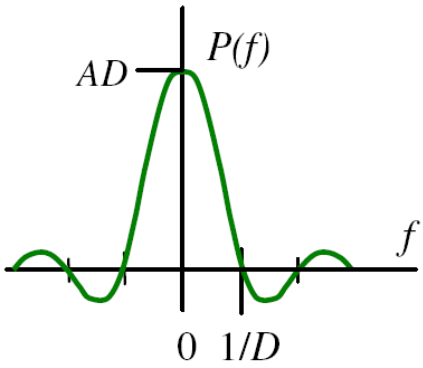
Ülesanne 35: Transpordikihi protokoll kasutab vookontrolliks ja vigade tuvastamiseks libiseva aknaga protokolli (*sliding window*). Akna pikkuseks W on 1800 B, viimase edastatud segmendi number SN on 3700, ning viimase kinnituse number AN on 2900. Maksimaalselt mitu baiti tohib saatja enne järgmise kinnituse saamist veel edastada?

Kokku tohib maksimaalselt saata 1800 B. Kuna viimane kinnitatud bait on numbriga 2900 seega hetkeseisuga tohiks saata baidid AN kuni AN + W ehk 2900 kuni 4700. Hetkel on viimasena saadetud SN = 3700 bait, seega enne järgmise kinnituse saatmist võib veel saata 4700-3700 ehk tuhat baiti.

Vastus: Enne järgmise kinnituse saamist võib edastada veel kuni 1000 baiti.

Ülesanne 36: Edastuskanalis mõõdeti bitijada spektrit. Mõõtmiste käigus selgus, et esimene nullkoht paiknes sagedusel 115,2kHz ja spektraaltiheduse maksimaalne väärtus oli $2{,}86 \cdot 10^{-5}$ V/Hz. Kui suur on bitikiirus r antud kanalis ja kui suur on edastatavate impulsside amplituud A ?



Joonis 36. Bitijada spekter [A. Meister]

Esimese nullkoha asukoht $f_0 = 1/D$ on võrdne edastuskiirusega r kanalis, seega edastuskiirus r = 115,2 kbitt/s. Spektraaltiheduse maksimaalne väärtus on kohal $f = 0$ olles seal võrdne $P(0) = AD = A/r$. Viimasest saame avaldada impulsside amplituudi, mis võrdub $A = r \cdot P(0) = 115200 \cdot 2{,}86 \cdot 10^{-5} = 3{,}295$ V.

Vastus: Bitikiirus kanalis on 115200 bitt/s ja impulsside amplituud on 3,3 V.

Ülesanne 37: Diskreetne signaal $[m]$ omab järgmisi väärtuseid $f[0] = 1$, $f[1] = 1$ ja $f[2] = -1$, kõik ülejäänud $f[m]$ väärtused on võrdsed nulliga. Arvuta signaali autokorrelatsioonifunktsioon. Esita tulemus graafiku või tabelina.

Kuna tegemist on reaalfunktsiooni autokorrelatsiooniga saame selle arvutada järgneva avaldise alusel.

$$R[n] = \sum_{m=-\infty}^{\infty} f[m]\, f[n+m]$$

Kuna funktsioon omab mittenulliseid väärtuseid ainult väärtustel m = 0, 1 ja 2, siis on tulemus ise mittenulline n väärtustel vahemikus -2 kuni 2 . Korrelatsiooni arvutamine on alljärgnevas tabelis sammhaaval välja toodud:

n = -3	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	0	0	0	0	0	1	1	-1	
	$f[m]\cdot f[m-3]$	0	0	0	0	0	0	0	0	0	0

n = -2	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	0	0	0	0	1	1	-1	0	
	$f[m]\cdot f[m-3]$	0	0	0	0	0	-1	0	0	0	-1

n = -1	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	0	0	0	1	1	-1	0	0	
	$f[m]\cdot f[m-3]$	0	0	0	0	1	-1	0	0	0	0

n = 0	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	0	0	1	1	-1	0	0	0	
	$f[m]\cdot f[m-3]$	0	0	0	1	1	1	0	0	0	3

n = 1	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	0	1	1	-1	0	0	0	0	
	$f[m]\cdot f[m-3]$	0	0	0	1	-1	0	0	0	0	0

n = 2	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	0	1	1	-1	0	0	0	-0	0	
	$f[m]\cdot f[m-3]$	0	0	0	-1	0	0	0	0	0	-1

n = 3	m	-3	-2	-1	0	1	2	3	4	5	$R[n]$
	$f[m]$	0	0	0	1	1	-1	0	0	0	
	$f[m-3]$	1	1	-1	0	0	0	0	0	0	
	$f[m]\cdot f[m-3]$	0	0	0	0	0	0	0	0	0	0

Nagu tehtud arvutustest ka näha on, on autokorrelatsioon sümmeetriline funktsioon $R[-n] = R[n]$, seega tegelikult piisaks ainult ühe poole arvutamisest, teine on sellega sümmeetriline. Ehk antud ülesande korral oleks vaja leida ainult $R[n]$ kohtadel -2, -1 ja 0 või 0, 1 ja 2. Tulemus on antud järgnevas tabelis:

n	-2	-1	0	1	2
$R[n]$	-1	0	3	0	-1

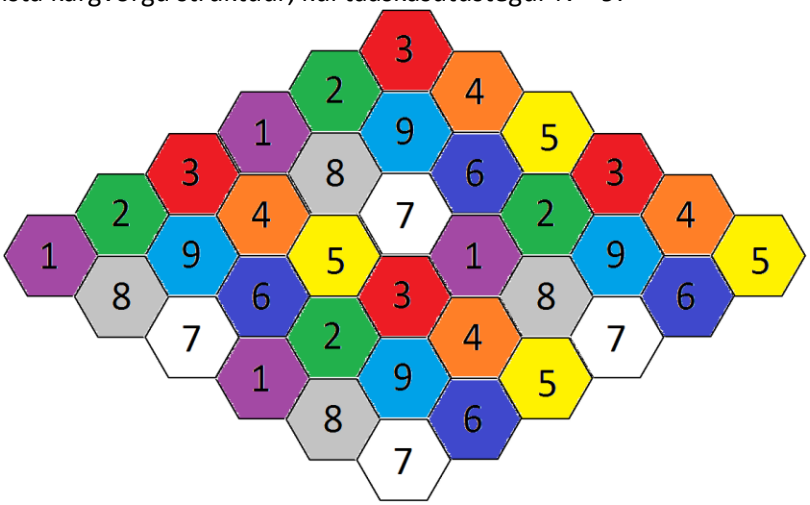
Ülesanne 38: IEEE 802.11a standardi korral on MCS = 7 korral andmeedastuskiirus 18 Mbit/s (vt tabel slaidil 35). Näita arvutuslikult, kuidas selline kiirus saavutatakse (Sümboli kestus, kanalite arv jne..).

IEEE 802.11a standardis kasutatakse andmete ülekandeks 48 andmesidekanalit. Sümboli kestus on 3,2 µs ja sümbolite vahel on lisaks 0,8 µs pikkune paus. Kui MCS (*Modulation and Coding Scheme*) väärtus on seitse, siis näeme tabelist, et igas kanalis kasutatakse QPSK (*Quadrature Phase Shift Keying*) modulatsiooni ja konvolutsioonilise koodi kiirus on ¾. QPSK modulatsiooni korral edastatakse igas kanalis ühte $M = 4$ erinevast sümbolist, seega igas kanalis edastatakse $\log_2(M) = \log_2(4) = 2$ bitti. Koodi kiirus k/n = ¾ tähendab, et iga $k = 3$ andmebiti kohta lisataks $n\text{-}k = 1$ paarsusbitt.

Kõike ülal toodut arvesse võttes leiame esmalt sümbolikiiruse. Üks sümbol koos vahepausiga kestab 3,2 + 0,8 = 4 µs, seega sümbolikiirus $r = 1/4 \cdot 10^{-6} = 2{,}5 \cdot 10^5$ baudi. Iga sümboli sees on 48 sageduskanalit milles igas edastatakse korraga kahte bitti, seega ühes sümbolis on 48·2 = 96 bitti.

Nüüd saame leida bitikiiruse $r_b = 2{,}5 \cdot 10^5 \cdot 96 = 2{,}4 \cdot 10^7$ bitt/s. Järgnevalt leiame kui suur osa sellest kiirusest on kasutusel kasutaja andmete edastamiseks. Kuna koodi kiirus on ¾ siis iga neljas bitt on paarsusbitt ja seega andmebittide osakaal on ¾, korrutame bitikiiruse selle konstandiga läbi ja saame tulemuseks $1{,}8 \cdot 10^7$ bitt/s ehk <u>18 Mbitt/s.</u>

Ülesanne 39: Joonista kärgvõrgu struktuur, kui taaskasutustegur N = 9.



Joonis 39. Kärgvõrgu struktuur, kui N = 9

Ülesanne 40: GSM1800 sagedusalas kasutatakse kanaleid järjekorranumbritega (*ARFCN*) 512-885. Üleslingi kanali sagedus on määratud avaldisega f_{UL} = 1710,2+0,2·(*ARFCN*-512). Üleslingi sagedus on allalingi omast 95MHz kõrgem. Milliseid sagedusvahemike kasutatakse kogu üleslingi ulatuses ja milliseid kogu allalingi ulatuses? Mis sagedustel töötab kanal numbriga 790?
Kui kanali number muutub vahemikus 512 kuni 885, siis üleslingi jaoks kasutatav sagedusvahemik on 1710,2+0,2·(512-512) kuni 1710,2+0,2·(885 -512) ehk 1710,1 kuni 1784,8 MHz. Kui üleslingi sagedus on allalingi omast 95 MHz kõrgem, siis järelikult kasutatakse selleks sagedusvahemiku 1710,1 + 95 kuni 1784,8 + 95 ehk 1805,2 kuni 1879,8 MHz.

Kanal numbriga 790 töötab sagedustel f_{UL} = 1710,2+0,2·(790-512) = 1765,8 MHz ja f_{DL} = 1860,8 MHz.

Ülesanne 41: Kui kaugel tugijaamast asub GSM mobiilterminal, kui TA väärtus on 12? Kui suur on kauguse suhteline täpsus selles asukohas? Kui kaua levib signaal mobiilterminalist tugijaamani ja tagasi?

TA number vastab 550m pikkusele lõigule, seega TA = 12 vastab kaugusele 6600m, ehk 6,6km. Kuna TA samm on 550m, siis täpsuseks võib lihtsamas käsitluses lugeda pool sellest vahemaast, ehk ±275 m.

Vahemaa mobiiltelefonini on 6,6 km, seega edasi tagasi on teepikkus kaks korda nii suur, ehk l = 13,2 km = $1{,}32\cdot10^4$ m. Raadiosignaal levib õhus praktiliselt valguse kiirusega c = $3\cdot10^8$ m/s. Seega edasi-tagasi leviaeg on $t = l/c = 4{,}4\cdot10^{-4}$s = 0,44 ms.

Ülesanne 42: 3G võrgus on ASU = 22, kui suur on vastuvõetava signaali võimsus W ?

Vastuvõetud signaali võimsus on P[dBm] = -113 + 2·ASU, seega P = -113 + 2·22 = -69dBm. Kuna vastust soovitakse lineaarsetes ühikutes, siis teisendame dBm'id esmalt millivattideks. P = $10^{-69/10}$ = $10^{-6,9}$ = $1{,}26\cdot10^{-7}$ mW, kuna üks mW = 10-3W siis võimsus vattides on $1{,}26\cdot10^{-10}$ W.

Vastus: Vastuvõetava signaali võimsus on $1{,}26\cdot10^{-10}$ W (126 pW).

Ülesanne 43: Mobiilsidevõrk koosneb 64 kärjest, igaüks raadiusega 1,2 km. Võrgu kasutuses on kokku 396 sidekanalit ja taaskasutustegur N = 9. Kui suur on selle võrgu maksimaalne geograafiline katteala (km^2), kui palju kanaleid saab ühes kärjes kasutada ja kui suur on kanalite koguhulk võrgus?

Kui me eeldame, et kärjed on ringikujulised, siis on ühe leviala pindala $A = \pi r^2 = 3{,}14\cdot1{,}2^2 = 4{,}52$ km^2. Kuna kärgi on kokku 64, siis on kogu võrgu leviala pindala vastavalt 64 korda suurem võrdudes 289,4 km^2. Realistlikuma tulemuse saame, kui eeldame, et kärje kuju on kuusnurkne. Kuusnurga pindala on

$$A = \frac{3\sqrt{3}}{2} r^2 \approx 2{,}59 r^2,$$

ehk ühe kärje pindala on 3,73 km^2 ja kogu võrgu oma 238,7 km^2.

Kuna meil on kokku kasutada 396 kanalit ja taaskasutustegur on 9, siis saab keskmiselt ühes kärjes kasutada 396/9 = 44 kanalit. Kogu võrgu peale teeb see siis kokku 44·64 = 2816 sidekanalit.

Ülesanne 44: Sagedustihendust kasutavas mobiilvõrgus on operaatorile eraldatud 25 MHz laiune sagedusala. Kui suur on ühe kanali ribalaius, kui antud sagedusalas on 400 kanalit ja kanalite vahel on 8 kHz laiused puhveralad.

Kui meil on n kanalit, siis nende vahele jääb n - 1 puhverala. Meie juhul siis 400 kanali vahele 399 puhvertsooni, igaüks laiusega 8 kHz, seega võtavad puhvertsooni kokku 399·8 = 3192 kHz. Seega jääb 400 kanali jaoks ruumi kokku 25000-3192 = 21808 kHz, mis teeb ühe kanali ribalaiuseks B = 21808/400 = 54,5 kHz.

Vastus: Ühe kanali ribalaius on 54,52 kHz.

Ülesanne 45: Ühekordse šifriga (OTP) krüpteeritud tekst (16-bitine) on kuueteistkümnendarvuna kujul 0xA257. Leia algne lahtine tekst (plaintext), kui võti on 0x1CBD.

Teisendame esmalt krüpteeritud teksti *Y* ja võtme *K* kahendarvudeks:

Y = 0xA257 = 1010 0010 0101 0111
K = 0x1CBD = 0001 1100 1011 1101

Lahtine tekst on leitav *X* = *Y* + *K* mod(2)

1010 0010 0101 0111
0001 1100 1011 1101
1011 1110 1110 1010

Vastus: Algne lahtine tekst on *X* = 1011 1110 1110 1010 = 0xBEEA

Ülesanne 46: Kui palju aega kuluks 40 bitise võtme toore jõuga lahti murdmiseks kui selleks kasutatava arvuti jõudlus on $2{,}5 \cdot 10^9$ võtit sekundis?

40 bitiseid võtmeid on 2^{40} erinevat, kõigi nende läbi proovimiseks kuluks meie ülesande tingimuste kohaselt $t = 2^{40} / 2{,}5 \cdot 10^9 = 1{,}1 \cdot 10^{12} / 2{,}5 \cdot 10^9 = 439{,}8$ sekundit. Keskmiselt kulub ühe võtme murdmiseks pool ajast, mis on vajalik kõikide kombinatsioonide proovimiseks, seega keskmine võtme lahti murdmise aeg oleks 220 sekundit ehk kolm minutit ja 40 sekundit.

Vastus: Antud võtme toore jõuga lahti murdmiseks kuluks keskmiselt 3 min ja 40 s.