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

Lecture 31: Concatenated Codes Achieve the GV Bound (I)

November 7,2007

Lecturer: Atri Rudra *Scribe: Kanke Gao*

In the last lecture, we have seen that a concatenated code can achieve the capacity of BSC_p. In today's lecture, we focus back on Hamming's world.

1 Achieving GV bound

Recall that there exists a linear code that lies on that GV bound. Till now the only explicit asymptotically good codes that we have seen are all based on code concatenation. Thus, a natural question to ask is the following:

Question 1.1. *Does there exist a concatenated code that lies on the GV bound?*

Before answering the question, we note some possible pitfalls for a positive answer to the question above.

- Concatenated codes might be too structured. Note that a linear code has some structure (recall that a random linear code lies on the GV bound w.h.p.). However, concatenated codes seem to be more "restrictive".
- The natural argument for the distance of a concatenated code seems to bottleneck at the Zyablov bound[1], which we know is far from the GV bound.

We now return to Question 1.1: the answer turns out to be positive. One can fix outer code to RS code, and use different random inner codes (like Justesen construction). This result was proved by Thommesen [1]. Before we state the result formally, we will need to define some notions.

Definition 1.2. $\alpha(z) \triangleq 1 - H(1 - 2^{z-1})$, $0 \le z \le 1$.

We have a RS $[N, RN]_{2^k}$ codes as outer code, while the inner code $C_{in}^1, C_{in}^2, \ldots, C_{in}^N$ map vectors from $\mathbb{F}_2^k$ to vectors in $\mathbb{F}_2^n$. Let $\mathbf{G}_i$ be the $k \times n$ generator matrix of C_{in}^i. We have the concatenated code $C^* = C_{out} \circ (C_{in}^1, C_{in}^2, \ldots, C_{in}^N)$, which is defined as follows. Let $\mathbf{m} \in (\mathbb{F}_{2^k})^{NR}$ and $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N) = C_{out}(\mathbf{m})$. According to the definition of concatenated codes,

$$C^*(\mathbf{m}) = (\mathbf{u}_1\mathbf{G}_1, \mathbf{u}_2\mathbf{G}_2, \ldots, \mathbf{u}_N\mathbf{G}_N) \triangleq \mathbf{u}\mathbf{G},\ where\ \mathbf{G} \triangleq (\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_N)$$

Theorem 1.3. *[1] For every $0 < r \le 1$ and $0 < R \le \frac{\alpha(r)}{r}$, let $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_N$ be independent random $(rn) \times n$ generator matrices C_{out} is a RS code with rate R and blocklength N. Then with probability $\ge 1 - 2^{-\Omega(nN)}$, $C_{out} \circ (C_{in}^1, C_{in}^2, \ldots, C_{in}^N)$ has relative distance $\ge H^{-1}(1 - rR) - \varepsilon$, for any $\varepsilon > 0$. Further, such a code $C_{out} \circ (C_{in}^1, C_{in}^2, \ldots, C_{in}^N)$ has rate $\ge rR$.*

[1]A generalization of code concatenation called multilevel concatenation gets us Blokh-Zyablov bound

2 Weight distribution of RS codes

The proof will require an estimate on the number of RS codewords of a given Hamming weight. We do this next. Given $[N, K, D]_{2^k}$ RS code, let A_w $(0 \leq w \leq N)$ denote the number of codewords that have hamming weight w. Obviously, $A_0 = 1,\ A_w = 0,\ 1 \leq w \leq D$. The following result follows from an exact characterization of A_w for MDS codes. However, below we give a simpler proof.

Proposition 2.1. *Let $0 \leq w \leq N$, then $A_w \leq \binom{N}{w} 2^{(w-D+1)K}$*[2].

Proof. Fix $D \leq w \leq N$. There are$\binom{N}{w}$ ways to choose the non-zero-position in a codeword of weight w. We will use the fact that if any K values of a codeword is fixed, then the entire codeword is determined. Note that $N - w$ position are already fixed to be 0. So if fix $t = K - (N - w)$ positions, fix the codeword. As $K = N - D + 1$, $t = N - D + 1 - (N - w) = w - D + 1$. W.o.l.g, fixing the "first" t positions in the non-zero position determined the codeword. Since there are $\leq 2^{k(w-D+1)}$ possible such "prefixed", $A_w \leq \binom{N}{w} 2^{k(w-D+1)}$. □

2.1 Some other function

Definition 2.2. $f_x(\theta) = (1-\theta)^{-1} H^{-1}(1-\theta x)$, $0 \leq \theta \leq 1$

The following property of this function will be crucial in the proof of Theorem 1.3.

Lemma 2.3. *For any $x \geq 0$, $0 \leq y \leq \frac{\alpha(x)}{x}$,*

$$\min_{0 \leq \theta \leq y} f_x(\theta) = f_x(y). \tag{1}$$

We will not formally prove this result. However, the following three facts are key in the proof of Lemma 2.3.

- Fact 1: the line segment connecting $(x, 0)$ and $(\alpha(x), H^{-1}(1-\alpha(x)))$ is tangent to $H^{-1}(1-r)$ at $(\alpha(x), H^{-1}(1-\alpha(x)))$.
- Fact 2: $H^{-1}(1-r)$ is strictly decreasing convex function.
- Fact 3:$f_x(\theta)$ is the intercept of line segment through $(x, 0)$ and $(x\theta, H^{-1}(1-x\theta))$ on the y-axis.

References

[1] C. Thommesen. The existence of binary linear concatenated codes with reed - solomon outer codes which asymptotically meet the gilbert- varshamov bound. *IEEE Trans. Inform. Theory*, pages 850–853, Nov 1983.

[2] This follows from exact characterization of A_w for MDS codes