More Sparse-Graph Codes for Quantum Error-Correction

David J.C. MacKay
Cavendish Laboratory, Cambridge, CB3 0HE.
mackay@mrao.cam.ac.uk

Graeme Mitchison
M.R.C. Laboratory of Molecular Biology, Hills Road, Cambridge, CB2 2QH.
gjm@mrc-lmb.cam.ac.uk

Amin Shokrollahi
EPFL
amin.shokrollahi@epfl.ch

June 15, 2007 – draft 1.21

Abstract

We use Cayley graphs to construct several dual-containing codes, all of which have sparse graphs. These codes' properties are promising compared to other quantum error-correcting codes.

This paper builds on the ideas of the earlier paper *Sparse-Graph Codes for Quantum Error-Correction* (quant-ph/0304161), which the reader is encouraged to refer to.

To recap: Our aim is to make classical error-correcting codes with practical potential for quantum error-correction. The rules of the game for classical binary codes are: (1) each code must be defined by a sparse graph (so that the circuit for computing the syndrome is simple, and so that we have the chance of getting good decoding with a low-complexity decoder); (2) the classical code must contain its own dual; equivalently, every row of the parity check matrix must be a codeword; equivalently, any two rows of the parity check matrix must have even overlap. (3) the code must have rate greater than 1/2.

While struggling to make codes satisfying these constraints, we formulated two mutually-exclusive conjectures

Conjecture G: Any dual-containing code defined by an $M \times N$ parity check matrix $\mathbf{H}$ with $M < N/2$, all of whose rows have weight $\leq k$, has codewords of weight $\leq k$ that are not in the dual.

Conjecture D: There exist dual-containing codes with sparse parity-check matrix and good distance. To be precise, such codes would have a parity-check matrix with maximum row weight k, and for increasing blocklength N the minimum distance d of codewords not in the dual would satisfy $d \propto N$.

In this paper we present some more algebraic constructions of binary codes that contain their duals. These codes have the nice property that their sparse parity check matrices have many redundant rows. (These redundant rows allow enhanced decoding performance.) We have found codes that are counterexamples to Conjecture G.

1 Cayley-graph construction of a parity-check matrix

Given a set of k generators of a group of size N, we can make a bipartite graph with N vertices on each side and degree k by putting an edge from each group element (vertex on the left) to each group element (vertex on the right) that can be reached by applying one of the generators. If the inverses of the generators are in the set of generators, if the group is abelian, and if k is even, then the graph will be symmetric and will define a square parity-check matrix with the property that the overlap between any two rows is even. This will thus define a code that is dual-containing.

An example. Throughout this paper, N will be a power of 2 ($N = 2^n$), and the group elements are the set $\{0,1\}^n$. Our method is easiest to describe if we number our vertices from 0 to $N-1$. A vertex (described by an integer in (0,$N-1$)) should be thought of as defining a binary string of length n.

```
    Input: A set of k integers g_1 ... g_k (the generators)
1. Create an N x N matrix consisting of zeros.
2. for n = 0 ... N-1 do
       for g in {g_1 .. g_k} do
          set entry [n, n^g] to 1   (where ^ denotes exclusive or)
```

2 Detailed Example

Some generators. d^* denotes lowest weight of word not in dual.

Code name	Generators	k	N	M_{true}	K	R	d^*
PARITY128.8	1, 2, 4, 8, 16, 32, 64, 127	8	128	56	72	0.5625	8
PARITY512.10	1, 2, 4, 8, 16, 32, 64, 128, 256, 511	10	512	240	272	$\simeq 0.53$	**16**
PARITY2048.12	1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2047	12	2048	992	1056	$\simeq 0.516$	32??
QR1.512.18	1, 2, 4, 9, 19, 39, 78, 156, 313, 114, 228, 456, 400, 288, 64, 128, 256, 511	18	512	240	272	$\simeq 0.53$	32??
GOLAY4096.24	1, 3, 6, 12, 24, 49, 99, 199, 398, 797, 1594, 3189, 2282, 468, 936, 1872, 3744, 3392, 2688, 1280, 2560, 1024, 2048, 4095	24	4096	1472	2624	$\simeq 0.64$	??

```
# weight enumerator of the (128, 16) subcode whose nonzero words are not in the dual
#     w    A(w)   Cumulative value (sum A(w))
      0       1       1
      8      54      55
     12     108     163
     14     216     379
     16     837    1216
     18      24    1240
     20    2916    4156
     22    5832    9988
     24    5832   15820
     26   12312   28132
     28   17496   45628
     30   12960   58588
     32    5508   64096
     34    1296   65392
     36     144   65536
```

3 Performance

The Golay-derived code seems the most interesting. Its rate is biggest. At a flip probability of 0.025, the block error probability is 5×10^{-5}.

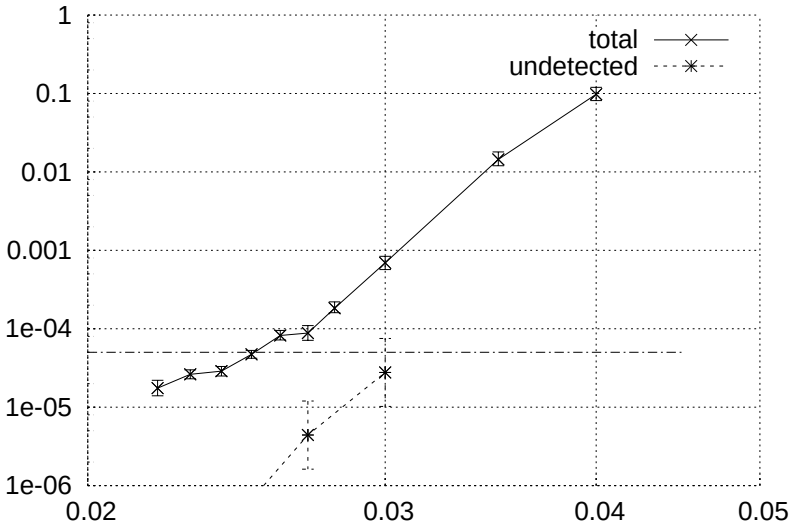

Figure 1. Performance of the dual-containing 'GOLAY.4096' code, on the binary symmetric channel, as a function of the flip probability f_{m}. The vertical axis shows the block error probability.

This is superior to all codes in figure 17 of our paper.

More graphs of performance results to come soon.

4 Amin's conjectures

Here is a conjecture on the dimensions of the parity-Cayley codes:

size $= 2^{2m+1}$. degree $= 2m + 2$. dimension of the rank $= a_m$, where $a_1 = 2$ and $a_{m+1} = 4a_m + 2^m$. dimension of the kernel $= 2^{2m+1} - a_m = b_m$ and $b_{m+1} = 4b_m - 2^m$.

The two first assertions are of course only notation, and the last follows from the third (and vice versa). I agree with you that these graphs are probably good candidates to settle the conjecture you mention.

5 Alternative decoder

Might add a section here on an improved decoding algorithm (work with Oliver Stegle).

6 Discussion

6.1 Weaknesses

This approach only creates codes with blocklength a power of 2; and only creates codes with particular rates.

6.2 Strengths

These algebraic constructions lead to codes having many redundant low-weight checks. These redundant checks help message-passing decoders work better.

Acknowledgments

DJCM is supported by the Gatsby Charitable Foundation.