10. Gyakorlás vizsgára

Kódolástechnika

1. feladat

Egy bináris hibajavító kód kódszavai

$$000010, \qquad 110011, \qquad 101001, \qquad 111100.$$

(a) Határozzuk meg a kód paramétereit.

(b) Mik a kód hibadetektálási és hibajavítási képességei?

1. feladat

Egy bináris hibajavító kód kódszavai

$$000010, \qquad 110011, \qquad 101001, \qquad 111100.$$

(a) Határozzuk meg a kód paramétereit.

(b) Mik a kód hibadetektálási és hibajavítási képességei?

Megoldás.

(a) A kódszavak hossza 6 bit, így $n = 6$. A kódszavak száma $2^k = 4$, így $k = 2$. Ez egy C(6,2) kód.

1. feladat

Egy bináris hibajavító kód kódszavai

$$000010, \qquad 110011, \qquad 101001, \qquad 111100.$$

(a) Határozzuk meg a kód paramétereit.

(b) Mik a kód hibadetektálási és hibajavítási képességei?

Megoldás.

(a) A kódszavak hossza 6 bit, így $n = 6$. A kódszavak száma $2^k = 4$, így $k = 2$. Ez egy C(6,2) kód.

(b) Páronkénti összehasonlítás alapján a kódszavak közötti minimális Hamming-távolság $d_{\min} = 3$:

000010	000010	000010	110001	110011	101001
110011	101001	111100	101011	111100	111100

Így a kód $d_{\min} - 1 = 2$ hibát tud detektálni és $\lfloor \frac{d_{\min}-1}{2} \rfloor = 1$ hibát tud javítani.

2. feladat

Egy bináris lineáris hibajavító kód paritás-ellenőrző mátrixa

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

(a) Szisztematikus-e a kód?

(b) Adjuk meg a G generátormátrixot.

(c) Ez egy Hamming-kód-e?

(d) Mik a kód kódszavai?

(e) Hány hibát tud a kód javítani?

(f) Adjuk meg az $e = (10100)$ hibavektorhoz tartozó szindrómavektort és hibacsoportot. Melyik a csoportvezető elem?

2. feladat

Megoldás.

(a) A kód szisztematikus, mivel H jobboldali 3×3-as blokkja az identitásmátrix:

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right].$$

2. feladat

Megoldás.

(a) A kód szisztematikus, mivel H jobboldali 3×3-as blokkja az identitásmátrix:

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right].$$

(b) Szisztematikus kódra

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

ahol G baloldali 2×2-es blokkja az identitásmátrix, G jobboldali 2×3-as blokkja pedig H baloldali 3×2-es blokkjának a transzponáltja.

2. feladat

(c) A Hamming-kódokra $n + 1 = 2^{n-k}$ kell teljesüljön, de G méretei alapján $n = 5$ és $k = 2$, amikre ez nem teljesül: $n + 1 = 6 \neq 8 = 2^{n-k}$. Tehát ez nem egy Hamming-kód.

2. feladat

(c) A Hamming-kódokra $n+1 = 2^{n-k}$ kell teljesüljön, de G méretei alapján $n = 5$ és $k = 2$, amikre ez nem teljesül: $n+1 = 6 \neq 8 = 2^{n-k}$. Tehát ez nem egy Hamming-kód.

(d) Lineáris kódoknál a kódszavak G sorainak a lineáris kombinációi, jelen esetben

$$(00000), \qquad (10101), \qquad (01111), \qquad (11010).$$

2. feladat

(c) A Hamming-kódokra $n+1 = 2^{n-k}$ kell teljesüljön, de G méretei alapján $n = 5$ és $k = 2$, amikre ez nem teljesül: $n+1 = 6 \neq 8 = 2^{n-k}$. Tehát ez nem egy Hamming-kód.

(d) Lineáris kódoknál a kódszavak G sorainak a lineáris kombinációi, jelen esetben

$$(00000), \qquad (10101), \qquad (01111), \qquad (11010).$$

(e) Mivel ez egy lineáris kód, így

$$d_{\min} = \min_{c \text{ kódszó}} w(c) = 3,$$

és a kód $\lfloor \frac{3-1}{2} \rfloor = 1$ hibát tud javítani.

2. feladat

(f) Az $e = (10100)$ hibavektorhoz tartozó szindrómavektor

$$s^T = He^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

2. feladat

(f) Az $e = (10100)$ hibavektorhoz tartozó szindrómavektor

$$s^T = He^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

A hibacsoportot megkaphatjuk úgy, hogy e-hez hozzáadjuk a kódszavakat:

$$\{(10100), (00001), (11011), (01100)\}.$$

A csoportvezető elem a legkisebb súlyú vektor, ami a (00001).

3. feladat

Egy csatorna kapacitása kódolás nélkül 1.5 Mbps, és a bithiba valószínűsége $P_b = 0.001$. C(15,11) Hamming-kód használatával mennyi lesz a módosított bithiba valószínűség és a csatorna effektív kapacitása?

3. feladat

Egy csatorna kapacitása kódolás nélkül 1.5 Mbps, és a bithiba valószínűsége $P_b = 0.001$. C(15,11) Hamming-kód használatával mennyi lesz a módosított bithiba valószínűség és a csatorna effektív kapacitása?

Megoldás. C(15,11) kód esetén a kódráta 11/15, így a csatorna effektív kapacitása

$$\frac{11}{15} \cdot 1.5 \text{ Mbps} = 1.1 \text{ Mbps}.$$

3. feladat

C(15,11) Hamming-kód használatával egy 11 bit hosszú üzenet helyett 15 bit hosszú kódolt üzenetet küldünk át, viszont a kód 1 hiba javítására képes, így a blokk hiba valószínűsége

$$1 - (1 - P_b)^{15} - 15(1 - P_b)^{14} P_b \approx 0.0001041.$$

3. feladat

C(15,11) Hamming-kód használatával egy 11 bit hosszú üzenet helyett 15 bit hosszú kódolt üzenetet küldünk át, viszont a kód 1 hiba javítására képes, így a blokk hiba valószínűsége

$$1 - (1 - P_b)^{15} - 15(1 - P_b)^{14} P_b \approx 0.0001041.$$

A módosított bithiba valószínűséget az

$$1 - (1 - P'_b)^{11} = 0.0001041$$

egyenlet megoldásával kapjuk (ennyi lenne a blokk hiba valószínűség egy olyan csatornán, ahol nem használunk hibajavító kódot.) Az eredmény

$$P'_b \approx 9.46 \cdot 10^{-6}.$$

4. feladat

Adjuk meg egy olyan GF(7) feletti kód G generátormátrixát, amely képes 2 hiba javítására.

4. feladat

Adjuk meg egy olyan GF(7) feletti kód G generátormátrixát, amely képes 2 hiba javítására.

Reed–Solomon kódot fogunk használni. Először a kód paramétereit határozzuk meg. GF(7) felett $n = 7 - 1 = 6$. Egy C(n,k) RS kód $\lfloor \frac{n-k}{2} \rfloor$ hiba javítására képes;

$$\left\lfloor \frac{6-k}{2} \right\rfloor \qquad \rightarrow \qquad k = 2.$$

4. feladat

Adjuk meg egy olyan GF(7) feletti kód G generátormátrixát, amely képes 2 hiba javítására.

Reed–Solomon kódot fogunk használni. Először a kód paramétereit határozzuk meg. GF(7) felett $n = 7 - 1 = 6$. Egy C(n,k) RS kód $\lfloor \frac{n-k}{2} \rfloor$ hiba javítására képes;

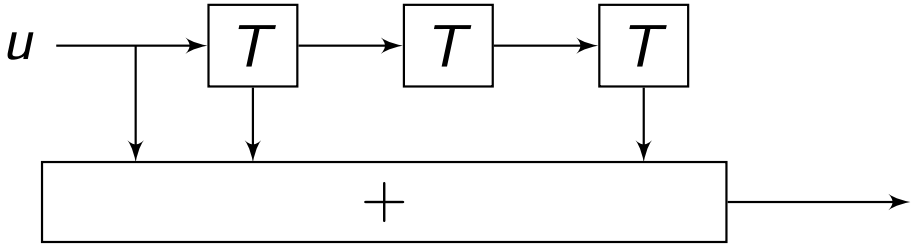
$$\left\lfloor \frac{6-k}{2} \right\rfloor \qquad \rightarrow \qquad k = 2.$$

Tehát egy C(6,2) kódot fogunk megadni. GF(7) felett két primitív elem van, a 3 és az 5. Bármelyiket választhatjuk, mondjuk a 3 használatával

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix}.$$

5. feladat

Tekintsük GF(8)-at a $p(y) = y^3 + y + 1$ irreducibilis polinommal. A következő eltolás regiszter architektúra egy GF(8) feletti lineáris kódot valósít meg:



(a) Mi a kód generátorpolinomja?

(b) Mik a kód paraméterei?

(c) Mi a kód hibajavítási képessége?

5. feladat

Megoldás.

(a) A shift regiszter architektúra egy polinommal való szorzást valósít meg. Nincs benne konstans szorzó, tehát a polinomnak minden együtthatója 0 vagy 1, aszerint, hogy bekerül-e a kimenő összeadásba. Összességében ez a $g(x) = x^3 + x + 1$ polinommal való szorzás. A kód generátorpolinomja az $x^3 + x + 1$.

5. feladat

Megoldás.

(a) A shift regiszter architektúra egy polinommal való szorzást valósít meg. Nincs benne konstans szorzó, tehát a polinomnak minden együtthatója 0 vagy 1, aszerint, hogy bekerül-e a kimenő összeadásba. Összességében ez a $g(x) = x^3 + x + 1$ polinommal való szorzás. A kód generátorpolinomja az $x^3 + x + 1$.

(b) A GF(8) feletti, 0-1 együtthatós generátorpolinomok a BCH kódokra jellemzőek. Ellenőrizzük, hogy ez a kód egy BCH kód generátorpolinomja-e.

5. feladat

Megoldás.

(a) A shift regiszter architektúra egy polinommal való szorzást valósít meg. Nincs benne konstans szorzó, tehát a polinomnak minden együtthatója 0 vagy 1, aszerint, hogy bekerül-e a kimenő összeadásba. Összességében ez a $g(x) = x^3 + x + 1$ polinommal való szorzás. A kód generátorpolinomja az $x^3 + x + 1$.

(b) A GF(8) feletti, 0-1 együtthatós generátorpolinomok a BCH kódokra jellemzőek. Ellenőrizzük, hogy ez a kód egy BCH kód generátorpolinomja-e.

Ehhez a GF(8) feletti konjugált csoportokat és minimálpolinomokat kell megnézni:

$$\{1\} \to x - 1$$
$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

5. feladat

Megoldás.

(b) Azt kell ellenőrizni, hogy a generátorpolinom előáll-e, mint a GF(8) feletti minimálpolinomok közül néhány szorzata. A $g(x)$ éppen az $\{y, y^2, y^4\}$ konjugált csoporthoz tartozó minimálpolinom, tehát igen.

5. feladat

Megoldás.

(b) Azt kell ellenőrizni, hogy a generátorpolinom előáll-e, mint a GF(8) feletti minimálpolinomok közül néhány szorzata. A $g(x)$ éppen az $\{y, y^2, y^4\}$ konjugált csoporthoz tartozó minimálpolinom, tehát igen.

Tehát ez egy BCH kód; a paramétereire teljesül, hogy $n = 8 - 1 = 7$ és a generátorpolinom foka $n - k = 3$, így $k = 4$, ez egy C(7,4) kód.

5. feladat

Megoldás.

(b) Azt kell ellenőrizni, hogy a generátorpolinom előáll-e, mint a GF(8) feletti minimálpolinomok közül néhány szorzata. A $g(x)$ éppen az $\{y, y^2, y^4\}$ konjugált csoporthoz tartozó minimálpolinom, tehát igen.

Tehát ez egy BCH kód; a paramétereire teljesül, hogy $n = 8 - 1 = 7$ és a generátorpolinom foka $n - k = 3$, így $k = 4$, ez egy C(7,4) kód.

(c) $g(x)$ gyökei tartalmazzák az y^1 és y^2 elemeket GF(8)-ból (a teljes konjugált csoportjukkal együtt), de y^3-t már nem, tehát ez a kód $t = 1$ hibát tud javítani.

6. feladat

Adott egy forrás a következő eloszlással és kódolással:

Forrás szimbólum	Valószínűség	Kódszó
A	0.29	0
B	0.21	10
C	0.20	110
D	0.19	1110
E	0.11	1111

(a) Prefix-mentes-e ez a kód?

(b) Számítsuk ki az átlagos kódhosszt.

(c) Mennyi az elméleti alsó korlát a tömöríthetőségre?

(d) Optimális-e ez a kód?

6. feladat

Megoldás.

(a) Igen, prefix-mentes a kód.

6. feladat

Megoldás.

(a) Igen, prefix-mentes a kód.

(b) Az átlagos kódhossz

$$0.29 \cdot 1 + 0.21 \cdot 2 + 0.20 \cdot 3 + 0.19 \cdot 4 + 0.11 \cdot 4 = 2.51.$$

6. feladat

Megoldás.

(a) Igen, prefix-mentes a kód.

(b) Az átlagos kódhossz

$$0.29 \cdot 1 + 0.21 \cdot 2 + 0.20 \cdot 3 + 0.19 \cdot 4 + 0.11 \cdot 4 = 2.51.$$

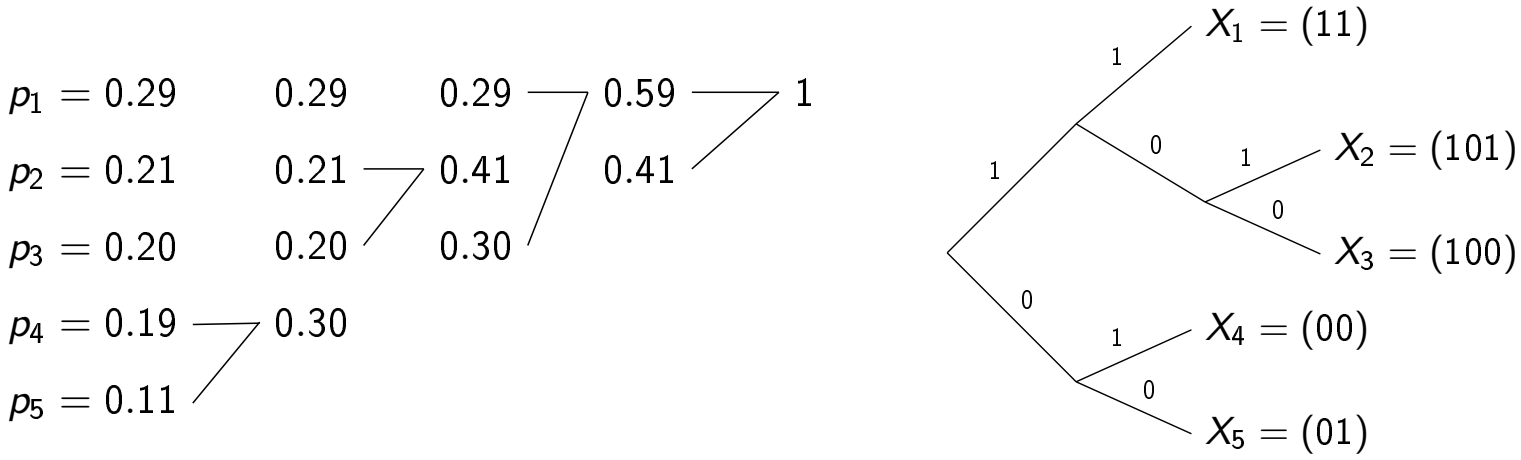
(c) Az elméleti alsó korlát a tömöríthetőségre az entrópia:

$$\sum_{i=1}^{5} -p_i \log_2(p_i) = 2.2606.$$

(d) Az optimalitást úgy tudjuk ellenőrizni, hogy összehasonlítjuk a Huffman kóddal.

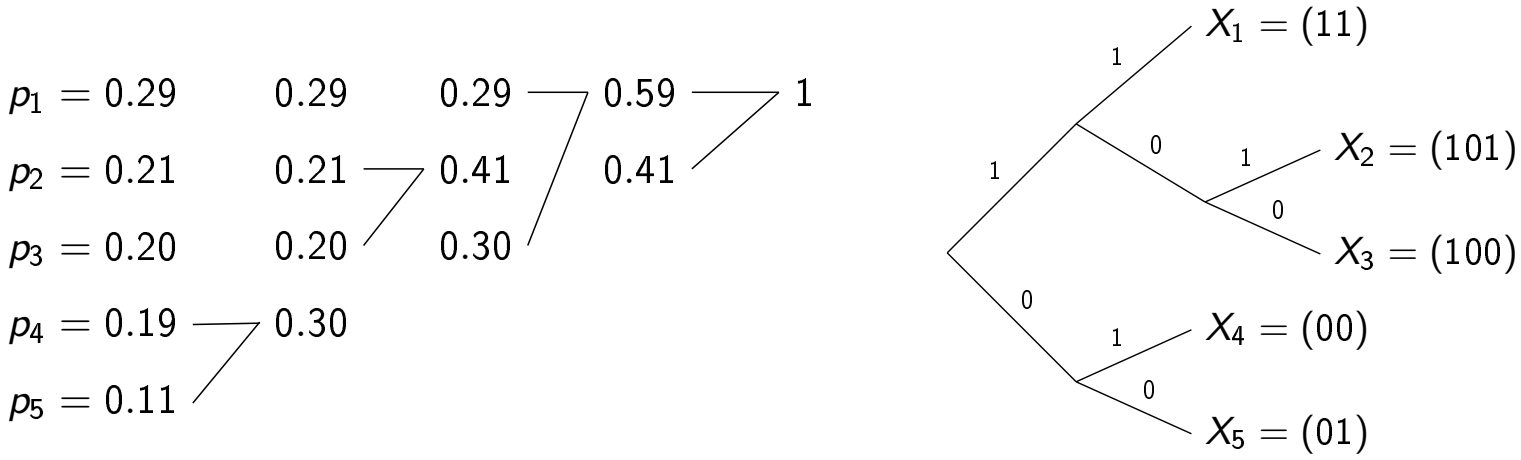
6. feladat

(d)


$p_1 = 0.29$
$p_2 = 0.21$
$p_3 = 0.20$
$p_4 = 0.19$
$p_5 = 0.11$
0.29
0.21
0.20
0.30
0.29
0.41
0.30
0.59
0.41
1
1
0
1
0
1
0
$X_1 = (11)$
$X_2 = (101)$
$X_3 = (100)$
$X_4 = (00)$
$X_5 = (01)$

6. feladat

(d)



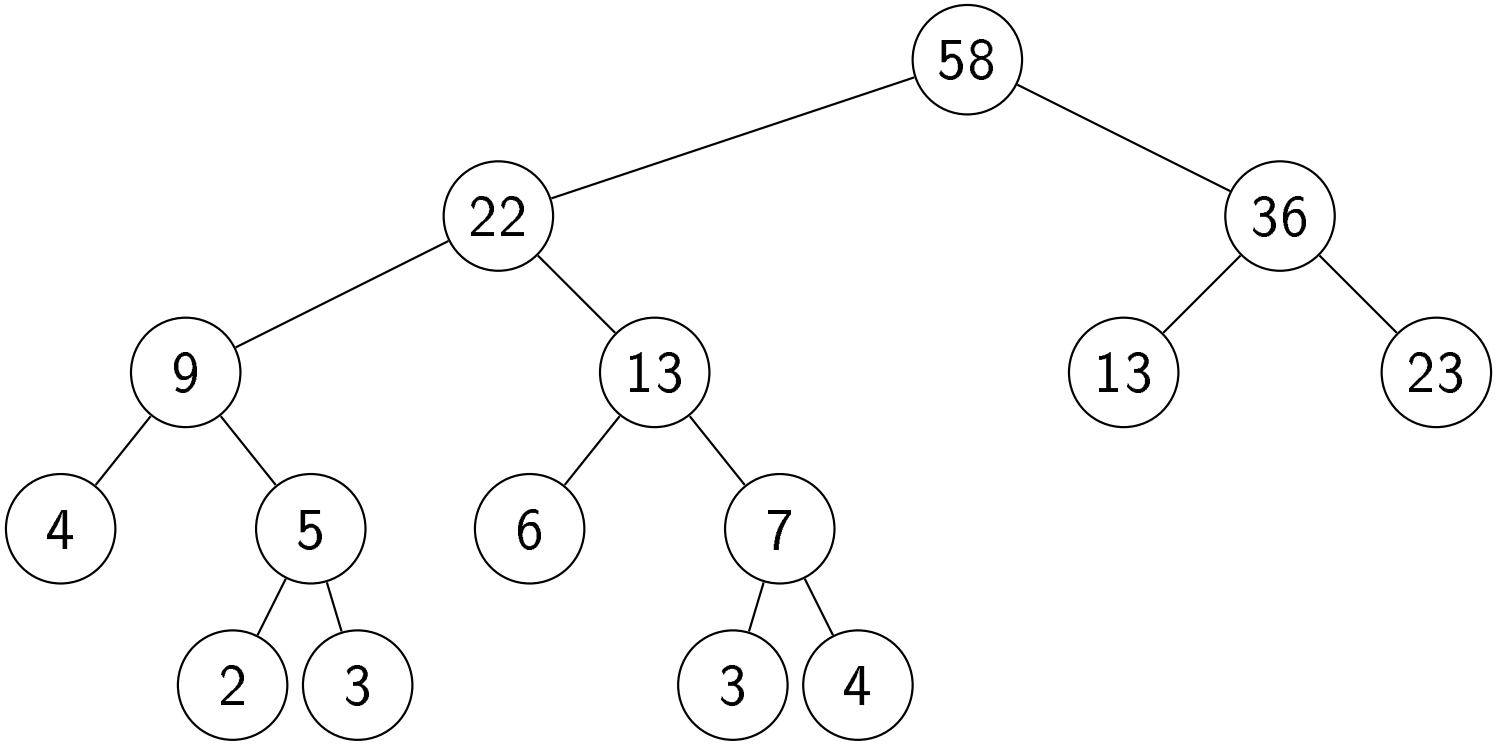
Az átlagos kódhossz

$$0.29 \cdot 2 + 0.21 \cdot 2 + 0.20 \cdot 2 + 0.19 \cdot 3 + 0.11 \cdot 3 = 2.30,$$

ami kisebb, mint az eredeti kódra, tehát az eredeti kód nem optimális.

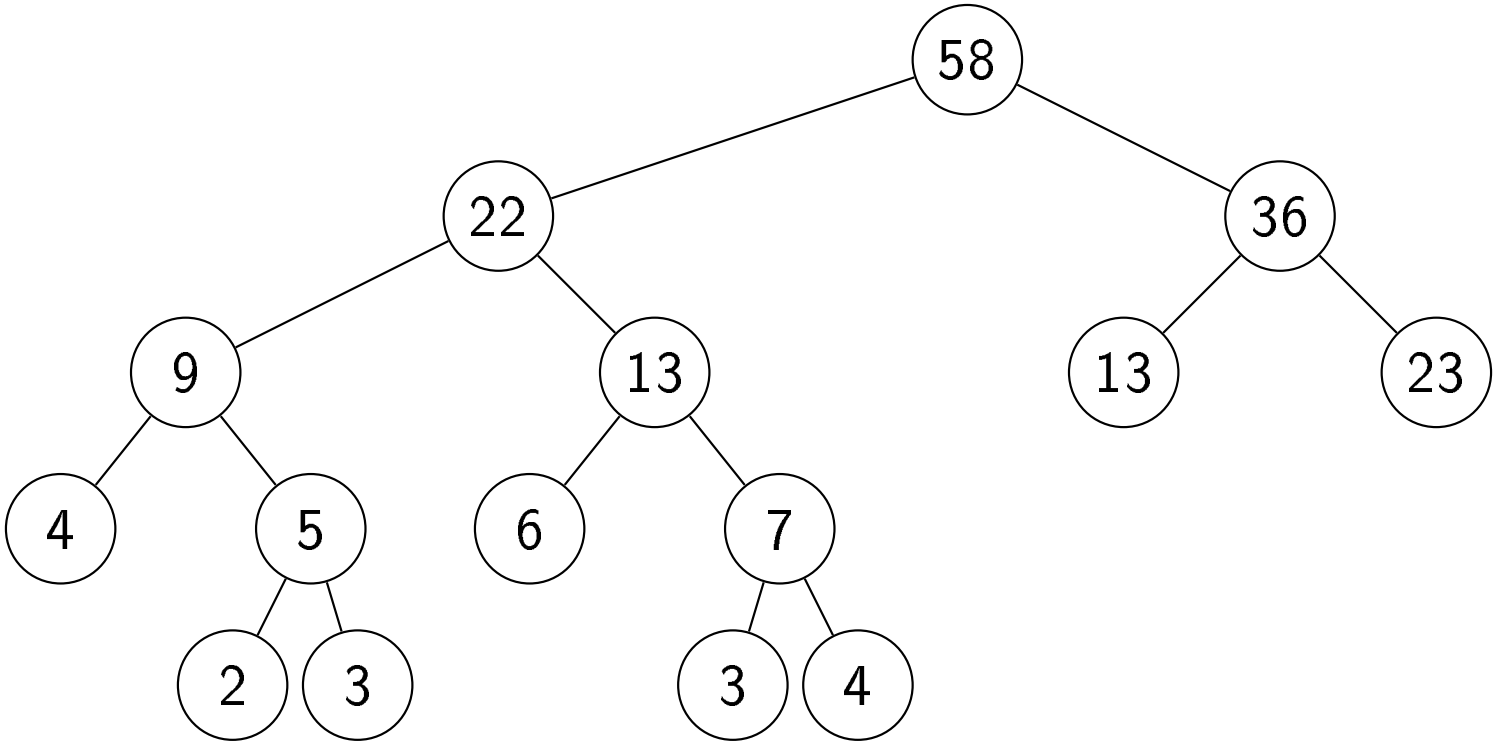
7. feladat

Teljesül-e a következő fára a testvérpár tulajdonság?



7. feladat

Teljesül-e a következő fára a testvérpár tulajdonság?



Megoldás. A kiolvasási sorrend: 2, 3, 3, 4, 4, 5, 6, 7, 9, 13, 13, 23, 22, 36, 58. A 23 után 22 következik, tehát a sorozat nem monoton növő, a testvérpár tulajdonság nem teljesül.

8. feladat

LZ77 algoritmussal tömörítjük az

a p r ó b a b a b a b e z á r j a a b a z á r t

szöveget; a paraméterek értéke $h_s = 6, h_l = 6$. A kurzor kezdetben a 6. és 7. karakter között áll. Adjuk meg az algoritmus kimenetét a kezdeti állapotra és a következő lépésre.

8. feladat

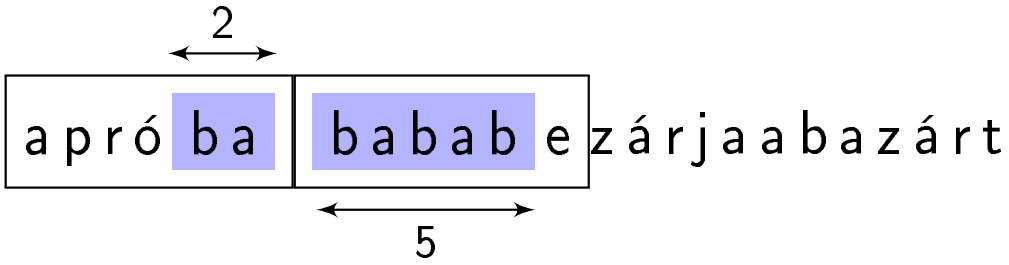
LZ77 algoritmussal tömörítjük az

a p r ó b a b a b a b e z á r j a a b a z á r t

szöveget; a paraméterek értéke $h_s = 6, h_l = 6$. A kurzor kezdetben a 6. és 7. karakter között áll. Adjuk meg az algoritmus kimenetét a kezdeti állapotra és a következő lépésre.

Megoldás.

- Kezdeti állapot:



kimenet: $(2, 5, e)$

8. feladat

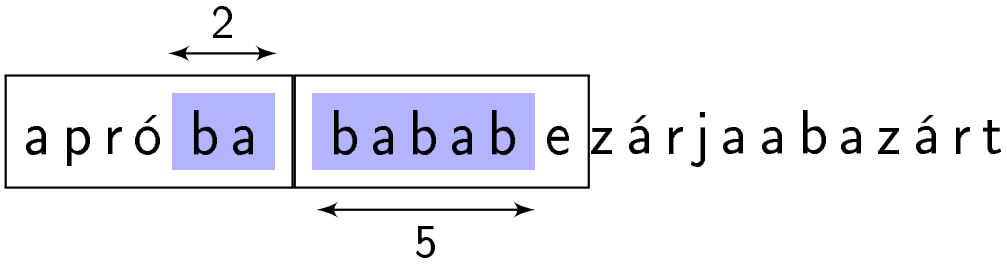
LZ77 algoritmussal tömörítjük az

a próbababababezárjaabazárt

szöveget; a paraméterek értéke $h_s = 6, h_l = 6$. A kurzor kezdetben a 6. és 7. karakter között áll. Adjuk meg az algoritmus kimenetét a kezdeti állapotra és a következő lépésre.

Megoldás.

- Kezdeti állapot:



kimenet: $(2, 5, e)$

- következő lépés:

a próba bababe zárjaa bazárt kimenet: $(0, 0, z)$

9. feladat

RSA titkosítást alkalmazunk $p = 5, q = 7$ választással.

(a) Mi lesz az (n, e) nyilvános kulcs, ha e-t a lehető legkisebbre választjuk?

(b) Mi az előbbi e-hez tartozó d privát kulcs?

(c) Mi az $x = 3$ nyílt szöveghez tartozó titkosított szöveg?

9. feladat

Megoldás.

(a) $n = pq = 35, \quad \phi(n) = (p-1)(q-1) = 24.$

e-re teljesülnie kell, hogy

$$\gcd(\phi(n), e) = 1 \qquad \text{és} \qquad 1 < e < \phi(n) = 24.$$

A legkisebb lehetséges választás $e = 5$. A nyilvános kulcs (35,5).

9. feladat

Megoldás.

(a) $n = pq = 35, \quad \phi(n) = (p-1)(q-1) = 24.$

e-re teljesülnie kell, hogy

$$\gcd(\phi(n), e) = 1 \qquad \text{és} \qquad 1 < e < \phi(n) = 24.$$

A legkisebb lehetséges választás $e = 5$. A nyilvános kulcs (35,5).

(b) Az $e = 5$-höz tartozó d privát kulcs a $de = 1 \bmod \phi(n)$, vagyis

$$5d = 1 \mod 24$$

egyenlet megoldása, ami

9. feladat

Megoldás.

(a) $n = pq = 35, \quad \phi(n) = (p-1)(q-1) = 24.$

e-re teljesülnie kell, hogy

$$\gcd(\phi(n), e) = 1 \qquad \text{és} \qquad 1 < e < \phi(n) = 24.$$

A legkisebb lehetséges választás $e = 5$. A nyilvános kulcs (35,5).

(b) Az $e = 5$-höz tartozó d privát kulcs a $de = 1 \bmod \phi(n)$, vagyis

$$5d = 1 \mod 24$$

egyenlet megoldása, ami $d = 5$.

9. feladat

Megoldás.

(a) $n = pq = 35, \quad \phi(n) = (p-1)(q-1) = 24.$

e-re teljesülnie kell, hogy

$$\gcd(\phi(n), e) = 1 \qquad \text{és} \qquad 1 < e < \phi(n) = 24.$$

A legkisebb lehetséges választás $e = 5$. A nyilvános kulcs (35,5).

(b) Az $e = 5$-höz tartozó d privát kulcs a $de = 1 \bmod \phi(n)$, vagyis

$$5d = 1 \mod 24$$

egyenlet megoldása, ami $d = 5$.

(c) Az $x = 3$ nyílt szöveghez tartozó titkosított szöveg

$$c = x^e = 3^5 = 243 \mod 35 = 33.$$