2 дугами.

Побудова прикладу: D має вигляд повного орграфа з вагами дуг строго більшими від одиниці.

Доведення. Візьмемо початковий імпульс з усіма додатними компонентами. Оскільки усі ваги дуг D додатні і строго більші за одиницю, то довільний цикл D буде нескінченно збільшувати імпульс на своїх вершинах. Зокрема нескінченно збільшувати імпульс будуть усі петлі (u', u') і усі цикли виду: (u', v'), (v', u'). Тому, щоби зробити імпульсний процес стійким на D, потрібно принаймні видалити усі петлі і по одній дузі з кожного циклу виду: (u', v'), (v', u'); для цього потрібно видалити не менше ніж $C_n^2 + n$ дуг. Виконаємо дані дії і запишемо матрицю ваг орграфа D^*:

$$\begin{vmatrix} 0 & a_{21} & . & . & a_{1n} \\ 0 & 0 & a_{23} & . & . \\ . & . & . & . & . \\ . & . & . & 0 & a_{n-1\,n} \\ 0 & . & . & 0 & 0 \end{vmatrix}$$

Очевидно, що власні значення даної матриці усі дорівнюють нулю, отже ми отримали орграф D^*, який є імпульсно стійкий для всіх імпульсних поцесів.

1. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. М., 1986
2. Ланкастер П. Теория Матриц. М., 1982
3. Оре О. Теория графов. М., 1980

УДК 621.372.542: 376.56

АЛГОРИТМИ І СТРУКТУРИ АДАПТИВНОГО РІЗНИЦЕВОГО КОДУВАННЯ З ПОПЕРЕДЖЕННЯМ ПЕРЕНАВАНТАЖЕННЯ ЗА КРУТИЗНОЮ

© І. Стрепко[1], О. Тимченко[2]
[1] Українська академія друкарства
[2] Національний університет "Львівська політехніка"

На основі аналізу методів адаптації різницевого кодування розроблені нові алгоритми та структурні схеми кодерів з попередженням перенавантаження за крутизною, що мають ефективну апаратну реалізацію.

Because of of analysis of methods of adaptation of difference coding the new algorithms and block diagrams of encoders with warning of transhipment on a steepness are developed which have effective hardware realization.

Вступ

Різноманітні різницеві методи подання і обробки сигналів широко застосовуються в цифрових системах керування [1, 2], передачі і стиску даних тощо. Вхідним елементом таких систем є кодер, який забезпечує перетворення вхідного, в основному аналогового, сигналу у відповідний код. Точність і швидкодія цього вузла великою мірою задає точність і швидкодію всієї системи обробки. Тому питанням вибору алгоритмів кодування і функціонування кодерів слід надавати велику увагу.

Залежно від виду кодування можна отримати або більш простий процесор системи обробки, або відповідно збільшити його швидкодію. При цьому необхідно перетворювати в код, як правило, нестаціонарний сигнал.

Характеристика квантувача лінійної (однорозрядної) дельта-модуляції (ДМ) є рівномірною і забезпечує при відсутності перенавантаження за крутизною однакову точність апроксимації в будь-якій точці діапазону зміни сигналу D [1]. При адаптивній обробці [2-4] часто також застосовуються інші характеристики квантування, наприклад, експоненційні та нелінійні. Останні, як правило, враховують статистичні та інші особливості джерела та приймача інформації. Для виконання адаптації в різницевих методах кодування сигналів необхідно змінювати параметри кодерів відповідно до вхідного сигналу. Проте при обробці нестаціонарних сигналів важко забезпечити високу точність кодування простими апаратними засобами. Саме тому доцільно застосовувати спрощені алгоритми, які при незначній втраті точності значно простіші в реалізації.

Аналіз методів адаптації кодерів

Експоненційні квантувачі (квантувачі з експоненційною зміною величини кроку) застосовуються у випадку адаптивного подання з ДМ (АДМ) та диференціальною імпульсно-кодовою модуляцією (АДІКМ) для обробки нестаціонарних випадкових процесів і забезпечують рівнократну зміну величини кроку квантування залежно від різницевого сигналу – приросту $\alpha_i^{(x)} = x_i - \hat{x}_i$ між відліками вхідного $\{x_i\}$ і апроксимуючого $\{\hat{x}_i\}$ сигналів в даному і попередньому періодах дискретизації. Для всіх видів АДМ та АДІКМ регулюється крок квантування при різкій зміні значення вхідного сигналу, яке не може бути оброблене кодером з постійним кроком:

$$s_i^{(x)} = E_i^{(x)} \left| s_i^{(x)} \right| = p_i^{(x)} \left| s_{\min}^{(x)} \right|, \qquad (1)$$

де $E_i^{(x)} = \operatorname{sgn}(\alpha_i^{(x)})$ – знак приросту, $p_i^{(x)}$ – цифровий еквівалент.

Величина $p_i^{(x)}$ в (1) вибирається аналізом попередніх значень кроків згідно з вибраним алгоритмом адаптації.

Метод АДІКМ найкраще підходить для обробки нестаціонарних сигналів [1]. В цьому випадку багаторівневий квантувач кодера виконується адаптивним, а в колі зворотного зв'язку апроксиматор реалізують на основі накопичення.

Розмір кроку при АДІКМ змінюється у відповідності з величиною різницевого сигналу $\alpha_i^{(x)} = x_i - \hat{x}_i$ та аналізу попереднього кроку $p_{i-1}^{(x)}$ так:

$$p_i^{(x)} = \mathrm{sgn}(\alpha_i^{(x)}) \begin{cases} 2p_{i-1}^{(x)}, \left|\alpha_i^{(x)}\right| > DQ\left|p_{i-1}^{(x)}\right|; \\ p_{i-1}^{(x)}/2, \left|\alpha_i^{(x)}\right| \le DQ\left|p_{i-1}^{(x)}\right|; \end{cases} \quad (2)$$

де $D = 2^{c^{(x)}}$ – діапазон зміни сигналу, $Q = k_n / 2D, k_n \in \{1, D\}$ – параметр порогу адаптації, $C^{(x)}$ – розрядність кроків квантування.

Позначимо через $s_0^{(x)} = s_{\min}^{(x)} 2^{c^{(x)}/2}$ – центральний розмір кроку. Тоді з (2) маємо, що

$$\left|s_n^{(x)}\right| = s_0^{(x)} 2^{q_n},$$

де $q_n \in \{-c^{(x)}/2, c^{(x)}/2\}$.

Тому кодер АДІКМ із вказаною характеристикою квантування обробляє сигнал, що змінюється в широкому динамічному діапазоні, формуючи низькорозрядний код вихідного сигналу:

$$s_n^{(x)} = \mathrm{sgn}(\alpha_n^{(x)}) s_0^{(x)} 2^{q_n}, \quad \{s_n^{(x)}\} \Rightarrow \{E_n^{(x)}, q_n\}. \quad (3)$$

Послідовність кроків квантування при АДІКМ кодується бітом знака та показником експоненти (3). Це дозволяє зменшити число бітів подання при обробці широкосмугових сигналів. Проте оптимальне значення параметра адаптації $Q \neq 2$, що погіршує точність кодування нестаціонарних сигналів і вимагає виконання цілого ряду вузлів кодера в аналоговому вигляді.

Розробка алгоритмів адаптації на основі аналізу кодованої послідовності

Аналіз послідовностей (1)-(3) дозволяє запропонувати ефективний метод цифрової адаптації кодерів при різкій зміні вхідного, наприклад, нестаціонарного сигналу, на основі аналізу кодованої послідовності $\{p_i^{(x)}\}$. Він полягає в наступному. При перенавантаженні за крутизною на виході кодера з постійним кроком квантування $s_{min}^{(x)}$ формується послідовність, що містить $q > 1$ однакових символів, які позначимо через $\{B_{1,n}^{(x)}\}$. При додатній крутизні сигналу апроксимації це значення кодується як $\{B_{1,n}^{(x)}\} = \{1\}$, а при від'ємній $\{B_{1,n}^{(x)}\} = \{0\}$. Застосуємо цю ознаку початку перенавантаження для вироблення сигналу адаптації (в даному випадку для формування сигналу додаткової корекції апроксимуючого сигналу):

$$d_n^{(x)} = ENT\left(\frac{\alpha_n^{(x)}}{s_{\min}^{(x)}}\right), \left|d_n^{(x)}\right| > 1. \quad (4)$$

Відповідна корекція сигналу апроксимації буде мати вигляд

$$\hat{x}_n = \hat{x}_{n-1} + d_n^{(x)} s_{\min}^{(x)}. \quad (5)$$

Це еквівалентне прив'язці вихідного коду до величини сигналу апроксимації в n-му такті незалежно від наявності перенавантаження. Отже, згідно з (5) сигнал апроксимації $\hat{x}_n$ коректується на квантоване значення стрибка вхідного сигналу $d_n^{(x)} s_{\min}^{(x)}$ за

період дискретизації (4). Такий сигнал не може бути відслідкований без перенавантаження кодером з постійним кроком $s_{\min}^{(x)}$.

Ширина спектра сигналу, оброблюваного кодером із вказаним алгоритмом адаптації, збільшується і визначається мінімально допустимою крутизною вхідного сигналу

$$S_{\max}^{(ADIKM)} = d_{\max}^{(x)} s_{\min}^{(x)} / qT \,. \qquad (6)$$

Позначимо через μ співвідношення між верхньою частотою спектра оброблюваного без перенавантаження за крутизною вхідного сигналу і частотою Найквіста. Тоді з використанням (6) визначимо розширення смуги частот за рахунок даного виду адаптації

$$\frac{\mu^{(ADIKM)}}{\mu^{(DIKM)}} = \frac{\pi U_m}{s_{\min}^{(x)}} \Bigg/ \frac{\pi}{2\arcsin\left(\dfrac{d_{\max}^{(x)} s_{\min}^{(x)}}{2qU_m}\right)} \approx \frac{d_{\max}^{(x)}}{q} \,. \qquad (7)$$

В останньому виразі прийнято, що кількість q розташованих підряд однакових символів визначають із статистичних властивостей сигналів та необхідного значення (7). Це відповідає відповідному збільшенню швидкодії кодера при заданій точності апроксимації.

Аналогічно запропонований метод можна застосувати в кодерах з іншими адаптивними видами різницевого подання. Наприклад, у випадку формування багаторівневого коду момент початку перенавантаження за крутизною фіксується після q розміщених підряд кроків з максимальним модулем $s_{\min}^{(x)}$. Корегуючий код має значення

$$d_n^{(x)} = ENT\left(\frac{\alpha_n^{(x)}}{s_{\max}^{(x)}}\right).$$

Його використовують, як описано раніше, для корекції сигналу апроксимації, а кодер обробляє сигнали з відповідною шириною смуги (7).

Необхідні обмеження діапазону зміни сигналу D для забезпечення стійкості цифрових кодерів враховуються відповідним виконанням суматора з накопиченням в колі зворотного зв'язку [2].

Даний метод не може бути застосований до АДМ безпосередньо, оскільки при цьому виді квантування і виконанні умови $|s_n^{(x)}| < s_{\min}^{(x)}$ значення $s_n^{(x)} \neq s_{n-1}^{(x)}$ для будь-якого n. Тому для реалізації адаптації з АДМ необхідно виключити перехідний процес, який займає час

$$t \le 2c^{(s)}T \,,$$

або $2c^{(s)}$ тактів. Після цього при перенавантаженні наступає рівність $s_n^{(x)} = s_{\max}^{(x)}$ і застосовується запропонований метод.

Реалізація методу адаптації для однорозрядного подання

Найбільш проста реалізація запропонованого методу адаптації у випадку однорозрядного подання вихідного коду. Кодер, що працює за запропонованим методом і

має постійний крок квантування (рис.1а), містить генератор *G* тактових імпульсів, алгебраїчний суматор, дворівневий квантувач, апроксиматор, побудований на реверсивному лічильнику СТ і перетворювач - ЦАП (D/A), селектор *SI* серій імпульсів, блок прив'язки рівня, виконаний на основі низькорозрядного аналогоцифрового перетворювача - АЦП (A/D) і суматора *SM*. На рис.1б показані основні сігнали кодера: $x(t)$ - аналоговий вхідний сигнал, $\{B_{1,n}^{(x)}\}$, для будь-якого $B \in \{0,1\}$ - вихідна однорозрядна кодова послідовність, $\{d_k\}$ - послідовність сигналу адаптації, $\{B_n^{(x)}\}, \hat{x}(t)$ - код сигналу і сигнал апроксимації.

При відсутності перенавантаження за крутизною стеження за вхідним сигналом здійснюється звичайно так: при збільшенні $x(t)$ квантувач формує $B_{1,i}^{(x)}=1$, що приводить до збільшення вмісту лічильника СТ - формуванню більшого значення сигналу апроксимації $\hat{x}(t)$. Аналогічні процеси проходять при зменшенні $x(t)$.

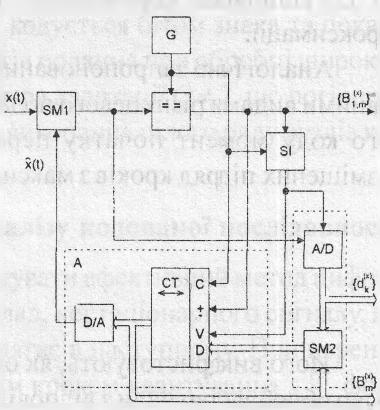
Кодер адаптується залежно від параметрів вхідного сигналу так.

Якщо кількість послідовних символів (0 або 1) у вихідній послідовності перевищує задану величину $q>1$ (на рис.1б $q=4$), тобто крутизна вхідного сигналу $x(t)$ перевищує або дорівнює максимальній швидкості зміни сигналу апроксимації $\hat{x}(t)$, то на виході селектора *SI* формується керуючий сигнал, який запускає АЦП A/D. На інформаційний вхід останнього подається сигнал різниці $\alpha^{(x)}(t) = x(t) - \hat{x}(t)$.

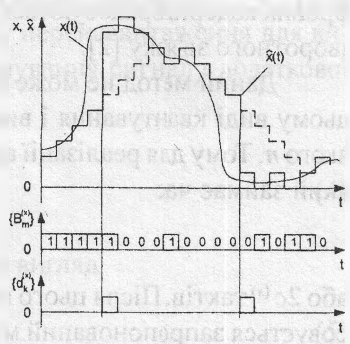
Цей сигнал за імпульсом з блоку *SI* перетворюється в код $d^{(x)} = \mathrm{ENT}(\alpha^{(x)}(t)/s_{\min}^{(x)})$ (необхідно, щоби АЦП мав рівномірну характеристику з мінімальним дискретом $s_{\min}^{(x)}$). Значення $|d^{(x)}| \geq q$ подається на суматор SM, на другі входи якого подано значення коду апроксимації $\{B_m^{(x)}\}$ з виходів лічильника СТ. Після додавання вказаних сигналів результат записується в лічильник СТ, в результаті чого коригується сигнал апроксимації $\hat{x}(t)$ на значення стрибка $\{d^{(x)}, s_{\min}^{(x)}\}$, який не може бути відпрацьований за допомогою кодера з постійним кроком квантування $s_{\min}^{(x)}$.

Отже, значення сигналу апроксимації і вихідного коду завжди відповідає значенню вхідного сигналу, що забезпечує високу точність обробки. При необхідності отримання вихідного повнорозрядного ІКМ-коду з частотою Найквіста відповідну послідовність проріджують в $\mu_{A/D/IKM}$ разів.

Для збільшення швидкодії схеми адаптації можна зафіксувати величину коригуючого коду. Це значення дорівнює $d^{(x)} = \mathrm{sgn}[\alpha^{(x)}]q$ у випадку однорозрядного різницевого подання і $d^{(x)} = \mathrm{sgn}[\alpha^{(x)}]q$ $s_{\max}^{(x)}$ для багаторозрядного і може формуватись безпосередньо, без використання АЦП. Зазначимо, що в даному випадку точність адаптації обмежена значенням мінімального кроку $\pm s_{\min}^{(x)}$, тому що не враховує початкової величини коду на виході



а)



б)

Кодер з попередженням перенавантаження за крутизною:
а) структурна схема; б) часові діаграми

квантувача. Ще одним методом збільшення швидкодії схеми адаптації є фіксація моментів адаптації. Проте в цьому випадку можлива початкова похибка перехідного режиму, яка після спрацьовування схеми адаптації швидко зменшується до значення мінімального кроку $\pm s_{min}^{(x)}$.

Поєднання обох методів збільшення швидкодії схеми адаптації призводить до максимально простої схеми, в якій повністю відсутній АЦП. Значення початкової похибки перехідного режиму може становити $\pm s_{max}^{(x)}$, яке в процесі адаптації зменшується до відповідно до $\pm s_{min}^{(x)}$.

Висновки

Застосування спрощених алгоритмів адаптації при кодуванні нестаціонарних сигналів із заданою точністю призводить до максимально простих реалізацій кодерів, які можуть з успіхом застосовуватись для обробки сигналів різної природи.

1. Тимченко О.В. Різницеві методи цифрової фільтрації. Львів, 1999.
2. Дурняк Б.В., Стрепко І.Т., Тимченко О.В. Алгоритми швидкодіючих систем реального часу, побудованих на основі різницевих підходів // Вісник ДУ "Львівська політехніка". 1999. №366. С.56-62.
3. Стрепко І.Т., Тимченко О.В., Дурняк Б.В. Проектування систем керування на однокристальних мікроЕОМ. К., 1998.
4. Дурняк Б., Стрепко І., Тимченко О. Розпаралелювання обчислень на основі вибору методів різницевого подання сигналів в САК реального часу // Комп'ютерні технології друкарства. Львів, 1998. С.120-123.

УДК 681.325

ТАБЛИЧНА РЕАЛІЗАЦІЯ ФУНКЦІЙ ПЕРЕТВОРЕННЯ В ПРОЦЕСОРІ ШИФРУВАННЯ ДАНИХ ЗА АЛГОРИТМОМ AES

© А. Мельник, С. Прудкий
Національний університет "Львівська політехніка"

Розглянуто алгоритм криптографічного захисту інформації за стандартом AES, основні проблеми, що виникають при його реалізації, а також запропоновано підходи до табличного обчислення основних перетворень алгоритму та скорочення обсягу таблиць.

The AES cryptographic algorithm of information protection and main problems that arise during its applications are considered. The approaches to look-up table calculation of the algorithm basic transformations and reduction of tables volume are offered.