

---

# PAL: 10. cvičení

Tomáš Sieger

26. 11. 2020

---

# Opakování z minula

## Př. 9/1a: Hammingovsky blízká slova - dynamicky

---

Najděte v textu  $T$  všechny výskyty řetězců, které mají od vzorku  $P$  Hammingovu vzdálenost rovnou nejvýše  $k$ . Použijte metodu dynamického programování.

a)  $T = ccacbaabccaccbcabccc$ ,  $P = abcba$ ,  $k = 2$

a/a k=2

$\emptyset$	c	c	a	c	b	a	a	b	c	c	a	c	c	b	c	a	b	c	c	c
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	-	1	1	0	1	1	0	0	1	1	1	0	1	1	1	1	0	1	1	1
b	-	-	2	2	1	1	2	1	0	2	2	2	1	2	1	2	2	0	2	2
c	-	-	-	3	2	2	2	3	2	0	2	3	2	1	3	1	3	3	0	2
b	-	-	-	-	4	2	3	3	3	3	1	3	4	3	1	4	2	3	4	1
a							<u>2</u>				<u>1</u>				<u>2</u>	3			<u>2</u>	

## Př. 9/1a: Hammingovsky blízká slova - dynamicky

---

Najděte v textu  $T$  všechny výskyty řetězců, které mají od vzorku  $P$  Hammingovu vzdálenost rovnou nejvýše  $k$ . Použijte metodu dynamického programování.

a)  $T = ccacbaabccaccbcabccc$ ,  $P = abcba$ ,  $k = 2$

a/a k=2

$\emptyset$	c	c	a	c	b	a	a	b	c	c	a	c	c	b	c	a	b	c	c	c
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	-	1	1	0	1	1	0	0	1	1	1	0	1	1	1	1	0	1	1	1
b	-	-	2	2	1	1	2	1	0	2	2	2	1	2	1	2	2	0	2	2
c	-	-	-	3	2	2	2	3	2	0	2	3	2	1	3	1	3	3	0	2
b	-	-	-	-	4	2	3	3	3	3	1	3	4	3	1	4	2	3	4	1
a							<u>2</u>				<u>1</u>				<u>2</u>	3			<u>2</u>	

Handwritten table for a dynamic programming problem with  $k=2$ . The table shows the number of ways to partition a string into  $k$  substrings such that each substring is a palindrome. The string is "ccacbaabccaccbeabccc".

a/a	$k=2$																				
$\emptyset$	$\emptyset$	c	c	a	c	b	a	a	b	c	c	a	c	c	b	e	a	b	c	c	c
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	-	1	1	0	1	1	0	0	1	1	1	0	1	1	1	1	0	1	1	1	1
b	-	-	2	2	1	1	2	1	0	2	2	2	1	2	1	2	2	0	2	2	2
c	-	-	-	3	2	2	2	3	2	0	2	3	2	1	3	1	3	3	0	2	2
b	-	-	-	-	4	2	3	3	3	3	1	3	4	3	1	4	2	3	4	1	3
a	-	-	-	-	-	5	2	-	1	-	2	3	-	2	3	-	2	-	-	-	

Red annotations include circles around 'b' and 'c' in the string, boxes around '1', '2', '1', '2', '1', '2' in the DP table, and arrows indicating transitions between cells.

$$m_{i,k} = m_{i-1, k-1} + \sum \{ t_k \neq p_i \}$$

## Př. 9/2a: Levenshteinovsky blízka slova - dynamicky

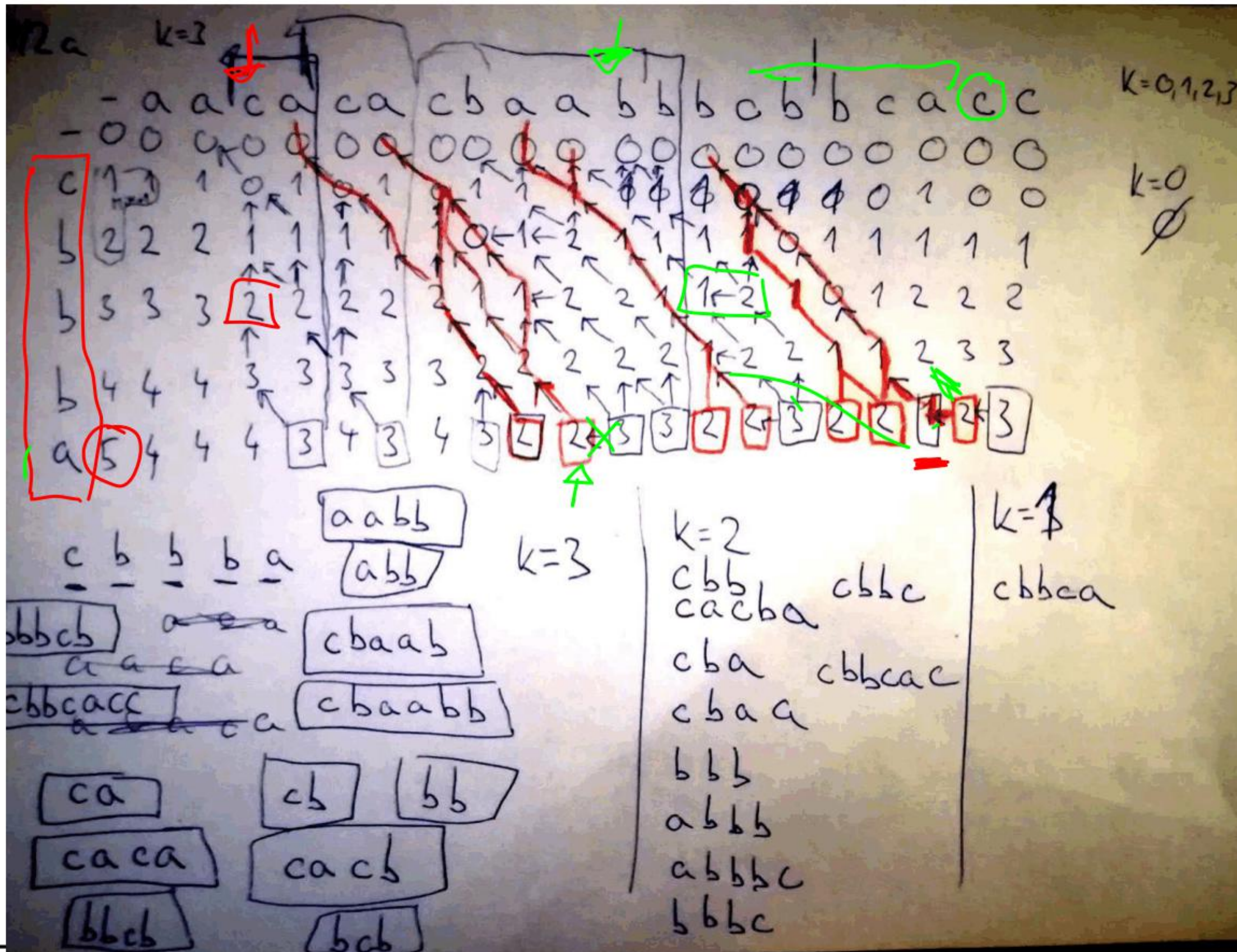
---

Najděte v textu  $T$  všechny výskyty řetězců, které mají od vzorku  $P$  Levenshteinovu vzdálenost rovnou nejvýše  $k$ . Použijte metodu dynamického programování.

a)  $T = aacacacbaabbbcbbcacc$ ,  $P = cbbba$ ,  $k = 3$





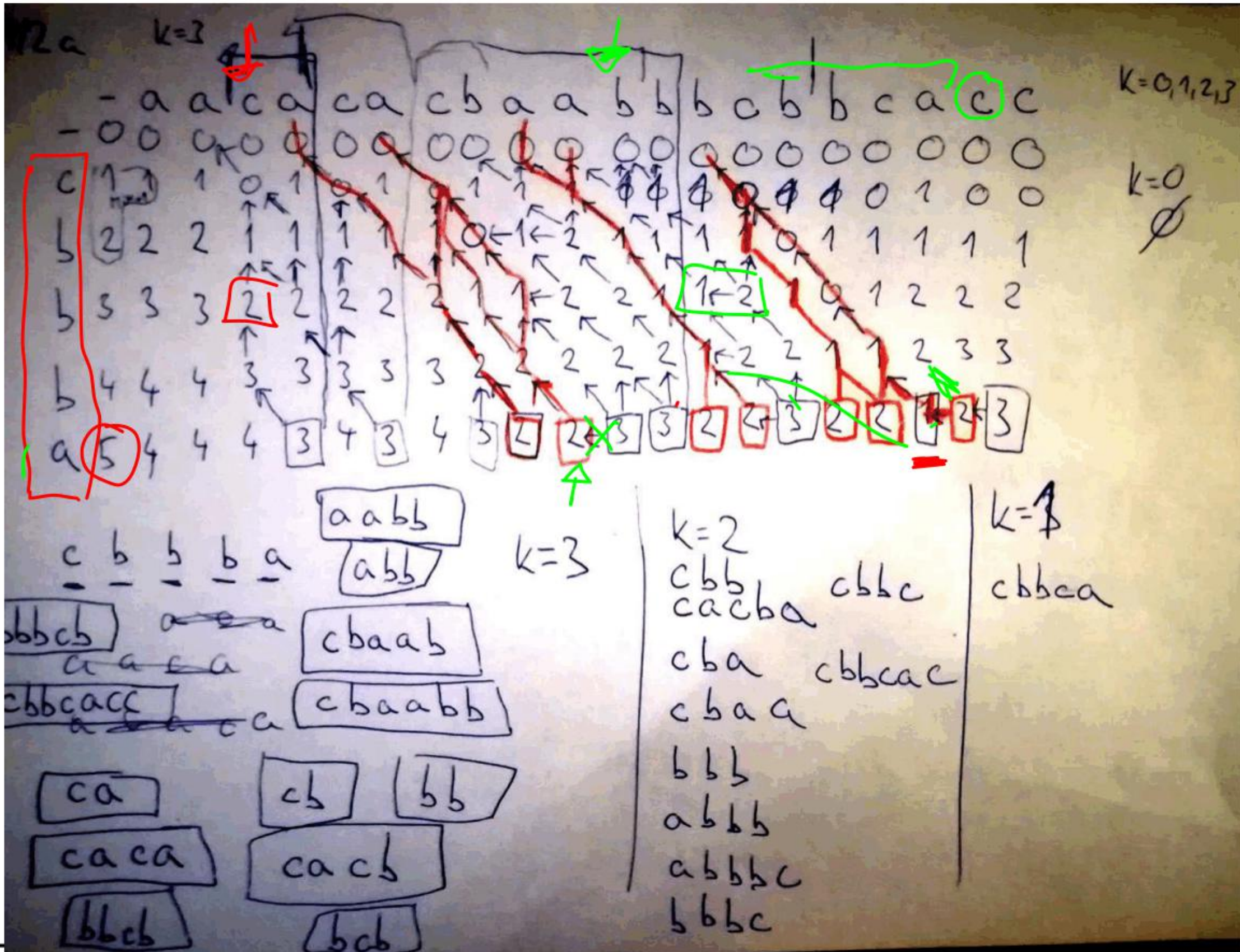


## Př. 8/13: generování podobných textů: Hamming

---

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?





7 2 4

1 INSERT

0/1 CHANGE

0/1 DELET

## Př. 8/13: generování podobných textů: Hamming

---

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

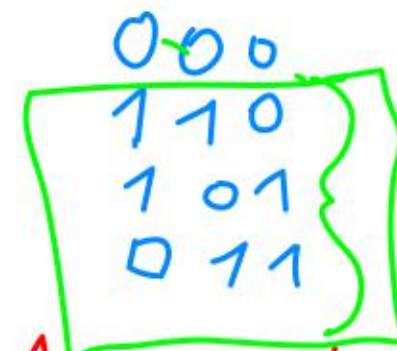
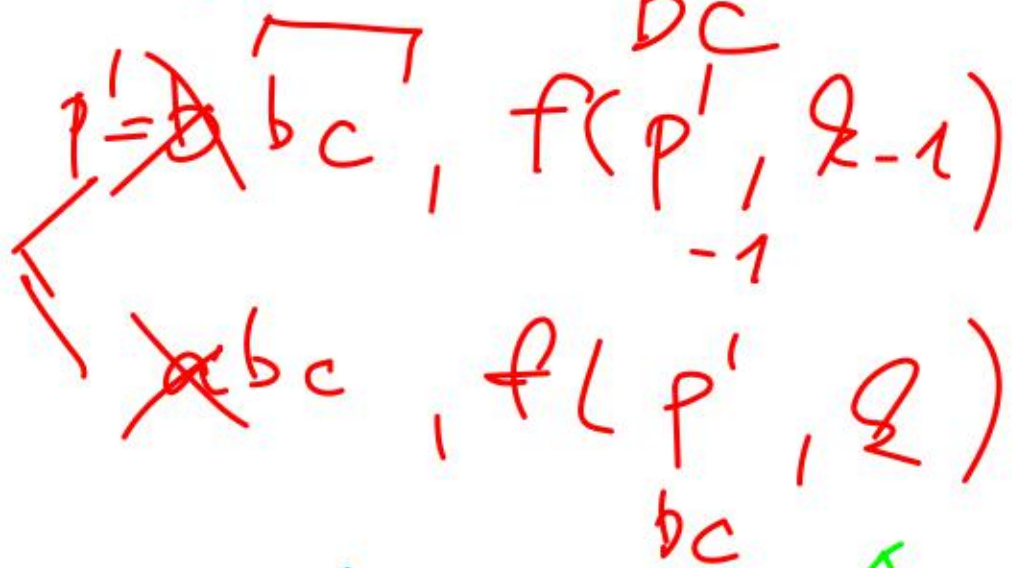
# Př. 8/13: generování podobných textů: Hamming

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

a b c

$k=2$

$f(p, k)$



$\Sigma = \{0, 1\}$   
 $\binom{n}{k} \cdot \binom{n-1}{k}$

$\lambda \neq \emptyset \ \& \ k=0$  1,2 1,2  
 $\lambda = \emptyset \ \& \ k > 0$  X

$|P| = n$   
 $k$   
 $|Z| = m$

~~$O(n \cdot m \cdot k)$~~   
 $\binom{n-k}{k} + \binom{n-k}{k} \cdot k$

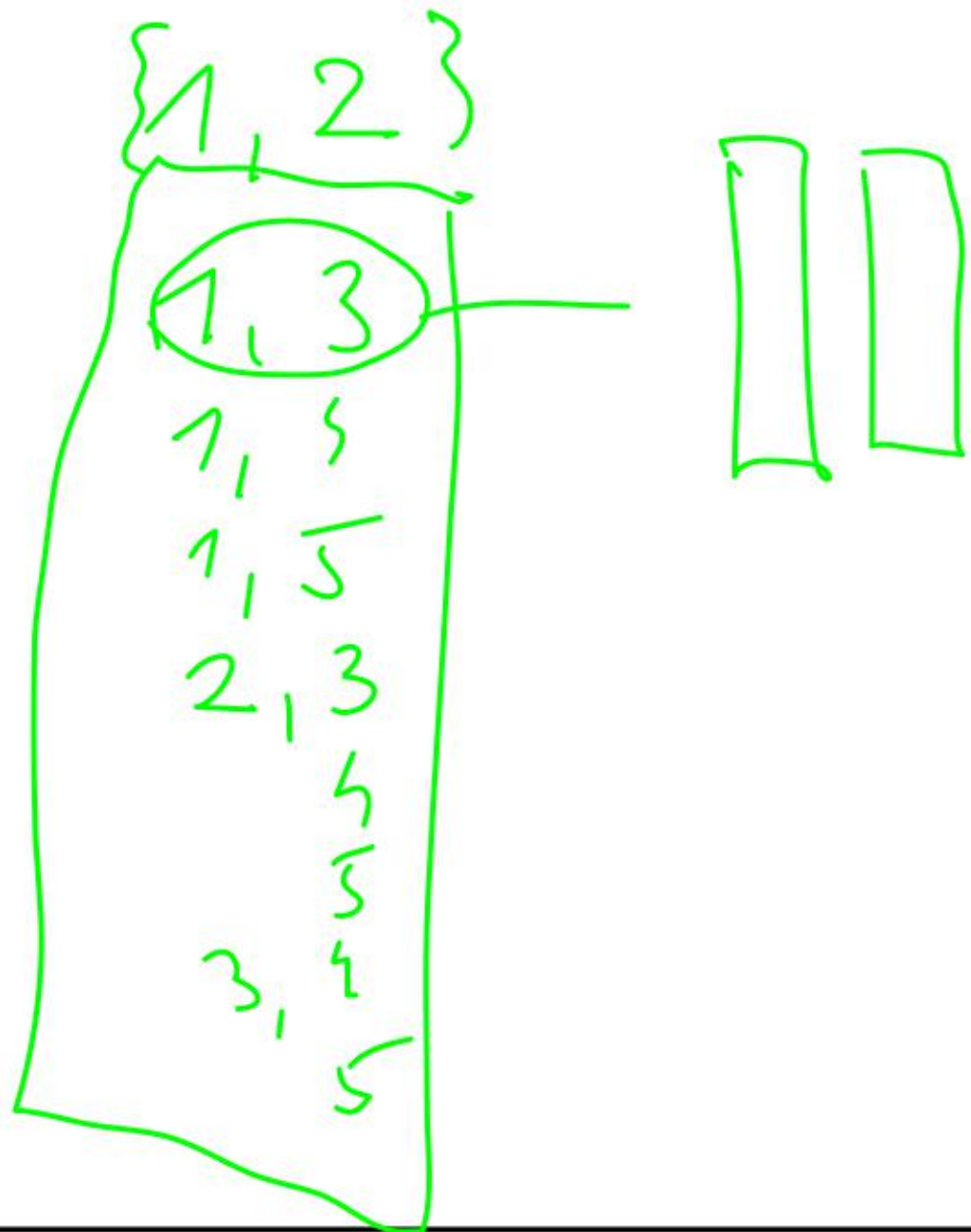






$\{1, 2, 3, 4, 5\}$

Podm. vel. 2



# Př. 8/13: generování podobných textů: Hamming

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

a b c

$k=2$

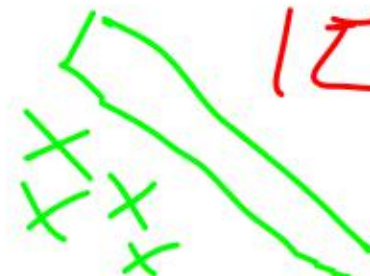
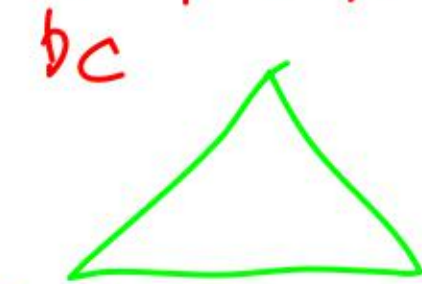
$f(p, k)$

$p' = abc$

$f(p', k-1)$

~~abc~~

$f(p', k)$



0	0	0
1	1	0
1	0	1
0	1	1

$\Sigma = \{0, 1\}$   
 $\binom{n}{k} \cdot \binom{n-1}{k}$

$\lambda \neq \emptyset$  &  $k=0$

$\lambda = \emptyset$  &  $k > 0$  ✗

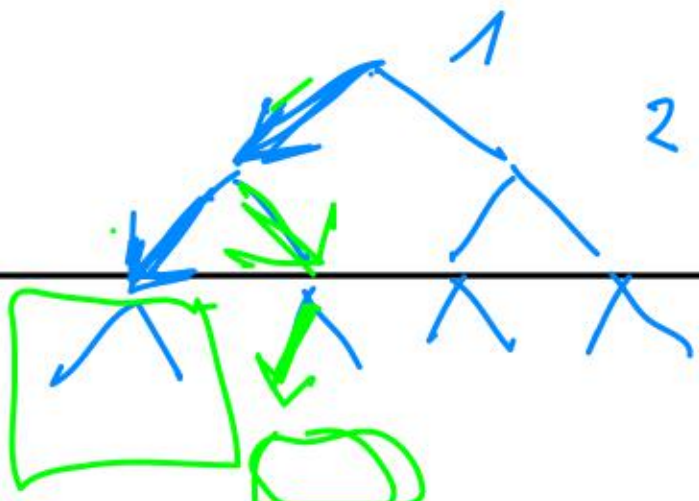
$|P| = n$

$k$

$|\Sigma| = m$

~~$O(n \cdot m \cdot k)$~~

$\binom{n-k}{k} + \binom{n-k}{k} \cdot k$



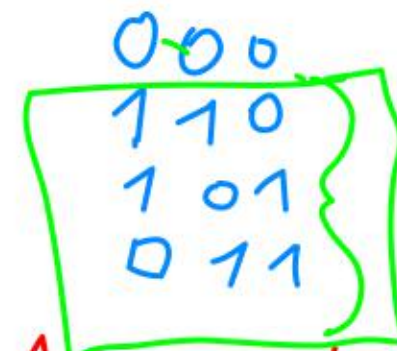
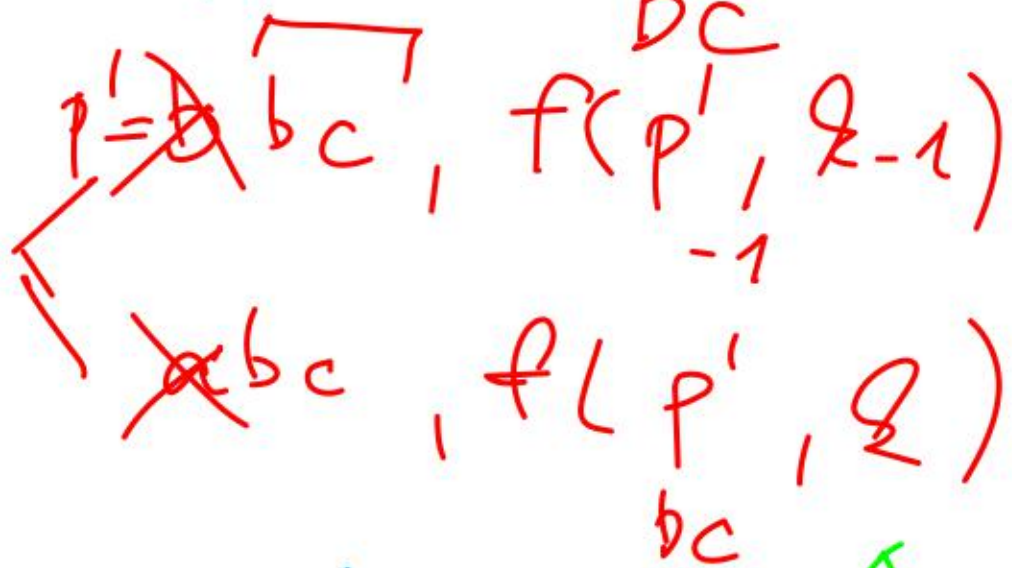
# Př. 8/13: generování podobných textů: Hamming

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Hammingovu vzdálenost právě  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

a b c

$k=2$

$f(p, k)$



$\Sigma = \{0, 1\}$   
 $\binom{m}{k} \cdot \binom{m-1}{k}$

$\lambda \neq \emptyset \quad k = 0 \quad 1, 2 \quad 1, 2$   
 $\lambda = \emptyset \quad k > 0 \quad \times$

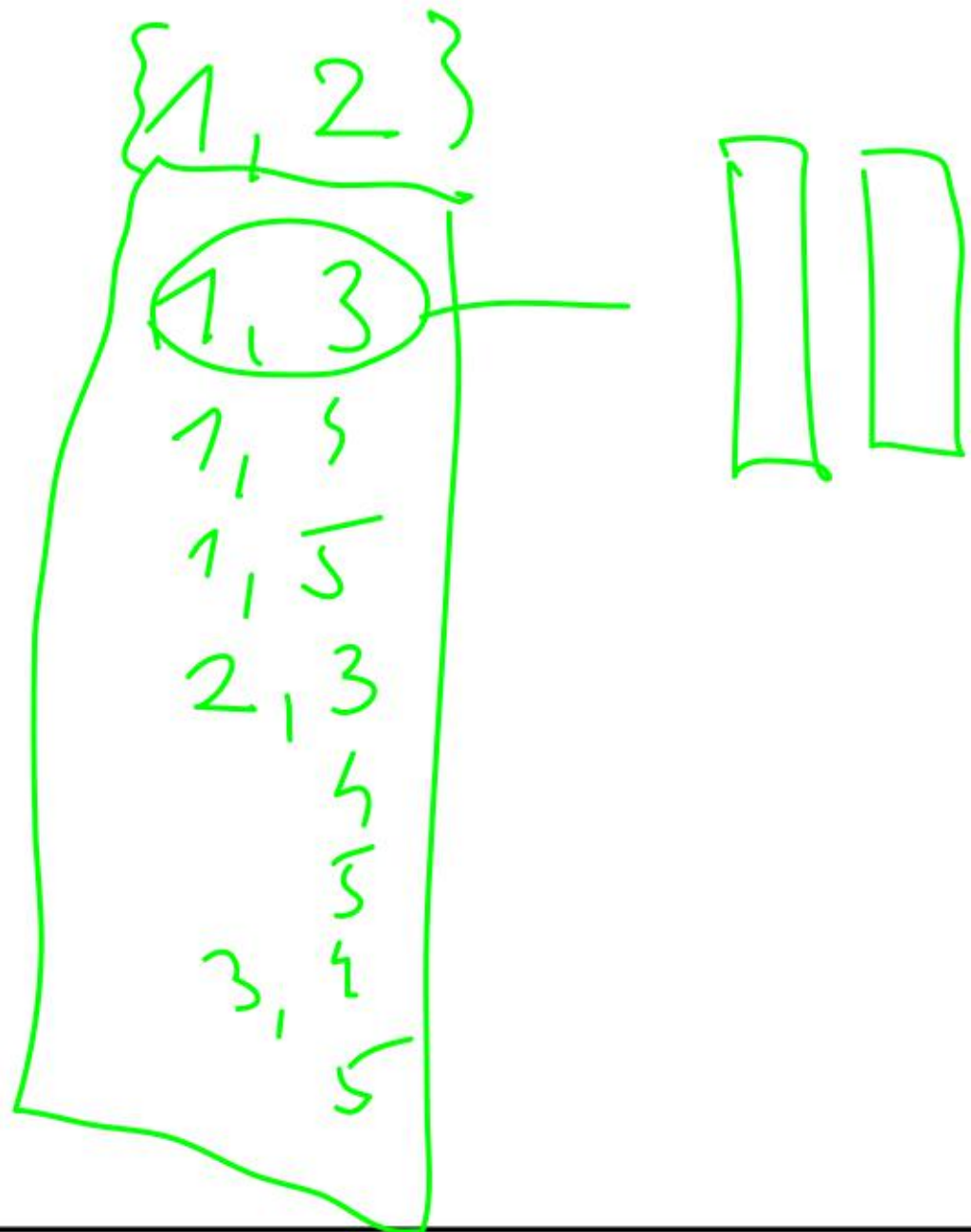
$|P| = m$   
 $k$   
 $|Z| = m$

~~$O(m \cdot m \cdot k)$~~   
 $\binom{m-k}{k} + \binom{m-k}{k} \cdot k$



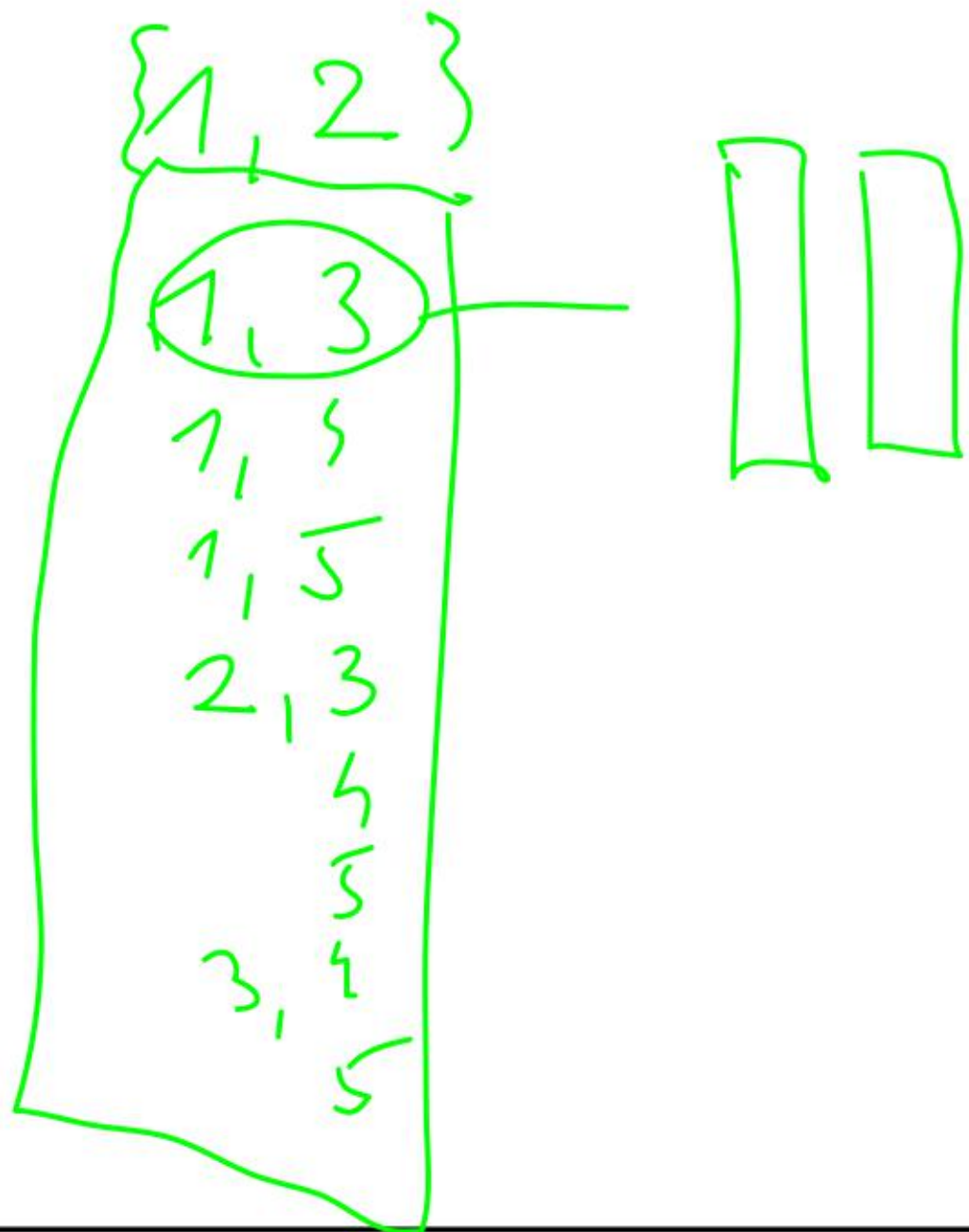
$\{1, 2, 3, 4, 5\}$

Podm. vel. 2



$\{1, 2, 3, 4, 5\}$

podm. vel. 2



## Př. 8/14: generování podobných textů: Levenshtein

---

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Levenshteinovu vzdálenost nejvýše  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

## Př. 8/14: generování podobných textů: Levenshtein

Navrhněte algoritmus pro vypsání všech slov nad abecedou  $A$ , která mají od daného vzorku  $p$  Levenshteinovu vzdálenost nejvýše  $k > 0$ . Hodnota  $k$  je pevně dána. Jaká bude asymptotická složitost tohoto algoritmu?

$a\ b$   
 $b\ b$   
 $b\ b$

$\Sigma = \{a, b, c\}$

## Př. 9/5a: bitový paralelizmus

---

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = abcbcaaccbbaa$ ,  $P = bbac$ ,  $k = 2$ ,

b)  $T = accbbaaabcba$ ,  $P = acbb$ ,  $k = 2$ .

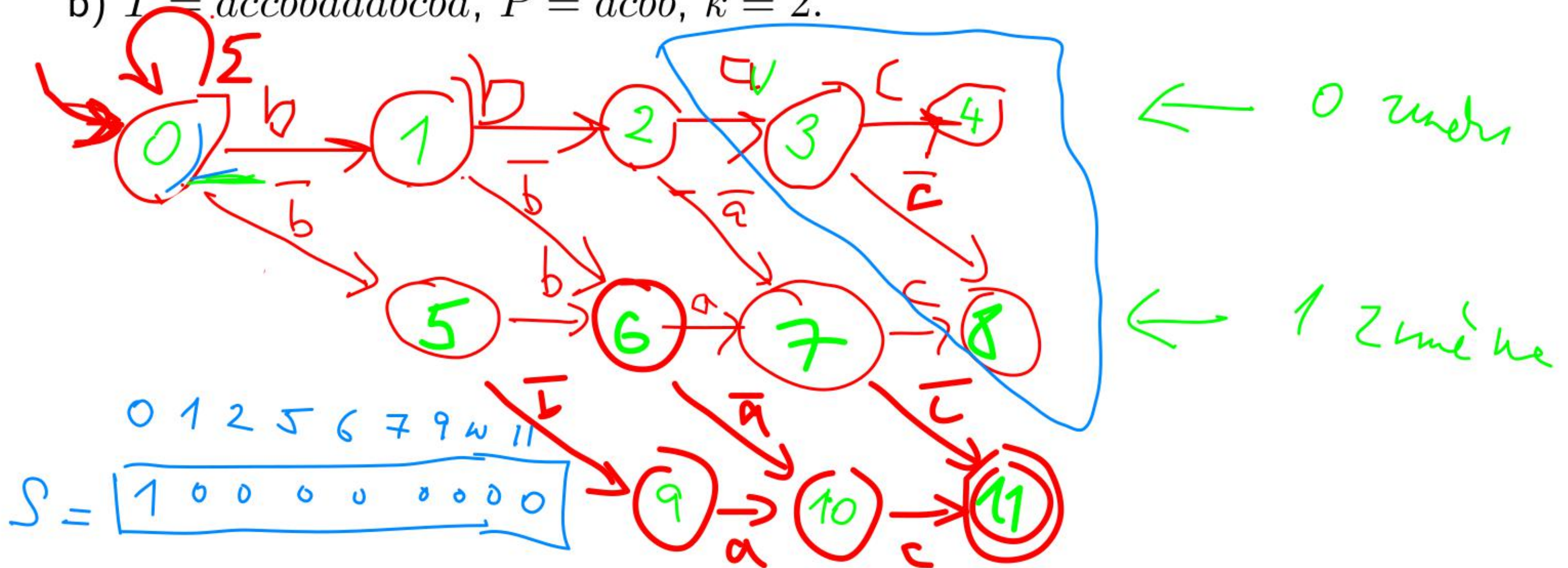


# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .





před. fce  
a b c

0

0

1

2

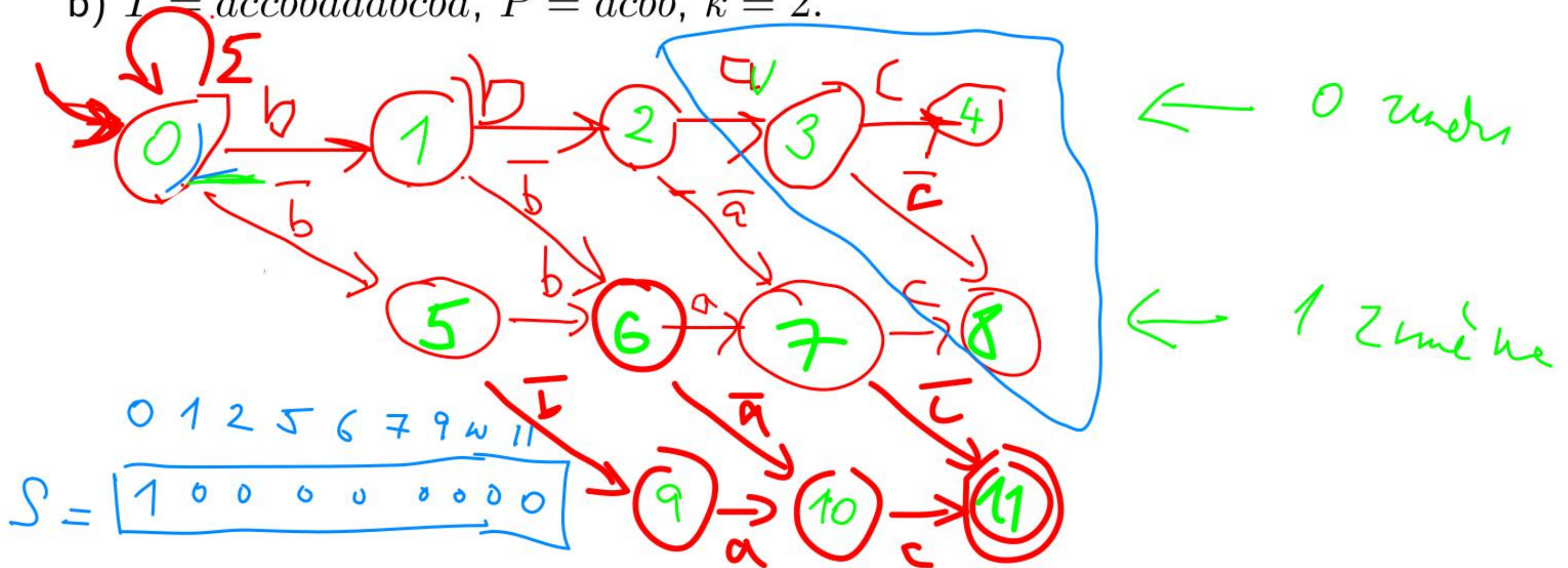
3

4

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

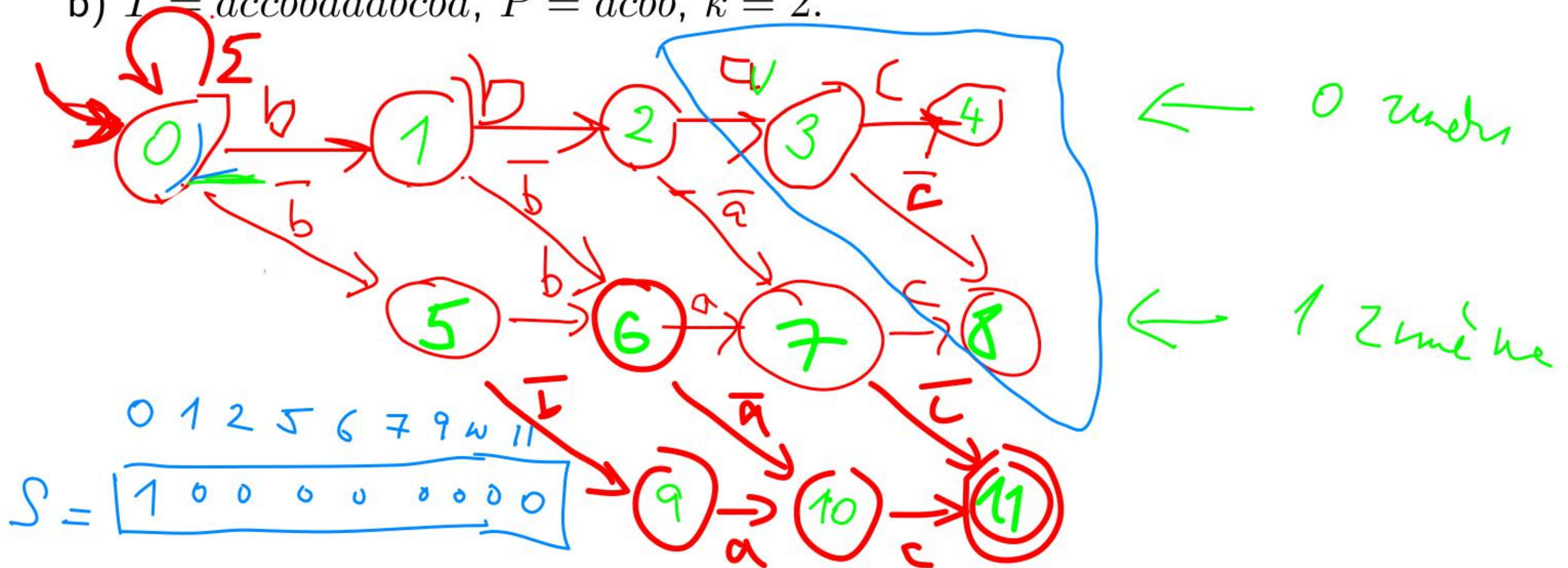
- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



před. fce  
a b c

0

0

1

2

3

4

před. fce

a b c

0

0

1

2

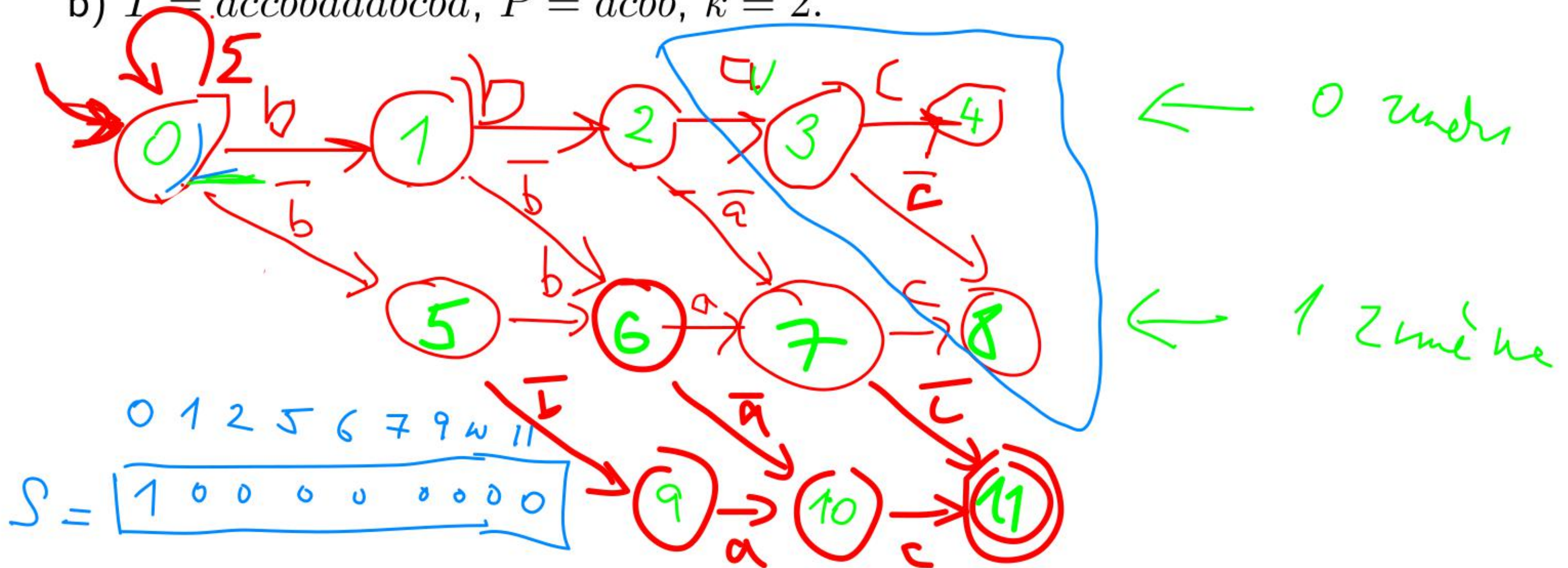
-

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .

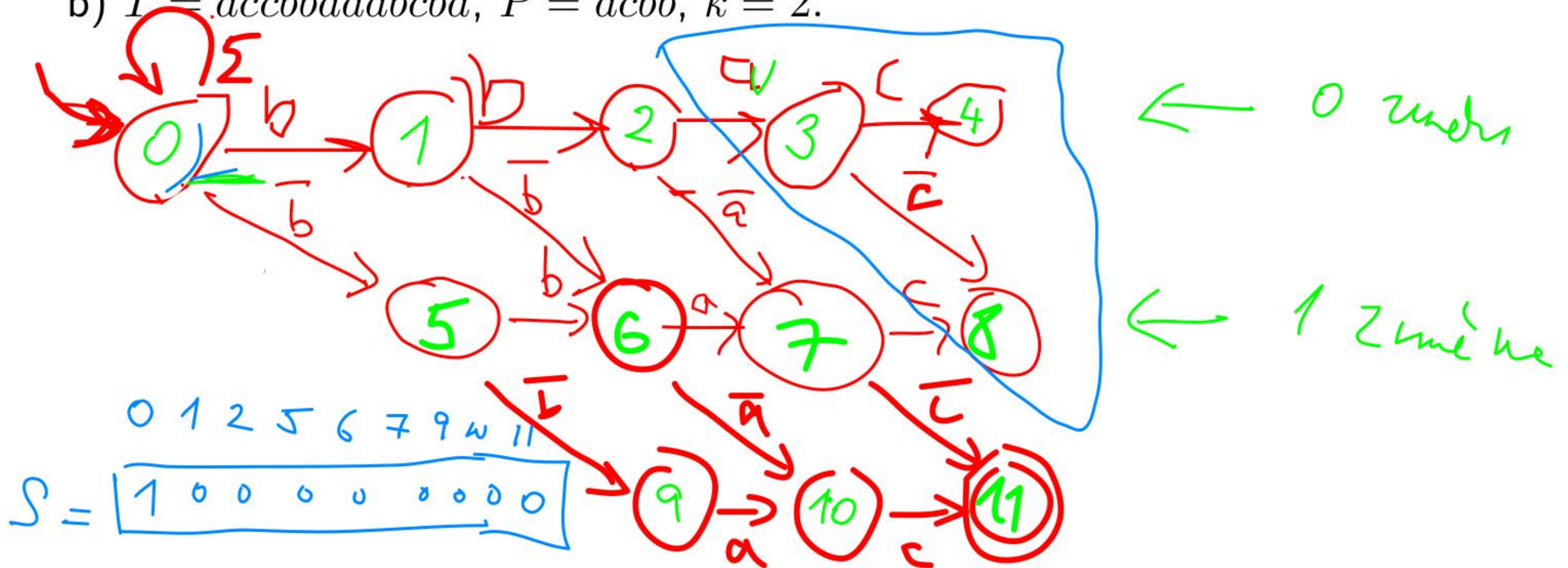




# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



před. fce

a b c

0

0

1

2

-

pred. fce

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

start →

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

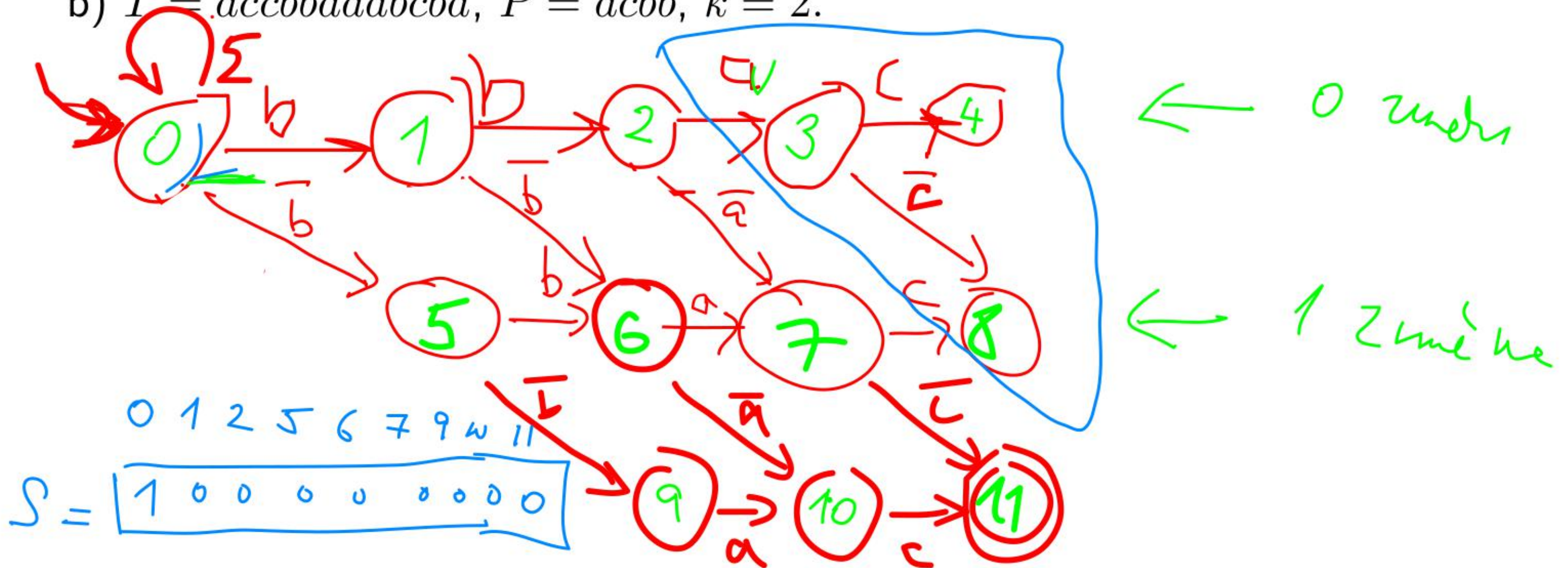
0	1	2	5	6	7	9	10	11
1	0	0	0	0	0	0	0	0

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

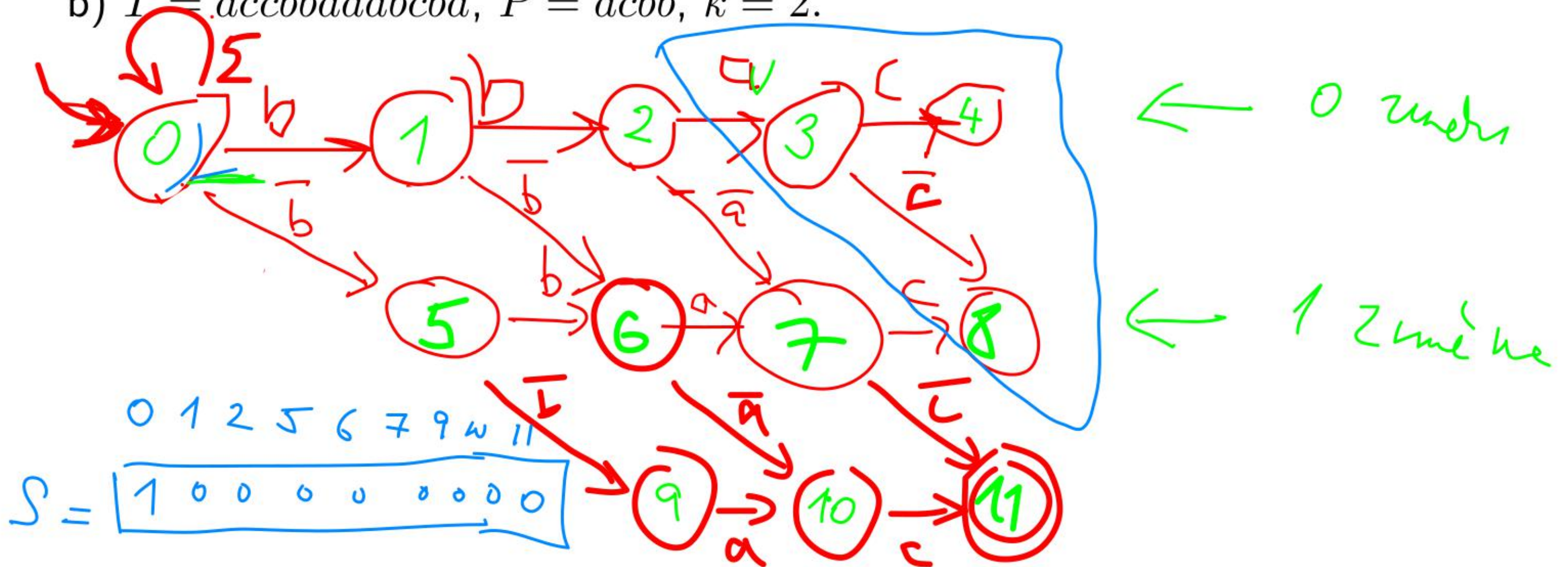
b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
 b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



pred. fce

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

start →

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

0	1	2	5	6	7	9	10	11
1	0	0	0	0	0	0	0	0

pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

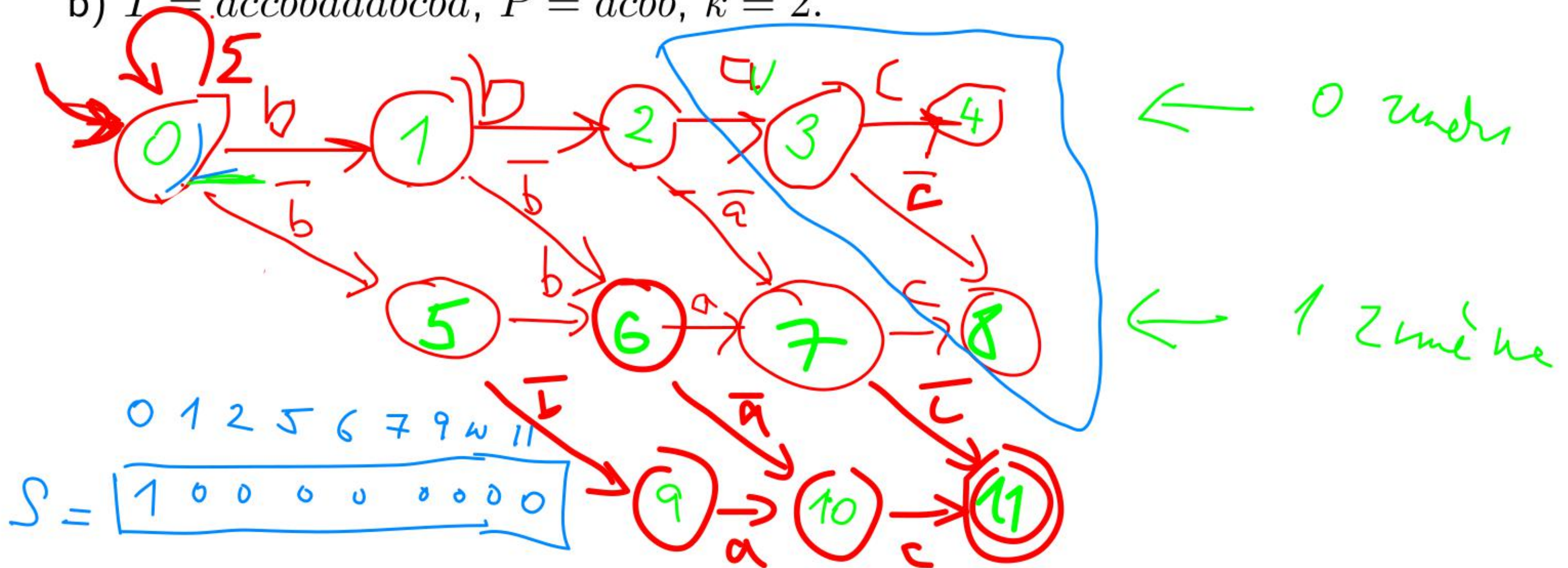
	0	1	2	5	6	7	9	10	11
$a$	1	0	0	0	0	0	0	0	0
	1	0	0	1	0	0	0	0	0

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



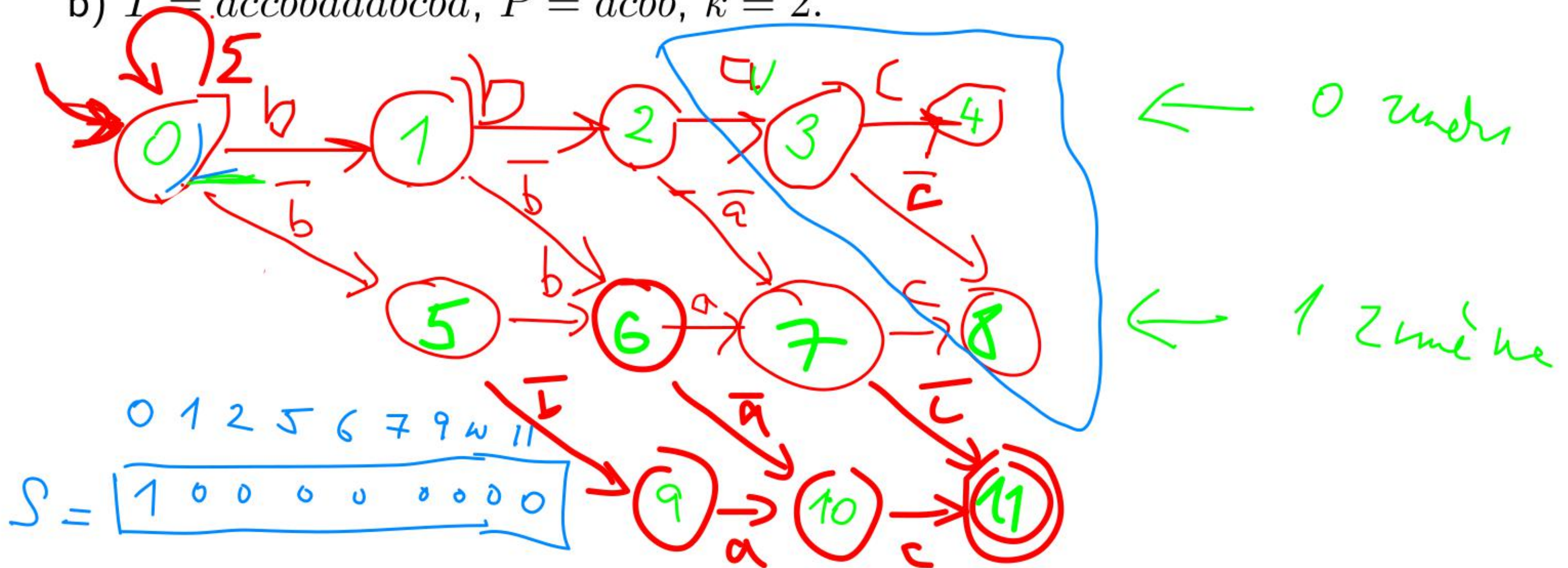


# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1\ 0\ 0\ 0\ 0\ 0}$$

for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
$a$	1	0	0	0	0	0	0	0	0
	1	0	0	1	0	0	0	0	0

pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

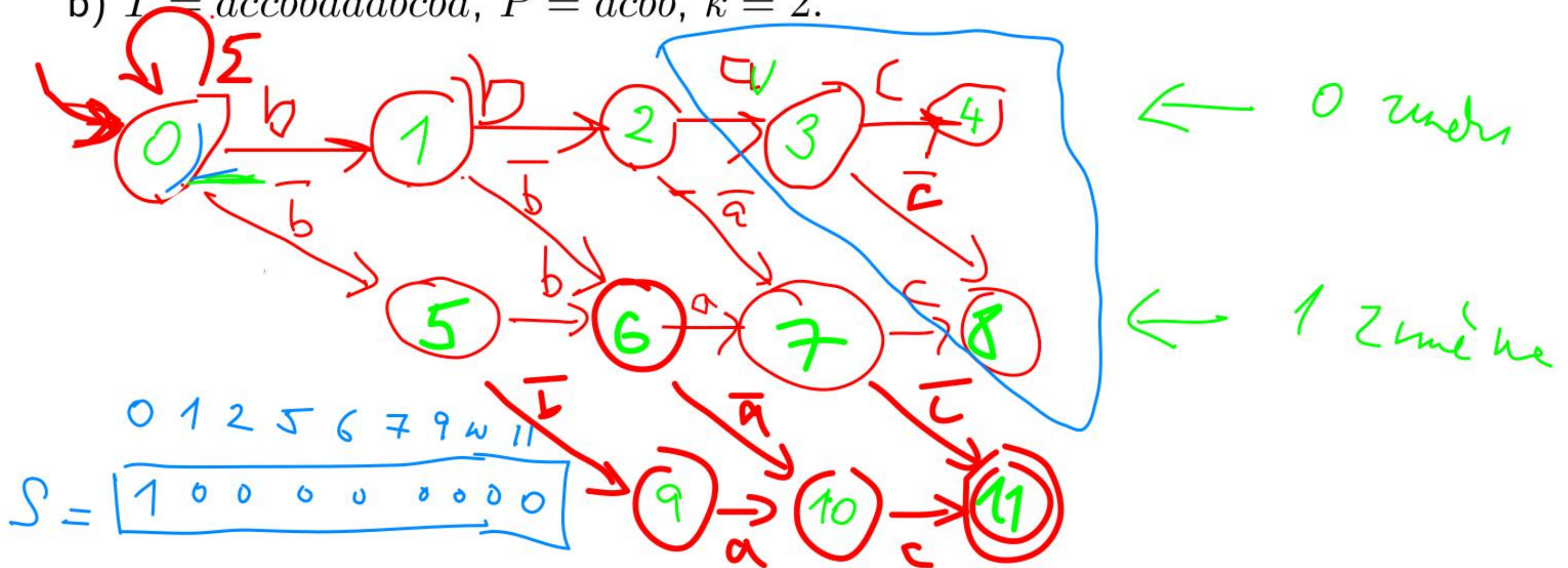
for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
d	1	1							

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .

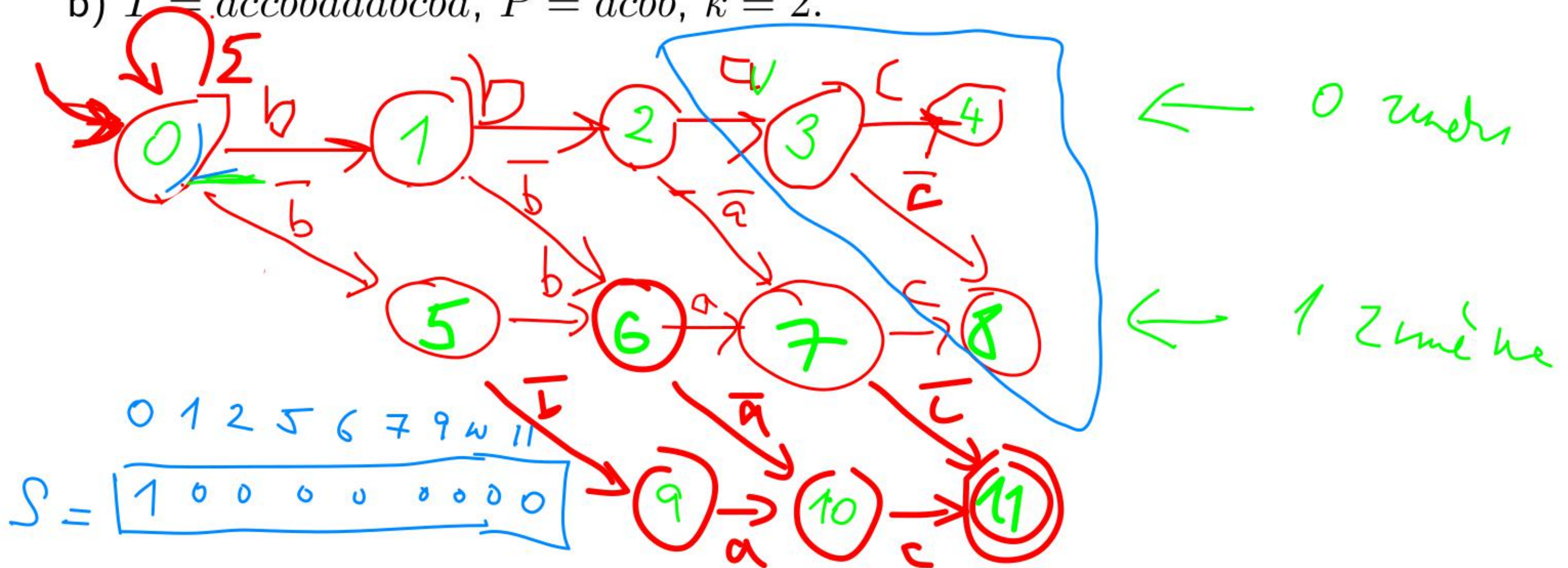


# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
b	1	1							

pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

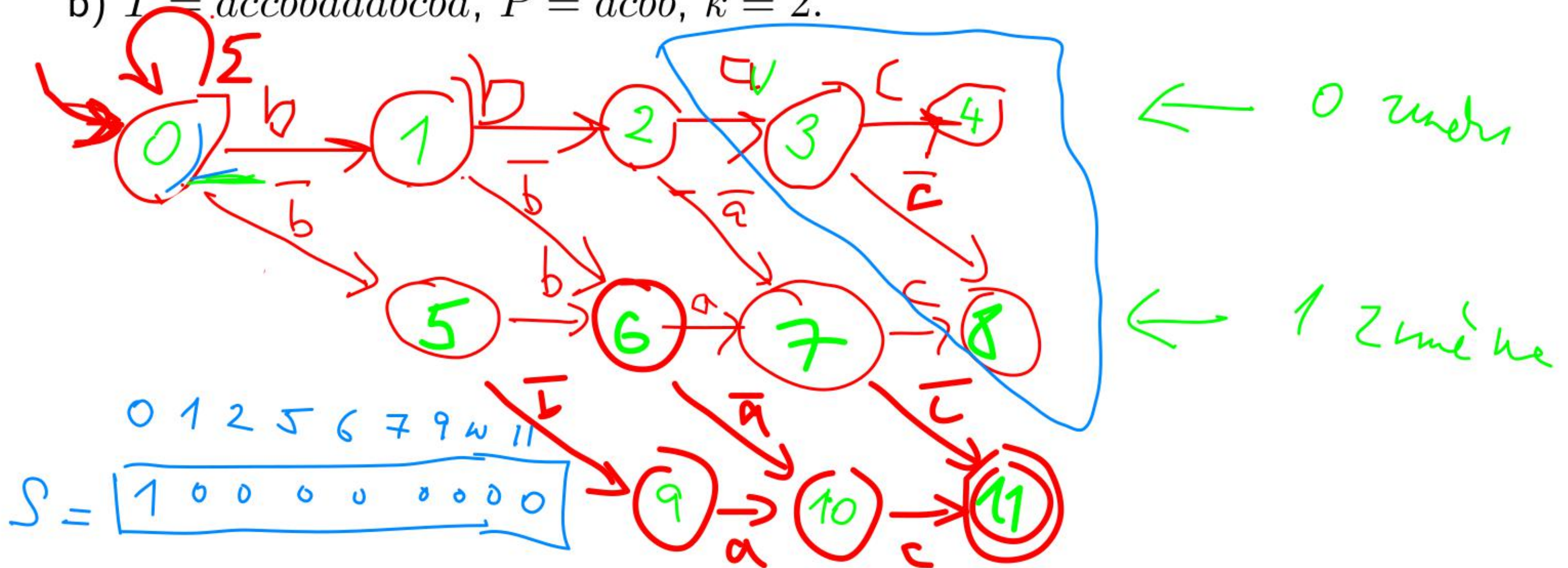
	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
b	1	1	0	0	1	0	0	0	0

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



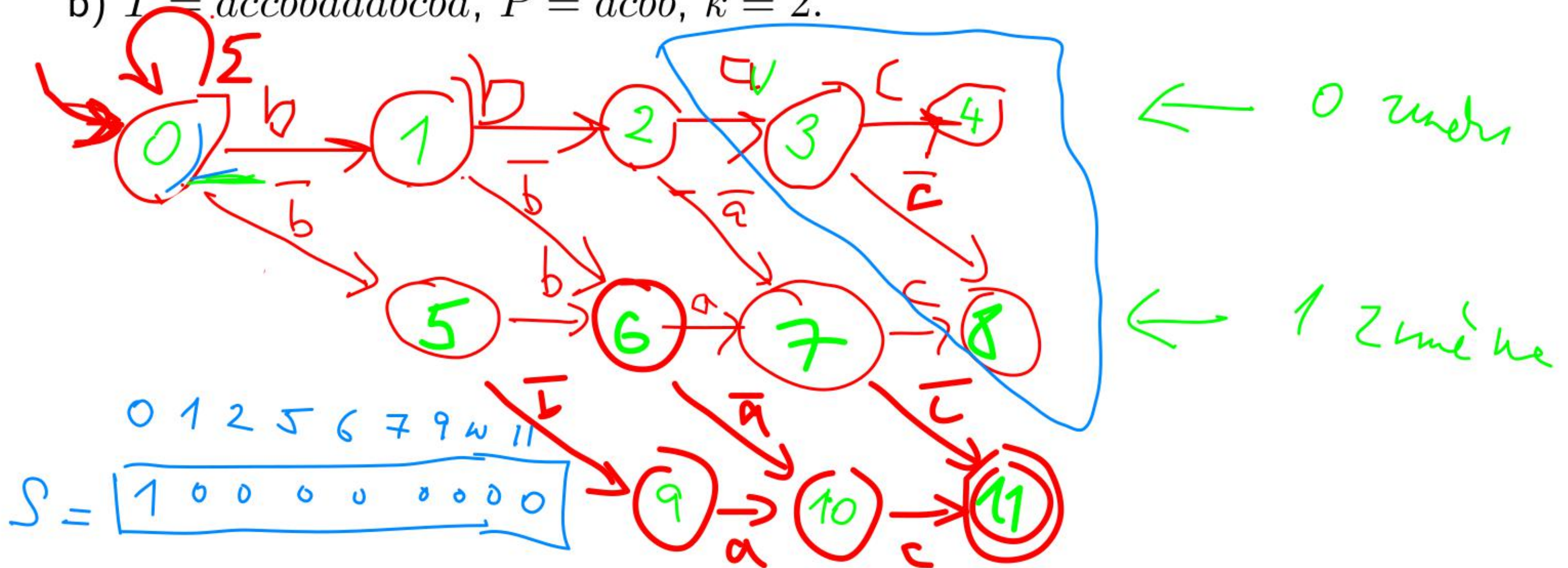


# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,

b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
b	1	1	0	0	1	0	0	0	0

pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1\ 0\ 0\ 0\ 0\ 0}$$

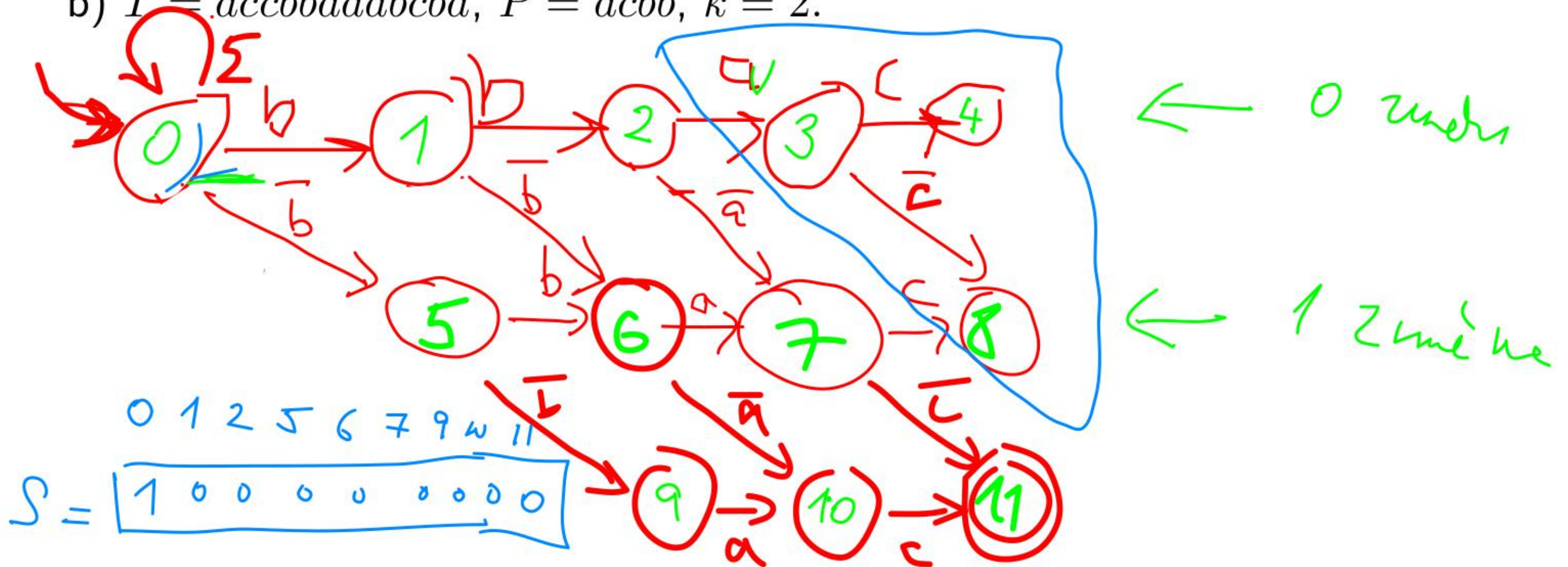
for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
c	1	1	0	0	1	0	0	0	0
S	1								

# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

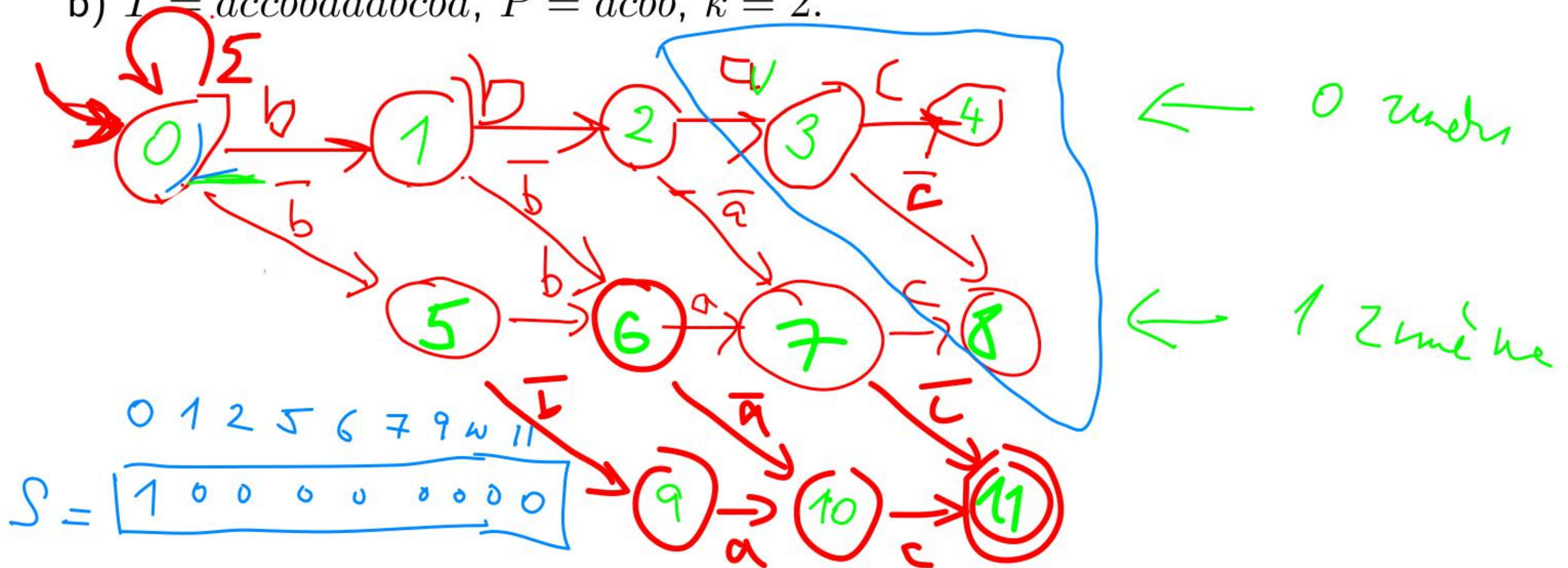
- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
 b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



# Př. 9/5a: bitový paralelizmus

Sestavte tabulky pro simulaci činnosti vyhledávacího automatu metodou bitového paralelizmu pro daný text  $T$ , vzorek  $P$  a Hammingovu vzdálenost  $k$ .

- a)  $T = \underline{abcbcaaccbbaa}$ ,  $P = \underline{bbac}$ ,  $k = 2$ ,  
 b)  $T = \underline{accbbaaabcba}$ ,  $P = \underline{acbb}$ ,  $k = 2$ .



pred. fce

start →

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$$S_0 = \boxed{1\ 0\ 0\ 0\ 0\ 0}$$

for  $i = 1..T$

	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
c	1	1	0	0	1	0	0	0	0
S	1								

pred. fce

start  $\nearrow$

	a	b	c	
0	1	1	1	0
	0	1	0	1
	0	0	0	2
	1	0	1	5
	0	0	0	6
				7
				9
				10
				11

$n = |Z|$

$n^2 = |Z|^2$

$$S_0 = \boxed{1 \ 0 \ 0 \ 0 \ 0 \ 0}$$

for  $i = 1..T$

$n$	0	1	2	5	6	7	9	10	11
a	1	0	0	0	0	0	0	0	0
b	1	0	0	1	0	0	0	0	0
c	1	1	0	0	1	0	0	0	0
	1								

$\textcircled{1}$

## Př. 9/3a: nedeterministické hledání slova z množiny

---

Sestrojte nedeterministický automat, který v textu nad abecedou  $A$  vyhledá právě každé slovo množiny  $M$ .

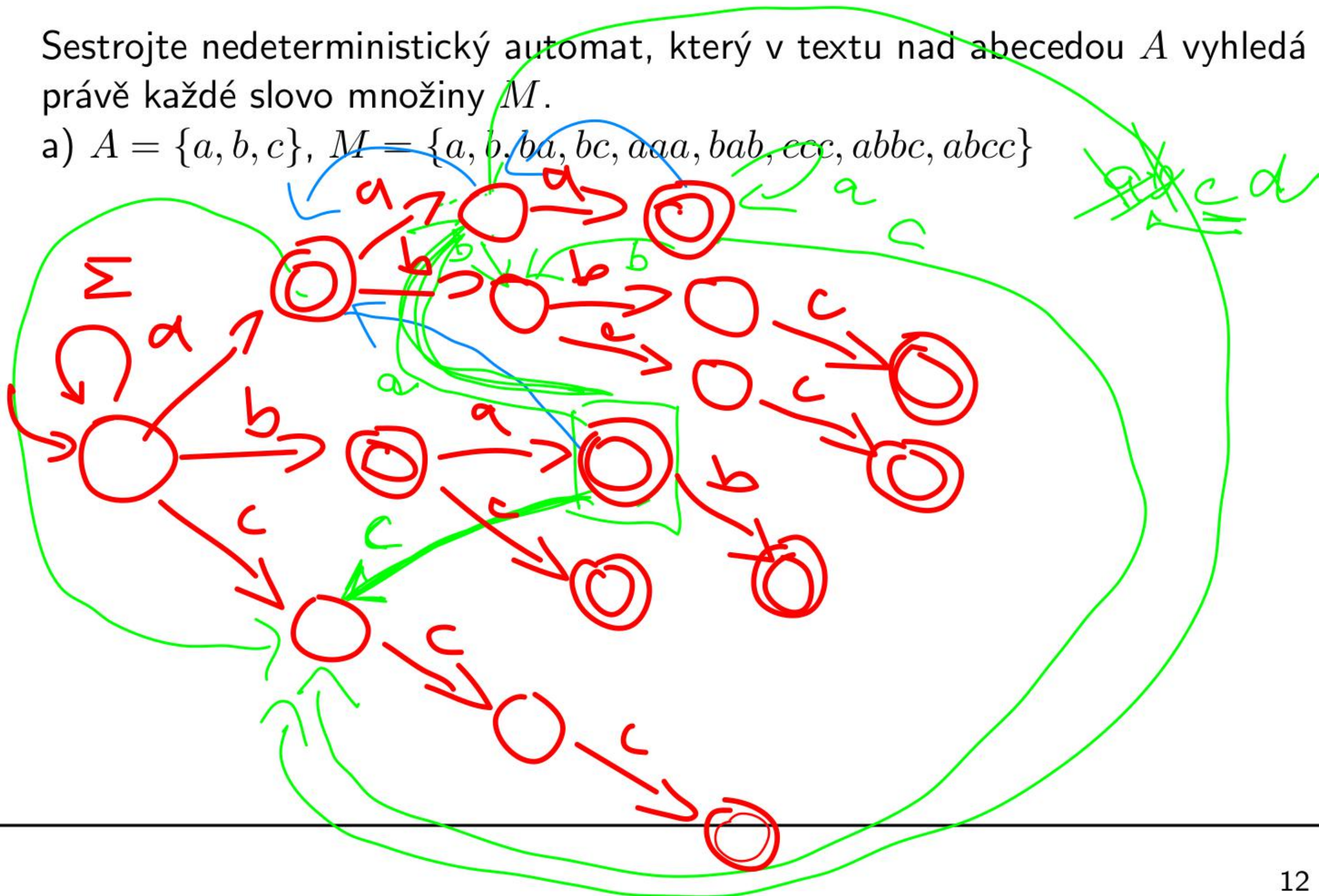
a)  $A = \{a, b, c\}$ ,  $M = \{a, b, ba, bc, aaa, bab, ccc, abbc, abcc\}$



# Př. 9/3a: nedeterministické hledání slova z množiny

Sestrojte nedeterministický automat, který v textu nad abecedou  $A$  vyhledá právě každé slovo množiny  $M$ .

a)  $A = \{a, b, c\}$ ,  $M = \{a, b, ba, bc, aaa, bab, ecc, abbc, abcc\}$



## Př. 9/4a: deterministické hledání slova z množiny

---

Sestrojte deterministický automat, který v textu nad abecedou  $A$  vyhledá právě každé slovo množiny  $M$ .

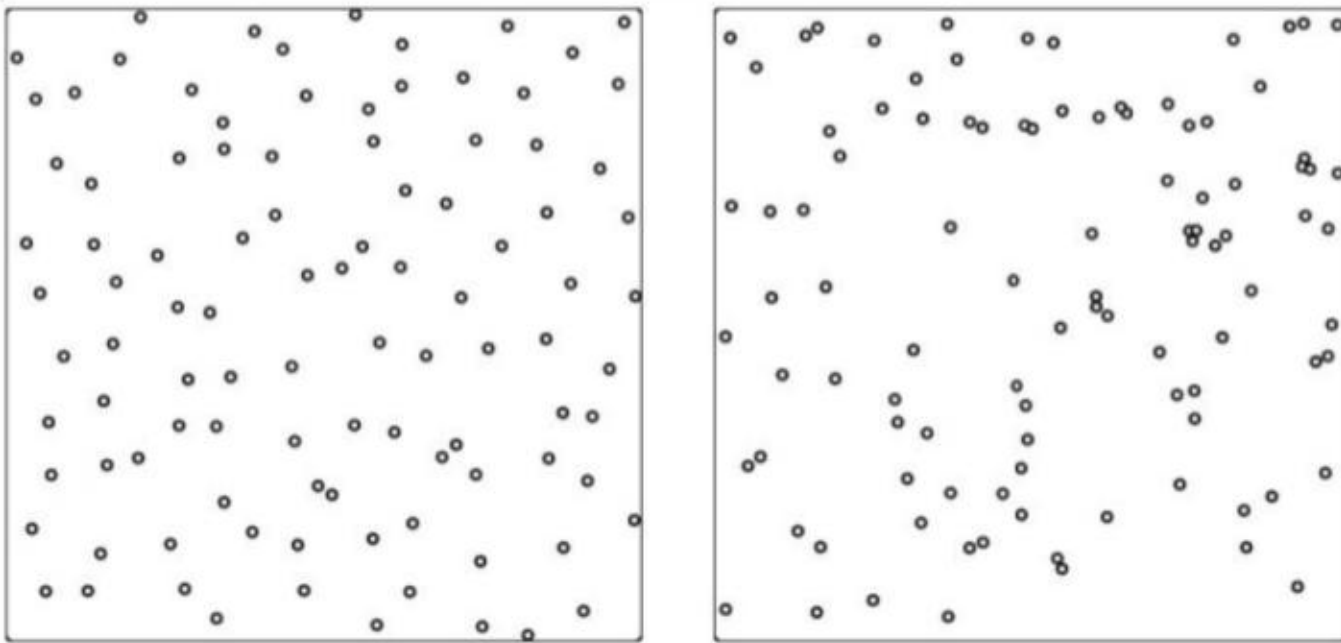
a)  $A = \{a, b, c\}$ ,  $M = \{a, b, ba, bc, aaa, bab, ccc, abbc, abcc\}$

---

Náhodná čísla. Prvočísla.  
Modulární umocňování.

## Př. 10/1: náhodné body

Máme dva obrázky - pokaždé jde o čtverec se 100 body uvnitř. V jednom případě byly souřadnice každého bodu generovány nezávisle a pseudonáhodně, ve druhém případě byly generovány analogicky, ale navíc byly souřadnice systematicky modifikovány (nám neznámým) způsobem. Odhadněte, kterého obrázku se týkají dodatečné úpravy a zdůvodněte svůj odhad.



## Př. 10/2: náhodná čísla

---

Máte jednu hrací kostku. Popište, jak využijte házení kostkou tak, abyste měli generátor náhodných celých čísel v rozmezí  $0 \dots 10$ . Všechna čísla  $0, 1, 2, \dots, 10$  musí být generována se stejnou pravděpodobností.



## Př. 10/3: náhodné uspořádání

---

Vysvětlete, jak pomocí generátoru náhodných čísel zamícháte do náhodného pořadí seřazené pole čísel. Akce musí proběhnout v čase úměrném délce pole.





## Př. 10/4: lin. kongruenční generátor náh. čísel

---

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a)  $x_{n+1} = (91x_n + 49) \pmod{600}$ ,

b)  $x_{n+1} = (8x_n + 80) \pmod{49}$ ,

c)  $x_{n+1} = (37x_n + 55) \pmod{144}$ ,

d)  $x_{n+1} = (99x_n + 81) \pmod{113}$ .

## Př. 10/4: lin. kongruenční generátor náh. čísel

---

Ověřte, zda lineární kongruenční generátor s danými parametry má maximální možnou délku periody.

a)  $x_{n+1} = (91x_n + 49) \bmod 600$ .

b)  $x_{n+1} = (8x_n + 80) \bmod 49$ ,

c)  $x_{n+1} = (37x_n + 55) \bmod 144$ ,

d)  $x_{n+1} = (99x_n + 81) \bmod 113$ .



## Př. 10/5: perioda Lehmerova generátoru náh. čísel

---

Určete délku periody v Lehmerově generátoru, který je dán předpisem  $x_{n+1} = ((M - 1) \cdot x_n) \bmod M$ , kde  $M$  je prvočíslo.

## Př. 10/6: počet prvočísel

---

Určete, kolik přibližně prvočísel leží v intervalu:

a)  $\langle 0, 10^9 \rangle$ ,

b)  $\langle 10^9, 2 \cdot 10^9 \rangle$ ,

c)  $\langle 2 \cdot 10^9, 3 \cdot 10^9 \rangle$ .

## Př. 10/7: poloprvočísla

---

Řekneme, že přirozené číslo je poloprvočíslu, pokud je buď prvočíslem nebo celou mocninou prvočísla. Popište modifikaci Eratosthenova síta, která bude generovat právě poloprvočísla. Napište pseudokód.

## Př. 10/8: skoroprvočísla

---

Jako skoroprvočísla označíme právě ta přirozená čísla, která jsou součinem dvou různých prvočísel. Popište modifikaci Eratosthena sítá, která bude generovat skoroprvočísla. Napište pseudokód.

## Př. 10/10: prvočísla v intervalu

---

Určete, jaký je maximální možný počet prvočísel v kterémkoli z intervalů  $\langle 30k, 30k + 29 \rangle$ ,  $k = 1, 2, 3, 4, \dots$