УДК 621.391

ОШИБКООБНАРУЖИВАЮЩАЯ СПОСОБНОСТЬ КОДА С БИТОМ ПАРИТЕТА

КУЛИК И.А., ЧЕРЕДНИЧЕНКО В.Б.

Анализируется ошибкообнаруживающая способность кода с битом паритета для двоичного асимметричного канала передачи без памяти, когда вероятности поразрядных ошибочных переходов в кодовой комбинации неравны друг другу. Определяется условие необнаруживаемости ошибочного перехода, а также зависимости вероятности необнаруживаемой ошибки от разрядности и числа двоичных единиц комбинации.

Ключевые слова: асимметричный канал, код с битом пари-тета, вероятность необнаруживаемой ошибки.

Key words: asymmetric channel, code with parity bit, unde-tected error probability.

1. Постановка и анализ проблемы

Двоичные коды с битом паритета или проверкой на четность (нечетность) являются одними из известных и широко используемых в информационных системах различного назначения [1–3]. Широкое распространение они получили благодаря простому алгоритму получения на основе операции "сумма по модулю два". Обнаружение ошибок для таких кодов заключается в контроле числа двоичных единиц в кодовой комбинации с использованием дополнительного разряда – бита паритета. Значение бита паритета должно дополнять число двоичных единиц исходной комбинации до четного значения при контроле по четности и нечетного значения при контроле по нечетности. Нарушение четности (нечетности) единиц для комбинации с битом паритета означает появление в ней ошибки вследствие действия помехи в канале связи или возникновения аппаратурного сбоя.

На сегодняшний день оценка ошибкообнаруживающей способности рассматриваемых кодов проведена только для двоичного симметричного канала связи без памяти [1 – 3]. Но на практике в большинстве случаев имеют дело с асимметричными каналами передачи, для которых вероятности p_{01} и p_{10} ошибочных переходов (0→1) и (1→0) не равны друг другу. Поэтому оценка ошибкообнаруживающей способности кодов с проверкой на четность (нечетность) и ее анализ для случая двоичного асимметричного канала передачи представляет собой актуальную задачу.

2. Определение условия необнаруживаемости ошибочных переходов

Используя признак четности числа k единиц как признак эквивалентности, множество U всех возможных n-разрядных двоичных комбинаций, представляемое как универсум, можно разбить на классы A и B – непересекающиеся подмножества двоичных слов с четным и нечетным числами единиц соответственно: $U = A \cup B$. Очевидно, что для кода с проверкой на четность подмножество A представляет собой класс разрешенных, а подмножество B – класс запрещенных комбинаций. Для кода с проверкой на нечетность подмножества A и B меняются местами. В качестве количественной меры ошибкообнаруживающей способности кодов воспользуемся таким критерием как вероятность $P_{но}$ необнаруживаемой ошибки [4].

Теорема 1. *Пусть* $a_i \in A$ *и* $b_x \in B$ *– двоичные слова с битом четности и нечетности соответственно. Для получения* $a_j \sim a_i$ *и* $b_y \sim b_x$ *суммарное число* $q_{пр}$ *переходов вида (0→1) и (1→0) должно быть четным, где* $i, j = 1, 2, ..., |A|$, $i \neq j$ и $x, y = 1, 2, ..., |B|$, $x \neq y$.

Доказательство. Поскольку $a_j \sim a_i$ и $b_y \sim b_x$, то в соответствии со свойством эквивалентности: $a_j \in A$ и $b_y \in B$. Отсюда следует, что число k_j единиц в слове a_j является четным, а число k_y единиц в слове b_y – нечетным, и при этом они должны быть равны:

$$k_j = k_i + q_{01} - q_{10} = k_i + \Delta, \qquad (1)$$

$$k_y = k_x + q_{01} - q_{10} = k_x + \Delta, \qquad (2)$$

где k_i и k_x – числа двоичных единиц в a_i и b_x соответственно;

q_{01} и q_{10} – количество переходов вида (0→1) и (1→0) соответственно, сумма которых равна $q_{пр} = q_{01} + q_{10}$, а разность – $\Delta = q_{01} - q_{10}$.

Определим условия, при которых k_j будет четным, а k_y – нечетным. По определению четность чисел k_j и k_i означает, что их можно представить в виде $k_j = 2m$, $k_i = 2r$, а нечетность для k_y и k_x означает их представление как $k_y = 2c + 1$, $k_x = 2d + 1$, где m, r, c и d – простые числа [5].

Предположим, что Δ в выражениях (1) и (2) имеет нечетное значение. Тогда, представив его как $\Delta = 2h + 1$, где h – простое число, получим

$$k_j = k_i + \Delta = 2r + 2h + 1 = 2(r + h) + 1 = 2m + 1,$$

$$k_y = k_x + \Delta = 2d + 1 + 2h + 1 = 2(d + h) + 2 =$$

$$= 2(d + h + 1) = 2c,$$

т.е. k_j – нечетное, k_y – четное число. Это означает $a_j \notin A$ и $b_y \notin B$, что противоречит условию теоремы. Таким образом, наше предположение неверное, и $\Delta = q_{01} - q_{10}$ имеет четное значение. Следовательно, если разность q_{01} и q_{10} имеет четное значение, то их сумма $q_{пр} = q_{01} + q_{10}$ также представляет собой четное число, что и требовалось доказать.

Следствие. Для получения $a_j \sim a_i$ и $b_y \sim b_x$ числа q_{01} и q_{10} переходов вида (0→1) и (1→0) одновременно являются или четными, или нечетными.

Справедливость следствия теоремы 1 вытекает из того факта, что сумма $q_{пр} = q_{01} + q_{10}$ будет четной только в двух случаях, когда одновременно обе слагаемые суммы являются четными или, наоборот, нечетными.

Как следует из теоремы 1, условием появления необнаруживаемых ошибок для кода с проверкой как на четность, так и на нечетность является четное число $q_{пр}$ поразрядных ошибочных переходов (0→1) и (1→0), которое в свою очередь определяет одновременность четности или нечетности значений q_{01} и q_{10}.

3. Определение количества вариантов переходов комбинации с битом паритета

Полученное условие необнаруживаемости ошибочных переходов позволяет выявить количество вариантов переходов в разрешенную комбинацию –

$$a_i \to a_j \text{ или } b_x \to b_y,$$

или запрещенную –

$$a_i \to b_x \text{ или } b_x \to a_i .$$

Теорема 2. *Двоичное слово с битом паритета* a_i *или* b_x *имеет количество вариантов перехода в* $a_j \sim a_i$ *или, соответственно,* $b_y \sim b_x$, *равное*

$$R_1 = \sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} C_m^{2\alpha+1} C_k^{2\beta+1} \qquad (3)$$

при нечетных q_{01} *и* q_{10}, *и равное*

$$R_2 = \sum_{\alpha=0}^{\left\lfloor \frac{m}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_m^{2\alpha} C_k^{2\beta} - 1 \qquad (4)$$

при четных q_{01} *и* q_{10}, *где* $a_i, a_j \in A$ *и* $b_x, b_y \in B$; n *– разрядность комбинаций;* k *– число двоичных единиц,* $m = n - k$.

Доказательство. В соответствии с основным правилом комбинаторики [5] число переходов r вида $a_i \to a_j$ и $b_x \to b_y$, $i \neq j$, $x \neq y$ при заданных n и k определяется как произведение числа вариантов переходов (0→1) на число вариантов переходов (1→0). Эти числа, в свою очередь, определяются как сочетание числа q_{01} нулевых разрядов, изменяющих свое значение, из общего числа нулей m и сочетание числа q_{10} единичных разрядов, изменяющих свое значение, из общего числа единиц k. Таким образом,

$$r = C_m^{q01} C_k^{q10}, \qquad (5)$$

где q_{01} и q_{10} принимают только нечетные или только четные значения. Представим нечетные числа q_{01} и q_{10} как $q_{01} = 2\alpha + 1$ и $q_{10} = 2\beta + 1$, где α и β – целые положительные числа. Так как $1 \le q_{01} \le m$ и $1 \le q_{10} \le k$, то $0 \le \alpha \le \lfloor (m-1)/2 \rfloor$ и $0 \le \beta \le \lfloor (k-1)/2 \rfloor$. Тогда, используя (5) и вычисленные пределы изменения α и β, число переходов $a_i \to a_j$ или $b_x \to b_y$, $i \neq j$, $x \neq y$, при нечетных q_{01} и q_{10} можно определить как

$$R_1 = \sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} C_m^{2\alpha+1} C_k^{2\beta+1}.$$

Теперь представим четными $q_{01} = 2\alpha$ и $q_{10} = 2\beta$. Аналогично рассуждая и вычисляя пределы изменения q_{01} и q_{10} для этого случая, получаем, что число переходов $a_i \to a_j$ или $b_x \to b_y$, $i \neq j$, $x \neq y$, при четных q_{01} и q_{10} определяется следующим образом (без учета перехода в правильную комбинацию, когда $\alpha = 0$ и $\beta = 0$):

$$R_2 = \sum_{\alpha=0}^{\left\lfloor \frac{m}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_m^{2\alpha} C_k^{2\beta} - 1,$$

что и требовалось доказать.

Принимая во внимание общий случай, когда $|A| = |B| = 2^{n-1}$, то, очевидно, должно выполняться равенство $R_1 + R_2 + 1 = 2^{n-1}$ (n-й разряд – бит паритета). Действительно, так как согласно [5]

$$\sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} C_m^{2\alpha+1} = \sum_{\alpha=0}^{\left\lfloor \frac{m}{2} \right\rfloor} C_m^{2\alpha} = 2^{m-1} \text{ и}$$

$$\sum_{\beta=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} C_k^{2\beta+1} = \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_k^{2\beta} = 2^{k-1},$$

то, предварительно сгруппировав индексируемые переменные по соответствующим суммам,

$$R_1 + R_2 + 1 = \sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} C_m^{2\alpha+1} \sum_{\beta=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} C_k^{2\beta+1} +$$

$$+ \sum_{\alpha=0}^{\left\lfloor \frac{m}{2} \right\rfloor} C_m^{2\alpha} \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_k^{2\beta} - 1 + 1 =$$

$$= 2^{m-1} 2^{k-1} + 2^{m-1} 2^{k-1} = 2^{m+k-1} = 2^{n-1}.$$

Теорема 3. *Двоичное слово* a_i *или* b_x *с битом паритета имеет количество вариантов переходов соответственно в* b_x *или* a_i, *равное*

$$R_3 = \sum_{\alpha=0}^{\left\lfloor \frac{m-1}{2} \right\rfloor} \sum_{\beta=0}^{\left\lfloor \frac{k}{2} \right\rfloor} C_m^{2\alpha+1} C_k^{2\beta} \qquad (6)$$

при нечетном q_{01} *и четном* q_{10}, *и равное*

$$R_4=\sum_{\alpha=0}^{\left\lfloor\frac{m}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k-1}{2}\right\rfloor}C_m^{2\alpha}C_k^{2\beta+1} \qquad (7)$$

при четном q_{01} *и нечетном* q_{10}, *где* $a_i\in A$ *и* $b_x\in B$, n *– разрядность комбинаций;* k *– число двоичных единиц,* $m=n-k$.

Доказательство теоремы 3 проводится аналогично доказательству теоремы 2 с учетом того, что к переходу $a_i\to b_x$ или $b_x\to a_i$ приводят нечетное q_{01} и четное q_{10} или, наоборот, четное q_{01} и нечетное q_{10} число поразрядных переходов.

Также можно показать, что $R_3+R_4=2^{n-1}$.

4. Определение вероятностей необнаруживаемой и обнаруживаемой ошибок при заданном канале передачи

Развернутые выражения для чисел R_1, R_2, R_3 и R_4 вариантов переходов являются необходимыми для следующего этапа анализа ошибкообнаруживающей способности кода с битом паритета.

Рассмотрим асимметричную двоичную модель канала передачи информации без памяти как наиболее часто встречаемую на практике. Модель такого канала задается переходными вероятностями p_{01} и p_{10}, где $p_{01}=1-p_{00}$ и $p_{10}=1-p_{11}$.

Теорема 4. *Для кодовой комбинации* a_i *и* b_x *с битом паритета вероятность перехода вида* $a_i\to a_j$ *и* $b_x\to b_y$ *при заданных* n *и* k, *где* $i\neq j$; $x\neq y$; $i,j,x\ \ y=1,\dots,(2^{n-1}-1)$ *и* $a_j\sim a_i$, $b_y\sim b_x$ *для асимметричного двоичного канала без памяти равна*

$$V_k=\sum_{\alpha=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k-1}{2}\right\rfloor}C_m^{2\alpha+1}C_k^{2\beta+1}p_{00}^{[m-(2\alpha+1)]}p_{01}^{(2\alpha+1)}\times$$
$$\times p_{11}^{[k-(2\beta+1)]}p_{10}^{(2\beta+1)}+ \qquad (8)$$
$$+\sum_{\alpha=0}^{\left\lfloor\frac{m}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k}{2}\right\rfloor}C_m^{2\alpha}C_k^{2\beta}p_{00}^{[m-2\alpha]}p_{01}^{2\alpha}p_{11}^{[k-2\beta]}p_{10}^{2\beta}-p_{00}^{m}p_{11}^{k}.$$

Доказательство. Поскольку разрядные переходы (0→1) и (1→0) для заданной модели канала являются независимыми и несовместными событиями, то вероятность появления комбинации $a_j\sim a_i$ путем $q_{пр}=q_{01}+q_{10}$ переходов определяется как

$$p(a_j)=p_{00}^{[m-q_{01}]}p_{01}^{q_{01}}p_{11}^{[k-q_{10}]}p_{10}^{q_{10}}. \qquad (9)$$

Используя из теоремы 2 количество R_1 вариантов переходов при нечетных q_{01}, q_{10} и представления $q_{01}=2\alpha+1$, $q_{10}=2\beta+1$, для вероятности появления $a_j\sim a_i$ можно записать

$$P_1=R_1p(a_j)=\sum_{\alpha=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k-1}{2}\right\rfloor}C_m^{2\alpha+1}C_k^{2\beta+1}\times \qquad (10)$$
$$\times p_{00}^{[m-(2\alpha+1)]}p_{01}^{(2\alpha+1)}p_{11}^{[k-(2\beta+1)]}p_{10}^{(2\beta+1)}.$$

При четных q_{01} и q_{10} необходимо использовать значение R_2, представления $q_{01}=2\alpha$ и $q_{10}=2\beta$ и учесть, что существует правильный переход $a_i\to a_i$, вероятность которого

$$p(a_i\to a_i)=p_{00}^{m}p_{11}^{k}. \qquad (11)$$

Тогда вероятность появления $a_j\sim a_i$ в этом случае

$$P_2=(R_2+1)p(a_j)-p(a_i\to a_i)= \qquad (12)$$
$$=\sum_{\alpha=0}^{\left\lfloor\frac{m}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k}{2}\right\rfloor}C_m^{2\alpha}C_k^{2\beta}p_{00}^{[m-2\alpha]}p_{01}^{2\alpha}p_{11}^{[k-2\beta]}p_{10}^{2\beta}-p_{00}^{m}p_{11}^{k}.$$

Вероятность V_k появления любого $a_j\in A$ в случае как нечетных, так и четных q_{01} и q_{10} представляет собой сумму вероятностей P_1 и P_2:

$$V_k=P_1+P_2=\sum_{\alpha=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k-1}{2}\right\rfloor}C_m^{2\alpha+1}C_k^{2\beta+1}\times$$
$$\times p_{00}^{[m-(2\alpha+1)]}p_{01}^{(2\alpha+1)}p_{11}^{[k-(2\beta+1)]}p_{10}^{(2\beta+1)}+$$
$$+\sum_{\alpha=0}^{\left\lfloor\frac{m}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k}{2}\right\rfloor}C_m^{2\alpha}C_k^{2\beta}p_{00}^{[m-2\alpha]}p_{01}^{2\alpha}p_{11}^{[k-2\beta]}p_{10}^{2\beta}-p_{00}^{m}p_{11}^{k}.$$

что и требовалось доказать.

Имея теорему 3, легко доказать теорему 5.

Теорема 5. *Для кодовой комбинации* a_i *и* b_x *с битом паритета вероятность перехода вида* $a_i\to b_x$ *или* $b_x\to a_i$ *при заданных* n *и* k, *где* $i,x=1,\dots,2^{n-1}$, *для асимметричного двоичного канала без памяти равна*

$$Z_k=\sum_{\alpha=0}^{\left\lfloor\frac{m-1}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k}{2}\right\rfloor}C_m^{2\alpha+1}C_k^{2\beta}\times$$
$$\times p_{00}^{[m-(2\alpha+1)]}p_{01}^{(2\alpha+1)}p_{11}^{[k-2\beta]}p_{10}^{2\beta}+ \qquad (13)$$
$$+\sum_{\alpha=0}^{\left\lfloor\frac{m}{2}\right\rfloor}\sum_{\beta=0}^{\left\lfloor\frac{k-1}{2}\right\rfloor}C_m^{2\alpha}C_k^{2\beta+1}p_{00}^{[m-2\alpha]}p_{01}^{2\alpha}p_{11}^{[k-(2\beta+1)]}p_{10}^{(2\beta+1)}.$$

Теорема 6. *Для кода с битом паритета*

$$V_k+Z_k+p(a_i\to a_i)=1.$$

Доказательство. Чтобы доказать данное тождество, определим множество пар значений индексов в суммах (8), (13). При этом следует учесть, что $0\le q_{01}\le m$, а $0\le q_{10}\le k$. В выражении (8) числа переходов ($0 \to 1$) и ($1 \to 0$) являются или одновременно нечетными $q_{01} = 2\alpha + 1$ и $q_{10} = 2\beta + 1$, или одновременно четными $q_{01} = 2\alpha$ и $q_{10} = 2\beta$, т.е. составляют следующее множество пар $\{(2\alpha+1, 2\beta+1); (2\alpha, 2\beta)\}$. В выражении (13) при четном q_{01} число q_{10} должно быть нечетным, и наоборот, при нечетном q_{01} число q_{10} – четное, т.е. имеется множество пар $\{(2\alpha+1, 2\beta); (2\alpha, 2\beta+1)\}$. При объединении рассматриваемых множеств пар обнаружим, что формируется множество всех пар $\{(q_{01}, q_{10}): 0 \le q_{01} \le m, 0 \le q_{10} \le k\}$. Таким образом, вместо α и β можно ввести индексы q_{01} и q_{10} соответственно, принимающие значения всех целых чисел на соответствующих числовых отрезках [0; m] и [0; k]. Это позволяет объединить суммы в выражениях (8), (13). Результатом объединения с учетом (11) является следующее выражение, которое представляет собой сумму вероятностей переходов a_i в любую другую комбинацию $u_r \in U$, где $r = 0,1,\ldots,2^n - 1$:

$$V_k + Z_k + p(a_i \to a_i) = \\ = \sum_{q_{01}=0}^{m} \sum_{q_{10}=0}^{k} C_m^{q_{01}} C_k^{q_{10}} p_{00}^{(m-q_{01})} p_{01}^{q_{01}} p_{11}^{(k-q_{10})} p_{10}^{q_{10}} = 1. \quad (14)$$

Переходы $a_i \to u_r$ в (14) представляют собой полную группу событий, поэтому сумма их вероятностей должна быть равна 1, что и требовалось доказать.

5. Определение ошибкообнаруживающей способности кода при заданных источнике информации и канале передачи

При заданной модели канала (известных p_{01} и p_{10}) вероятности V_k, Z_k и $p(u_i \to u_i)$ являются величинами, зависящими от свойств n и k двоичного слова u_i, появление которого, в свою очередь, зависит от распределения вероятностей $p(s_i)$ двоичных (n-1)-разрядных слов s_h источника S информации, $s_h \in S$, $h = 0,1,\ldots,2^{n-1}$. Таким образом, для кода с битом четности при заданных источнике информации и канале передачи вероятности правильной передачи $P_{пр}$, необнаруживаемых $P_{но}$ и обнаруживаемых $P_{об}$ ошибок соответственно равны

$$P_{пр} = \sum_{i=1}^{|A|} p(a_i[k]) p(a_i \to a_i), \quad (15)$$

$$P_{но} = \sum_{i=1}^{|A|} p(a_i[k]) V_k, \quad P_{об} = \sum_{i=1}^{|A|} p(a_i[k]) Z_k, \quad (16)$$

где $p(a_i[k])$ – вероятность появления кодовой комбинации с битом четности.

В случае кода с битом нечетности в выражениях (15), (16) для вероятностей $P_{пр}$, $P_{но}$ и $P_{об}$ область суммирования A заменяется на B, а элементы суммирования $a_i[k]$ – на $b_x[k]$. Основываясь на теореме 6, можно показать, что сумма вероятностей $P_{пр} + P_{но} + P_{об}$ для кода с битом как четности, так и нечетности равна 1.

Непересекающиеся подмножества A и B ($A \cup B = U$) для кода с битом паритета можно разбить на классы эквивалентности A_k и B_k, содержащие двоичные n-разрядные слова $a_i[k] \in A_k$ и $b_x[k] \in B_k$ с числом k единиц, $0 \le k \le n$ (n-й разряд представляет собой бит паритета). При этом классы A_k имеют признак эквивалентности, равный четным значениям и нулю, а классы B_k – нечетным значениям числа k. Очевидно, что

$$A = \bigcup_{\beta=0}^{\lfloor n/2 \rfloor} A_{2\beta}, \quad B = \bigcup_{\beta=0}^{\lfloor (n-1)/2 \rfloor} B_{2\beta+1}.$$

Число n-разрядных комбинаций с k единицами – C_n^k, тогда мощности подмножеств $A_{2\beta}$ и $B_{2\beta+1}$ равны

$$|A_{2\beta}| = C_n^{2\beta} \quad \text{и} \quad |B_{2\beta+1}| = C_n^{2\beta+1},$$

где $0 \le \beta \le \lfloor n/2 \rfloor$ для A_k, $0 \le \beta \le \lfloor (n-1)/2 \rfloor$ для B_k. Принимая во внимание известное рекуррентное соотношение для биномиальных коэффициентов [5]

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1},$$

можно записать

$$|A_{2\beta}| = C_{n-1}^{2\beta-1} + C_{n-1}^{2\beta} \quad \text{и} \quad |B_{2\beta+1}| = C_{n-1}^{2\beta} + C_{n-1}^{2\beta+1}, \quad (17)$$

что согласуется с алгоритмом построения рассматриваемого кода: дополнительный n-й разряд может иметь нулевое значение, если число k единиц исходного (n-1)-разрядного слова s_h соответствует условию паритета, или единичное, если не соответствует. Как следует из теорем 4 и 5, каждому классу A_k или B_k соответствуют значения V_k или Z_k.

Для известного источника информации Бернулли вероятность $p(s_h[r])$ появления исходного двоичного (n-1)-разрядного слова s_i с числом r единиц имеет вид

$$p(s_h[r]) = p_1^r p_0^{n-r-1},$$

где p_1 и p_0 – вероятности появления двоичных единицы и нуля соответственно.

При этом если дополнительный n-й разряд с битом паритета $z_n = 0$, то $r = k$, в противном случае, когда $z_n = 1$, $r = k-1$. Очевидно, что для кода с битом по четности

$$p(a_i[2\beta]) = p(s_i[2\beta-1]) + p(s_i[2\beta]) \qquad (18)$$

при $0 \le \beta \le \lfloor n/2 \rfloor$, или по нечетности

$$p(b_x[2\beta+1]) = p(s_x[2\beta]) + p(s_x[2\beta+1]) \qquad (19)$$

при $0 \le \beta \le \lfloor (n-1)/2 \rfloor$.

Для определения вероятностей $P_{пр}$, $P_{но}$ и $P_{об}$ выполним группирование двоичных слов $a_i[k] \in A_k$ и $b_x[k] \in B_k$ в выражениях (15), (16) по числу k находящихся в них единиц. Учитывая (17), (18)? в результате для кода с контролем по четности получаем

$$P_{пр} = \sum_{\beta=0}^{\lfloor n/2 \rfloor} \left(P_{2\beta-1} + P_{2\beta}\right) \cdot p_{00}^{n-2\beta} p_{11}^{2\beta}, \qquad (20)$$

$$P_{но} = \sum_{\beta=0}^{\lfloor n/2 \rfloor} \left(P_{2\beta-1} + P_{2\beta}\right) \cdot V_{2\beta}, \qquad (21)$$

$$P_{об} = \sum_{\beta=0}^{\lfloor n/2 \rfloor} \left(P_{2\beta-1} + P_{2\beta}\right) \cdot Z_{2\beta}, \qquad (22)$$

где P_k – вероятность признака k эквивалентности:

$$P_k = C_{n-1}^{k} p_1^{k} p_0^{n-k-1}. \qquad (23)$$

Учитывая (17), (19), но уже для кода с контролем по нечетности получаем

$$P_{пр} = \sum_{\beta=0}^{\lfloor (n-1)/2 \rfloor} \left(P_{2\beta} + P_{2\beta+1}\right) \cdot p_{00}^{n-2\beta-1} p_{11}^{2\beta+1}, \qquad (24)$$

$$P_{но} = \sum_{\beta=0}^{\lfloor (n-1)/2 \rfloor} \left(P_{2\beta} + P_{2\beta+1}\right) \cdot V_{2\beta+1}, \qquad (25)$$

$$P_{об} = \sum_{\beta=0}^{\lfloor (n-1)/2 \rfloor} \left(P_{2\beta} + P_{2\beta+1}\right) \cdot Z_{2\beta+1}. \qquad (26)$$

6. Заключение

Таким образом, для кода с битом паритета определены вероятности V_k необнаруживаемой и Z_k обнаруживаемой ошибок, которые в совокупности характеризуют ошибкообнаруживающую способность кода для случая как асимметричного, так и симметричного канала без памяти. Полученные выражения (8), (13) для кода с битом паритета позволят выделить область эффективного использования одного из наиболее широко применяемых кодов и провести сравнительную оценку рассматриваемого кода с другими в зависимости от модели канала передачи. На основе оценок (21), (25) более четкой представляется разработка способов повышения ошибкообнаруживающей способности кода с битом паритета при неизменных канале связи и мощности кода. Найденные расчетные соотношения можно распространить на другие ошибкообнаруживающие и корректирующие коды, в основе построения которых лежит операция "сумма по модулю 2", например, итеративные, плоскостные, коды Хэмминга.

Литература: 1. *Скляр Бернард.* Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом "Вильямс", 2003. 1104 с. **2.** *Жураковский Ю.П.* Передача информации в ГАП. К.: Вища шк., 1991. 216 с. **3.** *Кузьмин И.В., Ключко В.И., Литвин В.А.* Кодирование и декодирование в информационных системах. К.: Вища шк., 1985. 190 с. **4.** *Борисенко А.А., Бережная О.В., Кулик И.А.* Оценка помехоустойчивости системы передачи данных на основе равновесных кодов // Вісник Сумського державного ушверситету. Технічні науки. 1999. №1(12). С. 171-173. **5.** *Райзер Дж.* Комбинаторная математика. М.: Мир, 1966. 156 с.

Transliterated bibliography:

1. *Skljar Bernard*. Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie. M.: Izdatel'skij dom "Vil'jams", 2003. 1104 s.

2. *Zhurakovskij Ju.P.* Peredacha informacii v GAP. K.: Vishha shk., 1991. 216 s.

3. *Kuz'min I.V., Kljuchko V.I., Litvin V.A.* Kodirovanie i dekodirovanie v informacionnyh sistemah. K.: Vishha shk., 1985. 190 s.

4. *Borisenko A.A., Berezhnaja O.V., Kulik I.A.* Ocenka pomehoustojchivosti sistemy peredachi dannyh na osnove ravnovesnyh kodov // Vicnik Sums'kogo derzhavnogo ushversitetu. Tehnichni nauki. 1999. №1(12). S. 171-173.

5. Rajzer Dzh. Kombinatornaja matematika. M.: Mir, 1966. 156 s.

Поступила в редколлегию 07.06.2018

Рецензент: д-р техн. наук, проф. Безрук В.М.

Кулик Игорь Анатольевич, канд. техн. наук, доцент кафедры электроники и компьютерной техники Сумского государственного университета. Научные интересы: помехоустойчивое и нумерационное кодирование, сжатие данных. Адрес: Украина, 40007, Сумы, ул. Римского-Корсакова, 2. Email: i.kulyk@ekt.sumdu.edu.ua.

Чередниченко Виталий Борисович, старший преподаватель Сумского филиала Харьковского университета внутренних дел. Научные интересы: защита данных, кибербезопасность. Адрес: Украина, 40000, Сумы, ул. Мира, 24. Email: vi.chereda@gmail.com.

Kulyk Igor Anatoliyevich, Ph.D., Assistant Professor of Electronics and Computer Technics Department of Sumy State University. Scientific interests: noise-immunity and enumeration coding, data compression. Address: Ukraine, 40007, Sumy, 2, Rimskiy-Korsakov str. Email: i.kulyk@ekt.sumdu.edu.ua.

Cherednichenko Vitaliy Borysovich, Lecturer of Sumy Branch of Kharkov University of Internal Affairs. Scientific interests: data protection, cybersecurity. Address: Ukraine, 40000, Sumy, 24, Mir str. Email: vi.chereda@gmail.com.