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

Lecture 32: Concatenated Codes Achieve the GV Bound (II)

November 9, 2007

Lecturer: Atri Rudra *Scribe: Michael Pfetsch & Atri Rudra*

In the last lecture, we began to show that concatenated codes achieve the Gilbert-Varshamov (GV) bound. We started by asking the question, *Does there exist a concatenated code that lies on the GV bound?* We also made a proposition with a lemma [1] regarding the weight distribution of Reed-Solomon (RS) codes. We now continue to show that concatenated codes achieve the GV bound, starting with the declaration of a new theorem.

Theorem 0.1. *(Thommesen): For every $0 \leq r \leq 1$, $0 \leq R \leq \frac{\alpha(r)}{r}$, pick N independent random $k \times n$ matrices $\mathbf{G_1}, \cdots, \mathbf{G_N}$ (and let the corresponding codes be $C_{in}^1, \cdots, C_{in}^N$, rate R Reed-Soloman Code). Let the codewords C^* be defined to be $C^* = C_{out} \circ \left(C_{in}^1, \cdots, C_{in}^N\right)$. For large enough n and N, the following inequality holds true:*

$$Pr_{\mathbf{G}=(\mathbf{G_1},\cdots,\mathbf{G_N})}\left[\exists \textit{ a non-zero codeword in } C^* \textit{ of weight } < \left(H^{-1}\left(1-rR\right)-\varepsilon\right)nN\right] \leq 2^{-\Omega(nN)} \tag{1}$$

Note that N is the block-length of the outer code and that C^* has rate rR with high probability. We also define $\alpha(z)$ as,

$$\alpha(z) \triangleq 1 - H\left(1-2^{z-1}\right) \tag{2}$$

where $0 \leq z \leq 1$, and we define $f_x(\theta)$ as,

$$f_x(\theta) \triangleq (1-\theta) H^{-1}(1-x\theta) \tag{3}$$

where $x, \theta \in [0,1]$. We now make the following proposition:

Proposition 0.2. *If we let $0 \leq y \leq \frac{\alpha(x)}{x}$, then the following is true:*

$$\underset{0 \leq \theta \leq y}{min} f_x(\theta) = (1-y)^{-1} H^{-1}(1-xy) \tag{4}$$

Proof. We begin with a proof by "picture" and make a geometric interpretation of $\alpha(\cdot)$ and $f_x(\cdot)$, and make the following two observations:

1. Observation 1: The line segment between $(x,0)$ and $\left(\alpha(x), H^{-1}(1-\alpha(x))\right)$ is tangent to $H^{-1}(1-z)$.
2. Observation 2: $f_x(\theta)$ is the y-intercept of the line segment that joins $(x,0)$ and $\left(\theta x, H^{-1}(1-\theta x)\right)$.

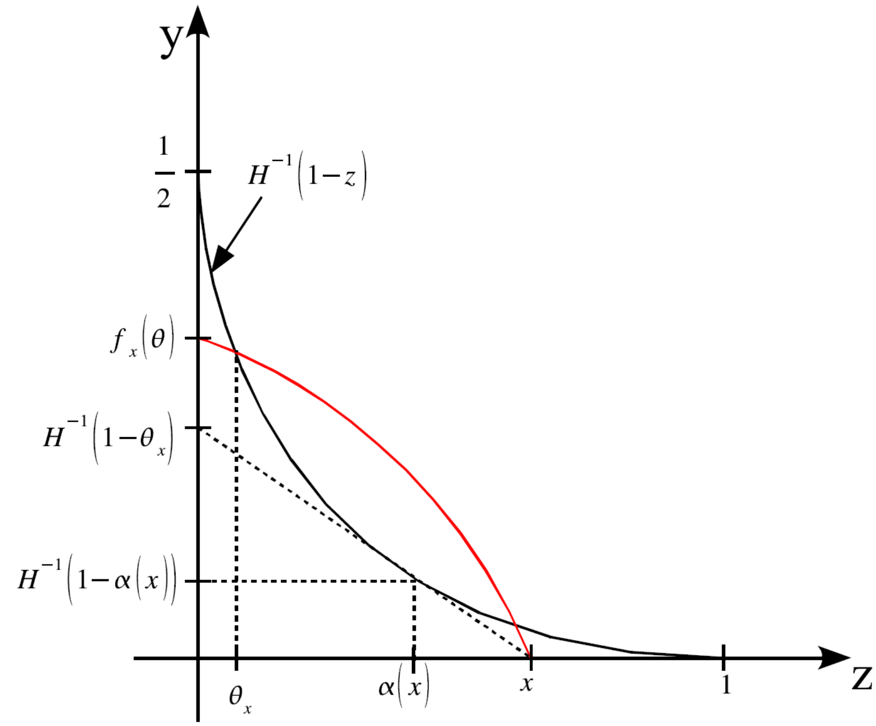

Figure 1: Geometric illustration of $\alpha(\cdot)$ and $f_x(\theta)$, adapted from [2, Figure 2].

Figure 1 is a graphical realization of the above observations. Note that the function $H^{-1}(1-z)$ is a strictly decreasing convex function in z. The above two observations and figure together imply the proposition.

□

Proposition 0.3. *Let* $\mathbf{u} = (u_1, \cdots, u_n) \in C_{out}$ *with* $wt(\mathbf{u}) = w$*, and let* $(y_1, \cdots, y_n) = \mathbf{y} \in (\mathbb{F}_2^n)^N$ *such that* $u_i = 0 \implies y_1 = 0$ *then* $\implies Pr[\mathbf{uG} = y] = 2^{-nw}$*, where the codewords are of the form* $\mathbf{uG} = (\mathbf{uG_1}, \cdots, \mathbf{u_N G_N})$ *[2].*

Proof. Since $\mathbf{u} = 0$, we know that $\mathbf{u_i G_i} = 0$. We can also make the following two observations:

1. Observation 1: $\mathbf{u_i} = 0 \implies \mathbf{u_i G_i}$ is a random vector in $\mathbb{F}_2^n$. This is because $u \neq 0 \implies Pr[\mathbf{u_i G_i} = y_i] = 2^{-n}$.

2. Observation 2: $i \neq j \implies \mathbf{u_i G_i}$ and $\mathbf{u_j G_j}$ are independent random vectors. This is true because $\mathbf{G_i}$ and $\mathbf{G_j}$ are independent, as they were initially chosen to be independent random matrices.

$wt_2(\mathbf{v}) \rightarrow$ binary Hamming at $h \left[\substack{\text{for } v \in \left(\mathbb{F}_2^n\right)^N \\ \triangleq (1-H^{-1}(1-rR)-\varepsilon)nN} \right]$.

□

We can now move on to the formal proof:

Proof. We want to prove that the probability that there exists a codeword, $\mathbf{u}$, in the RS code C, such that the weight of the product $\mathbf{uG}$ is less than h, is less than $2^{-\Omega(nN)}$, as follows:

$$Pr\left[\exists \mathbf{u} \in C_{out} \{0\} \text{ such that } \mathrm{wt}_2(\mathbf{uG}) < h\right] \leq 2^{-\Omega(nN)} \tag{5}$$

We now define a "bad event". We again define the received codeword as $\mathbf{u} = (u_1, \cdots, u_n) \in C_{out}$, and we let $w = wt(\mathbf{u})$ be the weight of that codeword ($D \leq w \leq N$). Note that $D = N - NR + 1$. For the received codeword, $\mathbf{u}$, the probability that the weight, $wt_2(\mathbf{uG})$, is less than h is small.

$$\begin{aligned}
Pr\left[wt_2(\mathbf{uG}) < h\right] &= \sum_{\mathbf{y} \in (\mathbb{F}_{2^n})^N, \text{ such that } wt_2(\mathbf{y}) < h} Pr\left[\mathbf{uG} = \mathbf{y}\right] = 2^{-nw} \\
&= \sum_{i-0}^{h} \binom{nw}{i} 2^{-nw} \\
&\leq 2^{nwH\left(\frac{h}{nw}\right)} \cdot 2^{-nw} \left[\text{as long as } h < \frac{nw}{2}\right] \\
&= 2^{-nw}\left(1 - H\left(\frac{h}{nw}\right)\right)
\end{aligned} \tag{6}$$

We now make a clever application of the Union bound:

$$\begin{aligned}
Pr_{\mathbf{G}}\left[\exists \mathbf{u} \in C_{out} \backslash \{0\} \text{ such that } wt_2(\mathbf{uG}) < h\right] &\leq \sum_{\mathbf{u} \in C_{out} \backslash \{0\}} Pr\left[wt_2(\mathbf{uG}) < h\right] \\
&= \sum_{w=D}^{N} \left[\sum_{\mathbf{u} \in C_{out}, wt(\mathbf{u}) = w} \left[Pr\left[wt_2(\mathbf{uG}) < h\right]\right]\right] \\
&\leq \sum_{w=D}^{N} A_w \cdot 2^{-nw\left(1 - H\left(\frac{h}{nw}\right)\right)} \qquad (7) \\
&\leq \sum_{w=D}^{N} \binom{N}{w} \left[\left(2^k\right)^{(w-D+1)}\right] \left[2^{-nw\left(1 - H\left(\frac{h}{nw}\right)\right)}\right] \qquad (8)
\end{aligned}$$

Where 7 follows from 6, and 8 follows because $\binom{N}{w} \leq 2^N$. Continuing with the proof, we have:

$$\leq \sum_{w=D}^{N} \left[\left(2^{k}\right)^{(w-D+1)}\right]\left[2^{-nw\left(1-H\left(\frac{h}{nw}\right)\right)}\right]$$

$$\leq \sum_{w=D}^{N} \left[2^{N}\right]\left[2^{nr(w-D+1)}\right]\left[2^{-nw\left(1-H\left(\frac{h}{nw}\right)\right)}\right]$$

$$= \sum_{w=D}^{N} \left[\underbrace{2^{-nw}}_{\geq 2^{-n(1-R)N} \geq 2^{-\Omega(nN)}}\right]\left[2^{\left[\underbrace{\left[1-H\left(\frac{h}{nw}\right)-r\left(1-\frac{D}{w}+\frac{1}{w}\right)-\frac{N}{nw}\right]}_{\geq \delta = \frac{\varepsilon}{2} > 0}\right]}\right] \tag{9}$$

In 9, note that $2^{-nw} \geq 2^{-n(1-R)N} \geq 2^{-\Omega(nN)}$. We define the term δ as follows:

$$\delta = \frac{\varepsilon}{2} \tag{10}$$

Note that the term $2^{\left[1-H\left(\frac{h}{nw}\right)-r\left(1-\frac{D}{w}+\frac{1}{w}\right)-\frac{N}{nw}\right]} \geq \delta$ is exponentially small and is strictly greater than 0. This term is satisfied if for every w such that $D \leq w \leq N$, the following inequality holds true:

$$1 - H\left(\frac{h}{nw}\right) - r\left(1-\frac{D}{w}+\frac{1}{w}\right) - \frac{N}{nw} \geq \delta \tag{11}$$

$$\Leftarrow (D \leq w \leq N)$$

$$\frac{h}{nw} \leq H^{-1}\left[1 - r\left(1-\frac{D}{w}+\frac{1}{w}\right) - \frac{1}{n(1-R)} - \delta\right] \tag{12}$$

$$\Leftarrow \frac{h}{nw} \leq \frac{w}{n} H^{-1}\left[1 - r\left(1-\frac{D}{w}+\frac{1}{w}\right) - \frac{1}{n(1-R)} - \delta\right] \tag{13}$$

$$0 \triangleq 1 - \frac{D}{w} + \frac{1}{w} = 1 - \frac{(1-R)N}{w} + \frac{1}{w} \tag{14}$$

$$\frac{w}{N} = (1-\Theta)^{-1}(1-R) \tag{15}$$

$$D \leq w \leq N \Leftarrow 0 \leq \theta \leq R$$

We need to show that for every θ such that $0 \leq \theta \leq R$, the following inequality is true:

$$\frac{h}{nw} \leq (1-R)\,(1-\theta)^{-1}\,H^{-1}\left[1 - r\theta - \frac{1}{n\,(1-R)} - \delta\right] \tag{16}$$

$$\Leftarrow \frac{h}{nw} \leq (1-R)\,\begin{matrix} min \\ 0 \leq \theta \leq R \end{matrix}\left[\underbrace{(1-\theta)^{-1}\,H^{-1}\left[1 - r\theta - \frac{1}{\underbrace{n\,(1-R)}_{-2\delta(\text{large enough n})}} - \delta\right]}_{fr(\theta)}\right] \tag{17}$$

In inequality 17, above, we note that, for large enough n, the following is true:

$$\frac{1}{n\,(1-R)} = -2\delta \tag{18}$$

This allows the above inequality to be simplified, as follows:

$$\Leftarrow \frac{h}{nw} \leq (1-R)\left[\begin{matrix} min \\ 0 \leq \theta \leq R \end{matrix}\left[\underbrace{(1-\theta)^{-1}\,H^{-1}\,[1 - r\theta]}_{fr(\theta)}\right]\right] \tag{19}$$

The proof is concluded by noting that, by proposition 0.2, the above inequality is true if the following is true:

$$\Leftarrow \frac{h}{nN} \leq (1-R)\,(1-R)^{-1}\,H^{-1}\,(1 - rR) - \varepsilon \tag{20}$$

and choosing

$$h \leq \left(H^{-1}\,(1 - rR) - \varepsilon\right) nN \tag{21}$$

This concludes the proof.

□

We need to show that the set of codewords, C^*, has rate rR not all G_i might have full rank, but as C^* has distance greater than or equal to one with high probability, it has rate rR.

References

[1] V. S and A. Rudra. "Concatenated codes can achieve list-decoding capacity." To appear in Proceeding of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). January 2008.

[2] 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, vol. IT-29, pp. 850-853, Nov. 1983.