ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

УДК 681.3

ДОСЛІДЖЕННЯ ПОХИБОК САМОКАЛІБРОВАНИХ АНАЛОГО-ЦИФРОВИХ ПЕРЕТВОРЮВАЧІВ НА ОСНОВІ НАДЛИШКОВИХ ПОЗИЦІЙНИХ СИСТЕМ ЧИСЛЕННЯ

Д. т. н., проф. Азаров О. Д., Біліченко Н. О., к. т. н. Захарченко С. М.

Основними вимогами, що висуваються до сучасних аналого-цифрових перетворювачів є високі: швидкодія, роздільна здатність, стабільність метрологічних характеристик як у заданому температурному діапазоні, так і у часі, низька вартість тощо. У більшості випадків спроби покращити один із параметрів приводять до погіршення інших. Так, більшість способів підвищення точності АЦП базується на введенні структурної надлишковості, що полягає у використанні додаткових аналогових та цифрових вузлів, а також функційних блоків. При цьому в ряді випадків додаткові аналогові вузли та блоки повинні мати високі метрологічні характеристики [1, 2], що передбачає використання вартісної прецизійної елементної бази. Крім того, досить часто вказані підходи приводять до значного ускладнення алгоритмів перетворення, і, як результат, зменшується швидкодія [3].

Принципово іншим напрямком покращання метрологічних характеристик АЦП є введення інформаційної надлишковості у формі надлишкових позиційних систем числення (НПСЧ) [4].

Підвищення точності АЦП на основі НПСЧ реалізується з використанням принципів самокалібрування інструментальних похибок [5]. У данному випадку передбачається організація роботи пристрою в двох режимах: самокалібрування та основного перетворення. В режимі самокалібрування відбувається визначення реальних ваг Q_i розрядів перетворювача, зсуву нуля $\Delta A_{зс}$ та масштабного коефіцієнта M. Слід відзначити, що процес калібрування в даному випадку не потребує використання спеціальних зразкових мір та приладів.

Базове положення самокалібрування полягає в тому, що розрядна сітка перетворювача розбивається на групи з m «неточних» (старших), $(n - m)$ «точних» (молодших) та d додаткових розрядів у вигляді, зображеному на рис. 1.

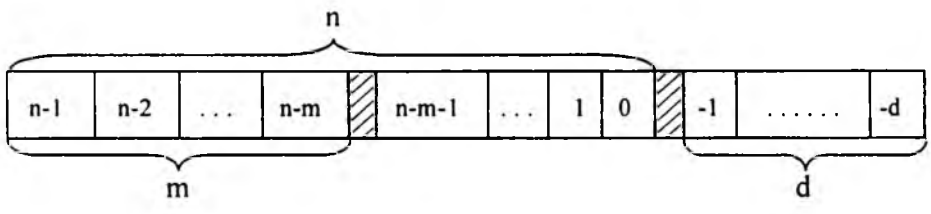

Рис. 1. Розрядна сітка перетворювача

При цьому «неточні» та точні розряди формують групу з n основних розрядів. Група додаткових розрядів використовується для зменшення методичної похибки в процесі самокалібрування.

Суть самокалібрування ваги i-го розряду Q_i для такого АЦП полягає в двократному врівноваженні допоміжного сигналу $A_д$, причому перший раз з використанням Q_i, а другий раз без використання. Після чого реальне значення Q_i може бути знайдене за формулою

$$Q_i = \sum_{j=0}^{i=1} a'_j Q_j - \sum_{j=0}^{i=1} a''_j Q_j , \qquad (1)$$

де a'_j та a''_j — відповідно двійкові біти кодів результатів першого та другого перетворення.

З формули (1) випливає, що процес калібрування носить послідовний рекурентний характер, оскільки вага i-го розряду визначається вагами $i - 1$, $i - 2$, ..., 0, вага $(i + 1)$-го розряду вагами i, $i - 1$, ..., 0 і т. д. Таким чином параметри даного процесу суттєво впливають на загальну точність перетворювача, тому актуальним є дослідження похибок калібрування та визначення методичних похибок аналого-цифрового перетворення в процесі самокалібрування.

Процес самокалібрування характеризується накопиченням методичної похибки і носить складний характер, що визначається різними чинниками, зокрема такими як алгоритм калібрування, відхилення ваг «неточних» розрядів, основа системи числення тощо.

Таким чином можна записати

$$\varepsilon_i = f(A, i, \Delta Q, \alpha, A_д),$$

де A — алгоритм самокалібрування; i — номер розряду, що калібрується; ΔQ — масив відхилень ваг розрядів від $(n-m)$-го до i-го; α — система числення; $A_д$ — значення допоміжного сигналу.

При використанні алгоритму двократного врівноваження (формула 1) похибка самокалібрування молодшого «неточного» $(n - m)$-го розряду дорівнюватиме

$$\varepsilon_{n-m} = \varepsilon'_{n-m} - \varepsilon''_{n-m} , \qquad (2)$$

де ε'_{n-m} та ε''_{n-m} — значення похибок першого та другого врівноваження відповідно, які визначаються у вигляді

$$\varepsilon'_{n-m} = Q_{n-m} + A_д - \sum_{i=0}^{n-m-1} a'_i Q_i , \qquad (3)$$

$$\varepsilon''_{n-m} = A_д - \sum_{i=0}^{n-m-1} a''_i Q_i , \qquad (4)$$

де a'_i та a''_i — розрядні коефіцієнти при першому та другому врівноваженні відповідно. Після підстановки (3) та (4) в (2) отримаємо

$$\varepsilon_{n-m} = Q_{n-m} + \sum_{i=0}^{n-m-1} (a''_i - a'_i) Q_i . \qquad (5)$$

Відсутність в останньому виразі в явному вигляді $A_д$ не означає, що ε_{n-m} не залежить від $A_д$, оскільки a'_i та a''_i є функціями $A_д$.

Похибка калібрування довільного k-го розряду буде визначатись виразом

$$\varepsilon_k = Q_k + \sum_{i=0}^{k-1} (a''_i - a'_i) Q_i + \sum_{j=n-m}^{k-1} \left(\varepsilon_j(a''_j) - \varepsilon_j(a'_j)\right). \qquad (6)$$

В останньому виразі можна виділити дві складові. Перша з них є безпосередньо похибкою квантування, коли калібрується k-ий розряд

$$\varepsilon_{\text{кв. }k} = Q_k + \sum_{i=0}^{k-1}(a_i'' - a_i')Q_i \,. \tag{7}$$

Значення $\varepsilon_{\text{кв. }k}$ для даного алгоритму лежить в діапазоні ± 1 квант [6].

Друга складова — це сума похибок квантування, які накопичились на попередніх тактах калібрування

$$\varepsilon_{sk} = \sum_{j=n-m}^{k-1}\left(\varepsilon_j(a_j'') - \varepsilon_j(a_j')\right). \tag{8}$$

Доведено [6], що абсолютне значення ε_{sk} збільшується зі зростанням k, і в загальному випадку можна стверджувати, що при $k - (n - m) >> 1$ $|\varepsilon_{sk}| >> |\varepsilon_{\text{кв.}k}|$. З урахуванням останнього вираз (6) матиме вигляд

$$\varepsilon_k \approx \sum_{j=n-m}^{k-1}\left(\varepsilon_j(a_j'') - \varepsilon_j(a_j')\right). \tag{9}$$

Графічна інтерпретація залежності $\varepsilon_k(A_Д)$ для різних значень k показана на рис. 2.

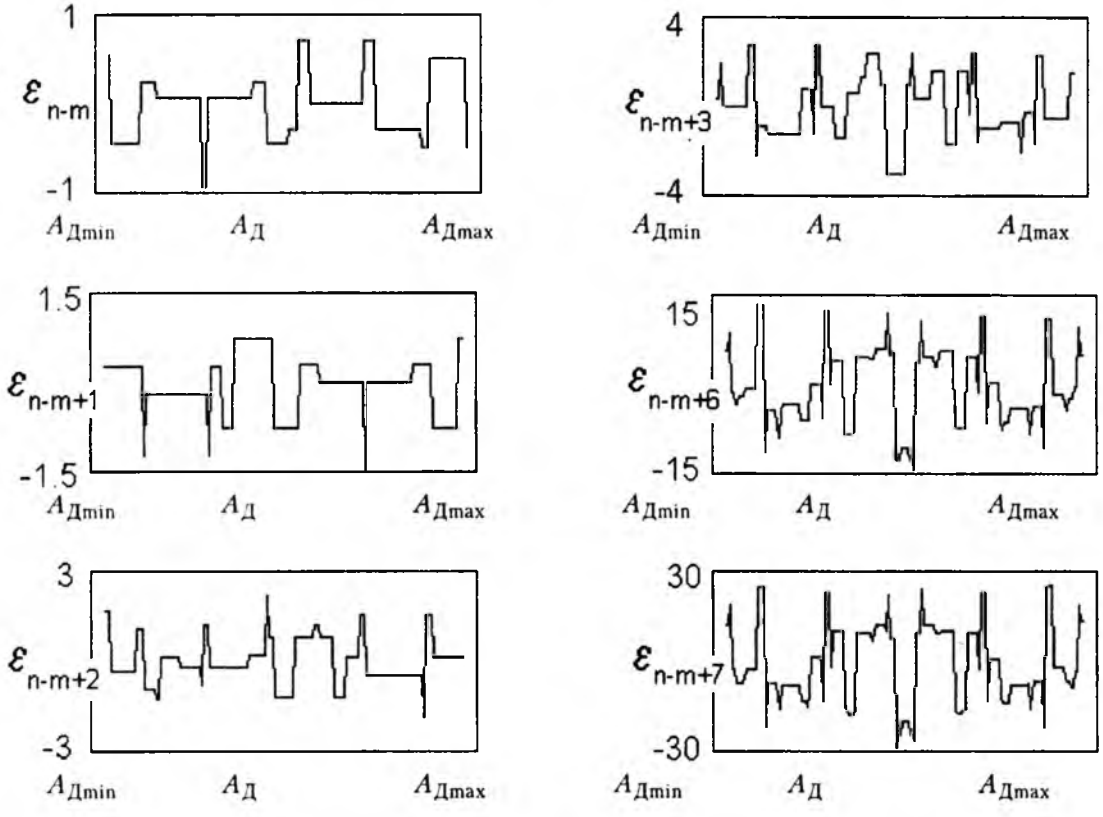

Рис. 2. Залежність ε_k від $A_Д$

Методична похибка самокалібрування приводить до появи двох типів похибки аналого-цифрового перетворення, а саме похибки масштабу та похибки нелінійності. Останні можуть бути розраховані за формулами (10) та (11)

$$k_m = \frac{\sum_{i=n-m}^{n-1}(\varepsilon_i + Q_i)}{\sum_{i=n-m}^{n-1} Q_i}, \tag{10}$$

$$\Delta_н = \sum_{i=n-m}^{n-1} \max\left\{\left|\varepsilon_i^+ + Q_i^+ + Q_i^+ k_m\right|,\ \left|\varepsilon_i^- + Q_i^- - Q_i^- k_m\right|\right\}, \tag{11}$$

де $\begin{cases}\varepsilon_i^+ = \varepsilon_i;\ Q_i^+ = Q_i;\ \varepsilon_i^- = 0;\ Q_i^- = 0, & \text{якщо } (\varepsilon_i + Q_i - Q_i k_m) \ge 0;\\ \varepsilon_i^+ = 0;\ Q_i^+ = 0;\ \varepsilon_i^- = \varepsilon_i;\ Q_i^- = Q_i, & \text{якщо } (\varepsilon_i + Q_i - Q_i k_m) < 0.\end{cases}$

Графічна інтерпретація залежностей $k_m(A_д)$ та $\Delta_н(A_д)$ зображена відповідно на рис. 3 та 4. Аналіз графіків на рис. 2—4 дає змогу зробити висновок, що значення ε_i, а як результат, і значення k_m та $\Delta_н$ змінюються зі зміненням значення допоміжного сигналу $A_д$, при цьому в діапазоні $A_д \in [A_{д\ min}; A_{д\ max}]$ значення ε_i приймають як додатні, так і від'ємні значення.

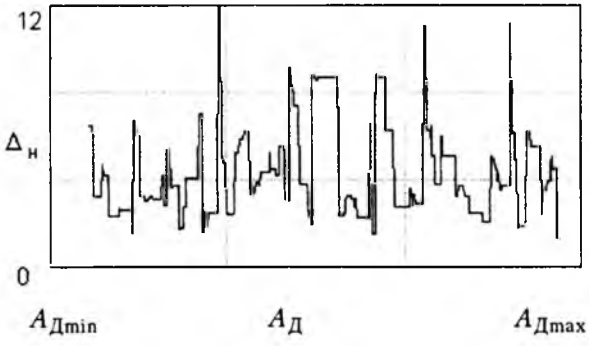

Рис. 3. Залежність $\Delta_н$ від $A_д$

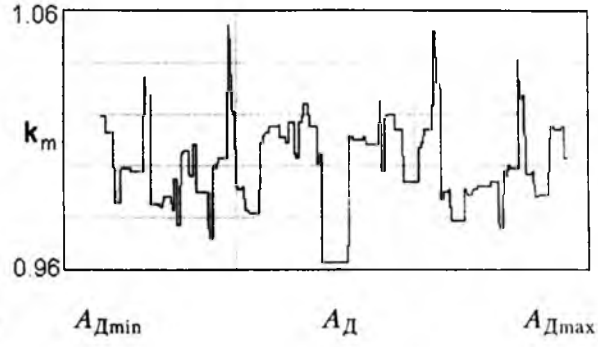

Рис. 4. Залежність k_m від $A_д$

Таким чином, якщо калібрування кожного розряду виконувати з різними значеннями $A_д$, і результат осереднювати за формулою

$$Q_{i\,oc} = \frac{\sum_{j=1}^{t} Q_i^j}{t},$$

де Q_i^j — значення i-го розряду, отримане в результаті калібрування з j-им значенням допоміжної величини $A_д$; t — кількість калібрувань i-го розряду, то сумарне значення методичної похибки може бути значно зменшене.

Залежності $k_m(A_д)$ та $\Delta_н(A_д)$, отримані після використання механізму осереднення, зображені на рис. 5 та 6 відповідно. З рис. 6 видно, що складова похибки нелінійності не перебільшує значення одного кванта в усьому діапазоні $A_{д\ min} \div A_{д\ max}$, та в більшості випадків знаходиться на рівні 0,5 кванта. Таким чином, використання додаткових розрядів при даному способі самокалібрування не має сенсу.

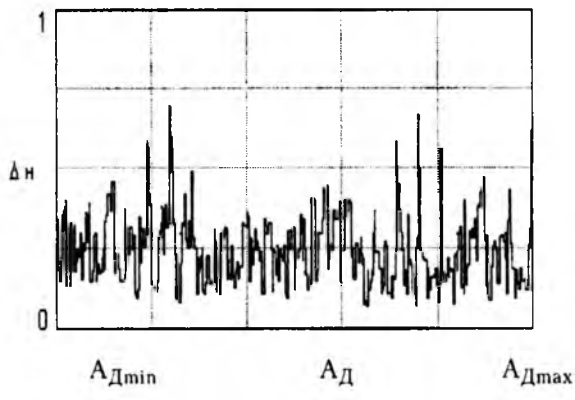

Рис. 5. Залежність $\Delta_н$ від $A_д$ після осереднення

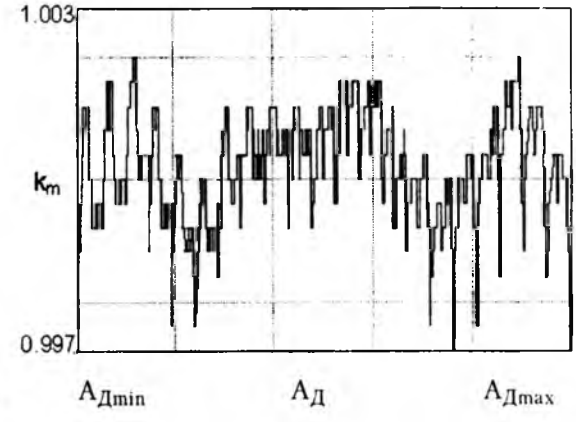

Рис. 6. Залежність k_m від $A_д$ після осереднення

Ефективність використання розглянутого принципу підвищення точності самокалібрування залежить від багатьох чинників, але найвпливовішими є значення $A_д$ та кількість калібрувань. Можуть бути використані різні підходи щодо вибору останніх. Найпростіший спосіб реалізації алгоритму з осередненням полягає в тому, що допоміжний аналоговий сигнал формується за допомогою додаткового малорозрядного ЦАП, причому ніякі спеціальні умови щодо його точності не висуваються. Одна із можливих структур блоку формування допоміжного сигналу (БФДС) зображена на рис. 7.

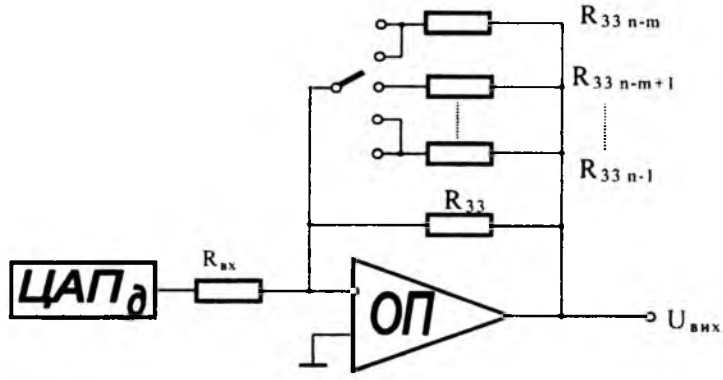

Рис. 7. Структура блоку формування допоміжного сигналу

Схема містить допоміжний малорозрядний ЦАП та операційний підсилювач зі змінним коефіцієнтом підсилення. Функція ОП — це масштабування вихідного сигналу ЦАП під час формування необхідних рівнів допоміжного сигналу $A_д$. Єдина вимога, що висувається до БФДС — значення $A_{дi}$ не повинні виходити за межі діапазону, який задається формулою

$$Q_i < A_{дi} < \sum_{j=0}^{i-1} Q_j .$$

Під час побудови АЦП на основі системи числення з розрядними коефіцієнтами $a_i \in \{1, \bar{1}\}$, структура БФДС значно спрощується. Це пояснюється тим, що в даному випадку всі розряди можуть бути відкалібровані за допомогою одного і того ж масиву допоміжних сигналів $A_д$ [6].

Визначення ефективного значення приросту допоміжного сигналу $\Delta A_д$, яке задається вагою молодшого розряду ЦАП$_д$, може бути виконане методом імітаційного моделювання процесу аналого-цифрового перетворення. Так дослідження показали, що значення $\Delta A_{д\ опт}$ (тобто значення, при якому задана точність досягається за мінімальну кількість калібрувань t) дорівнює приблизно 0,5 ÷ 0,7 ваги молодшого розряду основного ЦАП. А ефективна кількість калібрувань t (тобто кількість калібрувань, з якою суттєво покращуються характеристики) дорівнює приблизно 7 ÷10. Причому вищезгадані показники практично ніяк не залежать від значень відхилень розрядів, що калібруються ΔQ_i.

Слід відзначити, що використання однакової кількості калібрувань для всіх розрядів, що калібруються, не є доцільним. Це пояснюється тим, що вплив похибки калібрування різних розрядів на загальну точність калібрування є різним. Так, наприклад, похибка калібрування першого з «неточних» розрядів не впливає ніяким чином на інші розряди. Отже, для зменшення загального часу калібрування без суттєвого зменшення точності доцільно зменшувати кількість калібрувань t від першого «неточного» до останнього «неточного» розряду.

Висновки

— аналіз процесу накопичення методичної похибки самокалібрування показав, що значення останньої суттєво залежить від величини допоміжного сигналу і приймає як додатні, так і від'ємні значення;

— використання алгоритму багаторазового калібрування з осередненням дає змогу значно зменшити результатну похибку самокалібрування. Внаслідок цього, існує змога зниження кількості додаткових розрядів, до яких висуваються вимоги щодо точності та метрологічної стабільності.

ЛІТЕРАТУРА

1. Tan K. S. On board self-calibration of analog-to-digital and digital-to-analog converters // U. S. Patent 4399426. — 1983. — Aug. 16

2. Hae-Seung Lee, David A. Hodges, Paul R. Gray. A Self-calibriting 15-bit CMOS A/D Converter // IEEE J. Solid-State Circuits. — 1984. — Dec. — Vol. 19, № 6. — P. 813—817.

3. Khen-Sang Tan, Sami Kiriaki, Michiel de Wit. Error correction techniques for high-performance differential A/D Converters // IEEE J. Solid-State Circuits. — 1990. — Dec. — Vol. 25, № 6. — P. 1318—1327.

4. Bergman G. A. Number system with with an irrational base // Mathematics Magazine. — 1953. — № 3. — P. 98—119.

5. Азаров А. Д. Разработка теории аналого-цифрового преобразования на основе избыточных позиционных систем счисления. — Автореф. дис... канд. техн. наук. Винница, 1997. — 44 с.

6. Захарченко С. М. Исследование и разработка самокалибрующихся АЦП с накоплением заряда на основе избыточных позиционных систем счисления. — Автореф. дис... канд. техн. наук. — Винница, 1997. — 16 с.

Рекомендовано кафедрою обчислювальної техніки

Надійшла до редакції 2.12.99 р.
Рекомендована до опублікування9.12.99 р.

Азаров Олексій Дмитрович — завідувач кафедри обчислювальної техніки ВДТУ, ***Біліченко Наталія Олександрівна*** — асистент кафедри обчислювальної техніки ВДТУ, ***Захарченко Сергій Михайлович*** — старший викладач кафедри обчислювальної техніки ВДТУ.

УДК 681.3.067

ГЕНЕРАТОРИ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ *p*-ІНВЕРСІЙ

Асп. Яремчук Є. В.

Вступ

Серед алгоритмів криптографічного захисту інформації виділяють клас алгоритмів, які побудовані на основі послідовностей псевдовипадкових чисел [1—3]. Вони є найпоширенішими завдяки тому, що дозволяють отримувати послідовності великої довжини з порівняно коротким розміром ключа та відносній простоті програмної реалізації. В таких алгоритмах операції шифрування та дешифрування передбачають накладання псевдовипадкової послідовності або гами на відкритий текст за певним законом. Як правило, в основу закону накладання гами покладена побітна операція додавання за модулем 2, що дозволяє виконувати зашифрування і дешифрування однаково.

Таким чином, основною задачею під час реалізації алгоритму такого типу є розроблення ефективного алгоритму генерування послідовностей псевдовипадкових чисел на основі секретного ключа.

Основні положення

Найкращими з відомих на сьогодні є лінійні конгруенц-генератори псевдовипадкових чисел, які породжують послідовність за модулем m та періодом, що не перевищує m. Деякі поліпшені схеми дозволяють отримати послідовності з періодом m^2 або навіть більшим [4—5].

В даній статті пропонується генератор, який побудований на основі використання перестановок послідовності $\langle S \rangle = \{s_0, s_1, \ldots, s_{m-1}\}$ за модулем m.

Як відомо, існує $m!$ перестановок такої послідовності. Якщо записати їх послідовно одна за одною, отримаємо послідовність

$$\langle W \rangle = \{S_0, S_1, \ldots, S_n\}, \quad n = m! - 1, \tag{1}$$