Foreword

This chapter is based on lecture notes from coding theory courses taught by Venkatesan Guruswami at University at Washington and CMU; by Atri Rudra at University at Buffalo, SUNY and by Madhu Sudan at MIT.

This version is dated **April 30, 2013**. For the latest version, please go to

http://www.cse.buffalo.edu/ atri/courses/coding-theory/book/

The material in this chapter is supported in part by the National Science Foundation under CAREER grant CCF-0844796. Any opinions, findings and conclusions or recomendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

Chapter 10

Codes from Graphs: Expander Codes

In this chapter, we will again consider Question 9.2.2. Recall that we answered the question in the affirmative in Corollary 9.3.3 using Justesen codes. However, for the Justesen code we needed two families of codes to construct our final code. Aesthetically, it would be nice to be able to construct a strongly explicit asymptotically good code in "one shot." In this chapter, we will consider the following question

Question 10.0.1. *Can we construct strongly explicit asymptotically good binary codes without code concatenation?*

In addition to the aesthetic appeal of the question above, it makes sense to answer the above question because we will need a new technique to construct such a code. In this chapter we will see a new family of codes called *expander codes*, which are very different from concatenated codes. Indeed, to date the only ways we know to answer Question 9.2.2 for binary codes are through code concatenation and expander codes. Further, as we will see later expander codes have linear time decoding algorithms, which make them especially attractive for potential practical applications.

To define expander codes, we will need some notions from graph theory, which we define next.

10.1 Bipartite Graphs

We begin with the definition of the general class of graphs that we will consider in this chapter.

Definition 10.1.1 (Bipartite Graphs)**.** A bipartite graph is a triple $G = (L, R, E)$, where L is the set of "left" vertices and R is the set of "right" vertices and the set $E \subseteq L \times R$ is the set of edges.

For example, Figure 10.1 gives an example of a bipartite graph G_H with seven left vertices, three right vertices and twelve edges.

One way to represent such graphs is via its *adjacency matrix*:

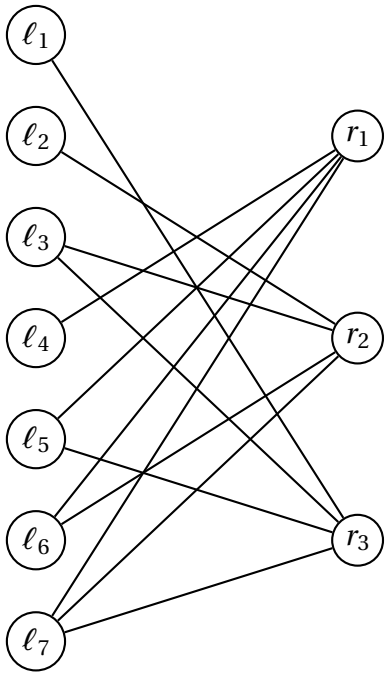

Figure 10.1: A bipartite graph G_H

Definition 10.1.2 (Adjacency matrix)**.** Given a bipartite graph $G = (L, R, E)$, its adjacency matrix, denoted by A_G, is an $|R| \times |L|$ binary matrix, where we index each row by an element of R and every column by an element of L such that for every $(r, \ell) \in R \times L$, the (r, ℓ)'th entry in A_G is 1 if $(\ell, r) \in E$ and 0 otherwise.

For example, the adjacency matrix of the graph in Figure 10.1 is given by

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Recall that the above is the parity check matrix of the $[7,4,3]_2$ Hamming code (see Section 2.3).

This connection between the Hamming code and a bipartite graph is not a co-incidence: we can assign a bipartite graph to any linear code. We do this next.

10.1.1 Factor Graphs

We define the natural bipartite graph representation for any linear code (via its parity check matrix) next.

Definition 10.1.3 (Factor graph)**.** Given any $[n,k]_2$ code C with parity check matrix H, we will call the bipartite graph G_H with $A_{G_H} = H$ to be a factor graph of C. Further, given a bipartite graph $G = (L, R, E)$ with $|L| \geq |R|$, we will denote the corresponding code with parity check matrix A_G to be $C(G)$.

In this chapter, we will consider codes whose factor graphs are so called “expander graphs."

10.2 Expander Graphs

In this section, we will define expander graphs and collect some known facts about them. Informally, expander graphs are sparse graphs that have good connection properties. In particular, we will consider graphs with only linear (in the number of vertices) many edges. Intuitively, for these graphs to have good connectivity, it has to be the case that any set of vertices are connected to as many vertices as possible.

We begin with a series of definitions that will help us formally define expander graphs.

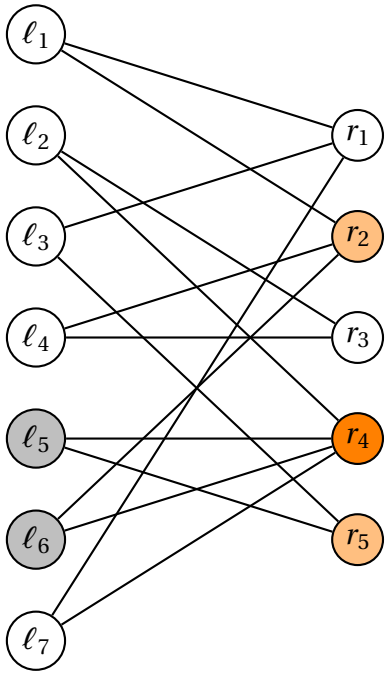

Figure 10.2: An expander graph

Definition 10.2.1 (Left Regularity)**.** A bipartite graph $G = (L, R, E)$ is said to be D-left regular if every vertex in L has degree exactly D.

For example, the graph in Figure 10.2 is 2-left regular.

Definition 10.2.2 (Neighbor Set)**.** For any left vertex set $S \subseteq L$, a vertex $u \in R$ is called a *neighbor* of S if it is adjacent to some vertex in S. We denote by $N(S)$ the set of neighbors of S.

For example, in the graph in Figure 10.2, if $S = \{\ell_5, \ell_6\}$ (set of gray left vertices), then $N(S) = \{r_2, r_4, r_5\}$ (the set of orange right vertices).

Definition 10.2.3 (Unique Neighbor Set)**.** For any left vertex set $S \subseteq L$, a vertex $u \in R$ is called a *unique neighbor* of S if it is adjacent to exactly one vertex in S. We denote by $U(S)$ the set of unique neighbors of S.

For example, in the graph in Figure 10.2, if $S = \{\ell_5, \ell_6\}$ (set of gray left vertices), then $U(S) = \{r_2, r_5\}$ (the set of light orange right vertices).

We are finally ready to define expander graphs.

Definition 10.2.4 (Bipartite Expander Graphs)**.** An $(n, m, D, \gamma, \alpha)$ bipartite expander is a D-left regular bipartite graph $G = (L, R, E)$ where $|L| = n$ and $|R| = m$ such that for every $S \subseteq L$ with $|S| \leq \gamma n$, we have

$$|N(S)| \geq \alpha |S|.$$

For example, the graph in Figure 10.2 is a $\left(7, 5, 2, \frac{2}{7}, \frac{3}{2}\right)$ bipartite expander.

In the above definition, γ gives a measure of how "small" the expanding set can be and α gives a measure of the expansion and is called the *expansion factor*. Note that we always have $\alpha \leq D$. Next, we collect some known results about the existence of bipartite expanders.

Existence of Bipartite Expander graphs. The following result shows that there exists expanders with an expansion factor that can get arbitrarily close to the upper bound of D:

Theorem 10.2.1. *For every $\varepsilon > 0$, $m \leq n$, there exists an $(n, m, D, \gamma, D(1-\varepsilon))$ bipartite expander where $D = \Theta\left(\frac{\log(n/m)}{\varepsilon}\right)$ and $\gamma = \Theta\left(\frac{\varepsilon m}{Dn}\right)$.*

The above can be proven with the probabilistic method and the proof is left as an exercise. We present few remarks on the above result:

- Note that we have $m \leq n$ (and this is needed for the connection to constructing codes), so we want expansion from the larger side to the smaller side. This is the harder direction since there is less room to expand to. (For example, if we could have $m = Dn$, then note that we have a trivial $(n, m, D, 1, D)$ bipartite expander.)
- The expansion factor can be brought arbitrarily close to the maximum value of D at the cost of increasing the value of D.
- By definition, $\gamma n D(1-\varepsilon)$ is a trivial lower bound on m since sets of size up to (and including) γn expand by a factor of $D(1-\varepsilon)$. The above result achieves a value of m that is $1/\varepsilon$ times larger than this trivial bound.

Theorem 10.2.1 is nice but to answer Question 10.0.1 in the affirmative we will need a strongly explicit construction of bipartite expanders with $\alpha > D/2$. It turns out that such a construction is known.

Theorem 10.2.2. *For every constant $\varepsilon > 0$ and every desired ratio $0 < \beta < 1$, there exist strongly explicit $(n, m, D, \gamma, D(1-\varepsilon))$ bipartite expanders for any large enough n (and $m = \beta n$) with D and $\gamma > 0$ being constants (that only depend on ε and β).*

We will use Theorem 10.2.2 later to construct strongly explicit asymptotically good codes.

A Property of Bipartite Expanders. We now state a property of D-left regular bipartite graphs with expansion factor $> D/2$, which will be crucial in our answer to Question 10.0.1.

Lemma 10.2.3. *Let $G = (L, R, E)$ be an $(n, m, D, \gamma, D(1-\varepsilon))$ bipartite expander graph with $\varepsilon < 1/2$. Then for any $S \subseteq L$ with $|S| \leq \gamma n$, we have*

$$|U(S)| \geq D(1-2\varepsilon)|S|.$$

Proof. The total umber of edges going out of S is exactly $D|S|$ by virtue of G being D-left regular. By the expansion property, $|N(S)| \geq D(1-\varepsilon)|S|$. Hence, out of the $D|S|$ edges emanating out of S, at least $D(1-\varepsilon)|S|$ go to distinct vertices, which leaves at most $\varepsilon D|S|$ edges. Therefore at most $\varepsilon D|S|$ vertices out of the at least $D(1-\varepsilon)|S|$ vertices in $N(S)$ can have more than one incident edge. Thus, we have

$$|U(S)| \geq D(1-\varepsilon)|S| - \varepsilon D|S| = (1-2\varepsilon)D|S|,$$

as desired. □

10.3 Expander Codes

We are now finally ready to define expander codes: if G is a bipartite graph with n left vertices and $n-k$ right vertices, then $C(G)$ is an expander graph.

We begin with a simple observation about $C(G)$ (for any bipartite graph G).

Proposition 10.3.1. *Let $G = (L, R, E)$ be a bipartite graph with $|L| = n$ and $|R| = n-k$. Then $(c_1, \ldots, c_n) \in \{0,1\}^n$ is in $C(G)$ if and only if the following holds (where $S = \{i \in [n] | c_i \neq 0\}$) for every $r \in N(S)$:*

$$\sum_{\ell \in S : r \in N(\{\ell\})} c_\ell = 0, \tag{10.1}$$

where the sum is over $\mathbb{F}_2$.

Proof. The proof follows from the definition of $C(G)$, a parity check matrix and the fact that c_j for every $j \notin S$, does not participate in any of the parity checks. □

We record our first result on expander codes.

Theorem 10.3.2. *Let G be an $(n, n-k, D, \gamma, D(1-\varepsilon))$ bipartite expander with $\varepsilon < 1/2$. Then $C(G)$ is an $[n, k, \gamma n + 1]_2$ code.*

Proof. The claim on the block length and the linearity of $C(G)$ follows from the definition of expander codes. The claim on the dimension would follow once we argue the distance of $C(G)$ (since then as the distance is at least one, every 2^k possible codewords are distinct).

For the sake of contradiction, let us assume that $C(G)$ has distance at most γn. Then by Proposition 2.3.4, there exists a non-zero codeword $\mathbf{c} \in C(G)$ such $wt(\mathbf{c}) \leq \gamma n$. Let S be the set of non-zero coordinates of $\mathbf{c}$. Since G is an expander, by Lemma 10.2.3,

$$|U(S)| \geq D(1-2\varepsilon)|S| > 0,$$

where the inequality follows from the fact that $\varepsilon < 1$ and $|S| \geq 1$ (since $\mathbf{c}$ is non-zero). This implies there exists an $r \in U(S)$. Now the parity check in (10.1) corresponding to r is just c_ℓ for some $\ell \in S$, which in turn implies that (10.1) is not satisfied (as $c_\ell \neq 0$). Thus, Lemma 10.3.1 implies that $\mathbf{c} \notin C(G)$, which leads to a contradiction, as desired. □

Note that Theorem 10.3.2 along with Theorem 10.2.2 answers Question 10.0.1 in the affirmative.

A Better Bound on Distance. It turns out that $C(G)$ has almost twice the distance as argued in Theorem 10.3.2.

Theorem 10.3.3. *Let G be an $(n, n-k, D, \gamma, D(1-\varepsilon))$ bipartite expander with $\varepsilon < 1/2$. Then $C(G)$ has distance at least $2\gamma(1-\varepsilon)n$.*

Proof Sketch. As in the proof of Theorem 10.3.2, for the sake of contradiction, let us assume that $C(G)$ has distance $< 2\gamma(1-\varepsilon)n$. Then by Proposition 2.3.4, there exists a non-zero codeword $\mathbf{c} \in C(G)$ such $wt(\mathbf{c}) < 2\gamma(1-\varepsilon)n$. Let S be the set of non-zero coordinates of $\mathbf{c}$. We will argue that $U(S) \neq \emptyset$ and the rest of the argument is the same as in the proof of Theorem 10.3.2.

If $|S| \leq \gamma n$, then we can just use the proof of Theorem 10.3.2. So let us assume that there exists a subset $T \subset S$ such that $|T| = \gamma n$. Then by Lemma 10.2.3, we have

$$|U(T)| \geq D(1-2\varepsilon)\gamma n. \tag{10.2}$$

Now since the total number of edges emanating out of $S \setminus T$ is at most $D|S \setminus T|$, we have

$$|N(S \setminus T)| \leq D|S \setminus T| < D\gamma(1-2\varepsilon)n, \tag{10.3}$$

where the inequality follows from the facts that $|S| < 2\gamma(1-\varepsilon)n$ and $|T| = \gamma n$.

Now, note that

$$|U(S)| \geq |U(T)| - |N(S \setminus T)| > 0,$$

where the inequality follows from (10.2) and (10.3). □