Определение величин ошибок.

Если номера искаженных позиций неизвестно, то величины искажений называются ошибками после того, как эти позиции определены иногда данные величины следов. "Стирание". Для стираний иногда разрабатывают "стирание" алгоритмы, или их кол-во известно заранее. Рассмотрим общий случай: проанализируем структуру компонент вектора синдрома.

$$\sum_{i=1}^{v} e_i \alpha^{l_i v} \alpha^{l_i (j-1)} = S_j.$$

e_i, α^{l_i} - известны. Пусть $p_i = \alpha^{l_i}$

Тогда распишем v уравн., начиная с $j=1$. Получим

$$e_1\alpha^{l_1 v} + e_2\alpha^{l_2 v} + e_3\alpha^{l_3 v} + \ldots + e_v\alpha^{l_v v} = S_1.$$

$$e_1\alpha^{l_1 v}p_1 + e_2\alpha^{l_2 v}p_2 + \ldots + e_v\alpha^{l_v v}p_v = S_2.$$

$$e_1\alpha^{l_1 v}p_1^2 + e_2\alpha^{l_2 v}p_2^2 + \ldots + e_v\alpha^{l_v v}p_v^2 = S_3.$$

$$\ldots\ldots\ldots$$

$$e_1\alpha^{l_1 v}p_1^{v-1} + e_2\alpha^{l_2 v}p_2^{v-1} + \ldots + e_v\alpha^{l_v v}p_v^{v-1} = S_v.$$

Эта система линейных ур-ний, которая может быть решена любым известным способом, однако, при большом кол-ве ошибок данное решение затруднительно, поэтому используем спец. метод.

Метод Форни.

Используем правило Крамера для нахождения k-той ошибки. $e_k = \frac{\Delta_k}{\Delta}$.

Δ - опред. системы ур-ний.
Δ_k - опред. в котором k-тый столбец заменен столбцом свободных членов.

Рассмотрим матрицу системы:

$$\begin{vmatrix} \alpha^{\varepsilon_1 \nu} & \alpha^{\varepsilon_2 \nu} & \alpha^{\varepsilon_3 \nu} & \dots & \alpha^{\varepsilon_r \nu} \\ \alpha^{\varepsilon_1 \nu}_{\rho_1} & \alpha^{\varepsilon_2 \nu}_{\rho_2} & \alpha^{\varepsilon_3 \nu}_{\rho_3} & \dots & \alpha^{\varepsilon_r \nu}_{\rho_r} \\ \alpha^{\varepsilon_1 \nu}_{\rho_1^2} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \alpha^{\varepsilon_1 \nu}_{\rho_1^{\nu-1}} & \alpha^{\varepsilon_2 \nu}_{\rho_2^{\nu-1}} & \dots & & \alpha^{\varepsilon_r \nu}_{\rho_r^{\nu-1}} \end{vmatrix}$$

Вычислим данный определитель.
Вычли из 1 столбца $\alpha^{\varepsilon_i \nu} = \rho_1^{\nu}$
из 2 столбца $\alpha^{\varepsilon_2 \nu} = \rho_2^{\nu}$
и т.д. из посл. столбца $\alpha^{\varepsilon_r \nu} = \rho_r^{\nu}$.

Получили коэф. $\rho_1^{\nu}, \rho_2^{\nu} \dots \rho_r^{\nu}$ в которых фигурируют все наборы подстановок $\rho_1, \rho_2 \dots \rho_r$.

В рез-те получили след. матрицу.

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \rho_1 & \rho_2 & \rho_3 & \dots & \rho_r \\ \rho_1^2 & \rho_2^2 & \rho_3^2 & \dots & \rho_r^2 \\ \dots & \dots & \dots & \dots & \dots \\ \rho_1^{r-1} & \rho_2^{r-1} & \rho_3^{r-1} & \dots & \rho_r^{r-1} \end{vmatrix}$$

Это определитель Вандермонда.

Определитель имеет вид $\bar{\Delta} = \prod\limits_{1 \le j \le i \le r} (\rho_i - \rho_j) =$

$= \prod\limits_{1 \le j \le i \le r} (\rho_i + \rho_j)$.

Пример: $\rho_1\ \rho_2\ \rho_3\ \rho_4$.

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ \rho_1^2 & \rho_2^2 & \rho_3^2 & \rho_4^2 \\ \rho_1^3 & \rho_2^3 & \rho_3^3 & \rho_4^3 \end{vmatrix} \Rightarrow$$

$\bar{\Delta} = (\rho_2 + \rho_1)(\rho_3 + \rho_2)(\rho_3 + \rho_1)(\rho_4 + \rho_3) \cdot (\rho_4 + \rho_2)(\rho_4 + \rho_1)$.

↓

Возьмем произв-ное число, например p_1. Рассмотрим в данном определителе те слагаемые, в которых p_1 отсутствует. $(p_3+p_2)(p_4+p_3)(p_4+p_2)$.

Это опред. Вандермонда построенного по элем. $p_2\ p_3\ p_4$ в степенях отсутств. p_1. Обозначим его Δp_1

В общем случае можно записать:

$$\Delta = (p_2+p_1)(p_3+p_2)(p_3+p_1)\dots(p_v p_{v-1})\dots(p_v+p_1).$$

Возьмем произв. любую p_k и рассмотрим мн. множ, в которых p_k отсутствует. Обозначим детерминант из этих мнетных множителей, как Δp_k. Он состав. определителю, построенному на элементах $p_1, p_2 \dots p_{k-1}, p_{k+1} \dots p_v$. А во вер оставшемся мнетном множ. входит p_k. Тогда детерминант матрицы системы можно записать в сл. виде.

$$\Delta = p_1^v p_2^v \dots p_v^v \ \Delta^{p_k} \prod_{i \neq k} (p_k + p_i)$$

Анализ полинома локатора.

Полином $\sigma(z)$ имеет корни $\frac{1}{p_1}, \frac{1}{p_2} \dots \frac{1}{p_v}$.

Т.е. $\sigma(z) = (1+zp_1)(1+zp_2)\dots(1+zp_v) =$

$= \sigma_v z^v + \sigma_{v-1} z^{v-1} + \dots + \sigma_1 z + \sigma_0$. $\sigma_0 = 1$.

$\sigma_1 = p_1 + p_2 + p_3 + \dots + p_v$.

$\sigma_2 = p_1p_2 + p_1p_3 + \dots + p_{v-1}p_v$.

$\sigma_3 = p_1p_2p_3 + p_1p_2p_4 + \dots + p_{v-2}p_{v-1}p_v$.

. . . . . .

$\sigma_v = p_1 p_2 \dots p_v$.

попробуем вычислить Δ через полином локатора

Для этого рассмотрим полином с инверсными коэф. $\overleftarrow{\sigma}(z)$

$\overleftarrow{\sigma}(z) = z^{\nu}\sigma\left(\frac{1}{z}\right)$. ; $\overleftarrow{\sigma}(z) = (z+p_1)(z+p_2)\dots(z+p_\nu)$.

При подстановке $z = p_k$ полином обращается в ноль.

Найдем производную полинома вместе производной произв. 2 функций.

$$\overleftarrow{\sigma}'(z) = (z+p_2)(z+p_3)\dots(z+p_\nu) + (z+p_1)\Big[(z+p_3)(z+p_4)\dots(z+p_\nu) + (z+p_2)\Big[$$

$$\Big[(z+p_4)(z+p_5)\dots(z+p_\nu) + \dots + (z+p_{\nu-2})\Big[(z+p_\nu) + (z+p_{\nu-1})\Big]\Big]\dots\Big] =$$

$$= (z+p_2)(z+p_3)\dots(z+p_\nu) + (z+p_1)(z+p_3)\dots(z+p_\nu) + (z+p_1)(z+p_2)\dots(z+p_{\nu-1}) =$$

$$= \sum_{k=1}^{\nu} \prod_{j,j\neq k} (p_j + p_j).$$

Подставим $z = p_k$. В результате все слагаемые обратятся в ноль за исключением одного, в котором отсутствует $z+p_k$.

$$\overleftarrow{\sigma}'(p_k) = (p_k+p_1)(p_k+p_2)\dots(p_k+p_{k-1})(p_k+p_{k+1})\dots(p_k+p_\nu).$$

При вычислении детерминанта матр. системы нет надежды прощь. тех синдромах членов, в которых отсутствует p_k и в которых p_k присутствует. $\Rightarrow$ можно записать

$$\Delta = p_1^{\nu} p_2^{\nu} \dots p_\nu^{\nu}\, \Delta^{p_k} \overleftarrow{\sigma}'(p_k).$$

Вычисление Δ_k.

Заменим k-тый столбец вектором столбцом $(S_1, S_2, \dots S_\nu)^T$.

$$\begin{vmatrix} \alpha^{i_1\nu} & \alpha^{i_2\nu} \dots \alpha^{i_{k-1}\nu} & S_1 & \alpha^{i_{k+1}\nu} \dots \alpha^{i_\nu\nu} \\ \alpha^{i_1\nu} p_1 & \alpha^{i_2\nu} p_2 \dots \alpha^{i_{k-1}\nu} p_{k-1} & S_2 & \alpha^{i_{k+1}\nu} p_{k+1} \dots \alpha^{i_\nu\nu} p_\nu \end{vmatrix}$$

$$\begin{vmatrix} \alpha^{l_1 1} p_1^2 & \alpha^{l_2 1} p_2^2 \dots \alpha^{l_{k-1} 1} p_{k-1} & S_3 \alpha^{l_{k+1} 1} p_{k+1} \dots \alpha^{l_v 1} p_v^2 \\ \alpha^{l_1 v} p_1^{v-1} & \alpha^{l_2 v} p_2^{v-1} \dots \alpha^{l_{k-1} v} p_{k-1}^{v-1} & S_v \alpha^{l_{k+1} v} p_{k+1}^{v-1} \dots \alpha^{l_v v} p_v^{v-1} \end{vmatrix}$$

Вынесем $\alpha^{l_1 1} = p_1^1$, $\alpha^{l_2 1} = p_2^1$, $\alpha^{l_{k-1} 1} = p_{k-1}^1$, $\alpha^{l_{k+1} 1} = p_{k+1}^1$, $\alpha^{l_v 1} = p_v^1$.

$$p_1^1 \; p_2^1 \dots p_{k-1}^1 \; p_{k+1}^1 \dots p_v^1$$

Разложим оставшийся определитель по столбцу, состоящего из компонент синдрома.

$$S_1 \begin{vmatrix} p_1 & p_2 & p_3 \dots & p_{k-1} & p_{k+1} \dots & p_v \\ p_1^2 & p_2^2 & \dots & p_{k-1}^2 & p_{k+1}^2 \dots & p_v^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ p_1^{\gamma-1} & p_2^{\delta-1} & \dots & p_{k-1}^{\delta-1} & p_{k+1}^{\gamma-1} \dots & p_v^{\gamma-1} \end{vmatrix} + S_2 \begin{vmatrix} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ p_1^2 & p_2^2 & \dots & p_{k-1}^2 & p_{k+1}^2 & \dots & p_v^2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_1^{v-1} & p_2^{v-1} & \dots & p_{k-1}^{v-1} & p_{k+1}^{v-1} & \dots & p_v^{v-1} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ p_1 & p_2 & \dots & p_{k-1} & p_{k+1} & \dots & p_v \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_1^{\ell-1} & p_2^{\ell-1} & \dots & p_{k-1}^{\ell-1} & p_{k+1}^{\ell-1} & \dots & p_v^{\ell-1} \end{vmatrix} + S_{\ell+1} \begin{vmatrix} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ p_1^{\ell+1} & p_2^{\ell+1} & \dots & p_{k-1}^{\ell+1} & p_{k+1}^{\ell+1} & \dots & p_v^{\ell+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_1^{v-1} & p_2^{v-1} & \dots & p_{k-1}^{v-1} & p_{k+1}^{v-1} & \dots & p_v^{v-1} \end{vmatrix} + S_v \begin{vmatrix} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ p_1 & p_2 & \dots & p_{k-1} & p_{k+1} & \dots & p_v \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_1^{v-2} & p_2^{v-2} & \dots & p_{k-1}^{v-2} & p_{k+1}^{v-2} & \dots & p_v^{v-2} \end{vmatrix}$$

Проанализируем структуру определителя:

Все определители имеют размер $v-1 * v-1$.

Последний определитель – это опред. Вандермонда, поэтому

на элементах $p_1 p_2 \dots p_{k-1} p_{k+1} \dots p_v$. Его $\det = \Delta^{p_k}$ – это не степень это символ обозначения.

Остальные определители имеют нулевую строку с номером e, кроме $e=0$ при S_1. эти определители сводятся к определителю Вандермонда, построенного на тех же элементах, что и контрит и $*$ из коэф. Qe. Т.е. имеет вид:

Δ^{p_k}. Qe. Причем Qe – это сумма всевозможных произведений p_i взятых в кол-ве $(v-1)-e$, $\Rightarrow$ при константе $\exists v$ $Q_{v-1} = 1$

При S_{v-1} $Q_{v-2} = p_1 + p_2 + \dots + p_{k-1} + p_{k+1} + \dots + p_v$.

$e = v-2$ и кол-во элементов в произв. $(v-1)-(v-2) = 1$

При S_{v-2} Q_{v-3} состоит из суммы по 2 элемента. везде отсутствуют элемент p_k. И т.д. при S_1 коэф. $Q_0 = p_1 p_2 \dots p_{k-1} p_{k+1} \dots p_v$.

Пример:

$$\begin{vmatrix} S_1 & 1 & 1 & 1 \\ S_2 & p_2 & p_3 & p_4 \\ S_3 & p_2^2 & p_3^2 & p_4^2 \\ S_4 & p_2^3 & p_3^3 & p_4^3 \end{vmatrix} = \underbrace{(p_2+p_3)(p_3+p_4)(p_2+p_4)}_{\Delta^{p_1}} \cdot \Big[S_4 + S_3(p_2+p_3+p_4) + S_2(p_2p_3 + p_3p_4 + p_2p_4) + S_1 p_2 p_3 p_4 \Big].$$

Т.О. $\Delta_k = p_1^v p_2^v \dots p_{k-1}^v p_{k+1}^v \dots p_v^v \Delta^{p_k} Z(S_i, Q)$ результат раскрытия определителя после вынесения за скобки Δ^{p_k}.

Анализ полинома ошибок.

Рассмотрим полином ошибок и выведем $Z(S_i, Q)$. Т.е. коэф. полинома определ. σ_i S_i, а σ зависит от p_i.

$$\omega_0 = S_1$$
$$\omega_1 = S_2 + \sigma_1 S_1$$
$$\omega_2 = S_3 + \sigma_1 S_2 + \sigma_2 S_1$$
$$\omega_3 = S_4 + \sigma_1 S_3 + \sigma_2 S_2 + \sigma_3 S_1$$
$$\dots\dots\dots\dots$$

(*
- p_k^{v-1}
- p_k^{v-2}
- p_k^{v-3}
- p_k^{v-4}.

Можно аналогично $\omega(p_k)$ и $\overleftarrow{\omega}(p_k)$. Однако $\overleftarrow{\omega}(p_k)$ приводит к требуемым выкладкам

Построим $\overleftarrow{\omega}(p_k)$.

смотри (*)

Сделаем эти отрезки. При этом вынесем за скобки S_1 и определим коэф. при нем, S_2 и его коэф., S_3 и т.д.

$$\overleftarrow{\omega}(p_k) = S_1\left[p_k^{\nu-1} + \sigma_1 p_k^{\nu-2} \dots + \sigma_{\nu-2} p_k + \sigma_{\nu-1}\right] +$$

$$S_2\left[p_k^{\nu-2} + \sigma_1 p_k^{\nu-3} \dots + \sigma_{\nu-3} p_k + \sigma_{\nu-2}\right] +$$

$$S_3\left[p_k^{\nu-3} + \sigma_1 p_k^{\nu-4} \dots + \sigma_{\nu-4} p_k + \sigma_{\nu-3}\right] +$$

$$\dots\dots\dots$$

$$+ S_{\nu-3}\left(p_k^3 + \sigma_1 p_k^2 + \sigma_2 p_k + \sigma_3\right) +$$

$$+ S_{\nu-2}\left(p_k^2 + \sigma_1 p_k + \sigma_2\right) +$$

$$+ S_{\nu-1}\left(p_k + \sigma_1\right) +$$

$$+ S_\nu.$$

Просчитаем коэф. при S. При S_ν коэф = 1 тоже совпадает с коэф! $\Sigma(S_i Q)$. $S_{\nu-1}$ коэф. $(p_k + \sigma_1) \to p_1 + p_2 + \dots p_{k-1} + p_{k+1} \dots + p_\nu$.

$S_{\nu-2}$ коэф - это сумма всех произв. по 2 элемента, не включ. p_k.

Аналогично, при $S_{\nu-3}$ коэф - это сумма по 3 элемента, не включающих p_k и т.д. $\Rightarrow$

$$\overleftarrow{\omega}(p_k) = \Sigma(S_i Q).$$

$$\Delta_k = p_1^\nu p_2^\nu \dots p_{k-1}^\nu p_{k+1}^\nu \dots p_\nu^\nu \Delta^{p_k} \overleftarrow{\omega}(p_k).$$

Тогда определим величину ошибки ε_k

$$\varepsilon_k = \frac{\Delta_k}{\Delta} = \frac{p_1^\nu p_2^\nu \dots p_{k-1}^\nu p_{k+1}^\nu \dots p_\nu^\nu \Delta^{p_k} \overleftarrow{\omega}(p_k)}{p_1^\nu p_2^\nu \dots p_\nu^\nu \Delta^{p_k} \overleftarrow{\sigma}'(p_k)}.$$

$$e_k = \frac{1}{p_k'} \frac{\omega(p_k)}{\sigma'(p_k)}$$ – формула Форни.

6.12.06.

Производная в конечном поле F_2^m

При определ. величин ошибок необх. вычислить произв.-ное от функц. вида z^k. Из анализа известно, что $(z^k)' = kz^{k-1}$.

$\Rightarrow z^{k-1}$ суммируется k-раз. В конечном поле данная формула имеет вид $((k))\, z^{k-1}$.

Если k – четное, то сумма одинаковых слагаемых, встр-ся четное число раз $= 0$.
Если k – нечетное, тогда данная сумма равна $z^{k-1} \Rightarrow$ в поле F_{2^m}. $(z^{2k+1})' = z^{2k}$

$$(z^{2k})' = \underbrace{z^{2k-1} + z^{2k-1} + \dots z^{2k-1}}_{2k \text{ раз}} = 0.$$

Частотный метод кодирования и декодирования.

Пусть дан информ. блок, состоящий из k символов. Дополним справа этот блок n нулями, тогда длина слова стала n. Построим обратное ФНС преобразование.

Если матрица прямого ФНС преобразования состоит из элементов $\alpha^{kl}, l = \overline{1,n}$ в F_{2^q}, то матрица обратного ФНС преобразов. построена из элементов $(\alpha^{-1})^{kl}$ $\alpha^{-1} = 15$. в F_{2^q}. Т.о. матрица обратного ФНС преобразования имеет вид единичную окантовку, а ее остров – инвертирован. (по отношению к матрице прямого преобразования)

Пусть Φ и Φ^{-1} прямое и обратное ФНС преобразов.

$(V_0, V_1 \dots V_{n-1})$ преобразующий вектор. Тогда $(V_0, V_1, \dots V_{n-1})\Phi^{-1} =$

$= (V_0, V_{n-1}, V_{n-2} \dots V_1) \cdot \Phi$. Нужно перегруппировать элементы преобраз. вектора и использовать матрицу прямого ФНС преобразования. Полученное слово передаем в канал.

Полученный из канала вектор может содержать ошибки.

Реализуем прямое ФНС преобразование. Если ошибки присутствуют, тогда m символов спектра будут отличны от нуля.

Если же они нулевые, то инф. k-символы будут совпадать...

Т.о. рассматриваемые „первые" m-символов имеют смысл синдрома. Возьмем эти символы и ТБМ или Сугиямы найдем $\sigma(z)$...

С помощью коэф. полинома $\sigma(z)$ рассчитаем продолжение синдрома, вычислив последов.-но k-символов.

Полученный вектор хар-ет спектр конфиг. ошибки.

Если теперь полученное из канала слово сложить по координатно с.о словом полученным продолжением, то m доп. символов станут 0 а k символов будут соотв. исходному информ. блоку.

Коды Рида - Майлера.

Коды бывают двоичные и недвоичные. Наиболее распространены двоичные коды. Для их описания удобно использовать теорию булевых функций.

Рассмотрим пространство: $V_m = F_2 \times F_2 \times \dots F_2 = F_2^m$. Его компонентами будут вектора x, содержащие набор из m компонент вектор принимающий значения в поле F_2.

Введем базис $e_1 = (1,0\dots0)$, $e_2 = (0,1,0\dots0) \dots e_m (0,0\dots1)$.

Тогда $X = x_1e_1 + x_2e_2 + \dots x_me_m$. где $x_1, x_2 \dots x_m$ координаты вектора.

Отображение $V_m \to F_2$ назв. булевой функцией.

Функция образ. таблицей или записывается в аналитической форме, где $x_1 x_2 \dots x_m$ рассматр. как переменные.

Рассмотрим $x_{i1}^{\sigma_1} x_{i2}^{\sigma_2} \dots x_{ik}^{\sigma_k}$ $\sigma_i \in F_2$.

$x_{im}^{1} = x_{im}$, $x_{im}^{0} = \bar{x}_{im}$.

конъюнкция назв. элементарной, если $x_{ip} \neq x_{im}$ $\forall p \neq m$ каждая переменная встречается в конъюнкции 1 раз.

Элементарная конъюнкция назв. монотонной, если в ней отсутствуют отрицания. Кол-во переменных в монотонной конъюнкции назв. ее рангом.

Рассмотрим $k_1 + k_2 \dots + k_{15}$ k_i - различные монотонные конъюнкции.

Данный полином - полином Жегалкина.

Пусть кол-во переменных $= n$, 1 - это монотонная конъюнкция $= 0$.

тогда можно рассмотреть всевозможные мономы. лин. и построить полином макс. длины.

Каждую конъюнкцию можно записать:

$x_1^{u_1} x_2^{u_2} \dots x_m^{u_m}$ $u_i = 1$, то данная переменная содержится в конъюнкции.

$u_i = 0$, то переменная отсутствует.

⇒ любую конъюнкцию можно записать.

$u = \{u_1, u_2 \dots u_m\} \in V_m$, которые определяют переменные.

Для этого вектора опред. ранг.

В полиноме Жегалкина все конъюнкции могут быть упорядочены в порядке 1-ми их рангов.
Внутри конъюнкции одного ранга также введем упорядоченность.

⇒ можно ввести коэф, зависящий от вектора u, который = 1, если данная конъюнкция присутствует в полиноме, а если = 0, то конъюнкция отсутствует.

Часто полиномную компакт. запись. Вида:

$g(u) x^u$ → конъюнкция
↓
коэф, опред. вектором u

∃ Теорема, утверждающая, что ∀ булевую функцию можно представить с помощью полинома Жегалкина

Max ранг конъюнкции в полиноме Жегалкина называется алгебраической степенью булевой функции. И записывается $\deg f(x)$.
Если алгебраич. степень не превышает 1, то такая степень назыв. АФФИННОЙ и ее полином Жегалкина:

$f(x) = g_1 x_1 + g_2 x_2 + \dots + g_m x_m + b$ $b \in F_2$

Если $b \equiv 0$, то такие функции назыв. линейные.

Часто говорят о степени нелинейности пол. Жегалкина, рассматривая так. ранг его конъюнкции.

Свойства и определения.

Пусть $f(x)$ булевая функция от m переменных. Возьмем $k < m$ переменных и подставим вместо них константы. (комб. 0 и 1).
Получившиеся т.о. функции назыв. подфункциями $f(x)$. Весом булевой функции $f(x)$ наз. кол-во векторов x при кот. $f(x)=1$.

Пусть задан вектор $u \in V_m$, тогда произв. $f(x)$ по направл. u

будет $D_u f(x) = f(x+u) + f(x)$.

Определение кодов Рида — Маллера.

Пусть $f(x)$ — булева функция от m переменных и её соотв. полином Жегалкина. Рассмотрим $u \in V_m$, расположенное в порядке естественного двоичного возрастания.
Рассмотрим строку $\Omega_f = \{f(u_0), f(u_1) \dots f(u_{2^m-1})\}$.

Но т.о. Введем $r \leq m$. Тогда кодом $RM(r,m)$ назыв.

множество всех строк Ω_f для тех функций f алгебр. степень которых не превышает r, т.е. огранич. макс. ранг конъюнкции в полиноме Жегалкина.

$\deg f(x) = r$.

Рассмотрим полином Жегалкина для функции со степенью r. Тогда можно посчитать кол-во коэффициентов в полиноме

$K = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}$ Всего в полином можно внести

k-коэф., которые явл. информ. символами.

Для опред. min. кодового расстояния сформулируем несколько предложений.

1. $f(x)$ имеет степень r, то ее произв. по любому направл. имеет степени не превышающие $r-1$
$\exists$ такие направл., в которых степень произв $= r-1$.

Выделим в $f(x)$ конъюнкц. ранга r и возьмем в ней произв. переменную x_i. Сгруппируем конъюнкц., содержащие x_i и вынесем x_i за скобки.
Тогда $f(x) = x_i \cdot f_1(x) + f_2(x)$.

$f_2(x)$ – остальн. конъюнкц., в которых нет x_i.

Выберем $u = (0,0 \ldots 1 \ldots 0)$, где единица соотв. x_i.

$f(x+u)$ $x_i \to x_i+1$. После прибавл. $f(x)$ получим произв-ную вида: $D_u f(x) = f_1(x)$.

Но $f_1(x)$ имеет алгебраич. степень $r-1$ $\Rightarrow$ такое направл. $\exists$-ет.

Рассмотрим произв. направл. т.е. вектор u и возьмем в $f(x)$ произв. конъюнкцию. Тогда $f(x+u)$ сводится к прибавлению единиц соотв. направлению соотв. переменных входящих в конъюнкцию.

Прибавлен. $f(x)$ для данной конъюнкции означает ее уничтожение и остается только конъюнкции меньшего ранга.

2. Если $f(x)$ булевая функция тогда вес $f(x)$ $wt[f(x)] \geq \frac{1}{2} wt[D_u f(x)]$.

Поскольку $D_u f(x) = f(x+u) + f(x)$. К тому же сдвиг аргумента на постоянный вектор u не меняет вес функции

вес = wt

$wt[D_u f(x)] \leq 2 wt f(x)$.

3. Пусть алгебраич. степень $f(x) = d$, тогда $\overset{всс}{wt} f(x) \geq 2^{m-d}$.

Доказем данное утверждение по индукции. Пусть $d=0$, тогда $\exists$ единственная ф-ция нулевой степени $f(x)=1$. При подстановке всевозможных векторов $x=\overline{0,n}$ получаем вес 1 $\Rightarrow$ вес этой функции 2^m. Для $d=0$ утверждение доказано.

Допустим, что данное утверждение выполняется $wt f(x) \geq 2^{m-d_0}$.

Докажем d_0+1 – для степени d_0. Тогда функция имеет свойство, что степень уменьш. будет равна $(d_0+1)-1=d_0$.

$\Rightarrow$ вращ. этой функции $wt[D_u f(x)] \geq 2^{m-d_0}$ (1).

Т.к. $f(x)$ имеет степень d_0+1 можно записать, что вес

$wt f(x) \geq \frac{1}{2} wt[D_u f(x)]$. подставим (1) в данное получим $wt f(x) \geq 2^{m-d_0-1} = 2^{m-(d_0+1)}$.

Данное утверждение определяет нижнюю границу веса функции.

4. Верхняя граница веса функции $f(x)$. Пусть в $f(x)$ m перем. $x_1, x_2 \dots x_m$. Возьмем в качестве значения, наборы их ранга d.

Зафиксируем эти значения, определим оставшиеся переменные $(m-d)$ их кол-во. построим 2^{m-d} подфункций путем подстановки 2^{m-d} переменных всевозможных комбинаций 0 и 1.

Получим подфункции f_i. $f_i \neq 0$.

$\Rightarrow wt f_i(x) \geq 1$, тогда $f_i \neq 1$, а у единичной функции 2^d

$wt f_i(x) \leq 2^d - 1$.

$1 \leq wt f_i(x) \leq 2^d - 1$.

Вес функции $f(x)$ будет равен весу всех подфункций.

$\Rightarrow 2^{m-d} \leq wt f(x) \leq 2^m - 2^{m-d}$.

Минимальное кодовое расстояние

В кодах Рида-Маллера min кодов. расст. опред. как min вес кодового слова. Определено, что вес f(x)

$W[f(x)] \geq 2^{m-d}$. d - алгебр. степень f(x).

RM(r,m).

В коде Рида-Маллера $d=r$. $\Rightarrow 2^{m-r}$.

Порождающая матрица кода.

Возьмем полный полином Жегалкина от m перемен. с упорядочением по рангам конъюнкций и с упоряд. конъюн. с множеством одинакового ранга.

Возьмем конъюн. 0 ранга 1. Подставим всевозможные значения x. Тогда получим строку 2^m, состоящую из 1.

Обозначим ее как матрицу $G_0=(1,1\ldots1)$.

Рассмотрим конъюн. 1 ранга и выберем x_1. Произведем те же самые операции, аналогично поступим с $x_2 \ldots x_m$. Полученные m строк объединим в G_1.

$$G_1 = \begin{pmatrix} \Omega x_1 \\ \Omega x_2 \\ \vdots \\ \Omega x_m \end{pmatrix}. \quad \text{и т.п.} \quad G_2 = \begin{pmatrix} \Omega x_1 x_2 \\ \vdots \\ \Omega_{m-1} \Omega_m \end{pmatrix}. \ldots$$

Последняя матрица будет G_m, которая порождена $x_1 x_2 \ldots x_m$. Очевидно, что эта строка содержит единственную 1. Тогда полная матрица будет иметь вид:

G_0
G_1
G_2
$\vdots$
G_m

Для того чтобы построить порожд-щую матрицу RM нужно вырезать из полной матрицы все матрицы до G_r включительно.