О ДОСТОВЕРНОСТИ КЛАССОВ СИГНАТУРНЫХ АНАЛИЗАТОРОВ, ПОРОЖДАЕМЫХ ПРОИЗВЕДЕНИЯМИ МИНИМАЛЬНЫХ МНОГОЧЛЕНОВ

Л. П. Махнист

Факультет водоснабжения и гидромелиорации, БПИ
Брест, Республика Беларусь

Получены точные аналитические выражения числа необнаруживаемых ошибок максимальной длины фиксированной кратности сигнатурным анализатором, порождаемым полиномом, который является образующим полиномом примитивного БЧХ-кода, исправляющего две ошибки, в зависимости от четной или нечетной степени порождающего полинома; найдены точные границы (верхние и нижние) достоверности указанных выше сигнатурных анализаторов и соответствующие кратности, при которых они достигаются; найдены классы сигнатурных анализаторов, имеющие такие же характеристики, как и сигнатурные анализаторы, порождаемые полиномами, являющимися образующими примитивных БЧХ-кодов, исправляющих две ошибки.

СИГНАТУРНЫЙ, АНАЛИЗ, ПОЛИНОМ, КОРРЕКТИРУЮЩИЕ, КОДЫ

Одним из способов повышения достоверности сигнатурного анализа является способ, основанный на применении нескольких сигнатурных анализаторов, реализованных с помощью примитивных и непримитивных полиномов, имеющих одинаковую степень.

В качестве меры оценки достоверности сигнатурного анализа, будем рассматривать распределение вероятностей необнаружения ошибки в зависимости от веса k последовательностей данных, которое определяется следующим образом: $P_n(k)=A_n(k)/C_n^k$, где $A_n(k)$ - количество необнаруживаемых определенным методом сжатия ошибочных последовательностей длины n, содержащих ошибки веса k, к общему числу последовательностей - C_n^k (число сочетаний из n по k) [1, 3].

В работе приведены результаты анализа достоверности классов сигнатурных анализаторов, порождаемых полиномами - образующими примитивных БЧХ-кодов, исправляющих две ошибки; исследован класс сигнатурных анализаторов, имеющий такие же характеристики, как и некоторые сигнатурные анализаторы, порождаемые полиномами - образующими примитивных БЧХ-кодов, исправляющих две ошибки.

Для сигнатурного анализатора, порождаемого полиномами нечетной степени, являющегося образующим БЧХ-кода, исправляющего две ошибки, найдены точные формулы числа двоичных последовательностей длины $n=2^m-1$ веса k, инициирующих нулевую сигнатуру для фиксированного сигнатурного анализатора, порождаемого полиномом степени 2m (m - четно) - образующего примитивного БЧХ-кода, исправляющего две ошибки; получено распределение величин $P_n(k)$ и найдена точная верхняя граница достоверности указанного выше сигнатурного анализатора.

Утверждение 1. Максимальное значение вероятности необнаружения ошибочной последовательности длины $n=2^m-1$ сигнатурным анализатором, порождаемым полиномом степени 2m (m - нечетно) - образующим примитивного кода БЧХ, исправляющего две ошибки, определяется выражением $\max P_n(k)=(n-7)/((n-2)(n-3)(n-4))$, и достигается при k=5, 6, n-6, n-5.

Также найдена и нижняя граница достоверности для соответствующего сигнатурного анализатора.

Рассмотрим класс сигнатурных анализаторов, обладающий такими же характеристиками, как и сигнатурный анализатор, порождаемый полиномом степени 2m (m - нечетно) - образующим примитивного БЧХ-кода, исправляющего две ошибки.

Утверждение 2. Пусть M_1 - примитивный полином нечетной степени $m=2t+1$ над полем GF(2), а элемент b поля $GF(2^m)$ - некоторый его корень [2]. Образуем множество минимальных многочленов M_l элементов b^l, где $l=2^i+1$, $1\leq i\leq t$, а числа m и i - взаимно просты. Построим множество сигнатурных анализаторов G_l, порождаемых произведениями примитивного полинома M_1 и некоторого минимального многочлена M_l. Тогда предельная оценка P_l вероятности необнаружения ошибочной последовательности сигнатурным анализатором G_l не зависит от l и определяется соотношением $P_l=(n-7)/((n-2)(n-3)(n-4))$.

Пример 1. Пусть m=9, t=4, $M_1=x^9+x^5+1$ - примитивный полином. Тогда i может принимать значения 1, 2, 4 и множество минимальных многочленов M_l состоит из многочленов $M_3=x^9+x^6+x^5+x^3+1$, $M_5=x^9+x^5+x^4+x+1$, $M_{17}=x^9+x^8+x^6+x^5+ +x^3+x^2+1$. Тогда сигнатурные анализаторы G_3, G_5, G_{17}, порождаемые полиномами M_1M_3, M_1M_5, M_1M_{17}, соответственно, имеют одну и туже предельную оценку вероятности необнаружения ошибочной последовательности.

В работе исследуется достоверность сигнатурного анализатора, порождаемого полиномом степени 2m (m - четно) - образующим примитивного БЧХ-кода, исправляющего две ошибки. В этом случае, порождающий полином является произведением примитивного на, в общем случае, непримитивный полином, степени которых равны некоторому четному числу m.

Утверждение 3. Максимальное значение вероятности необнаружения ошибочной последовательности длины $n=2^m-1$ сигнатурным анализатором, порождаемым полиномом степени 2m (m - четно) - образующим примитивного кода БЧХ, исправляющего две ошибки, определяется выражением max $P_n(k)=(n-3)/((n-1)(n-2)(n-4))$, и достигается при k=5, 6, n-6, n-5.

Для данного сигнатурного анализатора также определена нижняя граница достоверности, найдены точные формулы числа двоичных последовательностей длины $n=2^m-1$ веса k, инициирующих нулевую сигнатуру для фиксированного сигнатурного анализатора, порождаемого полиномом степени 2m (m - четно) - образующего примитивного БЧХ-кода, исправляющего две ошибки, а также распределение величин $P_n(k)$.

Рассмотрим класс сигнатурных анализаторов, обладающий такими же характеристиками, как и сигнатурный анализатор, порождаемый полиномом степени 2m (m - четно) - образующим примитивного БЧХ-кода, исправляющего две ошибки.

Утверждение 4. Пусть M_1 - примитивный полином четной степени m над полем GF(2), а элемент b поля $GF(2^m)$ - некоторый его корень [2]. Образуем множество минимальных многочленов M_l элементов b^l, где $l=2^i+1$, $1 \leq i<m/2$, а числа m и i - взаимно просты. Построим множество сигнатурных анализаторов G_l, порождаемых произведениями примитивного полинома M_1 и некоторого минимального многочлена M_l. Тогда предельная оценка P_l вероятности необнаружения ошибочной последовательности сигнатурным анализатором G_l не зависит от l и определяется соотношением $P_l=(n-3)/((n-1)(n-2)(n-4))$.

Пример 2. Пусть m=14, $M_1=x^{14}+x^{12}+x^{11}+x+1$ - примитивный полином, и числа i и m взаимно просты. Тогда i может принимать значения 1, 3, 5 и множество минимальных многочленов M_l состоит из многочленов $M_3=x^{14}+x^{13}+x^{11}+x^9+x^5+x+1$, $M_9=x^{14}+x^{11}+x^9+x^8+x^4+x^3+x^2+x+1$ и $M_{33}=x^{14}+x^{13}+x^{12}+x^{11}+x^9+ +x^5+x^2+x+1$. Тогда сигнатурные анализаторы G_3,

G_9, G_{33}, порождаемые полиномами M_1M_3, M_1M_9, M_1M_{33} , соответственно, имеют одну и туже предельную оценку вероятности необнаружения ошибочной последовательности. Заметим, что сигнатурный анализатор G_3, порождается полиномом M_1M_3, который является образующим примитивного БЧХ-кода, исправляющего две ошибки. Поэтому, для него, очевидно, выполняется утверждение 4.

Замечание. Следует отметить, что в качестве минимального многочлена M_1 можно взять в точности $\varphi(2^m-1)$ примитивных полиномов. Тогда количество сигнатурных анализаторов, обладающих одной и той же оценкой достоверности, определяется соотношением

$\varphi(2^m-1)\varphi(m, (m-1)/2)$, если m - нечетно, и $\varphi(2^m-1)\varphi(m, m/2)$, если m - четно, где $\varphi(i,j)$ - количество чисел, не превосходящих min (i,j) и взаимно простых с i.

Литература

1 Берлекэмп Э. Алгебраическая теория кодирования: Пер. с англ. - М.: Мир, 1971. - 477с.

2 Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2: Пер. с англ. - М.: Мир, 1988. – 824с.

3 Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. - М.: Связь, 1979. – 744с.

4 Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. - М.: Мир, 1976. - 594с.

ИНТЕГРАЛЬНЫЕ УРАВНЕНИЯ ТИПА СВЕРТКИ С ЯДРАМИ, ЗАВИСЯЩИМИ ОТ ЛИНЕЙНОЙ ФУНКЦИИ

Т.А. Тузик

Факультет водоснабжения и гидромелиорации, БПИ
Брест, Республика Беларусь

Указан способ решения трёх интегральных уравнений с ядрами, зависящими от линейной функции.

ИНТЕГРАЛЬНЫЙ, УРАВНЕНИЕ, СВЁРТКА, КРАЕВАЯ, ФУРЬЕ