

Lecture 15: Gilbert-Varshamov Bound

October 2, 2007

Lecturer: Atri Rudra

Scribe: Thanh-Nhan Nguyen

In the previous lectures, we have only seen upper bounds on the rate of a code (given a fixed relative distance). In this lecture, we study our first (and only) lower bound on rate of a code.

1 Gilbert-Varshamov Bound

In today's lecture we will prove the following result

Theorem 1.1. *Let $q \geq 2$. For every $0 \leq \delta < 1 - \frac{1}{q}$, and $0 < \varepsilon \leq 1 - H_q(\delta)$, there exists a code with rate $R \geq 1 - H_q(\delta) - \varepsilon$, and relative distance δ .*

The above result was proved for general codes by Gilbert (Section 1.1) and for linear codes by Varshamov (Section 1.2). Hence, the bound is called the Gilbert-Varshamov bound.

1.1 Gilbert Construction

Gilbert proved Theorem 1.1 by the following greedy construction (where $d = \delta n$)

- (i) Start with the empty code: $C \leftarrow \emptyset$
- (ii) If there exists a $\mathbf{v} \in [q]^n$ such that $\Delta(\mathbf{v}, \mathbf{c}) \geq d$ for every $\mathbf{c} \in C$, add \mathbf{v} to C .

We claim that the above algorithm terminates and C has distance d . The latter is true by step (ii). For the former claim, note that, if we cannot add \mathbf{v} at some point, we cannot add it later. The running time of this algorithm is $q^{O(n)}$ (as step (ii) in the worst-case could be repeated for every vector in $[q]^n$, that is at most q^n times). Further, we claim that after termination

$$\bigcup_{\mathbf{c} \in C} B(\mathbf{c}, d-1) \supseteq [q]^n,$$

because if not, then we can pick another another codeword. Therefore,

$$|\bigcup_{\mathbf{c} \in C} B(\mathbf{c}, d-1)| \geq q^n. \quad (1)$$

It is obvious that

$$\sum_{\mathbf{c} \in C} |B(\mathbf{c}, d-1)| \geq |\bigcup_{\mathbf{c} \in C} B(\mathbf{c}, d-1)|$$

which by (1) implies that

$$\sum_{\mathbf{c} \in C} Vol_q(\mathbf{c}, d-1) \geq q^n$$

or

$$\sum_{\mathbf{c} \in C} Vol_q(\mathbf{0}, d-1) \geq q^n.$$

Thus, we have

$$\begin{aligned} |C| &\geq \frac{q^n}{Vol_q(\mathbf{0}, d-1)} \\ &\geq \frac{q^n}{q^{nH_q(\delta)}} \\ &= q^{n(1-H_q(\delta))}, \end{aligned} \tag{2}$$

as desired. In the above, (2) follows from the fact that

$$\begin{aligned} Vol_q(\mathbf{0}, d-1) &\leq Vol_q(\mathbf{0}, \delta n) \\ &\leq q^{nH_q(\delta)}, \end{aligned} \tag{3}$$

where the second inequality follows from the upper bound on the volume of a Hamming ball that we proved in an earlier lecture.

It is worth noting that the code from Gilbert's construction is not guaranteed to have any special structure. In particular, even storing the code can take exponential space. We have seen that linear codes have a much more succinct representation. Thus, a natural question is if one can show that linear codes achieve the the $r \geq 1 - H_q(\delta)$ tradeoff that the Gilbert construction achieves. Varshamov showed that indeed this is the case and we look at his construction next.

1.2 Varshamov Construction

Now we turn to the result due to Varshamov who showed that a random linear code, with high probability, lies on the GV bound.

The Varshamov construction is yet another use of the probabilistic method. For a recap of the general idea behind the probabilistic method and other probability basics (such as the union bound), please refer to Lecture 4 from Spring 09.

Pick a random linear code by picking a random $k \times n$ matrix \mathbf{G} where each of kn entries is chosen uniformly and independently at random from \mathbb{F}_q . We are done if we can show that

$$\text{For every } \mathbf{m} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}, \text{wt}(\mathbf{m}\mathbf{G}) \geq d.$$

Fix $\mathbf{m} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$. Note that for a random \mathbf{G} , $\mathbf{m}\mathbf{G}$ is a uniformly random vector from \mathbb{F}_q^n . Thus, we have

$$\begin{aligned} \Pr[\text{wt}(\mathbf{m}\mathbf{G}) < d] &= \frac{Vol_q(\mathbf{0}, d-1)}{q^n} \\ &\leq \frac{q^{nH_q(\delta)}}{q^n} \end{aligned} \tag{4}$$

where (4) follows from (3). Thus, by the union bound

$$\begin{aligned} \Pr[\exists \mathbf{m}, \text{wt}(\mathbf{m}\mathbf{G}) < d] &\leq q^k q^{-n(1-H_q(\delta))} \\ &= q^{-\varepsilon \cdot n}, \end{aligned}$$

where the equality follows by choosing $k = (1 - H_q(\delta) - \varepsilon)n$. Since $q^{-\varepsilon n} \ll 1$, by the probabilistic method, there exists a linear code C with relative distance δ and rate at least $1 - H_q(\delta) - \varepsilon$. In fact, the proof shows that *most* linear codes (with appropriate parameters) meet the Gilbert-Varshamov bound.