2. Okeya K., Schmidt-Samoa K., Spahn C., Takagi T. Signed Binary Representations Revisited, in *«Advances in Cryptology. CRYPTO 2004»*, Lecture Notes in Computer Science 3152 (2004), P. 123–139.
3. Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL): [Електронний ресурс]. Режим доступу: https://github.com/miracl/MIRACL
4. Solinas J. A. Low-Weight Binary Representations for Pairs of Integers, Technical Report CORR 2001-41, University of Waterloo, 2001. 23 p. Режим доступу: http://cacr.uwaterloo.ca/techreports/2001/corr2001-41.ps
5. Dimitrov V., Jullien G., Muscedere R. Multiple-Base Number System: Theory and Applications. CRC Press, 2012. 294 p.

This paper presents functions addresses substitutions «trick» combining with data substitutions. This computational technique allows to eliminate conditional branches and thus to improve timing results for many algorithms, such as elliptic curve arithmetic algorithms. In this paper proposed technique is shown on simplest examples of several elliptic curve point multiplication algorithms with multiprecision integers signed digit representations. But it can give better results combined with more complicated highly branched algorithms.

Key words: *signed digit representations, elliptic curve arithmetic, elliptic curve point multiplication, elliptic curve cryptography, algorithm complexity.*

Одержано 20.02.2017

УДК 519.642

Л. В. Мосенцова, канд. техн. наук

Физико-технологический институт металлов и сплавов
НАН Украины, г. Киев

ЧИСЛЕННО-АНАЛИТИЧЕСКИЙ АЛГОРИТМ ИНТЕРПРЕТАЦИИ В ЗАДАЧЕ ВОССТАНОВЛЕНИЯ СИГНАЛА

Представлен численно-аналитический алгоритм интерпретации в задаче восстановления сигнала. Алгоритм состоит в преобразовании нелинейных интегральных уравнений типа Вольтерра I рода к уравнениям типа Вольтерра II рода и их численного решения путем применения алгоритма «естественной интерполяции».

Ключевые слова: *нелинейные интегральные уравнения типа Вольтерра I рода, задача восстановления сигнала, интерпретация результатов.*

Введение. Моделями динамической интерпретации результатов в задачах восстановления сигналов являются уравнения типа Вольтерра I рода, в частности нелинейные [1]. Отличительная особенность данного

класса задач заключается в проведении при их решении исследований на стыке традиционных численных методов и методов решения некорректных задач. С одной стороны, нелинейные интегральные уравнения Вольтерра I рода являются частным случаем нелинейных уравнений Фредгольма I рода и требуют тем самым применения соответствующих классических методов регуляризации [2]. С другой стороны, при некоторых ограничениях, например, при «хорошей» гладкости правой части и ядра, нелинейные уравнения типа Вольтерра I рода допускают непосредственное применение классических методов [3] (например, метода квадратур, причем сама процедура дискретизации в этом случае обладает регуляризирующим свойством, если связать шаг дискретизации с ошибкой исходных данных). Рассмотрим еще два способа преодоления сложностей, возникающих при решении нелинейных интегральных уравнений Вольтерра I рода, которые основываются на преобразовании их к уравнениям Вольтерра II рода.

Приведение нелинейных интегральных уравнений типа Вольтерра первого рода к уравнениям второго рода посредством дифференцирования. Рассмотрим нелинейное интегральное уравнение типа Вольтерра I рода вида

$$Ay \equiv \int_a^x K(x,s)F(y(s))ds = f(x),\ s \in [a,b],\ x \in [a,b], \qquad (1)$$

где $K(x,s)$ — ядро; $f(x)$ — правая часть; $y(s)$ — искомая функция.

Если правая часть и ядро уравнения (1) имеют производные $f'_x(x)$ и $K'_x(x,s)$, то продифференцировав обе части (1) по x, получим выражение

$$K(x,x)F(y(x)) + \int_a^x K'_x(x,s)F(y(s))ds = f'(x), \qquad (2)$$

или, в ином виде,

$$F(y(x)) + \int_a^x \frac{K'_x(x,s)}{K(x,x)}F(y(s))ds = \frac{f'(x)}{K(x,x)},$$

которое представляет собой нелинейное интегральное уравнение типа Вольтерра-Гаммерштейна II рода и имеет то же решение, что и (1). Таким образом, если выполнено условие $K(x,x) \neq 0$, то переход к уравнению (2) дает возможность применить методы решения уравнений второго рода.

Если $K(x,x) = 0$, то уравнение (2) является опять уравнением первого рода, с которым можно поступить так же, как с уравнением (1), если только правая часть имеет непрерывную вторую производную $f''_x(x)$,

а ядро допускает непрерывную вторую производную $K''_x(x,s)$. Дифференцирование (2) (при выполнении этих условий) дает

$$K'_x(x,x)F(y(x))+\int_a^x K''_x(x,s)F(y(s))ds = f''(x)\,.$$

Если $K'_x(x,x)\neq 0$, то это уравнение второго рода. Если же $K'_x(x,x)=0$, то можно применить дифференцирование и т. д. При p-кратном дифференцировании получается уравнение

$$K^{(p-1)}(x,x)F(y(x))+\int_a^x \frac{\partial^p K(x,s)}{\partial x^p}F(y(s))ds = f^{(p)}(x)\,, \qquad (3)$$

которое при $K^{(p-1)}(x,x)\neq 0$ является уравнением второго рода.

Приведение нелинейных интегральных уравнений типа Вольтерра первого рода к уравнениям второго рода посредством интегрирования по частям. Пусть

$$\int_a^x F(y(s))ds = Y(x),\ \ x\in[a,b]$$

и выполним интегрирование по частям в (1), обозначив $u=K(x,s)$, $dv=F(y(s))ds$, получим

$$K(x,x)Y(x)-\int_a^x K'_x(x,s)Y(s)ds = f(x)\,,\ x\in\left[a,b\right].$$

Поскольку $K(x,x)\neq 0$, $x\in\left[a,b\right]$, то

$$Y(x)-\int_a^x \frac{K'_x(x,s)}{K(x,x)}Y(s)ds = \frac{f(x)}{K(x,x)}\,,\ x\in\left[a,b\right], \qquad (4)$$

т. е. получено интегральное уравнение Вольтерра II рода. После его решения относительно $Y(s)$ искомая функция $y(s)$ будет найдена из нелинейного уравнения

$$F(y(s))=\frac{dY(s)}{ds}\,,\ s\in\left[a,b\right].$$

Выбирая способы для преобразования уравнения, будем исходить из таких их особенностей:

- при использовании способа интегрирования по частям требуется вычислять $K'_t(x,t)$ и $Y'_t(t)$;
- способ дифференцирования требует дифференцирования двух функций по x: $f'(x)$ и $K'_x(x,t)$.

В зависимости от условий конкретной задачи (недифференцируемость или дифференцируемость f и K и т. д.) можно применять тот или иной способ.

Далее для решения интегрального уравнения типа Вольтерра II рода, полученного одним из способов преобразования, будем использовать следующий алгоритм.

Алгоритм «естественной» интерполяции для нелинейных интегральных уравнений типа Вольтерра II рода. Пусть имеется некоторая непрерывная динамическая модель, описываемая операторным уравнением II рода

$$y = Ay + f\ , \tag{5}$$

где A — оператор, $y \in Y$, $f \in F$, Y и F — некоторые метрические пространства. При численном решении уравнение (5) заменяют аппроксимирующим уравнением

$$\tilde{y}^h = \tilde{A}^h \tilde{y}^h + \tilde{f}^h, \tag{6}$$

где $\tilde{A}^h$ — оператор, зависящий от шага сетки h, $\tilde{y} \in Y_h$, $\tilde{f}^h \in F_h$, а Y_h и F_h – конечномерные пространства.

Методом естественной интерполяции назовем численный алгоритм получения аппроксимирующей функции $\varphi(x)$ из операторного уравнения

$$\varphi^{h_1} = \tilde{A}_1^{h,h_1} \tilde{y}^h + \tilde{f}^{h_1}\ , \tag{7}$$

где $\tilde{A}_1^{h,h_1}$ — нелинейный оператор (в общем случае), зависящий от шагов сеток h и h_1, $h_1 < h$, $\varphi^{h_1} \in \Phi_{h_1}$, Φ_{h_1} — конечномерное пространство.

Пусть задано нелинейное интегральное уравнение типа Вольтерра II рода

$$y(x) - \int_a^x K(x,s)F(y(s))ds = f(x) \tag{8}$$

с ядром $K(x,s)$ и известно его приближенное решение $\tilde{y}(x_i)$ на отрезке $[a;b]$ в точках x_i, $i = \overline{1,n}$.

Из исходного уравнения (8) можно получить аналитическое выражение для приближенного решения, заменив непрерывную переменную x дискретным множеством точек x_i:

$$\tilde{y}(x_i) = f(x) + \int_a^{x_i} K(x_i,s)F(y(s))ds + \Delta y(x_i),$$

где $\Delta y(x_i)$ — погрешность приближенного решения.

Заменяя подинтегральную функцию $y(s)$ аппроксимирующей функцией $\psi(s)$, полученной с помощью лагранжевой интерполяции приближенного решения ($\psi(s) = \tilde{y}(s)$ при $s = x_i$), и полагая погрешность приближенного решения малой величиной, получим формулу естественной интерполяции:

$$\varphi(x_j) = f(x_j) + \int_a^{x_j} K(x_j, s)F(\psi(s))ds\ ,\ x_j \in [a,b]\,. \tag{9}$$

Заменив интегральный оператор в формуле (9) конечной суммой, получим окончательное выражение для вычисления $\varphi(x_j)$, что эквивалентно использованию метода квадратур [4] для численного решения уравнения (8).

$$\varphi(x_j) = f(x_j) + A_j \sum_{l=1}^{j} K(x_j, x_l)F(\psi(x_l)), \tag{10}$$

где A_j — коэффициенты квадратурной формулы. В случае применения формулы трапеции (10) принимает вид

$$\begin{gathered}\varphi_1 = f_1, \varphi_2 = \frac{f_2 + \frac{h_2}{2}K_{21}}{1 - \frac{h_2}{2}K_{22}}, \\ \varphi_k = \frac{f_k + \frac{h_2}{2}K_{k1} + \sum_{l=2}^{k-1}\left(\frac{x_{l+1} - x_{l-1}}{2}\right)K_{kl}}{1 - \frac{h_k}{2}K_{kk}},\ k = \overline{1,m},\end{gathered} \tag{11}$$

где $\varphi(x_k) = \varphi_k$, $f(x_k) = f_k$, $K(x_k, x_l)F(\psi(x_l)) = K_{kl}$, $h_k = x_k - x_{k-1}$, а значение m определяется по формуле

$$m = n_1 + n_2\,,$$

где n_1 — количество точек вектора исходного решения, для которых должно выполняться условие $x_i < x_j$, n_2 — количество точек, для которых выполняется интерполяция.

Далее проиллюстрируем предложенный численно-аналитический алгоритм на примере решения следующего уравнения.

Пример. Задано уравнение

$$\int_0^x \sin(x-s)y^2(s)ds = \exp(\frac{x^2}{2}) - 1\,,$$

дифференцирование которого дает

$$\sin(x-x)y^2(x)+\int_0^x \cos(x-s)y^2(s)ds = x\exp(\frac{x^2}{2}).$$

Поскольку $\sin(x-x)=0$, то имеем уравнение первого рода

$$\int_0^x \cos(x-s)y^2(s)ds = x\exp(\frac{x^2}{2}),$$

дифференцирование которого позволяет получить требуемое уравнение второго рода

$$y^2(x)-\int_0^x \sin(x-s)y^2(s)ds = (1+x^2)\exp(\frac{x^2}{2}),$$

эквивалентное исходному уравнению. Далее, применяя алгоритм «естественной» интерполяции к уравнению второго рода, получаем численное решение нелинейного интегрального уравнения типа Вольтерра I рода.

Выводы. Применение аналитических способов дифференцирования и интегрирования по частям позволяет привести нелинейные интегральные уравнение типа Вольтерра I рода к уравнениям типа Вольтера II рода. Использование алгоритма «естественной» интерполяции позволяет получить численное решение полученного уравнения типа Вольтерра II рода.

Список использованной литературы:

1. Сизиков В. С. Математические методы обработки результатов измерений. СПб.: Политехника, 2001. 240 с.
2. Леонов А. С. Решение некорректно поставленных обратных задач: Очерк теории, практические алгоритмы и демонстрации в Matlab. М.: Либроком, 2013. 336 с.
3. Brunner H. Collocation Methods for Volterra Integral and Related Functional Equations. Cambridge: Cambridge University Press, 2004. 597 p.
4. Верлань А. Ф., Сизиков В. С. Интегральные уравнения: методы, алгоритмы, программы. К.: Наук. думка, 1986. 268 с.

A numerical analytical algorithm of interpretation in the problem of signal reconstruction is presented. The algorithm consists in converting nonlinear integral equations of Volterra type I to Volterra type II equations and their numerical solution by applying the «natural interpolation» algorithm.

Key words: *nonlinear integral equations of the Volterra type of the first kind, the problem of signal reconstruction, interpretation of results.*

Получено 02.03.2017