Lec\_7

**Виявлення й виправлення помилок у повідомленнях.**

**Блочні лінійні коди**

Особливість кодів, які виявляють помилки, полягає в тому, що кодові комбінації, які входять до складу цих кодів, різняться кодовою відстанню, не меншою ніж dmin=2.

Такі коди умовно можна поділити на дві групи: коди, в яких використовуються всі комбінації, але до кожної з них за обумовленим правилом додаються г перевірних елементів; коди, утворені зменшенням кількості дозволених комбінацій.

До першої групи кодів, що виявляють помилки, належать коди з перевіркою на парність і непарність; код із простим повторенням; інверсний та кореляційний коди; до другої— код зі сталою вагою. Код з кількістю одиниць у комбінації, кратною трьом, може належати до першої або другої групи кодів залежно від методики його побудови.

**ДВІЙКОВІ КОДИ,** **ЩО ВИЯВЛЯЮТЬ ПОМИЛКИ**

**1. КОД ІЗ ПЕРЕВІРКОЮ НА ПАРНІСТЬ**

Це найпоширеніший код, який застосовується для виявлення поодиноких помилок і всіх помилок непарної кратності. Код містить (n-1) інформаційних й один перевірний елементи, належить до систематичних кодів і позначається як (n, n-1)-код.

Перевірний елемент коду визначається сумою за модулем 2 всіх інформаційних елементів:



тобто він утворюється доповненням комбінації k-елементного первинного коду одним елементом таким чином, щоб кількість одиниць у новому n-розрядному (n = k +1) коді була парною. Кодова відстань dmin=2.

Для виявлення помилки на приймальному боці перевіряють на парність усю прийняту кодову комбінацію, визначаючи кодовий синдром



де a', b' — прийняті на приймальному боці відповідно інформаційні та перевірний елементи.

Вважається, що при s1= 0 помилки в комбінації немає, а при s1 = 1 помилка є. Надмірність коду визначається виразом

Rнад=1-k/(k+1)=1/(k+1)

**2. КОД ІЗ ПЕРЕВІРКОЮ НА НЕПАРНІСТЬ**

Цей код відрізняється від попереднього тим, що кожна його комбінація має непарну кількість одиниць, тобто додатковий перевірний елемент формують, виходячи з кількості одиниць у початковій кодовій комбінації: при парній кількості перевірний елемент дорівнює одиниці, а при непарній — нулю.

Для виявлення помилки в кодовій комбінації на приймальному боці її перевіряють на непарність. Код є подільним завдовжки n - 1 інформаційних й один перевірний елементи; він може так само виявляти помилки та має надмірність, як і код із перевіркою на парність.

**3. КОД ІЗ ПРОСТИМ ПОВТОРЕННЯМ**

Код із простим повторенням (без інверсії) є подільним лінійним кодом. Він містить k інформаційних і r = k перевірних елементів. У цьому коді r перевірних елементів є простим повторенням k інформаційних елементів первинної кодової комбінації: bi = ai де і = 1.. .k.

Через те, що код має відстань dmin = 2, він може використовуватися для виявлення поодиноких помилок. Ця процедура зводиться до порівняння однойменних інформаційних і перевірних елементів у прийнятій кодовій комбінації. Незбіг їх свідчить про наявність помилок у ній. Код дає змогу виявити не тільки однократні помилки, а й деякі помилки більшої кратності, за винятком «дзеркальних», коли в інформаційній та перевірній послідовностях кодової комбінації внаслідок дії завад спотворюються елементи, що знаходяться на однакових за номером розрядах.

Надмірність коду визначається виразом Rнад=1-k/(2k)=1/2

**4. ІНВЕРСНИЙ КОД**

Інверсний код (із повторенням та інверсією) є подільним лінійним кодом, який має k інформаційних і стільки ж перевірних елементів. Його відмінність від попереднього коду полягає в тому, що значення перевірних елементів у ньому залежать від значення суми за модулем 2 всіх інформаційних елементів. За умови , тобто при парній кількості одиниць у початковій кодовій комбінації, перевірні елементи просто повторюють інформаційні (bi = ai де і = 1.. .k), а за умови , тобто при непарній кількості зазначених одиниць, перевірні елементи повторюють інформаційні в інвертованому вигляді (в оберненому коді): (bi = ai+1 де і = 1.. .k)

Для виявлення помилок на приймальному боці в послідовності, що складається з 2k елементів, спочатку підсумовують одиниці, які знаходяться в перших k елементах. Якщо їх кількість парна, то решту k елементів приймають у незмінному вигляді. Обидві зареєстровані частини комбінації поелементно порівнюють (перший елемент із першим, другий — з другим і т.д.). За наявності хоча б одного незбігу вся послідовність елементів бракується.

Якщо кількість одиниць серед перших k елементів непарна, то решту k елементів приймають у інверсному вигляді, після чого поелементно порівнюють їх. Наявність незбігу призводить до відбраковування всіх 2к елементів. Така побудова коду дає змогу виявляти майже всі випадки спотворення його елементів, крім двократних «дзеркальних» помилок.

Надмірність коду визначається виразом

Rнад=1-k/(2k)=1/2

**5. КОРЕЛЯЦІЙНИЙ КОД**

У цьому коді кожний розряд двійкового початкового коду записується у вигляді двох елементів: 0 — як 01, а 1 — як 10. Так, початковій кодовій комбінації 010011 відповідатиме комбінація 011001011010 кореляційного коду. В технічній літературі такий двійковий запис дуже часто називається Манчестер-кодом.

Приймальний пристрій в кожному такті, що складається з двох сусідніх елементів кореляційного коду, мас зафіксувати перехід 0 —> 1 або 1 —> 0. У разі прийняття двох нулів або одиниць приймальний пристрій фіксує наявність помилки.

Кореляційний код дає змогу виявляти помилки будь-якої кратності, але не здатний виявити двократні «дзеркальні» помилки, коли сусідні елементи одного такту під впливом завад змінюються на протилежні за значенням.

Надмірність коду визначається виразом

Rнад=1-k/(2k)=1/2

До переваг кореляційного коду, крім відсутності постійної складової в напрузі кодового сигналу при передачі кодової комбінації по каналу зв’язку, можна віднести також можливість самосинхронізації генератора приймача, оскільки прийняття кожного біта супроводжується фронтом сигналу, що приймається, в центрі біта.

**6. КОД ЗІ СТАЛОЮ ВАГОЮ**

Код зі сталою вагою, тобто з незмінною кількістю одиниць і нулів у комбінаціях, часто називається кодом на одне сполучення. Загальна кількість комбінацій цього коду визначається виразом



де m — кількість одиниць у кодовій комбінації завдовжки n.

Такий код утворюється з двійкового простого коду відбором комбінацій, що мають однакову кількість одиниць m. Приймальний пристрій, підраховуючи кількість одиниць у прийнятій кодовій комбінації, виявляє помилки, якщо кількість перших відрізнятиметься від n.

Код зі сталою вагою має мінімальну кодову відстань dmin = 2. Він виявляє всі помилки непарної кратності, а також усі помилки парної кратності, що призводять до порушення умови m = const.

Надмірність коду визначається виразом



Порівняно з кодом із простим повторенням цей код при меншій його надмірності дає змогу виявляти помилки тієї самої кратності.

**7. КОД ІЗ КІЛЬКІСТЮ ОДИНИЦЬ У КОМБІНАЦІЇ, КРАТНОЮ ТРЬОМ**

Цей код можна утворити або додаванням до кожної комбінації початкового коду r = 2 перевірних елементів, або зменшенням кількості дозволених комбінацій початкового коду з накладанням додаткової умови: кількість одиниць у кожній комбінації має бути кратною трьом.

У першому випадку до початкової кодової комбінації додаються два перевірних розряди, які мають такі значення, що сума одиниць у кодовій комбінації стає кратною трьом. Так, якщо початкова кодова комбінація має дві або п’ять одиниць, то для здобуття ваги w = 3 або 6 кодової комбінації треба доповнити її двома перевірними елементами 10. Якщо ж у початковій комбінації є одна або чотири одиниці, то вона доповнюється двома перевірними елементами 11. Так, комбінація 01010 початкового коду, закодована кодом із кількістю одиниць, кратною трьом, матиме вигляд 0101010, а 10000 -> 1000011, 0110 -> 011010, 101100 -> 10110000, 110110 —> 11011011, 0111011 —> 011101110 тощо.

У другому випадку з усіх комбінацій початкового коду вибирають тільки ті, які мають вагу w = 3 та 6. Решту комбінацій використовувати не можна.

Код дає змогу виявити всі поодинокі помилки та деякі помилки більшої кратності, що призводять до порушення умови w = 3 або 6, де w — кількість одиниць у кодовій комбінації. Здатність коду виявляти помилкові комбінації майже така сама, як і коду зі сталою вагою.

Надмірність коду з доповненням до необхідної кількості одиниць визначається виразом



а коду, що утворюється відбором із загальної кількості комбінацій з відповідною кількістю одиниць (3 або 6), — виразом



**Загальні поняття і визначення корегуючих кодів**

*Коди без надмірності виявляти, а тим більше виправляти помилки не можуть.* Мінімальна кількість символів, у яких будь-які дві комбінації коду відрізняються один від одного називаються *кодовою відстанню*. Мінімальна кількість символів, у яких усі комбінації коду відрізняються один від одного, називаються *мінімальною кодовою відстанню*. Мінімальна кодова відстань – параметр, що визначає завадостійкість коду й закладену в коді надмірності. Мінімальною кодовою відстанню визначаються коригувальні властивості коду.

**Теорема 1**. Якщо d0 парне, то код може одночасно виправляти (d0 −2)/ 2 помилок і виявляти d0/2 помилок.

Задача, яка виникає при побудові лінійного n-значного коду, коректуючого незалежні помилки, полягає у визначенні необхідного мінімального числа перевірочних символів r для виправлення t-кратних помилок. Для розв’язання цієї задачі в літературі з кодування є різні граничні співвідношення. Перша оцінка надлишкових символів для двійкових кодів може бути отримана внаслідок використання **граничної умови Хеммінга**

 (2.4)

Значення цього виразу полягає в наступному. Якщо задані основні параметри лінійного коду n і tвп = (d0 −1)/ 2 , то можлива мінімальна кількість надлишкових символів r = n – k може бути визначена за допомогою умови (2.4). Для наочності на рис. 2.4 наведені графіки границь Хеммінга згідно з виразом

 d=3, 5, 7

**Теорема 2**. Якщо при заданих параметрах n , k і d0 використовується нерівність



то існує ( n, k, d0 ) код, який реалізується за допомогою не більше r перевірок на парність.

Для виявлення й виправлення одиночної помилки співвідношення між числом інформаційних розрядів k і числом коригувальних розрядів r повинне задовольняти наступним умовам:

, (59)

, (60)

при цьому мається на увазі, що загальна довжина кодової комбінації

. (61)

Для практичних розрахунків при визначенні числа контрольних розрядів кодів з мінімальною кодовою відстанню *d*0 = 3 зручно користуватися виразом

, (62)

якщо відома довжина повної кодової комбінації *n*, і

, (63)

якщо при розрахунках зручніше виходити із заданого числа інформаційних символів k.

Для кодів, що виявляють трикратні помилки (*d*0=4),

 (64)

або

.(65)

Для кодів довжиною в *n* символів, що виправляють одну або дві помилки (*d*0=5),

. (66)

Для практичних розрахунків можна користуватися виразом

. (67)

Для кодів, що виправляють 3 помилки (*d*0=7),

. (68)

Для кодів, що виправляють *s помилок* (*d*0=2*s*+1),

. (69)

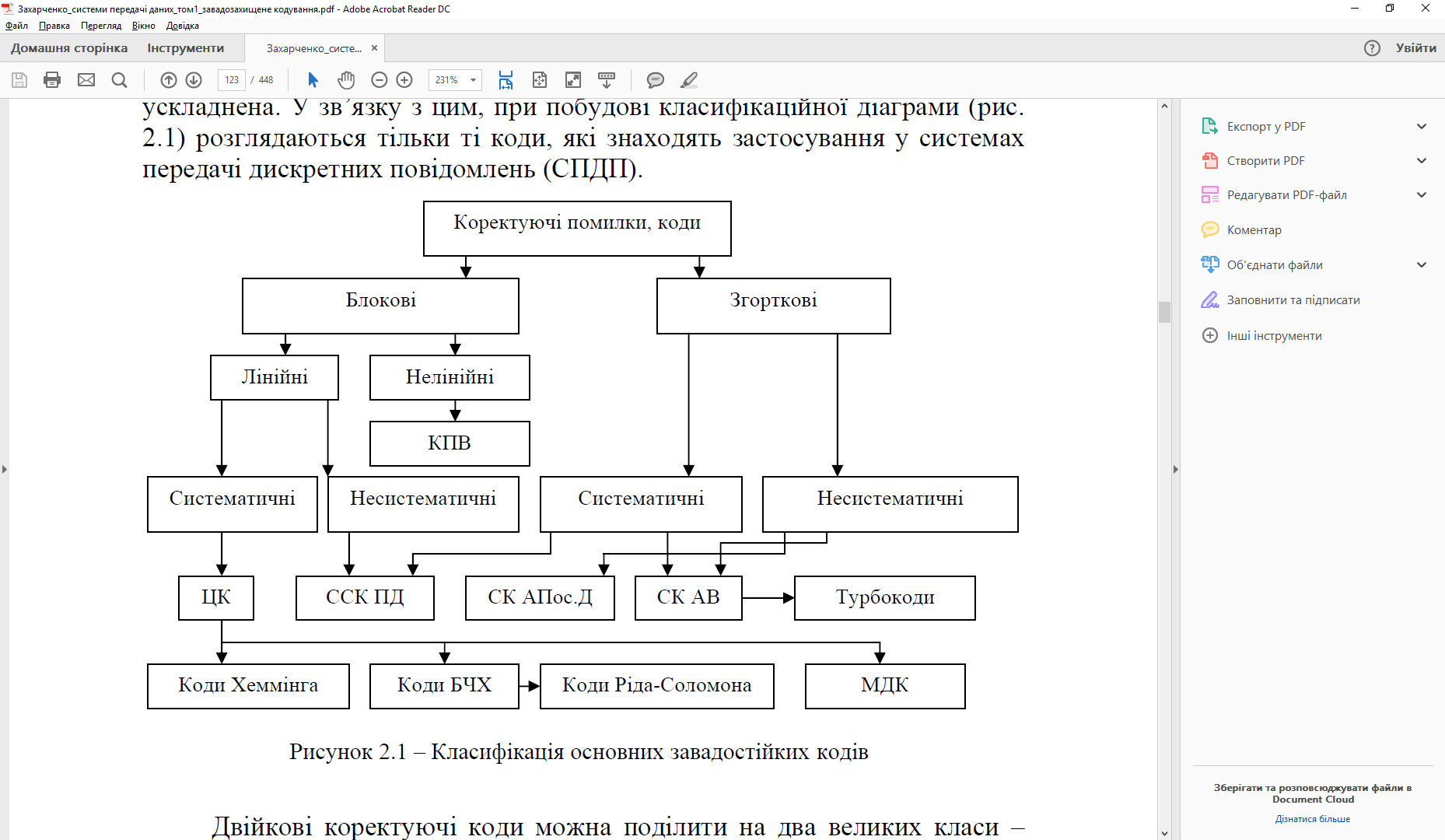
Вираз ліворуч відомий як нижня границя Хемінга [16], а виразя праворуч – як верхня границя Варшамова – Гільбета [3].

Для наближених розрахунків можна користуватися виразом

. (70)

Можна припустити, що значення *r* буде наближатися до верхньої або нижній границі залежно від того, на скільки виражені вираження під знаком логарифма наближається до цілого ступеня двох.

**ЛІНІЙНІ ГРУПОВІ КОДИ**



Блокові коди характеризуються довжиною блока або значністю кодового слова (КС) n і кількістю інформаційних символів k. Для них прийнято позначення (n, k). До лінійних (n, k) кодів належать такі, в яких r = n – k надлишкових символів формуються із k інформаційних за допомогою лінійних операцій, тобто операцій підсумовування і множення

Коди, для яких гранична умова Хеммінга виконується зі знаком рівності, називаються досконалими або щільноупакованими. Найпростішими прикладами таких кодів є всі коди Хеммінга з d0 =3, для яких n = 2r –1 і k = 2r − r −1, при r = 2, 3, 4, … . Всі досконалі коди володіють мінімальною надлишковістю ρ = r / n для досягнення потрібної коректуючої здатно

сті. Граничні умови Хеммінга для кодів (3, 1), (7, 4), (15, 11), (31, 26) ,...,що виконуються зі знаком рівності, можна показати простим виразом



Особливий інтерес становить код Голея (23, 12) – єдиний досконалий код, що виправляє помилки першої, другої і третьої кратностей (d0 = 7 ). Для цього коду, як і для кодів Хеммінга, гранична умова Хемінга виконується зі знаком рівності

*Лінійними* називаються коди, у яких перевірочні символи являють собою лінійні комбінації інформаційних символів.

Для двійкових кодів як лінійної операції використовують додавання по модулю 2.

Правила додавання по модулю 2 визначаються наступними рівностями:



Послідовність нулів і одиниць, що належать даному коду, будемо називати *кодовим вектором*.

В n-значних кодах з усіх можливих з’єднань кодових комбінацій



для передавання повідомлень використовується тільки Nk = 2k КК, які називаються дозволеними. Останні невикористовувані комбінації (Nr= Nn− Nk) називаються недозволеними.

Лінійні блокові коди мають властивості замкненості, які означають, що сума за mod 2 двох і більше дозволених кодових комбінацій утворюють іншу дозволену кодову комбінацію, що належить цьому ж коду. Із зазначеного можна зробити висновок, що будь-який лінійний код завжди має нульове кодове слово (000...000), утворене в результаті підсумовування декількох дозволених

*Властивості лінійних кодів*: сума (різниця) кодових векторів лінійного коду дає вектор, що належить даному коду.

Лінійні коди утворюють алгебраїчну групу стосовно операції додаванню по модулю 2. у цьому змісті вони є *груповими кодами*.

*Властивості групового коду*: мінімальна кодова відстань між кодовими векторами групового коду дорівнює мінімальній вазі ненульових кодових векторів.

*Вага кодового вектора* (кодової комбінації) дорівнює числу його ненульових компонентів

*Відстань між двома кодовими векторами* дорівнює вазі вектора, отриманого в результаті додавання вихідних векторів по модулю 2. Таким чином, для даного групового коду

Групові коди зручно задавати породжуючими матрицям, розмірність яких визначається параметрами коду k й r. Число рядків у матриці рівно k, число стовпців матриці рівно k+r=n:

**. (71)

Ліва частина породжуючої матриці являє собою квадратну одиничну підматрицю Ik,k , а права – підматрицю перевірочних елементів Pr, k

* 2.7*

Процес кодування, з математичної точки зору, означає множення матриці рядка послідовності інформаційних символів на породжуючу матрицю Gn, k . Результатом такого множення є матриця-рядок Dn , яка відповідає КС систематичного (n, k)-коду:



де перевірочні символи b1, b2 , ..., br визначаються системою двійкових

рівностей



а j = 1, 2, 3, …, r.

Задана система рівностей використовується як алгоритм для побудови функціональної схеми кодера систематичного (n, m) коду, коректуюча здатність якого повністю визначається видом перевірочної під матриці

**

Для того, щоб лінійний блоковий код мав кодову відстань не менше d0 > 2, необхідно і достатньо, щоб рядки підматриці надлишкових елементів Pr, k задовольняли таким умовам:

1) число перевірочних символів в КС повинно визначатися згідно з

умовою теореми 2;

2) вага кожного рядка повинна бути не менше d0 −1;

3) вага суми двох будь-яких рядків повинна бути не менше d0 − 2 ;

4) рядки повинні бути лінійно незалежні, тобто сума їх не повинна дорівнювати нулю.

Сформульовані умови дають відповідь на питання, яка повинна бути підматриця перевірочних елементів, що визначає код з заданими d0 . Але, на жаль, в ньому не вказується конкретний шлях її побудови. Недоліком кодів, отриманих цим методом, є те, що за відносно великих n важко побудувати підматрицю Pr, k і не завжди її можна віднести до оптимальної.

**Принципи декодування**.

Аналогічно тому, як при кодуванні часто використовується поняття породжуючої матриці Gn,k, в основу декодування може бути покладена перевірочна матриця Hn,r. Значення назви «перевірочна матриця» полягає в тому, що за допомогою цієї матриці виконується перевірка належності прийнятого КС до одного з дозволених.

Перевірочна матриця Hn,r легко отримується з породжуючої матриці Gn,k шляхом транспонування підматриці Pr,k і перестановки її місцями з одиничною матрицею



де PTk,r – транспонована підматриця перевірочних елементів Pr,k , тобто така, стовпцями якої є рядки вихідної підматриці, а Ir,r одинична квадратна підматриця розмірності r2.

У розгорнутому виді перевірочна матриця з використанням позначень згідно з (2.7) має вигляд:



Результат множення матриці-рядка прийнятого КС Dn′ = (Dn + En )mod 2, де En =||e1 e2 e3 ... en|| матриця-рядок вектора помилок, що містить одиниці тільки на тих позиціях, які спотворюють кодові символи в прийнятій КК на транспоновану матрицю HTn,r , називається ***синдромом***

Dn′*×*HTn,r=Sr

У розгорнутому вигляді вираз можна подати так:



Неважко переконатися в тому, що елементи матриці-рядка синдрома визначаються таким чином:



де j = 1, 2, …, r.

Якщо прийняте КС не було піддане дії завад, тобто En = 0, то Sr = 0. Важливою особливістю синдрома є те, що він не залежить від вигляду переданого КС, а визначається тільки конфігурацією помилок у прийнятому КС. Якщо код використовується для виправлення помилок, то при декодуванні установлюється відповідність між видом синдрома і номером спотвореного кодового символу. В двійкових кодах виправлення помилок зводиться до інвертування спотвореного кодового символу перед видачею прийнятого повідомлення споживачу. Якщо кількість помилок у прийнятому КС перевищує величину tпом > (d0 −1)/ 2, то в результаті декодування можуть вноситися хибні виправлення, тобто будуть спотворюватися правильно прийняті символи КС або не виправлятися символи з помилками. Від цього явища не застрахований ні один із відомих лінійних кодерів при синдромному декодуванні. Питання лише в тому, з якою ймовірністю це явище може відбуватися.

На закінчення необхідно визначити, що матриці Gn, k і Hn, r зв’язані таким співвідношенням:

Gn, k *×*HTn,r=0

Тут 0 означає нульову матрицю розмірністю k× r.