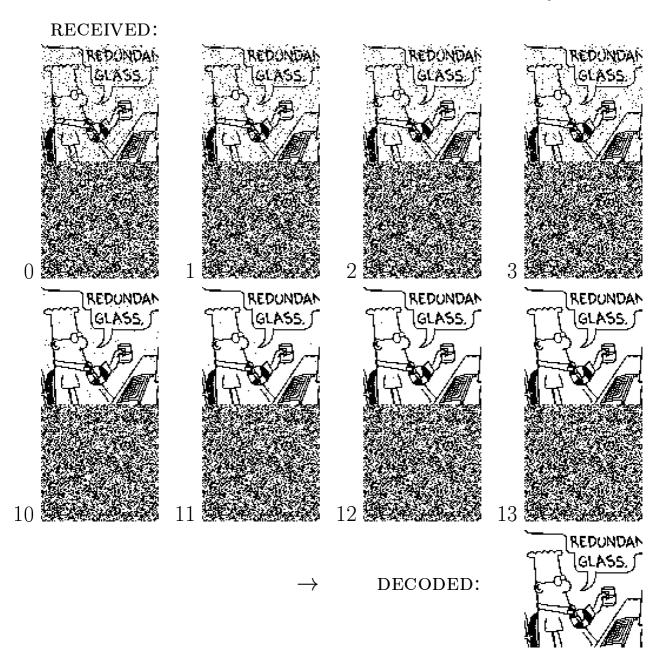
The encoder is derived from a very sparse 10000×20000 matrix **H** with three 1s per column.



| | 나라마다가 되고 하다 그는 아내가 하는 요즘 전쟁을 가지 하는 것이 하는 것도 되고 하는 것이다. 그는 그는 그는 이 요즘 맛집 안전하는 이라고 하는 것이라고 했다. 그는 |
|--------------|---|
| | 나 있는 위에 의하를 만하는 것 않는 사람이 가장 있다. 이 사람들은 사람들이 되었다고 있는 이 회사를 가장 되었다면 가장 하는 것 같은 것은 사람들이 되었다면 하는데 사람들이 되었다. |
| | 나이 되어 아들은 어머니에 그리다는 나는 경기를 하게 되어 있다면 나는 그래요? 아들이 아들이 아들이 아들아 그리다는 그 이렇게 되었다면 하는 것을 하셨다면 하는데 아들이 나를 |
| | 네트레마리 아마리아 아마리아 아마리 그 그 사람들이 하는 사람들이 있다. 그 사람이 되는 그는 그 사람이 하는 그들은 그 사람들이 살아 살아 들어 모습니다. 그 사람들이 없는 사람들은 그 사람들이 사람들이 없는 사람들이 되었다. |
| | 마트님의 하늘 생각이 들어왔다면서 아이들을 다음이다. 이 물에 가다는 그들은 하는 것은 이번 수가를 하는 것은 사람이들이 되어 하는 것이다. 그는 이 사람이 나는 사람이 나를 하는 것이다. |
| | 나는 하는데 그렇게 하는 그들의 눈을 하는데 하는데 된 사람들이 가지 않는데 하는데 하는데 그렇게 하는데 그렇게 되는 사람들이 되는데 되었다. 하는데 |
| | 나는 그 마시를 되어 다시 않는 것 같은 것이라고 있는 그 일이 있다. 하는 것은 나는 하는 것은 그는 것을 하는 것이다고 하는 것이다. 그 사이는 그는 일이다는 것이다는 것 같은 것은 |
| | 네트를 가게 하다. 아이들의 집에 가게 되었다면 그렇게 되었다면 하는데 하다 하는데 |
| | 내용이 나면 보는 나는 나는 이 사람들은 사람들이 가장 하는 사람들이 하는 것들이 하는 것은 사람들이 가장 하는 것을 하는 것이 되었다. 그는 것이 불러를 받는 것은 모든 사람 |
| | 나 마늘이 되는 어느에 어려움을 가는데 되어 가능한 수가 하는 이 가능을 모르게 하는 것이 아무리를 하는데 그 아이들은 이 등 사람들이 되고 하는데 되었다. 그는 사람들이 아이들이 다른데 나를 다 하는데 |
| | 내용한 가는 이번 전에 대통점을 위해 있다. 이번에 대한 경험 등에 하는 사람들의 하다고 있는데 이번 사람이 가장 그렇게 하는 것이라고 있는데 얼마를 하는데 하다고 있다. 그렇게 하는 그 없는데 하다 |
| | 나는 그 이 아이들은 하다 이 맛이 하는 것으로 나타지는 것이 나를 하는 하다가 하는 것이 되는 것은 사람들이 되었다. 그는 것이 가는 것은 그들은 그를 가지 않는데 그는 것이 하는 것이 없다. |
| | 나는 하는 동생에게 되었는 그의 역사는 중에게 가지만 그렇게 되었다. 나는 하는 동생님들은 생각이 되는 사람들은 수가 가지만 하지 않는 눈으로 가지 않는 것이다. |
| | 내가 가능하는 경우 이번 수 있는 것 같아. 이번 가는 이 이 이번에 되었는데, 이 사람이 되었다는 사람이 되었다면 하는데 이번 수 있었다. 그는 이 점점 하는데 이번 때문에 되었다. 그는 것이다. |
| | 나가 하는 것은 것은 이 그는 것 같아요. 그는 것 같아요. 그는 것은 것은 사람들이 하는 것은 것은 것이 되었다. 그는 것은 것이 되는 것은 것이다. |
| | 대비적이 되는 전문 전문 이번 시간을 하는 사람들이 되는 전략들이 되었다. 그 등 생각이 되는 사람들이 가장 하는 그렇게 하는 것이 되었다. 그 모양을 모양하고 하는 것들은 이 사람들이 되었다. |
| | 나는 보는 하는 등 들어가 된 것은 이번 회에는 생각을 하는 것을 가장 하는 것을 받는 것이다. 학생들은 이번 등에 가는 사람들은 가능한 경에 되었다면 하는 것을 하는 것이다. |
| | 나는 아직도 사람들이 하는 이 교육 사람들이 되는 이 경상에 하는 사람들이 되었다. 그렇게 하는 것은 아이를 하는 것이 되었다. 그는 사람들이 아이를 가지 않는데 그렇게 하다. |
| | 나타는 방문화를 하는 사용하는 사람들이 되었다. 그리는 사용을 하는 사람들이 살아내려면 하는 사람들이 가는 사용을 하는 사람들이 가지 않는 것은 사람들이 되었다. 그렇게 되었다면 다른 사람들이 되었다면 다른 사람들이 되었다면 하는 사람들이 되었다면 다른 사람들이 되었다면 되었다면 다른 사람들이 되었다면 다른 사람들이 되었다면 되었다면 다른 사람들이 되었다면 다른 사람들이 되었다면 되었다면 되었다면 되었다면 되었다면 되었다면 되었다면 되었다면 |
| | 나이 사람들이 어느를 하면 할 때 때문에 가장 가는 얼굴한 그들이 가까? 하는데 그리면 하는데 되어 가장되었다. 그들은 그 이렇게 이 말씀이 되었다. |
| | 나는 마시트 아들은 사람들은 그들은 그리고 있다. 그리고 아들은 사람들은 사람들은 사람들은 사람들은 사람들은 사람들은 사람들은 사람 |
| | 내가 하고 말하다 말하는 것이 많은 그는 항상하는 그리지는 다른 사람들이 그는 아이들이 그는 그들은 그리고 하는 것이 되는 것이다. 그는 사람이 시원하는데 그 사람이 하는 것이다. |
| | 나는 이 화장한 이번 그 없는 그를 가는 경기에 있는데 소문하는 아이들은 그리고 하는데 하는데 하는데 하는데 되는데 하는데 하는데 이번 하는데 이번 사람들은 이번 수를 받는다. |
| | 나는 사람들은 이번 사람들이 하는 이번 사람들은 살아가는 살아가는 살아가는 살아가는 사람들이 되었다. 그는 사람들은 사람들이 가는 살아가는 살아가는 살아가는 사람들이 되었다. |
| | 나이트 그들은 회문을 하는 아무리, 하늘 마음하는 그 아마마 아무리는 이들을 하는 것이 되는 것이 하셨다는 것 같은 것이 되었다. 아마를 다양하는 아무리를 다양한다. |
| | 내용에 그렇게 하면 하는 사람들은 그렇게 하면 사람들이 하는 것이다. 그는 아이들은 사람들은 그리를 하는 것이다. 그런 사람들은 그는 사람들이 나를 가장하는 것은 것이다. |
| | 나는 그리트를 하는 점점 마음이는 그는 하는 하는 하는 이름을 살아내려 하라는 살아내는 것이 하는데 이렇게 하는데 |
| | 내는 사가 다양했다. 이 집에 이 나는 이 아이를 가는 어려면 하는 사람들이 살아가 하는 생각이 되었다. 그는 사람들은 그는 사람들은 사람들은 그를 가게 되었다. |
| | 나는 그 장에 가는 사람들에게 하면 되는 것이 되었다. 살아는 것이 나를 하는데 되는 것이 되는 것이 없는데 그들은 것이 되었다. 그 가게 하면 되는 것이 없는데 하면 없다는 것이 없다. |
| | 네트트로 하다는 그는 그는 이렇게 되는 사람들이 되고 하고 있다면 하다면 하는 것이 되었습니다. 나는 그렇게 하는 사람들이 하는 사람들이 되는 것이라고 있어요? 그는 그 사람들은 생각은 |
| | 나는 이번 이렇게 보는 그 사람이 많은 가득하게 되는 것 같아. 하는데 가장하게 되는데 이렇게 되었다. 그 사람들이 모든 하는데 되었다. 그렇게 되었다. 그렇게 되었다. 그 없는데 그렇다는데 하다. |
| \mathbf{H} | 나는 이 그는 일반에 가장이 되었다. 그는 이 사람들은 이번 사람들은 사람들은 사람들이 되는 사람들이 되었다. 이 사람들은 사람들은 사람들이 가지 않는 것이 되었다. |
| | 나는데 마리트리 아이들 아이들 아이들 살아보다 하는 사람이 되었다. 그리고 있는 것 같은 사람들은 사람들은 사람들이 가지 않는데 가지 않는데 사람들이 다른 사람들이 되었다. |
| | 나들은 그렇게 얼굴하는 물론은 경험점이 가면 되는데 이번을 걸었다면까지 교육하는 이번을 하는데 되는데 되는데 되었다. 그리고 화학을 하게 하는데 이번 그를 살아가 하다면 모든 바다 |
| | 내용하는 어느리 그들은 그를 가장 이 이름을 가지고 주었다면 되었다는 아는 아느라는 그들은 이 없이는 물이 되고 말했다. 사이를 가장 모임이 느껴지는 어머니 이번 다른다. |
| | 나는 그가 그렇는 내 시간에 그리는 경기는 가지도 되어 뭐야 하면서 시간에 가지를 하는 것들이 하는 사람이 모든 사람이라면 하는 사람이 되고 있다. 사람이 되어 되었다. |
| | 나는 사람들이 있었다. 그렇게 되어야 하면 하는 이 남자들이 하는데 하고 되었다. 그 나는 사람들이 하는데 그는 사람들이 하는데 그는데 하는데 하는데 나를 하는데 |
| | 나 그는 그 이 내가 들어들어 그는 내는 그들은 점점을 가는 것을 하면 하는 것이 되었다. 그는 그는 사람들은 그는 사람들이 들었다. 그는 사람들이 하는 사람들이 얼굴하는 것은 |
| | 네트, 마이크레 등이 이 나이에, 얼굴 살으면 그리고 있는 아름이 어떻게 되었다. 이 그리다 하는 그리고 하는 아름다는 이 사람들이 살아 있다. 그리고 하는 아름이 어디어 아름다면 없다. |
| | 내용하는 이 방문 보고 있다. 아버지는 아니라 살아 이번 수 있는데 이렇게 모르고 있다. 아버지는 아버지를 하는데 생각하는 사람이 없는데 되는데 하는데 하는데 하는데 하는데 나를 다 되었다. |
| | 나왔다. 회사들에는 전문에는 학생에 가격되다. 나는 이 경험을 하는 학생들이 나를 가장하는 것이 없는데 가는 사람들이 본 사라들은 학생들은 학생들은 학생들이 들어왔다. |
| | 내가 가면 하면, 그는 그는데 나는데 하는데 된다면 하면 하면 하면 나는 그래요? 그리는 그는 그는 그들은 아무리를 하는데, 그는데 하면 모든데 나는데 그는데 하는데 하는데 하는데 하는데 하는데 하는데 하는데 하는데 하는데 하 |
| | 내가, 마음이 나는 생님들 생각에 가면 내려가는 남으로 가는 데이 물에 살 먹었다. 그들은 뭐 되어 되어 하면서 하다 되어 하면 없을 때문에 되어 되어 들었다. |
| | - 마음과 제도 어려면 하는 이 나는 이 의과 항문이 모든데 모든데 모든데 나는데 하나 그리고 되는데 그렇게 하다면서 그런데 하다면서 그런데 가는데 그리고 하는데 그리고 그리고 하는데 그리고 그리고 하는데 그리고 그리고 그리고 하는데 그리고 |
| | 네이트 사람이 아이는 사람들은 동안들이라고 이렇게 되는 사람들은 학교 회사의 그는 사람들은 사람들이 가는 사람들이 어떤 사람들이 가는 사람이 되는 사람이 사람들이 하는 것이다. |
| | 나 한다리는 아이들 중에서 하는 이번 하는 것들은 것이다. 나는 사람들이 되고 있다면 그렇게 하는 사람들이 되는 것이다. 그는 그들은 사람들이 되는 것이다는 것이다. 그렇게 되었다면 하는 사람들이 없다. |
| | 나이다고 그들은 아이들 이 그는 아이들이 들어 하는 것이 되었다. 이 이 등에 들어 보고 있는데 그 그 그 그는데 그를 내려가 되었다면 하는데 이 사람들이 되었다. 그 없는데 그를 다 먹었다. |
| | 나의 나는 가는 이 그릇이 되어 있다면 하지만 하지만 하지만 하지만 하면 되는 것이 되었다. 그는 것이 되었다는 사람들이 하지만 하는데 가는 것이다. 그는 것이라고 하는데 되었다. |
| | 내용하다 마이트를 가장 보다는 그렇게 그렇게 되는 그들은 이제 그는 그리는 이번 그리고 있는 아름다고 되었다. 그는 이번 살아 그는 아이를 가장하다는 그리고 싶는데, 이트를 하다 하다. |
| | 나는 가능한 그 가는 것으로 가는 것으로 가는 것을 가는 것을 가는 것이 되었다. 그는 것이 없는 것은 것은 것으로 가는 것으로 가는 것이 없는 것이 없는 것이다. 그는 것이 없는 것은 것이다. 그 사람들이 없는 것은 것이다. |
| | 네트 나는 것이 되었다. 전체 이 어머니를 모르는 그들은 아이는 것이 하는 사람들은 그렇지만 사람들이 그리는데 그리는데 그리를 하고 하는데 다른 사람들이 되었다. |
| | 나라 한 것 같다. 사람들은 것 이 작가에 살아왔다면 나는 이 사람들이 되었다. 아니라는 나는 아니라 얼마를 그리고 하는 것은 그는 사람이 되었다. 그는 사람이 나를 하는 것은 사람들이 없다고 있는 생각이 되었다. |
| | 나보는 강에는 이번도 하지 않는 그의 그는 전에 되어 하는데 아이를 가장 하는데 되었다. 그림에 하지만 이번 이번 사람이 되었다는 사람이 되었다. 아이를 하는데 하게 되었다. 그리고 있다. |
| | 마하다 하다면 회사에는 하나 회에는 사람이 가득하고 하는데 하는데 하는데 하고 있다. 그런데 하는데 하는데 하는데 하는데 하는데 하는데 나는데 그렇다 하는데 하다고 하는데 |
| | #DEST 등 이번 경제 보고있다. 그 전에 논리를 주는 때문에 가장 하는 경기자들은 이번 보고 하지만 하는 것이다. 그는 그리고 하는 이번 사람들이 함께 가장 함께 되고 있다. |
| | · Port Street (Street Performance Perform |
| | - POS 프로그램 - MOS - MOS - IN INTEREST - |
| | · Propriese (Several of the Control of the Several of Control of the Control of the Several of Control of Control of the Control of the Control of Contro |
| | 나는 그는 그 사람이 많은 그릇을 가는 것을 가려면 하면 그녀를 하다면 그렇다. 하는 이 하는 그 생생이는 그 나는 것은 것 같아야 하는 것이 말을 하는 것이다. 그렇게 모양하는 그 사람이다. |
| | 네트로 하다는 것이 있는 것이 그렇게 얼마를 하는 것이 되었다면 하는 생각이 되었다면 하는 것으로 살아왔다면 되었다면 생각이 얼마를 하는데 모든 것이 되었습니다. 이 사람들은 사람이 되었다면 하는데 |
| | |

Iterative decoding

After the transmission is sent over a channel with noise level f = 7.5%:

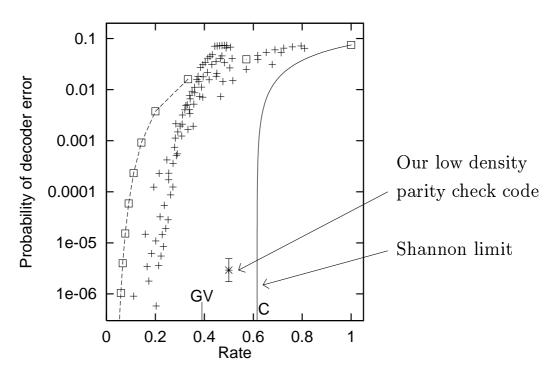


This final decoding is error free.

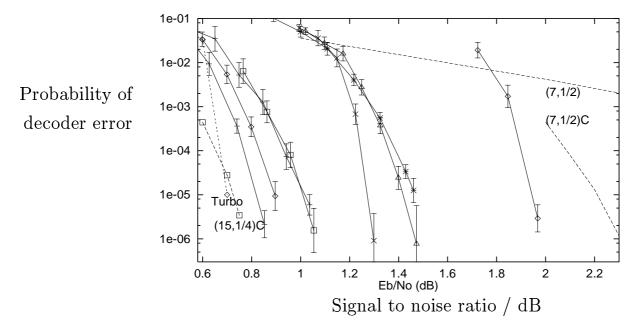
In the case of an unusually noisy transmission, the decoding algorithm fails to find a valid decoding. For this code and a channel with f=7.5%, such failures happen about once in every 100,000 transmissions.

These codes outperform textbook codes by a substantial margin.

Results for binary symmetric channel with f = 7.5%



Results for Gaussian channel



Shannon limit is off the left side of the figure.

Solid lines: low density parity check codes.

Dotted lines (right): textbook codes as used in satellites and the Voyager spacecraft.

Dotted lines (left): state of the art codes: 'Turbo' codes and 'Galileo' code (15,1/4).

Improving Gallager Codes

- Clump bits and checks together

Also known as...

Generalize to other finite fields GF(q)

Our original work on low density parity check codes used ordinary binary arithmetic, known as 'GF(2)'. The addition and multiplication tables for GF(2) are:

$$\begin{array}{c|ccccc} + & 0 & 1 & & \cdot & 0 & 1 \\ \hline 0 & 0 & 1 & & & 0 & 0 & 0 \\ 1 & 1 & 0 & & & 1 & 0 & 1 \end{array}$$

We can also define error-correcting codes using the addition and multiplication tables of other finite fields, for example GF(4):

| + | 0 | 1 | A | B | | • | 0 | 1 | \boldsymbol{A} | B |
|------------------|---|---|---|---|---|------------------|---|------------------|------------------|---|
| 0 | 0 | 1 | A | B | • | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | B | A | | 1 | 0 | 1 | \boldsymbol{A} | B |
| \boldsymbol{A} | A | B | 0 | 1 | | \boldsymbol{A} | 0 | \boldsymbol{A} | B | 1 |
| B | B | A | 1 | 0 | | B | 0 | B | 1 | A |

We define low density parity check matrices using elements of GF(4), and translate our binary messages into GF(4) using, for example:

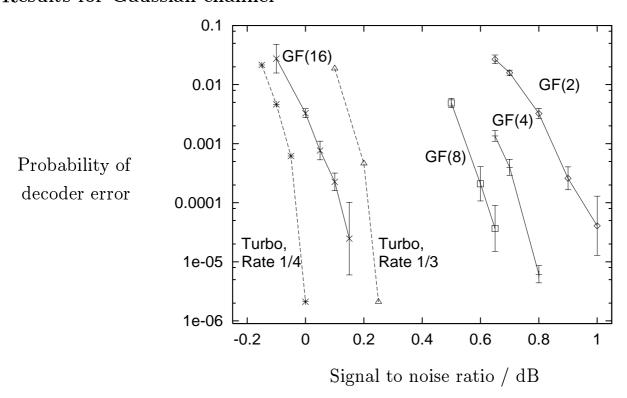
$$\begin{array}{ccc} \text{binary} & \leftrightarrow & GF(4) \\ \hline 00 & \leftrightarrow & 0 \\ 01 & \leftrightarrow & 1 \\ 10 & \leftrightarrow & A \\ 11 & \leftrightarrow & B \end{array}$$

Results

The resulting codes over GF(4), GF(8), GF(16), ..., when decoded with the iterative probabilistic decoder, perform nearly one decibel better.

The computational cost for working in GF(q) scales as q^2 .

Results for Gaussian channel



Shannon limit is off the left side of the figure.

Solid lines: low density parity check codes.

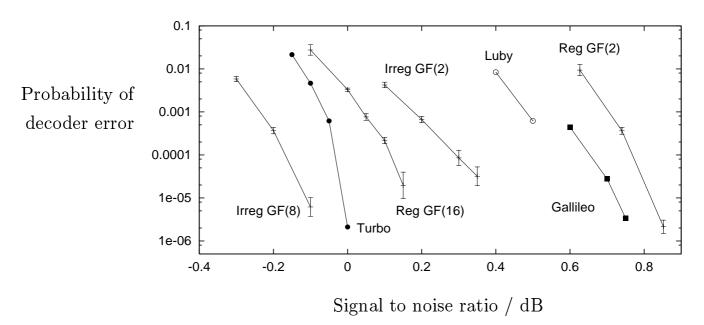
Dotted lines: JPL's latest 'Turbo' codes.

Improving Gallager Codes II

- Make the graph irregular

Luby et al showed that irregular constructions work better. The best graphs have irregular node connectivity and regular check connectivity.

Combining these two ideas (irregular graphs, and grouping nodes together), Matthew Davey produced the best known code of rate 0.25.



Conclusion

The state of the art solution to the communication problem is:

Combine a simple, **pseudo-random** code with an approximate **probability-based** decoder.

References

- BERLEKAMP, E. R., MCELIECE, R. J., and VAN TILBORG, H. C. A. (1978) On the intractability of certain coding problems. *IEEE Transactions on Information Theory* 24 (3): 384–386.
- Berrou, C., and Glavieux, A. (1996) Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Transactions on Communications* 44: 1261–1271.
- CHUNG, S.-Y., URBANKE, R. L., and RICHARDSON, T. J., (1999) LDPC code design applet. http://truth.mit.edu/~sychung/gaopt.html.
- DAVEY, M. C., and MACKAY, D. J. C. (1998) Low density parity check codes over GF(q). *IEEE Communications Letters* **2** (6): 165–167.
- Davey, M. C., and Mackay, D. J. C. (2000) Watermark codes: Reliable communication over insertion/deletion channels. In *Proceedings 2000 IEEE International Symposium on Information Theory*, p. 477.
- DIETTERICH, T., and BAKIRI, G., (1991) Error-correcting output codes: A general method for improving multiclass inductive learning programs. In Proceedings of the Ninth National Conference on Artificial Intelligence (AAAI-91), pages 572–577. AAAI Press, 1991.
- DIVSALAR, D., JIN, H., and MCELIECE, R. J. (1998) Coding theorems for 'turbo-like' codes. In *Proceedings of the 36th Allerton Conference on Communication, Control, and Computing, Sept. 1998*, pp. 201–210, Monticello, Illinois. Allerton House.
- Forney, Jr., G. D. (1966) Concatenated Codes. Cambridge, Mass.: MIT Press.
- FREY, B. J. (1998) Graphical Models for Machine Learning and Digital Communication. Cambridge MA.: MIT Press.
- Gallager, R. G. (1962) Low density parity check codes. IRE Trans. Info. Theory IT-8: 21-28.
- Gallager, R. G. (1963) Low Density Parity Check Codes. Number 21 in Research monograph series. Cambridge, Mass.: MIT Press.
- Gallager, R. G. (1968) Information Theory and Reliable Communication. New York: Wiley.
- GOLOMB, S. W., PEILE, R. E., and SCHOLTZ, R. A. (1994) Basic Concepts in Information Theory and Coding: The Adventures of Secret Agent 00111. New York: Plenum Press.
- Luby, M. G., Mitzenmacher, M., Shokrollahi, M. A., and Spielman, D. A. (1998) Improved low-density parity-check codes using irregular graphs and belief propagation. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 117.
- Mackay, D. J. C. (1995) Free energy minimization algorithm for decoding and cryptanalysis. *Electronics Letters* **31** (6): 446–447.
- MACKAY, D. J. C., (1997) Iterative probabilistic decoding of low density parity check codes. Animations available on world wide web. http://wol.ra.phy.cam.ac.uk/mackay/codes/gifs/.

- Mackay, D. J. C. (1999) Good error correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory* **45** (2): 399–431.
- MACKAY, D. J. C., and DAVEY, M. C. (2000) Evaluation of Gallager codes for short block length and high rate applications. In *Codes, Systems and Graphical Models*, ed. by B. Marcus and J. Rosenthal, volume 123 of *IMA Volumes in Mathematics and its Applications*, pp. 113–130. New York: Springer-Verlag.
- MACKAY, D. J. C., and NEAL, R. M. (1995) Good codes based on very sparse matrices. In *Cryptography and Coding. 5th IMA Conference*, ed. by C. Boyd, number 1025 in Lecture Notes in Computer Science, pp. 100–111. Berlin: Springer.
- MACKAY, D. J. C., and NEAL, R. M. (1996) Near Shannon limit performance of low density parity check codes. *Electronics Letters* **32** (18): 1645–1646. Reprinted *Electronics Letters*, **33**(6):457–458, March 1997.
- Mackay, D. J. C., Wilson, S. T., and Davey, M. C. (1998) Comparison of constructions of irregular Gallager codes. In *Proceedings of the 36th Allerton Conference on Communication, Control, and Computing, Sept. 1998*, pp. 220–229, Monticello, Illinois. Allerton House.
- MCELIECE, R. J. (1977) The Theory of Information and Coding: A Mathematical Framework for Communication. Reading, Mass.: Addison-Wesley.
- MCELIECE, R. J., MACKAY, D. J. C., and CHENG, J.-F. (1998) Turbo decoding as an instance of Pearl's 'belief propagation' algorithm. *IEEE Journal on Selected Areas in Communications* **16** (2): 140–152.
- Pearl, J. (1988) Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. San Mateo: Morgan Kaufmann.
- Shannon, C. E. (1948) A mathematical theory of communication. Bell Sys. Tech. J. 27: 379–423, 623–656.
- Spielman, D. A. (1996) Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory* **42** (6.1): 1723–1731.
- SWANSON, L. (1988?) A new code for Galileo. In *Proc. 1988 IEEE International Symposium Information Theory*, pp. 94–95.
- TANNER, R. M. (1981) A recursive approach to low complexity codes. *IEEE Transactions on Information Theory* 27 (5): 533–547.
- URBANKE, R., RICHARDSON, T., and SHOKROLLAHI, A., (1999) Design of provably good low density parity check codes. Submitted.
- Wiberg, N., (1996) Codes and Decoding on General Graphs. Dept. of Electrical Engineering, Linköping, Sweden dissertation. Linköping studies in Science and Technology. Dissertation No. 440.
- WIBERG, N., LOELIGER, H.-A., and KÖTTER, R. (1995) Codes and iterative decoding on general graphs. *European Transactions on Telecommunications* **6**: 513–525.