Spin-glass error-correcting codes with quantum decoding

Ching-Yi Lai and Yicong Zheng

Electrical Engineering Department
University of Southern California

April 26, 2012
Outline

1 Error-Correcting Codes
2 The Spin-Glass Code on the D-Wave Chip
3 BCH Codes
4 Simulation
5 Shortened Codes
6 Conclusion
Definition: An \([n, k, d]\) binary linear block code \(C\) is a \(k\)-dimensional subspace of all binary \(n\)-tuples \(\mathbb{Z}_2^n\) such that any two \(n\)-tuples in this code differ in at least \(d\) bits.

d is called the *minimum distance* of the linear code.

We can choose a basis of the codespace: \(\{g_1, g_2, \cdots, g_k\}\).

The matrix

\[
G = \begin{bmatrix}
-g_1 \\
-g_2 \\
\vdots \\
-g_k
\end{bmatrix}
\]

is called the *generator matrix* of the code \(C\). \(C\) is the rowspace of \(G\).

A \(k\)-bit information \(u = a_1 \cdots a_k\) is encoded into a codeword \(x \in C\) by

\[
x = uG = a_1 g_1 + a_2 g_2 + \cdots + a_k g_k.
\]
The orthogonal space of $C$, under the usual inner product of binary vectors, is an $[n, n-k]$ code space, and is denoted by $C^{\perp}$.

Denote the generator matrix of the orthogonal code $C^{\perp}$ by $H$.

A legal codeword $x \in C$ has to satisfy

$$Hx^T = 0.$$ 

Then we have

$$HG^T = O.$$ 

$H$ is called the parity-check matrix of the code $C$. 

The D-Wave chip corresponds to a specific 2-dimensional Ising model of 128 qubits.

Only 108 of the 128 qubits are working qubits.

255 pairs of qubits are coupled.
Let $i_1, \ldots, i_{108}$ be the numbers of the working qubits and we denote these working qubits by $s_{i_1}, \ldots, s_{i_{108}}$ and assume they carry classical messages:

$$s_{i_m} \in \{\pm 1\}.$$

Let $E$ denote the edge set

$$\{ (a, b) : s_a \text{ and } s_b \text{ are coupled} \},$$

and $|E| = 255$.

If two qubits $s_a$ and $s_b$ are coupled, the parity of $s_a$ and $s_b$ is encoded in the “edge” $J_{a,b}$:

$$J_{a,b} = s_a s_b.$$

Map $+1, -1$ to $0, 1$, respectively. This is equivalent to a linear block code.
The spin-glass code has a $108 \times 255$ generator matrix $G'$ such that each column is of weight 2.

Suppose $x = s_{i_1} \cdots s_{i_{108}}$ is a message string. Let $\bar{x} = (-s_{i_1}) \cdots (-s_{i_{108}})$. It can be observed that $x$ and $\bar{x}$ are encoded to the same codeword, since

$$J_{a,b} = s_a s_b = (-s_a)(-s_b)$$

for any $(a, b) \in E$.

The spin-glass code is equivalent to a $[255, 107]$ low-density generator matrix (LDGM) code.
A code $C$ is cyclic if it is linear and any cyclic shift of a codeword is also a codeword.

If $(c_0, c_1, \cdots, c_{n-1}) \in C$, $(c_1, c_2, \cdots, c_{n-2}) \in C$.

Let $c(x) = c_0 + c_1 x + \cdots c_{n-1} x^{n-1}$ denote a codeword $(c_0, c_1, \cdots, c_{n-1}) \in F^n$, where $F = GF(q)$.

A cyclic code $C$ is an *ideal* of $R_n = F[x]/(x^n - 1)$:
- If $c(x) \in C$, then $r(x)c(x) \in C$ for any $r(x) \in R_n$.
- $C = \langle g(x) \rangle$ for some generator polynomial $g(x)$. 

A cyclic code of length \( n \) over \( GF(q) \) is called a BCH code with designed distance \( \delta \) if one of its generator polynomial is of the form

\[
g(x) = \prod_{i \in K} (x - \alpha^i).
\]

\( \alpha \) is a primitive \( p \)-th root of unity

\( K = C_b \cup \ldots \cup C_{b+\delta-2} \) is the defining set of the code

\( C_s = \{ q^i \mod n \mid i \in K \} \) is the cyclotomic coset \( \mod n \) over \( GF(q) \) containing \( s \).

If \( n = q^m - 1 \) for some \( m \), it is called primitive. If \( b = 1 \), it is called a narrow-sense BCH code.
A comparable binary BCH code of $n = 255$ and $k = 107$ is a $[255, 107, 45]$ primitive binary BCH code.

Decoder: Berlekamp-Massey decoding algorithm (implemented in MATLAB)

The $[255, 107, 45]$ can be cyclicly generated by the following vector:

```
100000000000000000000000000000000000000
000000000000000000000000000000000000000
000000000000000000000000000001000010010
01101100000101111001111101011111000000
10001111001110101110010000110111100
01010100110011101010100110110000100101100
101111111010000100100,
```

which is found by MAGMA.
Bit Error Rate (BER) over Binary Symmetric Channel (BSC)

- Assume the noise channel is the binary symmetric channel (BSC) with bit-flip rate $p$.
- The channel capacity of a binary symmetric channel is
  \[ C = 1 - H(p), \]
  where $H(p) = -p \log p - (1 - p) \log(1 - p)$.
- Code rate $R = 107/255$.
- WLOS, we can assume that the all-zero vector is sent every time.

\[
\text{BER} = \frac{\text{sum of the weight of information bits}}{\text{total number of information bits}}.
\]
Classical analysis

For $R = \frac{107}{255}$, it is better doing error-correcting codes than without error correction when $p < 0.1385$.

BCH code is better for $0 < p < 0.06$. 
Simulation Environment

- classical local solver
- num_programming_cycle = number of times setting coupling coefficients and magnetization field = 100
- num_reads = number of quantum annealing for each = cycle 5
- number of noise sample = 60
Ground Space is in general highly degenerated

We need to find all the ground state, in order to find the one with minimum weight, otherwise it introduces additional decoding error

In classical case, we should run enough cycles to ensure all ground states has been found

However, in quantum annealing algorithm, it doesn’t guarantee running enough cycles can find all ground states
Input arbitrary random string
Input all zeroes string and arbitrary random string

Reason?
What if modified the topology of the chip?

- Eliminate edges on the graph just reduces the number of $N$, thus makes code worse
- Eliminate specified qubits and edges connected to them. (Reduce N and K simultaneously.)
- Qubits with small number of edges may affect the performance more than the others.
Shortened Codes

- This spin-glass code has a codeword of weight 1. This is because the qubit 28 is only coupled to one qubit (32).
- The qubit has two edges on the chip:
  - qubit 26, to qubit 32 (3 edges) and qubit 58 (5 edges)
  - qubit 27, to qubit 32 (3 edges) and qubit 59 (5 edges)
  - qubit 93, to qubit 85 (6 edges) and qubit 89 (6 edges)
  - qubit 94, to qubit 86 (6 edges) and qubit 89 (6 edges)
  - qubit 95, to qubit 87 (6 edges) and qubit 89 (6 edges)
  - qubit 96, to qubit 88 (6 edges) and qubit 89 (6 edges)
  - qubit 127, to qubit 121 (4 edges) and qubit 123 (3 edges)
Shortened Codes

- Remove qubit 28
- qubits 28 and 93
- qubits 28 and 94
- qubits 28 and 95
- qubits 28 and 96
- qubits 28, 93 and 94
- qubits 28, 93 and 95
- qubits 28, 93 and 96
- qubits 28, 94 and 95
- qubits 28, 94 and 96
- qubits 28, 95 and 96
- qubits 28, 89, 93, 94, 95, and 96
- Remove qubit 28
Remove qubit 28 and 95
Remove qubit 28 and 96
Remove qubit 28, 93, and 94.
Remove qubit 28, 93, and 95
Remove qubit 28, 93, and 96
Remove qubit 28, 94, and 95
Remove qubit 28, 94, and 96
Remove qubit 28, 95, and 96
Remove qubit 28, 89, 93, 94, 95, and 96
Future Work

- Check the performance of D-Wave Decoder
- Whether the performance of quantum decoder is better than the classical decoder of this spin glass code?
- The spin-glass code is equivalent to a LDGM code with a generator matrix of all weight-2 columns. How to couple pairs of qubits such that the equivalent LDGM code is good?
- Is it possible to find a shortened code with good error-correcting ability from this spin-glass code?