International Journal of Mathematical Archive-6(10), 2015, 182-186
Available online through www.ijma.info ISSN 2229 – 5046

A GRAPH THEORETIC APPROACH TO BOUNDS ON CODES

AVINASH J. KAMBLE*[1], T. VENKATESH[2]

[1]Department of Applied Sciences and Humanities,
St. John College of Engineering and Technology, Palghar – 401404, Maharashtra, India.

[2]Department of Mathematics,
Rani Channamma University, Belgavi -591156, Karnataka, India.

(Received On: 19-10-15; Revised & Accepted On: 31-10-15)

ABSTRACT

The aim of this paper is to discuss the bounds on codes based on graph theoretic techniques. The well-known Singleton and Hamming bounds can be derived as an application of a property relating the clique and independence number of vertex transitive graphs.

AMS Mathematics Subject Classification (2010): *94B65, 05C25.*

Keywords: *Hamming graph, Clique number, Independence number, Vertex transitive graph,*

1. INTRODUCTION

Let F_q be an alphabet of order q. A q-ary code C of length n and size $|C|$ is a subset of F_q^n containing $|C|$ elements called codewords. The Hamming weight $wt(C)$ 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. Finding the values of $A_q(n,d)$ is a fundamental problem in "classical" coding theory. The dual problem, consisting 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. Using the tools from algebraic graph theory, we draw a link between the maximal order of codes and that of anti-codes. Many known bounds on $A_q(n,d)$ follows directly from basic properties of graphs, such as relations among the clique, independence and chromatic numbers of graphs.

In this paper, we first briefly introduce some of the needed background in graph theory. We then use the tools introduced in the previous section to derive bounds on the maximum size of unrestricted codes.

2. PRELIMINARIES: GRAPH THEORY BACKGROUND

2.1. Basic Definitions and Results

Definition 2.1.1: A graph G is an ordered pair $(V(G), E(G))$, which consists of the disjoint sets of ***vertices*** $V(G)$ and ***edges*** $E(G)$ together with an ***incidence function*** ψ_G associating each edge with an unordered pair of not necessarily distinct vertices.

Corresponding Author: Avinash J. Kamble[1]*
[1]Department of Applied Sciences and Humanities,
St. John College of Engineering and Technology, Palghar – 401404, Maharashtra, India.

Definition 2.1.2: Two vertices u and v of G $(u, v \in G)$ are ***adjacent***, if (u, v) is an edge of G.
It is denote by $u \sim v$. 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***.

Definition 2.1.3: The ***degree*** $d(v)$ of a vertex v is the number of vertices adjacent to v. The maximum degree of the graph G is defined as $\Delta(G) := \max\{d(v); v \in V\}$.

Definition 2.1.4: The ***complement*** of a graph G is the graph $\overline{G}$ defined over the same vertex set but where two vertices are adjacent in $\overline{G}$, iff they are not in G.

Definition 2.1.5: The ***clique number*** $\omega(G)$ of a graph G is defined as the largest number of vertices of G that are pairwise adjacent.

Definition 2.1.6: The ***independence number*** $\alpha(G)$ of a graph G is the largest number of pairwise independent vertices in G.

It can be easily seen that $\alpha(G) = \omega(\overline{G})$.

Definition 2.1.7: (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 $\forall u, v \in V,\ u \sim v \Leftrightarrow \varphi(u) \sim \varphi(v)$.

The set of all automorphisms of G is a group under composition; it is called the automorphism group of G and it is denoted $Aut(G)$.

Definition 2.1.8: (Vertex Transitive Graph) A graph $G(V, E)$ is vertex transitive iff $\forall u, v \in V, \exists \varphi \in Aut(G)$ such that, $\varphi(u) = v$.

Theorem 2.1.9: Let $G(V, E)$ be a vertex transitive graph, then $\alpha(G)\omega(G) \le |V(G)|$.

3. BOUNDS ON CODES

In this section, we apply some of the 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 establish a link between codes and graphs.

Definition 3.1: (Hamming Graph) The Hamming graph $H_q(n, d)$, $n \in N$ and $1 \le d \le n$, 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, $V(H_q(n, d)) = F_q^n$, where $F_q = \{0, 1, ..., q-1\}$, and $u \sim v$ iff $d(u, v) \ge d$.

Note that, a q-ary code of length n and minimum Hamming distance d corresponds to a clique in the graph $H_q(n, d)$. Further, $A_q(n, d)$, the maximum size of such code is the clique number of the corresponding Hamming graph.

Remark 3.2: $A_q(n, d) = \omega(H_q(n, d))$.

Now we will show that Hamming graphs are vertex transitive. This property will then be used to derive the well-known Singleton and Hamming bounds.

Lemma 3.3: The Hamming graph $H_q(n,d)$ is vertex transitive.

Proof: Take $F_q = Z_q$, the integers modulo q. For all $u,v,x \in F_q^n$, define the function $\varphi_{u,v}(x) = x+v-u$. $\varphi_{u,v}(x)$ is an automorphism of $H_q(n,d)$.

In fact, $d\left(\varphi_{u,v}(x),\varphi_{u,v}(y)\right) = d(x+v-u, y+v-u) = wt\left(x+v-u-(y+v-u)\right) = wt(x-y) = d(x,y)$.

Also $\varphi_{u,v}(x)$ takes u to v.

Therefore by **Theorem 2.1.9**. and **Remark 3.2.** we have the following inequality.

Corollary 3.4: $A_q(n,d)\alpha\left(H_q(n,d)\right) \le q^n$

The independence number $\alpha\left(H_q(n,d)\right)$ of the Hamming graph $H_q(n,d)$ is the maximum number of sequences of length n such that the Hamming distance between any two of them is at most $d-1$. Define $N_q(n,s)$ to be the maximum number of q-ary sequences of length n that intersect paiwise, that is, have the same entries, in at least s positions. It follows that,

$$\alpha\left(H_q(n,d)\right) = N_q(n,t)\text{; with } t = n-d+1 \qquad (1)$$

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

Lemma 3.5: (Singleton Bound) $A_q(n,d) \le q^{n-d+1}$

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, $N_q(n,t) \ge \left|T(n,t)\right| = q^{n-t}$. Then, by **Eq. (1)** and **Corollary 3.4.**, $A_q(n,d) \le \dfrac{q^n}{q^{n-t}} = q^{n-d+1}$.

Lemma 3.6: (Hamming Bound) $A_q(n,d) \le \dfrac{q^n}{\sum_{i=0}^{\left\lfloor \frac{d-1}{2}\right\rfloor} \binom{n}{i}(q-1)^i}$

Proof: Let $r = \left\lfloor \dfrac{d-1}{2} \right\rfloor$ and consider the ball $B(n,r) = \left\{x \in F_q^n; wt(x) \le r\right\}$ By Triangle inequality, $\forall x,y \in B(n,r), d(x,y) \le 2r \le d-1$. Therefore, $N_q(n,t) \ge \left|B(n,r)\right|$

But, $\left|B(n,r)\right| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$ The result then follows directly from Eq. (1). The exact expressions of $N_q(n,t)$ can be used to derive better upper bounds on $A_q(n,d)$ 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, $B\left(n, \left\lfloor \dfrac{d-1}{2} \right\rfloor\right)$ is a maximal anticode and no improvement can be made in this case on the Hamming bound. However, when $n-t$ is odd, $N_2(n,t) = 2\sum_{i=0}^{\frac{n-t-1}{2}} \binom{n-1}{i}$. Therefore, we obtain the following lemma.

Lemma 3.7: $A(n,d) \le \dfrac{2^{n-1}}{\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i}}$, if d is even.

Notice that the above bound is tighter than Hamming bound for even d, since

$$2\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i} - \sum_{i=0}^{\frac{d-2}{2}} \binom{n}{i} = \binom{n-1}{\frac{d-2}{2}} > 0$$

Next we give a new upper bound on $A_q(n,d)$ for alphabets of arbitrary size.

Lemma 3.8: For $q \ge 3$ $t = n-d+1$, and $r = \left\lfloor \min\left\{ \frac{n-t}{2}, \frac{t-1}{q-2} \right\} \right\rfloor$

,

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

Proof: The proof follows from **Corollary 3.4.** Note that, for $q \ge t+1$, $N_q(n,t) = q^{n-t}$.

i.e. a maximal anticode would be the trivial set $T(n,t)$ described in the proof of **Lemma 3.6.**

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

Lemma 3.9: For d odd and

$$n \le t+1+\frac{\log t}{\log(q-1)}$$

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

Proof: Under the conditions of this Lemma,

$$N_q(n,t) = q\sum_{i=0}^{\frac{d-2}{2}} \binom{n-1}{i} (q-1)^i$$

The result then follows from **Corollary 3.4.**

4. CONCLUSION

In this paper, we have used graph theoretic techniques to give a nice sketch of well-known Singleton and Hamming bound by means of independence and clique number of general and vertex transitive graphs.

5. ACKNOWLEDGEMENT

The authors, would like to thank authorities of Department of Mathematics, St. John College of Engineering and Technology, Palghar-401404, Maharashtra–India and Department of Mathematics, Rani Channamma University, Belgavi- 591156 Karnataka, India for their constant support to make this paper successful one.

REFERENCES

1. Berlekamp, E.R,; *Algebraic Coding Theory*, New York; McGraw-Hill, 1968.

2. Cameron, P.J. and van Lint, J.H,; *Designs, Graphs and Codes and their Links*. London Math. Soc. Student Texts, Vol. 22. Cambridge; Cambridge Univ. Press, (1991).

3. C.Godsil and G.Royle, *Algebraic Graph Theory*, Springer, 2001.

4. F.J.MacWilliams and N. J. Sloane, *The theory of error-correcting codes*, North–Holland, Amsterdam, 1977.

5. R.W. Hamming, *Error detecting and error correcting codes*, Bell system Tech. J.; 29: 147-160, 1950

6. Richard W.Hamming, *Coding and Information theory*, Prentice Hall, Englewood Cliffs, N.J.; 1980.

7. Rudolf Lidl and Harald Niederreiter, *Introduction to Finite Fields and their Applications*,; Cambridge University Press, Cambridge, 1986.

8. R. Diestel, *Graph Theory*, Springer, 2006.

9. Vera Pless, *The Theory of Error Correcting Codes*, Wiley Interscience Series in Discrete Mathematics and Optimization; John Wiley and Sons. New York, 1989 (2nd edition).

10. Van Lint, J.H., *Introduction to Coding Theory*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

Source of support: Nil, Conflict of interest: None Declared