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

Lecture 24: Code concatenation

October 24, 2007

Lecturer: Atri Rudra *Scribe: Yang Wang*

Recall the following question we have encountered before:

Question 0.1. *Is there an explicit asymptotically good code? (that is, rate $R > 0$ and relative distance $\delta > 0$ for small q).*

Here, explicit means:

(i) polynomial time construction (of some representation of the code),

(ii) "super" explicit (like description of RS code).

We will answer the question at least in the sense of explicit codes of (i) in this lecture.

1 Code Concatenation

Code concatenation was first proposed by Forney[1]. For $q \geq 2$, $k \geq 1$ and $Q = q^k$, consider two codes which we call *outer* code and *inner* code:

$$C_{out} : [Q]^K \rightarrow [Q]^N,$$

$$C_{in} : [q]^k \rightarrow [q]^n.$$

Note that the alphabet size of C_{out} exactly matches $|C_{in}|$. Then given $\mathbf{m} = (m_1, \ldots, m_K) \in [Q]^K$, we have the code $C_{out} \circ C_{in} : [q]^{kK} \rightarrow [q]^{nN}$ defined as

$$C_{out} \circ C_{in}(\mathbf{m}) = (C_{in}(C_{out}(\mathbf{m})_1), \ldots, C_{in}(C_{out}(\mathbf{m})_N)),$$

where

$$C_{out}(\mathbf{m}) = \langle C_{out}(\mathbf{m})_1, \ldots, \mathbf{m})_N \rangle.$$

This construction is also illustrated in Figure 1. We now look at some properties of a concatenated codes.

Theorem 1.1. *Given C_{out} as an $(N, K, D)_{q^k}$ code and C_{in} as an $(n, k, d)_q$ code, $C_{out} \circ C_{in}$ is an $(nN, kK, dD)_q$ code.*

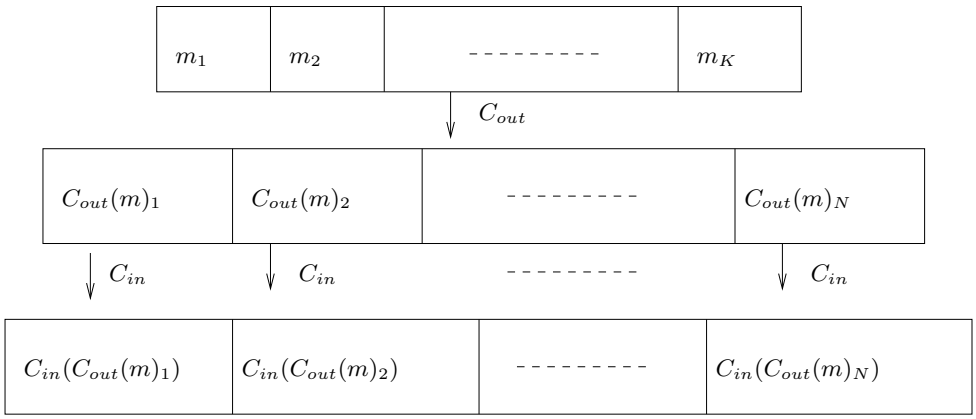

Figure 1: Concatenated code $C_{out} \circ C_{in}$.

Proof. The claims on the block length, dimension and alphabet of $C_{out} \circ C_{in}$ follow from the definition. Next we show that the distance is at least dD. Consider arbitrary $\mathbf{m}^1 \neq \mathbf{m}^2 \in [Q]^K$. Then,

$$\Delta(C_{out}(\mathbf{m}^1), C_{out}(\mathbf{m}^2)) \geq D. \tag{1}$$

Thus for each position $1 \leq i \leq N$ that contributes to the distance above, we have

$$\Delta(C_{in}(C_{out}(\mathbf{m}^1)_i), C_{out}(\mathbf{m}^2)_i) \geq d, \tag{2}$$

as C_{in} has distance d. Since there are at least D such positions (from (1)), (2) implies

$$\Delta(C_{in}(C_{out}(\mathbf{m}^1)), C_{out}(\mathbf{m}^2)) \geq dD.$$

The proof is complete as the choices of $\mathbf{m}^1$ and $\mathbf{m}^2$ were arbitrary. □

Remark 1.2. *If C_{in} and C_{out} are linear codes, then so is $C_{out} \circ C_{in}$, which can be proved for example, by defining a generator matrix for $C_{out} \circ C_{in}$ in terms of the generator matrices of C_{in} and C_{out}. The proof is left as an exercise.*

Suppose C_{out} meets the Singleton bound with rate of R, i.e. C_{out} has relative distance $\delta > 1 - R$. Note that we have a chicken and egg problem here. In order for $C_{out} \circ C_{in}$ to be an asymptotically good code, C_{in} needs to have rate $r > 0$ and relative distance $\delta_{in} > 0$ (i.e. C_{in} also needs to be an asymptotically good code). However the saving grace will be that k can be much smaller than the block length of the concatenated code.

Suppose C_{in} meets the GV bound with rate of r and thus with relative distance $\delta_{in} \geq H_q^{-1}(1 - r) - \varepsilon, \varepsilon > 0$, then $C_{out} \circ C_{in}$ has rate of rR and $\delta = (1 - R)(H_q^{-1}(1 - r) - \varepsilon)$. Expressing R as a function of δ, r, we get the following:

$$R = 1 - \frac{\delta}{H^{-1}(1 - r) - \varepsilon}.$$

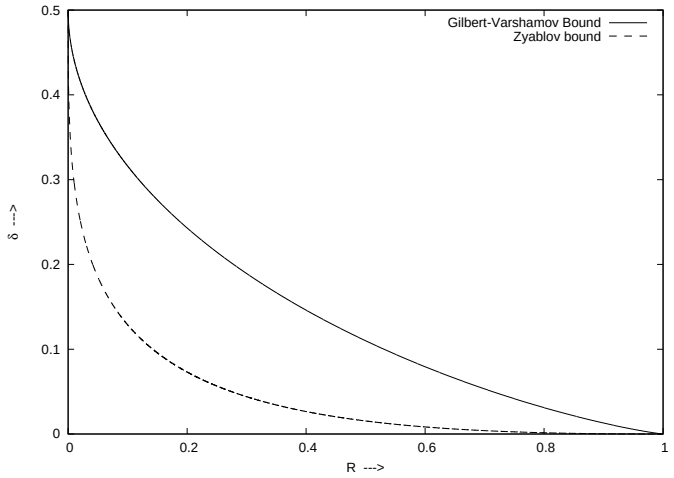

Figure 2: The Zyablov bound. For comparison, the GV bound is also plotted.

Then optimizing over the choice of r, we get that rate of the concatenated code satisfies

$$\mathcal{R} \geq \max_{0<r<1-H_q(\delta+\varepsilon)} r\left(1 - \frac{\delta}{H_q^{-1}(1-r)-\varepsilon}\right).$$

This lower bound is the so called Zyablov bound (the bound of $r < 1 - H_q(\delta + \varepsilon)$ is necessary to ensure that $\mathcal{R} > 0$). See Figure 2 for a plot of this bound.

Note that the Zyablov bound implies that for every $\delta > 0$, there exists a (concatenated) code with rate $R > 0$. Thus, a natural question to ask is the following:

Question 1.1. *Can we construct such a code in polynomial time?*

We will focus on linear codes in seeking an answer to the question above because linear codes have polynomial size representation. Let C_{out} be an $[N, K]_Q$ Reed-Solomon code where $N = Q-1$ (evaluation points being $\mathbb{F}_Q^*$ with $Q = q^k$, then $k = \Theta(\log N)$. However we still need an efficient construction of an inner code that lies on the GV bound. There are two options:

- Perform an exhaustive search among all generator matrices for one satisfying the required property for C_{in}. One can do this because the Varshamov bound states that there exists a linear code which lies on the GV bound. This will take $q^{O(kn)}$ time. Using $k = rn$ (or $n = O(k)$), we get $q^{O(kn)} = q^{O(k^2)} = N^{O(\log N)}$, which is upper bounded by $(nN)^{O(\log(nN))}$, a quasi-polynomial time bound.

- The second option is to construct C_{in} in $q^{O(n)}$ time and thus use $(nN)^{O(1)}$ time overall. This can be achieved by using the method of conditional expectation on the proof that random linear code lies on the bound with high probability.

Thus, we can construct a code that achieves the Zyablov bound in polynomial time. In particular, we can construct explicit asymptotically good code (over some alphabets) in polynomial time.

References

[1] G. David Forney. *Concatenated Codes*. MIT Press, Cambridge, MA, 1966.