# Lecture 12 <br> Guessing Decoders and Product Codes 

February 20, 2024
JOHN M. CIOfFI
Hitachi Professor Emeritus (recalled) of Engineering
Instructor EE379A - Winter 2024

## Announcements \& Agenda

## - Announcements

- PS5 due tomorrow.
- Today
- Retransmission - Error Detection
- Guessing Random Additive Noise Decoding
- GRAND Soft Information
- Product Codes \& GRAND
- Matlab software (MIT education-use permitted)


## Retransmission - ErrorDetecting Codes

Section 8.6.3

## CRC Error Detection and Retransmission

- Cyclic Redundancy Check codes are (usually) binary and only detect errors (so $s(D) \neq 0$ ).
- CRCs mostly use simple binary versions of the previous encoders/decoders.
- Table below lists some with $d_{\text {free }}=4$ and $n_{\max }=2^{2^{r}}-1$.
- These detect:
- all single and 2-bit errors, and also any odd number of bit errors. The $(D+1)$ factor forces even distance between codewords.
- any burst of length $\leq n-k$ (because this is the length of $g(D)$ - such a burst is not divisible by $g(D)$ ).

| Name | $g(\boldsymbol{D})$ | factored |
| :--- | :---: | :---: |
| CRC-7 | $D^{7}+D^{6}+D^{4}+1$ | $\left(D^{4}+D^{3}+1\right) \cdot\left(D^{2}+D+1\right) \cdot(D+1)$ |
| CRC-8 | $D^{8}+D^{2}+D+1$ | $\left(D^{7}+D^{6}+D^{5}+D^{4}+D^{3}+D^{2}+1\right) \cdot(D+1)$ |
| CRC-12 | $D^{12}+D^{11}+D^{3}+D^{2}+D+1$ | $\left(D^{11}+D^{2}+1\right) \cdot(D+1)$ |
| CRC-16 USA | $D^{16}+D^{15}+D^{2}+1$ | $\left(D^{15}+D+1\right) \cdot(D+1)$ |
| CRC-16 Euro | $D^{16}+D^{15}+D^{5}+1$ | $\left(D^{15}+D^{14}+D^{13}+D^{12}+D^{4}+D^{3}+D^{2}+D+1\right) \cdot(D+1)$ |
| CRC-24 | $D^{24}+D^{23}+D^{14}+D^{12}+D^{8}+1$ | $\left(D^{10}+D^{8}+D^{7}+D^{6}+D^{5}+D^{4}+D^{3}+D+1\right) \cdot$ <br> $\left(D^{10}+D^{9}+D^{6}+D^{4}+1\right) \cdot(D+1)$ |
| CRC-32 | $D^{32}+D^{26}+D^{23}+D^{22}+D^{16}+D^{12}+D^{11}+D^{10}+D^{8}+D^{7}+D^{5}+D^{4}+D^{2}+D+1$ |  |
| (appears prime, not sure) |  |  |

## Analysis - CRCs are for detection ONLY.

- $P_{u} \triangleq$ undetected error probability $P_{u}<2^{k-n} \cdot\left(\bar{P}_{b}\right)^{4} ; s=0$ for wrong codeword.

| Name | $P_{u} /\left(\bar{P}_{b}\right)^{4}$ | $1-P_{u} /\left(\bar{P}_{b}\right)^{4}$ | Reliability | High $\bar{P}_{b}$ if inner code fails$\{$ voice reliability) |
| :---: | :---: | :---: | :---: | :---: |
| CRC-7 | $2^{-7}$ | . 99221875 | 2 nines |  |
| CRC-8 | $2^{-8}$ | . 99609375 | 3 nines |  |
| CRC-12 | $2^{-12}$ | . 999755859375 | 4 nines | \{video reliability |
| CRC-16 USA | $2^{-16}$ | 0.999984741210938 | 5 nines | (core network reliability) |
| CRC-16 Euro | $2^{-16}$ | 0.999984741210938 | 5 nines | ( |
| CRC-24 | $2^{-24}$ | 0.999999940395355 | 7 nines | \{critical reliability |
| CRC-32 | $2^{-32}$ | 0.999999999767169 | 9 nines | \{storage |

- These are link-layer reliabilities $-\bar{P}_{b}$ could be high within a CRC codeword if large $-N$ inner-code fails, - but still, even if $\bar{P}_{b}=.1$, these get very low.
- TCP-IP and higher-level session/application CRC checks (possibly using RS codes for detection) would create super reliability with "once in a century" level failures.
- These are cyclic codes so use earlier simple generators and receiver-syndrome calculation circuits.


## Retransmission

- Automatic Repeat Request (ARQ): If the CRC detects an error, resend the codeword.
- ARQ requires a mechanism for acknowledgment (back-channel) or ACK/NAK.
- The NAK returns upon the receiver's non-zero CRC syndrome calculation.
- $P_{c}$ is the correct receipt probability (syndrome is zero).

$$
\mathbb{E}\left[L_{\text {retrans }}\right]=\sum_{l=1}^{\infty} l \cdot P_{c} \cdot\left(1-P_{c}\right)^{l}=\frac{1}{P_{c}}
$$

- Throughput $=\left(\frac{k}{n}\right) \cdot P_{c} \cdot R$ bps
- Throughput represents the "real data rate" with code redundancy and retransmission accounted.
- Throughput assumes infinite buffer delay is possible.
- There are entire courses in this network/queuing area, see EE384S (Bambos, Spring Q).


## Hybrid ARQ (HARQ)

- HARQ: A cyclic code is used with both detection and correction.
- If the correction part works, there is no need to retransmit.
- If the detection part discovers an error, and then retransmission occurs.
- Reed Solomon cyclic codes can split the parity bytes into those for correction and those for detection (sum is the allowed maximum P).
- HARQ with soft decoding
- Chase Decoding - use all instances of (re-) transmitted codeword (form of diversity) to decode.
- Incremental Redundancy - only retransmit additional parity bits (this is what 5G uses).


## GRAND



## Intelligent guessing of codewords



- If (sub) symbol-by-symbol-sequence guessed decision is not a codeword already (stop if codeword):
- GRAND reorders the subsymbols (bits) in terms of likelihood and
- Guess(es) other ss value(s) - usually means flipping $n_{g}$ bit decision(s) - for least reliable LLRs.
- Each failed guess not revisited, and it's possible (but not likely) to have up to $|C|^{n}$ guesses, more like $|C|^{n-k}$
- Grows as $\binom{n}{n_{\text {flipped ss }}}$ guesses at each stage, usually $g=0, \ldots, \rho$ for good codes because codewords not more than $\rho=n-k$ bits apart.
- Expected number of steps to find codeword is $\mathbb{E}[g]=2^{\rho}$.
- Ensure any "give-up" point occurs less frequently than the target $P_{e}$.
- With the ss reordering from worst to best, the first codeword found is the ML decision (low SNR).


## Return to our L8 4-state example (stops 12 dim)



## Is it a codeword?

- For the example, choosing 2 bits from 12 eventually picks times 1 and 5 , which is a codeword if both flipped.

- For the example $H^{t}=[\underbrace{\left[\begin{array}{llllll}1 & 1 & 0 & 0 & 0 & 0\end{array}\right]}_{h_{2}(D)} \underbrace{\left[\begin{array}{llllll}1 & 0 & 1 & 1 & 1 & 1\end{array}\right]}_{h_{1}(D)}]$, which checks (split 2 and 1).
- Usually, the parity check is the least complex way to check for valid codewords (linear code).
- Check after each guess to determine if ML estimate (which is first codeword to pass, given order).
- May continue also to create a list of codewords that are next-to-ML for some soft-decoding schemes.


## How many queries? $\rightarrow$ ORB (ordered reliability bits)

- Upper bound is $2^{n}$.
- The guess-sequence strategy is important with good code.
- Singleton bound suggests more like $2^{n-k}$ for good codes [1].
- Implementation has finite queries before exceeding compute budget.
- GRAND example's computation is largely the sort $\leq N^{2} / 2$
- Finding (next) largest/smallest value is $n-i(i=1, \ldots$ ) compares
- So $11+10+9=\left[\begin{array}{ll}21 & 30\end{array}\right]$ for black/red to find the ML codeword (the parity checks are trivial and number 13 and 79).
- Viterbi is $6 \times 4 \times 3=72$, roughly $2 \times$ more operations to find the same codeword (it searches unlikely paths unnecessarily).
- So there are $(12,6)$ codes that find ML sooner, on average.
- This curve was generated with MIT software (later).

- $|C|>2$ vastly increases guessing numbers, so GRAND compares better with binary codes.
- GRAND originators say correlated (nonwhite) noise (or equivalently ISI) is also well handled.
- Not clear what convergence looks like because the number of levels per subsymbol rises rapidly with ISI.
- As we'll see in next section of 379A and also B, there are better ways to make an ISI or correlated noise channel look like equivalent set of AWGNs to which usual good codes apply in usual manner.
- Instructor presently believes these better match GRAND's strengths.



## GRAND with BSC?



- Follows same order really - just the soft information is equal for each output bit.
- Thus, might have to go to guess 67 to get it right if unlucky (or 13 if lucky).
- With 3-bit-error case, the search could go to 299 checks $=\binom{n}{1}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}$ with $n=12$
- Sort is somewhat trivial for BSC, 11+10+9 = 30 compares


# MIT Matlab Software (educational uses) 

Eventually Section 7.6.2

## MIT programs

## - Web site https://github.com/kenrduffy/GRAND-MATLAB

> function [y_decoded,err_vec,n_guesses,abandoned] = bin_ORBGRAND1(H,max_query,y_soft) 1-line ORGBRAND (soft detection)

## From

K. R. Duffy, W. An, and M. Medard, "Ordered reliability bits guessing random additive noise decoding," IEEE Trans. Signal Process., vol. 70, pp. 4528-4542, 2022.
Uses the Landslide algorithm from that paper and the light-weight
1-line implementation introduced in
K. Galligan, M. Médard, K. R. Duffy, "Block turbo decoding with ORBGRAND" arXiv:2207.11149, 2022.

1-line ORBGRAND differs from Basic ORBGRAND by considering a dynamically determined intercept in its statistical model.

```
Inputs:
n - code length
H - Parity check matrix or CRC function
max_query - Maximum number of code-book queries to abandonment
y_soft - Channel soft information
Outputs:
y_decoded - Decoded ML codeword
err_vec - Putative noise
n_guesses - Number of guesses performed
abandoned - 1 if abandoned, 0 if found a codeword
```

- Calls
- Landslide.m
- bin_ORBGRAND.m
- Different guessing order
- bin_GRAND.m
- Hard-coded channel output


## Our Example with this software?

- 6 subsymbols and terminate, same $H(D)=\left[\begin{array}{ll}1+D^{2} & 1+D+D^{2}\end{array}\right]$ has the block-code $H$



## Recall that LLRi is <br> $$
L L R_{i}=-\frac{2}{\sigma^{2}} \cdot y_{i}
$$

ysoft=[
$-0.9000 \quad 0.5000-1.1000 \quad-0.9000 \quad-0.5000 \quad 1.0000 \quad-0.8000 \quad-0.7000 \quad 0.9000 \quad 1.0000-$
0.9000 1.0000];
>> [y_decoded,err_vec,n_guesses,abandoned] = bin_ORBGRAND1(H,30,-ysoft)
y_decoded $=0 \begin{array}{llllllllllll}0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\end{array}$
rr_vec =
n_guesses $=30 \%$ This is more than 12 , but less than 79
abandoned 0
> [y_decoded,err_vec,n_guesses,abandoned] = bin_ORBGRAND1(H,10,-ysoft);
ned =
soft =
$0.9000 \quad 0.9000$
[y_decoded,er__ec,n_guesses,abandoned] = bin_ORBGRAND1(H,300,-ysoft)

- Did not need 299 guesses, only 77 for 3-error case.


## With Hard Decoded

## - Bin_GRAND.m

```
function [y_decoded,putative_noise,n_guesses,abandoned] =
bin_GRAND(H,max_query,y_demod)
    GRAND (hard detection, BSC)
Inputs:
    n - code length
    H - Parity check matrix or CRC function
    max_query - Maximum number of code-book queries to abandonment
    y_demod - Channel hard output
Outputs:
    y_decoded - Decoded codeword
    putative_noise - noise
    n_guesses - Number of guesses performed
    abandoned - - if abandoned, 0 if found a codeword
```

```
>> y=[01000010011101]
>> [y_decoded,err_vec,n_guesses,abandoned] = bin_GRAND(H,30,y)
y_decoded =
    0
err_vec =
    0
n_guesses=28
abandoned = 0
>>y=[ 0 1 1 0 0 0 0 1 1 0 1 1 1 1 1 0 1];
>> [y_decoded,err_vec,n_guesses,abandoned] = bin_GRAND(H,300,y)
y_decoded= = 1 1 1 0
err_vec= 1 0 0 0 1 0
n_guesses = 101
abandoned = 0
```

- The query count differs slightly because the hard-decoded example has different LLR inputs.


# GRAND Soft Information 

Eventually Section 7.6.3

## An incorrect codeword guess

- ML codeword is not always correct - so GRAND may also guess this incorrect codeword.
- This is an error.
- A guess $\widehat{\boldsymbol{x}}$ is correct with probability (from Chapter 1 ), call this guess $q^{*}$.
$p_{x / \Delta}(\hat{\boldsymbol{x}} / \boldsymbol{\delta})$, where $\boldsymbol{\Delta} \triangleq\left[\begin{array}{lll}\left|y_{1}-\hat{x}_{1}\right|^{2} & \cdots & \left.\left|y_{n}-\hat{x}_{n}\right|^{2}\right] \text { with/without reordering }\end{array}\right.$
- Current/past guesses' probability, when subtracted from 1, is soft information.
- This is, possibly with scaling (seq to code), proportional to the probability that the ML $\widehat{x}$ is incorrect.
- For guess $q$, the intrinsic input probability will be $p_{q, i}$ for $i=1, \ldots, n$, initially this is $p_{0, i n t, i}=2^{-1}$.

$$
p_{q, i n t, i}=\frac{e^{L L R_{i}}}{1+e^{L L R_{i}}} \quad p_{q, \text { chan }, i}=\frac{e^{-\frac{\left\|\Delta_{q, i}\right\|^{2}}{2 \sigma^{2}}}}{\left(\sqrt{2 \pi \sigma^{2}}\right)} \quad p_{q, i}=p_{q, \text { chan }, i} \cdot p_{q, \text { int }, i}
$$

- Probability of channel-output (noise seq) guess $q$

$$
\begin{array}{r}
P\left(\boldsymbol{n}_{q}\right)=\prod_{i=1}^{n}\left(\underset{\text { seq has 0 }}{\left(p_{q, i \in\left\{n_{q, 0}\right\}}\right)}\right) \cdot\left(1-p_{q, i \in\left\{n_{q, 1}\right\}}\right) \\
\text { @ position } i
\end{array} \quad \begin{gathered}
\text { seq has } 1 \\
\text { @osition } i
\end{gathered}
$$

$$
P(A)=1-\underbrace{\sum_{q=0}^{q^{*}} P_{q}\left(\boldsymbol{n}_{q}\right)}_{\text {before and } q^{*}}
$$

## AEP-like GRAND Analysis

- $2^{n}$ possible $y$ (noise) guesses, $S$ :
- Continuous to discrete dist'n
- Grand guesses' path eliminates $q^{*}$ of these guesses.
- So, $1-\sum_{S \backslash\{q\}} P_{q}\left(\boldsymbol{n}_{q}\right)$ is the probability of the other outputs not yet guessed, which is $\propto$ probability of ML error.
- $2^{k}$ possible $\hat{\boldsymbol{x}}$ guesses
- On average, each associates with fraction $\frac{2^{k}-1}{2^{n}-q^{*}}$
$=\frac{\# \text { of (other) codewords }}{\# \text { of remaining guesses }}$


$$
P(A) \triangleq\left(1-\sum_{q=0}^{q^{*}} P\left(\boldsymbol{n}_{q}\right)\right) \cdot \underbrace{\frac{2^{k}-1}{2^{n}-q^{*}}}_{\begin{array}{c}
\text { scale for } \\
\text { codewords }
\end{array}}
$$

- The sequence likelihood of correct is

$$
\text { - } \frac{P\left(\boldsymbol{n}_{q^{*}}\right)}{P(A)+P\left(\boldsymbol{n}_{q^{*}}\right)}
$$

- While incorrect is

$$
\text { - } \frac{P(A)}{P(A)+P\left(\boldsymbol{n}_{q^{*}}\right)}
$$

The ML codeword $\widehat{x}$ and set of all others $S_{x \backslash \widehat{x}}$ are mutually exclusive, so can add their probabilities.

## Bit-level Likelihood

- When $\widehat{\boldsymbol{x}}_{i}=0$ for guess $q^{*}$ :
- $L L R_{i}=\frac{P\left(n_{q}\right)+P(A) \cdot p_{q^{*}, i}}{P(A) \cdot\left(1-p_{q^{*} ; i}\right)}$
- When $\widehat{\boldsymbol{x}}_{i}=1$ for guess $q^{*}$ :
- $L L R_{i}=\frac{P(A) \cdot p_{q^{*}}, i}{P\left(n_{q}\right)+P(A) \cdot\left(1-p_{q}^{*} ;\right)}$
seq prob +0 anyway with others
1 with others
0 with others
$\overline{\text { seq prob }+1 \text { anyway with others }}$
- These provide individual bit decision's soft information based on the codeword likelihood.
- These use the reordered $\Delta_{q}$ 's.


## But what about Ext? Int?

- After the above calculations are complete,
- $L L_{e x t, i}=L L_{i}-\log \left(p_{q, \text { chan }, i}\right)-\log \left(p_{q, \text { int }, i}\right)$ - where $p_{q, i}=p_{q, \text { chan }, i} \cdot p_{q, i n t, i}$ is time $i$ only ss prob.
- Where the intrinsic is the a priori or previous decoder's supplied extrinsic


## A GRAND Iterative Decoder

## Examples?

- I don't have one yet.
- There is no MIT publicly available software to compute this soft information.
- It appears tedious, but probably not that much calculation in that the successive guesses only differ in one or a few bit positions - so incrementally updated at only the guess-bit positions.
- The inventors claim very significant decoding complexity reduction, on average.
- And it appears they are correct.


## Great extra credit problem for motivated student,

But don't underestimate this either.

## Product Codes \& GRAND

Section 8.3.3

## Product Codes (PCs) in General

- Begin with Example (from J. Gill's EE387)
- Two $(8,4,4)$ expanded Hamming codes:

| Code1 / Code 2 | $k_{2}=4$ | $n_{2}-k_{2}=4$ |
| :---: | :--- | :---: |
| $k_{1}=4$ | Input data bits (16) | Parity for code 2 (16) |
| $n_{1}-k_{1}=4$ | Parity for code 1(16) | Parity on parity (16) |

- There are $k_{1} \cdot k_{2}$ input bits (so 16 ).
- There are $n_{1} \cdot n_{2}$ output bits (so 64 ).
- The rate is $r=r_{1} \cdot r_{2}$ (so $1 / 4$ ).
- Free distance is $d_{f r e e, 1} \cdot d_{f r e e, 2}$ (so 16).


## Larger distance, lower rate

- This product code corrects up to 7 errors.


## For AWGN, the ML decoder is difficult (like most serious block codes)

There are also product code of convolutional codes; this is turbo without the random interle

## GRAND offers PC an iterative decoding solution

- GRAND Code 1 (horizontally) - compute soft information (previous section).
- GRAND Code 2 (vertically) -- use Code 1's extrinsic information as intrinsic input
- Repeat the cycle
- $(16,11)^{\sim}$ Exp Hamming

Soft-output (SO) GRAND and long, low rate codes to outperform 5 LDPCs.


 Hamithon Insitute
Maynoorth Universit, reland
kevinell Maynoort Universin, Ireland
Kevingalligan.2020emumailie




Fig. 5: Decoding performance of the $(256,121)$ GG LDPC with maximum number of iterations $I_{\max }=50$ as compared to a $(256,251)=(16,11)^{2} \mathrm{eBCH}$ product code decoded using 1line-ORBGRAND for list decoding with list size $L=4$, $\alpha=0.5$ and maximum iteration number $I_{\max }=20$. Upper panel: BLER and BER performance. Lower panel: average number of queries per-bit until a decoding with GRAND, where parallelized assumes all rows/columns are decoded in parallel.

It's not clear (to met yet) exactly how the 50 iterations LDPC compares to GRAND's 20

## Seems to be best codes yet (full circle to beginning)

- It's the decoder. Most codes are good, just AWGN-ML decoder previously appeared too complex.
- via GRAND - perhaps ML decoding is not too complex after all on the simple product codes.
- Puncturing and rate-adaptation?
- The product codes need not be the same for horizontal and vertical.
- This creates a lot of flexibility - perhaps more than puncturing (so punt the puncture? :)
- High-speed parallel implementations
- Active research area.


# Now, we have a few good methods for $\Gamma \rightarrow 0 \mathrm{~dB}$ \& 

Can exploit them to optimize larger gains from other effects!

## Comparing Ethan's codes to ORBGRAND

- It's the decoder. Most codes are good, just AWGN-ML decoder previously appeared too complex.
- via GRAND - perhaps ML decoding is not too complex.

$$
\frac{E_{b}}{N_{0}}=R \cdot \mathrm{SNR} \Rightarrow \mathrm{SNR}=\frac{1}{\mathrm{R}} \frac{\mathrm{E}_{\mathrm{b}}}{\mathrm{~N}_{0}}
$$

- Consider operating with $\mathrm{SNR}=3 \mathrm{~dB}$ :
- The previous ORBGRAND plot operates at $r<1 / 2$, which implies their $\frac{E_{b}}{N_{0}}=3 \mathrm{~dB}$ corresponds to a better channel than the 3dB SNR in my channel. (There's a factor of 2 scaling somewhere).
- The list-decoded convolutional code outperforms ORBGRAND in terms of FER at higher code rate.


## End Lecture 12

[1] Ethan Liang , Hengjie Yang , Dariush Divsalary, and Richard D. Wesel, "List-Decoded Tail-Biting
Convolutional Codes with Distance-Spectrum Optimal CRCs for 5G," IEEE Globecom 2019.
[2] Hengjie Yang, Ethan Liang , Hanwen Yaoy, Alexander Vardyy, Dariush Divsalarz, and Richard D. Wesel , A List-Decoding Approach to Low-Complexity Soft Maximum-Likelihood Decoding of Cyclic Codes, Globecom 2019.

