Issue 14, 2023

https://doi.org/10.23939/sisn2023.14.327

УДК 004.(4+51+67):519.6

МЕТОДИ ВИПРАВЛЕННЯ ПОМИЛОК У ЗАКОДОВАНИХ ПОВІДОМЛЕННЯХ МАТРИЦЯМИ ФІБОНАЧЧІ

Павло Грицюк[1], Любомир Сікора[2], Юрій Грицюк[3]

[1, 2] Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління, вул. С. Бандери, 14, Львів, Україна
[3] Національний університет "Львівська політехніка",
кафедра програмного забезпечення, вул. С. Бандери, 14, Львів, Україна
E-mail: pavlo.y.hrytsiuk@lpnu.ua, ORCID: 0009-0003-5409-2043
E-mail: lybomyr.s.sikora@lpnu.ua, ORCID: 0000-0002-7446-1980
E-mail: yurii.i.hrytsiuk@lpnu.ua, ORCID: 0000-0001-8183-3466

Проаналізовано наявні методики виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, що дають можливість знаходити і виправляти декілька помилок у кодових словах, отриманих каналами зв'язку. З'ясовано, що за останнє десятиліття опубліковано багато різноманітних робіт, у кожній з яких обґрунтовано доцільність використання матриць Фібоначчі для (де)кодування даних. Встановлено, що елементи кодового слова, одержаного множенням блока повідомлення на матрицю Фібоначчі, мають чимало корисних властивостей, на яких ґрунтується методика виявлення та виправлення у ньому помилок. Дослідники стверджують, що відношення відповідних елементів кодового слова наближене до золотого перерізу, й це має важливе значення для відомих методик виправлення потенційних помилок. Така властивість кодового слова дає можливість ідентифікувати наявність подвійних і потрійних помилкових елементів, перевіривши, чи належать їхні відношення до фіксованого інтервалу. Хибна належність, як виявилось, свідчить про те, що в різних рядках кодового слова є дві помилки, для виправлення яких потрібно розв'язати відповідні діофантові рівняння. Розв'язки цих рівнянь повинні задовольнити певні умови виправлення помилок.

З'ясовано, що для виправлення двох помилок у одному рядку кодового слова ставлять 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 перевіряльними 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: 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

В інформаційних та комунікаційних технологіях важливе значення має так зване завадостійке кодування даних, для реалізації якого розроблено багато різних методів [18, 21]. Причина в тому, що під час передавання закодованих повідомлень каналами зв'язку через різні перешкоди в них

інколи виникають помилки чи навіть втрати даних [9]. Застосування сучасних методів кодування даних з виправленням помилок під час розроблення криптографічних систем [10, 11, 14], стійких до різних атак, спонукало багатьох науковців до творчих пошуків і сприяло появі нових досліджень. Проте у криптографії основний недолік кодування даних з виправленням помилок полягає у використанні ключів великої розмірності з недостатньою коригувальною здатністю [12, 13, 15]. Порівняно з іншими методами кодування даних, класична криптографія гарантує їх коригувальну здатністю тільки за умови, що використовують ефективні алгоритми кодування, а також дотримуються секретності та цілісності ключів кодування.

Наприклад, у роботах [9, 10] розглянуто особливості реалізації матричної афінної криптосистеми захисту інформації. Основну увагу зосереджено на розробленні надійної криптосистеми (де)шифрування даних, яка поєднує матричні афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом дає можливість значно підвищити стійкість криптосистеми до брутальних атак. Математично описано алгоритм шифрування даних за допомогою багатораундової матричної афінної перестановної криптосистеми з різними ключами шифрування на кожному раунді. Результати криптоаналізу запропонованого алгоритму показали, що він забезпечує достатню стійкість зашифрованих повідомлень до брутальних атак навіть за значний проміжок часу за достатньої продуктивності обчислювальної системи.

Постановка проблеми

У 2005 р. О. Стахов у роботі [32] 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 [28] для виправлення помилок у закодованих повідомленнях. Автор стверджував, що запропонований метод декодування даних здатний виправити 93,33 % помилок і що такі коди мають надмірність 33,3 %. Проте його обнадійливі заяви в багатьох дослідників [2, 3, 5, 22, 34] викликали деякі сумніви, насамперед з погляду теорії інформації. Вони вважали, що потрібен дещо глибший і точніший аналіз результатів дослідження О. Стахова як щодо надмірності його кодів, так і щодо можливості підходів до виявлення та виправлення помилок у закодованих повідомленнях, які він запропонував.

Наприклад, у роботі [5, розд. 5] пояснено, що деякі методології та висновки, які зробив О. Стахов, є оманливими та недостовірними. Практично важко придумати реальний канал передавання даних, у якому можна було б використати коди, що запропонував О. Стахов. Водночас науковці 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'язання потенційно складних діофантових рівнянь [28]. Також вони вказали, як обмежити простір вхідних повідомлень, щоб не було неоднозначності під час їх кодування та декодування, і надали явну формулу для визначення надмірності цих кодів.

Проте дослідження, виконане в роботі [5], як і в багатьох інших [3, 22, 34], стосується матриці Фібоначчі розміром 2×2 і, як наслідок, закодованих повідомлень із блоками аналогічного розміру, що в практиці передавання 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 – проаналізувати методи виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, що дають змогу ефективно передавати каналами зв'язку блоки даних різних розмірів.

Для досягнення цієї мети визначено такі основні *завдання дослідження*:

- проаналізувати останні дослідження та публікації, а також встановити основні ускладнення під час виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі;
- проаналізувати традиційні методи (де)кодування даних матрицями Фібоначчі, які мають багато корисних і цікавих властивостей, вибрати тільки ті із них, які можна було б використовувати у запропонованому методі кодування даних;
- проаналізувати різні можливості виявлення та виправлення помилок у закодованому повідомленні, навести концептуальні підходи, на яких ґрунтуються наявні методи виправлення декількох помилок у закодованих повідомленнях;
- 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 р. О. Стахов [32], сподіваючись на детальніший аналіз результатів майбутніх досліджень, висловив кілька цікавих ідей щодо використання чисел Фібоначчі для отримання оригінального коду з можливістю виправлення помилок і компактним його поданням. Метод (де)кодування даних p-числами Фібоначчі, який запропонував О. Стахов, він удосконалив у подальших дослідженнях. Наприклад, у роботі [33] вказано на деякі особливості p-коду Фібоначчі, надано певну оцінку його надмірності. Однак під час такого оцінювання дослідник не брав до уваги зростання величини блока повідомлення через збільшення розмірів матриць Фібоначчі, задіяних у методі кодування даних, а тільки розглядав передавання визначника цих матриць, які й використовували для декодування повідомлень.

О. Стахов у своїх дослідженнях здебільшого зосереджував увагу на випадку $p = 1$, що відповідає класичним числам Фібоначчі, тоді як у роботі [7] продемонстровано результати аналізу обчислювальної складності методу (де)кодування даних у загальному випадку і для наочності наведено деякі числові приклади. Цими прикладами автори показали, що в найгіршому випадку, хоча й можна виправляти помилки в закодованих повідомленнях, проте це потребує тривалого проміжку часу $Q(2^{p^2})$, наприклад, за $p = 3$, $2^{3^2} = 512$. Водночас науковці уточнили, що такий найгірший випадок не є серйозною проблемою для криптографічних систем [9, 14], оскільки практично ніколи не виникає, враховуючи сучасні характеристики каналів передавання даних, і визначили коефіцієнт виправлення помилок $(2^{p^2} - 1) / 2^{p^2}$ методу (де)кодування даних, який запропонували. Однак під час обговорення результатів дослідження автори навіть не згадують про процедуру розв'язування відповідних діофантових рівнянь [28], яка виконується на етапі виправлення помилок. Адже відомо [5, розд. 3], що ця процедура може бути досить тривалою, якщо не внести деякі коригування в початкові дані, щоб успішно потім виявляти та виправляти помилки у закодованих повідомленнях.

Аналогічно у роботі [3] автори наводять дещо уточнений коефіцієнт виправлення помилок $(2^{p^2} - 2) / (2^{p^2} - 1)$ і спеціально розглядають результати свого дослідження для $p = 2$. Також у цьому дослідженні вони взяли до уваги тільки матричні операції, задіяні на етапі виявлення помилок, без обговорення потреби використання 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 [28]. Також вони надають результати детального аналізування 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, оснований 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 [12, 13] розглянуто особливості ефективного генерування Q_p-матриць Фібоначчі, які можна використовувати як ключі (де)шифрування даних для багатораундової матричної криптосистеми їх перетворення. З'ясовано, що основна проблема багатораундової матричної афінної криптосистеми полягає в генеруванні множини звичайних і обернених матриць – ключів шифрування даних, елементами яких мають бути цілі числа. Розроблено процедуру, яка за відомими значеннями степеня матриці (n) та p-чисел Фібоначчі дає змогу генерувати відповідну множину ключів шифрування даних, здійснювати їхнє розширення для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й зручна у разі передавання каналами зв'язку.

У роботі [24] розглянуто доцільність використання апарату арифметики Фібоначчі у сфері криптографії. Продемонстровано перспективність цього напряму досліджень у межах удосконалення статистичних показників симетричних криптографічних перетворень даних. Сформульовано і доведено гіпотезу про гомоморфізм p-чисел і Q_p-матриць Фібоначчі, які розробив проф. О. Стахов, у кільці цілих чисел за модулем q, що дало змогу уникнути виникнення надмірності під час використання арифметики Фібоначчі у різних додатках. Проаналізовано доцільність використання множення на матрицю Фібоначчі у схемах обміну криптографічними шифрами, що істотно пришвидшило дифузійні процеси порівняно із звичайною схемою Фейстеля.

У роботі [25] розглянуто числа і матриці Стахова в кільці цілих чисел за модулем q. Доведено виконання основних властивостей Q_p^n-матриць у кільці цілих чисел за модулем q, що дає можливість уникнути значної надлишковості у разі використання їх у криптографічних методах шифрування даних.

У роботі [8] запропоновано 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 $Q_m^n(x)$-матрицею кодування даних, елементами якої є поліноми Фібоначчі. Для декодування даних автори вводять обернену $Q_m^{-n}(x)$-матрицю, особливість якої у тому, що її 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 доволі великих значень m. Наведено наочні приклади (де)кодування даних, а також різні випадки виявлення та виправлення помилок у закодованих повідомленнях.

У роботі [6] наведено 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] подано привабливі, 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 ґрунтується на можливості отримання відповідних обернених $Q_{pm}^{-n}(x)$-матриць, визначник яких становить ± 1. Спостерігалися як великі швидкості виконання таких процедур, так і отриманих закодованих повідомлень, стійких до криптографічних атак [10, 14].

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 проаналізовано достовірність цього методу і показано, що для $n = 2$ його коригувальна здатність становить 93,33 %, тоді як для $n = 3$ – вже 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 із використанням m-розширення p-чисел Фібоначчі. Автори навели квадратну $G_{p,m}$-матрицю Фібоначчі, де $p \geq 0$ є цілим невід'ємним числом і $m>0$, а 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. Дослідники показали, що співвідношення між елементами $G_{p,m}$-матриці для різних значень p і $m = 1$ збігаються із відношенням між елементами матриці кодування для різних значень p [3]. Загалом, достовірність запропонованого методу зростає зі збільшенням цього значення, але не залежить від значення m.

У роботі [11, 14] розглянуто особливості ефективного генерування $G_p(\lambda)$-матриць Фібоначчі, які можна використати як ключі (де)шифрування для багатораундової матричної криптосистеми перетворення даних. Розроблено процедуру, яка за відомими значеннями степеня матриці (n) та $p(\lambda)$-чисел Фібоначчі дає змогу генерувати відповідну множину ключів шифрування даних, розширяти ключі для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й зручність під час передавання каналами зв'язку.

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 дослідники показали, що, за умови правильного вибору початкових членів для (m, t)-розширення p-чисел Фібоначчі, можна застосувати процедуру (де)кодування даних із використанням $G_{p,m,t}$-матриці Фібоначчі. Зроблено висновок, що для $t = 1$ зв'язки між елементами матриці кодування даних для різних значень p і m збігаються з аналогічними початковими членами чисел Фібоначчі [4].

У роботі [3] наведено узагальнені співвідношення між елементами матриці кодування даних числами Фібоначчі. Автори розглядали клас квадратної матриці Фібоначчі ($p+1$)-порядку, елементи якої ґрунтуються на p-числах Фібоначчі з визначником, що становить ± 1. Вони стверджують, що існує зв'язок між числами Фібоначчі з початковими членами, відомий як формула Кассіні, а саме: $F_{n+1} \times F_{n-1} - F_n^2 = (-1)^n$, $n \geq 1$. Дослідники встановили, що послідовність чисел Фібоначчі та золотий переріз мають важливе значення під час побудови порівняно нової теорії простору-часу, відомої як E-теорія нескінченності. Оригінальний метод (де)кодування даних числами Фібоначчі випливає з аналогічних матриць, де відомим залишається зв'язок між її елементами для випадку $p = 1$ [32].

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 [32] 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 ($p = 0, 1, 2, 3, \ldots$), а їхній визначник становить ± 1. Ця унікальна властивість матриць Фібоначчі приводить до узагальнення формули Кассіні. Запропонований оригінальний метод (де)кодування даних числами Фібоначчі випливає 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 істотно перевищує відомі коригувальні можливості інших методів.

У роботі [7] наведено новий клас кодів із 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 [32] щодо методів коригування помилок, спричинених передаванням 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 $E_p = M_p' \, M_p^n$. Ці відносини 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 випливає з цієї комплексної $H_{p,n}$-матриці Фібоначчі, а також встановлено зв'язки між її елементами. Запропоновано підхід до виявлення та виправлення помилок у закодованих повідомленнях, що ґрунтується на потребі розв'язування діофантових рівнянь [28].

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 із 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. Висвітлюючи результати свого дослідження, автори стверджують, що достовірність цього методу зростає зі збільшенням значення p, але вона не залежить від значень поліномів $h(x)$ і $g(y)$, які істотно удосконалюють криптографічну стійкість закодованих повідомлень [9, 11]. Складність цього методу зростає із підвищенням степеня поліномів $h(x)$ і $g(y)$. Також виявлено зв'язок між золотою $(p, h(x), g(y))$-пропорцією, між золотою $(p, h(x))$-пропорцією та між золотою p-пропорцією.

У роботі [33] 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. Дослідник наводить широкий вступ до вишуканої теми “Математика гармонії”, нового міждисциплінарного напряму в сучасній науці. Цей напрям започаткований 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 золотої пропорції, “золотих” алгебричних рівнянь, узагальненої формули Біне для чисел Фібоначчі та “золотих” матриць [30]. Математика гармонії торкається й теоретичної фізики (нові гіперболічні моделі природи) та інформатики, передусім алгоритмічної теорії вимірювання, системи числення з ірраціональними радикалами тощо.

Отже, за результатами аналізування 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 передавання даних трапляється вкрай рідко. Тому додаткові дослідження щодо виявлення та виправлення помилок у закодованих повідомленнях матрицями Фібоначчі значно більших розмірів – актуальна проблема, яку й спробуємо частково вирішити в цьому дослідженні.

Викладення основного матеріалу дослідження

1. Традиційний метод (де)кодування даних числами Фібоначчі. Числа Фібоначчі $(F_n)_{n=0}^{+\infty}$ є однією із найвідоміших лінійних рекурентних послідовностей, визначених у такий спосіб:

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

Таку лінійну рекурентну послідовність другого порядку можна узагальнити й на вищі порядки, а саме:

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

елементи якої називають p-числами Фібоначчі $(p+1)$-го порядку із характеристичним поліномом $x^{p+1} - x^p - 1$ [31].

У 2006 р. О. Стахов [32] висловив кілька цікавих ідей щодо використання чисел Фібоначчі для отримання оригінального коду з можливістю виправлення помилок. Так звані матриці Фібоначчі, елементами яких є відповідні послідовності чисел (1) чи (2), мають багато корисних і цікавих властивостей, а саме:

- для матриці $\bar{\bar{Q}}^1 = \begin{Vmatrix} 1 & 1 \\ 1 & 0 \end{Vmatrix}$ можна отримати $\bar{\bar{Q}}^n = \begin{Vmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{Vmatrix}$ і $\bar{\bar{Q}}^{-n} = \begin{Vmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{Vmatrix}$ $\forall\, n \geq 1$;
- якщо $\det \bar{\bar{Q}}^n = (-1)^n$, то існує тотожність Кассіні $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ $\forall\, n \geq 1$;
- $\bar{\bar{Q}}^{-2k} = \begin{Vmatrix} F_{2k-1} & -F_{2k} \\ -F_{2k} & F_{2k+1} \end{Vmatrix}$ $\forall\, k > 0$; $\bar{\bar{Q}}^{-(2k+1)} = \begin{Vmatrix} -F_{2k} & F_{2k+1} \\ F_{2k+1} & -F_{2k+2} \end{Vmatrix}$ $\forall\, k > 0$;
- $\lim_{n \to +\infty} \left(\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}} \right) = \varphi$, де φ – золотий переріз, тобто найбільший за модулем корінь рівняння $x^2 - x - 1$.

Якщо елементами повідомлення $\bar{P}$ є цілі додатні числа, розділені на блоки по чотири в кожному, то їх можна подати у вигляді такої матриці

$$\bar{\bar{M}} = \begin{Vmatrix} m_1 & m_2 \\ m_3 & m_4 \end{Vmatrix}. \tag{3}$$

Процедура кодування даних полягає у множенні матриці $\overline{\overline{M}}$ на $\overline{\overline{Q}}^n$-матрицю n-го степеня, внаслідок чого отримаємо:

$$\overline{\overline{C}} = \overline{\overline{M}} \times \overline{\overline{Q}}^n = \begin{Vmatrix} m_1 & m_2 \\ m_3 & m_4 \end{Vmatrix} \times \begin{Vmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{Vmatrix} = \begin{Vmatrix} c_1 & c_2 \\ c_3 & c_4 \end{Vmatrix}, \tag{4}$$

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

Отже, маючи кодове слово $\overline{\overline{C}}$, одержувач може його декодувати за допомогою такого матричного виразу:

$$\overline{\overline{C}} \times \overline{\overline{Q}}^{-n} = \overline{\overline{M}} = \begin{Vmatrix} c_1 & c_2 \\ c_3 & c_4 \end{Vmatrix} \times \begin{Vmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{Vmatrix} = \begin{Vmatrix} m_1 & m_2 \\ m_3 & m_4 \end{Vmatrix}, \tag{5}$$

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

У своєму дослідженні [32] О. Стахов сформулював гіпотезу щодо можливості виявлення та виправлення потенційних помилок. Якщо кодове слово $\overline{\overline{C}}$ не містить помилок, то:

- існує тотожність між визначниками матриць

$$\det \overline{\overline{C}} = (-1)^n \det \overline{\overline{M}}; \tag{6}$$

- відношення певних елементів кодового слова відповідають золотому перерізу

$$\frac{c_1}{c_2} \approx \frac{c_3}{c_4} \approx \varphi; \tag{7}$$

- значення обчислених елементів є цілими числами

$$\begin{aligned} c_1 &= \frac{(-1)^n \det \overline{\overline{M}} + c_2 c_3}{c_4}, \; c_2 = \frac{(-1)^n \det \overline{\overline{M}} + c_1 c_4}{c_3}, \\ c_3 &= \frac{(-1)^n \det \overline{\overline{M}} + c_1 c_4}{c_2}, \; c_4 = \frac{(-1)^n \det \overline{\overline{M}} + c_2 c_3}{c_1}. \end{aligned} \tag{8}$$

2. Можливість виявлення та виправлення помилок у закодованому повідомленні. У процедурі кодування даних, яку запропонував О. Стахов [32], перевіряльний елемент $\det \overline{\overline{M}}$ потрібно надсилати одержувачу разом із кодовим словом $\overline{\overline{C}}$. Якщо перевіряльний елемент надходить без помилок, то повідомлення $\overline{\overline{M}}$ можна відновити за допомогою виразу (5). Якщо $\det \overline{\overline{C}} \neq (-1)^n \det \overline{\overline{M}}$, то кодове слово $\overline{\overline{C}}$ містить одну або більше помилок, для виявлення яких потрібно оцінити кожен з елементів за виразом (8).

Якщо хоча б один з елементів c_i є цілим числом, то кодове слово $\overline{\overline{C}}$ містить одну помилку, яку можна виправляти за допомогою одного із виразів (8). Якщо ж декілька елементи c_i не є цілими числами, то кодове слово містить більше від однієї помилки. У цьому випадку О. Стахов рекомендує розв'язувати деякі діофантові рівняння та використати умову (7), щоб виправити помилки. Спочатку потрібно перевірити можливість появи подвійних помилок. Наприклад, якщо елементи c_1 та c_2 помилкові, то для їх виправлення розв'язують таке діофантове рівняння

$$xc_4 - yc_3 = (-1)^n \det \overline{\overline{M}}, \tag{9}$$

а якщо c_3 та c_4 помилкові, то розв'язують таке діофантове рівняння

$$-xc_2 + yc_1 = (-1)^n \det \overline{\overline{M}}. \tag{10}$$

Серед численних розв'язків діофантового рівняння (9) правильні значення елементів c_1 і c_2 можна забезпечити тими із них, які задовольняють властивість обчислених елементів (8). За допомогою такої процедури можна виправити всі випадки появи двох і навіть трьох помилок у кодовому слові $\overline{\overline{C}}$. Метод не працює тільки тоді, коли всі елементи c_i неправильні.

Деякі автори [4, 20] зазначають, що процедура розв'язання діофантового рівняння не є простим завданням і може тривати довго [28]. Окрім цього, без деяких конкретних умов щодо повідомлення (3) і певних гіпотез щодо точності обчислення елементів (8) інколи буде неможливо виявити правильне повідомлення (3) серед значної кількості розв'язків діофантових рівнянь (9) чи (10). Водночас, у роботі [5] автори навели деякі гіпотези щодо можливості виявлення та виправлення помилок у закодованих повідомленнях числами Фібоначчі, а також показали, як виправляти помилки, які неможливо було б виправляти взагалі. В їхньому дослідженні йдеться не про бітові помилки, як переважно у теорії кодування даних. Вони використовують термінологію О. Стахова та посилаються на цілочисельні помилки, які зазвичай містять декілька десятків чи навіть сотень біт.

Отже, одержуючи повідомлення $\overline{\overline{M}}$ і відповідне кодове слово $\overline{\overline{C}}$, з використанням матричного виразу (5) можна отримати такі нерівності:

$$\frac{F_{n+1}}{F_n} < \frac{c_1}{c_2} < \frac{F_n}{F_{n-1}}, \quad \frac{F_{n+1}}{F_n} < \frac{c_3}{c_4} < \frac{F_n}{F_{n-1}}, \tag{11}$$

які виражають точність наближень певних відношень (7). Нижче наведено деякі властивості нерівності (11) у вигляді відповідних тверджень, які використовують для обґрунтування відповідних 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 належність будь-якого відношення фіксованому інтервалу

$$\left[\frac{c_1+h}{c_2}, \frac{c_1}{c_2+h}, \frac{c_3+h}{c_4}, \frac{c_3}{c_4+h}\right] \subset \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}}\right] \tag{12}$$

істинна тоді, коли $h = 0$. У роботі [5] наведено відповідне доведення цього твердження, а також приналежності інших уточнених відношень елементів кодового слова $\overline{\overline{C}}$ фіксованому інтервалу (12).

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

$$\left[\frac{c_1+h}{c_2+k}, \frac{c_3+h}{c_4+k}\right] \subset \left[\frac{F_{n+1}}{F_n}, \frac{F_n}{F_{n-1}}\right] \tag{13}$$

істинна тоді, коли виконується така нерівність

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

У роботі [5] наведено відповідне доведення цього твердження, а також належності уточненого другого відношення елементів кодового слова $\overline{\overline{C}}$ фіксованому інтервалу (13).

Для оцінювання значень елементів c_i за виразами (8) керуються такими міркуваннями:

1) якщо тільки один з елементів c_i є цілим числом, то кодове слово $\overline{\overline{C}}$ 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 $\overline{\overline{C}}$ містить дві або більше помилок, виправити які також можливо.

О. Стахов у роботі [32] запропонував деякі стратегії вирішення проблем, які випливають із другого міркування, але вони потребують дещо глибшого аналізу та обговорення результатів. Передусім, неефективно перевіряти всі гіпотези щодо появи як подвійних, так і потрійних помилок. Зазвичай зручніше використовувати деякі властивості елементів у кодовому слові $\overline{\overline{C}}$, які можуть ідентифікувати наявну ситуацію (7). Для цього потрібно перевірити, чи відношення c_1/c_2 і c_3/c_4 належить фіксованому інтервалу $[a,b]$, де $a = F_{n+1}/F_n$ і $b = F_n/F_{n-1}$.

1) якщо відношення $c_1/c_2 \in [a,b]$ істинне, а відношення $c_3/c_4 \notin [a,b]$ хибне, то елементи c_1 і c_2 правильні, а елементи c_3 і c_4 – помилкові;

2) якщо відношення $c_1 / c_2 \in [a,b]$ хибне, а відношення $c_3 / c_4 \in [a,b]$ 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) три елементи з чотирьох помилкові: 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) помилковими є чотири елементи.

Зрозуміло, чотири помилкові елементи виправити неможливо. Тому в роботі [5] автори детально розглядають ситуацію не з трьома помилковими елементами, а тільки із двома помилками.

2.1. ***Можливість виправлення двох помилок у різних рядках***. Для кращого викладення матеріалу використаємо такі позначення:

- $\overline{\overline{C}}' = \begin{Vmatrix} c_1' & c_2' \\ c_3' & c_4' \end{Vmatrix}$ – отримане хибне повідомлення, яке може містити деякі помилкові елементи, тобто $\overline{\overline{C}}' = \overline{\overline{C}} + \overline{\overline{E}}$;
- $\overline{\overline{E}} = \begin{Vmatrix} e_1 & e_2 \\ e_3 & e_4 \end{Vmatrix}$ – матриця помилок, елементи якої є цілими числами.

Якщо всі елементи матриці $\overline{\overline{E}}$ нульові, то так зване хибне повідомлення $\overline{\overline{C}}'$ не має помилкових елементів, тобто воно тотожне із кодовим словом $\overline{\overline{C}}$.

Нехай отримано хибне повідомлення $\overline{\overline{C}}'$, де маємо такі відношення $c_1' / c_2' \in [a,b]$ і $c_3' / c_4' \in [a,b]$, тобто є дві помилки. Можливі помилки в таких елементах: $c_1' c_3'$; c_2', c_4'; $c_3' c_4'$ або c_2', c_3', тобто ці помилки містяться у різних рядках матриці $\overline{\overline{C}}'$. У цьому випадку О. Стахов запропонував підхід [32], який потребує розв'язання таких діофантових рівнянь:

$$\begin{aligned} xc_4' - yc_2' &= (-1)^n \det \overline{\overline{M}}, \quad xc_1' - yc_3' = (-1)^n \det \overline{\overline{M}}, \\ xy - c_2' c_3' &= (-1)^n \det \overline{\overline{M}}, \quad c_1' c_4' - xy = (-1)^n \det \overline{\overline{M}}. \end{aligned} \tag{14}$$

Розв'язки рівнянь за цими виразами потрібно підібрати так, щоб вони задовольняли умову виправлення помилок (8). Цей підхід спричиняє декілька проблем. Насамперед, без будь-якої додаткової умови на повідомлення $\overline{\overline{M}}$ серед значної кількості розв'язків діофантових рівнянь (14), можливо, буде важко знайти ті, що належать фіксованому інтервалу $[a, b]$. Водночас, ці діофантові рівняння важко розв'язати [28], якщо значення перевіряльного елемента $\det \overline{\overline{M}}$ надто велике, тобто така процедура еквівалентна задачі факторизації великого цілого числа [29]. Якщо ж вважати повідомлення $\overline{\overline{M}}$ 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.

Наприклад, розглянемо так зване хибне повідомлення $\overline{\overline{C}}'$, 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 знайти ціле число e_1. Справді, 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 $c_1' - c_2' \times b = c_1' - c_2 \times b$, тобто значення елемента становить $e_1 = \lfloor c_1' - c_2 \times b \rfloor$, де $\lfloor q \rfloor$ – функція, що визначає стелю числа. Аналогічно можемо отримати значення помилкового елемента $e_3 = \lfloor c_3' - c_4 \times b \rfloor$.

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 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 $\bar{\bar{C}}'$, можна виявляти та виправляти за однаковими методиками.

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

1) якщо відношення $c_i'/c_j > b$ істинне, то обчислюємо елемент $e_i = \lfloor c_i' - c_j \times b \rfloor$ для ($i = 1 \wedge j = 2$) $\vee$ ($i = 3 \wedge j = 4$);

2) якщо відношення $c_i / c_j' > b$ істинне, то обчислюємо елемент $e_j = \lfloor c_j' - c_i / b \rfloor$ для ($i = 1 \wedge j = 2$) $\vee$ ($i = 3 \wedge j = 4$);

3) якщо відношення $c_i'/c_j < a$ істинне, то обчислюємо елемент $e_i = \lceil c_i' - c_j \times a \rceil$ для ($i = 1 \wedge j = 2$) $\vee$ ($i = 3 \wedge j = 4$);

4) якщо відношення $c_i / c_j' < a$ істинне, то обчислюємо елемент $e_j = \lceil c_j' - c_i / a \rceil$ для ($i = 1 \wedge j = 2$) $\vee$ ($i = 3 \wedge j = 4$).

Як бачимо, перевіряльні співвідношення (1–4) набагато легше оцінювати, ніж розв'язувати діофантові рівняння (14). Якщо б одержувачу кодового слова $\bar{\bar{C}}$ були відомі позиції помилкових елементів у матриці $\bar{\bar{C}}'$, не було б потреби надсилати ще перевіряльний елемент $\det \bar{\bar{M}}$. Оскільки позиції цих елементів наперед не відомі, необхідно використовувати $\det \bar{\bar{M}}$ 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 $e_1 = \lfloor c_1' - c_2' \times b \rfloor$, так і елемента $e_2 = \lceil c_2' - c_1'/b \rceil$. Якщо для одержання елемента $c_1 = c_1' - e_1$ скористались помилковим елементом e_1, то відношення $c_1 / c_2' \notin [a, b]$ істинне. Якщо ж помилковим елементом e_2 скористались для отримання елемента $c_2 = c_2' - e_2$, то маємо відношення c_1'/c_2, яке не дає змоги отримати кодове слово $\bar{\bar{C}}$, що відповідає надісланому повідомленню. У цій ситуації єдиним рішенням є використання перевіряльного елемента $\det \bar{\bar{M}}$ і порівняння їхніх визначників за тотожністю (6).

2.2. ***Можливість виправлення двох помилок у одному рядку***. Випадок, коли в одному рядку хибної матриці $\bar{\bar{C}}'$ трапляються два помилкові елементи, складніше виявити та виправити. Вважатимемо, що помилки є в елементах c_1' і c_2', тобто помилкові елементи $\{e_1, e_2\} \neq 0$ і правильні $\{e_3, e_4\} = 0$. У цій ситуації О. Стахов у роботі [32] пропонує розв'язувати діофантове рівняння (9) і виправляти помилки за допомогою отриманих розв'язків, які належать фіксованому інтервалу $[a, b]$. Однак, як зазначено у роботі [5], цього недостатньо для виявлення та виправлення таких помилок. Пояснимо це на конкретному прикладі.

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

$$\bar{\bar{M}} = \begin{Vmatrix} m_1 & m_2 \\ m_3 & m_4 \end{Vmatrix} \text{ і } \bar{\bar{M}}' = \begin{Vmatrix} m_1' & m_2' \\ m_3 & m_4 \end{Vmatrix} = \begin{Vmatrix} m_1 + k\, m_3 & m_2 + k\, m_4 \\ m_3 & m_4 \end{Vmatrix}, \tag{15}$$

а їхні елементи є натуральними числами, відмінними від нуля. Матриці закодованих повідомлень (отримане кодове слово і хибне повідомлення) відповідно мають такий вигляд:

$$\bar{\bar{C}} = \begin{Vmatrix} c_1 & c_2 \\ c_3 & c_4 \end{Vmatrix} \text{ і } \bar{\bar{C}}' = \begin{Vmatrix} c_1' & c_2' \\ c_3 & c_4 \end{Vmatrix} = \begin{Vmatrix} c_1 + k\, c_3 & c_2 + k\, c_4 \\ c_3 & c_4 \end{Vmatrix}, \tag{16}$$

Оскільки перевіряльні елементи будуть однаковими, тобто $\det(\bar{\bar{M}}) = \det(\bar{\bar{M}}')$, то для виправлення помилок, які є в першому рядку, потрібно розв'язати діофантове рівняння (9) для обох матриць $\bar{\bar{C}}$ і $\bar{\bar{C}}'$. Їхні розв'язки будуть різними – (c_1, c_2) і $(c_1 + k \times c_3, c_2 + k \times c_4)$, вони задовольнятимуть перевіряльні співвідношення (1–4) та умову належності фіксованому інтервалу $[a, b]$. Це означає,

що, отримавши матриці (16), ми 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 $\bar{\bar{M}}$ – матриця розміром 2×2 вигляду (3), в якій $m_1 \neq m_3$ і $m_2 \neq m_4$ або навпаки – $m_1 \neq m_3$ і $m_2 \neq m_4$. Таку матрицю називають *мінімальною* [5]. Це означає, що не існує такого натурального числа k, щоб $m_1 = a + k \times m_3$ і $m_2 = b + k \times m_4$, де $a, b \in \{0, 1\}$ (або $m_3 = a + k \times m_1$ і $m_4 = b + k \times m_2$). Тому набір блоків вхідних повідомлень повинен містити тільки мінімальні матриці. В такий спосіб можна виправляти дві помилки в одному рядку, оскільки братимемо найменші розв'язки діофантового рівняння, придатність яких виявляємо перевіряльними співвідношеннями (1)–(4).

Щоб пояснити зазначене, розглянемо повідомлення (15), де матриця $\bar{\bar{M}}$ є мінімальною, а очікуване кодове слово $\bar{\bar{C}}$ – хибною матрицею $\bar{\bar{C}}'$, яка містить помилкові елементи в першому рядку (16). Для їх виправлення розв'язуємо діофантове рівняння (9), знайшовши два розв'язки (x_1, y_1) і (x_2, y_2), які відповідають таким виразам:

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

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

$$\begin{cases} x_2 = F_{n+1}m_1 + F_n m_2 + k(F_{n+1}m_3 + F_n m_4) = x_1 + kc_3 = -\det \bar{\bar{M}}\, x_0 + (k + t_1)c_3; \\ y_2 = F_n m_1 + F_{n-1} m_2 + k(F_n m_3 + F_{n-1} m_4) = y_1 + kc_4 = -\det \bar{\bar{M}}\, y_0 + (k + t_1)c_4, \end{cases}$$

і $t_2 > t_1$, то, щоб знайти розв'язок (x_1, y_1), тобто виправити помилкові елементи й отримати кодове слово $\bar{\bar{C}}$, достатньо взяти найменший розв'язок діофантового рівняння (9) та перевірити виконання перевіряльних співвідношень (1–4).

2.3. ***Можливість виправлення трьох помилок***. Розглянемо випадок з появою трьох помилок. Припустимо, ми отримали таку хибну матрицю

$$\bar{\bar{C}}' = \begin{Vmatrix} c_1 & c_2' \\ c_3' & c_4' \end{Vmatrix}, \tag{17}$$

в якій є помилки, наприклад, у 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 [32] пропонує розв'язувати нелінійне діофантове рівняння $zc_1 - xy = (-1)^n \det \bar{\bar{M}}$ і виправляти похибки за допомогою розв'язків, що належать фіксованому інтервалу $[a, b]$. Однак, як виявилося згодом [5], розв'язати це нелінійне діофантове рівняння надзвичайно важко [28]. Насамперед це зумовлено рівняннями (14), коли z фіксоване, і процедура розв'язування такого рівняння еквівалентна 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, а потім вже 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. 2.1.

2. Розглядаємо другий рядок і виправляємо в ньому помилковий елемент, розв'язавши діофантове рівняння, як показано в п. 2.2.

Щоб пояснити зазначене припустимо, що отримано хибну матрицю (17) за істинного відношення $c_1 / c_2' > b$. Як і в п. 2.1, потрібно обчислити значення елемента $e_2 = \lfloor c_2' - c_1 / b \rfloor$ і відновити елемент $c_2 = c_2' - e_2$. Тепер у матриці (17) замінюємо елемент c_2' на c_2, отримуючи дещо уточнену

матрицю $\overline{\overline{C}}=\begin{Vmatrix} c_1 & c_2 \\ c_3 & c_4 \end{Vmatrix}$. Щоб виправити в ній ще два елементи, потрібно розв'язати діофантове рівняння (10) і вибрати найменший позитивний розв'язок (x_0, y_0), який перевіряємо на дотримання умови за допомогою перевіряльного співвідношення (1–4) та належності відношень фіксованому інтервалу $[a, b]$.

Однак зазвичай ми наперед не знаємо, де містяться помилкові елементи в хибному повідомленні $\overline{\overline{C}}$, а це означає, що невідомий рядок, що містить тільки одну помилку. Щоб знайти позиції елементів без помилок, потрібно послідовно брати кожен елемент хибної матриці $\overline{\overline{C}}$ і намагатися декодувати його, як описано в п. 2.1. Потрібно також здійснити перевірку дотримання умови за допомогою перевіряльного 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 помилкові елементи. Нехай ми отримали матрицю $\overline{\overline{C}}$ вигляду (17) 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 $\overline{c}_3$ і c_4 та перевіряємо, чи відношення $\overline{c}_3 / c_4 \in [a,b]$ істинне.

1. Якщо відношення $\overline{c}_3 / c_4 \notin [a,b]$ хибне, то розуміємо, що зробили помилку, і тому виконуємо процедуру заново, змінюючи початкові припущення. Наприклад, припускаємо, що єдиним правильним елементом у хибній матриці $\overline{\overline{C}}$ є елемент c_3, і знову починаємо процедуру пошуку та виправлення помилок.

2. Якщо відношення $\overline{c}_3 / c_4 \in [a,b]$ істинне, то не розуміємо, що робимо помилку, і тому припускаємо, що це рішення $(\overline{c}_3, c_4)$ є правильним. Продовжуємо виправлення двох інших елементів c_1 і c_2, розв'язуючи відповідне діофантове рівняння (9), внаслідок чого знаходимо елементи c_1 і $\overline{c}_2$. Тепер, щоб виявити відсутність помилки, потрібно перевірити, чи відношення $c_1 / \overline{c}_2 \in [a,b]$ істинне. Якщо ж відношення $\overline{c}_3 / c_4 \in [a,b]$ істинне, то відношення $x_1 / y_1 \notin [a,b]$ хибне (див. лему 1).

Тепер розглянемо докладніше, як виконують процедуру декодування даних. Нехай отримано хибну матрицю $\overline{\overline{C}}$ вигляду (17), в якій єдиним правильним елементом є c_4. Спочатку розглянемо випадок істинного відношення $c_3 / c_4 > b$, для чого обчислюємо значення елемента

$$e_3 = \left\lfloor c_3 - c_4 \times b \right\rfloor = e_3 + \left\lfloor \frac{m_3}{F_{n-1}} - e_4 \times b \right\rfloor = e_3 + h, \tag{18}$$

де $h \in \mathbb{Z}$ і $\overline{c}_3 = c_3 - e_3 = c_3 - h$. Щоб перевірити, чи відношення $\overline{c}_3 / c_4 \in [a,b]$ істинне, скористаємося твердженням 3 і, задаючи значення h, для елемента e_4 перевіримо виконання такої нерівності

$$\frac{-hF_{n-1} - m_3}{F_n} < e_4 < \frac{-hF_n + m_4}{F_{n+1}}. \tag{19}$$

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

$$\overline{\overline{C}} = \begin{Vmatrix} \overline{c}_1 & \overline{c}_2 \\ \overline{c}_3 & c_4 \end{Vmatrix}. \tag{20}$$

Якщо обчислимо елементи $\overline{c}_3$ і c_4, то відношення $\overline{c}_3 / c_4 \in [a,b]$ істинне тоді, коли

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

Доведення. Нехай $m \in \mathbb{Z}$ і $n \in \mathbb{N}$, тоді функція стелі $\left\lfloor m/n \right\rfloor$ має такий вигляд:

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

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

Нехай маємо такі елементи $\overline{c_3} = c_3 - h$ і $\overline{c_4} = c_4 + e_4$, де $h = \left\lfloor \frac{m_3 + e_4 F_n}{F_{n-1}} \right\rfloor$. Розглянемо два різні випадки:

1) якщо значення $e_4 > 0$, то 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, відношення $\overline{c_3} / \overline{c_4} \in [a,b]$ істинне тоді, коли нерівність (19) виконується, тобто справедлива 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 $\overline{c_3} / \overline{c_4} \notin [a,b]$ 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 (19) і рівність $e_4 = (qF_{n-1} + r - m_4) / F_n$. 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, згідно із твердженням 3, відношення $\overline{c_3} / \overline{c_4} \in [a,b]$ істинне;

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

a) якщо $|e_4|F_n - m_3 < F_{n-1}$, то $e_4 = -1 \Rightarrow h = 1$. Нескладно перевірити, якщо відношення $c_3 / c_4 \in [a,b]$ істинне, то відношення $\overline{c_3} / \overline{c_4} = (c_3 - 1) / (c_4 - 1) \notin [a,b]$ хибне;

b) якщо $|e_4|F_n - m_3 = qF_{n-1}$, то $h = q$. Відношення $\overline{c_3} / \overline{c_4} < b$ 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 $\overline{c_3} / \overline{c_4} \notin [a,b]$ 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 (19) 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

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

внаслідок чого встановимо, що відношення $\overline{c_3} / \overline{c_4} \notin [a,b]$ істинне.

Припустимо, виникла ситуація леми 1, тобто елемент e_4 належить цьому діапазону. Тож припускаємо, що належно виправляємо помилкові елементи і переходимо до наступного кроку: обчислюємо інші два елементи c_1 і c_2, розв'язуючи діофантове рівняння (9). Його розв'язки правильні, якщо виконуються такі тотожності:

$$\begin{cases} x_1 = -\det \bar{\bar{M}}\, x_0 + t\bar{c}_2, \\ y_1 = -\det \bar{\bar{M}}\, y_0 + tc_2, \end{cases} \tag{21}$$

де $t \in \mathbb{Z}$, а для знаходження x_0, y_0 розв'язуємо таке рівняння $c_2 x_0 - \bar{c}_2 y_0 = 1$.

Лема 2. Нехай отримали хибну матрицю (20). Обчислюємо елементи $\bar{c}_2$ і c_2, припустивши, що відношення $\bar{c}_2 / c_2 \in [a,b]$ істинне. Тоді знаходимо розв'язок (x_1, y_1) як результат розв'язання діофантового рівняння (9). Тому, якщо відношення $\bar{c}_2 / c_2 \in [a,b]$ істинне, то відношення $x_1 / y_1 \notin [a,b]$ хибне.

Доведення. Оскільки відношення $\bar{c}_2 / c_2 \in [a,b]$ істинне, то за лемою 1 маємо два випадки:

1. Якщо $e_4 > 0$, повинна виконуватися рівність $e_4 F_n = qF_{n-1} + r - m_3$, де $r < F_{n-1} \wedge h = -q$. Оскільки (x_1, y_1) є розв'язком діофантового рівняння (9), маємо таке відношення

$$\frac{x_1}{y_1} = \frac{y_1(\bar{c}_2 + q) - \det \bar{\bar{M}}}{y_1(c_2 + e_4)}.$$

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

a) відношення $x_1/y_1 > a$ істинне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} < 0$. Фактично, виконується така нерівність

$$\frac{x_1}{y_1} > \frac{F_{n+1}}{F_n} \vee \; F_n y_1(\bar{c}_2 + q) - F_n \det \bar{\bar{M}} > F_{n+1} y_1(c_2 + e_4).$$

Оскільки значення e_4 перевіряє нерівність (19), то, з одного боку, маємо нерівність $F_{n+1} y_1(c_2 + e_4) < F_{n+1} y_1 c_2 + F_n y_1 q + y_1 m_4$, але, з іншого боку, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$, – іншу нерівність

$$F_n y_1(\bar{c}_2 + q) - F_n \det \bar{\bar{M}} > F_{n+1} y_1 c_2 + F_n y_1 q + y_1 m_4,$$

тобто $F_n y_1(F_{n+1} m_3 + F_n m_4) - F_n \det \bar{\bar{M}} > F_{n+1} y_1(F_n m_3 + F_{n-1} m_4) + y_1 m_4$, отже, $F_n \det \bar{\bar{M}} > 0$. Це означає, що відношення $x_1 / y_1 \notin [a,b]$ хибне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$.

b) відношення $x_1/y_1 < b$ істинне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$. Фактично, виконується така нерівність

$$\frac{x_1}{y_1} < \frac{F_n}{F_{n+1}} \vee \; F_{n-1} y_1(\bar{c}_2 + q) - F_{n-1} \det \bar{\bar{M}} < F_n y_1(c_2 + e_4).$$

Оскільки значення e_4 перевіряє нерівність (19), то, з одного боку, маємо нерівність $F_n y_1(c_2 + e_4) > F_n y_1 c_2 + F_{n+1} y_1 q - y_1 m_3$, але, з іншого боку, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$, то маємо таку нерівність

$$F_n y_1 c_2 + F_{n-1} y_1 q - y_1 m_3 > F_{n-1} y_1(\bar{c}_2 + q) - F_{n-1} \det \bar{\bar{M}},$$

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

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

Аналогічно можна довести такий випадок.

2. Якщо $e_4 < 0$, повинна виконуватися рівність $|e_4|F_n = qF_{n-1} + r + m_3$, де $r < F_{n-1}$ Ù $F_n^2 + 1 < F_{n+1}(m_3 + r) + F_n m_4$ Ù $h = q + 1$. Оскільки (x_1, y_1) є розв'язком діофантового рівняння (9), то маємо таке відношення

$$\frac{x_1}{y_1} = \frac{y_1(\bar{c}_3 - (q+1)) - \det \bar{\bar{M}}}{y_1(c_4 - |e_4|)}.$$

Якщо відношення $x_1 / y_1 \ddot{I} [a,b]$ хибне, виникають дві різні ситуації:

a) відношення $x_1/y_1 > a$ істинне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} < 0$. Фактично, виконується така нерівність

$$\frac{x_1}{y_1} > \frac{F_{n+1}}{F_n} \hat{U} \; F_n y_1(\bar{c}_3 - (q+1)) - F_n \det \bar{\bar{M}} > F_{n+1} y_1(c_4 - |e_4|).$$

Оскільки значення e_4 перевіряє нерівність (19), то, з одного боку, маємо 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 боку, коли перевіряльний елемент $\det \bar{\bar{M}} < 0$, маємо таку нерівність

$$(q+1)F_n y_1 - F_{n+1}y_1 c_4 + y_1 m_4 > F_n y_1(\bar{c}_3 - (q+1)) - F_n \det \bar{\bar{M}},$$

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

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

b) відношення $x_1/y_1 < b$ істинне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$. Фактично, виконується така нерівність

$$\frac{x_1}{y_1} < \frac{F_n}{F_{n+1}} \hat{U} \; F_{n-1} y_1(\bar{c}_3 - (q+1)) - F_{n-1} \det \bar{\bar{M}} < F_n y_1(c_4 - |e_4|).$$

Оскільки значення e_4 перевіряє нерівність (19), то, з одного боку, маємо 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 боку, коли перевіряльний елемент $\det \bar{\bar{M}} > 0$, матимемо нерівність

$$(q+1)F_{n-1} y_1 - F_n y_1 c_4 + y_1 m_3 < F_{n-1} y_1((q+1) - \bar{c}_3) + F_{n-1} \det \bar{\bar{M}},$$

тобто $y_1 m_3 - F_n y_1(F_n m_3 + F_{n-1} m_4) < -F_{n-1} y_1(F_{n+1} m_3 + F_n m_4) + F_{n-1} \det \bar{\bar{M}}$, отже, $F_n \det \bar{\bar{M}} > 0$. Це означає, що відношення $x_1 / y_1 \ddot{I} [a,b]$ хибне тоді, коли перевіряльний елемент $\det \bar{\bar{M}} < 0$.

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

$$\bar{\bar{C}}_1 = \begin{Vmatrix} c_1 & c_2 \\ c_3 & c_4 \end{Vmatrix}. \qquad (22)$$

Починаємо виправляти перший рядок, намагаючись знайти помилку елемента e_1. Припустимо, відношення $c_1 / c_2 > b$ істинне, тож обчислюємо значення

$$e_1 = \left[c_1 - c_2 \times b \right] = \left[\frac{m_1}{F_{n-1}} - e_2 \times b \right] = h,$$

де $h \hat{I} \, ¢$, і $c_1 = c_1 - e_1 = c_1 - h$. Результат аналогічний, як і у випадку 1, тому можемо продовжувати виконувати дії, як і раніше.

Отже, показано можливість виправлення трьох помилок у кодовому слові. Встановлено, що у такій ситуації потрібно перевіряти належність відношень елементів кодового слова фіксованому

інтервалу, для їх виправлення 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 помилкових 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 ґрунтуються методики виявлення та виправлення однієї, двох і трьох помилок у рядках кодового слова. Однак фактично аналогічні дослідження в цій галузі знань здійснювали й інші науковці, тому розглянемо деякі їхні результати дещо детальніше.

У роботі [35, 36] проаналізовано доцільність використання апарату арифметики Фібоначчі для побудови хеш-функцій, насамперед побудови функцій хешування даних на підставі симетричного блокового перетворення із використанням узагальнених чисел та матриць Фібоначчі. Показано перспективність цього напряму досліджень у межах удосконалення статистичних показників симетричних криптографічних перетворень даних за рахунок пришвидшення дифузійних процесів під час використання у схемах обміну підблоками мережі Фейстеля матричного перетворення Фібоначчі.

У роботі [5] автори деталізували особливості виявлення та виправлення подвійних помилкових елементів у матрицях кодування розміром 2×2, які ввів О. Стахов, тобто кодах виправлення помилок 1-Фібоначчі. Такий аналіз виконано 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].

У роботі [27] визначено *k*-матриці Фібоначчі Ганкеля, а також розглянуто різні норми цих матриць. Знайдено співвідношення між евклідовою нормою, нормою стовпця та спектральною нормою цих спеціальних матриць. Наведено кососиметричні *k*-матриці Фібоначчі розміром 4×4 і знайдено цікаву формулу для суми *k*-чисел Фібоначчі.

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 [34], які дещо узагальнюють *p*-числа Фібоначчі та методи (де)кодування даних з їхнім використанням. Наприклад, автор роботи [20] запропонував використовувати рекурентні послідовності $F_n^{(p)}(x,y)$, застосовуючи поліноми Фібоначі [30]. Подальші узагальнення результатів вирішення цієї проблеми можна знайти в роботах [1, 2, 8, 19].

У роботі [26] наведено результати побудови дуально-узагальнених комплексних кватерніонів Фібоначчі та Лукаса. Автори розглядали властивості як дуального узагальненого комплексного числа, так і кватерніона. Окрім цього, 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 та Лукаса у вигляді їхніх різних матричних подань.

У роботі [17] наведено особливості формування *p*-матриці Лукаса, попередньо вивчено *p*-числа Фібоначчі та Лукаса. 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 із використанням p-чисел Лукаса. Якщо в роботі [17] тільки наведено p-матрицю Лукаса $R_pQ_p^n$, елементами якої є p-числа Лукаса, то в цій роботі розроблено новий метод (де)кодування даних на підставі p-матриці Лукаса $R_pQ_p^n$. Також автори встановили зв'язки між елементами матриці кодування даних, з'ясували особливості виявлення та виправлення помилок у закодованих повідомленнях. Висвітлюючи результати 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 [34] наведено узагальнену теорію кодування даних на підставі p-чисел Пелля-Лукаса S_pA^n та відповідний метод їх (де)кодування. Автори встановили співвідношення між елементами матриці кодування для p = 1 та I = 1, які дають змогу виявляти та виправляти помилки в закодованих повідомленнях. Розглядаючи результати 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 наукову новизну та обґрунтувати практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження: проаналізовано методи виявлення та виправлення помилок у закодованих повідомленнях 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 методи виявлення помилок у закодованих повідомленнях матрицями Фібоначчі та уточнені методи їх виправлення можна застосувати у криптографічних системах для передавання каналами зв'язку відповідних блоків кодових слів різної величини із достатньою коригувальною здатністю.

Висновки

Проаналізовано основні підходи щодо виявлення та наявні методи виправлення помилок у закодованих повідомленнях матрицями Фібоначчі, які загалом 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. У результаті аналізу наявних досліджень та публікацій з'ясовано, що навіть за останнє десятиліття опубліковано значну кількість різноманітних робіт, 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 передавання даних трапляється вкрай рідко.

2. За результатами аналізу традиційного методу (де)кодування даних матрицями Фібоначчі встановлено, що елементи кодових слів мають багато корисних і цікавих властивостей, на яких якраз і ґрунтуються підходи щодо виявлення та методи виправлення у них помилок. Сформульовано відповідне твердження, згідно з яким відношення певних елементів кодового слова наближене до золотого перерізу, що має важливе значення для наявних методів 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 ситуації наявності таких помилкових елементів, перевіривши належність відношень відповідних елементів до фіксованого інтервалу.

4. З'ясовано, що хибна належність до фіксованого інтервалу відношень відповідних елементів кодового слова свідчить про те, що в різних його рядках є дві помилки, для виправлення яких пот-

рібно розв'язати відповідні діофантові рівняння, розв'язки яких підбирають так, щоб вони дали змогу задовольнити певні умови виправлення помилок.

5. Встановлено, що за наявності двох помилок у одному рядку кодового слова потрібно розв'язати діофантове рівняння та перевірити належність до фіксованого 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 перевіряльними співвідношеннями.

6. Виявлено, що для виправлення трьох помилок у кодовому слові потрібно перевірити належність до фіксованого інтервалу відношень відповідних його елементів та розв'язати нелінійне діофантове рівняння, реалізація якого надзвичайно складна. 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.

Список літератури

1. 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

2. 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

3. Basu, Manjusri, & Prasad, Bandhu. (2009). The generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons, & Fractals*, Vol. 41, Iss. 5(15), 2517–2525. https://doi.org/10.1016/j.chaos.2008.09.030

4. Basu, Manjusri, & Prasad, Bandhu. (2009, November). Coding theory on the *m*-extension of the Fibonacci *p*-numbers. *Chaos, Solitons, & Fractals*, Vol. 42, Iss. 4, 30, 2522–2530. https://doi.org/10.1016/j.chaos.2009.03.197

5. 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

6. Esmaeili, M., Esmaeili, M., & Gulliver, T. A. (2011). High-rate Fibonacci polynomial codes. In: Proceedings of IEEE International Symposium on Information Theory Proceedings, St. Petersburg, Russia, 1921–1924. https://doi.org/10.1109/ISIT.2011.6033886

7. 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

8. Esmaili, Mostafa, & Esmaeili, 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

9. Gryciuk, Yurij, Grytsyuk, Pavlo. (2015). Perfecting of the matrix Affine cryptosystem information security. Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT'2015), 14–17 September, 2015, 67–69. https://doi.org/10.1109/stc-csit.2015.7325433

10. 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

11. 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 13*th *International Scientific and Practical Conference*, 53–54, November 18–20, 2015, Dnipropetrovsk, Ukraine. Dnipropetrovsk: Department of Dnipropetrovsk National University named after Olesya Honchara.

12. 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

13. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci Q_p-matrices – keys for implementing cryptographic transformations. *Bulletin of the Lviv Polytechnic National University. Series: Computer Science and Information Technology*, Vol. 843, 251–263. URL: https://vlp.com.ua/taxonomy/term/3448

14. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci $G_p(\square)$-matrices for implementation of cryptographic transformations. *Information extraction and processing: interdepartmental collection of scientific papers*, 43(119), 86–95.

15. Hrytsiuk, Yuriy, & Grytsyuk, Pavlo (2016). Generation of Fibonacci $Q_p(\square)$-matrices – keys for data encryption. *Information protection and security of information systems: materials of the 5th International Scientific and Technical Conference*, 39–40, June 02–03, 2016, Lviv, Ukraine. Lviv: Lviv Polytechnic State University.

16. Hrytsiuk, Yuriy, Grytsyuk, Pavlo, Dyak, Tetiana, & Hrynyk, Heorhiy. (2019). Software Development Risk Modeling. IEEE 2019 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2019), Vol. 2, 134–137, 17–20 September, Lviv, Ukraine. Lviv: Lviv Polytechnic National University, 206 p. https://doi.org/10.1109/stc-csit.2019.8929778

17. Kuhapatanakul, K. (2015). The Lucas *p*-matrix. *International Journal of Mathematical Education in Science and Technology*. https://doi.org/10.1080/0020739X.2015.1026612

18. Lagun, A. E., & Hrytsiuk, Yu. I. (2016). *Information theory and coding*. Tutorial. Lviv: SPOLOM Publishing House, 168 p.

19. 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

20. 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/ujcmj.2014.020102

21. 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

22. 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

23. 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

24. Samoilenko, M. I., & Ufimtseva, V. B. (2012). On the possibilities of using Fibonacci arithmetic to increase the efficiency of cryptographic transformations. *Trinitarian Academy*, 77–656. URL: http://www/trinitas/ru/rus/doc/0232/013a/02322115/htm. [In Russian].

25. Samoilenko, N. I., & Ufimtseva, V. B. (2003). Properties of *p*-numbers and Stakhov Q_p^n-matrices in the ring of integers $Z/(q)$. Radioelectronics and computer science. Kharkov: KNURE. No. 1, 111–115. URL: https://cyberleninka.ru/article/n/svoystva-r-chisel-i-qp-matrits-stahova-v-koltse-tselyh-chisel-z-q. [In Russian].

26. 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

27. Sergio Falcon. (2017, Jan.-Feb.). On the K-Fibonacci Hankel and the 4 X 4 Skew Symmetric K-Fibonacci Matrices. IOSR Journal of Mathematics (IOSR-JM), 13(01), 52–58. https://doi.org/10.9790/5728-1301035258

28. 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, Iss. 2, 263–282. https://doi.org/10.1093/ce/zkac066

29. 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. Vol. 15, 201–207. URI: http://dspace.nbuv.gov.ua/handle/123456789/133957

30. Slyusarenko, V. (2008). Fibonacci numbers and the golden ratio. *Mathematics*. Kyiv: School World Publishing House, No. 8(452), 18–24.

31. Slyusarenko, V. (2008). Fibonacci numbers and the golden ratio. Math. Kyiv: School World Publishing House, No. 8(452), 18–24.

32. Stakhov, A. P. (2006, October). Fibonacci matrices, a generalization of the “Cassini formula”, and a new coding theory. *Chaos, Solitons, & Fractals*, Vol. 30, Iss. 1, 56–66. https://doi.org/10.1016/j.chaos.2005.12.054

33. 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

34. 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

35. Ufimtseva, V. B., & Karpenko, N. Yu. (2015). Using sequences of generalized Fibonacci numbers in cryptographic algorithms. *Information processing systems*. Vol. 8, 106–110. URL: http://nbuv.gov.ua/UJRN/soi_2015_8_24. [In Russian].

36. Ufimtseva, Victoria (2005). On the possibilities of using Fibonacci arithmetic to increase the efficiency of cryptographic transformations. *Legal, regulatory and metrological support of the information protection system in Ukraine: scientific and technical collection*. Vol. 10, 137–142. URL: https://ela.kpi.ua/handle/123456789/11453. [In Russian].

METHODS OF CORRECTING ERRORS IN MESSAGES ENCODED BY FIBONACCI MATRICES

Pavlo Grytsiuk[1], Lyubomyr Sikora[2], Yurii Hrytsiuk[3]

[1, 2] Lviv Polytechnic National University, Department of Automated Control Systems,
14, S. Bandery str., Lviv, Ukraine
[3] Lviv Polytechnic National University, Department of Software,
14, S. Bandery str., Lviv, Ukraine
E-mail: pavlo.y.hrytsiuk@lpnu.ua, ORCID: 0009-0003-5409-2043
E-mail: lybomyr.s.sikora@lpnu.ua, ORCID: 0000-0002-7446-1980
E-mail: yurii.i.hrytsiuk@lpnu.ua, ORCID: 0000-0001-8183-3466

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 codeword, 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.

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