15-750
2/1/16

Codes & Uniquely Decipherable Codes

Code:

Alphabet $\equiv \Sigma = \{0, \ldots, r-1\}$ this lecture $\{0,1\}$

CodeWord $\equiv$ string $w = a_1 \cdots a_\ell$ $a_i \in \Sigma$

Code $\equiv$ Set of codewords $\{w_1, \ldots, w_K\}$

Message $\equiv$ String of code words (concatenation)

eg: $\Sigma = \{0,1\}$

Code $\equiv \{w_1 = 01, w_2 = 0, w_3 = 10\}$

Message $\equiv w_1 w_2 w_3 = 01010$

$w_2 w_3 \cdot w_3 = 01010$

Code is <u>not</u> Uniquely Decipherable

Def: $P \cdot S = w \in \Sigma^*$ Then P prefix of w

S suffix of w

Testing UD

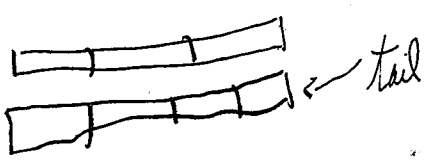
Input: Code $= \{C_1, \ldots, C_K\} = C$

Def A non-empty word (string) t is a tail if $\exists$ messages $C_1 \cdots C_m$ & $C_1' \cdots C_n'$ s.t.

1) C_i, C_j' are code words & $C_1 \neq C_1'$
2) t is a suffix of C_n'
3) $C_1 \cdots C_m t = C_1' \cdots C_n'$

Lemma C is UD iff no tail is a code word.

($\Leftarrow$) (contrapositive) if not UD $\Rightarrow \exists$ tail as codeword



($\Rightarrow$)($\exists$ tail codeword $\Rightarrow$ not UD)

Same argument

Alg (Generate All Tails)

Generate-All-Tails (tails = $\emptyset$)

1) $\forall C_i \& C_j$ $(i \neq j)$

   a) $C_i = C_j$ return "not UD"

   b) $\exists s$ s.t. $C_i s = C_j$ or $C_i = C_j s$

      tails = tails $\cup \{s\}$

2) $\forall c \in C \; \forall t \in$ tails (memoize)

   a) $t = C$ return not UD

   b) $\exists s$ $ts = C$ (2b') or $Cs = t$ (2b'')

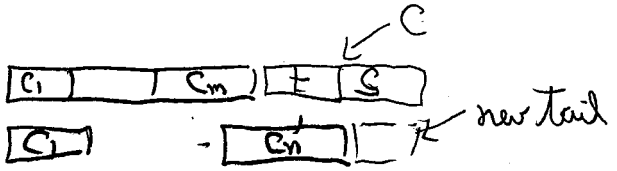
      tails = tails $\cup \{s\}$

3) return C is UD

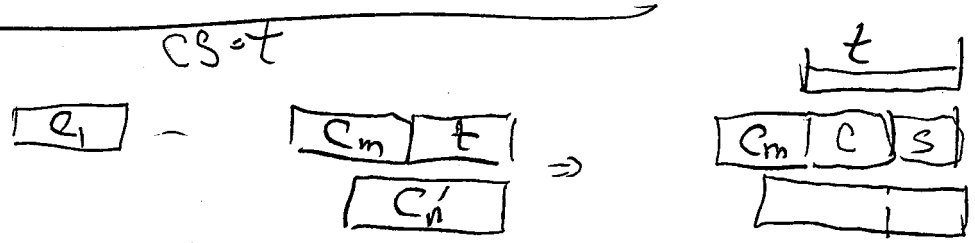
Claim 1 Alg generates only tails

1b) is OK

2b) $ts = c$



$cs = t$



Claim2 Either Alg returns "not UD" or it generates all Tails

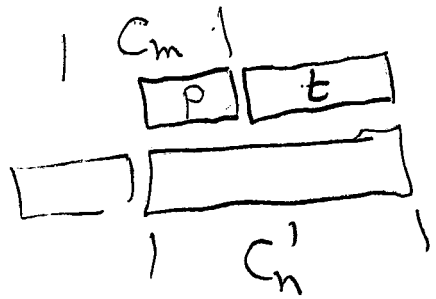
Let t be a tail $c_1 \cdots c_m t$ with min n+m
$c_1' \cdots c_n'$

Def $m(t) = \min\{n+m\}$

Induct on $m(t)$

$m(t) = 1$ done by step 1)

Assume true for $k < n+m$

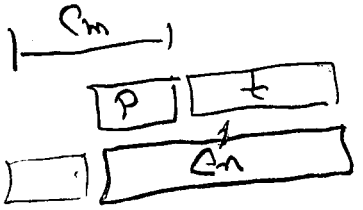


Case a

$P = C_m$ then P is found trivially and alg returns "not UD"

Case b

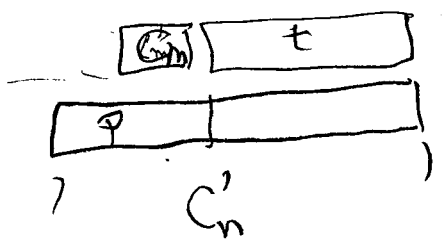
P suffix of C_m



induct $P \in Tails \Rightarrow t \in Tails$ (2b')

Case c

C_m suffix of P



$C_m t \in Tails \Rightarrow t \in Tails$ (2b'')

Timing: n words max length l

$\#\,tails \leq n \cdot l$

Step 1 $O(n^2 \cdot l)$ $O(n \cdot l)$?

Step 2 $\#words = n$, $\#tail = n \cdot l$, cost per pair l $\Big)$ $O(n^2 \cdot l^2)$