第15卷 第4期 电子科学学刊 Vol. 15, No. 4
1993年7月 JOURNAL OF ELECTRONICS July, 1993

关于线性分组码的不可检错误概率

徐 大 专
(南京航空学院电子工程系,南京 210016)

摘要 本文给出了检错好码的定义，证明了 GF(2) 上的(n, k)线性分组码为检错好码的充要条件是其对偶码也为检错好码。文中还得到了关于检错好码的一系列新的结果. 对二元(n,k) 线性分组码，我们给出了不可检错误概率新的下限. 这些限只与 n 和 k 有关，而与码的重量结构无关.

关键词 信息论;线性分组码;对偶码;不可检错误概率;检错好码

1. 引言

在差错控制系统中有两种基本的差错控制方式[1]，一种是前向错误纠正(FEC)方式，另一种是自动请求重传(ARQ)方式. ARQ 体制已经在数据通信系统中获得了广泛的应用. 在 ARQ 体制中，线性分组码通常用来检错，这时 ARQ 体制的性能与分组码的不可检错误概率有关. 因此,研究线性分组码的检错性能有非常重要的意义.

本文一方面研究线性分组码和它的对偶码在检错能力方面的对应关系，证明了关于检错码的一个对偶定理,并用该定理得到了关于检错码的一系列新的结果.

另一方面,研究线性分组码不可检错误概率的限. 目前,关于上限的研究已经取得了一定的进展,如线性规划上限[2]等，但关于下限的研究则很少. 文献[3]给出了两个不可检错误概率的下限，这些限与码的最大重量有关. 本文将给出两个新的下限，这些下限只与码长 n 和信息位数目 k 有关,而与码的重量结构无关.

2. 关于检错码的对偶定理

考虑 GF(q) 上的 (n,k) 线性分组码 C，设信道为 q 进制离散无记忆信道(DMC)，每个符号正确接收的概率为 1—ε，错成其它 $q-1$ 个符号中任何一个的概率为 $\varepsilon/(q-1)$. 令 $P_{ud}(C,\varepsilon)$ 表示 C 的不可检错误概率,那么

$$P_{ud}(C,\varepsilon)=\sum_{i=1}^{n}A_i\left(\frac{\varepsilon}{q-1}\right)^i(1-\varepsilon)^{n-i} \tag{1}$$

其中 A_i 表示 C 中汉明重量为 i 的码字数目,$0\leqslant\varepsilon\leqslant(q-1)/q$. 当 $\varepsilon=(q-1)/q$ 时，q 个符号出现的概率相等,这对应于信道最差的情况. 此时

$$P_{ud}\left(C,\frac{q-1}{q}\right)=q^{-n}\sum_{i=1}^{n}A_i=q^{-n}(q^k-1)<q^{-(n-k)} \tag{2}$$

通常总是认为,信道错误概率 ε 越小,不可检错误概率 $P_{ud}(C,\varepsilon)$ 也越小. 然而，对某些

1992.01.22 收到,1992.05.03 定稿.
徐大专 男，1963年生，讲师,正在从事编码理论、神经网络和全球定位系统(GPS)方面的研究.

分组码而言，$P_{ud}(C,\varepsilon)$并不是ε的单调下降函数，即不可检错误概率不一定满足上限$q^{-(n-k)}$. 为了叙述方便，我们首先给出如下定义.

定义 1 令 $P_{ud}(C,\varepsilon)$ 表示 q 进制(n,k)线性分组码 C 的不可检错误概率，如果对任意的 $\varepsilon\in[0,(q-1)/q]$ 都有

$$P_{ud}(C,\varepsilon)<q^{-(n-k)}$$

则称 C 为检错好码.

现在我们开始证明本文的主要结论. 令 $C^{\perp}$ 表示 q 进制(n,k)线性分组码 C 的对偶码，B_i 表示 $C^{\perp}$ 中汉明重量为 i 的码字数目，那么，$\{A_i,\ 0\leqslant i\leqslant n\}$和$\{B_i,\ 0\leqslant i\leqslant n\}$称为 C 和 $C^{\perp}$ 的重量分布. 令

$$A(x)=\sum_{i=0}^{n}A_ix^i,\quad B(x)=\sum_{i=0}^{n}B_ix^i$$

$A(x)$ 和 $B(x)$ 分别称为 C 和 $C^{\perp}$ 的重量算子.

定理 1 如果 C 是检错好码，那么 $C^{\perp}$ 也是检错好码.

证明 由 C 是检错好码的条件，我们有

$$P_{ud}(C,\varepsilon)=\sum_{i=1}^{n}A_i\left(\frac{\varepsilon}{q-1}\right)^i(1-\varepsilon)^{n-i}<q^{-(n-k)},\quad 0\leqslant\varepsilon\leqslant(q-1)/q \tag{3}$$

上式可改写成

$$(1-\varepsilon)^n\left[A\left(\frac{\varepsilon}{(q-1)(1-\varepsilon)}\right)-1\right]<q^{-(n-k)},\quad 0\leqslant\varepsilon\leqslant(q-1)/q \tag{4}$$

由 MacWilliams 恒等式[4]

$$A(x)=q^{-(n-k)}[1+(q-1)x]^nB\left[\frac{1-x}{1+(q-1)x}\right] \tag{5}$$

(4)式可改写成

$$q^{-(n-k)}B[1-q\varepsilon/(q-1)]-(1-\varepsilon)^n<q^{-(n-k)},\quad 0\leqslant\varepsilon\leqslant(q-1)/q \tag{6}$$

注意到 $B_0=1$，则有

$$\sum_{i=1}^{n}B_i[1-q\varepsilon/(q-1)]^i<q^{n-k}(1-\varepsilon)^n,\quad 0\leqslant\varepsilon\leqslant(q-1)/q \tag{7}$$

$C^{\perp}$ 的不可检错误概率

$$\begin{aligned}P_{ud}(C^{\perp},\delta)&=\sum_{i=1}^{n}B_i[\delta/(q-1)]^i(1-\delta)^{n-i}\\&=(1-\delta)^n\sum_{i=1}^{n}B_i\left[\frac{\delta}{(q-1)(1-\delta)}\right]^i\end{aligned} \tag{8}$$

令

$$\delta/[(q-1)(1-\delta)]=1-q\varepsilon/(q-1) \tag{9}$$

那么

$$\delta=[(q-1)-q\varepsilon]/[q(1-\varepsilon)],\quad 1-\delta=1/[q(1-\varepsilon)] \tag{10}$$

当 $\varepsilon=0$ 时，$\delta=(q-1)/q$，对应于信道最坏的情况，当 $\varepsilon=(q-1)/q$ 时，$\delta=0$，对应于信道最好的情况. 又

$$d\delta/d\varepsilon = -1/[q(1-\varepsilon)^2] < 0$$

即 δ 是 ε 的单调下降函数，因此，当 $\varepsilon \in [0,(q-1)/q]$ 时，也有 $\delta \in [0,(q-1)/q]$，反之亦然．现在把(9)，(10)式代入(8)式得

$$P_{ud}(C^{\perp},\delta) = [q(1-\varepsilon)]^{-n}\sum_{i=1}^{n} B_i[1-q\varepsilon/(q-1)]^i,\quad 0 \leqslant \varepsilon \leqslant (q-1)/q \tag{11}$$

再由(7)式的条件得

$$P_{ud}(C^{\perp},\delta) < q^{-k},\quad 0 \leqslant \delta \leqslant (q-1)/q \tag{12}$$

即 $C^{\perp}$ 也是检错好码，证毕．

推论 1　如果 C 不是检错好码，那么其对偶码 $C^{\perp}$ 也不是检错好码．

证明　用反证法．如果 $C^{\perp}$ 是检错好码，由定理 1，$C^{\perp}$ 的对偶码 C 也是检错好码．这与 C 不是检错好码的条件矛盾，所以 $C^{\perp}$ 不是检错好码．

由定理 1 和推论 1 立即得到

定理 2　GF(q) 上的线性分组码 C 是检错好码的充要条件是其对偶码 $C^{\perp}$ 也是检错好码．

支持定理 2 的例子有二元线性完备码及其对偶码[5,6]，包括汉明码和极长码，奇偶校验码和重复码，Golay(23，12) 码及其对偶码(23，11)．这些码都分别被证明是检错好码．

3. 关于检错好码的进一步结果

目前，已经证明了某些码是检错好码，而其对偶码是否为检错好码尚不清楚．由定理 2 可以立即得到如下一系列结论．

结论 1　一阶 Reed-Muller 码是检错好码．

结论 2　距离等于 5 的本原 BCH 码的对偶码 $(2^m-1,2m)$ 是检错好码．

结论 3　距离等于 6 的扩展本原 BCH 码的对偶码$(2^m,2m)$是检错好码．

结论 4　距离等于 8 的扩展本原 BCH 码的对偶码$(2^m,3m)$是检错好码．

结论 5　最大距离可分码的对偶码是检错好码．

结论 1—结论 5 的证明　一阶 Reed-Muller 码是扩展汉明码的对偶码，而扩展汉明码是检错好码[6]，由定理 2 得结论 1．距离等于 5 的本原 BCH 码，距离等于 6 和 8 的扩展本原 BCH 码以及最大距离可分码都是检错好码[2,6,7]，由定理 2 得结论 2—结论 5．

结论 6　距离等于 7，码长 $n = 2^m-1$ 的本原 BCH 码及其对偶码$(2^m-1,3m)$，当 m 为大于等于 6 的偶数时，不是检错好码；当 $m=4$ 时，是检错好码．

证明　文献[8]已经证明，当 $m \geqslant 6$ 且为偶数时，距离等于 7 的本原 BCH 码$(2^m-1,2^m-3m-1)$不是检错好码．由定理 2，结论 6 的前一部分是显然的．

当 $m=4$ 时，本原 BCH 码为(15，5，7)．该码的重量算子 $A(x) = 1+15x^7+15x^8+x^{15}$，因此，不可检错误的概率

$$\begin{aligned} P_{ud}(C,\varepsilon) &= 15\varepsilon^7(1-\varepsilon)^8 + 15\varepsilon^8(1-\varepsilon)^7 + \varepsilon^{15} \\ &= 15\varepsilon^7(1-\varepsilon)^7 + \varepsilon^{15} \end{aligned}$$

对 $P_{ud}(C,\varepsilon)$ 求导得

$$dP_{ud}(C,\varepsilon)/d\varepsilon = 15\varepsilon^6[7(1-\varepsilon)^6(1-2\varepsilon)+\varepsilon^8] > 0,\quad 0 \leqslant \varepsilon \leqslant 1/2$$

所以(15,5,7) BCH 码及其对偶码是检错好码.

结论 7 距离等于 8,码长 $n=2^m$ 的扩展本原 BCH 码及其对偶码$(2^m, 3m)$,当 $m\geqslant 6$ 且为偶数时,不是检错好码;当 $m=4$ 时,是检错好码.

证明 结论 7 的前一部分由文献[8]和定理 2 得到. $m=4$ 的扩展本原 BCH 码(16,5,8)的重量算子 $A(x)=1+30x^8+x^{16}$,则 $P_{ud}(C,\varepsilon)=30\varepsilon^8(1-\varepsilon)^8+\varepsilon^{16}$,那么

$$dP_{ud}(C,\varepsilon)/d\varepsilon=16\varepsilon^7[15(1-\varepsilon)^7(1-2\varepsilon)+\varepsilon^8]>0,\ 0\leqslant\varepsilon\leqslant 1/2$$

所以(16,5,8)扩展 BCH 码及其对偶码是检错好码.

4. 不可检错误概率的下限

考虑二元(n,k)线性分组码 C,在 BSC 信道上 C 的不可检错误概率为

$$P_{ud}(C,\varepsilon)=\sum_{i=1}^{n}A_i\varepsilon^i(1-\varepsilon)^{n-i}=(1-\varepsilon)^n\sum_{i=1}^{n}A_i\left(\frac{\varepsilon}{1-\varepsilon}\right)^i \tag{13}$$

也可以用对偶码的重量分布来表达

$$P_{ud}(C,\varepsilon)=2^{-(n-k)}\sum_{i=0}^{n}B_i(1-2\varepsilon)^i-(1-\varepsilon)^n \tag{14}$$

这里 $0\leqslant\varepsilon\leqslant 1/2$, 那么 $0\leqslant\varepsilon/(1-\varepsilon)\leqslant 1$, $0\leqslant 1-2\varepsilon\leqslant 1$, $[\varepsilon/(1-\varepsilon)]^i$ 和$(1-2\varepsilon)^i$ 都是 i 的单调下降函数. 利用这个性质,文献[3]得到了两个下限

$$P_{ud}(C,\varepsilon)\geqslant(2^k-1)(1-\varepsilon)^n[\varepsilon/(1-\varepsilon)]^{d_{\max}} \tag{15}$$

$$P_{ud}(C,\varepsilon)\geqslant 2^{-(n-k)}[1+(2^{n-k}-1)(1-2\varepsilon)^{d'_{\max}}]-(1-\varepsilon)^n \tag{16}$$

其中 $d_{\max}$ 和 $d'_{\max}$ 分别是 C 和 $C^{\perp}$ 中码字的最大重量. 目前大部分码的最大重量还不知道,因此用(15)和(16)式估计不可检错误概率有一定的困难.

下面我们研究不可检错误概率新的下限. 首先给出几个引理.

引理 1 $f(x)=a^x$, $0\leqslant a\leqslant 1$ 是 x 的下凸函数.

证明 $f'(x)=a^x\ln a<0$, $f''(x)=a^x\ln^2 a>0$. 因为二阶导数 $f''(x)>0$, 所以 $f(x)$ 是 x 的下凸函数.

引理 2 $\sum_{i=1}^{n}\lambda_i a^{x_i}\geqslant a^{\sum_{i=1}^{n}\lambda_i x_i}$ $0\leqslant a\leqslant 1$,其中 $\sum_{i=1}^{n}\lambda_i=1$.

证明 由引理 1,a^x 是 x 的下凸函数,由 Janson 不等式[9]即得引理 2.

引理 3 令 A_i 表示(n,k)线性分组码 C 中重量为 i 的码字数目. 如果 C 的对偶码的最小距离大于 1,那么

$$\sum_{i=1}^{n}iA_i=n2^{k-1}$$

证明 见文献[4]

定理 3 如果 (n,k) 线性分组码 C 的对偶码的最小距离大于 1, 那么 C 的不可检错误概率满足

$$P_{ud}(C,\varepsilon)\geqslant(2^k-1)(1-\varepsilon)^{n/2}\varepsilon^{n2^{k-1}/(2^k-1)} \tag{16}$$

和

$$P_{ud}(C,\varepsilon)\geqslant 2^{-(n-k)}[1+(2^{n-k}-1)(1-2\varepsilon)^{(n2^{n-k-1})/(2^{n-k}-1)}]-(1-\varepsilon)^n \tag{17}$$

证明 由(13)式

$$P_{ud}(C,\varepsilon) = (2^k-1)(1-\varepsilon)^n \sum_{i=1}^{n} \frac{A_i}{2^k-1}\left(\frac{\varepsilon}{1-\varepsilon}\right)^i \tag{18}$$

因 $\sum_{i=1}^{n} A_i/(2^k-1) = 1$，由引理 2

$$P_{ud}(C,\varepsilon) \geqslant (2^k-1)(1-\varepsilon)^n \left(\frac{\varepsilon}{1-\varepsilon}\right)^{\left(\sum_{i=1}^{n} iA_i\right)/(2^k-1)} \tag{19}$$

再由引理 3 得

$$P_{ud}(C,\varepsilon) \geqslant (2^k-1)(1-\varepsilon)^n \left(\frac{\varepsilon}{1-\varepsilon}\right)^{n2^{k-1}/(2^k-1)}$$

或者

$$\begin{aligned} P_{ud}(C,\varepsilon) &\geqslant (2^k-1)(1-\varepsilon)^{n(2^{k-1}-1)/(2^k-1)}\varepsilon^{n2^{k-1}/(2k-1)} \\ &\geqslant (2^k-1)(1-\varepsilon)^{n/2}\varepsilon^{n2^{k-1}/(2k-1)} \end{aligned} \tag{20}$$

这就证明了定理 3 的前一部分，同理可证定理 3 的后一部分。

在多数情况下，线性分组码的最大重量 $d_{\max}$ 大于 $n/2$，这时定理 3 给出的限更紧一些。由于该限不涉及码的重量结构，因此，可以方便地估计线性分组码的不可检错误概率。

5. 结论

本文证明了一个 q 进制线性分组码为检错好码的充要条件是其对偶码也为检错好码。该定理是研究检错码性能的重要工具。本文用这个定理得出了关于检错码的一系列新的结果。我们还给出了二元线性分组码不可检错误概率新的下限。这些限只与码长和信息位数目有关，可以方便地估计线性分组码的不可检错误概率。

参　考　文　献

[1] 林舒，科斯特洛著，王育民，王新梅译，差错控制编码基础和应用，人民邮电出版社，北京，1989 年，第 15—16 页.

[2] T. Kassmi, T. Klove, S. Lin, *IEEE Trans. on IT*, **IT-29**(1983)1, 131—136.

[3] J. K. Wolf, A. H. Michelson, A. H. Levesque, *IEEE Trans. on COM*, **COM-30**(1982)2, 317—324.

[4] F. J. Macwilliams, N. J. A. Sloane, The theory of error-correcting codes, Amsterdam: North-Holland, (1977), pp. 225—232.

[5] S. K. Leung-Yan-Cheong, M. E. Hellman, *IEEE Trans. on IT*, **IT-22**(1976)2, 235—237.

[6] S. K. Leung-Yan-Cheong, E. R. Barnes, D. U. Friedman, *IEEE Trans. on IT*, **IT-25**(1979)1, 110—112.

[7] T. Kassmi, S. Lin, *IEEE Trans. on COM*, **COM-32**(1984)9, 998—1006.

[8] P. Perry, *IEEE Trans. on IT*, **IT-37**(1991)2, 375—378.

[9] R. J. McEliece, The theory of information and coding, Addison-Wesley, Reading, Mass., (1977), pp. 245—249.

ON UNDETECTABLE ERROR PROBABILITIES OF LINEAR BLOCK CODES

Xu Dazhuan

(Nanjing Aeronautical Institute, Nanjing 210016)

Abstract The definition of good codes for error detection is given. It is proved that linear block codes in GF(q) are good codes for error detection if and only if its dual codes are good ones also. A series of new results about good codes for error detection is derived. New lower bounds on undetectable error probabilities of binary (n, k) linear block codes are obtained, which have no relation to the weight structure of the codes but only to n and k.

Key words Information theory; Linear block code; Dual code; Undetectable error probability; Good code for error detection