# A (4,8) Cyclotomic LDPC Code 

Guoyong Shi
March 10, 2005

I'll be using the notation presented in my previous note.
A $(4,8)$ cyclotomic code is given in pattern matrix as

| 2 | 7 | 29 | 36 | 43 | 51 | 79 | 122 |
| ---: | ---: | ---: | :--- | :--- | ---: | ---: | ---: |
| 4 | 14 | 45 | 49 | 53 | 58 | 72 | 86 |
| 5 | 8 | 28 | 90 | 98 | 106 | 111 | 116 |
| 10 | 13 | 16 | 23 | 33 | 35 | 56 | 89 |

The identity matrix is of dimension $128 \times 128$.

## How this matrix is generated?

I did quite some search work. It turned out that the cyclotomic algorithm did not always work for any code rate and any prime number for the dimension of the identity matrix.

In generating the above pattern matrix, I played quite some tricks, as described below.

1. $I$ chose $c=11$, not 8 . The reason is, when $I$ chose $c=8$, and solved the equation $q^{c}=1(\bmod p)$, the sequence $\left\{\mathrm{s}, \mathrm{sq}, \mathrm{sq}^{2}, \mathrm{sq}^{3}, \ldots\right\}$ always broke up at the $4^{\text {th }}$ place. Hence, it could not give a full row sequence with 8 entries. The reason is that 8 is not a prime number. Hence I had to choose $\mathrm{c}=11$.
2. Another tricky issue is, the cyclotomic code did not allow me to choose an arbitrary prime number for $p$. After several rounds of trial and error, I got a solution of $q^{c}=1(\bmod p)$ for $p=199, q=18$.
3. After generating the sequences, each with length 11 , I truncated the trailing 3 entries and picked up those truncated sequences with values all less than 128 , the size of the identity matrix we need. (Remember that these numbers are for shifting the columns, hence should be less than 128.)
