УДК 681.325

РЕВЕРСИВНІ ОБЧИСЛЕННЯ НА ОСНОВІ ЛІНІЙНИХ АВТОМАТІВ

В. П. Семеренко, к.т.н., доцент,
Вінницький національний технічний університет
vpsemerenko@mail.ru

Обчислення, які можуть виконуватись не в звичайному порядку (від вхідних даних до вихідних), а навпаки, прийнято називати реверсивними або зворотними.

Починаючи з класичних робіт Р.Ландауера та Ч.Беннетса зворотність в обчисленнях розглядається, як правило, з позицій збереження термодинамічної ентропії. Однак, до практичного застосування термодинамічно зворотних комп'ютерів ще далеко, оскільку вони вимагають спеціальної ("консервативної") логіки. Тому будемо розглядати реверсивні обчислення на алгоритмічному рівні, що дозволяє отримати практичну користь в рамках нині існуючої техніки.

Як відомо, фундаментальні закони науки (в класичній і квантовій динаміці, в теорії відносності Ейнштейна) інваріантні в часі, з чого випливає еквівалентність минулого і майбутнього в математичному плані. Але, як довів нобелівський лауреат І. Пригожин, зворотність в часі справедлива тільки для інтегрованих динамічних систем.

Прикладом таких систем може бути спеціальний клас лінійних автоматів – автономні лінійні послідовнісні схеми (ЛПС). Головною особливістю автономної ЛПС є незмінні в часі вхідні дані.

В системі координат реверсивних обчислень координатна вісь t_i часу направлена в протилежні сторони: додатну ($t_i > 0$) і від'ємну ($t_i < 0$), що означає развиток подій "вперед" і "назад" в часі (момент часу $t_i = 0$ відповідає теперішньому часу). Відповідно розглянемо і два типи автономних ЛПС.

ВИЗНАЧЕННЯ 1. Автономна ЛПС називається прямою (автономною ПЛПС), якщо її робота розпочинається в момент часу $t_0 = 0$, і момент часу t_{i+1} знаходиться правіше моменту часу t_i по додатній часовій координатній вісі ($i = 0, 1, 2, \ldots$).

ВИЗНАЧЕННЯ 2. Автономна ЛПС називається оберненою (автономною ОЛПС), якщо її робота розпочинається в момент часу $t_0 = 0$, і момент часу t_{i+1} знаходиться лівіше моменту часу t_i по від'ємній часовій координатній вісі ($i = 0, 1, 2, \ldots$).

При нульових вхідних даних вказані ЛПС з характеристичними матрицями A, B і вектором станів $S(t)$, описуються над полем Галуа $GF(q)$ такими функціями переходів і виходів:

для автономної ПЛПС –

$$S(t+1) = A \times S(t), \quad GF(q),$$
$$Y(t) = S(t),$$

і для автономної ОЛПС –

$$S(-t-1) = A_{inv} \times S(-t), \quad GF(q).$$
$$Y(-t) = S(-t),$$

Матрицю A_{inv} автономної ОЛПС легко визначити в результаті розв'язання матричного рівняння $A_{inv} \times A = E$ відносно одиничної матриці E і відомої матриці A.

Автономні ЛПС, як динамічні системи з однією степінню свободи, мають замкнуту фазову траєкторію

(цикл), в якій містяться початковий стан S_{beg} та кінцевий стан S_{end}.

Фактично автономні ПЛПС и ОЛПС – це дві копії однієї автономної ЛПС, які функціонують по протилежним часовим вісям. Обидві копії одночасно розпочинають свою роботу з одного початкового стану S_{beg} і, рухаючись в різні сторони по фазовій траєкторії, закінчують роботу в кінцевому стані S_{end}. В загальному випадку тривалість переходу із стану S_{beg} в стан S_{end} для обох копій ЛПС різна, тому одна з них досягне заданої мети раніше.

Одночасний перехід ПЛПС і ОЛПС до спільного кінцевого стану S_{end} по циклічній фазовій траєкторії від початкового стану S_{beg} в протилежні сторони можна інтерпретувати як одночасний рух від “теперішнього часу” в “майбутнє” та в “минуле”. Після досягнення стану S_{end} будь-якою з цих копій ЛПС, друга копія, яка “програла”, також закінчує свою роботу, оскільку спільна ціль досягнута. Таким чином, завдяки паралельній роботі двох автономних ЛПС, ми в середньому вдвічі швидче отримуємо необхідний результат.

Така постановка задачі характерна для завадостійкого кодування. Особливістю графу переходів циклічних кодів, які виправляють кратні помилки, є наявність численних нульових циклів (НЦ), які утворені нульовими дугами. Методи пошуку помилок по графу переходів полягають в побудові кодового шляху помилки, який проходить через НЦ і особливі вершини v_{ks}, за допомогою яких різні НЦ зв’язані між собою одиничними дугами. В термінах теорії систем особливі вершини v_{ks} в кожному НЦ грають роль кінцевих станів в фазовій траєкторії.

На основі розглянутих теоретичних моделей розроблені алгоритми декодування циклічних кодів в двійкових і недвійкових полях Галуа і реалізовані програмно мовою С++ з використанням технології паралельних обчислень OpenMP.

Реверсивні обчислення знаходять своє використання і в задачах криптоаналізу. В цьому випадку також використовується два автомати, але вже зі змінними в часі вхідними даними. Прямий автомат під дією заданих вхідних сигналів $U(t)$ переходить із початкового стану S_{beg} в кінцевий стан S_{end}. Отримані на виході прямого автомата вихідні сигнали можно розглядати як зашифровані вхідні дії. Математично дії прямого автомата описуються такою функцією переходів:

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(q).$$

Задача оберненого автомату полягає в тому, щоб на основі відомої вихідної послідовності і стану S_{end} відновити вхідну послідовність і повернутись в стан S_{beg}.

Безумовно, при використанні тільки лінійних автоматів можно розв’язати лише прості задачі криптоаналізу, наприклад, в поточному шифруванні або скремблюванні. Для проведення більш складного криптоаналізу необхідно використовувати нелінійні математичні перетворення.