Graph Theoretic Methods in Coding Theory

Salim El Rouayheb[1] and Costas N. Georghiades[2]

[1] ECE Department,Texas A&M University, College Station, TX 77843
salim@ece.tamu.edu
[2] ECE Department,Texas A&M University, College Station, TX 77843
c-georghiades@tamu.edu

Summary. This paper is a tutorial on the application of graph theoretic techniques in classical coding theory. A fundamental problem in coding theory is to determine the maximum size of a code satisfying a given minimum Hamming distance. This problem is thought to be extremely hard and still not completely solved. In addition to a number of closed form expressions for special cases and some numerical results, several relevant bounds have been derived over the years.

We show here that many of these bounds can be derived using special properties of certain graphs. For instance, the well-known Gilbert-Varshamov bound can be easily proven using a general bound on the chromatic number of graphs. Furthermore, both the Hamming and Singleton bounds can be derived as an application of a property relating the clique and independence numbers of vertex transitive graphs.

1 Introduction

Let $\Sigma_q = \{0, 1, \ldots, q-1\}$ be an alphabet of order q. A q-ary code C of length n and size $|C|$ is a subset of Σ_q^n containing $|C|$ elements called codewords. The Hamming weight $\mathrm{wt}(c)$ of a codeword c is the number of its non-zero entries. A constant-weight code is a code where all the codewords have the same Hamming weight. The Hamming distance $d(c, c')$ between two codewords c and c' is the number of positions where they have different entries. The minimum Hamming distance of a code C is the largest integer Δ such that $\forall c, c' \in C, d(c, c') \geq \Delta$.

Let $A_q(n, d)$ be the maximum size of a q-ary code of length n and minimum Hamming distance d [1, Chapter 17]. $A(n, d, w)$ is defined similarly for binary codes with constant weight w. Finding the values of $A_q(n, d)$ and $A(n, d, w)$ is a fundamental problem in "classical" coding theory [1, 2]. This problem is considered to be very difficult and was in fact described in [3], as "a hopeless task". For this reason, much of the research done has focused on bounding these quantities. Note that the dual problem of finding the maximal order of a set of codewords satisfying an upper bound on their pairwise Hamming distance (anticodes), is well studied in extremal combinatorics. Surprisingly enough, it has a closed form solution [3, 4, 5].

In this paper, we showcase the basic interplay between graph theory and coding theory. Many known bounds on $A_q(n,d)$ and $A(n,d,w)$ follow directly from basic properties of graphs, such as relations among the clique, independence and chromatic numbers of graphs. Other can be proven using deeper algebraic results. For example, using a property of vertex transitive graphs, an inequality relating the maximal size of codes and that of anticodes can be found, leading thus to several bounds on $A_q(n,d)$ and $A(n,d,w)$.

This paper is organized as follows. In Section 2 we briefly introduce some of the needed background in graph theory. In Section 3 we use the tools introduced in the previous section to derive bounds on the maximum size of unrestricted codes. In Sections 4, we focus on constant-weight codes and derive some bounds and inequalities on their maximal size.

2 Graph Theory Background

We start by giving a brief summary of some graph theoretical concepts and results that will be needed in this paper. For more details, we refer the interested reader to [6] and [7].

2.1 Basic Notation and Results

A *graph* is a pair $G = (V, E)$ of sets such that the elements of E are subsets of order two of V. The elements of V are the *vertices* of the graph G and those of E are its *edges*. For any graph X, we let $V(X)$ denote its vertex set and $E(G)$ its edge set.

Two vertices u and v of G ($u, v \in V$) are *adjacent* if $\{u, v\}$ is an edge of G ($\{u, v\} \in E$), and we write $u \sim v$. If all the vertices of G are pairwise adjacent, then G is *complete*. A complete graph on n vertices is denoted as K^n. Two vertices that are not adjacent are called *independent*. The degree $d(v)$ of a vertex v is the number of vertices adjacent to v. The maximum degree of the graph G is then defined as $\Delta(G) := \max\{d(v); v \in V\}$. The graph G is called connected if for any disjoint partition V_1 and V_2 of its vertex set, i.e. $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \emptyset$, there exists at least one vertex in V_1 that is adjacent to a vertex in V_2. A graph C_n having $V(C_n) = \{v_1, \ldots, v_n\}$ and $E(C_n) = \{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_n, v_1\}\}$ is called an odd *cycle* if n is odd, even otherwise

The complement of a graph G is the graph $\bar{G}$ defined over the same vertex set but where two vertices are adjacent in $\bar{G}$ iff they are not in G. We denote by $\omega(G)$ the *clique number* of a graph G, defined as the largest number of vertices of G that are pairwise adjacent. In contrast $\alpha(G)$, the *independence number* of G, is the largest number of pairwise independent vertices in G. It can be easily seen that $\alpha(G) = \omega(\bar{G})$.

A coloring of the graph G is an assignment of colors to its vertices such that adjacent vertices are never given the same color. Formally, a graph G has a *k-coloring* if there exists a map $c : V \to \{1, \ldots, k\}$ such that $c(u) \neq c(v)$ whenever the two vertices u and v are adjacent. The smallest integer k such that G has a k-coloring is called the chromatic number of G and denoted by $\chi(G)$. It is easy to show that the chromatic number of G is upper bounded by $\Delta(G) + 1$. This bound can be slightly improved in many cases:

Theorem 1 (Brooks, 1941). *If G is a connected graph but neither complete nor an odd cycle then*

$$\chi(G) \leq \Delta(G).$$

Given a coloring of the graph G, vertices assigned the same color are pairwise independent and their average number is $\frac{|V(G)|}{\chi(G)}$. Therefore, using Brooks Theorem, we obtain the following bound on the independence number of a graph G.

Lemma 1. *If G is a connected graph but neither complete nor an odd cycle then*

$$\alpha(G) \geq \frac{|V(G)|}{\Delta(G)}.$$

The next result, known as Turán Theorem [8, Thm. 4.1], is a famous result in extremal graph theory and relates the clique number of a graph to the number of its edges. Define

$$M(n, p) := \frac{p-2}{2(p-1)}n^2 - \frac{r(p-1-r)}{2(p-1)},$$

where r is the remainder of the division of n by $p - 1$.

Theorem 2 (Turán, 1941). *A graph G on n vertices having more than $M(n, p)$ edges satisfies $\omega(G) \geq p$.*

2.2 Algebraic Graph Theory

We define here the notions of graph automorphism and homomorphism and describe the class of vertex transitive graphs and state some of their useful properties. For the proofs of the theorems presented here and further related details reference [7] can be consulted.

Definition 1 (Graph Automorphism). *Let $G(V, E)$ be a graph and ϕ a bijection from V to itself. ϕ is called an* automorphism *of G iff*

$$\forall u, v \in V, u \sim v \Leftrightarrow \phi(u) \sim \phi(v).$$

The set of all automorphisms of G is a group under composition; it is called the automorphism group of G and it is denoted $\mathrm{Aut}(G)$. For example, the complete graph on n vertices K_n has S_n, the symmetric group of order n, as its automorphism group. A graph is *vertex transitive* if the action of its automorphism group on its vertex set is transitive:

Definition 2 (Vertex Transitive Graph). *A graph $G(V,E)$ is vertex transitive iff $\forall u, v \in V, \exists \phi \in Aut(G)$ s.t. $\phi(u) = v$.*

The following theorem [7, Lemma 7.2.2] gives a very important property of vertex transitive graphs which will be instrumental in deriving the results in the coming sections.

Theorem 3. *Let $G(V,E)$ be a vertex transitive graph, then*

$$\alpha(G)\omega(G) \leq |V(G)|.$$

Let X and Y be two graphs.

Definition 3 (Graph Homomorphism). *A mapping $f : V(X) \to V(Y)$ is a homomorphism from G to G' if $\forall x, y \in V \; x \sim y \Rightarrow f(x) \sim f(y)$.*

Theorem 4. *If Y is vertex transitive and there is a homomorphism from X to Y, then*

$$\frac{\alpha(X)}{|V(X)|} \geq \frac{\alpha(Y)}{|V(Y)|}$$

Proof. An application of Lemma 7.14.2 in [7].

3 Bounds on Unrestricted Codes

In this section, we start applying some of the previously discussed graph theoretical results to obtain some bounds on the maximal size of codes. First we define a family of graphs called *Hamming graphs* that will be instrumental in establishing the link between codes and graphs.

Definition 4 (Hamming Graph [2]). *Given the positive integers n, q and d such that $q > 1$ and $2 \leq d \leq n$, the Hamming graph $H_q(n,d)$, has as vertices all the q-ary sequences of length n, and two vertices are adjacent iff their Hamming distance is larger or equal to d. That is, $V(H_q(n,d)) = \Sigma_q^n$, where $\Sigma_q = \{0, 1, \ldots, q-1\}$, and $u \sim v$ iff $d(u,v) \geq d$.*

Notice that a q-ary code of length n and minimum Hamming distance d corresponds to a clique in the graph $H_q(n,d)$. Furthermore, $A_q(n,d)$, the maximum size of such code is the clique number of the corresponding Hamming graph. This is concisely stated in the following easy observation which has interesting consequences.

Observation 1 $A_q(n,d) = \omega(H_q(n,d))$.

We now give the first application by showing how Lemma 1 immediately implies the Gilbert-Varshamov Bound. Taking the graph G to be the complement of the Hamming graph $H_q(n,d)$, we have, by Observation 1, $A_q(n,d) = \alpha(G)$. Furthermore, $\Delta(G) = \Delta(\bar{H}_q(n,d)) = \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$. Thus, by Lemma 1 we get:

Lemma 2 (Gilbert-Varshamov Bound).

$$A_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

For specific numerical values, this bound can be slightly improved by using Turán's Theorem as noted in [13]. Next, we will show that the Hamming graphs are vertex transitive. This property will then be used to derive the well-known Singleton and Hamming bounds.

Lemma 3. *The Hamming graph $H_q(n,d)$ is vertex transitive.*

Proof. Take $\Sigma_q = \mathbb{Z}_q$, the integers modulo q. For all $u, v, x \in \Sigma_q^n$, define the function $\phi_{u,v}(x) = x + v - u$. $\phi_{u,v}(x)$ is an automorphism of $H_q(n,d)$. In fact, $d(\phi_{u,v}(x), \phi_{u,v}(y)) = d(x+v-u, y+v-u) = \mathrm{wt}(x+v-u-(y+v-u)) = \mathrm{wt}(x-y) = d(x,y)$. Also, $\phi_{u,v}(x)$ takes u to v.

Thus, we deduce from Theorem 3 and Observation 1 the following inequality [14]:

Corollary 1. $A_q(n,d)\alpha(H_q(n,d)) \leq q^n$

The independence number $\alpha(H_q(n,d))$ of the Hamming graph $H_q(n,d)$ is actually the maximum number of sequences of length n such that the Hamming distance between any two of them is at most $d-1$. A set of sequences satisfying this property is called an *anticode* with maximum distance $d-1$. Define $N_q(n,s)$ to be the maximum number of q-ary sequences of length n that intersect pairwise, i.e., have the same entries, in at least s positions [4]. It follows that

$$\alpha(H_q(n,d)) = N_q(n,t); \quad \text{with } t = n-d+1. \tag{1}$$

By bounding from below the value of $N_q(n,t)$ in two different ways, we get the Singleton and the Hamming Bounds [11].

Lemma 4 (Singleton Bound). $A_q(n,d) \leq q^{n-d+1}$

Proof. Consider the set $T(n,t)$ of all q-ary sequences of length n having the same value 0 in the first $t = n-d+1$ entries. Therefore, by definition, $N_q(n,t) \geq |T(n,t)| = q^{n-t}$. Then, by Eq. (1) and Corollary 1, $A_q(n,d) \leq \frac{q^n}{q^{n-t}} = q^{n-d+1}$.

Lemma 5 (Hamming Bound).

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i}.$$

Proof. Let $r = \lfloor \frac{d-1}{2} \rfloor$ and consider the ball $B(n,r) = \{x \in \Sigma_q^n; \mathrm{wt}(x) \leq r\}$. By the triangle inequality, $\forall x, y \in B(n,r), d(x,y) \leq 2r \leq d-1$. Therefore $N_q(n,t) \geq |B(n,r|$. But $|B(n,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$. The result then follows directly from Eq. (1).

The number $N_q(n,t)$ is well studied in extremal combinatorics [4] [5], and a closed form for it is known. Thus, exact expressions of $N_q(n,t)$ can be used to derive better upper bounds on $A_q(n,d)$ [9]. For instance, if $n-t$ is even, $N_2(n,t) = \sum_{i=0}^{\frac{n-t}{2}} \binom{n}{i}$. Thus, in this case, $B(n, \lfloor \frac{d-1}{2} \rfloor)$ is a maximal anticode and no improvement can be made in this case on the Hamming bound. However, when $n-t$ is odd, $N_2(n,t) = 2\sum_{i=0}^{\frac{n-t-1}{2}} \binom{n-1}{i}$ [4, Thm. Kl] and [10]. Therefore, we obtain the following improvement on the Hamming bound for even values of d [11, 12].

Lemma 6.

$$A(n,d) \leq \frac{2^{n-1}}{\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i}}, \quad \textit{if } d \textit{ is even.} \tag{2}$$

Using the exact expression of $N_q(n,t)$ given in Thm. 2 in [5] or the Diametric Theorem of [4], we get this improved upper bound on $A_q(n,d)$ for non-binary alphabets.

Lemma 7. *For $q \geq 3$, $t = n-d+1$ and $r = \lfloor \min\{\frac{n-t}{2}, \frac{t-1}{q-2}\} \rfloor$,*

$$A_q(n,d) \leq \frac{q^{t+2r}}{\sum_{i=0}^{r} \binom{t+2r}{i} (q-1)^i}. \tag{3}$$

Note that for $q \geq t+1$, $N_q(n,t) = q^{n-t}$ [5, Corollary 1], i.e. a maximal anticode would be the trivial set $T(n,t)$ described in the proof of Lemma 4. In this case, the bound of (3) boils down to the Singleton bound.

For d even and n not much larger than t, the next lemma provides another improvement on the Hamming bound for non-binary alphabets.

Lemma 8. *For d odd and $n \leq t + 1 + \frac{\log t}{\log(q-1)}$*

$$A_q(n,d) \leq \frac{q^{n-1}}{\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i} (q-1)^i} \tag{4}$$

Proof. Under the conditions of this lemma, $N_q(n,t) = q\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i}(q-1)^i$ [4, Eq. 1.7]. The result then follows from Corollary 1.

By constructing homomorphisms between Hamming graphs with different parameters, we get the following recursive inequalities on $A_q(n,d)$ by Theorem 4:

Lemma 9.

$$A_q(n,d) \leq \frac{1}{q}A_q(n+1,d+1) \tag{5}$$

$$A_q(n,d) \leq qA_q(n-1,d) \tag{6}$$

$$A_q(n,d) \leq \frac{q^n}{(q-1)^n}A_{q-1}(n,d) \tag{7}$$

Proof. Let $\phi_1 : \Sigma_q^{n+1} \to \Sigma_q^{n+1}$ such that $\phi_1((x_1,\ldots,x_n,x_{n+1})) = (x_1,\ldots,x_n)$. ϕ_1 is a graph homomorphism from $\bar{H}_q(n+1,d+1)$ to $\bar{H}_q(n,d)$. Applying then Thm. 4, we get Eq. (5). Similarly, taking $\phi_2 : \Sigma_q^{n-1} \to \Sigma_q^n$ such that $\phi_1((x_1,\ldots,x_{n-1})) = (x_1,\ldots,x_n,0)$, we get Eq. (6). The third inequality is obtained by taking $\phi_3 : \Sigma_{q-1}^n \hookrightarrow \Sigma_q^n$ to be the inclusion map.

4 Bounds for Constant-Weight Codes

Let $A(n,2\delta,w)$ be the maximum possible number of codewords in a *binary* code of length n, constant weight w and minimum distance 2δ [2, 15].

Let $K(n,2\delta,w)$ be the graph whose vertices are all the binary sequences of length n and Hamming weight w and where two vertices u,v are adjacent iff $d(u,v) \geq 2\delta$. In analogy with Hamming graphs, we observe here the following:

Observation 2 $A(n,2\delta,w) = \omega(K(n,2\delta,w))$.

Let $\binom{[n]}{w}$ denote the set of all subsets of $[n] = \{1,2,\ldots,n\}$ of order w. There is a natural bijection ν between $\mathrm{V}(K(n,2\delta,w))$ and $\binom{[n]}{w}$. Namely, $\forall u \in \mathrm{V}(K(n,2\delta,w))$, $\nu(u) = U = \{i; u(i) = 1\}$.

Lemma 10. *$\forall p,q \in \mathrm{V}(K(n,2\delta,w)), p \sim q$ iff $|P\cap Q| \leq w-\delta$ where $P = \nu(q)$ and $Q = \nu(q)$.*

Proof. $2\delta \leq d(p,q) = |(P\cap\bar{Q})\cup(\bar{P}\cap Q)| = 2w - 2|P\cap Q|$.

Lemma 11. *$K(n,2\delta,w)$ is vertex transitive.*

Proof. For any two vertices p,q of $K(n,2\delta,w)$, any bijection on $[n]$ such that the image of $P = \nu(p)$ is $Q = \nu(q)$, takes p to q and belongs to $Aut(K(n,2\delta,w))$.

The first result that follows directly from Lemma 11 is the Bassalygo-Elias inequality [15] which relates the maximum size of constant-weight codes to that of unrestricted codes.

Lemma 12 (Bassalygo-Elias inequality).

$$A(n,d) \leq \frac{2^n}{\binom{n}{w}} A(n,d,w)$$

Proof. Consider the two graphs $Y = \bar{H}(n,d)$ and $X = \bar{K}(n,d,w)$. Y is vertex transitive. Since X is an induced subgraph of Y, the inclusion map is a homomorphism that takes X to Y. The result then follows from applying Theorem 4.

By the same token, we can show the following inequalities. The last two are known as Johnson's bounds [16].

Lemma 13.

$$A(n,d,w) \leq \frac{n-w+1}{w} A(n,d+2,w-1) \tag{8}$$

$$A(n,d,w) \leq \frac{n+1}{w+1} A(n+1,d+2,w+1) \tag{9}$$

$$A(n,d,w) \leq \frac{n}{w} A(n-1,d,w-1) \tag{10}$$

$$A(n,d,w) \leq \frac{n}{n-w} A(n-1,d,w) \tag{11}$$

Proof. We start by proving inequality 8. Let ϕ be a mapping from $\binom{[n]}{w-1}$ to $\binom{[n]}{w}$, such that $\forall P \in \binom{[n]}{w-1}, P \subset \phi(P)$. ϕ is a homomorphism from $K(n,d+2,w-1)$ to $K(n,d,w)$. In fact, $\forall P,Q \in K(n,d+2,w-1)$ such that $P \sim Q, |\phi(P) \cap \phi(Q)| \leq |P \cap Q| + 2 \leq w-1-(d+2)/2+2 = w-d/2$ (by Lemma 10). Therefore, $\phi(P) \sim \phi(Q)$. The inequality then follows by applying Theorem 4.

To prove inequality 9, take the homomorphism ϕ from $K(n+1,d+2,w+1)$ to $K(n,d,w)$ to be $\phi(X) = X \setminus \{\max_{x \in X} x\}, \forall X \in \binom{[n+1]}{w+1}$.

The rest of the inequalities can be proved similarly by considering the corresponding graphs and taking the homomorphism to be the inclusion map.■

Next we use the vertex transitivity property of the graphs $K(n,2\delta,w)$ to rederive a number of upper bounds on $A(n,d,w)$.

Lemma 14. *Let $t = w - \delta + 1$, then*

$$A(n,2\delta,w) \leq \frac{\binom{n}{w}}{\binom{n-t}{w-t}} \tag{12}$$

Proof. Let $G = K(n, d, w)$. Since G is vertex transitive, we have

$$A(n, 2\delta, w)\alpha(G) \leq |V(G)| = \binom{n}{w}.$$

Define $M(n, w, s)$ as in [3] to be the maximum number of subsets of $[n]$ of order w that intersect pairwise in at least s elements. By Lemma 10, $\alpha(G) = M(n, w, t)$. But, $M(n, w, t) \geq \binom{n-t}{w-t}$ (for instance, consider the system of all subsets of $[n]$ of order w that contain the set $\{1, 2, \ldots, t\}$).

The previous bound is the same as the one in Theorem 12 in [15] which was given there with a different proof. One can improve on the bound of Lemma 14 by using the exact value of $M(n, w, t)$ [3]. It is known that for $n \geq (w - t + 1)(t + 1)$, the famous Erdős-ko-Rado theorem [18] holds and $M(n, w, t) = \binom{n-t}{w-t}$ [18, 19]. However, this is not the case for lower values of n.

Lemma 15. *Let* $t = w - \delta + 1$ *and* $r = \max\{0, \lceil \frac{\delta(w-\delta)}{n-d} - 1 \rceil\}$*, then*

$$A(n, 2\delta, w) \leq \frac{\binom{n}{w}}{\sum_{i=t+r}^{w} \binom{t+2r}{i} \binom{n-t-2r}{w-i}}; \tag{13}$$

with $\binom{n}{k} = 0$ *when* $k > n$*.*

Proof. (sketch) $A(n, d, w) \leq \frac{\binom{n}{w}}{M(n,w,t)}$, then use the exact value of $M(n, w, t)$ given by the main theorem of [3].

5 Conclusion

We illustrated in this paper the use of graph theoretic techniques to answer a fundamental problem in coding theory, that is determining the maximal size of codes of a certain length and a given minimum Hamming distance. Inequalities involving the independence and clique numbers of general and vertex transitive graphs are shown to lead to many well-known bounds on codes, such as the Hamming, Singleton, Gilbert-Varshamov and Bassalygo-Elias bounds. Additional interesting applications were omitted here due to space restriction. For instance, advanced results in extremal graph theory were used in reference [20] to get asymptotic improvement on the Gilbert-Varshamov bound. Furthermore, graph theory has many applications in modern coding theory such as the design of Low Density Parity Check (LDPC) codes and the design of their iterative decoders [21].

References

1. F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting-Codes,* North-Holland, 1977.
2. N. J. A. Sloane, "Unsolved Problems in Graph Theory Arising from the Study of Codes," *Graph Theory Notes of New York*, 1989.
3. R. Ahlswede and L. H. Khachatrian, "The Complete Intersection Theorem for Systems of Finite Sets," *European Journal of Combinatorics*, vol. 18, pp. 125–136, 1997.
4. R. Ahlswede and L. H. Khachatrian, "The Diametric Theorem in Hamming Spaces - Optimal anticodes," *Adv. in Appl. Math*, vol. 20, pp. 429–449, 1998.
5. P. Frankl and N. Tokushige, "The Erdős-Ko-Rado Theorem for Integer Sequences," *Combinatorica*, vol. 19, pp. 55–63, 1999.
6. R. Diestel, *Graph Theory,* Springer, 2006.
7. C. Godsil and G. Royle , *Algebraic Graph Theory,* Springer, 2001.
8. J.H. van Lint and R.M. Wilson, A course in combinatorics. Cambridge University Press, United Kingdom, 2001.
9. R. Ahlswede, "On Perfect Codes and Related Concepts," *Designs, Codes and Cryptography*, Vol. 22, pp. 221–237, 2001.
10. D. J. Kleitman, "On a Combinatorial Conjecture of Erdős," *J. of Combinatorial Theory*, vol. 1, pp. 209–214, 1966.
11. S. El Rouayheb, C. N. Georghiades, E. Soljanin and A. Sprintson, "Bounds on Codes Based on Graph Theory," *International Symposium on Information Theory (ISIT)*, Nice, 2007.
12. R. Matsumoto, K. Kurosawa, T. Itoh, T. Konno and T. Uyematsu, "Primal-Dual Distance Bounds of Linear Codes with Applications to Cryptography," *IEEE Trans. Inform. Th.,* vol. 52, pp. 4251–4256, 2006.
13. L. Tolhuizen, "The Generalized Gilbert-Varshamov bound is implied by Turàn's theorem," *IEEE Transaction on Information Theory* , vol. 43, pp. 1605–1606, 1997.
14. P. Delsarte, "An algebraic approach to association schemes of coding theory," *Phillips J. Res.*, Vol. 10, 1973.
15. E. Agrell, A. Vardy and K. Zeger, "Upper Bounds for Constant-Weight Codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2373–2395, 2000.
16. S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, 1962.
17. V. I. Levenshtein, "Upper Bound Estimates For Fixed-Weight Codes," *Probl. Inform. Trans.*, vol. 7, pp. 281–287, 1974.
18. P. Erdős, C. Ko and R. Rado, "Intersection Theorems for systems of finite sets," *Quart. J. Math. Oxford*, vol. 12, pp. 313–320, 1961.
19. R. M. Wilson, "The exact bound on the Erdos-ko-Rado Theorem," *Combinatorica*, vol. 4, pp. 247–260, 1984.
20. T. Jiang and A. Vardy, "Asymptotic Improvement of the Gilbert-Varshamov Bound on the Size of Binary Codes," *IEEE Trans. Inform. Theory*, vol. 50, NO. 8, pp. 1655–2395, 2000.
21. T. Richardson and R. Urbanke, "Modern Coding Theory," Cambridge University Press, 2008.