Пример нестационарного расчета статического давления в трубопроводе длиной 1.8 м, диаметром 63 мм по приведенной методике представлен на рис. 4. Полное давление на входе 5 атм. Давление наружного воздуха 1 атм. Температура воздуха в покое 30 °С. Выход в атмосферу осуществляется без препятствий.

**Выводы.** В статье представлена математическая модель нестационарных гидравлических процессов в пневматическом трубопроводе, которая учитывает возникновение скачков уплотнения. Данная модель позволит определять задержки при моделировании работы системы управления пневматической системы.

1. *Идельчик И.Е.* Гидравлические сопротивления. - Изд. 3-е, перераб. и доп. – М.:Машиностроение, 1992.-559с.
2. *Абрамович Г.Н.* Прикладная газовая динамика. – Изд. 3-е, перераб. – М.: Наука, 1969. – 824 с.
3. *Винничук С.Д.* Особенности формирования второго закона Кирхгофа для задач расчета потокораспределения в распределительных системах сжимаемой жидкости//Электронное моделирование. Вып. 6. Т. 30 – Киев: ИПМЭ им. Г.Е.Пухова НАН Украины, 2008 – С.49-58
4. *С. К. Годунов,* Разностный метод численного расчета разрывных решений уравнений гидродинамики, Матем. сб., 1959, том 47(89), номер 3, 271–306
5. *Валландер С.В.* Лекции по гидроаэромеханике. Учеб. пособие – Л.: Изд-во Ленингр. ун-та, 1978. – 296 с.
6. *Патанкар С.* Численные методы решения задач теплообмена и динамики жидкости/ Пер. с англ., под ред. В.Д. Виленского. – М.: Энергоатомиздат , 1984. – 152 стр.

*Поступила 15.09.2016 р.*

УДК 510.2

В.В. Мохор, Е.В. Максименко, г. Киев

## ИСПОЛЬЗОВАНИЕ РАЗРЯДНОЙ МОДЕЛИ ДВОИЧНОГО ПРЕДСТАВЛЕНИЯ КВАДРАТА ЧИСЛА В ПРОЦЕДУРАХ ВЫЧИСЛЕНИЯ КВАДРАТНОГО КОРНЯ

The algorithm of using the discharge model of the binary representation of the squared number in procedures of calculating the square root without using the multiplication and division operations has been reviewed. A comparative analysis of this method was held with diagonal method of direct extraction of square roots. This method proposed to use in problems of fast calculation of the square roots.

 

**Актуальность.** При решении задач, связанных с криптографической защитой информации, часто возникает необходимость вычисления квадратных корней больших или многоразрядных чисел [1, 2, 3]. Сама процедура извлечения квадратного корня, в основе которой лежит давно известный алгоритм Ньютона и его модификации [4, 5], является достаточно тривиальной задачей. Функция «sqrt», используемая для ее решения, реализована в стандартных математических библиотеках практически всех современных языков программирования [6, 7, 8]. Тогда как для вычисления квадратных корней больших чисел применяется алгоритм Карацубы («Karatsuba Squar Root»), использующий процедуры Быстрого Преобразования Фурье (БПФ) и являющийся модификацией того же метода Ньютона [9, 10].

При этом следует отметить, что все используемые методы извлечения корней относятся к числу итерационных и требуют выполнения достаточно большого количества наиболее трудоемких арифметических операций умножения и деления. Это в свою очередь существенно влияет на их временную оценку. Как следствие, уменьшение количества итераций является одним из способов повышения производительности существующих методов вычисления квадратных корней.

Кроме этого существуют ряд способов целочисленного извлечения корня [11]. В частности, авторами статьи предлагается метод прямого определения квадратного корня. Алгоритм его реализации не предполагает использования операций умножения или деления. Благодаря этому можно предположить, что обозначенный метод является более эффективным в сравнении с существующими методами вычисления квадратных корней.

**Изложение основного материала исследования**. Предлагаемый метод вычисления квадратного корня основан на использовании разрядной модели двоичного представления квадрата n-разрядного числа [12]. В общем виде данная модель имеет следующий вид:

| **n** | **n-1** | **n-2** | **n-3** | | **2** | **1** |
|---|---|---|---|---|---|---|
| $X_n$ | $X_nX_{n-1}$ | | | | | |
| | $X_nX_{n-2}$ | | | | | |
| $X_{n-1}$ | $X_nX_{n-3}$ | $X_{(n-1)}X_{(n-2)}$ | | | | |
| | $X_nX_{n-4}$ | $X_{(n-1)}X_{(n-3)}$ | | | | |
| $X_{n-2}$ | $X_nX_{n-5}$ | $X_{(n-1)}X_{(n-4)}$ | $X_{(n-2)}X_{(n-3)}$ | . | | |
| | … | $X_{(n-1)}X_{(n-5)}$ | $X_{(n-2)}X_{(n-4)}$ | . | | |
| | $X_nX_2$ | … | $X_{(n-2)}X_{(n-5)}$ | . | | |
| | $X_nX_1$ | $X_{(n-1)}X_2$ | $X_{(n-2)}X_{(n-6)}$ | | | |
| | | $X_{(n-1)}X_1$ | … | | | |
| | | | $X_{(n-2)}X_2$ | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | $X_{(n-2)}X_1$ | | | |
| | | | . . . | | | |
| | | | | | | |
| $X_3$ | | | | | $X_3X_2$ | |
| | | | | | $X_3X_1$ | |
| $X_2$ | | | | | | $X_2\ X_1$ |
| | | | | | | |
| $X_1$ | | | | | | |

Например, разрядное представление квадрата четырехразрядного числа будет иметь следующий вид:

| | | | | |
|---|---|---|---|---|
| **7** | $X_4$ | $X_4X_3$ | | |
| **6** | | $X_4X_2$ | | |
| **5** | $X_3$ | $X_4\ X_1$ | $X_3X_2$ | |
| **4** | | | $X_3X_1$ | |
| **3** | $X_2$ | | | $X_2X_1$ |
| **2** | | | | |
| **1** | $X_1$ | | | |

С помощью цифр в первой колонке обозначим номера строк разрядной модели. Этими же значениями определяются номера разрядов числа, корень из которого необходимо извлечь. Для удобства восприятия материала, разряды пронумерованы с «1», а не традиционно с «0».

Следует отметить, что предлагаемый метод извлечения квадратного корня основан на использовании следующих свойств разрядной модели, являющихся следствием основных свойств алгебры логики.

*Свойство 1.* Если сумма значений двух любых разрядов числа, представленного в двоичной системе исчисления, равна единице, то эти значения противоположны.

Из соотношения $X_j + X_k = 1$ следует: $X_j = \overline{X}_k$ .

*Свойство 2.* Если сумма двух любых разрядов равна нулю, то значения этих разрядов идентичны.

Из соотношения $X_j + X_k = 0$ следует: $X_j = X_k$.

*Свойство 3.* Результатом суммирования прямого и обратного значений любого разряда является единица.

Для любого $X_j$ справедливо: $X_j + \overline{X}_j \equiv 1$.

*Свойство 4.* Произведение прямого и обратного значений любого разряда тождественен нулю.

Для любого $X_j$ справедливо: $\overline{X}_j \cdot X_j \equiv 0$.

*Свойство 5.* Произведение значения любого разряда само на себя дает то же значение.

Для любого $X_j$ справедливо: $X_j \cdot X_j \equiv X_j$.

Процедуру прямого вычисления корней рассмотрим на примере числа 121, представленного семью разрядами в двоичной системе счисления:

$$Z_2 = 1\ 1\ 1\ 1\ 0\ 0\ 1.$$

Дополним представленную ранее модель значениями соответствующих разрядов двоичного представления числа $Z_n$, в результате чего приведем ее к следующему виду:

| | | | | | | | $Z_n$ |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4X_3$ | | | | = | 1 |
| 6 | | $X_4X_2$ | | | | = | 1 |
| 5 | $X_3$ | $X_4X_1$ | $X_3X_2$ | | | = | 1 |
| 4 | | | $X_3X_1$ | | | = | 1 |
| 3 | $X_2$ | | | $X_2X_1$ | | = | 0 |
| 2 | | | | | | = | 0 |
| 1 | $X_1$ | | | | | = | 1 |

Основная идея предлагаемого метода прямого вычисления квадратного корня заключается в определении баланса между левой и правой частями разрядной модели.

Анализируя соотношение в строке №1, определяем значение первого разряда:

$$X_1=1.$$

Заменим $X_1$ на единицу во все строках модели, в результате чего получим следующий вид исходной модели:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4X_3$ | | | | = | 1 |
| 6 | | $X_4X_2$ | | | | = | 1 |
| 5 | $X_3$ | $X_4$ | $X_3X_2$ | | | = | 1 |
| 4 | | | $X_3$ | | | = | 1 |
| 3 | $X_2$ | | | $X_2$ | | = | 0 |
| 2 | | | | | | = | 0 |
| 1 | 1 | | | | | = | 1 |

В строке №3 имеем:

$$X_2 + X_2 = 0.$$

После приведения подобных членов в представленном равенстве, получаем модель вида:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4X_3$ | | | | = | 1 |
| 6 | | $X_4X_2$ | | | | = | 1 |
| 5 | $X_3$ | $X_4$ | $X_3X_2$ | | | = | 1 |
| 4 | | | $X_3$ | | | = | 1 |
| 3 | | | | $2X_2$ | | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

В этой же строке за счет коэффициента 2 при элементе $X_2$ согласно правил разрядного сложения в двоичной системе исчисления будет реализован перенос значения $X_2$ в старший разряд (строку №4). Причем коэффициент 2 при переносе в старший разряд соответственно опускается.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4X_3$ | | | | = | 1 |
| 6 | | $X_4X_2$ | | | | = | 1 |
| 5 | $X_3$ | $X_4$ | $X_3X_2$ | | | = | 1 |
| 4 | | | $X_3$ | $X_2$ | | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Во второй и третьей строках модели сформировались тривиальные тождества $0 \equiv 0$.

Проанализируем соотношение в строке №4:

$$X_3 + X_2 = 1.$$

В соответствии с установленным свойством (1) разрядных моделей получаем:

$$X_3 = \overline{X}_2 .$$

Выполним замену всех элементов $X_3$ модели на элементы $\overline{X}_2$, в результате чего модель эволюционирует к виду:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4\overline{X}_2$ | | | | = | 1 |
| 6 | | $X_4X_2$ | | | | = | 1 |
| 5 | $\overline{X}_2$ | $X_4$ | $\overline{X}_2X_2$ | | | = | 1 |
| 4 | | | $\overline{X}_2$ | $X_2$ | | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Учитывая ранее определенное свойство (3):

$$X_j + \overline{X}_j \equiv 1,$$

тождество в строке №4:

$$X_2 + \overline{X}_2 \equiv 1,$$

можно записать в виде $1 \equiv 1$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4 \overline{X}_2$ | | | | = | 1 |
| 6 | | $X_4 X_2$ | | | | = | 1 |
| 5 | $\overline{X}_2$ | $X_4$ | $\overline{X}_2 X_2$ | | | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

В соответствии со свойством (4), результат произведения прямого и обратного значений элемента $\overline{X}_2 \cdot X_2$ пятой строки тождественен 0:

$$\overline{X}_2 \cdot X_2 \equiv 0,$$

с учетом этого данный элемент модели в строке №5 можно исключить.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_4$ | $X_4 \overline{X}_2$ | | | | = | 1 |
| 6 | | $X_4 X_2$ | | | | = | 1 |
| 5 | $\overline{X}_2$ | $X_4$ | | | | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Как следствие, соотношение в строке №5 имеет следующий вид:

$$\overline{X}_2 + X_4 = 1.$$

На основании свойства (3) из данного соотношения следует:

$$X_4 = \overline{\overline{X}_2} = X_2.$$

Проведем замену элементов $X_4$ на $X_2$, в результате чего модель преобразуется к виду:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_2$ | $X_2 \overline{X}_2$ | | | | = | 1 |
| 6 | | $X_2 X_2$ | | | | = | 1 |
| 5 | $\overline{X}_2$ | $X_2$ | | | | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Согласно свойству (3), в строке №5 имеем тождество:

$$X_2 + \overline{X}_2 \equiv 1.$$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | $X_2$ | $X_2\overline{X}_2$ | | | | = | 1 |
| 6 | | $X_2X_2$ | | | | = | 1 |
| 5 | | | | | 1 | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Свойство (5) разрядной модели позволяет реализовать замену произведения $X_2 \cdot X_2$ на $X_2$ в строке №6, в результате чего получим:

$$X_2 = 1.$$

С помощью полученного значения элемента $X_2 = 1$, модель преобразуется к виду:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | 1 | $X_2\overline{X}_2$ | | | | = | 1 |
| 6 | | | | | 1 | = | 1 |
| 5 | | | | | 1 | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

В строке №7 исключаем элемент $X_2 \cdot \overline{X}_2$ согласно свойству (4), в результате чего получаем окончательный вид модели числа $Z_2$ = 1 1 1 1 0 0 1:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | | | | | 1 | = | 1 |
| 6 | | | | | 1 | = | 1 |
| 5 | | | | | 1 | = | 1 |
| 4 | | | | | 1 | = | 1 |
| 3 | | | | | 0 | = | 0 |
| 2 | | | | | 0 | = | 0 |
| 1 | | | | | 1 | = | 1 |

Итак, в результате эволюции представленной разрядной модели квадрата числа были получены следующие соотношения:

$X_1 = 1;$

$X_3 = \overline{X}_2;$

$X_4 = X_2;$

$X_2 = 1,$

на основании которых не сложно определить значения всех разрядов двоичного представления результата извлечения квадратного корня.

В рассматриваемом примере окончательным результатом вычисления квадратного корня из числа $Z_{10} = 121$ будет:

$X_1 = 1;$

$X_2 = 1;$

$X_3 = 0;$

$X_4 = 1,$

или $\sqrt{121} = 11_{10} = 1011_2$.

А.Н. Терещенко в [11] был предложен диагональный метод прямого возведения в квадрат больших чисел, который может быть использован для решения обратной задачи – вычисления квадратного корня. В указанном методе так же не применяются трудоемкие операции умножения и деления, что позволяет использовать его в процедурах факторизации больших чисел. Эффективность указанного метода обусловлена отказом от использования трудоемких операций умножения и деления при извлечении квадратного и кубического корней. Поэтому оценка вычислительной сложности предложенного разрядного метода авторами проводилась путем сравнительного анализа процедуры вычисления квадратных корней и диагонального метода А.Н. Терещенко на примере чисел Zn = 25, 121, 289 и 1369. Для этого подсчитывалось количество элементарных операций в каждом из рассматриваемых случаев, выполняемых за один такт процессора.

В результате эксперимента были получены следующие значения.

| Zn | Диагональный метод (метод Терещенко) | Метод, основанный на разрядной модели квадрата числа |
|---|---|---|
| 25 | 40 | 30 |
| 121 | 66 | 52 |
| 289 | 72 | 80 |
| 1369 | 105 | 109 |

**Вывод.** Как видно из таблицы, существенных отличий с точки зрения вычислительной сложности представленные методы вычисления квадратных корней не имеют. Они имеют одинаковую асимптотическую сложность. Однако следует отметить, что, в методе, основанном на использовании разрядной модели, работа ведется с битовыми величинами. В случае метода А.Н. Терещенка работа ведется с большими числами, значения регистров которых переопределяются. Кроме того, в [11] было отмечено, что “математическая модель предложенного метода хоть и является простой, так как не использует операции умножения и деления, но является “жадной к памяти”. “Жадность” проявляется в том, что при программной реализации метода активно используется память, что сильно замедляет время выполнения”.

1. *Шнаер Б.* Прикладная криптографія. – М.:Триумф, 2012. – 815 с.
2. *Мао В.* Современная криптография. Теория и практика. – М.:Вильямс, 2005. 763 с.
3. *Bellare, P.* Rogaway Optimal Asymmetric Encryption. – Springer Berlin Heidelberg, 1995. – Vol. 950.
4. Алгоритмы. Методы. Исходники. [Электронный ресурс]. / Под ред. И. Кантора. Вариант вычисления квадратного корня. Алгоритм Ньютона. – Режим доступа: http://algolist.manual.ru/maths/count_fast/sqrt.php.
5. Алгоритмы вычисления квадратного корня. [Электронный ресурс]. – Режим доступа: http://www.azillionmonkeys.com/qed/sqroot.html
6. *Дональд Э.* Кнут Искусство программирования. Том 2. – М.: Мир, 1979. – 727 с.
7. *Дэвид Вандевурд, Николай М. Джосаттис* Шаблоны С++. Справочник разработчика: Пер. с англ. – М.: Вильямс, 2015 . - 544 с.
8. *Стефан Кочан* Программирование на языке С, 3-е издание: Пер. с англ. – М.:Вильямс, 2006. – 496 с.
9. Square Root algorithm for C. [Электронный ресурс]. – Режим доступа: http://www.codeproject.com/Articles/570700/SquareplusRootplusalgorithmplusforplusC.
10. Best Square Root Method. Algorithm. Function. [Электронный ресурс]. – Режим доступа:http://www.codeproject.com/Articles/69941/Best-Square-Root-Method-Algorithm-Function-Precisi.
11. *Терещенко А.Н.* Быстрое вычисление квадратного и кубического корней без использования операций умножения и деления // Искусственный интеллект. – 2005. – Вип. 3. – С. 670-680.
12. *Жилін А.В.* Ідентифікація парності елементів розрядним методом при факторизації чисел алгоритмом Ферма / В.В. Мохор, А.В. Жилин // Спеціальні телекомунікаційні системи та захист інформації. – 2010. – Вип. 1(17). – С. 96-102.

*Поступила 1.09.2016 р.*

УДК 621.396

В.М. Колчар, І.П. Лісовий, м.Одеса

## ВИКОРИСТАННЯ СИНХРОННОГО ФІЛЬТРА В ЯКОСТІ СЛІДКУЮЧОГО ФІЛЬТРА ВИДІЛЬНИКА ТАКТОВОЇ СИНХРОНІЗАЦІЇ

**Abstract.** The conditions under which synchronous filter (SF) can be used as a tracking filter of devices of clock synchronization were defined i n the article.

**Вступ**

Проблема зниження порогу завадостійкості при прийомі тактового синхросигналів особливо актуальна. В даний час існують різні методи, що дозволяють звузити смугу пропускання на вході пристрою виділення тактової частоти (ВТЧ) і тим самим знизити поріг завадостійкості. До них відносяться

 