Обнаружение и коррекция ошибок в кодах полиномиальной системы классов вычетов на основе нулевизации.

Калмыков И.А., Емарлукова Я.В.

Применение базисов безизбыточной системы оснований ПСКВ в цифровой обработке сигналов позволяет повысить скорость и точность обработки, кроме того, ПСКВ увеличивает информационную надежность за счет обнаружения ошибки и ее коррекции.

Если на диапазон возможного изменения кодируемого множества полиномов наложить ограничения, то есть выбрать k из n оснований ПСКВ ($k<n$), то это позволит осуществлять разбиение полного диапазона $P_{полн}(z)$ расширенного поля Галуа $GF(p^n)$ на два непересекающихся подмножества.

Первое подмножество называется рабочим диапазоном и определяется выражением

$$P_{раб}(z)=\prod_{i=1}^{k} p_i(z)$$

Многочлен $A(z)$ с коэффициентами из поля $GF(p)$ будет считаться разрешенным в том и только в том случае, если он является элементом нулевого интервала полного диапазона $P_{полн}(z)$, то есть принадлежать диапазону $A(z)\in P_{раб}(z)$.

Второе подмножество $GF(p^n)$, определяемое произведением $r=n-k$ контрольных оснований

$$P_{конт}(z)=\prod_{i=k+1}^{k+r} p_i(z),$$

задает совокупность запрещенных комбинаций. Если $A(z)$ является элементом второго подмножества, то считается, что данная комбинация содержит ошибку. Таким образом, местоположение полинома $A(z)$относительно двух данных подмножеств позволяет однозначно определить, является ли кодовая комбинация

$A(z)=(a_1(z),\ a_2(z),\ ...,a_{k+r}(z))$ разрешенной, или содержит ошибочные символы.

Нулевизация заключается в последовательном вычитании из исходного полинома, представленного в модулярном коде, некоторых минимальных полиномов - констант нулевизации таких, что полином $A(z)$ последовательно преобразуется в полином вида

$$A_1(z)=A(z)-M_1(z)=$$
$$=(a_1(z)-s_1^1(z),a_2(z)-s_2^1(z),...,a_{k+1}(z)-s_{k+1}^1(z),...,a_{k+r}(z)-s_{k+r}^1(z))=$$
$$=(0,a_2^2(z),...,a_{k+1}^2(z),...,a_{k+r}^2(z)),$$

где $M_1(z)=(s_1^1(z),s_2^1(z),s_3^1(z),...,s_k^1(z),s_{k+1}^1(z),...,s_{k+r}^1(z))$ - константа нулевизации по первому основанию $p_1(z)$.

Затем из полученный результата вычитается следующая константа нулевизации для получения полинома

$$A_2(z)=A_1(z)-M_2(z)=$$
$$=(0,a_2^2(z)-s_2^2(z),...,a_{k+1}^2(z)-s_{k+1}^2(z),.....,a_{k+r}^2(z)-s_{k+r}^2(z))=$$
$$=(0,0,a_3^3(z),...,a_{k+1}^3(z),...,a_{k+r}^3(z)),$$

где $M_1(z)=(0,s_2^2(z),s_3^2(z),...,s_k^2(z),s_{k+1}^2(z),...,s_{k+r}^2(z))$ - константа нулевизации по второму основанию $p_2(z)$,

и так далее. Продолжая данный процесс в течение k итераций, получается

$$A_k(z)=A_{k-1}(z)-M_k(z)=(0,0,...,x_{k+1}(z),...,x_{k+r}(z)).$$

Применение метода нулевизации позволяет последовательно получать наименьший полином, кратный сначала $p_1(z)$, затем полином – кратный $p_1(z)p_2(z)$, и в конечном итоге – кратный рабочему диапазону $P_{раб}(z)=\prod_{i=1}^{k} p_i(z)$.

Если в результате последовательного выполнения процедуры нулевизации будет получен нулевой результат, т.е.

$$x_{k+1}(z)=0,\ x_{k+2}(z)=0,\ \ldots,\ x_{k+r}(z)=0,$$

то это свидетельствует, что исходная комбинация $A(z)$, представленная в модулярном коде, не содержит ошибок. В противном случае – модулярный код $A(z)$ – содержит ошибки.

Основным недостатком метода нулевизации является последовательный характер вычислительного процесса. Это обусловлено прежде всего тем, что константы нулевизации представляют собой наименьшие возможные числа вида

$$M_1(z)=(s_1^1(z),s_2^1(z),...,s_k^1(z),s_{k+1}^1(z),...,s_{k+r}^1(z));$$
$$M_2(z)=(0,s_2^2(z),...,s_k^2(z),s_{k+1}^2(z),...,s_{k+r}^2(z));$$
$$\text{M}$$
$$M_k(z)=(0,0,...,s_k^k(z),s_{k+1}^k(z),...,s_{k+r}^k(z)).$$

где $s_j^i(z)=1,z,z+1,...,z^{osdp_i(z)-1}+...+z+1; i=1,2,...,k+r; j=1,...,k$.

Повысить скорость выполнения процедуры нулевизации можно за счет модификации констант нулевизации $M_i(z)$. Оставляя неизменным условие невыхода константы нулевизации $M_i(z)$ за пределы рабочего диапазона $P_{раб}(z)=\prod_{i=1}^{k} p_i(z)$, возьмем в качестве последних значения произведение остатков рабочих оснований на величину ортогональных базисов безизбыточной системы оснований

$$\begin{cases} a_1(z)B_1^*(z) \bmod P_{раб}(z)=(a_1(z),0,0,...,0,x_{k+1}^1(z),x_{k+2}^1(z),...,x_{k+1}^1(z)); \\ a_2(z)B_2^*(z) \bmod P_{раб}(z)=(0,a_2(z),0,...,0,x_{k+1}^2(z),x_{k+2}^2(z),...,x_{k+1}^2(z)); \\ \text{M} \\ a_k(z)B_k^*(z) \bmod P_{раб}(z)=(0,0,0,...,a_k(z),x_{k+1}^k(z),x_{k+2}^k(z),...,x_{k+1}^k(z)). \end{cases}$$

где $B_i^*(z)$ - ортогональный базис, безизбыточной системы оснований; $i=1,2,\ldots,k$.

Тогда если положить условие, что $A(z)\in P_{раб}(z)$, где $P_{раб}(z)=\prod_{i=1}^{k} p_i(z)$, то полином $A(z)=(a_1(z),a_2(z),...,a_k(z))$ согласно китайской теореме об остатках (КТО) можно представить в виде

$$A(z)=(a_1,(z),0,0,...,0)+(0,a_2(z),0,...,0)+...(0,0,0,...,a_k(z)).$$

Каждое слагаемое выражения (9) представляет собой

$$(0,0,\ldots 0,a_i(z),0,\ldots,0) = a_i(z)B_i^*(z) \bmod P_{раб}(z),$$

Подставим выражения (8) в равенство (10). Получаем

$$A(z) = (a_1(z),0,0,\ldots,0,(z),x_{k+1}^1(z),x_{k+2}^1(z),\ldots,x_{k+r}^1(z)) +$$
$$+(0,a_2(z),0,\ldots,0,x_{k+1}^2(z),x_{k+2}^2(z),\ldots,x_{k+r}^2(z)) + \ldots +$$
$$+(0,0,0,\ldots,a_k(z),x_{k+1}^k(z),x_{k+2}^k(z),\ldots,x_{k+r}^k(z)).$$

Следовательно, значения остатков по контрольным основаниям будут определяться

$$\begin{cases} a_{k+1}(z) = \sum_{j=1}^{k} x_{k+1}^j(z), \bmod p_{k+1}(z), \\ \text{M} \\ a_{k+r}(z) = \sum_{j=1}^{k} x_{k+r}^j(z), \bmod p_{k+r}(z). \end{cases}$$

Значит, разность полинома $A(z)$ и модифицированных констант нулевизации $M_i(z)$, $i=1, 2,\ldots, k$, псевдоортогональных форм, полученных согласно (4.5), задаёт величину нормированного следа полинома

$$\begin{cases} x_{k+1}(z) = (a_{k+1}(z) - \sum_{j=1}^{k} x_{k+1}^j(z)) \bmod p_{k+1}(z), \\ \text{M} \\ x_{k+r}(z) = (a_{k+r}(z) - \sum_{j=1}^{k} x_{k+r}^j(z)) \bmod p_{k+r}(z). \end{cases}$$

Исходя из условия, что модифицированные константы нулевизации $M_i(z)$ представляют собой ортогональные базисы безизбыточной системы оснований ПСКВ, то операция нулевизации (13) может быть реализована параллельно.

Для уменьшения объема хранимых значений констант нулевизации $M_i(z)$, $i=1, 2,\ldots, k$, представим остатком числа $\alpha_i(z)$ в виде

$$a_i(z) = a_i^{ordp_i(z)-1} z^{ordp_i(z)-1} + a_i^{ordp_i(z)-2} z^{ordp_i(z)-2} + \ldots + a_i^2 z^2 + a_i^1 z^1 + a_i^0 z^0,$$

где $a_i^j = \{0,1\}$ элементы поля $GF(2)$; $j = 0, 1, \ldots, ord\ p_i(z)-1$.

Тогда справедливо

$$a_i(z)B_i^*(z) = \left| \sum_{j=0}^{ordp_i(z)-1} (a_i^j z^j B_i(z)) mod\, P_{раб}(z) \right|_2^+ .$$

Поэтому вместо хранения $2^{ordp_i(z)}$ констант нулевизации $M_i(z)$ достаточно определить $ord\ p_i(z)$ констант.

Таким образом, два контрольных основания позволяют 100% обнаружить ошибку, а одно контрольное основание – 95% обнаружения ошибки.