Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 16: Plotkin Bound

October 2, 2007

Lecturer: Atri Rudra *Scribe: Nathan Russell & Atri Rudra*

In the last lecture we proved the GV bound, which states that for all δ with $0 \le \delta \le 1-\frac{1}{q}$, there exists a q-ary code of distance δ and rate at least $1 - H_q(\delta) - \varepsilon$, for every $\varepsilon > 0$. In fact we proved that with high probability, a random linear code C lies on the GV bound. We picked a generator matrix $\mathbf{G}$ at random and proved the latter result. At this point, we might ask what happens if $\mathbf{G}$ does not have full rank?

There are two ways to deal with this. First, we can show that with high probability $\mathbf{G}$ does have full rank, so that $|C| = q^k$. However, the proof from last lecture already showed that, with high probability, the distance is greater than zero, which implies that distinct messages will be mapped to distinct codewords and thus $|C| = q^k$.

Further, the proof required that $\delta \le 1 - \frac{1}{q}$ because it is needed for the volume bound – $Vol_q(\mathbf{0}, \delta n) \le q^{H_q(\delta)n}$– to hold. It is natural to wonder if the above is just an artifact of the proof or, for example, is it possible to get $R > 0$ and $\delta > 1 - \frac{1}{q}$? In today's lecture, we will show that this cannot be the case by proving the Plotkin bound.

1 Plotkin Bound

We start by stating the Plotkin bound.

Theorem 1.1 (Plotkin bound)**.** *The following holds for any $C \subseteq [q]^n$ with distance d:*

1. *If $d = (1 - \frac{1}{q})n$, $|C| \le 2qn$.*

2. *If $d > (1 - \frac{1}{q})n$, $|C| \le \frac{qd}{qd-(q-1)n}$.*

Note that the Plotkin bound implies that a code with relative distance $\delta \ge 1 - \frac{1}{q}$, must necessarily have $R = 0$.

Remark 1.2. *The upper bound in the first part of Theorem 1.1 can be improved to $2n$ for $q = 2$, which is tight. Recall that the Hadamard code is a $[n, \log n, \frac{n}{2}]_2$ code. If we add the complement of each codeword, then it can be shown that the distance of the new code is still $\frac{n}{2}$. This new code proves that part 1 of Theorem 1.1 is tight.*

The statement of Theorem 1.1 gives a trade-off only for relative distance greater than $1 - 1/q$. However, as the following corollary shows, the result can be extended to work for $0 \le \delta \le 1-1/q$:

Corollary 1.3. *For any q-ary code with distance δ, $R \le 1 - \left(\frac{q}{q-1}\right)\delta + o(1)$.*

Proof. The proof proceeds by shortening the codewords. We group the codewords so that they agree on the first $n - n'$ places, where $n' = \lfloor \frac{qd}{q-1} \rfloor - 1$. In particular, for any $x \in [q]^{n-n'}$, define

$$C_x = \{(c_{n-n'+1}, \dots c_n) \mid (c_1 \dots c_N) \in C, (c_1 \dots c_{n-n'}) = x\}.$$

Define $d = \delta n$. For all x, C_x has distance d as C has distance d.[1] Additionally, it has block length $n' < (\frac{q}{q-1})d$ and thus, $d > (1 - \frac{1}{q})n'$. By Theorem 2.1, this implies that

$$|C_x| \leq \frac{qd}{qd - (q-1)n'} \leq qd, \tag{1}$$

where the second inequality follows from the facts that $d > (1 - 1/q)n'$ and that $qd - (q-1)n'$ is an integer.

Note that by the definition of C_x:

$$|C| = \sum_{x \in [q]^{n-n'}} |C_x|,$$

which by (1) implies that

$$|C| \leq \sum_{x \in [q]^{n-n'}} qd = q^{n-n'} \cdot qd \leq q^{n - \frac{q}{q-1}d + o(n)}.$$

In other words, $R \leq 1 - \left(\frac{q}{q-1}\right)\delta + o(1)$ as desired. □

Remark 1.4. *Corollary 1.3 implies that for any q-ary code of rate R and relative distance δ (where q is a* constant *independent of the block length of the code), $R < 1 - \delta$. In other words, such codes cannot meet the Singleton bound.*

Let us pause for a bit at this point and recollect the bounds on R versus δ that we have proved till now. Figure 1 depicts all the bounds we have seen till now (for $q = 2$). The GV bound is the best known lower bound till date. Better upper bounds are known and we will see one such trade-off (called the Elias-Bassalygo bound) in a few lectures.

We now turn to the proof of Theorem 2.1, for which we will need two more lemmas.

The first lemma deals with vectors over real spaces. We quickly recap the necessary definitions. Consider a vector $\mathbf{v}$ in $\mathbb{R}^n$, that is, a tuple of n real numbers. This vector has (Euclidean) norm $\|\mathbf{v}\| = \sqrt{v_1^2 + v_2^2 + \ldots + v_n^2}$, and is a unit vector if and only if its norm is 1. The inner product of two vectors, $\mathbf{u}$ and $\mathbf{v}$, is $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_i \mathbf{u_i v_i}$.

Lemma 1.5 (Geometric Lemma). *Let $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_m} \in \mathbb{R}^n$ be non-zero vectors.*

1. *If $\langle \mathbf{v_i}, \mathbf{v_j} \rangle \leq 0$ for all $i \neq j$, then $m \leq 2n$*

[1] If for some x, $\mathbf{c}_1 \neq \mathbf{c}_2 \in C_x$, $\Delta(\mathbf{c}_1, \mathbf{c}_2) < d$, then $\Delta((x, \mathbf{c}_1), (x, \mathbf{c}_2)) < d$, which implies that the distance of C is less than d (as by definition of C_x, both $(x, \mathbf{c}_1), (x, \mathbf{c}_2) \in C$).

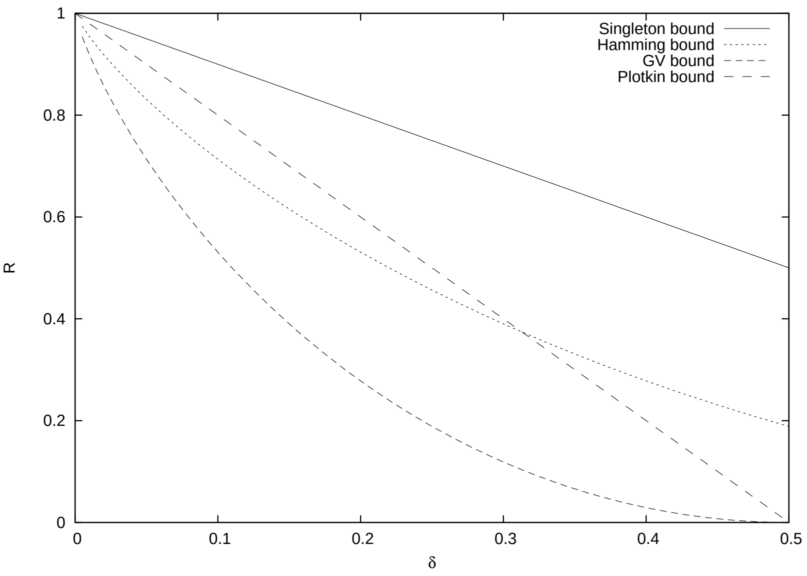

Figure 1: The current bounds on the rate R vs. relative distance δ for binary codes. The GV bound is a lower bound on rate while the other three bounds are upper bounds on R.

2. *Let* $\mathbf{v}_i$ *be unit vectors for* $1 \leq i \leq m$. *Further, if* $\langle \mathbf{v_i}, \mathbf{v_j} \rangle \leq -\varepsilon \leq 0$ *for all* $i \neq j$, *then* $m \leq 1 + \frac{1}{\varepsilon}$

We will prove the lemma in the next lecture.

Lemma 1.6. *There is a one-to-one map* $f : C \to \mathbb{R}^{nq}$ *such that for all* $\mathbf{c} \in C$, $\|f(\mathbf{c})\| = 1$ *and for all* $\mathbf{c_1} \neq \mathbf{c_2} \in C$, $\langle f(\mathbf{c_1}), f(\mathbf{c_2}) \rangle \leq 1 - (\frac{q}{q-1})(\frac{\Delta(\mathbf{c_1},\mathbf{c_2}}{n})$.

We will also prove this lemma in the next lecture. We are now in a position to prove Theorem 1.1.

Proof of Theorem 1.1 Let $\{\mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_m}\} = C$. For all $i \neq j$, $\langle f(\mathbf{c_i}), f(\mathbf{c_j}) \rangle \leq 1 - (\frac{q}{q-1})\frac{\Delta(c_i,c_j)}{n} \leq 1 - (\frac{q}{q-1})\frac{d}{n}$. The first inequality holds by Lemma 1.6, and the second holds as C has distance d.

For part 1, if $d = (1 - \frac{1}{q})n = \frac{(q-1)n}{q}$, then for all $i \neq j$, $\langle f(\mathbf{c_i}), f(\mathbf{c_j}) \rangle \leq 0$ and so by the first part of Lemma 1.5, $m \leq 2nq$.

For part 2, $d > \left(\frac{q-1}{q}\right) n$ and so for all $i \neq j$, $\langle f(\mathbf{c_i}), f(\mathbf{c_j}) \rangle \leq 1 - (\frac{q}{q-1})\frac{d}{n} = -(\frac{qd-(q-1)n}{(q-1)n})$ and, since $(\frac{qd-(q-1)n}{(q-1)n}) = \varepsilon > 0$, we can apply the second part of Lemma 1.5. Thus, $m \leq 1 + \frac{(q-1)n}{qd-(q-1)n} = \frac{qd}{qd-(q-1)n}$. □