

$$N=10$$

Курсовый № А-8-16

$$A = (N+9) \cdot 5 + 6 = 19 \cdot 5 + 6 = 101$$

$$B = (N+3) \cdot 5 + 4 = 13 \cdot 5 + 4 = 69$$

1) Проверка корректности по формулам  
для цифровых сумм и цифровых

а)  $C = A - B$ ;  $S_A = A + B$ , нуль  $m = 7$

цифровой контроль

1) а)  $C = 101 - 69 = 32$

$$\tau(C') = 32 \bmod 7 = 4$$

$$\tau'(C) = \tau(A) - \tau(B) \bmod 7 = (101 \bmod 7 - 69 \bmod 7) \bmod 7 =$$

$$= (3 - 6) \bmod 7 = -3 \bmod 7 = 4$$

$$\tau(C') = \tau'(C) = 4$$

б)  $C = 101 \cdot 69 = 6969$

$$\tau(C') = 6969 \bmod 7 = 4$$

$$\tau'(C) = (101 \bmod 7 \cdot 69 \bmod 7) \bmod 7 = (3 \cdot 6) \bmod 7 =$$

$$= 18 \bmod 7 = 4$$

$$\tau(C') = \tau'(C) = 4$$



# Шуфровый компрессор

$$n = km + 1$$

$m$  - модуль,  $k$  - произвольное число

Пусть  $k = 7$ , тогда  $n = 7 \cdot 7 + 1 = 50$ .

$$A = 101_{10} = 21_{50}$$

$$B = 69_{10} = 1[19]_{50}, \text{ где } [19] - \text{это шуфра.}$$

$$1 \cdot 50^1 + 19 \cdot 50^0 = 50 + 19 = 69_{10}$$

$$z_4(A) = z(2+1) = z(3) = 3 \bmod 7 = 3$$

$$z_4(B) = z(1+19) = z(20) = 20 \bmod 7 = 6$$

$$a) \quad z_4(C') = z(32) = 32 \bmod 7 = 4$$

$$z_y'(C) = (z(A) - z(B)) \bmod 7 = (3 - 6) \bmod 7 = \\ = -3 \bmod 7 = 4.$$

$$z_4(C') = z_y'(C) = 4$$

$$\delta' C = 8969_{10} = 50^2 \cdot 2 + 50^1 \cdot 39 + 50^0 \cdot 19 = 5000 + 1950 +$$

$$+ 19 = 2[39][19]_{50}, \text{ где } [39] \text{ и } [19] \text{ шуфры } \delta$$

Минимум шуфры  $\delta$  основан на 50.

$$z_4(C') = z(2+39+19) = 60 \bmod 7 = 4$$

$$z_y'(C) = (z_4(A) * z_4(B)) \bmod 7 = 18 \bmod 7 = 4$$

$$z_y'(C) = z_4(C') = 4$$



2) Показать корректность по времени поворота операций.

$$a) C = A \oplus B \quad b) C = A \wedge B \quad b) C = A \vee B$$

$$N = 10 \Rightarrow m = 7$$

$$A = 101_{10} = 01100101_2$$

$$B = 69_{10} = 01000101_2$$

$$a) C = A \oplus B = 00100000_2 = 32_{10}$$

Умножение корректно

$$z(A) = 101 \bmod 7 = 3$$

$$z(B) = 69 \bmod 7 = 6$$

$$z(C') = 32 \bmod 7 = 4$$

$$D = z(A \wedge B) = z_{10}(\cdot \cdot \cdot 01000101_2) = 2 \cdot 69 = 138$$

$$z(D) = 138 \bmod 7 = 5$$

$$z'(C) = (z(A) + z(B) - z(D)) \bmod 7 = (3 + 6 - 5) \bmod 7 = 4 \bmod 7 = 4$$

$$z'(C) = z(C') = 4$$



~~Умножить компоненты~~

$$k = k \cdot m + 1, \text{ где } k = 7, m = 7.$$

$$k = 7 \cdot 7 + 1 = 50$$

$$z_g(A) = z_g(21_{50}) = z_g(2+1) = 3 \bmod 7 = 3.$$

$$z_g(B) = (1+19) \bmod 7 = 6$$

$$z_g(C) = 32 \bmod 7 = 4 \quad (32 - \text{это сумма } 6 \text{ компонент умноженного компонента } 50)$$

$$D = 138_{10} = 2 [38]_{50}$$

$$z_g(D) = (2+38) \bmod 7 = 5$$

$$\begin{aligned} z_g'(C) &= (z_g(A) + z_g(B) - z_g(D)) \bmod 7 = \\ &= (3 + 6 - 5) \bmod 7 = 4 \end{aligned}$$

$$z_g'(C) = z_g(C') = 4.$$

$$\text{Д) } C = A \wedge B = 69_{10} = 1 [19]_{50} \quad \text{Умножить компоненты.}$$

$$z(A) = 3$$

$$z(B) = 6$$

$$z(C') = 6.$$

$$D = A \vee B = 01100101_2 = 101_{10} = 21_{50} = A$$

$$\begin{aligned} z'(C) &= (z(A) + z(B) - z(D)) \bmod 7 = (3 + 6 - 3) \bmod 7 = \\ &= 6. \\ z(C') &= z'(C) = 6. \end{aligned}$$

Условный конъюнкт

$$\tau_y(A) = (2+1) \bmod 7 = 3$$

$$\tau_y(B) = (1+19) \bmod 7 = 6$$

$$\tau_y(C) = (1+19) \bmod 7 = 6$$

$$D = A \vee B = A = 21_{50}$$

$$\tau_y(D) = (2+1) \bmod 7 = 3$$

$$\tau_y'(C) = (\tau_y(A) + \tau_y(B) - \tau_y(D)) \bmod 7 = (3 + 6 - 3) \bmod 7 = 6$$

$$\tau_y'(C) = \tau_y(C') = 6$$

$$b) C = A \vee B = A = 01100101_2 = 21_{50}$$

$$\tau(A) = 3; \tau(B) = 6$$

$$\tau(C) = \tau(A) = 3$$

Условный конъюнкт

$$D = A \wedge B = B = 11191_{50}$$

$$\tau(D) = \tau(B) = 6$$

$$\tau'(C) = (\tau(A) + \tau(B) - \tau(D)) \bmod 7 = (3 + 6 - 6) \bmod 7 = 3$$

$$\tau'(C) = \tau(C') = 3$$



Угловый компонент

$$z_y(A) = (2+1) \bmod 7 = 3.$$

$$z_y(B) = 6.$$

$$z_y(C) = z_y(A) = 3$$

$$D = B = 1 \ll 19350$$

$$z_y(D) = (1+19) \bmod 7 = 6.$$

$$z_{y'}(C) = z(z_y(A) + z_y(B) - z_y(D)) = (3+6-6) \bmod 7 = 3 \bmod 7 = 3.$$

$$z_{y'}(C) = z_y(C) = 3.$$

Все операции выполняются быстро

Угловый компонент функции  $z(C')$

$$z(C') = z(A+B) = z(169) = 1.$$

$$z'(C) = ((z(A) + z(B)) \bmod 7) = (3+6) \bmod 7 = 9 \bmod 7 = 2.$$

$$z(C') \neq z'(C)$$

$$1 \neq 2.$$

функция, неэрмитова