Блочные коды для борьбы с пакетными ошибками

Пример независимых и пакетных ошибок

Двоичный кодовый поток, принятый из канала связи											
1	0	1	1	0	0	0	1	1	…	0	1
Ошибки одиночные, характеризуются кратностью ошибки											

Двоичный кодовый поток, принятый из канала связи											
1	0	0	0	1	1	1	1	1	…	0	1
Ошибки пакетные, характеризуются длиной пакета P											

Коды Файра

Коды Файра являются циклическими кодами, позволяющими исправлять пакеты ошибок определенной длины за счет выбора соответствующего образующего полинома.

Образующий (порождающий) полином кода Файра $G(X)_Ф$

Образующий полином кода Файра $G(X)_Ф$ определяется произведением двух примитивных полиномов:

$$G(X)_Ф = G(X)(X^c+1)$$

Старшая степень t полинома G(X) должна равняться или превышать длину предполагаемого пакета ошибок P: $t \geq P$. В качестве полинома G(X) может быть выбран любой неприводимый полином из таблицы образующих полиномов циклических кодов, приведенных ниже:

Примеры образующих (порождающих) полиномов G(X)

Старшая степень полинома (соответствует числу проверочных разрядов r в кодовом слове)	Вид образующего полинома G(X)	Двоичное представление полинома G(X)	Десятичное представление полинома G(X)
2	X^2+X+1	111	7
3	X^3+X+1	1011	11
4	X^4+X+1 $X^4+X^3+X^2+X+1$	10011 11111	19 31
5	$X^5+X^4+X^3+X^2+1$	111101	61
6	X^6+X+1 X^6+X^3+1 $X^6+X^5+X^2+X+1$	1000011 1001001 1100111	67 73 103
7	X^7+X+1 $X^7+X^4+X^3+X^2+1$	10000011 10011101	131 157
…	…	…	…

Старшая степень c второго полинома должна равняться или превышать удвоенную длину предполагаемого пакета ошибок P: $c \geq 2 \cdot P$. При этом c не должно делиться нацело на число e, где $e = 2^t - 1$.

При этом блоковая длина кода Файра будет являться произведением чисел e и c: $n = e \times c$, а длина проверочной группы r в кодовой комбинации будет являться суммой старших степеней обоих образующих полиномов: $r = t+c$.

Код Файра (12,6) исправляющий пакеты ошибок длиной 2 символа

Рассмотрим код Файра, способный исправлять пакеты длиной 2 символа. Для этого выберем из таблицы образующий полином G(X), старшая степень которого будет не меньше длины исправляемого пакета. В качестве такого полинома подходит полином $G(X) = X^2+X+1$ со старшей степенью t=2. Степень второго образующего полинома c должна быть не меньше четырех. Таким образом, в качестве полинома (X^c+1) может быть выбран полином (X^4+1). Отмечаем, что c=4 не имеет общих делителей с $e=2^t-1=3$. Образующий полином кода Файра $G(X)_Ф = G(X)(X^c+1)$ примет вид:

$$G(X)_Ф = (X^2+X+1)(X^4+1) = X^6 + X^5 + X^4 + X^2 + X + 1$$

Блоковая длина кода составит $n = e \times c = 3 \times 4 = 12$, а число проверочных символов в блоке будет равно $r = t+c = 6$

Пример получения кодовой комбинации путем деления информационного полинома Q(X) на образующий полином $G(X)_Ф$

Информационная 6-разрядная комбинация: 000101. Соответствующий ей информационный полином $I(X) = X^2 + 1$

Производим увеличение степени информационного полинома I(X) на старшую степень образующего полинома $G(X)_Ф$

$$Q(X) = I(X) \cdot X^6 = (X^2 + 1) \cdot X^6 = X^8 + X^6$$

Выполняем деления расширенного информационного полинома Q(X) на образующий полином $G(X)_Ф$

$$\begin{array}{ccccccccc|l}
X^8+ & & +X^6 & & & & & & & X^6+X^5+X^4+X^2+X+1 \\
X^8+ & +X^7 & +X^6 & & +X^4 & +X^3 & +X^2 & & & \hline X^2+X+1 \\
\hline
 & X^7+ & & & +X^4 & +X^3 & +X^2 & & & \\
 & X^7+ & +X^6 & +X^5 & & +X^3 & +X^2 & +X & & \\
\hline
 & & X^6+ & +X^5 & +X^4 & & & +X & & \\
 & & X^6+ & +X^5 & +X^4 & & +X^2 & +X & +1 & \\
\hline
 & & & & & & X^2+ & & +1 &
\end{array}$$

Кодовый полином C(X) получается путем добавления остатка от деления Q(X) на $G(X)_Ф$ к расширенному информационному полиному Q(X). В нашем случае: $C(X) = X^8 + X^6 + X^2 + 1$

Декодирование кодового полинома $C(X) = X^8 + X^6 + X^2 + 1$ кода Файра (12,6)

Декодирование осуществляется путем деления кодового полинома C(X) последовательно на обе компоненты образующего полинома кода Файра $G(X)_Ф$: на (X^2+X+1) и на (X^6+1). Остаток от деления, равный нулю, на каждый из полиномов соответствует случаю отсутствия ошибок при передаче кодовой комбинации. Отличие от нуля остатка от деления означает возникновение пакета ошибок, позиция которого определяется путем сравнения остатков от деления на оба образующих полинома. Проведем декодирование кодового полинома кода Файра (12,6) в случае возникновения пакета ошибок длиной 2 символа, соответствующего полиному $P(X)=X^7+X^6$. Искаженный таким пакетом ошибок кодовый полином пример следующий вид: $C^*(X) = X^8+X^7+X^2+1$.

Выполним деление полинома на каждую из компонент образующего полинома кода Файра $G(X)_Ф$: на (X^2+X+1) и на (X^6+1)

$$\begin{array}{l|l}
X^8+X^7+X^2+1 & X^2+X+1 \\
X^8+X^7+X^6 & X^6+X^4+X^3+X \\
\hline
X^6+X^2+1 & \\
X^6+X^5+X^4 & \\
\hline
X^5+X^4+X^2+1 & \\
X^5+X^4+X^3 & \\
\hline
X^3+X^2+1 & \\
X^3+X^2+X & \\
\hline
\mathbf{X+1} &
\end{array}
\qquad
\begin{array}{l|l}
X^8+X^7+X^2+1 & X^4+1 \\
X^8+X^4 & X^4+X^3+1 \\
\hline
X^7+X^4+X^2+1 & \\
X^7+X^3 & \\
\hline
X^4+X^3+X^2+1 & \\
X^4+1 & \\
\hline
\mathbf{X^3+X^2} &
\end{array}$$

Из приведенных вычислений видно, что остатки от деления на образующие полиномы отличны от нуля и не равны между собой. Выполним необходимое число циклических сдвигов кодового полинома $C^*(X)$ и деление их на образующие полиномы до тех пор, пока остатки от деления для обоих образующих полиномов не сравняются.

Первый циклический сдвиг кодового полинома $C^*(X)$ имеет вид $C_1^*(X) = X^9+X^8+X^3+X$

$$\begin{array}{l|l}
X^9+X^8+X^3+X & X^2+X+1 \\
X^9+X^8+X^7 & X^7+X^5+X^4+X^2+1 \\
\hline
X^7+X^3+X & \\
X^7+X^6+X^5 & \\
\hline
X^6+X^5+X^3+X & \\
X^6+X^5+X^4 & \\
\hline
X^4+X^3+X & \\
X^4+X^3+X^2 & \\
\hline
X^2+X & \\
X^2+X+1 & \\
\hline
\mathbf{1} &
\end{array}
\qquad
\begin{array}{l|l}
X^9+X^8+X^3+X & X^4+1 \\
X^9+X^5 & X^5+X^4+X+1 \\
\hline
X^8+X^5+X^3+X & \\
X^8+X^4 & \\
\hline
X^5+X^4+X^3+X & \\
X^5+X & \\
\hline
X^4+X^3 & \\
X^4+1 & \\
\hline
\mathbf{X^3+1} &
\end{array}$$

Поскольку остатки от деления вновь не совпадают, выполняем еще один циклический сдвиг кодового полинома $C^*(X)$, который теперь примет вид $C_2^*(X) = X^{10}+X^9+X^4+X^2$

$$\begin{array}{l|l}
X^{10}+X^9+X^4+X^2 & X^2+X+1 \\
X^{10}+X^9+X^8 & X^8+X^6+X^5+X^3+X \\
\hline
X^8+X^4+X^2 & \\
X^8+X^7+X^6 & \\
\hline
X^7+X^6+X^4+X^2 & \\
X^7+X^6+X^5 & \\
\hline
X^5+X^4+X^2 & \\
X^5+X^4+X^3 & \\
\hline
X^3+X^2 & \\
X^3+X^2+X & \\
\hline
\mathbf{X} &
\end{array}
\qquad
\begin{array}{l|l}
X^{10}+X^9+X^4+X^2 & X^4+1 \\
X^{10}+X^6 & X^6+X^5+X^2+X+1 \\
\hline
X^9+X^6+X^4+X^2 & \\
X^9+X^5 & \\
\hline
X^6+X^5+X^4+X^2 & \\
X^6+X^2 & \\
\hline
X^5+X^4 & \\
X^5+X & \\
\hline
X^4+X & \\
X^4+1 & \\
\hline
\mathbf{X+1} &
\end{array}$$

Поскольку остатки от деления вновь не совпадают, выполняем очередной циклический сдвиг кодового полинома $C^*(X)$, который теперь примет вид $C_3^*(X) = X^{11}+X^{10}+X^5+X^3$

$$\begin{array}{l|l}
X^{11}+X^{10}+X^5+X^3 & X^2+X+1 \\
X^{11}+X^{10}+X^9 & X^9+X^7+X^6+X^4+X^2+1 \\
\hline
X^9+X^5+X^3 & \\
X^9+X^8+X^7 & \\
\hline
X^8+X^7+X^5+X^3 & \\
X^8+X^7+X^6 & \\
\hline
X^6+X^5+X^3 & \\
X^6+X^5+X^4 & \\
\hline
X^4+X^3 & \\
X^4+X^3+X^2 & \\
\hline
X^2 & \\
X^2+X+1 & \\
\hline
\mathbf{X+1} &
\end{array}
\qquad
\begin{array}{l|l}
X^{11}+X^{10}+X^5+X^3 & X^4+1 \\
X^{11}+X^7 & X^7+X^6+X^3+X^2+X \\
\hline
X^{10}+X^7+X^5+X^3 & \\
X^{10}+X^6 & \\
\hline
X^7+X^6+X^5+X^3 & \\
X^7+X^3 & \\
\hline
X^6+X^5 & \\
X^6+X^2 & \\
\hline
X^5+X^2 & \\
X^5+X & \\
\hline
\mathbf{X^2+X} &
\end{array}$$

Поскольку остатки от деления вновь не совпадают, выполняем очередной циклический сдвиг кодового полинома $C^*(X)$, который теперь примет вид $C_4^*(X) = X^{11}+X^6+X^4+1$

$$\begin{array}{l|l}
X^{11}+X^6+X^4+1 & X^2+X+1 \\
X^{11}+X^{10}+X^9 & X^9+X^8+X^6+X^5+X^4 \\
\hline
X^{10}+X^9+X^6+X^4+1 & \\
X^{10}+X^9+X^8 & \\
\hline
X^8+X^6+X^4+1 & \\
X^8+X^7+X^6 & \\
\hline
X^7+X^4+1 & \\
X^7+X^6+X^5 & \\
\hline
X^6+X^5+X^4+1 & \\
X^6+X^5+X^4 & \\
\hline
\mathbf{1} &
\end{array}
\qquad
\begin{array}{l|l}
X^{11}+X^6+X^4+1 & X^4+1 \\
X^{11}+X^7 & X^7+X^3+X^2+1 \\
\hline
X^7+X^6+X^4+1 & \\
X^7+X^3 & \\
\hline
X^6+X^4+X^3+1 & \\
X^6+X^2 & \\
\hline
X^4+X^3+X^2+1 & \\
X^4+1 & \\
\hline
\mathbf{X^3+X^2} &
\end{array}$$

Выполняем очередной циклический сдвиг кодового полинома $C^*(X)$, который теперь примет вид $C_5^*(X) = X^7+X^5+X+1$

$$\begin{array}{l|l}
X^7+ \quad +X^5 \quad +X \quad +1 & X^2+ \quad +X \quad +1 \\
X^7+ \quad +X^6 \quad +X^5 & X^5+ \quad +X^4 \quad +X^3+ \\ \hline
X^6+ \quad +X \quad +1 & +X \quad +1 \\
X^6+ \quad +X^5 \quad +X^4 & \\ \cline{1-1}
X^5+ \quad +X^4 \quad +X \quad +1 & \\
X^5+ \quad +X^4 \quad +X^3 & \\ \cline{1-1}
X^3+ \quad +X \quad +1 & \\
X^3+ \quad +X^2 \quad +X & \\ \cline{1-1}
X^2+ \quad +1 & \\
X^2+ \quad +X \quad +1 & \\ \cline{1-1}
\mathbf{X} &
\end{array}
\qquad
\begin{array}{l|l}
X^7+ \quad +X^5 \quad +X \quad +1 & X^4+ \quad +1 \\
X^7+ \quad +X^3 & X^3+ \quad +X \\ \hline
X^5+ \quad +X^3 \quad +X \quad +1 & \\
X^5+ \quad +X & \\ \cline{1-1}
\mathbf{X^3+ \quad +1} &
\end{array}$$

Выполняем очередной циклический сдвиг кодового полинома $C^*(X)$, который теперь примет вид $C_6^*(X) = X^8+X^6+X^2+X$

$$\begin{array}{l|l}
X^8+ \quad +X^6 \quad +X^2 \quad +X & X^2+ \quad +X \quad +1 \\
X^8+ \quad +X^7 \quad +X^6 & X^6+ \quad +X^5 \quad +X^4+ \\ \hline
X^7+ \quad +X^2 \quad +X & +X^2 \quad +X \quad +1 \\
X^7+ \quad +X^6 \quad +X^5 & \\ \cline{1-1}
X^6+ \quad X^5+ \quad +X^2 \quad +X & \\
X^6+ \quad +X^5 \quad +X^4 & \\ \cline{1-1}
X^4+ \quad +X^2 \quad +X & \\
X^4+ \quad +X^3 \quad +X^2 & \\ \cline{1-1}
X^3+ \quad +X & \\
X^3+ \quad +X^2 \quad +X & \\ \cline{1-1}
X^2 & \\
X^2+ \quad +X \quad +1 & \\ \cline{1-1}
\mathbf{X+ \quad +1} &
\end{array}
\qquad
\begin{array}{l|l}
X^8+ \quad +X^6 \quad +X^2 \quad +X & X^4+ \quad +1 \\
X^8+ \quad +X^4 & X^4+ \quad +X^2 \quad +1 \\ \hline
X^6+ \quad +X^4 \quad +X^2 \quad +X & \\
X^6+ \quad +X^2 & \\ \cline{1-1}
X^4+ \quad +X & \\
X^4+ \quad +1 & \\ \cline{1-1}
\mathbf{X+ \quad +1} &
\end{array}$$

После того, как остатки от деления на образующие полиномы сравнялись, необходимо выполнить правые циклические сдвиги полученного остатка от деления, причем их число должно соответствовать числу левых циклических сдвигов кодового полинома, которые были выполнены для поиска одинакового остатка от деления. В данном случае необходимо выполнить шесть циклических сдвигов вправо остатка от деления X+1. Полученный полином X^7+X^6 будет являться корректирующим полиномом, совпадающим с полиномом пакета ошибок. Для исправления пакета ошибок достаточно сложить принятый кодовый полином $C^*(X)$ с полученным корректирующим полиномом. Информационный полином будет получен из кодового путем отбрасывания проверочной части полинома и делению полученного полинома на X^6:
$C(X) = X^8+X^7+X^2+1+X^7+X^6= X^8+X^6+X^2+1$; $Q(X) = X^8+X^6$; $I(X) = X^2 + 1$. Информационная 6-разрядная комбинация: 000101.

Примеры образующих полиномов и параметры некоторых кодов Файра

Длина исправляемого пакета	Вид образующего полинома G(X)	Вид образующего полинома (X^c+1)	Блоковая длина n кода	Число проверочных символов r в блоке
2	X^2+X+1	X^4+1	12	6
3	X^3+X+1	X^6+1	42	9
4	X^4+X+1	X^8+1	120	12
…	…	…	…	…
7	X^7+X+1	$X^{14}+1$	1778	21