J. Algebra Comb. Discrete Appl.
9(2) • 9–14

Received: 14 September 2021
Accepted: 6 January 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

# A new formula for the minimum distance of an expander code

Research Article

Sudipta Mallik

**Abstract:** An expander code is a binary linear code whose parity-check matrix is the bi-adjacency matrix of a bipartite expander graph. We provide a new formula for the minimum distance of such codes. We also provide a new proof of the result that $2(1-\varepsilon)\gamma n$ is a lower bound of the minimum distance of the expander code given by an $(m,n,d,\gamma,1-\varepsilon)$ expander bipartite graph.

**2010 MSC:** 94B05, 94B25

**Keywords:** Linear code, Minimum distance, Expander graph, Adjacency matrix

## 1. Introduction

Binary linear codes can be constructed from graphs. One such construction was given from bipartite graphs by Tanner in [7]. Sipser and Spielman constructed expander codes from bipartite expander graphs in [6]. One of the goals of all these constructions was to have linear codes with relatively large minimum distance for efficient error correction. For more details on the literature of linear codes and bipartite graphs, see [1, 2, 6, 8]. In this article we provide a new formula for the minimum distance of expander codes. We also provide a new proof of the result that $2(1-\varepsilon)\gamma n$ is a lower bound of the minimum distance of the expander code given by an $(m,n,d,\gamma,1-\varepsilon)$ expander bipartite graph.

Now we present a brief introduction to coding theory: A binary linear code $C$ of length $n$ and dimension $k$ is a $k$ dimensional subspace of $\mathbb{F}_2^n$ where $\mathbb{F}_2$ is the binary field. The code $C$ is called an $[n,k]$-code. The support of a codeword $\in C$ is the set of indices $i$ such that $i$th entry of $x$ is 1. The *Hamming weight* $w_H(x)$ of a vector $x \in \mathbb{F}_2^n$ is the size of the support of $x$. The *Hamming distance*, denoted by $d_H(x,y)$, between two codewords $x$ and $y$ in $C$ is $d_H(x,y) = w_H(x-y)$. The *minimum distance* of $C$, denoted by $d(C)$, is the minimum distance between distinct codewords in $C$. Note that $d(C)$ is the minimum Hamming weight of a nonzero codeword in $C$. We call $C$ to be an $[n,k,d]$ code when $d(C) = d$. A binary matrix $H$ is called the *parity-check matrix* of $C$ if $C$ the null space of $H$, i.e.,

$$C = \{c \in \mathbb{F}_2^n | Hc^T = 0\}.$$

*Sudipta Mallik; Department of Mathematics and Statistics, Northern Arizona University, 801 S. Osborne Dr. PO Box: 5717, Flagstaff, AZ 86011, USA (email: sudipta.mallik@nau.edu).*

https://doi.org/10.13069/jacodesmath.1111379

ISSN 2148-838X

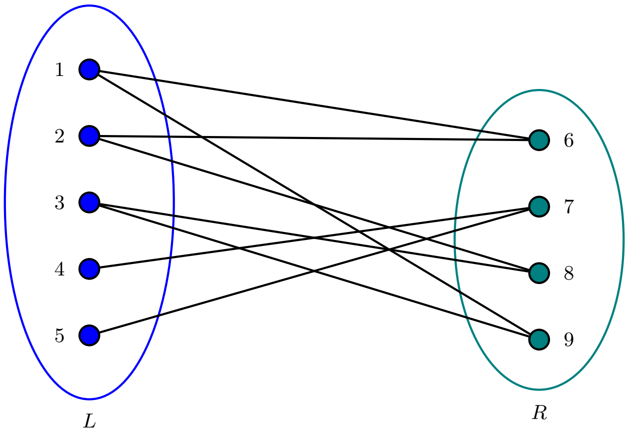

**Figure 1.** **A** $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ **expander graph.**

The minimum distance $d(C)$ can be expressed as the minimum number of linear dependent columns of the parity-check matrix of $C$ as follows:

**Theorem 1.1.** *[5, Theorem 2.2] Let $C$ be a linear code and $H$ its parity-check matrix. Then $C$ has minimum distance $d$ if and only if any $d-1$ columns of $H$ are linearly independent and some $d$ columns of $H$ are linearly dependent.*

For a vertex $v$ of a graph $G$, the set of all vertices in $G$ adjacent to $v$ is called the *neighbor* of $v$, denoted by $\mathrm{N}(v)$. For a set $S$ of vertices of $G$, $\mathrm{N}(S)$ denotes the union of neighbors of vertices in $S$. Now we define a bipartite expander graph based on its definition in [6, 7] with the roles of left and right set of vertices switched:

**Definition 1.2.** *Suppose $G$ is a bipartite graph with vertex set $L\dot{\cup}R$ such that $|L| = m$, $|R| = n$, each edge of $G$ joins a vertex of $L$ with a vertex of $R$, and each vertex of $R$ is adjacent to exactly $d$ vertices of $L$. For positive $\gamma$ and $\alpha$, $G$ is called an $(m, n, d, \gamma, \alpha)$ expander graph if for each set $S \subseteq R$ satisfying $|S| \le \gamma n$, we have*

$$|N(S)| \ge d\alpha|S|.$$

**Example 1.3.** *The bipartite graph in Figure 1 is a $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ expander graph. Each vertex in $R$ has degree $d = 2$. If $S \subseteq R$ satisfies $|S| \le \gamma n = 2$, then $|S| = 1$ or $2$. For $|S| = 1$, $|N(S)| = 2 \ge \frac{4}{3} = d\alpha|S|$. Also for $|S| = 2$, $|N(S)| \ge \frac{8}{3} = d\alpha|S|$.*

**Definition 1.4.** *Suppose $G$ is an $(m, n, d, \gamma, \alpha)$ expander graph and $B$ is the $m \times n$ bi-adjacency matrix of $G$, i.e.,*

$$A = \left[\begin{array}{c|c} O_m & B \\ \hline B^T & O_n \end{array}\right]$$

*is the adjacency matrix of $G$. The binary linear code whose parity-check matrix is $B$ is called the expander code of $G$, denoted by $C(G)$. In other words,*

$$C(G) = \{c \in \mathbb{F}_2^n \mid Bc^T = 0 \text{ in } \mathbb{F}_2\}.$$

**Example 1.5.** *The bi-adjacency matrix of the* $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ *expander graph* $G$ *in Figure 1 is given by*

$$B = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

*The expander code* $C(G)$ *of* $G$ *is given by*

$$C(G) = \{c \in \mathbb{F}_2^4 \mid Bc^T = 0 \textit{ in } \mathbb{F}_2\}.$$

## 2. Main results

We start with the following notation and definition of *von* from [3, 4].

**Definition 2.1.** *For a nonempty subset* $S$ *of vertices of a graph* $G$*, the set of vertices of* $G$ *with odd number of neighbors in* $S$ *is denoted by* $\mathrm{von}(S)$*, i.e.,*

$$\mathrm{von}(S) = \{v \in V(G) \ : \ |\mathrm{N}(v) \cap S| \textit{ is odd}\}.$$

**Example 2.2.** *Consider the* $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ *expander graph* $G$ *in Figure 1. For* $v = 6, 7, 8, 9$*,* $\mathrm{von}(\{v\}) = \mathrm{N}(v)$*. For* $S = \{6, 7, 8\}$*,* $\mathrm{von}(S) = \{1, 3, 4, 5\}$*. For* $S = \{6, 8, 9\}$*,* $\mathrm{von}(S) = \varnothing$*.*

Now we proceed to the main results of this article which give a new formula of the minimum distance of an expander code.

**Theorem 2.3.** *Suppose* $G$ *is a bipartite graph with vertex set* $L\dot{\cup}R$ *such that* $|L| = m$*,* $|R| = n$*, and* $B$ *is the* $m \times n$ *bi-adjacency matrix of* $G$*. Let* $S$ *be a nonempty subset of* $R$*. If* $\mathrm{von}(S) = \varnothing$*, then the columns of* $B$ *indexed by* $S$ *are linearly dependent. Conversely if the columns of* $B$ *indexed by* $S$ *are minimally linearly dependent, then* $\mathrm{von}(S) = \varnothing$*.*

***Proof.*** Suppose $\mathrm{von}(S) = \varnothing$ where $S = \{i_1, i_2, \dots, i_t\} \subseteq R$. Then

$$B_{i_1} + B_{i_2} + \cdots + B_{i_t} \equiv 0 \pmod 2$$

which implies columns $B_{i_1}, B_{i_2}, \dots, B_{i_t}$ of $B$ are linearly dependent.

Conversely suppose $S = \{1, 2, \dots, k\} \subseteq R$ and $B_1, B_2, \dots, B_k$ are minimally linearly dependent columns of $B$. Then $B_1 + B_2 + \cdots + B_k \equiv 0 \pmod 2$. We claim $\mathrm{von}(S) = \varnothing$. Otherwise let $i \in \mathrm{von}(S)$. Then

$$(B_1 + B_2 + \cdots + B_k)_i \equiv 1 \pmod 2,$$

which contradicts $B_1 + B_2 + \cdots + B_k \equiv 0 \pmod 2$. Thus $\mathrm{von}(S) = \varnothing$. □

**Theorem 2.4.** *Suppose* $G$ *is a bipartite graph with vertex set* $L\dot{\cup}R$ *such that* $|L| = m$*,* $|R| = n$*, and* $B$ *is the* $m \times n$ *bi-adjacency matrix of* $G$*. Suppose* $C$ *is the binary linear code whose parity-check matrix is* $B$*. Then the minimum distance* $d(C)$ *of* $C$ *is given by*

$$d(C) = \min\{|S| \ : \ \varnothing \neq S \subseteq R, \ \mathrm{von}(S) = \varnothing\}.$$

***Proof.*** First note that $B$ is the parity-check matrix of $C$. By Theorem 1.1, the support of a code word in $C$ with weight $d(C)$ is the set of indices of some minimally dependent columns of $B$, say indexed by $T$ for some nonempty subset $T$ of $R$. By Theorem 2.3, $\mathrm{von}(T) = \varnothing$. Then

$$d(C) = |T| \geq \min\{|S| \ : \ \varnothing \neq S \subseteq R, \ \mathrm{von}(S) = \varnothing\}.$$

To show the equality, on the contrary suppose there is a nonempty subset $S$ of $R$ for which $d(C) > |S|$ and $\operatorname{von}(S) = \varnothing$. Then by Theorem 2.3, we find $|S|$ linearly dependent columns of $B$ giving a codeword of $C$ with weight less than $d(C)$, a contradiction. □

**Example 2.5.** *Consider the $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ expander graph $G$ in Figure 1. Suppose $C$ is the binary linear code whose parity-check matrix is the bi-adjacency matrix of $G$. We can verify that for any nonempty set $S \subseteq R$ with $|S| \leq 2$, we have $\operatorname{von}(S) \neq \varnothing$. Now for $S = \{6, 8, 9\}$, $\operatorname{von}(S) = \varnothing$. Thus by Theorem 2.4,*

$$d(C) = \min\{|S| \,:\, \varnothing \neq S \subseteq R,\ \operatorname{von}(S) = \varnothing\} = |\{6, 8, 9\}| = 3.$$

The preceding theorem results in a new formula for the minimum distance of expander codes.

**Theorem 2.6.** *Suppose $G$ is an $(m, n, d, \gamma, \alpha)$ expander graph with vertex set $L\dot{\cup}R$ such that $|L| = m$ and $|R| = n$. Then the minimum distance $d(C)$ of the expander code $C$ of $G$ is given by*

$$d(C) = \min\{|S| \,:\, \varnothing \neq S \subseteq R,\ \operatorname{von}(S) = \varnothing\}.$$

Using the minimum distance formula given in Theorem 2.6, we provide a new proof of the following known result which gives a lower bound of the minimum distance of an expander code.

**Theorem 2.7.** *Let $0 < \varepsilon < \frac{1}{2}$ and $\gamma > 0$ such that $\gamma n$ is a positive integer. Suppose $G$ is an $(m, n, d, \gamma, 1-\varepsilon)$ expander graph with vertex set $L\dot{\cup}R$ such that $|L| = m$ and $|R| = n$. Then the minimum distance $d(C)$ of the expander code $C$ of $G$ has the following lower bound:*

$$d(C) \geq 2(1 - \varepsilon)\gamma n.$$

To prove Theorem 2.7, we first prove the following lemmas:

**Lemma 2.8.** *Let $0 < \varepsilon < \frac{1}{2}$. Suppose $G$ is an $(m, n, d, \gamma, 1-\varepsilon)$ expander graph with vertex set $L\dot{\cup}R$ such that $|L| = m$ and $|R| = n$. For each set $S \subseteq R$ satisfying $|S| \leq \gamma n$, we have*

$$d(1 - 2\varepsilon)|S| \leq |\operatorname{von}(S)| \leq |\operatorname{N}(S)|.$$

***Proof.*** Suppose $S \subseteq R$ satisfies $|S| \leq \gamma n$. The second inequality follows from the fact $\operatorname{von}(S) \subseteq \operatorname{N}(S) \subseteq L$ by definition. To show the first inequality, note that there are $d|S|$ edges between vertices in $S$ and vertices in $\operatorname{N}(S) \subseteq L$ and each vertex in $\operatorname{von}(S)$ has at least one neighbor in $S$. Also each vertex in $\operatorname{N}(S) \setminus \operatorname{von}(S)$ has even number (at least 2) of neighbors in $S$. Thus

$$d|S| \geq |\operatorname{von}(S)| + 2|\operatorname{N}(S) \setminus \operatorname{von}(S)| = 2|\operatorname{N}(S)| - |\operatorname{von}(S)|$$

which implies

$$|\operatorname{von}(S)| \geq 2|\operatorname{N}(S)| - d|S|.$$

Since $|S| \leq \gamma n$ and $G$ is an $(m, n, d, \gamma, 1-\varepsilon)$ expander graph, $|\operatorname{N}(S)| \geq d(1-\varepsilon)|S|$. Thus

$$|\operatorname{von}(S)| \geq 2|\operatorname{N}(S)| - d|S| \geq 2d(1-\varepsilon)|S| - d|S| = d(1 - 2\varepsilon)|S|.$$

□

**Lemma 2.9.** *Suppose $G$ is a bipartite graph with vertex set $L\dot{\cup}R$. Let $A$ and $B$ be nonempty disjoint subsets of $S \subseteq R$ such that $S = A \cup B$. If $\operatorname{von}(S) = \varnothing$, then $\operatorname{von}(A) = \operatorname{von}(B)$.*

***Proof.*** Let $\operatorname{von}(S) = \varnothing$. To show $\operatorname{von}(A) \subseteq \operatorname{von}(B)$, suppose $x \in \operatorname{von}(A)$. We claim $x \in \operatorname{von}(B)$. Otherwise $x \notin \operatorname{von}(B)$, i.e., $x$ is adjacent to an even number of vertices in $B$. Since $x \in \operatorname{von}(A)$, $x$ is adjacent to an odd number of vertices in $A$. Thus $x$ is adjacent to an odd number of vertices in $S = A \cup B$. Therefore $\operatorname{von}(S) \neq \varnothing$, a contradiction. Thus $\operatorname{von}(A) \subseteq \operatorname{von}(B)$. Similarly we can show that $\operatorname{von}(B) \subseteq \operatorname{von}(A)$. □

Using the above lemmas, we prove Theorem 2.7.

*Proof of Theorem 2.7.* By Theorem 2.6, consider a nonempty set $S \subseteq R$ such that $d(C) = |S|$ and $\mathrm{von}(S) = \varnothing$. To prove by contradiction, suppose $2(1-\varepsilon)\gamma n > d(C) = |S|$.

Case 1. $|S| \leq \gamma n$
By Lemma 2.8, $d(1-2\varepsilon)|S| \leq |\,\mathrm{von}(S)|$. Since $\varepsilon < \frac{1}{2}$, we have

$$0 < d(1-2\varepsilon)|S| \leq |\,\mathrm{von}(S)|,$$

which implies $\mathrm{von}(S) \neq \varnothing$, a contradiction.

Case 2. $|S| > \gamma n$
In this case

$$2(1-\varepsilon)\gamma n > |S| > \gamma n.$$

Choose a nonempty subset $T$ of $S \subseteq R$ such that $|T| = \gamma n$. Then by Lemma 2.8,

$$d(1-2\varepsilon)\gamma n = d(1-2\varepsilon)|T| \leq |\,\mathrm{von}(T)| \leq |\,\mathrm{N}(T)|. \tag{1}$$

Note that

$$|S \setminus T| = |S| - |T| < 2(1-\varepsilon)\gamma n - \gamma n = (1-2\varepsilon)\gamma n.$$

Since each vertex in $S \setminus T$ has $d$ neighbors in $L$, by Lemma 2.8,

$$|\,\mathrm{von}(S \setminus T)| \leq |\,\mathrm{N}(S \setminus T)| \leq d|S \setminus T| < d(1-2\varepsilon)\gamma n. \tag{2}$$

Combining (1) and (2), we have

$$|\,\mathrm{von}(S \setminus T)| < d(1-2\varepsilon)\gamma n \leq |\,\mathrm{von}(T)|,$$

which implies $\mathrm{von}(S \setminus T) \neq \mathrm{von}(T)$. Since $S = S \cup (S \setminus T)$ and $\mathrm{von}(S) = \varnothing$, by Lemma 2.9, we have $\mathrm{von}(S \setminus T) = \mathrm{von}(T)$, a contradiction.

□

**Observation 2.10.** *If we like to find the minimum distance $d(C)$ of the expander code $C$ of an $(m, n, d, \gamma, 1-\varepsilon)$ expander graph $G$ with vertex set $L\dot{\cup}R$ by brute force using Theorem 2.6, then we need to consider all possible subset $S \subseteq R$ such that $\mathrm{von}(S) = \varnothing$. But because of Theorem 2.7, we need to look at only $S \subseteq R$ satisfying $|S| > 2(1-\varepsilon)\gamma n$.*

**Example 2.11.** *Consider the expander code $C(G)$ of the $(5, 4, 2, \frac{1}{2}, \frac{2}{3})$ expander graph $G$ in Figure 1. Note that $1-\varepsilon = \frac{2}{3}$. By Theorem 2.7, we need to look at only $S \subseteq R$ satisfying $|S| > 2(1-\varepsilon)\gamma n = \frac{8}{3}$. So we look at nonempty sets $S \subseteq R$ satisfying $|S| \geq 3$ and verify whether $\mathrm{von}(S) = \varnothing$. For $S = \{6, 8, 9\}$, $\mathrm{von}(S) = \varnothing$. Thus by Theorem 2.6,*

$$d(C(G)) = \min\{|S| \ :\ \varnothing \neq S \subseteq R,\ \mathrm{von}(S) = \varnothing\} = |\{6, 8, 9\}| = 3.$$

**Acknowledgment:** The author would like to thank his colleague Dr. Bahattin Yildiz for his valuable suggestions. The author would also like to thank the anonymous referee for the quick review.

## References

[1] N. Alon, J. Bruck, J. Naor, M. Naor, R. Roth, Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs, IEEE Trans. Inf. Theory 38(2) (1992) 509–516.

[2] M. R. Capalbo, O. Reingold, S. Vadhan, A. Wigderson, Randomness conductors and constant-degree lossless expanders, Proceedings of the ACM Symposium on Theory of Computing (2002) 659–668.

[3] Sudipta Mallik, Bahattin Yildiz, Graph theoretic aspects of minimum distance and equivalence of binary linear codes, Australas. J. Combin. 79(3) (2021) 515–526.

[4] Sudipta Mallik, Bahattin Yildiz, Isodual and self-dual codes from graphs, Algebra Discrete Math. 32(1) (2021) 49–64.

[5] R. M. Roth, Introduction to coding theory, Cambridge University Press (2006).

[6] M. Sipser, D. Spielman, Expander codes, IEEE Trans. Inf. Theory 42(6) (1996) 1710–1722.

[7] M. Tanner, A recursive approach to low complexity codes, IEEE Trans. Inf. Theory 27(5) (1981) 533–547.

[8] G. Zemor, On expander codes, IEEE Trans. Inf. Theory 47(2) (2001) 835-837.