Adam Klivans 17 Feb 1999 Constructing log degree expander

Let M be an $m \times n$ matrix corresponding to the code generator matrix of an error-correcting code with minimum distance d. Let A_i be the ith column of this matrix M. Hence $A_i \in \{0,1\}^m$. For each codeword C, some combination of the rows of M, define the following map:

$$V_C(A_i) = \begin{cases} 1 & \text{if } C_i \text{ is } 0 \\ -1 & \text{if } C_i \text{ is } 1 \end{cases}$$

Here C_i equals the ith entry of C. Now we can extend this mapping to be linear by letting $V_C(x)V_C(y) = V_C(A_i$ if $x + y = A_i$. Notice that $\Sigma_i V_C(A_i) = n - 2w(C)$ where $w(C)$ is the number of ones in C. Now construct a Cayley graph on 2^m vertices where S is the columns of the code generator matrix. I.e., two nodes x and y are connected if there exists a column c such that $x + c = y$. We claim that each V_C for each codeword is an eigenvector of the adjacency matrix of this graph. We also claim that each eigenvector is linearly independent. Thus, we will be able to characterize all of the eigenvalues of the matrix. The largest one will be n corresponding to the all 1's vector. The second largest one will be $n - 2w(C) = n - 2d$ so if the minimum distance is some constant fraction of n then our graph will be an expander. Let N be the adjacency matrix of this Cayley graph. N is a $2^m \times 2^m$ matrix. We can view V_C as a truth table (vector) of length 2^m.

Consider the vector obtained by multiplying N by V_C. Let $x \in \{0,1\}^m$. Let $NV_C(x)$ denote the x'th entry of NV_C. We will show that the quantity $NV_C(x)/V_C(x)$ is a constant for all x. Thus, V_C will be an eigenvector. Notice that

$$\begin{aligned} NV_C(x) &= \Sigma_{y \in \text{nbrs}(x)} V_C(y) \\ &= \Sigma_{x+A_i} V_C(x + A_i) \\ &= \Sigma_{x+A_i} V_C(x) V_C(A_i) \end{aligned}$$

Thus $NV_C(x)/V_C(x) = \Sigma_i V_C(A_i) = n - 2wt(C)$. Hence V_C is an eigenvector. To build the error correcting code we will need to use the Justesen code. We have only left to prove that each V_C is linearly independent.