А. А. Давыдов, Построение линейных покрывающих кодов, *Пробл. передачи информ.*, 1990, том 26, выпуск 4, 38–55

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 26 1990 Вып. 4

УДК 621.391.15

А. А. Давыдов

ПОСТРОЕНИЕ ЛИНЕЙНЫХ ПОКРЫВАЮЩИХ КОДОВ

Предложена конструкция линейных двоичных покрывающих кодов (covering codes), позволяющая на основе любого кода с радиусом покрытия R построить бесконечное семейство кодов с тем же радиусом покрытия. Построены бесконечные семейства линейных двоичных покрывающих кодов с $R \geqslant 2$, имеющие лучшие параметры, чем известные коды.

§ 1. Введение

В последнее время покрывающие коды и другие вопросы, связанные с покрытием пространств над конечным алфавитом, интенсивно изучаются (см., например, [1—19] и библиографию в них). В данной работе рассматриваются линейные двоичные покрывающие коды.

Некоторые идеи данной работы можно рассматривать как развитие и обобщение результатов работы [18].

Введем обозначения: $[n, k]R$-код — линейный код длины n, размерности k и радиуса покрытия R; $t[n, k]$ — минимально возможный радиус покрытия линейного кода длины n и размерности k; $[n, n-r]R$-код — линейный код длины n, избыточности r и радиуса покрытия R; $\lfloor x \rfloor$ — целая часть x; $\lceil x \rceil$ — ближайшее к x целое, не меньшее x; $l(r, R)$ — минимальная длина линейного кода избыточности r и радиуса покрытия R [16]; $\mu[n, R, C]$ — плотность покрытия n-мерного пространства шарами радиуса R, центры которых соответствуют словам кода C длины n и радиуса покрытия R (плотность покрытия вычисляется как отношение суммарного объема всех шаров к объему пространства [4, с. 692; 14]).

Для бесконечного семейства кодов U, состоящего из кодов радиуса покрытия R, представляет интерес следующая величина:

$$\bar{\mu}[R, U] \stackrel{\Delta}{=} \liminf_{n \to \infty, U(n) \in U} \mu[n, R, U(n)], \tag{1.1}$$

где $U(n)$ — код длины n из семейства U.

Код с избыточностью r имеет радиус покрытия R, если любой столбец длины r может быть представлен как сумма R или менее столбцов проверочной матрицы [2, 3]. Добавив любой столбец в проверочную матрицу $[n, n-r]R$-кода, получим $[n+1, n+1-r]R_1$-код, $R_1 \leqslant R$. Поэтому бесконечные семейства покрывающих кодов с фиксированным R часто описывают путем указания для заданного r наименьшей длины n кода из данного семейства, записывая n как функцию от r.

В данной работе рассматривается построение бесконечных семейств покрывающих $[n, n-r]R$-кодов. При построении таких семейств следует стремиться к уменьшению n для заданных r и R [1, 16].

Лучшие коды с $R=1$ — $[n=2^r-1, n-r]1$ — коды Хэмминга [1].

Для $R=2$ в [18] построено семейство кодов S с параметрами

$$R=2, n=\begin{cases} 5\times 2^{c-2}-1 & \text{для } r=2c-1, \\ 7\times 2^{c-2}-2 & \text{для } r=2c, \end{cases} \quad c \geqslant 4, \bar{\mu}[2, S]=49/32. \tag{1.2}$$

Для $R\geqslant 3$ бесконечные семейства покрывающих кодов строятся (см., например, [1, 5, 11, 16, 18]) путем использования кодов с $R=1$, 2 в предложенных Грэхэмом и Слоэном [1] конструкциях DS (direct sum — прямая сумма), ADS (amalgamated DS — амальгамная прямая сумма), EDS (extended DS — расширенная прямая сумма), BEDS (bordered EDS — окаймленная прямая сумма).

В данной работе предложена конструкция, позволяющая для любого заданного R построить проверочную матрицу линейного двоичного кода V с радиусом покрытия R, исходя из проверочной матрицы произвольного двоичного кода V_0 с радиусом покрытия R_0, где $R_0\leqslant R$. (Чаще всего при использовании предложенной конструкции $R_0=R$.)

Если исходный код V_0 имеет длину Q и избыточность s, то построенный код V имеет длину n и избыточность r

$$n=2^mQ+N(m),\ r=s+mR, \tag{1.3}$$

где m — целый параметр, $N(m)$ — число столбцов используемой в конструкции вспомогательной матрицы.

Параметр m ограничен снизу, но может произвольно расти, т. е. строится *бесконечное семейство* кодов V.

Для уменьшения $N(m)$ исходный код V_0 в рассматриваемой конструкции трактуется как R_0^*, l-подмножество Q-мерного пространства (определение см. в § 2). При этом для $l\geqslant 1$ любой столбец длины s, включая нулевой, может быть получен как сумма не менее l и не более R_0^* столбцов проверочной матрицы кода V_0. Соотношение между параметром R_0^* и радиусами покрытия кодов V и V_0 имеет вид $R\geqslant R_0^*\geqslant R_0$. (Часто справедливо $R=R_0^*=R_0$.)

Построенные коды V — нормальные [1] и могут использоваться в конструкции ADS.

Предложенная конструкция достаточно гибкая и допускает различные варианты реализации.

В качестве примеров использования предложенной конструкции и ее вариантов в работе построены бесконечные семейства кодов с радиусом покрытия $R\geqslant 2$, имеющие лучшие параметры, чем известные коды. В частности, построены семейства кодов V^1-V^4 с параметрами

$$R=2,\ n=55\times 2^{c-5}-2,\ r=2c,\ c\geqslant 5,\ \bar{\mu}[2, V^1]\approx 1{,}477, \tag{1.4}$$

$$R=3, n=\begin{cases} 311\times 2^{c-7}-3 & \text{для } r=3c,\ c\geqslant 7,\\ 823\times 2^{c-9}-3 & \text{для } r=3c-1,\ c\geqslant 9,\ \bar{\mu}[3, V^2]\approx 1{,}384,\\ 2^{c+1}-1 & \text{для } r=3c-1,\ c=\overline{5,8}, \end{cases} \tag{1.5}$$

$$R=4,\ n=2^{c+1}-2,\ r=4c-3,\ c\geqslant 5, \tag{1.6}$$

$$R\geqslant 16,\ r=Rc,\ 2^c\geqslant 8R+5{,}2\sqrt{R}+16, \tag{1.7}$$

$$n<0{,}5R\times 2^{r/R}(1+1{,}5/\sqrt{R})+0{,}15\times 2^{r/R}-\sqrt{R}.$$

Из (1.4)—(1.6) следует, что

$$t[53, 43]=2,\ t[63, 49]=t[64, 50]=3,\ t[62, 45]=t[63, 46]=4. \tag{1.8}$$

Соотношения (1.4)—(1.7) являются верхними границами величины $l(r, R)$. Так, из (1.4) имеем

$$l(10,2)\leqslant 53,\ l(12,2)\leqslant 108,\ l(14,2)\leqslant 218,\ l(16,2)\leqslant 438. \tag{1.9}$$

Предложенная конструкция естественным образом переносится на недвоичные линейные покрывающие коды над полем $GF(q)$, $q>2$. (Для иллюстрации в § 3 построено семейство кодов V^5 с параметрами $q=3$, $R=2$, $\bar{\mu}[2, V^5]\approx 1{,}185$.)

Работа организована следующим образом. В § 2 даны обозначения и определения, в § 3 описана общая конструкция покрывающих кодов и варианты ее реализации, в §§ 4, 5 приведены примеры использования предложенной конструкции для построения семейств кодов с $R=2$ и $R\geqslant 3$.

§ 2. Обозначения и определения

Рассматриваются двоичные столбцы и матрицы. Верхний индекс в обозначении матрицы (столбца) равен числу строк (позиций) в матрице (столбце), исключая tr — знак транспонирования.

Судя по контексту, матрицы могут рассматриваться как множества, элементами которых являются столбцы. При этом знаки $+$, $\cup$, $\in$, ... трактуются соответственно. Так, выражение $\{T_1+\ldots+T_v\}$, где T_i — матрица, понимается следующим образом:

$$\{T_1+\ldots+T_v\}=\{x : x=t_1+\ldots+t_v,\ t_i\in T_i,\ i=\overline{1, v}\}.$$

Запись элемента h поля $GF(2^m)$ как элемента матрицы или столбца обозначает двоичное представление элемента h в виде m-разрядного вектор-столбца. Для определенности примем

$$h=h_m\alpha^{m-1}+\ldots+h_2\alpha+h_1=(h_m\ldots h_2h_1)^{\mathrm{tr}}, \tag{2.1}$$

где $h\in GF(2^m)$; α — примитивный элемент $GF(2^m)$; $h_i\in\{0, 1\}$, $i=\overline{1, m}$.

Введем матрицы $P^s(\varphi_i)$, 0^m, E^m, $E_0{}^m$, W^{mR}, $B_\xi^{mR}(b)$.

$P^s(\varphi_i)=\|\varphi_i\varphi_i\ldots\varphi_i\|$ — матрица, состоящая из одинаковых столбцов, причем каждый столбец является двоичным представлением элемента φ_i поля $GF(2^s)$. 0^m — нулевая матрица, имеющая m строк.

Число столбцов матриц $P^s(\varphi_i)$ и 0^m определяется из контекста. Матрица E^m содержит все столбцы длины m: $E^m=\|e_0e_1\ldots e_M\|$, $M=2^m-1$; $e_i\in GF(2^m)$, $i=\overline{0, M}$; $e_i\neq e_j$ при $i\neq j$.

Матрица $E_0{}^m$ суть матрица E^m без нулевого столбца, $E_0{}^m$ совпадает с проверочной матрицей $[2^m-1, 2^m-1-m]1$-кода Хэмминга.

$$W^{mR}=\left\|\begin{matrix}0^{m(R-1)}\\ E^m\end{matrix}\right\|. \tag{2.2}$$

$$B_\xi^{mR}(b)=\left\|\begin{matrix}e_0 & e_1 & \ldots & e_M\\ e_0b & e_1b & \ldots & e_Mb\\ e_0b^2 & e_1b^2 & \ldots & e_Mb^2\\ & \ldots & & \\ e_0b^{R-\xi-1} & e_1b^{R-\xi-1} & \ldots & e_Mb^{R-\xi-1}\\ \hline e_0(a_1+b)^{-1} & e_1(a_1+b)^{-1} & \ldots & e_M(a_1+b)^{-1}\\ e_0(a_2+b)^{-1} & e_1(a_2+b)^{-1} & \ldots & e_M(a_2+b)^{-1}\\ & \ldots & & \\ e_0(a_\xi+b)^{-1} & e_1(a_\xi+b)^{-1} & \ldots & e_M(a_\xi+b)^{-1}\end{matrix}\right\|, \tag{2.3}$$

где $M=2^m-1$; b, e_i, e_ib^u, a_j, $e_i(a_j+b)^{-1}\in GF(2^m)$, $i=\overline{0, M}$, $u=\overline{1, R-\xi-1}$, $j=\overline{1, \xi}$; $\xi\in\{\overline{0, R-1}\}$; ξ — число строк с элементами вида $e_i(a_j+b)^{-1}$ (при $\xi=0$ такие строки отсутствуют); $e_i\neq e_j$ при $i\neq j$; $b\neq a_j$, $j=\overline{1, \xi}$; $a_v\neq a_j$ при $v\neq j$.

Введем класс $G(\rho)$ векторов с целыми положительными компонентами. Вектор $g\in G(\rho)$, если выполняются следующие условия:

$$g=(R_1, R_2, \ldots, R_\gamma);\ R_\lambda\in\{\overline{1, \rho}\},\ \lambda=\overline{1, \gamma}; \tag{2.4}$$

$$\sum_{\lambda=1}^{\gamma} R_\lambda=\rho;\ \gamma\geqslant\lceil\log_2(\rho+1)\rceil;$$

любое целое число t, $t\in\overline{\{1,\ \rho\}}$, может быть представлено как сумма компонент вектора g, т. е. существует (не обязательно единственное) множество $\theta(t)$, состоящее из компонент вектора, сумма которых равна t, т. е. $\sum_{R_\lambda\in\theta(t)} R_\lambda=t$.

В классе $G(\rho)$ укажем подклассы $G_1(\rho, \nu, a)$, $G_2(\rho)$, $G_3(\rho)$:

(2.5) $$G_1(\rho, \nu, a)=\{g : g\in G(\rho);\ R_\lambda=1,\ \lambda=\overline{1,\ \nu};\ R_i\leqslant\nu+a,$$

$$t=\overline{\nu+1,\ \gamma}\},\ a\in\{0,\ 1\},\ \nu\in\{\overline{1,\ \rho}\},$$

(2.6) $$G_2(\rho)=\{g : g\in G(\rho);\ \gamma=\lceil\log_2(\rho+1)\rceil;\ R_1=\lceil\rho/2\rceil,$$

$$R_\lambda=\left\lceil\frac{1}{2}\left(\rho-\sum_{i=1}^{\lambda-1}R_i\right)\right\rceil,\quad \lambda=\overline{2,\ \gamma}\Big\},$$

(2.7) $$G_3(\rho)=\{g : g\in G(\rho);\ \gamma=\lceil\log_2(\rho+1)\rceil;\ R_1=\rho-2^{\gamma-1}+1,\ R_i=2^{\gamma-i},$$

$$i=\overline{2,\ \gamma}\}.$$

В подклассе $G_1(\rho, \nu, a)$ при фиксированных ρ, ν, a вектор g задан неоднозначно, исключая ситуации $\nu=\rho$ и $\nu=1$, $a=0$, когда $g=(1, 1, \ldots, 1)$. Подклассы $G_2(\rho)$ и $G_3(\rho)$ содержат по одному элементу.

Построение множества $\theta(t)$ вытекает из построения вектора g. Так, для $g\in G_2(\rho)$ можно положить: $R_\lambda\in\theta(t)$, если и только если $t-\sigma_\lambda\geqslant R_\lambda$, $\lambda=\overline{1,\gamma}$, где $\sigma_1=0$, $\sigma_\lambda=\sum_{R_i\in\theta(t),\,i<\lambda} R_i$, $\lambda=\overline{2,\gamma}$. Для вектора $g\in G_1(\rho, \nu, a)$ обозначим через $K(t)$ множество $\theta(t)$, состоящее из компонент вектора с последовательными номерами, причем по меньшей мере одна из двух компонент R_ν, $R_{\nu+1}$ принадлежит $K(t)$:

(2.8) $$K(t)\triangleq\{R_{X(t)}, R_{X(t)+1}, R_{X(t)+2}, \ldots, R_{\nu+y(t)}\},$$

где

$$X(t)=\nu+1-(t-Y(t)),\ Y(t)=\sum_{i=1}^{y(t)} R_{\nu+i}\leqslant t<\sum_{i=1}^{y(t)+1} R_{\nu+i};$$

если $t<R_{\nu+1}$ или $\nu=\rho$, то $Y(t)=y(t)=0$.

Пример 1.1. $(1, 1, 1, 3, 3)\in G_1(9, 3, 0)$, $K(5)=\{R_2, R_3, R_4\}$. $(1, 1, 1, 2, 3, 1)\in G_1(9, 3, 0)$, $K(5)=\{R_4, R_5\}$, $K(6)=\{R_3, R_4, R_5\}$, $(1, 1, 1, 1, 4, 5, 5)\in G_1(18, 4, 1)$, $K(4)=\{R_5\}$, $K(10)=\{R_4, R_5, R_6\}$.

Введем функцию: $f(g)=i$, если для любого t можно построить множество $\theta(t)$ так, что из факта $R_u\in\theta(t)$, $u\leqslant i$ следует $R_p\in\theta(t)$, $p=\overline{1,\ u-1}$, но для $u\geqslant i+1$ сказанное неверно.

Пример 1.2. $g=(12, 6, 3, 2, 1)\in G_2(24)$, $\theta(17)=\{R_1, R_3, R_4\}$, $f(g)=1$.

Пример 1.3. $g=(7, 8, 4, 2, 1)\in G_3(22)$, $\theta(17)=\{R_1, R_2, R_4\}$, $f(g)=2$.

Вектор g можно формировать итеративно. Если $\rho\leqslant 2u+1$ и $(R_2, R_3, \ldots, R_\gamma)\in G(u)$, то $g=(R_1=\rho-u, R_2, R_3, \ldots, R_\gamma)\in G(\rho)$.

Пример 1.4. $(12, 6, 3, 2, 1)\in G(24)$, $g=(10, 12, 6, 3, 2, 1)\in G(34)$, $f(g)=2$.

Введем матрицу $D_\varkappa^{mR}(g, \rho)$, структура которой зависит от параметров m, R, $\varkappa$, ρ и компонент вектора g, где $g\in G(\rho)$.

(2.9) $$D_{\varkappa}^{mR}(g,\rho)=$$

$$=\left\|\begin{array}{c|ccc|c}
A^{mR_1} & 0^{mR_1} & \dots & 0^{mR_1} & \\
0^{mR_2} & A^{mR_2} & \dots & 0^{mR_2} & 0^{m(R_1+R_2+\dots+R_{\varkappa})} \\
\dots & & & & \\
0^{mR_{\varkappa}} & 0^{mR_{\varkappa}} & \dots & A^{mR_{\varkappa}} & \\
\hline
0^{m\Lambda} & 0^{m\Lambda} & \dots & 0^{m\Lambda} & 0^{m\Lambda}\ \ 0^{m\Lambda}\dots 0^{m\Lambda} \\
\hline
 & & & & A^{mR_{\varkappa+1}}\ \ 0^{mR_{\varkappa+1}}\dots 0^{mR_{\varkappa+1}} \\
0^{m(R_{\varkappa+1}+\dots+R_{\gamma})} & & & & 0^{mR_{\varkappa+2}}\ \ A^{mR_{\varkappa+2}}\dots 0^{mR_{\varkappa+2}} \\
 & & & & \dots \\
 & & & & 0^{mR_{\gamma}}\ \ 0^{mR_{\gamma}}\dots A^{mR_{\gamma}}
\end{array}\right\|,$$

где $g=(R_1, R_2, \dots, R_\gamma)\in G(\rho)$, $R_1+\dots+R_\gamma=\rho$; $A^{mR\lambda}$ — проверочная матрица $[N_\lambda, N_\lambda-mR_\lambda]R_\lambda$-кода с радиусом покрытия R_λ, $\lambda=\overline{1,\gamma}$; $A^{m\times 1}=E_0{}^m$, $N_\lambda=2^{m-1}-1$ при $R_\lambda=1$, $\Lambda=R-\rho$, $R\geqslant\rho$; при $R=\rho$ подматрицы $0^{m\Lambda}$ отсутствуют, $\varkappa\in\{\overline{0,\gamma}\}$, при $\varkappa=0$ ($\varkappa=\gamma$) отсутствует верхняя (нижняя) часть матрицы с $A^{mR\lambda}$, $\lambda\leqslant\varkappa$ ($\lambda>\varkappa$).

Число столбцов $N(m)$ матрицы $D_{\varkappa}{}^{mR}(g,\rho)$ составляет $N(m)=N_1+\dots+N_\gamma$. **Матрица, полученная из** $D_{\varkappa}{}^{mR}(g,\rho)$ **исключением нулевых строк** (образованных подматрицами $0^{m\Lambda}$), суть прямая сумма [1, с. 391] матриц $A^{mR\lambda}$, $\lambda=\overline{1,\gamma}$, и является проверочной матрицей $[N(m), N(m)-m\rho]\rho$-кода.

Введем столбец

$$(u_1,\dots,u_R)^{mR}=\left\|\begin{array}{c}u_1\\ \dots\\ u_R\end{array}\right\|,\quad u_i\in GF(2^m),\quad i=\overline{1,R}. \tag{2.10}$$

Введем обозначения: $[B^m]A$, l — **множество, элементами которого являются** всевозможные суммы столбцов матрицы B^m, содержащие не менее l и не более A слагаемых, причем каждый столбец входит в сумму не более одного раза и $l\geqslant 1$; $[B^m]0$, $l=\varnothing$; $[B^m]_2A$, l — подмножество множества $[B^m]A$, l, состоящее из сумм с четным числом слагаемых.

Определение 1. *Линейный двоичный код длины Q, избыточности s, с проверочной матрицей Φ^s называется R^*, l-подмножеством Q-мерного пространства и обозначается через $[Q, Q-s]R^*$, l-код, если справедливо следующее. При $l\geqslant 1$ любой столбец из E^s, включая нулевой, может быть представлен как сумма не менее l и не более R^* столбцов матрицы Φ^s. При $l=0$ любой ненулевой столбец из E^s может быть представлен как сумма не более R^* столбцов матрицы Φ^s. Во всех случаях R^* — наименьшее целое с указанным свойством*[1] *для заданного l. Другими словами:*

$$[\Phi^s]R^*,\ l=E^s \text{ и } [\Phi^s]A,\ l\subset E^s \text{ для } A<R^*,\ l\geqslant 1. \tag{2.11}$$

$$[\Phi^s]R^*,\ 1=E_0{}^s \text{ и } [\Phi^s]A,\ 1\subset E_0{}^s \text{ для } A<R^*,\ l=0. \tag{2.12}$$

Легко увидеть, что на расстоянии не менее l и не более R^* от любой точки Q-мерного пространства имеется точка, принадлежащая R^*, l-подмножеству (это свойство могло бы служить определением R^*, l-подмножества, в том числе и в нелинейном случае). R^*, 0-подмножество соответствует обычному покрытию сферами.

$[Q, Q-s]$-код с проверочной матрицей Φ^s имеет радиус покрытия R [2, 3], если и только если любой столбец из $E_0{}^s$ может быть представлен

[1] Поэтому иногда R^* обозначается через $R^*(l)$.

как сумма не более R столбцов матрицы Φ^s и для $A<R$ это неверно:

(2.13) $\quad [\Phi^s]R,1=E_0{}^s$, $[\Phi^s]A,\ 1\subset E_0{}^s$ для $A<R$.

Обозначения $[Q,\ Q-s]R$, 0-код и $[Q,\ Q-s]R$-код имеют один и тот же смысл, т. е. $R^*(0)=R$, где R — радиус покрытия кода. Если $R\geqslant l>0$, то $R^*(l)\geqslant R$.

Определение 2. *Для $R<Q$ совокупность матриц $(T_1{}^w, \ldots, T_Q{}^w)$ называется R-замкнутой, если для любого набора несовпадающих индексов вида $J_R=\{j_1, \ldots, j_R\}$, $j_k\in\overline{\{1, Q\}}$, $k=\overline{1, R}$, любой столбец из E^w, включая нулевой, может быть представлен как сумма R столбцов, где столбцы берутся по одному из каждой матрицы $T_{j_1}{}^w, \ldots, T_{j_R}{}^w$, т. е.*

(2.14) $\quad \{T_{j_1}{}^w+\ldots+T_{j_R}{}^w\}=E^w.$

Определение 3. *Для $l\geqslant 0$, $R<Q$ матрица L^w называется R, l-дополнительной к R-замкнутой совокупности матриц $(T_1{}^w, \ldots, T_Q{}^w)$, если выполняются следующие два условия.*

1. *Для любого набора несовпадающих индексов вида $J_z=\{j_1, \ldots, j_z\}$, $z\in\overline{\{l, R\}}$, $z\geqslant 1$, $j_k\in\overline{\{1, Q\}}$ $k=\overline{1, z}$, справедливо: любой столбец из E^w, включая нулевой, может быть представлен как сумма не менее z и не более R столбцов, где первые z столбцов, обязательно входящие в сумму, берутся по одному из каждой матрицы $T_{j_1}{}^w, \ldots, T_{j_z}{}^w$, а остальные столбцы (вторая группа слагаемых) берутся из матриц $L^w, T_1{}^w, \ldots, T_Q{}^w$. При этом во вторую группу слагаемых (если она присутствует в сумме) из каждой матрицы $T_i{}^w$, $i=\overline{1, Q}$, включается четное число столбцов или ни одного столбца, а из матрицы L^w включается произвольное (в смысле четности) число столбцов.*

2. *При $l=0$ любой ненулевой столбец из E^w может быть представлен как сумма не более R столбцов из матриц $L^w, T_1{}^w, \ldots, T_Q{}^w$, причем из каждой матрицы $T_i{}^w$, $i=\overline{1, Q}$ берется четное число столбцов или ни одного столбца, а из матрицы L^w — произвольное (в смысле четности) число столбцов.*

Для выполнения условия 1 в определении 3 достаточно, чтобы для любого набора несовпадающих индексов $\{j_1, \ldots, j_z\}$ выполнялось соотношение

(2.15) $\quad \{T_{j_1}{}^w+\ldots+T_{j_z}{}^w\}+\{\nu^w\cup[L^w]R-z,\ 1\}=E^w,\ z\in\overline{\{l, R\}},$

где $z\geqslant 1$, $j_k\in\overline{\{1, Q\}}$, $k=\overline{1, z}$, ν^w — нулевой столбец из E^w. В случае (2.15) все столбцы во второй группе слагаемых (если эта группа присутствует в сумме) берутся из матрицы L^w.

Для выполнения условия 2 в определении 3 достаточно, чтобы матрица L^w была проверочной матрицей кода с радиусом покрытия R, т. е.

(2.16) $\quad [L^w]R,1=E_0{}^w$ при $l=0$.

Достаточно для выполнения условия 2 и такое соотношение

(2.17) $\quad [L^w]R,\ 1\cup\bigcup_{j=1}^{Q}[T_j{}^w]_2R,\ 2=E_0{}^w$ при $l=0$.

§ 3. Конструкции линейных покрывающих кодов

Теорема 1. *Пусть $\varphi_i\in GF(2^s)$, $i=\overline{1, Q}$ и $\Phi^s=\|\varphi_1\varphi_2\ldots\varphi_Q\|$ — проверочная матрица $[Q,\ Q-s]R_0{}^*$, l-кода V_0, являющегося $R_0{}^*$, l-подмножеством Q-мерного пространства. Пусть также $T_j{}^w$ — матрица размера $w\times\Gamma$, $j=\overline{1, Q}$, $(T_1{}^w, \ldots, T_Q{}^w)$ — R-замкнутая совокупность матриц; L^w — матрица размера $w\times N$, являющаяся R, l-дополнительной к совокупности матриц*

$(T_1^w, \ldots, T_Q^w)$; $R \geqslant R_0^* \geqslant l \geqslant 0$. *Тогда*

$$H^{s+w} = \left\| \begin{array}{c|c|ccc} 0^s & P^s(\varphi_1) & P^s(\varphi_2) & \ldots & P^s(\varphi_Q) \\ \hline L^w & T_1^w & T_2^w & \ldots & T_Q^w \end{array} \right\| \tag{3.1}$$

(*где при* $l=R$ *подматрицы* 0^s *и* L^w *отсутствуют*) *суть проверочная матрица* $[n, n-r]R$*-кода* V *длины* $n=\Gamma Q+N$, *избыточности* $r=s+w$, *с радиусом покрытия* R.

Доказательство. Покажем, что произвольный столбец U^{s+w} из E_0^{s+w} является суммой не более R столбцов матрицы (3.1). Запишем U^{s+w} в виде

$$U^{s+w} = \left\| \begin{array}{c} v^s \\ \hline u^w \end{array} \right\|, \tag{3.2}$$

где v^s и u^w — столбцы длины s и w соответственно. Для простоты предположим, что имеют место ситуации (2.15) и (2.16). Общий случай R, l-дополнительности рассматривается аналогично.

Пусть $l \geqslant 1$. Так как код V_0 суть R_0^*, l — подмножество, то по определению 1 столбец v^s можно представить как сумму z столбцов из Φ^s:

$$v^s = \varphi_{j_1} + \varphi_{j_2} + \ldots + \varphi_{j_z},\ z \in \overline{\{l, R_0^*\}}. \tag{3.3}$$

Теперь для получения u^w мы *обязаны* взять по одному столбцу из каждой матрицы $T_{j_1}^w, \ldots, T_{j_z}^w$. Кроме того, можно использовать (но не в обязательном порядке) не более $R-z$ столбцов из L^w. Другими словами, нужно показать, что существует представление

$$u^w = t_{i_1, j_1} + \ldots + t_{i_z, j_z} + l_{a_1} + \ldots + l_{a_f},\quad z+f=F \leqslant R, \tag{3.4}$$

где t_{i_k, j_k} — i_k-й столбец из $T_{j_k}^w$, $j_k \in J_z$, $k=\overline{1, z}$, $J_z=\{j_1, \ldots, j_z\}$ — набор несовпадающих индексов, образованный номерами столбцов, вошедших в сумму (3.3); $f \geqslant 0$; $l_{a_i} \in L^w$, $i=\overline{1, f}$; при $f=0$ слагаемые l_{a_i} отсутствуют.

Пусть $z=R_0^*=R$. Так как $(T_1^w, \ldots, T_Q^w)$ суть R-замкнутая совокупность матриц, то по определению 2 существование представления (3.4) с $f=0$ следует из (2.14).

Пусть $z<R$. Существование представления (3.4) с $f \geqslant 0$ следует из (2.15).

Пусть $l=0$. Тогда при $v^s \neq 0$ представления (3.3), (3.4) по-прежнему имеют место. При $v^s=0$ столбец U^{s+w} получаем по условию (2.16) как сумму не более R столбцов матрицы $\left\| \begin{array}{c} 0^s \\ \hline L^w \end{array} \right\|$. ◂

В теореме 2 для $w=mR$ описана естественная реализация конструкции (3.1), использующая матрицу $D_\varkappa^{mR}(g, \rho)$ в качестве L^w и матрицы $B_\xi^{mR}(b_j)$ (с несовпадающими b_j) в качестве матриц T_j^w. Рассмотрены варианты с различными соотношениями между параметрами Q, m, ξ, ρ и с различными векторами g.

Столбец $u^w=u^{mR}=(u_1, \ldots, u_R)^{mR}$ представляется в виде суммы (3.4) в два этапа. На первом этапе путем суммирования z столбцов t_{i_k, j_k} из матриц $B_\xi^{mR}(b_{j_k})$ **формируется столбец** $(u^*)^{mR}$, совпадающий с u^{mR} в z элементах $u_{\tau_1}, \ldots, u_{\tau_z}$. Номера i_k определяются путем решения над полем $GF(2^m)$ системы уравнений с невырожденной матрицей, являющейся подматрицей матрицы Вандермонда, Коши или сочетания этих матриц. Появление матриц такого вида связано со структурой $B_\xi^{mR}(b_j)$ (2.3).

На втором этапе к $(u^*)^{mR}$ прибавляется f столбцов l_{a_i} из $D_\varkappa^{mR}(g, \rho)$, $0 \leqslant f \leqslant R-z$. Также прибавляемые столбцы не меняют элементов $u_{\tau_1}, \ldots, u_{\tau_z}$. Чтобы найти столбцы l_a, в $D_\varkappa^{mR}(g, \rho)$ выделяется подматрица d^{mR},

в которой позициям $u_{\tau_1}, \ldots, u_{\tau_z}$ соответствуют нулевые строки. Остальные строки d^{mR} образуют проверочную матрицу кода с радиусом покрытия $R-z$. Возможность выделения d^{mR} связана со структурой и свойствами вектора g (2.4)–(2.8).

Если код V_0 задан, то параметры построенного кода V зависят от $N(m)$ — числа столбцов матрицы $D_\varkappa^{mR}(g, \rho)$, которое в свою очередь зависит от вида вектора g.

Теорема 2. *Пусть* $\varphi_i \in GF(2^s)$, $i=\overline{1, Q}$, $\Phi^s=\|\varphi_1\varphi_2 \ldots \varphi_Q\|$ — *проверочная матрица* $[Q, Q-s]R_0^*$, *l-кода* V_0, *являющегося* R_0^*, *l-подмножеством Q-мерного пространства;* $R \geqslant R_0^* \geqslant l \geqslant 0$; *проверочная матрица кода V имеет вид* [2]

$$H^{s+mR} = \left\| \begin{array}{c|c} 0^s & P^s(\varphi_1) \ldots P^s(\varphi_{Q-1})\, P^s(\varphi_Q) \\ \hline D_\varkappa^{mR}(g, \rho) & B_\xi^{mR}(b_1) \ldots B_\xi^{mR}(b_{Q-1})\, B_\xi^{mR}(b_Q) \end{array} \right\|, \tag{3.5}$$

где $b_i \in GF(2^m)$ *для всех* i; $b_i \neq b_j$ *для* $i \neq j$; $\rho = R-\Lambda \geqslant 0$; *при* $\rho=0$ *матрицы* 0^s, $D_\varkappa^{mR}(g, \rho)$ *отсутствуют; при* $Q=2^m+1$ *матрица* $B_\xi^{mR}(b_Q)$ *заменяется матрицей* W^{mR}.

Обозначим через $N(m)$ *число столбцов матрицы* $D_\varkappa^{mR}(g, \rho)$.

Тогда для того чтобы код V являлся нормальным $[n, n-r]R$-*кодом с радиусом покрытия R, избыточностью* $r=s+mR$ *и длиной* $n=2^mQ+N(m)$, *достаточно, чтобы имела место любая из ситуаций:*

1) $2^m+1=Q$, $\xi=0$, $\Lambda=\max\{0, l-2\}$, $g \in G_1(\rho, \nu, 0)$, $\nu \geqslant 1$, $R_\tau=1$, $\varkappa=\nu$;
2) $2^m+1=Q$, $\xi=0$, $\Lambda=\max\{0, l-1\}$, $g=(1, 1, \ldots, 1)$, $\varkappa=0$;
3) $2^m \geqslant Q$, $\xi=0$, $\Lambda=\max\{0, l-1\}$, $g \in G_1(\rho, \nu, 0)$, $\nu \geqslant 1$, $\varkappa=\nu$;
4) $2^m \geqslant Q$, $\xi=0$, $\Lambda=l$, $g=(1, 1, \ldots, 1)$, $\varkappa=0$;
5) $2^m-1 \geqslant Q$, $\xi=0$, $b_i \neq 0$ *для всех* i, $\Lambda=l$, $g \in G_1(\rho, \nu, 1)$, $\nu \geqslant 1$, $\varkappa=\nu$;
6) $2^m-\xi \geqslant Q$, $\xi=\rho-\sum_{\lambda=1}^{j} R_\lambda$, $1 \leqslant j \leqslant f(g)$, $\Lambda=l$, $\varkappa=0$, $\forall g \in G(\rho)$.

Доказательство. Из (2.5)–(2.7) видно, что существует $R_i=1$. Следовательно, $A^{mR_t}=E_0^m$, в коде V минимальное расстояние $d \leqslant 3$ и по теореме 24 работы [4] код V — нормальный.

По теореме 1 достаточно показать, что совокупность матриц $(B_\xi^{mR}(b_1), \ldots, B_\xi^{mR}(b_Q))$ — R-замкнутая и матрица $D_\varkappa^{mR}(g, \rho)$ является R, l-дополнительной к этой совокупности. Следовательно (см. определения 2, 3), достаточно показать выполнение условий (2.15), (2.16).

Если $l=0$, то $R=\rho$, $D_\varkappa^{mR}(g, \rho)$ — проверочная матрица кода с радиусом покрытия R, и условие (2.16) выполняется.

Докажем выполнение условия (2.15). Разобьем (сверху вниз) строки матриц $D_\varkappa^{mR}(g, \rho)$, $B_\xi^{mR}(b_j)$ на R групп, по m строк в каждой группе, и пронумеруем эти группы от 1 до R. Если столбец матрицы рассматривается как совокупность R двоичных представлений элементов поля $GF(2^m)$, то каждая группа строк соответствует одному элементу поля.

Пусть $\theta(0)=\phi$ и $d^{mR}(\theta(z-\Lambda))$ матрица, составленная из столбцов матрицы $D_\varkappa^{mR}(g, \rho)$, содержащих все подматрицы A^{mR_β} с $R_\beta \notin \theta(z-\Lambda)$. $R-z$ групп строк матрицы $d^{mR}(\theta(z-\Lambda))$, содержащих эти подматрицы A^{mR_β}, образуют проверочную матрицу кода с радиусом покрытия $R-z$. Остальные z групп строк матрицы $d^{mR}(\theta(z-\Lambda))$ — нулевые. Их номера обозначим $\tau_1, \ldots, \tau_z$. Группы строк, соответствующие подматрицам $0^{m\Lambda}$, всегда нулевые. Номера этих групп строк: $T+1, T+2, \ldots, T+\Lambda$, где $T=R_1+R_2+\ldots+R_\varkappa$. Ясно, что $\{T+1, \ldots, T+\Lambda\} \subseteq \{\tau_1, \ldots, \tau_z\}$.

[2] Чаще всего при использовании этой конструкции $R=R_0^*$.

Пусть $u^{mR}=(u_1, \ldots, u_R)^{mR}$ — произвольный столбец из E^{mR}. Покажем, что для любого набора индексов $J_z=\{j_1, \ldots, j_z\}$, $z\in\overline{\{l, R\}}$, можно построить множество $\theta(z-\Lambda)$, удовлетворяющее условию: найдутся столбцы по одному в каждой матрице $B_\xi^{mR}(b_{j_k})$, $k=\overline{1, z}$, такие, что их сумма даст столбец $(u^*)^{mR}$, совпадающий со столбцом u^{mR} в позициях $\tau_1, \ldots, \tau_z$, т. е.

$$(u^*)^{mR}=(\ldots, u_{\tau_1}, \ldots, u_{\tau_z}, \ldots)^{mR}\in\{B_\xi^{mR}(b_{j_1})+\ldots+B_\xi^{mR}(b_{j_z})\}, \tag{3.6}$$

где в ситуации 1) одной из матриц в скобках может быть матрица W^{mR}.

Столбец u^{mR} можно получить, складывая с $(u^*)^{mR}$ не более $R-z$ столбцов матрицы $d^{mR}(\theta(z-\Lambda))$. Это и означает выполнение условия (2.15).

Пусть $e_i f_v(b)$ — элемент, расположенный в $B_\xi^{mR}(b)$ или в W^{mR} на пересечении v-й строки и $(i+1)$-го столбца. «Локаторы» e_{i_k} столбцов, обеспечивающих выполнение (3.6), являются решением системы

$$\sum_{k=1}^{z} e_{i_k} f_{\tau_c}(b_{j_k})=u_{\tau_c}, \quad c=\overline{1, z}. \tag{3.7}$$

Обозначим определитель системы через Δ_z. Покажем, что $\Delta_z\neq 0$.

1. Пусть $j_z=Q$, $b_{j_{z-1}}=0$, $q=z-\Lambda-2$, $K(0)=\phi$. Для $q>0$ определим из (2.8) $K(q)$, $X(q)$ и обозначим $X=X(q)$. Положим $\theta(z-\Lambda)=\{R_1, R_\Upsilon\}\cup K(q)$. Тогда для $q>0$ имеем $\tau_1=1$, $\tau_i=X+i-2$, $i=\overline{2, z-1}$, $\tau_z=R$; Δ_z имеет вид (см. [20, § 11.5])

$$\Delta_z=\begin{Vmatrix} 1 & \ldots & 1 & 1 & 0 \\ b_{j_1}^{X-1} & \ldots & b_{j_{z-2}}^{X-1} & 0 & 0 \\ & & \ldots & & \\ b_{j_1}^{X+z-4} & \ldots & b_{j_{z-2}}^{X+z-4} & 0 & 0 \\ b_{j_1}^{R-1} & \ldots & b_{j_{z-2}}^{R-1} & 0 & 1 \end{Vmatrix}\neq 0.$$

(Такой вид определителя объясняет, почему $\Lambda=l-2$ при $l\geqslant 3$.) Другие случаи рассматриваются аналогично. Например, если $j_i\neq Q$, $i=\overline{1, z}$, $b_{j_z}=0$, то $q=z-\Lambda-1$, $\theta(z-\Lambda)=R_1\cup K(q)$. Если $j_i\neq Q$, $b_{j_i}\neq 0$, $i=\overline{1, z}$, то $q=z-\Lambda$, $\theta(z-\Lambda)=K(q)$.

2–5. Рассуждаем аналогично ситуации 1.

6. Построим $\theta(z-\Lambda)$ так, что если $R_u\in\theta(z-\Lambda)$, $u\leqslant j$, то $R_p\in\theta(z-\Lambda)$, $p=\overline{1, u-1}$; Δ_z имеет вид (см. [20, § 11.4; 21, § 2, 5, с. 126–127])

$$\Delta_z=\begin{Vmatrix} 1 & \ldots & 1 \\ b_{j_1} & \ldots & b_{j_z} \\ b_{j_1}^{\delta-1} & \ldots & b_{j_z}^{\delta-1} \\ \hline (a_{c_1}+b_{j_1})^{-1} & \ldots & (a_{c_1}+b_{j_z})^{-1} \\ & \ldots & \\ (a_{cz-\delta}+b_{j_1})^{-1} & \ldots & (a_{c_{z-\delta}}+b_{j_z})^{-1} \end{Vmatrix}\neq 0,$$

где δ и $z-\delta$ — число строк с элементами вида $b_{j_k}^u$ и $(a_{c_e}+b_{j_k})^{-1}$. ◀

Рассмотренные ситуации не исчерпывают возможностей конструкций (3.1), (3.5). Из доказательства теорем виден путь построения новых вариантов. В конкретных случаях надо стремиться ослабить ограничения снизу на m (чтобы конструкция начала работать при меньших r и была эффективней на конечных длинах) и выбрать величины R_λ так, чтобы

уменьшить величину $N(m)$. Сумма ρ величин R_λ фиксирована, но в разных ситуациях оказываются эффективными различные сочетания значений R_λ, что и объясняет разнообразие рассмотренных векторов g. Векторы из подклассов $G_2(\rho)$, $G_3(\rho)$ часто уменьшают $N(m)$, но при этом усиливают ограничения снизу на m.

В матрицах $B_\xi^{mR}(b)$ вместо элементов вида $e_i(a_j+b)^{-1}$ можно использовать элементы вида $e_i(1+a_jb)^{-1}$ [22].

Непосредственно радиус покрытия R_0 исходного кода V_0 здесь не рассматривается. Напомним: $R_0^*(0)=R_0$; $R\geqslant R_0^*(l>0)\geqslant R_0$; часто $R=R_0^*(l>>0)=R_0$.

Замечание 1. Как видно из доказательства теоремы 1, в конструкции (3.1) требования о R-замкнутости матриц $(T_1^w, \ldots, T_Q^w)$ и R, l-дополнительности матрицы L^w можно заменить более мягким требованием (R, l, Φ^s)-дополнительности.

Далее в этом замечании (как в теореме 1): $\varphi_i\in GF(2^s)$, $i=\overline{1, Q}$; $\Phi^s=\|\varphi_1, \varphi_2, \ldots, \varphi_Q\|$ — проверочная матрица $[Q, Q-s]R_0^*$, l-кода V_0, являющегося R_0^*, l-подмножеством Q-мерного пространства; $R\geqslant R_0^*\geqslant l\geqslant 0$.

Пусть d_p — столбец из E^s, $d_0=0$, $d_p\neq d_j$ при $p\neq j$. Для $z\in\overline{\{l, R\}}$ обозначим через $J_z(d_p)$ набор несовпадающих индексов, соответствующий *одному из возможных* представлений столбца d_p в виде суммы не менее l и не более R столбцов матрицы Φ^s:

$$
\begin{aligned}
(3.8)\qquad & J_z(d_p)=\{j_1(p), \ldots, j_z(p)\},\\
& \varphi_{j_1(p)}+\ldots+\varphi_{j_z(p)}=d_p,\\
& z\in\overline{\{l, R\}},\ z\geqslant 1,\ j_k(p)\in\overline{\{1, Q\}},\ k=\overline{1, z},\\
& p\in\overline{\{0, 2^s-1\}}.
\end{aligned}
$$

Введем множество $J(R, l, \Phi^s)$, состоящее из наборов индексов:

$$
\begin{aligned}
(3.9)\qquad & J(R, l, \Phi^s)=\{J_z(d_p),\ z\in\overline{\{l, R\}},\ z\geqslant 1,\ p=\overline{0, 2^s-1} \text{ при } l\geqslant 1,\\
& p=\overline{1, 2^s-1} \text{ при } l=0\}.
\end{aligned}
$$

Множество $J(R, l, \Phi^s)$ параметрами R, l и матрицей Φ^s задано неоднозначно. Оно содержит *по одному* возможному *представлению* всех столбцов из E^s (при $l\geqslant 1$) или E_0^s (при $l=0$). Ниже речь идет о построении удачного в некотором смысле варианта этого множества, «согласованного» с матрицами L^w, T_i^w и позволяющего ослабить требования к ним за счет того, что требования определения 2 и условия 1 определения 3 будут выполняться не для «любых наборов несовпадающих индексов» J_R и J_z, а только для наборов из множества.

Определение 4. *Для $l\geqslant 0$, $R<Q$ матрица L^w называется (R, l, Φ^s)-дополнительной к совокупности матриц $(T_1^w, \ldots, T_Q^w)$, если существует множество $J(R, l, \Phi^s)$ такое, что выполняются следующие условия*:

1. $\forall J_R(d_p)=\{j_1(p), \ldots, j_R(p)\}\in J(R, l, \Phi^s)$, $\{T_{j_1(p)}^w+\ldots+T_{j_R(p)}^w\}=E^w$.

2. *Для любого набора индексов $J_z(d_p)=\{j_1(p), \ldots, j_z(p)\}$, принадлежащего множеству $J(R, l, \Phi^s)$, справедливо: любой столбец из E^w, включая нулевой, может быть представлен как сумма не менее z и не более R столбцов, где первые z столбцов, обязательно входящие в сумму, берутся по одному из каждой матрицы $T_{j_1(p)}^w, \ldots, T_{j_z(p)}^w$, а остальные столбцы (вторая группа слагаемых) берутся из матриц L^w, $T_1^w, \ldots, T_Q^w$. При этом во вторую группу слагаемых (если она присутствует в сумме) из каждой матрицы T_i^w, $i=\overline{1, Q}$, включается четное число столбцов или ни одного столбца, а из матрицы L^w включается произвольное (в смысле четности) число столбцов.*

3. *При* $l=0$ *справедливо условие* 2 *определения* 3.

Для выполнения условия 2 в определении 4 достаточно, чтобы выполнялось следующее соотношение, аналогичное (2.15):

$$\forall J_z(d_p)=\{j_1(p),\ldots,j_z(p)\}\in J(R,\ l,\ \Phi^s), \tag{3.10}$$

$$\{T^w_{j_1(p)}+\ldots+T^w_{j_z(p)}\}+\{v^w\cup[L^w]R-z,\ 1\}=E^w,$$

где v^w — нулевой столбец из E^w, $z\in\{\overline{l,\ R}\}$, $z\geqslant 1$.

Теорема 3. *Теорема* 1 *справедлива, если вместо требований* R*-замкнутости и* R, l*-дополнительности потребовать, чтобы матрица* L^w *была* $(R,\ l,\ \Phi^s)$*-дополнительной к совокупности матриц* $(T_1^w,\ldots,T_Q^w)$.

Доказательство теоремы 3 аналогично доказательству теоремы 1.

Примером конструкции с $(R,\ l,\ \Phi^s)$-дополнительностью являются коды работы [18]. (В условии 2 определения 3 эти коды реализуют (2.17).)

Условие 1 определения 4 можно назвать $R,\ \Phi^s$-замкнутостью.

Множеству наборов индексов $J(R,\ l,\ \Phi^s)$ сопоставим граф $\Gamma(J)$ с Q вершинами. Вершине с номером j соответствует столбец φ_j матрицы Φ^s. Вершины с номерами j_k и j_t соединены ребром, если и только если j_k и j_t одновременно входят хотя бы в один набор из $J(R,\ l,\ \Phi^s)$. Обозначим через $h(J)$ хроматическое число [23, с. 294] графа $\Gamma(J)$.

Конструкции проверочных матриц из теорем 1—3 обозначим соответственно через ФLT (см. (3.1)), ФDB (см. (3.5)) и ФLTJ.

Введем конструкцию ФDBJ. Формально допустим символ * как значение b в $B_\xi^{mR}(b)$ и примем $B_\xi^{mR}(*)=W^{mR}$. Используется матрица Φ^s такая же, как в теореме 2. Строится множество $J(R,\ l,\ \Phi^s)$ и граф $\Gamma(J)$. Проверочная матрица кода V имеет вид (3.5), где $b_i\in\{GF(2^m)\cup *\}$ для всех i. Если вершины графа с номерами i и j соединены ребром, то обязательно неравенство $b_i\neq b_j$. Допускается равенство $b_u=b_v$, если вершины с номерами u, v не соединены ребром.

Теорема 4. *Для того, чтобы код* V, *проверочная матрица которого имеет конструкцию* ФDBJ, *являлся нормальным* $[n,\ n-r]R$*-кодом с* $r=s+mR$, $n=2^mQ+N(m)$ *и радиусом покрытия* R, *достаточно выполнения любого из условий* 1—6 *теоремы* 2, *причем значение* Q *во всех условиях заменяется хроматическим числом*[3] $h(J)$ *и по-прежнему в условиях* 3—6 *имеем* $b_i\neq *$ *для всех* i.

Доказательство теоремы 4 аналогично доказательству теоремы 2.

Если $h(J)<Q$ (например, когда код V_0 получен с помощью ADS или теорем 1—4), то конструкция ФDBJ начинает работать при меньших m, чем ФDB. В конструкции ФDBJ при $h(J)<2^m+1\leqslant Q$ полезно использовать все значения b из множества $\{GF(2^m)\cup *\}$, что позволяет уменьшить ρ в матрице $D_\varkappa^{mR}(g,\ \rho)$ (и следовательно, уменьшить $N(m)$) за счет включения во вторую группу слагаемых (см. определение 4) четного числа столбцов из матриц $B_\xi^{mR}(b_i)$, $i\in\{\overline{1,\ Q}\}$.

Замечание 2. Введем обозначения: Ω^{mR} — проверочная матрица некоторого $[Q,\ Q-R]$-кода МДР [20] над полем $GF(2^m)$; $e_i\Omega^{mR}$ — матрица Ω^{mR}, в которой все элементы умножены на элемент $e_i\in GF(2^m)$ и даны в двоичном представлении. Перестановкой столбцов матрицу (3.5) можно привести к виду

$$H^{s+mR}=\left\|\begin{array}{c|cccc} 0^s & \Phi^s & \Phi^s & \ldots & \Phi^s \\ \hline D_\varkappa^{mR}(g,\ \rho) & e_0\Omega^{mR} & e_1\Omega^{mR} & \ldots & e_M\Omega^{mR}\end{array}\right\|, \tag{3.11}$$

где $M=2^m-1$, $e_i\in GF(2^m)$, $i=\overline{0,\ M}$, $e_i\neq e_j$ при $i\neq j$.

От вида Ω^{mR} зависят структура матрицы $D_\varkappa^{mR}(g,\ \rho)$ и ограничения на m.

Замечание 3. Код V, построенный с помощью конструкций (3.1), (3.5), (3.11), является $R,\ l'$-подмножеством n-мерного пространства, где $l'\geqslant l$.

[3] Минимальное число красок, достаточное, чтобы окрасить в разные цвета вершины графа $\Gamma(J)$, являющиеся концами одного ребра.

Матрица $D_{\varkappa}^{mR}(g, \rho)$ всегда содержит проверочную матрицу кода Хэмминга, в которой имеются группы из w линейно зависимых столбцов, $w \geqslant 3$. Такие группы есть и в других матрицах $A^{mR\lambda}$. Поэтому для $R \geqslant 3$ код V, построенный по конструкциям (3.5), (3.11), часто имеет $l'=R-2$. Это повышает эффективность итеративного применения рассмотренных конструкций, когда построенный код V используется в свою очередь как код V_0.

Замечание 4. Для R-замкнутой совокупности матриц $(T_1^w, \ldots, T_Q^w)$, имеющих одинаковые размеры $w \times \Gamma$, справедливо $\Gamma^R \geqslant 2^w$. В (3.5) $w=mR$ и Γ имеет минимально возможное значение 2^m.

Замечание 5. При $l \geqslant 1$ точки R_0^*, l-подмножества можно трактовать как центры покрывающих пространство «сферических оболочек» (spherical capsules), имеющих внутренний радиус l, внешний радиус R_0^* и «толщину стенки» R_0^*-l+1.

Полезно рассматривать и «слоистые сферические оболочки», состоящие из совокупностей поверхностей сфер с радиусами $l_1 > l_2 > \ldots > l_v \geqslant 0$. В этом случае любой столбец d из E^s (при $l_v \geqslant 1$) или из E_0^s (при $l_v=0$) может быть представлен как сумма $z(d)$ столбцов матрицы Φ^s, где

$$z(d) \in \{l_1=R_0^*, l_2, l_3, \ldots, l_v=l\} \stackrel{\triangle}{=} \mathscr{L}(R_0^*, l).$$

Для $R \geqslant R_0^*$ можно ввести понятие R, $\mathscr{L}(R_0^*, l)$-дополнительности, промежуточное между R, l-дополнительностью и (R, l, Φ^s)-дополнительностью. При этом в условии 1 определения 3 $z \in \mathscr{L}(R_0^*, l)$. Такой подход уменьшает $N(m)$, смягчая требования к L^w.

Оболочки являются здесь не самоцелью, а средством уменьшить $N(m)$. Но можно специально рассматривать такие покрытия и их плотность.

Замечание 6. Обобщим предыдущие определения дополнительности.

Определение 5. *Матрица L^w является R, Φ^s-дополнительной к совокупности матриц $(T_1^w, \ldots, T_Q^w)$, если матрица H^{s+w} вида* (3.1) *суть проверочная матрица кода с радиусом покрытия R.*

Приблизим определение 4 к определению 5. Построим множество $J^*(R, l, \Phi^s)$ как объединение подмножеств $J^*(d_p)$, $p=\overline{0, 2^s-1}$ при $l \geqslant 1$, $p=\overline{1, 2^s-1}$ при $l=0$. Подмножество $J^*(d_p)$ состоит из $f(p)$ наборов индексов $J_z(d_p)$ вида (3.8), $f(p) \geqslant 1$. Введем понятие $(R, l, \Phi^s)^*$-дополнительности, заменив в определении 4 условия 1, 2 на следующее условие: для любого столбца $u^w \in E^w$ в любом подмножестве $J^*(d_p)$ найдется набор индексов $J_z(d_p)$, позволяющий получить этот столбец u^w тем путем, который изложен в условии 2 определения 4.

Замечание 7. Конструкции (3.1), (3.5), (3.11) естественным образом переносятся на недвоичные покрывающие коды над полем $GF(q)$, $q>2$.

$[Q, Q-s]$-код над $GF(q)$ с проверочной матрицей Φ^s имеет радиус покрытия R_0 [3, 16], если и только если любой ненулевой q-ичный столбец длины s может быть представлен как линейная комбинация (с коэффициентами из $GF(q)$) не более R_0 столбцов матрицы Φ^s.

Поэтому при переносе конструкции на q-ичные коды вместо суммы столбцов рассматриваются линейные комбинации столбцов (в выражениях $\{T_1+\ldots+T_v\}$, $[B^m]A$, l, в соотношениях (2.11)–(2.17), в определениях 1–5, при доказательстве теорем 1–4 и т. д.). В матрицах $P^s(\varphi_i)$, E^m, (2.2), (2.3), (2.9), (3.1), (3.5), столбце (2.10), определителе Δ_z вместо элементов поля $GF(2^m)$ фигурируют элементы поля $GF(q^m)$, которые записываются в q-ичном представлении в виде m-разрядных вектор-столбцов. В (3.11) рассматривается код МДР над полем $GF(q^m)$. В теореме 2 при формулировке ограничений снизу на m в ситуациях 1–6 вместо 2^m записывается q^m. Длина построенного кода V равна $n=q^mQ+N(m)$.

Пример 2. $q=3$, $R=2$, V_0 – [11, 6] 2,0-код Голея над $GF(3)$; $D_{\varkappa}^{m\times 2}(g, \rho)$ – прямая сумма двух проверочных матриц $[(3^m-1)/2, (3^m-1)/2-m]$ 1-кода Хэмминга над $GF(3)$. Конструкция (3.5) с $\xi=0$, $3^m-1 \geqslant 11$ дает се-

мейство кодов V^5 с параметрами

$$q=3,\ R=2,\ n=12\times 3^m-1,\ r=5+2m, \tag{3.12}$$

$$m\geqslant 3,\ \bar{\mu}[2,\ V^5]\approx 1{,}185.$$

§ 4. Коды с радиусом покрытия 2

В отличие от (3.5), построим L^w без использования прямой суммы матриц. В данном параграфе положим в (3.1): $V_0-[5,\ 1]$ 2,0-код,

$$\Phi^s=F^4=\left\|\begin{matrix}10001\\01001\\00101\\00011\end{matrix}\right\|=\|\,f_1f_2f_3f_4f_5\,\|,\ f_i\in GF(2^4). \tag{4.1}$$

При $\Phi^s=F^4$ конструкция (3.5) (ситуация 1) дает коды, не совпадающие по структуре с кодами из [18], но имеющие параметры (1.2). В данном параграфе строятся коды с параметрами (1.4) лучшими, чем (1.2).

Улучшение параметров кодов с $R=2$ представляет интерес не только как самостоятельная задача, но и потому, что коды с $R=2$ используются при построении матриц A^{mR_λ} для кодов с $R>2$.

Методами работы [1, с. 391, 393] построим проверочные матрицы [13, 7] 2-кода и [28, 20] 2-кода:

$$\Pi_3{}^6=\left\|\begin{matrix}001111000000\\110011000000\\010101100000\\000000001111\\000000110011\\000001010101\end{matrix}\right\|,$$

$$\Pi_4{}^8=\left\|\begin{matrix}000000111111\ 10\ 00000000000\ 111\\000111000111\ 01\ 00000000000\ 111\\011001011001\ 01\ 00000000000\ 111\\101010101010\ 01\ 00000000000\ 111\\000000000000\ 11\ 00000111111\ 100\\000000000000\ 11\ 00111000111\ 010\\000000000000\ 11\ 11001011001\ 010\\000000000000\ 11\ 01010101010\ 011\end{matrix}\right\|.$$

Для $m\geqslant 5$ проверочную матрицу $[n=7\times 2^{m-3}-2,\ n-2(m-1)]$ 2-кода из [18] можно представить в виде

$$K^{2m-2}=\left\|\begin{array}{c|c|c|c|c|c|c}0\ldots0&0\ \ldots\ 0&0\ \ldots\ 0&0\ \ldots\ 0&0\ \ldots\ 0&1\ \ldots\ 1&1\ \ldots\ 1\\0\ldots0&1\ \ldots\ 1&1\ \ldots\ 1&1\ \ldots\ 1&1\ \ldots\ 1&0\ \ldots\ 0&1\ \ldots\ 1\\\hline E_0^{m-3}&F_0^{2m-6}(a)&F^{2m-6}(b)&F^{2m-6}(c)&0^{m-3}&E^{m-3}&E^{m-3}\\\hline 0^{m-3}&&&&E^{m-3}&0^{m-3}&0^{m-3}\\\hline 0\ldots0&0\ \ldots\ 0&0\ \ldots\ 0&1\ \ldots\ 1&1\ \ldots\ 1&0\ \ldots\ 0&0\ \ldots\ 0\\0\ldots0&0\ \ldots\ 0&1\ \ldots\ 1&0\ \ldots\ 0&1\ \ldots\ 1&0\ \ldots\ 0&0\ \ldots\ 0\end{array}\right\|, \tag{4.2}$$

где $a,\ b,\ c\in GF(2^{m-3})$: $a+b=c$, $a\neq b$, $a,\ b\neq 0$;

$$F^{2m-6}(d)=\left\|\begin{matrix}e_0=0 & e_1 & e_2 & \dots & e_\Psi\\ e_0=0 & e_1^{-1}d & e_2^{-1}d & \dots & e_\Psi^{-1}d\end{matrix}\right\|, \quad \Psi=2^{m-3}-1,$$

$d, e_i\in GF(2^{m-3})$, $i=\overline{0,\ \Psi}$, $e_i\neq e_j$ при $i\neq j$; $F_0^{2m-6}(a)$ — матрица $F^{2m-6}(a)$ без нулевого столбца.

Как верхние, так и нижние $m-1$ строк матрицы K^{2m-2} содержат все столбцы из E_0^{m-1}. Отсюда, используя конструкцию из доказательства теоремы 3.3 работы [16, с. 104], получаем следующую лемму.

Лемма 1. *Проверочная матрица вида*

$$\Pi_5^{2m}=\left\|\begin{array}{c|c|c}0\ \dots\ 0 & 1\ \dots\ 1 & 0\ \dots\ 0\\ \hline & E^{m-1} & 0^{m-1}\\ K^{2m-2} & \hline & \\ & 0^{m-1} & E^{m-1}\\ \hline 0\ \dots\ 0 & 0\ \dots\ 0 & 1\ \dots\ 1\end{array}\right\|, \quad m\geqslant 5, \tag{4.3}$$

задает $[n=15\times 2^{m-3}-2,\ n-2m]$ 2-*код с радиусом покрытия* 2.

Теорема 5. *Пусть* $m\geqslant 3$; *проверочная матрица кода* V *имеет вид*

$$H^{4+2m}=\left\|\begin{array}{c|ccccc}0^4 & P^4(f_1) & P^4(f_2) & \dots & P^4(f_5)\\ \hline \Pi_\sigma^{2m} & B_0^{2m}(b_1) & B_0^{2m}(b_2) & \dots & B_0^{2m}(b_5)\end{array}\right\|, \tag{4.4}$$

где $B_0{}^{2m}(b)$ — *матрица* $B_0{}^{mR}(b)$ *с* $R=2$; $b_i\in GF(2^m)$, $i=\overline{1,\ 5}$; $b_i\neq b_j$ *для* $i\neq j$; α — *примитивный элемент* $GF(2^m)$; *справедливо соотношение* (2.1); $b_5=0$;

для $m=3$ $\Pi_\sigma{}^{2m}=\Pi_3{}^6$, $b_1=\alpha$, $b_2=\alpha+1$, $b_3=\alpha^2+1$, $b_4=\alpha^2+\alpha$;

для $m=4$ $\Pi_\sigma{}^{2m}=\Pi_4{}^8$, $\alpha^4=\alpha+1$, $b_1=\alpha$, $b_2=\alpha^4$, $b_3=\alpha^{10}$, $b_4=\alpha^{11}$;

для $m\geqslant 5$ $\Pi_\sigma{}^{2m}=\Pi_5{}^{2m}$, $b_1=\alpha^3$, $b_2=\alpha^3+\alpha$, $b_3=\alpha^3+\alpha^2$, $b_4=\alpha^3+\alpha^2+\alpha$.

Тогда код V — *нормальный* $[n=55\times 2^{c-5}-2,\ n-2c]$ 2-*код для* $c\geqslant 5$.

Доказательство. Пусть $m\geqslant 5$. Из (4.2)—(4.4) видно, что в коде V минимальное расстояние $d\leqslant 3$ и по теореме 24 из [4] код V — нормальный. По теореме 1 достаточно показать, что матрица $\Pi_5{}^{2m}$ является 2,0-дополнительной к 2-замкнутой совокупности матриц $(B_0{}^{2m}(b_1), \dots, B_0{}^{2m}(b_5))$. По лемме 1 условие (2.16) выполняется.

В (2.15) рассмотрим случаи $z=1, 2$. Пусть $u=(u_1, u_2)^{2m}$ — произвольный столбец из E^{2m} вида (2.10) с $R=2$. Для $z=2$: $u=X_1+X_2$, $X_i=(e_{x_i}, e_{x_i}b_{j_i})^{2m}\in B_0{}^{2m}(b_{j_i})$, $i=1, 2$. «Локаторы» e_{x_i} определяются из системы — $e_{x_1}+e_{x_2}=u_1$, $e_{x_1}b_{j_1}+e_{x_2}b_{j_2}=u_2$. Решение этой системы существует, так как $b_{j_1}\neq b_{j_2}$.

Пусть $z=1$, $u\notin B_0{}^{2m}(b_{j_1})$. Если $j_1=5$, то $u=Y+X$, $Y=(v, u_2)^{2m}\in\Pi_5{}^{2m}$, $X=(v+u_1, 0)^{2m}\in B_0{}^{2m}(b_5)$. Такие столбцы X, Y можно найти, так как $b_5=0$ и нижние m строк матрицы $\Pi_5{}^{2m}$ содержат все столбцы из E^m.

Если $j_1\neq 5$, то вначале будем искать u как сумму $u=Y+X$, $Y=(y, 0)^{2m}\in\Pi_5{}^{2m}$, $X=(e, eb_{j_1})^{2m}\in B_0{}^{2m}(b_{j_1})$. Тогда $y=u_1+u_2b_{j_1}^{-1}$. Из (4.2), (4.3) видно, что $(y, 0)^{2m}\notin\Pi_5{}^{2m}$, если $y=(001\,a_1\dots a_{m-3})^{tr}$, $a_i\in\{0, 1\}$, $i=\overline{1,\ m-3}$. В этом случае получим u как сумму $u=Y^*+X^*$, $Y^*=(0, y^*)^{2m}\in\Pi_5{}^{2m}$, $X^*=(e^*, e^*b_{j_1})^{2m}\in B_0{}^{2m}(b_{j_1})$. Тогда $y^*=u_2+u_1b_{j_1}=yb_{j_1}$. Так как $b_1=\alpha^3$, $b_2=\alpha^3+\alpha$, $b_3=\alpha^3+\alpha^2$, $b_4=\alpha^3+\alpha^2+\alpha$, то $y^*=(c_1\dots c_{m-1}1)^{tr}$, $c_i\in\{0, 1\}$, $i=\overline{1,\ m-1}$. Все столбцы $(0, y^*)^{2m}$ с y^* такого вида есть в $\Pi_5{}^{2m}$ (см. (4.3)). Случаи $m=3, 4$ доказываются аналогично (их можно проверить на ЭВМ). ◀

§ 5. Примеры бесконечных семейств покрывающих кодов с $R\geqslant 3$

Далее используется конструкция (3.5) в ситуации 5). В матрице $D_\varkappa^{mR}(g, \rho)$ подматрица $A^{m\times 2}$ — проверочная матрица кода (1.4).

Пример 3. $R=3$. а) V_0 — [23, 12]3,0-код Голея. $g=(1, 2)$. V — код с параметрами (1.5) для $r=3c-1$, $c\geqslant 9$; б) V_0 — [7, 1]3,0-код, $g=(1, 2)$. V — код с параметрами (1.5) для $r=3c$; в) V_0 — [7, 2]3,2-код с проверочной матрицей вида

$$\Phi^5=\begin{Vmatrix}0&0&0&0&1&0&1\\0&0&0&1&0&0&1\\0&0&1&0&0&0&1\\0&1&0&0&0&1&0\\1&0&0&0&0&1&0\end{Vmatrix}. \tag{5.1}$$

$\Lambda=2$, $\rho=1$, $g=(1)$. Код V имеет параметры (1.5) для $r=3c-1$, $c=\overline{5,8}$. ◀

Далее в $D_\varkappa^{mR}(g, \rho)$ подматрица $A^{m\times 3}$ — проверочная матрица кода (1.5) с $r=3c$.

Пример 4. $R=4$. V_0 — [6, 1]4,2-код с проверочной матрицей, полученной исключением последнего столбца из матрицы (5.1). $\Lambda=2$, $g=(1,1)$. Код V имеет параметры (1.6). ◀

В [1] показано, что $2\leqslant t[53, 43]\leqslant 3$, $3\leqslant t[63, 49]\leqslant 4$, $3\leqslant t[64, 50]\leqslant 4$, $4\leqslant t[62, 45]\leqslant 5$, $4\leqslant t[63, 46]\leqslant 5$. Поэтому из (1.4)—(1.6) имеем (1.8).

Пример 5. $R=5$, V_0 — [5, 1]5,3-код с проверочной матрицей F^4 вида (4.1), $R_0=2$. $\Lambda=3$, $\rho=2$, $g=(1,1)$. Код V имеет параметры: $r=4+5m$, $m\geqslant 3$, $n=7\times 2^m-2$. Для $r=24$ имеем $n=110$, для $r=29$ имеем $n=222$. Альтернативой может служить код V', построенный, когда V_0 — [10, 1]5,0-код. Но для $r=24$ код V' построить нельзя, а для $r=29$ код V' имеет длину 230. Таким образом, ситуация $R=R_0^*(l>0)>R_0$ бывает полезной. ◀

Пример 6. $R=3v+2$. V_0 — $[2R+1, 1]R$,0-код. $g=(1,1,3,\ldots, 3)$. Параметры кода V: $r=RC$, $c\geqslant 9$, $2^c>8R$, $n<0{,}7R2^{r/R}+0{,}35\times 2^{r/R}-R$. ◀

Для уменьшения $N(m)$ следует увеличивать l и Λ, стараясь получить $R_0^*(l>0)=R_0$. Для оценки величины $R_0^*(l)$ полезно знать спектры весов смежных классов кода V_0, конфигурации слов кода V_0 или (что то же самое) конфигурации групп линейно зависимых (л. з.) столбцов матрицы Φ^s. Такие группы можно использовать, чтобы получать нулевой столбец из E^s и изменять число столбцов матрицы Φ^s, суммой которых является некоторый столбец из E_0^s. Последнее достигается включением в сумму (в качестве слагаемых) некоторой группы л. з.-столбцов. Те столбцы из группы, которые до этого включения входили в сумму, «сократятся». Если $d_0\leqslant R_0$, где d_0 — минимальное расстояние кода V_0, то $R_0^*(1)=R_0$. Если $d_0>R_0$, то всегда $R_0^*(l>0)>R_0$.

Пусть Φ^s строится из матриц Φ_j, $j=1, 2, \ldots$ с помощью конструкций ADS или DS [1]. ADS целесообразно строить так, чтобы только один столбец в Φ^s был «смешанным» и содержал по одному столбцу из всех матриц Φ_j. В этом случае в Φ^s сохраняются все группы л. з.-столбцов из Φ_j, которые не включали смешанного столбца. (Хорошие результаты дает использование в качестве Φ_j проверочной матрицы кода Голея, позволяющее построить коды с $n\approx 0{,}577R2^{r/R}$.)

DS сохраняет в матрице Φ^s все группы л. з.-столбцов, имеющиеся в матрицах Φ_j.

Пример 7. $R\geqslant 16$ (ограничение связано с упрощением оценок параметров), $R_0=R$, V_0 — $[2R+b, b]R$-код, $b=\lceil R/a\rceil$, $1\leqslant a\leqslant R/3$. Матрица Φ^s получена как DS $b-1$ проверочных матриц $[2a+1, 1]a$-кода и проверочной матрицы $[2a_M+1, 1]a_M$-кода, $a_M=R-(b-1)a$. Каждая матрица Φ_j, $j=\overline{1, b-1}$ суть группа из $2a+1$ л. з.-столбцов. Это позволяет показать, что $R_0^*(R-2a)=R$ и V_0 суть $[2R+b, b]R$, $(R-2a)$-код. Положим $\Lambda=l=R-2a$, $\rho=2a$, $g=(1,1,1,3,3,\ldots, 3)$ для $2a=3\mu$, $g=(1,1,2,3,3,\ldots, 3)$ для $2a=3\mu+1$, $g=(1,1,3,3,\ldots, 3)$ для $2a=3\mu+2$. Используя (1.5) и минимизируя n в (1.3), после некоторых вычислений принимаем $a=\lfloor(192R/311)^{1/3}\rfloor\approx 0{,}785\sqrt[3]{R}$, $b\approx 1{,}27\sqrt[3]{R}$, что дает параметры (1.7). ◀

Сопоставляя примеры 6 и 7, видим, что параметры исходного кода V_0,

рассматриваемого как покрывающий код, лучше в примере 6. Но параметры построенного кода V лучше в примере 7, так как здесь эффективнее параметры кода V_0, рассматриваемого как R_0^*, l-подмножество.

В (1.7) константу 1,5 в сомножителе $(1+1{,}5/\sqrt{R})$ можно уменьшить, например, так: не все матрицы Φ_j делать одинаковыми, использовать $g\in G_i(\rho)$, $i=2,3$, использовать в $D_\varkappa^{mR}(g,\rho)$ коды примера 6 или (итеративно) коды примера 7. Конструктивным путем уменьшения указанной константы (до 0,5) является использование в качестве Φ_j проверочной матрицы $[2^t,\ t+1]\,a_t$-кода Рида — Маллера 1-го порядка, где $a_t=2^{t-1}-2^{t/2-1}$, t — четное [1, с. 389; 20, § 1.9, гл. 14]. (Эту матрицу можно разбить 2^t-1 способом на две непересекающиеся группы л. з.-столбцов, по 2^{t-1} столбцов в каждой группе.)

Матрицу Φ^s можно строить и следующим путем. Выберем (в качестве базы для построения кода V_0) некоторый вспомогательный код V_0^* с проверочной матрицей Φ_*^s. Включив в Φ_*^s дополнительные столбцы, образующие л. з.-группы, получим матрицу Φ^s.

Пример 8. $R\geqslant 16$, $R_0=R$, $V_0^*-[Q^*,\ Q^*-s]R$-код, $Q^*=w_1^*R2^{s/R}+w_2^*2^{s/R}$, w_1^*, w_2^* — константы. Пусть $p\leqslant R/3$, $f=\lceil Q^*/p\rceil$. Разобьем столбцы проверочной матрицы Φ_*^s кода V_0^* на f непересекающихся групп, $f-1$ из которых содержит по p столбцов. Добавим в каждую группу столбец, равный сумме ее столбцов. Получим матрицу Φ^s. Легко увидеть, что $V_0-[Q^*+f,\ Q^*+f-s]R$, $(R-p)$-код. Положим $\Lambda=R-p$; $\rho=p$; $g\in G_1(p,2,1)$, например, $g=(1,1,3,3,\ldots,3)$ для $p=3\mu+2$. Как в примере 6, используем (1.5) и, минимизируя длину n кода V, после вычислений примем $p=\lfloor(384Q^*/311)^{1/4}\rfloor\approx 1{,}1\sqrt{Q^*}$, $f\approx 0{,}9\sqrt{Q^*}$. Это дает код V с параметрами

$$r=s+mR,\quad 2^m>Q^*+0{,}9\sqrt{Q^*},\quad q=1+2{,}2/\sqrt{Q^*},\tag{5.2}$$
$$n<w_1^*qR2^{r/R}+(w_2^*q+0{,}6/2^{s/R})2^{r/R}.\ \blacktriangleleft$$

Константу 2,2 можно уменьшить, используя в $D_\varkappa^{mR}(g,\rho)$ коды примера 7.

Коды, построенные в данной работе, имеют высокую скорость передачи. Из примеров 3—8 видно, что параметры построенных кодов для больших R удобно записывать в виде

$$n=wR2^{r/R}+o(R2^{r/R})=UR^2+o(R^2),\tag{5.3}$$
$$U=wg2^v,\ r=r_{\min}+vR,\ r_{\min}=\lceil R\log_2 gR\rceil,\ 2^{r/R}=gR2^v,$$

где $w<1$, $g>1$ — константы (вообще говоря, не целые), фиксированные для конкретного семейства кодов; $v\geqslant 0$ — целая константа, которая может неограниченно возрастать (что и задает *семейство* кодов); $r_{\min}$ — минимальное значение r, для которого можно построить код V из данного семейства.

Константа w определяет качество построенного семейства кодов, ее уменьшение является основной задачей при построении асимптотически хороших кодов с параметрами вида (5.3). Константа g ограничивает величину r снизу. Для кодов (1.7) $16\geqslant g>8$.

Оценим w с помощью границы сферической упаковки: $2^r\leqslant\sum_{i=0}^{R}C_n^i$. Из формулы Стирлинга — $C_n^R<n^Re^R/(\sqrt{2\pi RR^R})$. Для достаточно больших R: $(2\pi R)^{1/2R}\sim 1$; $n\sim UR^2$ и $n>e^{-1}R2^{r/R}\approx 0{,}367R2^{r/R}$.

Для кодов (1.7) $w=0{,}5$. Для сравнения заметим, что если строить код с радиусом покрытия R как ADS кодов Хэмминга, то $w=1$, а если использовать ADS кодов (1.2) из [18], то $w=0{,}875$.

Для достаточно больших R плотность покрытия, которую обеспечивают коды с параметрами (5.3) и $w=0{,}5$, $\bar{\mu}[R,V]=\sum_{i=0}^{R}C_n^i/2^r\sim(we)^R/\sqrt{2\pi R}\sim$ $\sim(e/2)^R$.

В соответствии с примером 8 конструкция (3.5) сохраняет то значение константы w, которое было в базовом коде V_0^*. С этой точки зрения заслуживает внимания использование в качестве V_0^* кодов Рида — Маллера 1-го порядка; кодов, применяемых при анализе переключательной игры Гэйла — Берлекэмпа (light-bulb кодов) [1, 5, 12, 17]; ADS указанных кодов. Эти коды позволяют получить $w<0{,}5$. Так [1, ф-ла (80)], из light-bulb кодов с $l=m=81$ получаем код V с $w=0{,}4977$.

Код V_0^* существенно короче кода V. Поэтому если код V_0^* с хорошим значением w найден перебором, то сложность построения кода V может оказаться приемлемой (при $m\sim Q^*$, $n\sim 2^{q^*}Q^*$ сложность построения кода V полиномиальна, даже если сложность построения кода V_0^* экспоненциальна).

Сопоставим полученные результаты с известными для конечных n, R.

Результаты (1.8) и (1.9) улучшают соответственно таблицу I из [1] и таблицу II из [16]. Большая часть результатов, следующих из (3.1), (3.5), (4.4), лежит за пределами этих таблиц.

Для $R=2$ известен ряд бесконечных семейств кодов [1, 16, 18]. Среди них лучшими параметрами обладают коды из [18] (см. (1.2)). Построенные в данной работе коды (1.4) для четных $r\geqslant 10$ имеют по сравнению с кодами (1.2) меньшую длину и меньшую плотность покрытия.

В [1, теорема 30 и замечание к ней] приведены пары значений n, k, для которых точно не известно, $t[n, k]$ равно 2 или 3. Используя коды (1.4), можно сократить число этих пар. Так, для $55\times 2^{c-5}-2\leqslant n<56\times 2^{c-5}-2$ из (1.4) следует $t[n, k=n-2c]=2$, из [1, 18] имеем $2\leqslant t[n, k]\leqslant 3$.

Коды с $R=3$ для сопоставления с (1.5) можно построить как ADS кодов Хэмминга и кодов (1.2). Это дает, например, семейство $\overline{V}$ с параметрами $R=3$, $n=9\times 2^{c-2}-3$, $r=3c-1$, $c\geqslant 4$, $\bar{\mu}[3, \overline{V}]\approx 3{,}79$, которые хуже, чем в (1.5). Но следует отметить (в этом и других случаях), что новые коды не строятся для относительно маленьких r. Так, в (1.5) $r\geqslant 26$, $r\geqslant 21$, $r\geqslant 14$, но в последней формуле для известных кодов $r\geqslant 11$.

В целом для конечных n, R конструкции (3.1), (3.5) дают *разнообразные* возможности построения покрывающих кодов. Для тех значений r, где конструкции можно применять, они часто приводят к лучшим результатам, чем известные конструкции. Обратим внимание на относительно небольшую плотность покрытия в (1.4), (1.5).

Автор признателен В. М. Блиновскому, Г. А. Кабатянскому и А. Н. Скоробогатову за полезные советы и благодарит всех участников семинара по алгебраической теории кодирования ИППИ АН СССР за конструктивное обсуждение результатов работы.

СПИСОК ЛИТЕРАТУРЫ

1. *Graham R. L., Sloane N. J. A.* On the Covering Radius of Codes // IEEE Trans. Inform. Theory. 1985. V. 31. № 3. P. 385–401.
2. *Cohen G. D., Karpovsky M. G., Mattson H. F., Jr., Shatz J. R.* Covering Radius-Survey and Recent Results // IEEE Trans. Inform. Theory. 1985. V. 31. № 3. P. 328–343.
3. *Helleseth T.* On the Covering Radius of Cyclic Linear Codes and Arithmetic Codes // Discrete Appl. Math. 1985. V. 11. № 2. P. 157–173.
4. *Cohen G. D., Lobstein A. C., Sloane N. J. A.* Further Results on the Covering Radius of Codes // IEEE Trans. Inform. Theory. 1986. V. 32. № 5. P. 680–694.
5. *Mattson H. F., Jr.* An Improved Upper Bound on Covering Radius // Lecture Notes Computer Sci. 1986. № 228. P. 90–106.
6. *Delsart P., Pivet P.* Do Most Binary Linear Codes Achieve the Goblick Bound on the Covering Radius? // IEEE Trans. Inform. Theory. 1986. V. 32. № 6. P. 826–828.
7. *Sloane N. J. A.* A New Approach to the Covering Radius of Codes // J. Combin. Theory. Ser. A. 1986. V. 42. № 1. P. 61–86.
8. *Блиновский В. М.* Нижняя асимптотическая граница для числа слов линейного кода в произвольной сфере с заданным радиусом из F_q^n // Пробл. передачи информ. 1987. Т. 23. № 2. С. 50–53.

9. *Kilby K. E., Sloane N. J. A.* On the Covering Radius Problem for Codes I. Bounds on Normalized Covering Radius // SIAM J. Alg. Disc. Meth. 1987. V. 8. № 4. P. 604–618.
10. *Kiby K. E., Sloane N. J. A.* On the Covering Radius Problem for Codes II. Of Low Dimension; Normal and Abnormal Codes // SIAM J. Alg. Disc. Meth. 1987. V. 8. № 4. P. 619–627.
11. *Calderbank A. R., Sloane N. J. A.* Inequalities for Covering Codes // IEEE Trans. Inform. Theory. 1988. V. 34. № 5. Pt 2. P. 1276–1280.
12. *Pach J., Spencer J.* Explicit Codes with Low Covering Radius // IEEE Trans. Inform. Theory. 1988. V. 34. № 5. Pt 2. P. 1281–1285.
13. *Honkala I. S., Hämäläinen H. O.* A New Construction for Covering Codes // IEEE Trans. Inform. Theory. 1988. V. 34. № 5. Pt 2. P. 1343–1344.
14. *Кабатянский Г. А., Панченко В. И.* Упаковки и покрытия пространства Хэмминга шарами единичного радиуса // Пробл. передачи информ. 1988. Т. 24. № 4. С. 3–16.
15. *Влэдуц С. Г., Скоробогатов А. Н.* Радиус покрытия длинных кодов БЧХ // Пробл. передачи информ. 1989. Т. 25. № 1. С. 38–45.
16. *Brualdi R. A., Pless V. S., Wilson R. M.* Short Codes with a Given Covering Radius // IEEE Trans. Inform. Theory. 1989. V. 35. № 1. P. 99–109.
17. *Fishburn P. C., Sloane N. J. A.* The Solution to Berlekamp's Switching Game // Discrete Math. 1989. V. 74. № 3. P. 263–290.
18. *Габидулин Э. М., Давыдов А. А., Томбак Л. М.* Коды с радиусом покрытия 2 и другие новые покрывающие коды // Тр. X Всесоюз. симпозиума по проблеме избыточности в информационных системах. Тез. докл. Л., 1989. Ч. 1. С. 14–17.
19. *Блиновский В. М.* Асимптотически точные равномерные оценки для спектров смежных классов линейных кодов // Пробл. передачи информ. 1990. Т. 26. № 1. С. 99–103.
20. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
21. *Самойленко С. И., Давыдов А. А., Золотарев В. В., Третьякова Е. И.* Вычислительные сети (адаптивность, помехоустойчивость, надежность). М.: Наука, 1981.
22. *Айдинян А. К.* О матрицах с невырожденными квадратными подматрицами // Пробл. передачи информ. 1986. Т. 22. № 4. С. 106–108.
23. *Татт У.* Теория графов. М.: Мир, 1988.

Поступила в редакцию
21.06.89
После переработки
25.06.90