

i תהי  $msg$  הוקדשה באורך  $k$ .  $s/c$ :

$$n = |C(msg)| = |R(msg) + par(R(msg))| = k \cdot t + 1$$

ס"כ  $n = k \cdot t + 1$

ביטויים  $k$  תווים  $t$  שונים  $s/c$   $par$   $t$  תווים  $t$  שונים

תהיו  $msg_1, msg_2$  הוקדשו באורך  $k$  כך ש

$$C(msg_1) \neq C(msg_2) \text{ מכך ש } C \text{ חתך } msg_1 \neq msg_2 \text{ s/c ק"ס}$$

מקום  $i$  שבו יושבים תווים שונים ב  $msg_1, msg_2$   $k$  ה"א

ש  $C(msg_1), C(msg_2)$  ישם  $t$  אינדקסים עם תווים שונים

אם  $t$  שונה בין הוסיית יהיה  $(\text{בהנחה שאין תווים שונים})$

נחסים בין  $msg_1, msg_2$  ונקב  $s$   $d \geq t$  עבור  $msg_1 = 00 \dots 0$   $k-1$

$$\Delta(C(msg_1), C(msg_2)) = t \quad msg_2 = 10 \dots 0 \quad k-1$$

$$d \leq t \quad \boxed{d = t}$$

אם  $t$  כ"ס-שונה בין הוסיית יהיה שונה (בהנחה שליון תווים

שונים נחסים בין  $msg_1, msg_2$  ונקב  $s$   $d \geq t+1$  עבור

$$\Delta(C(msg_1), C(msg_2)) = t+1 \quad msg_2 = 10 \dots 0 \quad k-1, \quad msg_1 = 00 \dots 0 \quad k-1$$

$$d \leq t+1 \quad \boxed{d = t+1}$$

$$n = |C(msg)| = |C_1(msg) + C_2(msg)| = n_1 + n_2 \quad ii$$

$$\boxed{n = n_1 + n_2} \quad \text{ס"כ}$$

תהיו  $msg_1, msg_2$  הוקדשו באורך  $k$  כך ש  $C_1(msg_1) \neq C_1(msg_2)$   $k$

$$C_2(msg_1) \neq C_2(msg_2) \text{ s/c } msg_1 \neq msg_2 \text{ כיוון ש } C_1, C_2 \text{ חתך. כיוון ש}$$

$msg_1 \neq msg_2$   $C_1$   $C_2$  חתך מקיים:

$$\Delta(C(msg_1), C(msg_2)) = \Delta(C_1(msg_1) + C_2(msg_1), C_1(msg_2) + C_2(msg_2)) = \Delta_{2N}^{(1)}$$

$$\Delta(C_1(msg_1), C_1(msg_2)) + \Delta(C_1(msg_1), C_2(msg_2)) + \Delta(C_2(msg_1), C_1(msg_2))$$

$$+ \Delta(C_2(msg_1), C_2(msg_2)) \geq d_1 + 0 + 0 + d_2 = d_1 + d_2$$

מקיים שיון אם הנתון בין  $msg_1, msg_2$  ה"א הנתון

המיון  $C_1$   $C_2$   $C_1$   $C_2$   $C_1(msg_1) = C_2(msg_2)$