码长为$\frac{3(q^2-1)}{2}$的对偶包含BCH码及其应用

高　楠

安徽新华学院 通识教育部，中国·安徽　合肥　230088

【摘　要】　BCH码是一类构造量子纠错码的码源，满足一定结构关系的BCH码可以构造参数较好的量子纠错码。本文研究了有限域上码长为$\frac{3(q^2-1)}{2}$的BCH码，其中（$q=6l-1(l>1)$或$q=6l+1$）。基于分圆陪集中元素的结构特点，给出了这类BCH码满足厄米特对偶包含的条件，确定了每个分圆陪集所含元素个数，计算出了此类厄米特对偶包含的BCH码的维数，并利用厄米特构造法，由厄米特对偶包含的BCH码得到了一些参数较好的量子纠错码。

【关键词】有限域；BCH码；量子纠错码；厄米特对偶包含码；分圆陪集

【基金项目】安徽新华学院校级自然科学项目(2022zr018)；安徽省级质量工程项目(2022jyxm673)

1　引言

经典纠错码保障了传统的通信，同样量子纠错码在量子通信中也起到了重要作用。1997年，Calderbank，Rains，Shor，Sloane[1]给出了量子纠错码丰富的理论基础。2001年，Ashikhmin等人[2]给出了厄米特构造法。2007年，Aly等人[3]利用厄米特对偶包含条件构造了多族量子BCH码。2015年，Ma等人[4]研究了码长为$3(q^2-1)$的BCH码，由此构造出了参数较好的量子纠错码，其中$q=3l+1$或$q=3l+2$，$\mathrm{ord}_n(q^2)=3$。2020年，Zhang等人[5]研究长为$r(q^2-1)$的BCH码并由此构造了的量子纠错码，其中$\mathrm{ord}_n(q^2)=4$。此外，许多学者也由各种码长的BCH码构造出很多参数优良的量子纠错码。

引理1（BCH界）设C是有限域F_{q^2}上设计距离为δ false的BCH码，则C的最小距离$d\geq\delta$。

有限域F_{q^2}上长为n的线性码C的厄米特对偶码为$C^{\perp_H}=\{x\in F_{q^2}^n:\langle x,y\rangle_H=0,\forall y\in C\}$，其中$\langle x,y\rangle_H\coloneqq\sum_{i=1}^{n}x_iy_i^q$。下面我们给出有限域$F_{q^2}$上循环码是厄米特对偶包含码的一个充要条件。

引理2[6]设C是在F_{q^2}上的循环码且定义集为Z，$C^{\perp_H}\subseteq C$当且仅当$Z\cap Z^{-q}=\varnothing$，其中$Z^{-q}=\{-qz(\mathrm{mod}\,n)|z\in Z\}$。

引理3[6]　假设C是一个$[n,k,d]_{q^2}$的线性码且$C^{\perp_H}\subseteq C$，则存在一个$[[n,2k-n,\geq d]]_q$的量子纠错码。

2　码长为$\frac{3(q^2-1)}{2}$厄米特对偶包含BCH码的构造

设$n=\frac{3(q^2-1)}{2}$，n是一个正整数且有$\gcd(n,q)=1,m=ord_n(q^2)=3$时，下面分为$q=6l-1(l>1)$和$q=6l+1$两种情况进行讨论。

情况1　$q=6l-1(l>1)$，$r=q+1$的BCH码

引理4 设$Z=\bigcup_{i=0}^{\delta-2}C_{r+i}$，当$2\leq\delta\leq\frac{q-3}{2}$时，$Z\cap Z^{-q}=\varnothing$。

证明假设$Z\cap Z^{-q}\neq\varnothing$，则存在$f$和$h$，使得$(r+h)q^{2l}\equiv-q(r+f)\,\mathrm{mod}\,n$，其中$0\leq f,h\leq\delta-2$，且　$0\leq l\leq3$。设f=h=0，则$rq^{2l}\equiv-qr\,\mathrm{mod}\,n\Rightarrow r(q^{2l-1}+1)\equiv0\,\mathrm{mod}\,n\Rightarrow\frac{3}{2}(q-1)\Big|(q^{2l-1}+1)$，矛盾。

（1）当$l=0$时，$(r+h)\equiv-q(r+f)\,\mathrm{mod}\,n\Rightarrow r(q+1)+qf+h\equiv0\,\mathrm{mod}\,n,$

由于$0<r(q+1)\leq r(q+1)+qf+h\leq(q+1)(r+f)<n,$矛盾。

（2）当$l=1$时，$(r+h)q^2\equiv-q(r+f)\,\mathrm{mod}\,n\Leftrightarrow r(q+1)+qh+f\equiv0\,\mathrm{mod}\,n$，类似$l=0$可推出矛盾。

(3) 当$l=2$时，注意到$\gcd(n,q)=1,\ rq^2\equiv r\,\mathrm{mod}\,n$。

$(r+h)q^4\equiv-q(r+f)\,\mathrm{mod}\,n\Rightarrow r(q^3+1)+q^3h+f\equiv0\,\mathrm{mod}\,n\Rightarrow r(q+1)+q^3h+f\equiv0\,\mathrm{mod}\,n$

$\Rightarrow(q^3h+f)(q-1)\equiv0\,\mathrm{mod}\,n\Rightarrow\frac{3(q+1)}{2}\Big|(q^3h+f),$　即有$q^3h+f\equiv0\,\mathrm{mod}\frac{3}{2}(q+1)$，那么可得$f-h\equiv0\,\mathrm{mod}\frac{3}{2}(q+1)$，若$f\neq h$时，$0<f-h\leq\frac{q-7}{2}<\frac{3(q+1)}{2}$推出矛盾；若$f=h$

时，$(r+f)q^4 \equiv -q(r+f) \bmod n$

$\Rightarrow (r+f)(q^3+1) \equiv 0 \bmod n \Rightarrow n \mid (r+f)(q^3+1) \Rightarrow \frac{3(q-1)}{2} \mid (r+f)(q^2-q+1),$

由带余除法得 $\gcd(q-1, q^2-q+1)=1$，因此得 $\frac{3(q-1)}{2} \mid (r+f)$，由于 $0<r+f \le \frac{3q-5}{2} < \frac{3(q-1)}{2}$，矛盾。

引理5 当 $0 \le i \le \frac{q-7}{2}$，有 $|C_{r+i}| = \begin{cases} 1, & i=0; \\ 3, & \text{其他}. \end{cases}$

证明 由于 $\mathrm{ord}_n(q^2)=3$，则 $|C_{r+i}| \mid 3$，q^2 模 n 分圆陪集只能含1个或3个元素。C_{r+i} 只有一个元素当且仅当 $(r+i)(q^2-1) \equiv 0 \bmod n \Rightarrow \frac{3}{2} \mid (r+i) \Leftrightarrow 3 \mid i$，当 $0<i \le \frac{q-7}{2}$ 时，$|C_{r+i}|=1 \Leftrightarrow 3 \mid i$，否则 $|C_{r+i}|=3$。

引理6 当 $2 \le \delta \le \frac{q-3}{2}$ 时，分圆陪集 C_r，C_{r+1}，…，$C_{r+\delta-2}$ 互不相交。

证明 由引理5，$C_r=\{r\}$ 与其它分圆陪集不相交。不妨设 $f>h$，其中 $1 \le f,h \le \delta-2$。下证 C_{r+f} 和 C_{r+h} 不相交。

如果 $r+f \equiv r+h \bmod n$，则 $n \mid f-h$。由于 $0<f-h \le \delta-2-1 \le (q-7)/2-1<n$，矛盾。

如果 $r+f \equiv (r+h)q^2 \bmod n$，则能推出

$r(q^2-1)+q^2h-f \equiv 0 \bmod n \Rightarrow q^2h-f \equiv 0 \bmod n$

$\Rightarrow 3(q^2-1)h+3h-3f \equiv 0 \bmod n \Rightarrow 3h-3f \equiv 0 \bmod n,$

由于 $0<3f-3h \le 3((q-7)/2-1)<n$，矛盾。

如果 $r+f \equiv (r+h)q^4 \bmod n$，则能推出

$q^4h-f \equiv 0 \bmod n \Rightarrow 3f-3h(q^4-1)-3h \equiv 0 \bmod n \Rightarrow 3f-3h \equiv 0 \bmod n$

，矛盾。

定理1 当 $2 \le \delta \le \frac{q-3}{2}$ 时，存在参数为 $[n, n-6\delta+4\lceil(\delta-1)/3\rceil+6, \ge \delta]_q$ 的量子纠错码。

证明 设有限域 F_{q^2} 上长为 n 的循环码 C 的定义集为 $Z=\bigcup_{i=0}^{\delta-2} C_{r+i}$，当 $2 \le \delta \le (q-3)/2$，即 $0 \le i \le (q-7)/2$ 时，由引理5，可得 $|Z|=\lceil(\delta-1)/3\rceil+3(\delta-1-\lceil(\delta-1)/3\rceil)=3\delta-2\lceil(\delta-1)/3\rceil-3$。

因此，码 C 是参数为 $[n, n-3\delta+2\lceil(\delta-1)/3\rceil+3, \ge \delta]_{q^2}$ 的BCH码。由引理3，存在参数为 $[n, n-6\delta+4\lceil(\delta-1)/3\rceil+6, \ge \delta]_q$ 的量子纠错码。

情况2 $q=6l+1$，$r=3$ 的BCH码

引理7 设 $Z=\bigcup_{i=0}^{\delta-2} C_{r+i}$，当 $2 \le \delta \le \frac{3q-7}{2}$ 时，$Z \cap Z^{-q}=\varnothing$。

引理8 当 $0 \le i \le \frac{3q-11}{2}$，有 $|C_{r+i}| = \begin{cases} 1, & i=0; \\ 3, & \text{其他}. \end{cases}$

引理9 当 $2 \le \delta \le \frac{3q-7}{2}$ 时，分圆陪集 C_r，C_{r+1}，…，$C_{r+\delta-2}$ 互不相交。

定理2 当 $2 \le \delta \le \frac{3q-7}{2}$ 时，存在参数为 $[n, n-6\delta+4\lceil(\delta-1)/3\rceil+6, \ge \delta]_q$ 的量子纠错码。

3 比较与总结

下面将本文构造的量子纠错码与文献[6]中的量子纠错码进行比较。在码长 n 和设计距离 δ 相同时，文献[6]构造了维数为 $n-6\lceil(\delta-1)(1-1/q^2)\rceil$ 的量子纠错码，本文构造了维数为 $n-6\delta+4\lceil(\delta-1)/3\rceil+6$ 的量子纠错码，易知本文的维数更大。

表1 本文与文献[6]构造的量子纠错码比较

q	本文的量子纠错码	文献[6]的量子纠错码
$q=11$	$[[180,172,\ge 3]]_{11}$	$[[180,168,\ge 3]]_{11}$
	$[[180,166,\ge 4]]_{11}$	$[[180,162,\ge 4]]_{11}$
	$[[180,164,\ge 5]]_{11}$	$[[180,156,\ge 5]]_{11}$
	…	…
$q=7$	$[[72,64,\ge 3]]_7$	$[[72,60,\ge 3]]_7$
	$[[72,58,\ge 4]]_7$	$[[72,54,\ge 4]]_7$
	$[[72,56,\ge 5]]_7$	$[[72,48,\ge 5]]_7$
	…	…

参考文献：

[1] CALDERBANK A R, RAINS E M, SHOR P W, et al. Quantum error correction via codes over GF(4)[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1369-1387.

[2] ASHIKHMIN A, KNILL E. Nonbinary quantum stabilizer codes[J]. IEEE Transactions on Information Theory, 2001, 47(7): 3065-3072.

[3] ALY S A, KLAPPENECKER A, SARVEPALLI P K. Primitive quantum BCH codes over finite fields[C]//2006 IEEE International Symposium on Information Theory. Seattle: IEEE, 2006: 1114-1118.

[4]马月娜,梁放驰等.码长 $n=3(q^2-1)$ 的对偶包含BCH及量子码的构造[J].空军工程大学学报: 自然科学版, 2015, 16(2): 82-85.

[5] ZHANG H, ZHU S X. New quantum BCH codes of length $n=r(q^2-1)$[J]. International Journal of Theoretical Physics, 2021, 60(1): 172-184.

[6] ALY S A, KLAPPENECKER A, SARVEPALLI P K. On quantum and classical BCH codes[J]. IEEE Transactions on Information Theory, 2007, 53(3): 1183-1188.