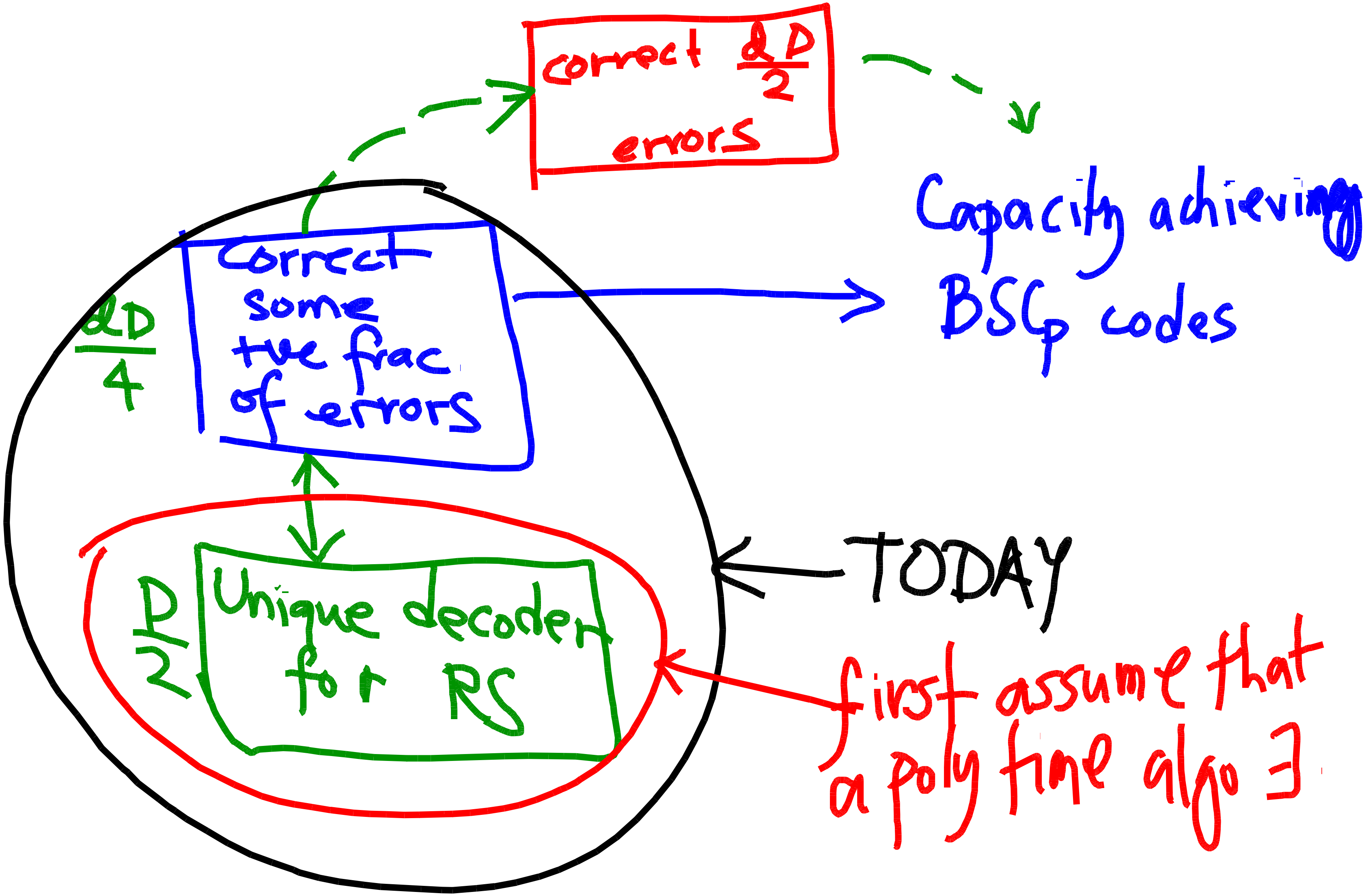
ANNOUNCEMENT: (*) APRIL 20 deadline for Wikipedia entry

↳ Start playing with in-house wiki soon

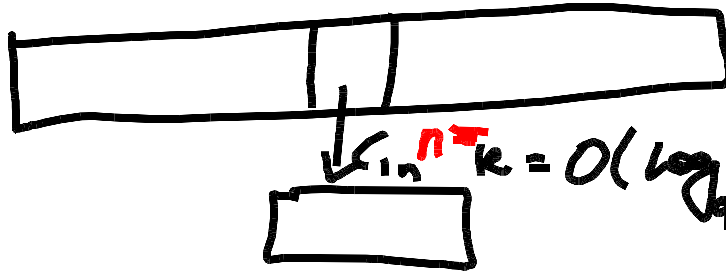
(*) MAY 7, 8 ; 1-4 pm Bell 242
paper presentations

RECAP: Strongly explicit asymptotically good codes.

Q: Can we design poly time decoding algo for concatenated codes that correct $< \frac{dD}{2}$ errors?


correct $\frac{\alpha D}{2}$ errors
Capacity achieving $BSC_p$ codes
Correct some +ve frac of errors
$\frac{\alpha D}{4}$
$\frac{D}{2}$
Unique decoder for RS
TODAY
first assume that a poly time algo $\exists$

(RS) $C_{out}$



$C_{in}$ $n = k = O(\log_q N)$

$N' = nN$

poly($N'$)

→ Suggest and go?

$\boxed{\text{ALG1}}$

→ "Reverse" the encoding process

$y = (y_1, \ldots, y_N) \in [q^n]^N$

→ Decode inner codes first

Define $y' \in [q^k]^N$ s.t. $y'_i = MLD_{C_{in}}(y_i)\ \forall i$ — $O(nq^k) = O(nN)$

How many errors?

→ Decode outer code

Run RS decoder on $y'$ — poly($N$)

poly($nN$)

**THM:** ALG 1 can correct $< \frac{dD}{4}$ errors.

unique → ($m \to$ transmitted message)

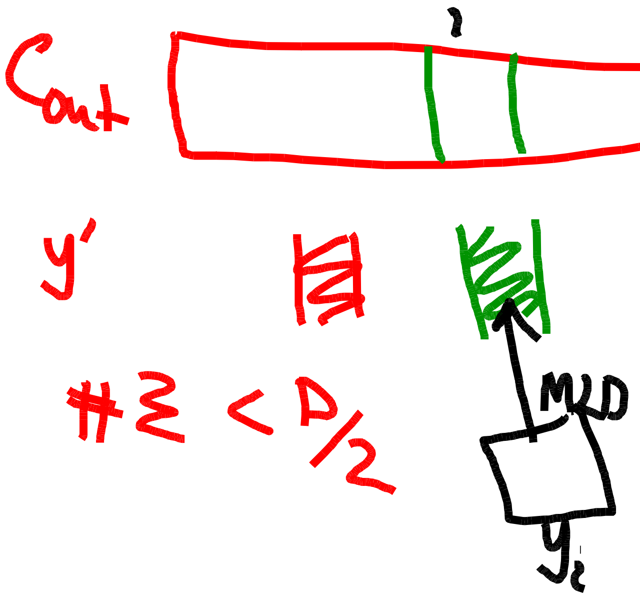
**Idea:** $< \frac{dD}{4} \Rightarrow$ sufficient condition is satisfied

**Suff. condition:** Step 2 works i.e.

$$\Delta(y', C_{out}(m)) < \frac{D}{2}$$

we get $\boxtimes$ if $\Delta(y_i, C_{in}((C_{out}(m))_i)) < \frac{d}{2}$

as $MLD(y_i) = C_{out}(m)_i$




$\boxtimes$ disagree

$\boxtimes$ agree

$\# \boxtimes < D/2$

$< \frac{dD}{4}$ errors $\Rightarrow$

$< \frac{D}{2}$ positions where

$\Delta(y_i, C_{in}((C_{out}(m))_i)) \geq \frac{d}{2}$

# Poly time unique decoder for RS codes

Correct $< \frac{D}{2}$ errors

→ Peterson 1960 $O(n^3)$

↳ poly time being efficient was not yet established.

→ Berlekamp-Massey $O(n^2)$

→ $O(n \, \mathrm{poly}(\log n))$ algo

→ Berlekamp-Welch $O(n^3)$

↳ US patent

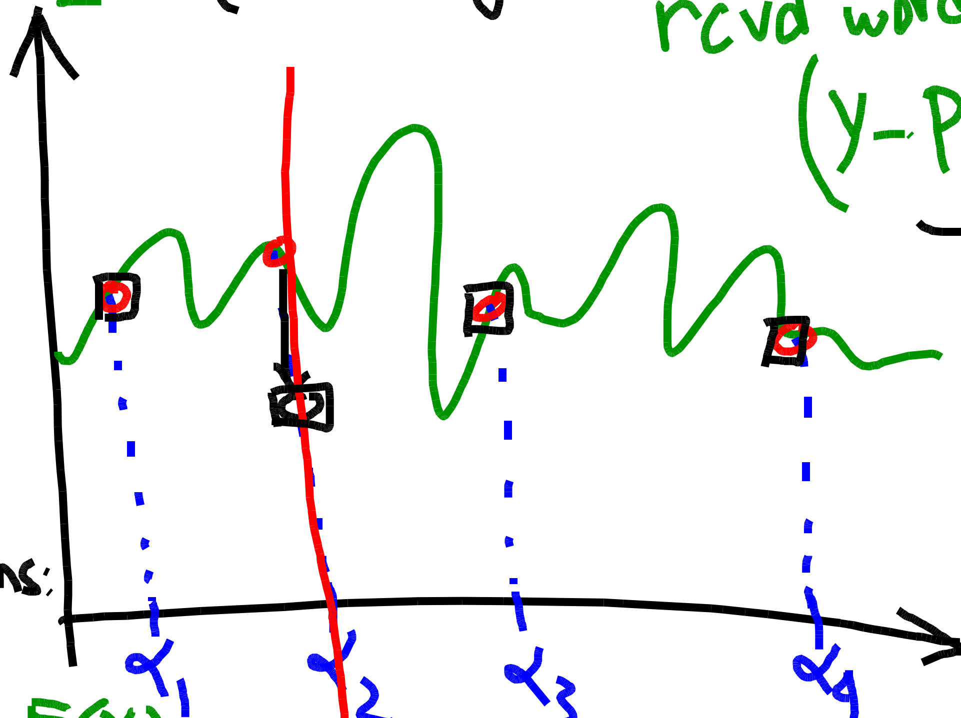
↳ Gemell-Sudan 92

$e < \frac{D}{2} = \frac{N-K+1}{2}$ (knowing E ⇒ erasure noise model)

rcvd word:

$$\underbrace{(y-P(x))\,(x-\alpha_2)}_{0 \qquad =0}=0$$

E → set of error locations:




$y-P(x)=0$

$x-\alpha_2=0$

$$(y-P(x))\underbrace{\prod_{\alpha\in E}(x-\alpha)}_{E(x)} = 0 \text{ (for rcvd word)}$$

<u>Claim:</u> Knowing E ⇒ a polytime algo

or decoding erasures is easy for RS codes ($< N-K$ erasures)

can do polynomial interpolation ⇐ know $\geq K$ codeword symbols ⇐ ($< N-K$ erasures)

$$Q(X,Y) = (Y - P(X))\,E(X)$$

$$= \underbrace{Y\,E(X)}_{\text{degree} \le e} - \underbrace{P(X)\,E(X)}_{\deg \le e+K-1} \Big\}(*)$$

rcvd word is $(\alpha_i, y_i)$
$\Rightarrow \forall i,\ Q(\alpha_i, y_i) = 0$

$\rightarrow$ $Q(X,Y)$ explains $(\alpha_i, y_i)$
i.e $1 \le i \le N$, $Q(\alpha_i, y_i) = 0$

$\rightarrow$ $Q(X,Y) = Y\,\underbrace{A(X)}_{\deg = e} + \underbrace{B(X)}_{\deg \le e+K-1}$

IDEA: Compute $Q(X,Y)$ as and show that degree constraints $\Rightarrow (*)$ is the "only" solution to $Q(X,Y)$