



П. Ю. Грицюк, Л. С. Сікора, Ю. І. Грицюк

Національний університет "Львівська політехніка", м. Львів, Україна

ПРОБЛЕМИ ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК У ЗАКОДОВАНИХ ПОВІДОМЛЕННЯХ МАТРИЦЯМИ ФІБОНАЧЧІ

Проаналізовано основні проблеми виявлення та наявні методики виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, що дають можливість знаходити і виправляти одну, дві та три помилки в однакових чи різних рядках кодового слова. З'ясовано, що за останнє десятиліття надруковано багато різноманітних публікацій, в кожній з яких обґрунтовано доцільність використання матриць Фібоначчі для (де)кодування даних. Встановлено, що елементи кодового слова, отриманого множенням блоку повідомлення на матрицю Фібоначчі, мають багато корисних властивостей, на яких ґрунтується методика виявлення та виправлення у них помилок. Наведено твердження, згідно з яким відношення відповідних елементів кодового слова наближене до золотого перерізу, що має важливе значення для наявних методик виправлення потенційних помилок. Така властивість елементів дає можливість ідентифікувати присутність подвійних і потрійних помилкових елементів, перевіряючи приналежність їхніх відношень фіксованому інтервалу. З'ясовано, що хибна приналежність свідчить про те, що в різних рядках кодового слова є дві помилки, для виправлення яких потрібно розв'язати відповідні діофантові рівняння, придатність розв'язку якого має задовольнити певні умови виправлення помилок. З'ясовано, що для виправлення двох помилок в одному рядку кодового слова було поставлено умову, згідно з якою набір блоків вхідного повідомлення має містити тільки мінімальні матриці, що дає можливість брати найменші розв'язки діофантового рівняння, придатність яких уточнюють перевірочними співвідношеннями. Виявлено, що для виправлення трьох помилок у кодовому слові потрібно перевірити приналежність фіксованому інтервалу відношень відповідних його елементів та розв'язати нелінійне діофантове рівняння, реалізація якого є надзвичайно складною. Запропонований підхід зводиться до проб і помилок, згідно з яким спочатку потрібно знайти точне місце розташування помилкових елементів, а вже потім їх виправляти за відповідними методиками.

Ключові слова: числа Фібоначчі; рекурентна послідовність; кодове слово; золотий переріз; діофантові рівняння; методи виправлення помилок.

Вступ / Introduction

Теорія кодування даних упродовж багатьох десятиліть має важливе значення для інформаційно-комунікаційних технологій [31, 32], внаслідок чого розроблено багато різних підходів до виявлення та виправлення можливих помилок, що виникають під час передачі закодованих повідомлень [9]. Водночас, застосування сучасних методів кодування даних з виправленням помилок під час розроблення криптографічних систем [10, 11, 14], стійких до квантових атак, зацікавило багатьох науковців до творчих пошуків і сприяло появі нових досліджень. Проте, основний недолік кодування даних з виправленням помилок у криптографії в тому, що там використовують ключі великої розмірності з недостат-

ньою коригувальною здатністю [12, 13, 15]. Тому розроблення нових підходів до (де)кодування даних з виявленням і виправленням помилок є актуальною дослідницькою роботою, а для криптографічних систем проблема пошуку компактних ключів досі є відкритою.

У 2005 році О. Стахов у своїй роботі [28] запропонував так звану теорію кодування даних і коригування помилок p -числами Фібоначчі, метод декодування яких використовував певні властивості цих чисел, їх узагальнення та наближення до золотого перерізу. Його теорія передбачала потребу розв'язування діофантових рівнянь для виправлення помилок у закодованих повідомленнях. Автор стверджував, що запропонований метод (де)кодування даних має здатність виправлення помилок 93,33% і що такі коди мають надмірність 33,3%.

Інформація про авторів:

Грицюк Павло Юрійович, аспірант, кафедра автоматизованих систем управління. Email: pavlo.hrytsiuk.mmtias.2022@lpnu.ua

Сікора Любомир Степанович, д-р техн. наук, професор, кафедра автоматизованих систем управління. Email: lssikora@gmail.com;
<https://orcid.org/0000-0002-7446-1980>

Грицюк Юрій Іванович, д-р техн. наук, професор, кафедра програмного забезпечення. Email: yurii.i.hrytsiuk@lpnu.ua;
<https://orcid.org/0000-0001-8183-3466>

Цитування за ДСТУ: Грицюк П. Ю., Сікора Л. С., Грицюк Ю. І. Проблеми виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі. Науковий вісник НЛТУ України. 2023, т. 33, № 4. С. 45–58.

Citation APA: Grytsiuk, P. Yu., Sikora, L. S., & Hrytsiuk, Yu. I. (2023). Problems of detecting and correcting errors in messages encoded by Fibonacci matrices. *Scientific Bulletin of UNFU*, 33(4), 45–58. <https://doi.org/10.36930/40330407>

Проте, його обнадійливі заяви в багатьох дослідників [2, 3, 5, 22, 30] викликали деякі підозри насамперед з точки зору теорії інформації. Вони вважали, що потрібно провести дещо глибший і точніший аналіз результатів дослідження О. Стахова як щодо надмірності кодів, так і щодо їхньої можливості виявлення та виправлення помилок у закодованих повідомленнях.

Наприклад, у роботі [5, розд. 5] було пояснено, що деякі методології та висновки, зроблені О. Стаховим, є оманливими та недостовірними. З практичної точки зору важко придумати реальний канал передачі даних, у якому можна було б використати коди, запропоновані О. Стаховим. Водночас, вони розглядали згадані вище проблеми тільки у разі використання оригінальних кодів на підставі чисел 1-Фібоначчі. Спочатку автори показали можливість удосконалення етапу виявлення помилок, потім продемонстрували можливість виправлення деяких помилок без потреби розв'язувати потенційно складні діофантові рівняння. Також вони вказали, як обмежити простір вхідних повідомлень, щоб не було неоднозначності під час їх кодування, так і декодування, та надали явну формулу для визначення надмірності цих кодів.

Проте, виконане в роботі [5] дослідження, як і в багатьох інших [3, 22, 30], стосується матриці Фібоначчі розміром 2×2 і, як наслідок, закодованих повідомлень, блоки яких мають аналогічний розмір, що в практиці передачі даних трапляється вкрай рідко. Тому виникає потреба в проведенні додаткових досліджень як щодо виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі значно більших розмірів, так і отримання оригінального коду з можливістю виправлення помилок і компактним його поданням.

Об'єкт дослідження – виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі.

Предмет дослідження – алгоритми і методи отримання оригінального коду на підставі матриць Фібоначчі з можливістю виправлення помилок і компактним його поданням, що дасть можливість передавати каналами зв'язку відповідні блоки закодованих повідомлень різної величини.

Мета роботи – з'ясувати проблеми виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, що дасть змогу ефективно передавати каналами зв'язку блоки даних різної величини.

Для досягнення зазначеної мети визначено такі основні завдання дослідження:

- проаналізувати останні дослідження та публікації та встановити основну складність проблеми виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі;
- проаналізувати традиційні методи (де)кодування даних матрицями Фібоначчі, які мають багато корисних і цікавих властивостей, навести тільки ті із них, які використовують у традиційному методі кодування даних;
- проаналізувати можливість виявлення та виправлення помилок у закодованому повідомленні, навести деякі твердження та їхні доведення, на яких базуються наявні методики виправлення однієї, двох і трьох помилок у рядках кодового слова;
- зробити висновки за результатами виконаного дослідження та надати відповідні рекомендації щодо їх практичного використання.

Аналіз останніх досліджень та публікацій. Дослідження оригінальних кодів із компактним їх поданням,

які б давали можливість виявляти та виправляти помилки у закодованих повідомленнях, за останнє десятиліття привернуло увагу багатьох дослідників, особливо через їх використання у стійких до атак криптосистемах, що працюють на квантових комп'ютерах.

У 2006 році О. Стахов [28], сподіваючись на детальніший аналіз результатів майбутніх досліджень, дав декілька цікавих ідей щодо використання чисел Фібоначчі для отримання оригінального коду з можливістю виправлення помилок і компактним його поданням. Він вважав, що числа Фібоначчі $(F_n)_{n=0}^{+\infty}$ є однією з найвідоміших лінійних рекурентних послідовностей, визначених у такий спосіб:

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}, \forall n \geq 1. \quad (1)$$

Таку лінійну рекурентну послідовність 2-го порядку можна узагальнити й на вищі порядки, а саме:

$$F_1^{(p)} = \dots = F_{p+1}^{(p)} = 1, F_n^{(p)} = F_{n-1}^{(p)} + F_{n-p}^{(p)}, \forall n > p+1, \quad (2)$$

елементи якої мають назву p -чисел Фібоначчі $(p+1)$ -го порядку з характеристичним поліномом $x^{p+1} - x^p - 1$ [27].

Метод (де)кодування даних p -числами Фібоначчі, запропонований О. Стаховим [28], було удосконалено у подальших його дослідженнях. Наприклад, у роботі [29] вказано на деякі особливості p -коду Фібоначчі, надаючи йому певну оцінку надмірності. Однак, під час такого оцінювання він не брав до уваги зростання величини блоку повідомлення через збільшення розмірів матриць Фібоначчі, задіяних у методі кодування даних, а тільки розглядав передачу визначника цих матриць, які й використовували для декодування повідомлень.

Тоді, як О. Стахов у своїх дослідженнях здебільшого зосереджував увагу на випадку $p = 1$, що відповідає класичним числам Фібоначчі, то в роботі [7] продемонстровано результати аналізу обчислювальної складності методу (де)кодування даних у загальному випадку, пропонуючи для наочності деякі числові приклади. Цими прикладами вони показали, що в найгіршому випадку хоча й можна виправляти помилки в закодованих повідомленнях, проте це потребує тривалого проміжку часу $\Theta(2^{p^2})$, наприклад, за $p = 3$, $2^{3^2} = 512$. Водночас, автори дали уточнення, що такий найгірший випадок не є серйозною проблемою для криптографічних систем [9, 14], оскільки він практично ніколи не виникає, враховуючи сучасні характеристики каналів передачі даних. Вони також показали, що запропонований ними метод (де)кодування даних має коефіцієнт виправлення помилок $(2^{p^2} - 1) / 2^{p^2}$ ($p = 3$, $(2^{3^2} - 1) / 2^{3^2} = 0,998047$). Однак, під час обговорення результатів дослідження автори навіть не згадують про процедуру розв'язування відповідних діофантових рівнянь, яка існує на етапі виправлення помилок. Адже відомо [5, розд. 3], що ця процедура може бути досить тривалою, якщо не внести деякі коригування в початкових даних, щоб успішно потім виявляти та виправляти помилки у закодованих повідомленнях.

Аналогічно у роботі [3] наведено дещо уточнений коефіцієнт виправлення помилок $(2^{p^2} - 2) / (2^{p^2} - 1)$, що для $p = 3$ становить $(2^{3^2} - 2) / (2^{3^2} - 1) = 0,998043$, і запропонували спеціальне обговорення результатів свого дослідження для $p = 2$. Також у цьому дослідженні вони взяли до уваги тільки матричні операції, задіяні на етапі виявлення помилок, без обговорення потреби викорис-

тання діофантових рівнянь для їх виправлення в закодованих повідомленнях.

У роботі [5] йдеться про декодування повідомлень з виправленням помилок за допомогою матриць 1-Фібоначчі. Автори наводять явну формулу для обчислення надмірності кодів Стахова, ідентифікують деякі потоки даних у початковій процедурі їх декодування, ключовим моментом якої є потреба розв'язування деяких нетривіальних діофантових рівнянь. Також вони надали результати детального обговорення деяких випадків уникнення процедури розв'язання таких рівнянь і рекомендації, як ефективніше виявляти та виправляти помилки в закодованих повідомленнях.

У роботі [19] наведено новий метод (де)кодування даних з використанням Q -матриць Фібоначчі, заснований на матрицях заблокованих повідомлень. Головною перевагою такого методу є кодування кожної матриці вхідного повідомлення ключами різної величини [13, 15]. Як стверджують автори, такий підхід не тільки підвищує безпеку закодованих повідомлень від криптографічних атак [10, 14], але й має високу коригувальну здатність, однак не вказують, чим саме чи як саме це забезпечується.

У роботі [2] запропоновано нову теорію кодування даних з використанням узагальнених n -крокових поліномів Фібоначчі. На підставі цих поліномів було визначено новий клас квадратної $M_{h,n}(x)$ -матриці n -го порядку ($x \geq 1$) та отримано певні співвідношення між елементами цієї матриці. В результатах дослідження було обговорено достовірність цього методу, де показано, що для $n = 2$ його коригувальна здатність становить 93,33 %, тоді як для $n = 3$ його достовірність вже становить 99,80 %. Цікавою особливістю розробленого методу (де)кодування даних є те, що його достовірність не залежить від коефіцієнтів полінома Фібоначчі, за винятком n -го коефіцієнта $h_n(x) = 1$, і зростає зі збільшенням порядку квадратної $M_{h,n}(x)$ -матриці.

У роботі [4] запропоновано нову теорію кодування даних з використанням m -розширення p -чисел Фібоначчі. Автори навели квадратну $G_{p,m}$ -матрицю Фібоначчі, де $p \geq 0$ є цілим невід'ємним числом і $m > 0$. Також описали різні властивості $G_{p,m}$ -матриці, яка є основою теорії кодування даних, встановили зв'язки між елементами цієї матриці для різних значень p і m . Автори показали, що співвідношення між елементами $G_{p,m}$ -матриці для різних значень p і $m = 1$ збігаються з відношенням між елементами матриці кодування для різних значень p [3]. Загалом, достовірність запропонованого методу зростає зі збільшенням цього значення, але вона не залежить від значення m .

У роботі [1] наведено узагальнену теорію кодування даних на (m,t) -розширенні поліномів p -числами Фібоначчі. Насамперед вони визначають (m,t) -розширення p -чисел Фібоначчі та золотих (p,m,t) -пропорцій, де $p \geq 0$ є цілим невід'ємним числом, $m > 0$ і $t > 0$. Автори встановили співвідношення між золотою (p,m,t) -пропорцією, між золотою (p,m) -пропорцією та між золотою p -пропорцією. У такий спосіб вони визначили квадратну $G_{p,m,t}$ -матрицю Фібоначчі. Також автори показали, що, за умови правильного вибору початкових членів для (m,t) -розширення p -чисел Фібоначчі, можна застосувати процедуру (де)кодування даних з використанням $G_{p,m,t}$ -матриці Фібоначчі. Було зроблено висновок, що для $t = 1$ зв'язки між елементами матриці кодування да-

них для різних значень p і m збігаються з аналогічними початковими членами чисел Фібоначчі [4].

У роботі [3] розроблено узагальнені співвідношення між елементами матриці кодування даних числами Фібоначчі. Автори розглядали клас квадратної матриці Фібоначчі $(p+1)$ -порядку, елементи якої базуються на p -числах Фібоначчі з визначником, що становить ± 1 . Вони стверджують, що існує зв'язок між числами Фібоначчі з початковими членами, який відомий як формула Кассіні, а саме: $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$, $n \geq 1$. Було встановлено, що послідовність чисел Фібоначчі та золотий переріз мають важливе значення під час побудови відносно нової теорії простору-часу, яка відома як E -теорія нескінченності. Оригінальний метод (де)кодування даних числами Фібоначчі впливає з аналогічних матриць, де відомим залишається зв'язок між її елементами для випадку $p = 1$ [28]. Також автори встановили узагальнені співвідношення між елементами матриці кодування даних для різних значень p . Наприклад, для $p = 2$ достовірність запропонованого методу становить 99,80 % і зростає зі збільшенням цього значення.

У роботі [28] розроблено матрицю Фібоначчі, наведено узагальнення формули Кассіні та нову теорію кодування даних. Автори розглядали новий клас квадратних матриць розміром $(p+1) \times (p+1)$, елементами яких були p -числа Фібоначчі ($p = 0, 1, 2, 3, \dots$), а їхній визначник становить ± 1 . Ця унікальна властивість матриць Фібоначчі приводить до узагальнення формули Кассіні. Запропонований оригінальний метод (де)кодування даних числами Фібоначчі впливає з аналогічних матриць n -порядку. На відміну від класичних надлишкових кодів основною особливістю запропонованого методу є те, що він дає змогу коригувати закодовані елементи матриці, які теоретично можуть бути необмеженими цілими числами. Для найпростішого випадку коригувальна здатність цього методу становить 93,33 %, що значно перевищує відомі коригувальні можливості інших методів.

У роботі [7] наведено новий клас кодів з можливістю виправлення помилок на підставі послідовності чисел Фібоначчі. Запропоновано клас квадратних M_p^n -матриць n -го степеня p -го порядку для (де)кодування даних і запропоновано методику контролю за появою помилок. Це значно розширює результати попередніх досліджень [28] щодо методів коригування помилок, зумовлених під час передачі закодованих повідомлень каналами зв'язку. Автори вважають, що для цілого числа p можна згенерувати двійкову M_p^n -матрицю n -го степеня розміром $(p+1) \times (p+1)$, ненульові елементи якої розташовані або на супердіагоналі, або в останньому рядку матриці. Звичайну M_p^n - та обернену M_p^{-n} -матриці n -го ступеня використовують як матриці кодування та даних декодування відповідно. Також вони показали, що для достатньо великих значень n , незалежно від значень елементів матриці повідомлення M_p , між елементами закодованої матриці існують зв'язки $E_p = M_p \times M_p^n$. Ці відношення мають важливе значення під час виявлення та виправлення помилок у закодованих повідомленнях.

У роботі [23] розглянуто узагальнені співвідношення між елементами матриці кодування даних, запропоновано нову комплексну $H_{p,n}$ -матрицю Фібоначчі, елементами якої є відповідні числа. Розроблено метод (де)кодування, що впливає з цієї комплексної $H_{p,n}$ -мат-

риці Фібоначчі, а також встановлено зв'язки між її елементами. Також запропоновано підхід до виявлення та виправлення помилок у закодованих повідомленнях, що ґрунтується на потребі розв'язування діофантових рівнянь.

У роботі [8] розроблено метод кодування даних на підставі поліномів Фібоначчі з можливістю виявлення та виправлення помилок у закодованих повідомленнях. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$ розроблено Q_m^n -матрицю n -го степеня розміром $m \times m$, яку названо $Q_m^n(x)$ -матрицю кодування даних, елементами якої є поліноми Фібоначчі. Для декодування даних автори вводять обернену $Q_m^n(x)$ -матрицю, особливість яких у тому, що їхній визначник становить ± 1 . Наведено простий критерій виявлення помилок і відповідний метод їх виправлення для цього класу матриць. Також показано, що ймовірність появи помилок у закодованих повідомленнях майже дорівнює нулю за досить великих значень m . Наведено наочні приклади (де)кодування даних, а також різні випадки виявлення та виправлення помилок у закодованих повідомленнях.

У роботі [6] розроблено новий метод кодування даних на підставі поліномів Фібоначчі з високою швидкістю їх генерування. Для цілих чисел m , n і $x \geq 1$ можна згенерувати квадратну $Q_{2m}^n(x)$ -матрицю n -го степеня $2m$ -го порядку, елементами якої є поліноми Фібоначчі, і відповідну обернену $Q_{2m}^n(x)$ -матрицю для їх декодування [12, 13, 15]. Також показано, що швидкість (де)кодування даних за допомогою цих матриць значно вища, ніж з оригінальними матрицями на підставі звичайних чисел Фібоначчі.

У роботі [21] наведено привабливі, як на перший погляд, показники надійності теорії кодування даних поліномами Фібоначчі. Розроблено новий клас квадратних $Q_{pm}^n(x)$ -матриць n -го степеня та pm -го порядку для кодування даних, де $p \geq 3$, $m \geq 1$, $n \geq 1$, $x \geq 1$, елементами яких є поліноми Фібоначчі. Запропонований метод декодування даних впливає з можливості отримання відповідних обернених $Q_{pm}^n(x)$ -матриць, визначник яких становить ± 1 . При цьому спостерігалися як великі швидкості виконання таких процедур, так і отриманих закодованих повідомлень, стійких до криптографічних атак [10, 14].

У роботі [20] запропоновано нову теорію кодування даних на $(h(x), g(y))$ -розширенні поліномів p -числами Фібоначчі. Визначено також золоті $(p, h(x), g(y))$ -пропорції, де $p \geq 0$ – цілі числа, $h(x) > 0$, $g(y) > 0$ – поліноми з дійсними коефіцієнтами. Встановлено, що співвідношення між елементами квадратної $G_{p,h,g}$ -матриці Фібоначчі повністю збігаються зі співвідношеннями між елементами матриці кодування для різних значень p і поліномів $h(x) = m$ і $g(y) = t$ [1]. Також співвідношення між елементами матриці кодування для поліномів $h(x) = 1$ і $g(y) = 1$ збігаються з узагальненими співвідношеннями між елементами матриці кодування числами Фібоначчі [3]. Завдяки відповідному вибору початкових членів у $(h(x), g(y))$ -розширенні поліномів p -числами Фібоначчі квадратну $G_{p,h,g}$ -матрицю можна застосувати для (де)кодування даних різної величини. Під час обговорення результатів свого дослідження автори стверджують, що достовірність цього методу зростає зі збіль-

шенням значення p , але вона не залежить від значень поліномів $h(x)$ і $g(y)$, які значно удосконалюють криптографічну стійкість закодованих повідомлень [9, 11]. Складність цього методу зростає зі збільшенням степеня поліномів $h(x)$ і $g(y)$. Також знайдено зв'язок між золотою $(p, h(x), g(y))$ -пропорцією, між золотою $(p, h(x))$ -пропорцією та між золотою p -пропорцією.

У роботі [29] О. Стахов розглядає математику гармонії – від Евкліда до сучасної математики та інформатики. Це видання є результатом чотирьох десятиліть досліджень автора в галузі чисел Фібоначчі та золотого перерізу, а також їх застосування для (де)кодування даних. Він дає широкий вступ до вишуканої теми "Математика гармонії", нового міждисциплінарного напрямку в сучасній науці. Цей напрям бере свій початок від елементів Евкліда і має багато несподіваних застосувань у сучасній математиці. Насамперед це стосується нового підходу до трактування історії математики, узагальнених чисел Фібоначчі та узагальненої золотой пропорції, "золотих" алгебричних рівнянь, узагальненої формули Біне для чисел Фібоначчі та "золотих" матриць [27]. Математика гармонії торкається й теоретичної фізики (нові гіперболічні моделі природи) та інформатики, передусім алгоритмічної теорії вимірювання, системи числення з ірраціональними радикалами тощо.

У праці "Узагальнена формула Біне та її застосування" [18] детально розглянуто властивості чисел Фібоначчі, обґрунтовує достовірність формули Біне, розглядає аналог формули Біне та можливості її застосування. Показано, що особливе значення при вивченні властивостей чисел Фібоначчі має формула

$$U_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right], \quad (3)$$

яку називають формулою Біне (Жак Біне (1786–1856 рр.) – французький математик і астроном). Існують різні способи обґрунтування достовірності цієї формули, проте автор стверджує, що числа U_n , визначені цією рівністю, задовольняють певне рекурентне співвідношення. Наприклад, за $n = 1$ і $n = 2$, $U_1 = 1$, $U_2 = 1$. Якщо ж $n > 2$, то маємо такий вираз

$$U_n + U_{n-1} = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n-1} \left(\frac{1+\sqrt{5}}{2} + 1 \right) - \left(\frac{1-\sqrt{5}}{2} \right)^{n-2} \left(\frac{1-\sqrt{5}}{2} + 1 \right) \right], \quad (4)$$

$$\text{де: } \frac{1+\sqrt{5}}{2} + 1 = \frac{3+\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2} \right)^2; \quad \frac{1-\sqrt{5}}{2} + 1 = \frac{3-\sqrt{5}}{2} = \left(\frac{1-\sqrt{5}}{2} \right)^2.$$

Але тоді права частина формули становить U_{n+1} і, як наслідок, члени послідовності $U_1, U_2, \dots, U_n, \dots$ задовольняють рекурентне співвідношення (4), тобто збігаються з відповідними членами послідовності чисел Фібоначчі [18].

Отже, за результатами проведеного аналізу останніх досліджень та публікацій стосовно проблеми виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі встановлено, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано доцільність використання матриць Фібоначчі для (де)кодування даних. Проте, більшість досліджень стосується матриць Фібоначчі розміром 2×2 і, як наслідок, закодованих повідомлень, блоки яких мають аналогічний розмір, що в практиці передачі даних трапляється вкрай рідко. Тому проведення додаткових дос-

ліджень щодо виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі значно більших розмірів є актуальною проблемою, яку й спробуємо частково вирішити в цьому дослідженні.

Результати дослідження та їх обговорення / Research results and their discussion

1. Традиційний метод (де)кодування даних матрицями Фібоначчі. Проаналізуємо метод кодування даних, який запропонував О. Стахов у роботі [28]. Для спрощення викладення матеріалу далі зосередимо увагу на випадку $p = 1$ [1, 3, 4, 7, 21], тобто на класичних числах Фібоначчі (1) та на аналогічних матрицях. Проте, досить легко узагальнити результати дослідження для більших значень p . У будь-якому випадку матриці Фібоначчі, елементами яких є відповідні послідовності чисел (1) чи (2), мають багато корисних і цікавих властивостей. Наведемо тільки ті властивості матриць Фібоначчі, які використовують у традиційному методі кодування даних, а саме:

- задано матрицю $\bar{Q}^1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, отримаємо $\bar{Q}^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ і $\bar{Q}^{-n} = \begin{bmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{bmatrix} \forall n \geq 1$;
- $\det \bar{Q}^n = (-1)^n$, що є тотожністю Кассіні $F_{n+1}F_{n-1} - F_n^2 = (-1)^n \forall n \geq 1$;
- $\bar{Q}^{-2k} = \begin{bmatrix} F_{2k-1} & -F_{2k} \\ -F_{2k} & F_{2k+1} \end{bmatrix} \forall k > 0$; $\bar{Q}^{-(2k+1)} = \begin{bmatrix} -F_{2k} & F_{2k+1} \\ F_{2k+1} & -F_{2k+2} \end{bmatrix} \forall k > 0$;
- $\lim_{n \rightarrow +\infty} \left\{ \frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right\} = \varphi$, де φ – золотий переріз, тобто най-більший за модулем корінь рівняння $x^2 - x - 1$.

Нехай задано повідомлення $\bar{P}$, елементами якого є цілі додатні числа, розділене на блоки по чотири в кожному. Подамо кожен блок за допомогою матриці розміром 2×2 , а саме

$$\bar{M} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}, \quad (5)$$

елементи якої є додатними ненульовими цілими числами, тобто будь-який блок повідомлення $\bar{P}$ можна ідентифікувати матрицею (5). Процедура кодування блоку такого повідомлення полягає в множенні матриці $\bar{M}$ на матрицю її кодування, тобто на $\bar{Q}^n$ -матрицю n -го степеня, внаслідок чого отримаємо:

$$\bar{C} = \bar{M} \times \bar{Q}^n = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}, \quad (6)$$

де: $c_1 = m_1 \cdot F_{n+1} + m_2 \cdot F_n$; $c_2 = m_1 \cdot F_n + m_2 \cdot F_{n-1}$;
 $c_3 = m_3 \cdot F_{n+1} + m_4 \cdot F_n$; $c_4 = m_3 \cdot F_n + m_4 \cdot F_{n-1}$.

Якщо О. Стахов у своїй роботі [28] посилається на так зване кодове слово $\bar{C}$, то в роботі [5] також використано як аналогічну $\bar{Q}^n$ -матрицю кодування даних з відповідними елементами, так і методи отримання такого кодового слова. Окрім цього, щоб виявляти та виправляти можливі помилки, кодове слово $\bar{C}$ потрібно надсилати разом із перевірочним елементом $\det \bar{M}$, який має важливе значення для виправлення помилок.

Отже, маючи кодове слово $\bar{C}$, отримувач може його декодувати, щоб отримати початкове повідомлення $\bar{M}$ за допомогою такого матричного виразу:

$$\bar{C} \times \bar{Q}^{-n} = \bar{M} \Rightarrow \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \times \begin{bmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{bmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}, \quad (7)$$

де: $m_1 = -F_{n-1} \cdot c_1 + F_n \cdot c_2$; $m_2 = F_n \cdot c_1 - F_{n+1} \cdot c_2$;
 $m_3 = -F_{n-1} \cdot c_3 + F_n \cdot c_4$; $m_4 = F_n \cdot c_3 - F_{n+1} \cdot c_4$.

У своєму дослідженні [28] О. Стахов сформулював гіпотезу щодо можливості виявлення та виправлення потенційних помилок у вигляді такого твердження.

Твердження 1. Нехай задано повідомлення $\bar{M}$. Якщо кодове слово $\bar{C}$ не містить помилок, то:

- існує тотожність між визначниками матриць

$$\det \bar{C} = (-1)^n \det \bar{M}; \quad (8)$$

- відношення певних елементів кодового слова відповідають золотому перерізу

$$\frac{c_1}{c_2} \approx \frac{c_3}{c_4} \approx \varphi, \quad (9)$$

а значення обчислених елементів

$$c_1 = \frac{(-1)^n \det \bar{M} + c_2 c_3}{c_4}, c_2 = \frac{(-1)^n \det \bar{M} + c_1 c_4}{c_3}, \quad (10)$$

$$c_3 = \frac{(-1)^n \det \bar{M} + c_1 c_4}{c_2}, c_4 = \frac{(-1)^n \det \bar{M} + c_2 c_3}{c_1}$$

є цілими числами [28]. Наближення відношення певних елементів (9) до золотого перерізу має важливе значення під час виправлення потенційних помилок, тобто їх можна визначити явно, як буде видно з наведеного нижче матеріалу.

У процедурі (де)кодування даних, яку запропонував О. Стахов у роботі [28], перевірочний елемент $\det \bar{M}$ потрібно надіслати отримувачу разом із кодовим словом $\bar{C}$. Як і О. Стахов, так і в роботі [5] надано припущення, що перевірочний елемент надходить отримувачу без помилок. Якщо $\det \bar{C} \neq (-1)^n \det \bar{M}$, то кодове слово $\bar{C}$ містить одну або більше помилок. Інакше автори роблять висновок, що кодове слово $\bar{C}$ не містить жодних помилок і повідомлення $\bar{M}$ можна відновити за допомогою виразу (7). За умови, якщо $\det \bar{C} \neq (-1)^n \det \bar{M}$ виконується, то потрібно оцінити кожен з елементів за одним з виразів (10).

Якщо хоча б один з елементів c_i є цілим числом, то кодове слово $\bar{C}$ містить одну помилку, яку можна виправляти за допомогою одного з виразів (10). Якщо ж кодове слово містить більше однієї помилки, то всі елементи c_i не є цілими числами. У цьому випадку О. Стахов у роботі [28] рекомендує розв'язувати деякі діофантові рівняння та використати умову (9), щоб виправити помилки. Зокрема, він пропонує спочатку перевірити всі гіпотези щодо появи подвійних помилок (наприклад, елементи c_1 та c_2 помилкові), для виправлення яких потрібно розв'язати таке діофантове рівняння:

$$xc_4 - yc_3 = (-1)^n \det \bar{M}. \quad (11)$$

Якщо ж перевіряємо гіпотезу про те, що елементи c_3 та c_4 помилкові, то потрібно розв'язати таке діофантове рівняння:

$$-xc_2 + yc_1 = (-1)^n \det \bar{M}. \quad (12)$$

Серед значної кількості розв'язків діофантового рівняння (11) правильні значення елементів c_1 і c_2 можна забезпечити тими із них, які задовольняють властивість

обчислених елементів (10). У роботі [28] О. Стахов за-
явив, що за допомогою подібної процедури можна вип-
равити всі випадки появи двох і навіть трьох помилок у
кодівому слові $\bar{C}$. Метод не працює тільки тоді, коли
всі елементи c_i неправильні. У цьому випадку, як пояс-
нює О. Стахов, він не виконував поглибленого аналізу
можливості виявлення та виправлення всіх помилок,
позаяк мав за мету викласти тільки загальну гіпотезу
щодо їх виправлення та відповідні ідеї для їх реалізації.

Однак, у багатьох інших роботах [3, 4, 7, 20, 21] з
вирішення проблеми виявлення та виправлення поми-
лок у закодованих повідомленнях, бракує адекватного
аналізу отриманих результатів. Зокрема, деякі автори
[4, 20] тільки відзначають, що процедура розв'язання ді-
офантового рівняння складним завданням і може займа-
ти багато часу. Окрім цього, без деяких конкретних умов
щодо повідомлення (5) і деяких конкретних гіпотез що-
до точності обчислення елементів (10) може статися
так, що буде неможливо виявити правильне повідомлен-
ня серед значної кількості розв'язків діофантових рів-
нянь (11) чи (12).

Водночас, у роботі [5] була спроба дещо детальніше
обговорити ці питання, навівши деякі гіпотези, які знач-
но наближають можливість виявлення та виправлення
помилки у закодованих повідомленнях числами Фібо-
наччі. Вони також показали можливість виправлення
помилки, які неможливо було б виправляти взагалі. Ав-
тори стверджують, що правильність визначення та точ-
ність передачі перевірконого елемента $\det \bar{M}$ має фун-
даментальне значення для достовірності методу декоду-
вання даних. Однак, з практичної точки зору важко
уявити реальний канал передачі даних, у якому можна
було б гарантувати правильну передачу тільки значення
 $\det \bar{M}$, а не всього закодованого повідомлення. Одним
із рішень, що запропонував О. Стахов у роботі [28], є
надсилання перевірконого елемента $\det \bar{M}$ за допомо-
гою стандартного потоку передачі даних каналами
зв'язку, хоча це й виглядає не вельми практичним рі-
шенням, як стверджують автори в роботі [5].

Отже, за результатами аналізу традиційного методу
(де)кодування даних матрицями Фібоначчі встановле-
но, що елементи кодових слів мають багато корисних і
цікавих властивостей, на яких якраз і ґрунтується мето-
дика виявлення та виправлення помилок у закодованих
повідомленнях. Наведено відповідне твердження, згідно
з яким відношення певних елементів кодового слова наб-
лижене до золотого перерізу, має важливе значення для
наявних методик виправлення потенційних помилок.

**2. Можливість виявлення та виправлення поми-
лок у закодованому повідомленні.** У роботі [5] спо-
чатку підтверджено властивість (9) щодо точності наб-
лиження відношень елементів кодового слова $\bar{C}$ до зо-
лотого перерізу. Також вони показують можливість удо-
сконалення етапу виявлення помилок, який дає змогу
уникнути зайвої перевірки всіх гіпотез щодо появи под-
війних помилок. Автори наводять методику виправлен-
ня подвійних помилок у різних рядках за допомогою
простих обчислень замість потреби розв'язування від-
повідних діофантових рівнянь. Окрім цього, вони пока-
зали можливість обмеження простору повідомлення,
щоб уникнути неоднозначності в декодуванні подвій-
них помилок в одному рядку. Водночас, автори попере-

джають читача, що в їхньому дослідженні йдеться не
про бітові помилки, як це переважно роблять в методах
кодування даних. Натомість вони використовують тер-
мінологію О. Стахова та посилаються на цілочисельні
помилки, які зазвичай містять декілька десятків чи на-
віть сотень біт.

Для розуміння змісту наведеного нижче матеріалу
дослідження розглянемо деякі твердження та їхні дове-
дження, на яких базується методика виявлення та виправ-
лення помилок у закодованих повідомленнях матриця-
ми Фібоначчі, яку запропоновано в роботі [5].

Отже, за умови фіксованого значення n як натураль-
ного числа та для $\bar{Q}^n$ -матриць кодування даних наведе-
ні нижче результати доведення відповідних тверджень
істинні [5]. У цьому випадку, отримуючи повідомлення
 $\bar{M}$ і відповідне кодове слово $\bar{C}$ з використанням мат-
ричного виразу (6), отримаємо такі нерівності:

$$\frac{F_{n+1}}{F_n} < \frac{c_1}{c_2} < \frac{F_n}{F_{n-1}}, \frac{F_{n+1}}{F_n} < \frac{c_3}{c_4} < \frac{F_n}{F_{n-1}}, \quad (13)$$

які виражають точність наближень певних відношень
(9), викладених у твердженні 1. Нижче наведено деякі
властивості нерівності (13) у вигляді відповідних твер-
джень, які часто використовують для обґрунтування від-
повідних стратегій виявлення та виправлення помилок.

Твердження 2. Нехай задано h – ціле число. Якщо
 $\{m_1, m_2, m_3, m_4\} < F_{n-1}$, то приналежність будь-якого від-
ношення фіксованому інтервалу

$$\left\{ \frac{c_1 + h}{c_2}, \frac{c_1}{c_2 + h}, \frac{c_3 + h}{c_4}, \frac{c_3}{c_4 + h} \right\} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right] \quad (14)$$

істинне тоді, коли $h = 0$.

Доведення. Якщо $h = 0$, то, згідно з нерівністю (13),
приналежність першого відношення фіксованому інтер-

валу $\frac{c_1}{c_2} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ істинне. Тепер припустимо, прина-
лежність уточненого відношення цьому інтервалу

$\frac{c_1 + h}{c_2} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ також істинне. Це означає, що з ура-

хуванням (6) для верхньої межі фіксованого інтервалу
(14) матимемо таку нерівність: $\frac{m_1 F_{n+1} + m_2 F_n + h}{m_1 F_n + m_2 F_{n-1}} < \frac{F_n}{F_{n-1}}$.

Виконанням простих обчислень отримуємо таку нерів-
ність: $m_1(F_{n+1}F_{n-1} - F_n^2) + hF_{n-1} < 0$, звідки з урахуванням

тотожності Кассіні матимемо, що $h < \frac{m_1(-1)^{n-1}}{F_{n-1}}$. Анало-

гічно, з урахуванням (6) для нижньої межі фіксованого
інтервалу (14) матимемо таку нерівність:

$\frac{m_1 F_{n+1} + m_2 F_n + h}{m_1 F_n + m_2 F_{n-1}} > \frac{F_{n+1}}{F_n}$. Виконанням простих обчислень

отримуємо таку нерівність: $m_2(F_{n+1}F_{n-1} - F_n^2) + hF_n > 0$,
звідки з урахуванням тотожності Кассіні матимемо, що

$h > \frac{m_2(-1)^n}{F_n}$. Отже, якщо $\{m_1, m_2\} < F_{n-1}$, то в інтервалі

$\left[\frac{m_2(-1)^n}{F_n}, \frac{m_1(-1)^{n-1}}{F_{n-1}} \right]$ єдине ціле число $h = 0$.

Твердження 2 доведено. $\square$

Аналогічно можна довести приналежність інших
уточнених відношень елементів кодового слова $\bar{C}$ фік-
сованому інтервалу (14).

Твердження 3. Нехай задано h, k – цілі числа. Якщо $\{m_1, m_2, m_3, m_4\} < F_{n-1}$, то приналежність будь-якого відношення фіксованому інтервалу

$$\left\{ \frac{c_1 + h}{c_2 + k}, \frac{c_3 + h}{c_4 + k} \right\} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right] \quad (15)$$

істинне тоді, коли виконується така нерівність:

$$\frac{hF_{n-1} - m_1}{F_n} < k < \frac{hF_n + m_2}{F_{n+1}}.$$

Доведення. Візьмемо перше відношення та сформуємо нерівність $\frac{c_1 + h}{c_2 + k} < \frac{F_n}{F_{n-1}}$ для верхньої межі фіксованого інтервалу (15). Тоді, з урахуванням (6), матимемо таку нерівність:

$$\frac{m_1 F_{n+1} + m_2 F_n + h}{m_1 F_n + m_2 F_{n-1} + k} < \frac{F_n}{F_{n-1}}.$$

Припустимо, $k > -(m_1 F_n + m_2 F_{n-1})$, то легко отримати нерівність $h > \frac{hF_{n-1} - m_1}{F_n}$. Аналогічно, сформуємо таку нерівність

$$\frac{c_1 + h}{c_2 + k} > \frac{F_{n+1}}{F_n} \text{ для нижньої межі фіксованого інтервалу}$$

(15). Тоді, з урахуванням (6), матимемо таку нерівність: $\frac{m_1 F_{n+1} + m_2 F_n + h}{m_1 F_n + m_2 F_{n-1} + k} > \frac{F_{n+1}}{F_n}$. Якщо ж $k < -(m_1 F_n + m_2 F_{n-1})$, то

легко отримати нерівність $k < \frac{hF_n + m_2}{F_{n+1}}$. Водночас, якщо

$k < -(m_1 F_n + m_2 F_{n-1})$, то жодне можливе значення k не задовольняє приналежність цього відношення фіксованому інтервалу

$$\frac{c_1 + h}{c_2 + k} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right].$$

Твердження 3 доведено. $\square$

Аналогічно можна довести приналежність уточненого другого відношення елементів кодового слова $\bar{C}$ фіксованому інтервалу (15).

Отже, за результатами аналізу можливості виявлення та виправлення помилок у закодованому повідомленні підтверджено корисну властивість елементів кодового слова щодо точності наближення їхніх відношень до золотого перерізу, на яких якраз і ґрунтується відповідна методика. Для цього наведено деякі властивості певної нерівності у вигляді відповідних тверджень та їхніх доведень, які часто використовують для обґрунтування відповідних стратегій виявлення та виправлення помилок.

2.1. Удосконалення етапу виявлення помилок. У п. 1 коротко наведено стратегію виявлення та виправлення помилок у кодовому слові $\bar{C}$. Зокрема, спочатку потрібно використати значення елемента $\det \bar{M}$ для перевірки умови $\det \bar{C} \neq (-1)^n \det \bar{M}$. Якщо вона виконується, то кодове слово $\bar{C}$ містить одну або більше помилок. Для оцінювання значень елементів c_i за виразами (10) дотримуються таких гіпотез:

- 1) якщо тільки один з елементів c_i є цілим числом, то кодове слово $\bar{C}$ містить тільки одну помилку, яку можна виправити за методикою, наведеною в п. 1;
- 2) якщо всі елементи c_i не є цілими числами, то кодове слово $\bar{C}$ містить дві або більше помилок, виправлення яких, як виявиться згодом, також можливе.

О. Стахов у роботі [28] запропонував деякі стратегії вирішення другої гіпотези, але вони потребують дещо

глибшого аналізу та обговорення отриманих результатів. Передусім, неефективно перевіряти всі гіпотези щодо появи як подвійних, так і потрійних помилок. Зазвичай, зручніше використовувати деякі властивості елементів у кодовому слові $\bar{C}$, які можуть ідентифікувати наявну ситуацію (див. твердження 1). Для цього потрібно перевірити, чи відношення c_1/c_2 і c_3/c_4 належить фіксованому інтервалу $\left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$:

1) якщо відношення $\frac{c_1}{c_2} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ істинне, а відношення

$\frac{c_3}{c_4} \notin \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ хибне, то елементи c_1 і c_2 правильні, а елементи c_3 і c_4 – помилкові;

2) якщо відношення $\frac{c_1}{c_2} \notin \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ хибне, а відношення

$\frac{c_3}{c_4} \in \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right]$ істинне, то елементи c_1 і c_2 помилкові, а елементи c_3 і c_4 – правильні;

3) інакше маємо одну з таких ситуацій:

- а) елементи c_1 і c_3 помилкові або елементи c_2 і c_4 помилкові;
- б) елементи c_1 і c_4 помилкові або елементи c_2 і c_3 помилкові;
- в) є три елементи з чотирьох помилковими: c_1, c_2, c_3 (c_4); c_1, c_2, c_4 (c_3); c_1, c_3, c_4 (c_2); c_2, c_3, c_4 (c_1), де в дужках правильні елементи;
- г) є чотири елементи помилковими.

Зрозуміло, чотири помилкові елементи виправляти неможливо. Тому в роботі [5] детально обговорено ситуацію не з трьома помилковими елементами, а випадок, коли виникають тільки дві помилки.

Отже, показана можливість удосконалення етапу виявлення помилок, який дає змогу уникнути зайвої перевірки всіх гіпотез щодо появи як подвійних, так і потрійних помилок. Встановлено, що набагато зручніше використовувати деякі властивості елементів кодового слова, які можуть ідентифікувати наявні ситуації присутності помилок. Для цього потрібно перевірити приналежність фіксованому інтервалу відношень відповідних елементів кодового слова, що дасть можливість виявляти в ньому одну, дві та три помилки.

2.2. Можливість виправлення двох помилок у різних рядках. Для розуміння викладеного матеріалу використаємо такі позначення:

- $\bar{C}' = \begin{bmatrix} c'_1 & c'_2 \\ c'_3 & c'_4 \end{bmatrix}$ – отримане хибне повідомлення, яке може містити деякі помилкові елементи, тобто $\bar{C}' = \bar{C} + \bar{E}$;
- $\bar{E} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$ – матриця помилок, елементи якої є цілими числами;
- $a = \frac{F_{n+1}}{F_n}$ і $b = \frac{F_n}{F_{n-1}}$ – відповідно нижнє і верхнє значення фіксованого інтервалу.

Якщо всі елементи матриці $\bar{E}$ нульові, то так зване хибне повідомлення $\bar{C}'$ не має помилкових елементів, тобто воно тотожне кодовому слову $\bar{C}$.

Нехай отримано хибне повідомлення $\bar{C}'$, де маємо такі хибні відношення $c'_1/c'_2 \notin [a, b]$ і $c'_3/c'_4 \notin [a, b]$, тобто

матимемо наявність двох помилок. Можливі помилки можуть бути в таких елементах: c'_1, c'_3 ; c'_2, c'_4 ; c'_1, c'_4 або c'_2, c'_3 , тобто це ті помилки, які трапляються не в одному рядку матриці $\bar{C}'$. У цьому випадку О. Стахов запропонував підхід [28], який потребує розв'язання таких діофантових рівнянь:

$$\begin{aligned} xc'_4 - yc'_2 &= (-1)^n \det \bar{M}, & xc'_1 - yc'_3 &= (-1)^n \det \bar{M}, \\ xy - c'_2 c'_3 &= (-1)^n \det \bar{M}, & c'_1 c'_4 - xy &= (-1)^n \det \bar{M}. \end{aligned} \quad (16)$$

Розв'язки рівнянь за цими виразами потрібно підібрати так, щоб вони дали можливість задовольнити умову виправлення помилок (10). Цей підхід має декілька проблем. Насамперед без будь-якої додаткової умови на повідомлення $\bar{M}$ може статися так, що серед значної кількості розв'язків діофантових рівнянь (16) буде важко знайти ті, що належать фіксованому інтервалу $[a, b]$. Водночас, ці діофантові рівняння важко розв'язати, якщо значення перевірного елемента $\det \bar{M}$ надто велике, тобто така процедура еквівалентна задачі факторизації великого цілого числа [26]. Якщо ж розглядати повідомлення $\bar{M}$ таким, що $\{m_1, m_2, m_3, m_4\} < F_{n-1}$, то, згідно з твердженням 2, можемо виправити помилки, не розв'язуючи жодного діофантового рівняння.

Нагадаємо, факторизація цілого числа (англ. *Integer Factorization*) – розкладання заданого числа на прості множники. На відміну від задачі розпізнавання простого числа, факторизація є надзвичайно складною задачею, особливо, якщо йдеться про великі цілі числа. Передбачувана складність такої задачі знаходиться в основі криптостійкості деяких алгоритмів шифрування з відкритим ключем [15], таких як RSA. Метод перебору можливих дільників, або метод пробного поділу – найбільш тривіальний алгоритм факторизації, має обчислювальну складність $\Theta(N^{1/2} \log(N))$, де N – число, що підлягає факторизації.

Наприклад, розглянемо так зване хибне повідомлення $\bar{C}'$, яке містить помилки елементів головної діагоналі, тобто помилкові елементи $\{e_1, e_3\} \neq 0$, а правильні $\{e_2, e_4\} = 0$. Згідно з твердженням 2, елемент c_1 є єдиним цілим числом тоді, коли відношення $c_1 / c_2 \in [a, b]$ істинне, тоді легко можемо знайти ціле число e_1 . Дійсно, якщо нерівність $c'_1 / c'_2 = c'_1 / c_2 > b$ виконується, то помилковий елемент e_1 є найменшим цілим числом, більшим за раціональне число $c'_1 - c'_2 \cdot b = c'_1 - c_2 \cdot b$, тобто значення елемента становить $e_1 = \lceil c'_1 - c_2 \cdot b \rceil$, де $\lceil \cdot \rceil$ – функція, що визначає стелю числа. Аналогічно можемо отримати значення помилкового елемента $e_3 = \lceil c'_3 - c_4 \cdot b \rceil$.

Можемо помітити, що в розглянутих тут ситуаціях, коли дві помилки трапляються не в одному рядку, процедури виправлення відповідних елементів є незалежними. Наприклад, для оцінювання помилкового елемента e_1 було використано елементи c'_1 і $c'_2 = c_2$, а для оцінювання помилкового елемента e_3 – елементи c'_3 і $c'_4 = c_4$. Усі випадки появи двох помилок, які трапляються не в одному рядку матриці $\bar{C}'$, можна виявляти та виправляти за однаковими методиками.

Підсумовуючи зазначене вище, спробуємо оцінити помилковий елемент e_i усіма перевірочними співвідношеннями, які можуть тут виникнути:

- 1) якщо відношення $c'_i / c_j > b$ істинне, то обчислюємо елемент $e_i = \lceil c'_i - c_j \cdot b \rceil$ для $(i=1 \wedge j=2) \vee (i=3 \wedge j=4)$;
- 2) якщо відношення $c_i / c'_j > b$ істинне, то обчислюємо елемент $e_j = \lceil c'_j - c_i / b \rceil$ для $(i=1 \wedge j=2) \vee (i=3 \wedge j=4)$;
- 3) якщо відношення $c'_i / c_j < a$ істинне, то обчислюємо елемент $e_i = \lfloor c'_i - c_j \cdot a \rfloor$ для $(i=1 \wedge j=2) \vee (i=3 \wedge j=4)$;
- 4) якщо відношення $c_i / c'_j < a$ істинне, то обчислюємо елемент $e_j = \lfloor c'_j - c_i / a \rfloor$ для $(i=1 \wedge j=2) \vee (i=3 \wedge j=4)$.

Можемо помітити, що перевірочні співвідношення 1)–4) не використовують перевірочний елемент $\det \bar{M}$, тобто їхні значення набагато легше оцінювати, ніж розв'язувати діофантові рівняння (16). Якщо б отримувачу кодового слова $\bar{C}$ були відомі позиції помилкових елементів у матриці $\bar{C}'$, тоді немає потреби надсилати перевірочний елемент $\det \bar{M}$ разом із цим кодовим словом. Оскільки позиції цих елементів наперед невідомі, тому необхідно використовувати їх для реалізації методики виправлення помилок.

Наприклад, якщо відношення $c'_1 / c'_2 > b$ істинне і не знаємо, який помилковий елемент $e_1 \neq 0$ чи $e_2 \neq 0$, то потрібно оцінити значення як елемента $e_1 = \lceil c'_1 - c'_2 \cdot b \rceil$, так і елемента $e_2 = \lfloor c'_2 - c'_1 / b \rfloor$. У випадку використання помилкового елемента e_1 для отримання елемента $c_1 = c'_1 - e_1$, то відношення $c_1 / c'_2 \in [a, b]$ істинне. Якщо ж використовуємо помилковий елемент e_2 для отримання елемента $c_2 = c'_2 - e_2$, тобто маємо відношення c'_1 / c_2 , яке не дає можливості отримати кодове слово $\bar{C}$, що відповідає надісланому повідомленню. У цій ситуації єдиним рішенням є використання перевірного елемента $\det \bar{M}$ і порівняння їхніх визначників за тотожністю (8).

Отже, показана можливість виправлення двох помилок у різних рядках кодового слова, для чого введено такі поняття, як хибне повідомлення, матриця помилок, а також хибне та істинне відношення елементів кодового слова. Встановлено, що за умови наявності таких хибних відношень, то матимемо в кодовому слові дві помилки, для виправлення яких потрібно розв'язати відповідні діофантові рівняння. Розв'язки рівнянь потрібно підбирати так, щоб задовольнити певні умови виправлення помилок.

2.3. Можливість виправлення двох помилок в одному рядку. Випадок, коли в одному рядку хибної матриці $\bar{C}'$ трапляються два помилкові елементи, є дещо складнішим для їх виявлення та виправлення, ніж у різних рядках хибної матриці. Вважатимемо, що помилки знаходяться в елементах c'_1 і c'_2 , тобто помилкові елементи $\{e_1, e_2\} \neq 0$ і правильні $\{e_3, e_4\} = 0$. За цієї ситуації О. Стахов у роботі [28] пропонує розв'язувати діофантове рівняння (11) і перевіряти приналежність відношення елементів кодового слова фіксованому інтервалу $[a, b]$. Однак, як було з'ясовано згодом у роботі [5], цього недостатньо для виправлення таких помилок. Пояснимо це на конкретному прикладі.

Нехай $k \in \mathbb{N}$. Розглянемо дві матриці повідомлень $\bar{M}$ і $\bar{M}'$, які мають такий вигляд:

$$\bar{M} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \text{ і } \bar{M}' = \begin{bmatrix} m'_1 & m'_2 \\ m_3 & m_4 \end{bmatrix} = \begin{bmatrix} m_1 + k m_3 & m_2 + k m_4 \\ m_3 & m_4 \end{bmatrix}, \quad (17)$$

а їхні елементи є натуральними числами, що не дорівнюють нулю. Матриці закодованих повідомлень (отримане кодове слово і хибне повідомлення) відповідно мають такий вигляд:

$$\bar{C} = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \text{ і } \bar{C}' = \begin{pmatrix} c'_1 & c'_2 \\ c'_3 & c'_4 \end{pmatrix} = \begin{pmatrix} c_1 + k c_3 & c_2 + k c_4 \\ c_3 & c_4 \end{pmatrix}. \quad (18)$$

Оскільки перевірочні елементи будуть однаковими, тобто $\det(\bar{M}) = \det(\bar{M}')$, то для виправлення помилок, які є в першому рядку, потрібно розв'язати діофантове рівняння (11) для обох матриць $\bar{C}$ і $\bar{C}'$. Їхні розв'язки будуть мати два різних рішення (c_1, c_2) і $(c_1 + k c_3, c_2 + k c_4)$, які задовольнятимуть перевірочні співвідношення 1)–4) та умову приналежності фіксованому інтервалу $[a, b]$. Це означає, коли отримаємо матриці (18), то не зможемо виправити помилки, оскільки матимемо більше ніж одну можливу пару помилкових елементів.

Щоб уникнути цієї ситуації, потрібно обмежити набір блоків можливих повідомлень. Для цього вважатимемо, що повідомлення $\bar{M}$ – матриця розміром 2×2 вигляду (5), в якій $m_1 \geq m_3$ і $m_2 \leq m_4$ або навпаки – $m_1 \leq m_3$ і $m_2 \geq m_4$. Таку матрицю називають *мінімальною* [5]. Це означає, що не існує такого натурального числа k , щоб $m_1 = a + k m_3$ і $m_2 = b + k m_4$, де $a, b \in \mathbb{N}$ (або $m_3 = a + k m_1$ і $m_4 = b + k m_2$). Тому набір блоків вхідного повідомлення має містити тільки мінімальні матриці. В такий спосіб можна виправляти дві помилки в одному рядку, оскільки братимемо найменші розв'язки діофантового рівняння, придатність яких виявляємо перевірочними співвідношеннями 1)–4).

Для розуміння зазначеного розглянемо повідомлення (17), де матриця $\bar{M}$ є мінімальною, а очікуване кодове слово $\bar{C}$ є хибною матрицею $\bar{C}'$, яка містить помилкові елементи в першому рядку (18). Для їх виправлення розв'язуємо діофантове рівняння (11), внаслідок чого знаходимо два розв'язки (x_1, y_1) і (x_2, y_2) , які відповідають таким виразами:

$$\begin{cases} x_1 = F_{n+1} m_1 + F_n m_2 = -\det \bar{M} x_0 + t_1 c_3; \\ y_1 = F_n m_1 + F_{n-1} m_2 = -\det \bar{M} y_0 + t_1 c_4, \end{cases} \quad \text{і} \quad \begin{cases} x_2 = -\det \bar{M} x_0 + t_2 c_3; \\ y_2 = -\det \bar{M} y_0 + t_2 c_4. \end{cases}$$

У цих виразах $t_1, t_2 \in \mathbb{Z}$, а для знаходження x_0, y_0 розв'язуємо таке рівняння $c_4 x_0 - c_3 y_0 = 1$. Оскільки

$$\begin{cases} x_2 = F_{n+1} m_1 + F_n m_2 + k(F_{n+1} m_3 + F_n m_4) = x_1 + k c_3 = \\ = -\det \bar{M} x_0 + (k + t_1) c_3; \\ y_2 = F_n m_1 + F_{n-1} m_2 + k(F_n m_3 + F_{n-1} m_4) = y_1 + k c_4 = \\ = -\det \bar{M} y_0 + (k + t_1) c_4, \end{cases}$$

і $t_2 > t_1$, то щоб знайти розв'язок (x_1, y_1) , тобто виправити помилкові елементи і отримати кодове слово $\bar{C}$, достатньо взяти найменший розв'язок діофантового рівняння (11) та перевірити виконання перевірочних співвідношень 1)–4).

Отже, показана можливість виправлення двох помилок в одному рядку кодового слова, що є набагато складнішим випадком їх виправлення, ніж у різних рядках матриці. Встановлено, що за цієї ситуації потрібно розв'язувати діофантове рівняння та перевірити приналежність фіксованому інтервалу відношень відповідних його елементів. Однак, цього недостатньо для виправлення таких помилок. Тому було введено умову, згідно з якою набір блоків вхідного повідомлення має містити

тільки мінімальні матриці. В такий спосіб можна виправляти дві помилки в одному рядку хибної матриці, оскільки потрібно брати найменші розв'язки діофантового рівняння, придатність яких виявляють перевірочними співвідношеннями.

2.4. Можливість виправлення трьох помилок. Розглянемо випадок з появою трьох помилок. Припустимо, отримали таку хибну матрицю:

$$\bar{C}' = \begin{pmatrix} c'_1 & c'_2 \\ c'_3 & c'_4 \end{pmatrix}, \quad (19)$$

в якій є помилки, наприклад, в елементах c'_2, c'_3 і c'_4 , тобто помилкові елементи $\{e_2, e_3, e_4\} \neq 0$, а правильний $e_1 = 0$. Тому будь-яке з відношень $\{c_1 / c'_2, c'_3 / c'_4\} \notin [a, b]$ хибне. У цій ситуації О. Стахов у роботі [28] пропонує розв'язувати нелінійне діофантове рівняння $z c_1 - x y = (-1)^n \det \bar{M}$ і виправляти похибки за допомогою розв'язків, що належать фіксованому інтервалу $[a, b]$. Однак, як виявилось згодом [5], розв'язати це нелінійне діофантове рівняння надзвичайно важко. Насамперед це пов'язано з рівняннями (16), коли z фіксоване, і процедура розв'язування такого рівняння еквівалентно розкладанню цілого числа на множники, що практично неможливо для великих цілих чисел.

Автори в роботі [5] пропонують підхід, який зводиться до проб і помилок. Згідно з цим підходом спочатку потрібно знайти точне місце розташування цих помилкових елементів у однакових чи різних рядках матриці, а вже потім спробувати їх виправляти. Тобто, коли знаємо, де є помилки, то діємо в такий спосіб:

- 1) Розглядаємо рядок, який містить тільки один помилковий елемент. Виправляємо його за допомогою методу, описаного в п. 2.2.
- 2) Розглядаємо другий рядок і виправляємо в ньому помилковий елемент за допомогою розв'язку діофантового рівняння, як це показано в п. 2.3.

Для розуміння зазначеного, припустимо, що отримано хибну матрицю (19) при істинному відношенні $c_1 / c'_2 > b$. Як і в п. 2.2, потрібно обчислити значення елемента $e_2 = \lceil c'_2 - c_1 / b \rceil$ і відновити елемент $c_2 = c'_2 - e_2$. Тепер у матриці (19) замінюємо елемент c'_2 на c_2 , отримуючи при цьому дещо уточнену матрицю $\bar{C}' = \begin{pmatrix} c_1 & c_2 \\ c'_3 & c'_4 \end{pmatrix}$.

Щоб виправити в ній ще два елементи, потрібно розв'язати діофантове рівняння (12) і вибрати найменший позитивний розв'язок (x_0, y_0) , який перевіряємо на дотримання умови за допомогою перевірочного співвідношення 1)–4) та приналежності відношень фіксованому інтервалу.

Однак, зазвичай наперед не знаємо, де знаходяться помилкові елементи в хибному повідомленні $\bar{C}'$, а це означає, що не знаємо рядок, який містить тільки одну помилку. Щоб знайти позиції елементів без помилок, потрібно послідовно брати кожен елемент хибної матриці $\bar{C}'$ і намагатися декодувати його, як це було описано в п. 2.1, і здійснити перевірку дотримання умови за допомогою перевірочного співвідношення 1)–4) після першого кроку декодування даних. Спробуємо дещо детальніше продемонструвати можливі випадки виконання таких дій на прикладі, наведеному на початку п. 2.1.

Випадок 1. Неправильний рядок. Трапляється тоді, коли пробуємо виправляти рядок, який містить два по-

милкові елементи. Нехай отримали матрицю $\bar{C}'$ вигляду (19), і припускаємо, що єдиним правильним елементом у цій матриці є елемент c'_4 . Отже, спробуємо виправити другий рядок, знайшовши помилку елемента e_3 . Потім обчислюємо елементи $\bar{c}'_3$ і c'_4 та перевіряємо, чи відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне.

- 1) Якщо відношення $\bar{c}'_3 / c'_4 \notin [a, b]$ хибне, то розуміємо, що зробили помилку, і тому виконуємо процедуру заново, змінюючи початкові припущення. Наприклад, припускаємо, що єдиним правильним елементом у хибній матриці $\bar{C}'$ є елемент c'_3 , і знову починаємо процедуру пошуку та виправлення помилок.
- 2) Якщо відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне, то не розуміємо, що робимо помилку, і тому припускаємо, що це рішення $(\bar{c}'_3, c'_4)$ є правильним, і продовжуємо виправлення двох інших елементів c'_1 і c'_2 , розв'язуючи відповідне діофантове рівняння (11), внаслідок чого знаходимо елементи c'_1 і $\bar{c}'_2$. Тепер, щоб виявити відсутність помилок, потрібно перевірити, чи відношення $c'_1 / \bar{c}'_2 \in [a, b]$ істинне. Якщо ж відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне, то відношення $x_1 / y_1 \notin [a, b]$ хибне (див. лему 5).

Тепер розглянемо докладніше, як виконують процедуру декодування даних. Нехай отримали хибну матрицю $\bar{C}'$ вигляду (19), в якій єдиним правильним елементом є c'_4 . Спочатку розглянемо випадок істинного відношення $c'_3 / c'_4 > b$, для чого обчислюємо значення елемента

$$e'_3 = \lceil c'_3 - c'_4 \cdot b \rceil = e_3 + \left\lceil -\frac{m_3}{F_{n-1}} - e_4 \cdot b \right\rceil = e_3 + h, \quad (20)$$

де $h \in \mathbb{Z}$ і $\bar{c}'_3 = c'_3 - e'_3 = c_3 - h$. Щоб перевірити, чи відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне, скористаємося твердженням 3 і, задаючись значенням h , для елемента e_4 перевіримо виконання такої нерівності:

$$\frac{-hF_{n-1} - m_3}{F_n} < e_4 < \frac{-hF_n + m_4}{F_{n+1}}. \quad (21)$$

Лема 1. Нехай отримали хибну матрицю, елементи якої мають такий вигляд:

$$\bar{C}' = \begin{bmatrix} \bar{c}'_1 & \bar{c}'_2 \\ \bar{c}'_3 & c'_4 \end{bmatrix}. \quad (22)$$

Якщо обчислимо елементи $\bar{c}'_3$ і c'_4 , то відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне тоді, коли

$$m_3 + e_4 F_n = \begin{cases} qF_{n-1} + r, & \text{якщо } r \leq F_{n-1}, & e_4 > 0; \\ qF_{n-1} - r, & \text{якщо } r \leq F_{n-1} \wedge F_n^2 + 1 < \\ < F_{n+1}(m_3 + r) + F_n m_4, & e_4 < 0. \end{cases}$$

Доведення. Нехай $m \in \mathbb{Z}$ і $n \in \mathbb{N}$, тоді функція стелі $\lceil m/n \rceil$ має такий вигляд:

$$\bullet \text{ якщо } m < 0, \text{ то } \left\lceil \frac{m}{n} \right\rceil = \begin{cases} 0, & \text{якщо } m < n; \\ q, & \text{якщо } m = qn; \\ q, & \text{якщо } m = qn + r, r < n; \end{cases}$$

$$\bullet \text{ якщо } m > 0, \text{ то } \left\lceil \frac{m}{n} \right\rceil = \begin{cases} 1, & \text{якщо } m < n; \\ q, & \text{якщо } m = qn; \\ q+1, & \text{якщо } m = qn + r, r < n. \end{cases}$$

Нехай маємо такі елементи $\bar{c}'_3 = c_3 - h$ і $c'_4 = c_4 + e_4$, де $h = \left\lceil -\frac{m_3 + e_4 F_n}{F_{n-1}} \right\rceil$. Розглянемо два різні випадки:

1) значення $e_4 > 0$. У цьому випадку чисельник функції стелі завжди від'ємний, оскільки $m_3 > F_{n-1}$. Отже, тут розглянемо три різні ситуації:

- a) якщо $m_3 + e_4 F_n < F_{n-1}$, то це неможливо.
- b) якщо $m_3 + e_4 F_n = qF_{n-1}$, то $h = -q$. Згідно з твердженням 3, маємо, що відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне тоді, коли нерівність (21) виконується, тобто виконується така нерівність: $(qF_{n-1} - m_3) / F_n < e_4$. Але в нашому випадку $e_4 = qF_{n-1} - m_3 F_n$, тому відношення $\bar{c}'_3 / c'_4 \notin [a, b]$ хибне.
- c) якщо $m_3 + e_4 F_n = qF_{n-1} + r$, де r — ціле число, якщо $r < F_{n-1}$, то $h = -q$. Розглянемо нерівність (21) і рівність $e_4 = (qF_{n-1} + r - m_3) / F_n$. Оскільки $\{m_3, m_4\} < F_{n-1}$, то, з одного боку, маємо нерівність

$$\frac{qF_{n-1} - m_3}{F_n} < e_4 = \frac{qF_n + r - m_4}{F_n} \Leftrightarrow m_4 < q(F_n + F_{n-1}) + 2F_{n-1}$$

— це завжди істина. З іншого боку, маємо таку нерівність:

$$e_4 = \frac{qF_n + r - m_4}{F_n} < \frac{qF_n + m_4}{F_{n+1}} \Leftrightarrow rF_{n+1} < q + F_{n+1}F_{n+2}$$

— це також завжди істина, оскільки $r < F_{n-1}$. Отже, за твердженням 3 маємо, що відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне.

2) значення $e_4 < 0$. У цьому випадку чисельник функції стелі завжди додатний, оскільки $m_3 < F_{n-1}$. Отже, тут розглянемо три різні ситуації:

- a) якщо $|e_4|F_n - m_3 < F_{n-1}$, то $e_4 = -1 \wedge h = 1$. Нескладно перевірити, якщо відношення $c_3 / c_4 \in [a, b]$ істинне, то відношення $\bar{c}'_3 / c'_4 = (c_3 - 1) / (c_4 - 1) \notin [a, b]$ хибне.
- b) якщо $|e_4|F_n - m_3 = qF_{n-1}$, то $h = q$. Відношення $\bar{c}'_3 / c'_4 < b$ істинне тоді, коли виконується така нерівність: $F_{n-1}(F_{n+1}m_3 + F_n m_4 - q) < F_n(F_n m_3 + F_{n-1}m_4 - |e_4|)$, тобто нерівність $(qF_{n-1} + m_3)(1 - F_n) > 0$ істинна, що неможливо. Отже, відношення $\bar{c}'_3 / c'_4 \notin [a, b]$ хибне.

- c) якщо $|e_4|F_n - m_3 = qF_{n-1} + r$, де r — ціле число, якщо $r < F_{n-1}$, то $h = q + 1$. Розглянемо нерівність (21) і рівність $-|e_4| = (-qF_{n-1} - r - m_3) / F_n$. Оскільки $\{m_3, m_4\} < F_{n-1}$, то, з одного боку, маємо нерівність

$$\frac{-(q+1)F_{n-1} - m_3}{F_n} < -|e_4| = \frac{-qF_{n-1} - r - m_3}{F_n} \Leftrightarrow r < F_{n-1}$$

— це завжди істина. З іншого боку, враховуючи $|e_4|F_n = qF_{n-1} + r + m_3$, маємо таку нерівність:

$$-|e_4| < \frac{-(q+1)F_n + m_4}{F_{n+1}} \Leftrightarrow F_n(F_{n+1}|e_4| + m_4) > (q+1)F_n^2 \Leftrightarrow \Leftrightarrow F_{n+1}(m_3 + r) + F_n m_4 > F_n^2 + 1,$$

внаслідок чого отримаємо, що відношення $\bar{c}'_3 / c'_4 \in [a, b]$ істинне.

Припустимо, перебуваємо в ситуації леми 1, тобто елемент e_4 належить цьому діапазону. Тож припускаємо, що належно виправляємо помилкові елементи і переходимо до наступного кроку, обчислюючи інші два елементи c'_1 і c'_2 шляхом розв'язання діофантового рівняння (11). Його розв'язки є правильними, якщо виконуються такі тотожності:

$$\begin{cases} x_1 = -\det \bar{M} x_0 + t\bar{c}'_3; \\ y_1 = -\det \bar{M} y_0 + tc'_4, \end{cases} \quad (23)$$

де $t \in \mathbb{Z}$, а для знаходження x_0, y_0 розв'язуємо таке рівняння $c'_4 x_0 - \bar{c}'_3 y_0 = 1$.

Лема 2. Нехай отримали хибну матрицю (22). Обчислюємо елементи $\bar{c}'_3$ і c'_4 , де припускаємо, що відно-

шення $\bar{c}_3'/c'_4 \in [a, b]$ істинне. Тоді знаходимо розв'язок (x_1, y_1) як результат розв'язання діофантового рівняння (11). Тому, якщо відношення $\bar{c}_3'/c'_4 \in [a, b]$ істинне, то відношення $x_1/y_1 \notin [a, b]$ хибне.

Доведення. Оскільки відношення $\bar{c}_3'/c'_4 \in [a, b]$ істинне, то за лемою 1 маємо два випадки:

- 1) якщо $e_4 > 0$, то має виконуватися така рівність: $e_4 F_n = q F_{n-1} + r - m_3$, де $r < F_{n-1} \wedge h = -q$. Оскільки (x_1, y_1) є розв'язком діофантового рівняння (11), то маємо таке відношення:

$$\frac{x_1}{y_1} = \frac{y_1(\bar{c}_3' + q) - \det \bar{M}}{y_1(c'_4 + e_4)}.$$

Якщо відношення $x_1/y_1 \notin [a, b]$ хибне, то маємо дві різні ситуації:

- a) відношення $x_1/y_1 > a$ істинне тоді, коли перевірочний елемент $\det \bar{M} < 0$. Фактично, має виконуватися така нерівність:

$$\frac{x_1}{y_1} > \frac{F_{n+1}}{F_n} \Leftrightarrow F_n y_1(\bar{c}_3' + q) - F_n \det \bar{M} > F_{n+1} y_1(c'_4 + e_4).$$

Оскільки значення e_4 перевіряє нерівність (21), то, з одного боку, маємо таку нерівність

$$F_{n+1} y_1(c'_4 + e_4) < F_{n+1} y_1 c'_4 + F_n y_1 q + y_1 m_4,$$

але, з іншого —, коли перевірочний елемент $\det \bar{M} > 0$, то маємо таку нерівність:

$$F_n y_1(\bar{c}_3' + q) - F_n \det \bar{M} > F_{n+1} y_1 c'_4 + F_n y_1 q + y_1 m_4,$$

тобто

$$F_n y_1(F_{n+1} m_3 + F_n m_4) - F_n \det \bar{M} > F_{n+1} y_1(F_n m_3 + F_{n-1} m_4) + y_1 m_4,$$

отже, $F_n \det \bar{M} > 0$. Це означає, що відношення $x_1/y_1 \notin [a, b]$ хибне тоді, коли перевірочний елемент $\det \bar{M} > 0$.

- b) відношення $x_1/y_1 < b$ істинне тоді, коли перевірочний елемент $\det \bar{M} > 0$. Фактично, має виконуватися така нерівність:

$$\frac{x_1}{y_1} < \frac{F_n}{F_{n+1}} \Leftrightarrow F_{n-1} y_1(\bar{c}_3' + q) - F_{n-1} \det \bar{M} < F_n y_1(c'_4 + e_4).$$

Оскільки значення e_4 перевіряє нерівність (21), то, з одного боку, маємо таку нерівність:

$$F_n y_1(c'_4 + e_4) > F_n y_1 c'_4 + F_{n+1} y_1 q - y_1 m_3,$$

але, з іншого —, коли перевірочний елемент $\det \bar{M} > 0$, то маємо таку нерівність:

$$F_n y_1 c'_4 + F_{n-1} y_1 q - y_1 m_3 > F_{n-1} y_1(\bar{c}_3' + q) - F_{n-1} \det \bar{M},$$

тобто

$$F_n y_1(F_n m_3 + F_{n-1} m_4) > F_{n-1} y_1(F_{n+1} m_3 + F_n m_4) - F_{n-1} \det \bar{M},$$

отже, $F_{n-1} \det \bar{M} > 0$. Це означає, що відношення $x_1/y_1 \notin [a, b]$ хибне тоді, коли перевірочний елемент $\det \bar{M} < 0$.

Аналогічно можна довести такий випадок.

- 2) якщо $e_4 < 0$, то має виконуватися така рівність: $|e_4| F_n = q F_{n-1} + r + m_3$, де $r < F_{n-1} \wedge F_n^2 + 1 < F_{n+1}(m_3 + r) + F_n m_4 \wedge h = q + 1$. Оскільки (x_1, y_1) є розв'язком діофантового рівняння (11), то маємо таке відношення:

$$\frac{x_1}{y_1} = \frac{y_1(\bar{c}_3' - (q + 1)) - \det \bar{M}}{y_1(c'_4 - |e_4|)}.$$

Якщо відношення $x_1/y_1 \notin [a, b]$ хибне, то маємо дві різні ситуації:

- a) відношення $x_1/y_1 > a$ істинне тоді, коли перевірочний елемент $\det \bar{M} < 0$. Фактично, має виконуватися така нерівність:

$$\frac{x_1}{y_1} > \frac{F_{n+1}}{F_n} \Leftrightarrow F_n y_1(\bar{c}_3' - (q + 1)) - F_n \det \bar{M} > F_{n+1} y_1(c'_4 - |e_4|).$$

Оскільки значення e_4 перевіряє нерівність (21), то, з одного боку, маємо таку нерівність:

$$F_{n+1} y_1(|e_4| - c'_4) > (q + 1) F_n y_1 - F_{n+1} y_1 c'_4 + y_1 m_4,$$

але, з іншого —, коли перевірочний елемент $\det \bar{M} < 0$, то маємо таку нерівність:

$$(q + 1) F_n y_1 - F_{n+1} y_1 c'_4 + y_1 m_4 > F_n y_1(\bar{c}_3' - (q + 1)) - F_n \det \bar{M},$$

тобто

$$y_1 m_4 - F_{n+1} y_1(F_n m_3 + F_{n-1} m_4) > F_{n+1} y_1(F_{n+1} m_3 + F_n m_4) - F_n \det \bar{M},$$

отже, $F_n \det \bar{M} < 0$. Це означає, що відношення $x_1/y_1 \notin [a, b]$ хибне тоді, коли перевірочний елемент $\det \bar{M} > 0$.

- b) відношення $x_1/y_1 < b$ істинне тоді, коли перевірочний елемент $\det \bar{M} > 0$. Фактично, має виконуватися така нерівність:

$$\frac{x_1}{y_1} < \frac{F_n}{F_{n+1}} \Leftrightarrow F_{n-1} y_1(\bar{c}_3' - (q + 1)) - F_{n-1} \det \bar{M} < F_n y_1(c'_4 - |e_4|).$$

Оскільки значення e_4 перевіряє нерівність (21), то, з одного боку, маємо таку нерівність:

$$F_n y_1(|e_4| - c'_4) < (q + 1) F_{n-1} y_1 - F_n y_1 c'_4 + y_1 m_3,$$

але, з іншого —, коли перевірочний елемент $\det \bar{M} > 0$, то маємо таку нерівність:

$$(q + 1) F_{n-1} y_1 - F_n y_1 c'_4 + y_1 m_3 < F_{n-1} y_1((q + 1) - \bar{c}_3') + F_{n-1} \det \bar{M},$$

тобто

$$y_1 m_3 - F_n y_1(F_n m_3 + F_{n-1} m_4) < -F_{n-1} y_1(F_{n+1} m_3 + F_n m_4) + F_{n-1} \det \bar{M},$$

отже, $F_n \det \bar{M} > 0$. Це означає, що відношення $x_1/y_1 \notin [a, b]$ хибне тоді, коли перевірочний елемент $\det \bar{M} < 0$.

Випадок 2. Правильний рядок, неправильний елемент. Цей випадок схожий на попередній. Припустимо, отримано хибну матрицю, елементи якої мають такий вигляд:

$$\bar{C}' = \begin{bmatrix} c'_1 & c'_2 \\ c'_3 & c'_4 \end{bmatrix}. \quad (24)$$

Починаємо виправляти перший рядок, намагаючись знайти помилку елемента e_1 . Припустимо, відношення $c_1/c'_2 > b$ істинне, тож обчислюємо значення

$$e'_1 = \lceil c_1 - c'_2 \cdot b \rceil = \left\lceil -\frac{m_1}{F_{n-1}} - e_2 \cdot b \right\rceil = h,$$

де $h \in \mathbb{Z}$, і $c'_1 = c_1 - e'_1 = c_1 - h$. Тут маємо аналогічний результат, як і у випадку 1, тому можемо продовжувати виконувати дії так, як і раніше.

Отже, показана можливість виправлення трьох помилок у кодовому слові. Встановлено, що за цієї ситуації потрібно перевіряти приналежність відношень елементів кодового слова фіксованому інтервалу, для виправлення яких потрібно розв'язати нелінійне діофантове рівняння. Однак, розв'язати його надзвичайно складно, позаяк процедура розв'язання еквівалентна розкладанню цілого числа на множники, що проблемно для великих цілих чисел. Тому запропоновано підхід, який зводиться до проб і помилок, згідно з яким спочатку потрібно знайти точне місце розташування цих помилок.

вих елементів у однакових чи різних рядках матриці, а вже потім спробувати їх виправляти за відповідними методиками.

Обговорення результатів дослідження. Проаналізовано можливість виявлення та виправлення помилок у закодованому повідомленні матрицями Фібоначчі [12, 13, 15], а також способи вдосконалення етапу виявлення помилок, який дає змогу уникнути зайвої перевірки всіх гіпотез щодо появи подвійних помилок. Наведено деякі твердження та їхні доведення, на яких базуються методики виявлення та виправлення однієї, двох і трьох помилок у рядках кодового слова. Однак, практично аналогічні дослідження в цій галузі знань здійснювали й інші науковці, тому обговоримо деякі їхні результати дещо детальніше.

У роботі [5] автори деталізували особливості виявлення та виправлення подвійних помилкових елементів у матрицях кодування розміром 2×2 , введених О. Стаховим, тобто кодах виправлення помилок 1-Фібоначчі. Подібний аналіз проведено для матриць кодування $p \times p$ і для більшої кількості помилок. Через особливий тип помилок, які можна виправляти, коди 1-Фібоначчі важко зрозуміти, насамперед у якому реальному випадку їх можна застосувати як інструмент виправлення помилок. З іншого боку, компактне подання матриці кодування може бути корисним для створення однобічних функцій для криптографії [10, 11, 14], де часто стандартні коди пропонують надзвичайно великі ключі [12].

Як зазначено в роботах [4, 21], так звані p -числа Фібоначчі також можна узагальнити, враховуючи деякі лінійні рекурентні послідовності (1) і (2), такі як p -числа Лукаса [17, 22] або Пелля-Лукаса [30], які дещо узагальнюють p -числа Фібоначчі та методи (де)кодування з їхнім використанням. Наприклад, автор роботи [20] запропонував використовувати рекурентні послідовності $F_n^{(p)}(x, y)$, застосовуючи поліноми Фібоначчі [27]. Подальші узагальнення результатів вирішення цієї проблеми можна знайти в роботах [1, 2, 8, 19].

У роботі [24] наведено результати побудови дуально-узагальнених комплексних кватерніонів Фібоначчі та Лукаса. Авторі розглядали властивості як дуального узагальненого комплексного числа, так і кватерніона. Окрім цього, було отримано загальні рекурентні співвідношення для відповідних послідовностей кватерніонів, формули Біне, тотожності Тагіурі (або Вайди), Гонсбергера, д'Оканя, Кассіні та Каталана. Наведено набір матричних подань цих спеціальних кватерніонів і виражено добуток дуально-узагальнених комплексних кватерніонів Фібоначчі і Лукаса у вигляді їхніх різних матричних подань.

У роботі [17] наведено особливості формування p -матриці Лукаса, попередньо вивчаючи p -числа Фібоначчі та Лукаса. Було введено p -матрицю Лукаса та супутні матриці для сум p -чисел Фібоначчі та Лукаса, щоб отримати деякі їхні цікаві тотожності. Водночас, у роботі [22] наведено узагальнену теорію кодування даних з використанням p -чисел Лукаса. Якщо в роботі [17] тільки наведено p -матрицю Лукаса $R_p Q_p^n$, елементами якої є p -числа Лукаса, то в цій роботі розроблено новий метод (де)кодування даних на підставі p -матриці Лукаса $R_p Q_p^n$. Також автори встановили зв'язки між елементами матриці кодування даних, з'ясували особливості виявлення та виправлення помилок у закодованих пові-

домленнях. Під час обговорення результатів свого дослідження автори стверджують, що коригувальна здатність їхнього методу для $p=1$ становить 93,33 %, а для $p=2$ – 99,80 % і зростає зі збільшенням цього значення.

У роботі [30] наведено узагальнену теорію кодування даних на підставі p -чисел Пелля-Лукаса $S_p A^n$ та відповідний метод їх (де)кодування. Вони встановили співвідношення між елементами матриці кодування для $p=1$ та $i=1$, які дають змогу виявляти та виправляти помилки в закодованих повідомленнях. Під час обговорення результатів свого дослідження автори стверджують, що коригувальна здатність цього методу становить 93,33% для $p=1$, $i=1$, а для $p=2$, $i=2$ – 99,80 % і зростає зі збільшенням цього значення.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – вперше проаналізовано можливість виявлення та виправлення помилок у закодованому повідомленні матрицями Фібоначчі, наведено способи удосконалення етапу виявлення помилок, що дає змогу уникнути зайвої перевірки всіх гіпотез щодо появи подвійних помилок як у різних, так і в однакових рядках кодового слова.

Практична значущість результатів дослідження – розроблені методики виявлення помилок у закодованих повідомленнях матрицями Фібоначчі та уточнені методи їх виправлення можна застосувати у криптографічних системах для передачі каналами зв'язку відповідних блоків кодових слів різної величини з достатньою коригувальною здатністю.

Висновок / Conclusions

Проаналізовано основні проблеми виявлення та наявні методики виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, що дають можливість знаходити і виправляти одну, дві та три помилки в однакових чи різних рядках кодового слова. За результатами виконаного дослідження можна зробити такі основні висновки.

1. Внаслідок проведеного аналізу наявних досліджень та публікацій з'ясовано, що навіть за останнє десятиліття надруковано значну кількість різноманітних публікацій, в яких обґрунтовано доцільність використання матриць Фібоначчі для (де)кодування даних. Проте, більшість з них стосується відповідних матриць розміром 2×2 і, як наслідок, закодованих блоків повідомлень аналогічного розміру, що в практиці передачі даних трапляється вкрай рідко.

2. За результатами аналізу традиційного методу (де)кодування даних матрицями Фібоначчі було встановлено, що елементи кодових слів мають багато корисних і цікавих властивостей, на яких якраз і ґрунтується методика виявлення та виправлення у них помилок. Наведено відповідне твердження, згідно з яким відношення певних елементів кодового слова наближене до золотого перерізу, має важливе значення для наявних методик виправлення потенційних помилок.

3. Показано можливість удосконалення етапу виявлення помилок, який дає змогу уникнути зайвої перевірки всіх гіпотез щодо появи як подвійних, так і потрійних помилок. Встановлено, що набагато зручніше використовувати деякі властивості елементів кодового слова, які можуть ідентифікувати наявні ситуації при-

сутності таких помилкових елементів шляхом перевірки приналежності відношень відповідних елементів фіксованому інтервалу.

4. З'ясовано, що хибна приналежність фіксованому інтервалу відношень відповідних елементів кодового слова свідчить про те, що в різних його рядках присутні дві помилки, для виправлення яких потрібно розв'язати відповідні діофантові рівняння, розв'язки якого підбирають так, щоб вони дали можливість задовольнити певні умови виправлення помилок.

5. Встановлено, що за наявності двох помилок в одному рядку кодового слова потрібно розв'язати діофантове рівняння та перевірити приналежність фіксованому інтервалу відношень відповідних його елементів. Для виправлення таких помилок введено умову, згідно з якою набір блоків вхідного повідомлення має містити тільки мінімальні матриці, щоб брати найменші розв'язки діофантового рівняння, придатність яких уточнюють перевірочними співвідношеннями.

6. Виявлено, що для виправлення трьох помилок у кодовому слові потрібно перевірити приналежність фіксованому інтервалу відношень відповідних його елементів та розв'язати нелінійне діофантове рівняння, реалізація якого є надзвичайно складною. Тому запропоновано підхід, який зводиться до проб і помилок, згідно з яким спочатку потрібно знайти точне місце розташування цих помилкових елементів у рядках матриці, а вже потім спробувати їх виправляти за відповідними методиками.

References

- Basu, M., & Prasad, B. (2011). Coding theory on the (m, t) -extension of the Fibonacci p -numbers. *Discrete Mathematics, Algorithms and Applications*. Vol. 3, 259–267. <https://doi.org/10.1142/S1793830911001097>
- Basu, Manjusri, & Das, Monojit. (2017). Coding theory on generalized Fibonacci n -step polynomials. *Journal of Information and Optimization Sciences*. Vol. 38, Issue 1, 83–131. <https://doi.org/10.1080/02522667.2016.1160618>
- Basu, Manjusri, & Prasad, Bandhu. (2009). The generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons, & Fractals*. Vol. 41, Issue 5(17), 2517–2525. <https://doi.org/10.1016/j.chaos.2008.09.030>
- Basu, Manjusri, & Prasad, Bandhu. (2009, November). Coding theory on the m -extension of the Fibonacci p -numbers. *Chaos, Solitons, & Fractals*. Vol. 42, Issue 4, 30, 2522–2530. <https://doi.org/10.1016/j.chaos.2009.03.197>
- Bellini, Emanuele, Marcolla, Chiara, & Murru, Nadir. (2020, March). On the decoding of 1-Fibonacci error correcting codes. *Discrete Mathematics, Algorithms and Applications*. Vol. 13, No. 05, 2150056. <https://doi.org/10.13140/RG.2.2.27280.97281>; <https://doi.org/10.1142/S1793830921500567>
- Esmaili, M., Esmaili, M., & Gulliver, T. A. (2011). High-rate Fibonacci polynomial codes. In: *Proceedings of IEEE International Symposium on Information Theory Proceedings*, St. Petersburg, Russia, pp. 1921–1924. <https://doi.org/10.1109/ISIT.2011.6033886>
- Esmaili, M., Moosavi, M., & Gulliver, T. A. (2017, January). A new class of Fibonacci sequence based error correcting codes. *Cryptography and Communications*. Vol. 9, 379–396. <https://doi.org/10.1007/s12095-015-0178-x>
- Esmaili, Mostafa, & Esmaili, Morteza. (2010). A Fibonacci-polynomial based coding method with error detection and correction. *Computers and Mathematics with Applications*, 60, 2738–2752. <https://doi.org/10.1016/j.camwa.2010.08.091>
- Gryciuk, Yuriy, Grytsyuk, Pavlo. (2015). Perfecting of the matrix Affine cryptosystem information security. *Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT2015)*, 14–17 September, 2015, pp. 67–69. <https://doi.org/10.1109/stc-csit.2015.7325433>
- Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2015). Peculiarities of the implementation of the matrix Athena cryptosystem of information protection. *Scientific Bulletin of UNFU*, 25(5), 346–356. URL: <https://nv.nltu.edu.ua/index.php/journal/article/view/1092>
- Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2015). Implementation of cryptographic transformations using Fibonacci $G(\lambda)$ -matrices. *Mathematical and software support of intelligent systems: materials of the 13th International Scientific and Practical Conference*, (pp. 53–54), November 18–20, 2015, Dnipropetrovsk, Ukraine. Dnipropetrovsk: Department of Dnipropetrovsk National University named after Olesya Honchara.
- Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2015). Methods and means of generating Fibonacci Q_p -matrices – keys for implementing cryptographic transformations. *Scientific Bulletin of UNFU*, 25(6), 334–351. URL: <https://nv.nltu.edu.ua/index.php/journal/article/view/974>
- Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci Q_p -matrices – keys for implementing cryptographic transformations. *Bulletin of the National University "Lviv Polytechnic". Series: Computer Science and Information Technology*. Vol. 843, 251–263.
- Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci $G_p(\lambda)$ -matrices for implementation of cryptographic transformations. *Information extraction and processing: inter-departmental collection of scientific papers*, 43(119), 86–95.
- Hrytsiuk, Yuriy, & Grytsyuk, Pavlo (2016). Generation of Fibonacci $Q_p(\lambda)$ -matrices – keys for data encryption. *Information protection and security of information systems: materials of the 5th International Scientific and Technical Conference*, (pp. 39–40), June 02–03, 2016, Lviv, Ukraine. Lviv: Lviv Polytechnic State University.
- Knuth, Donald. (1968). *The art of computer programming 1: Fundamental algorithms 2: Semi Numerical algorithms 3: Sorting and searching*. MA: Addison-Wesley 30.
- Kuhapatanakul, K. (2015). The Lucas p -matrix. *International Journal of Mathematical Education in Science and Technology*. <https://doi.org/10.1080/0020739X.2015.1026612>
- Kuzhel, O. V. (1997). Binets generalized formula and its application. In *the world of mathematics*. Kyiv: TViMS Publishing House. Vol. 3, Issue 3, pp. 52–59.
- Nihal Tas, Sumeyra Ucar, Nihal Yilmaz Ozgur, & Oztunc Kaymak. (2018). A new coding/decoding algorithm using Fibonacci numbers. *Discrete Mathematics, Algorithms and Applications*. Vol. 10, No. 02, 1850028. <https://doi.org/10.1142/S1793830918500283>; <https://doi.org/10.48550/arXiv.1712.02262>
- Prasad, Bandhu. (2014). Coding theory on $(h(x), g(y))$ -extension of Fibonacci p -numbers polynomials. *Universal Journal of Computational Mathematics*. Vol. 2(1), 6–10. <https://doi.org/10.13189/ujcm.2014.020102>
- Prasad, Bandhu. (2014). High rates of Fibonacci polynomials coding theory. *Discrete Mathematics, Algorithms and Applications*. Vol. 06, No. 04, 1450053. <https://doi.org/10.1142/S1793830914500530>
- Prasad, Bandhu. (2016). Coding theory on Lucas p -numbers. *Discrete Mathematics, Algorithms and Applications*. Vol. 08, No. 04, 1650074. <https://doi.org/10.1142/S1793830916500749>
- Prasad, Bandhu. (2019). The generalized relations among the code elements for a new complex Fibonacci matrix. *Discrete Mathematics, Algorithms and Applications*. Vol. 11, No. 02, 1950026. <https://doi.org/10.1142/S1793830919500265>
- Sentürk, G. Y., Gürses, N., & Yüce, S. (2022). Construction of dual-generalized complex Fibonacci and Lucas quaternions. *Carpathian Mathematical Publications*, 14(2), 406–418. <https://doi.org/10.15330/cmp.14.2.406-418>
- Singh, Sweta, Kanwar, Neeraj, & Zindani, Divya. (2023, April). Linear diophantine uncertain linguistic-based prospect theory approach for performance evaluation of islanded microgrid-

- system scenarios. *Clean Energy*. Vol. 7, Issue 2, 263–282. <https://doi.org/10.1093/ce/zkac066>
26. Skuratovsky, R. V. (2017). Factorization of an integer of the form $n = pq$. *Mathematical and computer modeling. Series: Physical and mathematical sciences: collection of scientific papers*. Kamianets-Podilskyi National University. Issue 15, pp. 201–207. URI: <http://dspace.nbuv.gov.ua/handle/123456789/133957>
 27. Slyusarenko, V. (2008). Fibonacci numbers and the golden ratio. *Mathematics*. Kyiv: "School World" Publishing House, № 8(452), pp. 18–24.
 28. Stakhov, A. P. (2006, October). Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. *Chaos, Solitons, & Fractals*. Vol. 30, Issue 1, 56–66. <https://doi.org/10.1016/j.chaos.2005.12.054>
 29. Stakhov, Alexey, & Olsen, Scott. (2009). The Mathematics of Harmony: From Euclid to Contemporary Mathematics and Computer Science. *Series on Knots and Everything*, 22. World Scientific Publishing Company; First Edition, 748 p. URL: <https://www.amazon.com/Mathematics-Harmony-Contemporary-Computer-Everything/dp/981277582X>
 30. Sundarayya, P., & Prasad, M. G. Vara. (2019). Coding theory on Pell-Lucas p -numbers. *Journal of Physics: Conference Series*, 1344. <https://doi.org/10.1088/1742-6596/1344/1/012017>
 31. Yuriy Hrytsiuk, Pavlo Grytsyuk, Tetiana Dyak, Heorhiy Hrynyk. (2019). Software Development Risk Modeling. IEEE 2019 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2019), (Vol. 2, pp. 134–137), 17–20 September, Lviv, Ukraine. Lviv: Lviv Polytechnic National University, 206 p. <https://doi.org/10.1109/stc-csit.2019.8929778>
 32. Tony Rosqvist, Mika Koskela, & Hannu Harju. (2003, May). Software Quality Evaluation Based on Expert Judgement. *Software Quality Journal*. Vol. 11, Issue 1, 39–55. <https://doi.org/10.1023/A:1023741528816>

P. Yu. Grytsiuk, L. S. Sikora, Yu. I. Hrytsiuk

Lviv Polytechnic National University, Lviv, Ukraine

PROBLEMS OF DETECTING AND CORRECTING ERRORS IN MESSAGES ENCODED BY FIBONACCI MATRICES

The main problems of detection and available methods of correcting errors in encoded messages with Fibonacci matrices, which make it possible to find and correct one, two and three errors in the same or different lines of the code word, are analyzed. It has been found that even in the last decade, many scientists have published a significant number of various publications, each of which to one degree or another substantiates the expediency of using Fibonacci matrices for (de)coding data. It has been established that the elements of a codeword obtained by multiplying a message block by a Fibonacci matrix have many useful properties, which are the basis for the method for detecting and correcting errors in them. The statement is given, according to which the ratio of the corresponding elements of the code word is close to the golden ratio, which is important for the existing methods of correcting potential errors. This property of the elements makes it possible to identify the presence of double and triple false elements by checking whether their ratios belong to a fixed interval. It is found that the false affiliation indicates that there are two errors in different lines of the code-word, which require solving the corresponding Diophantine equations, the suitability of the solution of which must satisfy certain conditions for error correction. It was found that in order to correct two errors in one line of the code word, a condition was introduced according to which the set of blocks of the input message should contain only minimal matrices, which makes it possible to take the smallest solutions of the Diophantine equation, the suitability of which is specified by test ratios. It was found that in order to correct three errors in a codeword, it is necessary to check whether the relations of its corresponding elements belong to a fixed interval and to solve a nonlinear Diophantine equation, the implementation of which is extremely difficult. The proposed approach boils down to trial and error, according to which you first need to find the exact location of the erroneous elements, and only then correct them according to the appropriate methods.

Keywords: Fibonacci numbers; recurrent sequence; code word; golden ratio; Diophantine equation; error correction method.