The Hamming Codes

Mitsuru Takigahira

TL;DR

ハミング [7, 4] 符号 $\mathcal{H}_7$ は 1 重誤り訂正完全 2 元符号で、伝送速度 $\frac{4}{7}$ である。
実際これは 1 重誤り訂正 2 元符号の無限列のうちの 1 つであり、
この列は符号長 n が増えるほど伝送速度 R は 1 に近づく。
この符号はハミングによって 1950 年に考案された[1]が、
ゴレイも同時期に独自にこれらを発見した
(どちらが先に発見されたかの議論については [Th83] を見よ。)

[1] [Ha50]

ハミング符号の構成

1 重誤り訂正 2 元符号に対して、ハミングの球充填限界式 (系 6.17) において $t = 1$ 及び $q = 2$ とおくため、 完全符号に対して以下の条件が成立する。

$$2^{n-k} = 1 + \binom{n}{1} = n + 1$$

$c = n - k$ (検査桁の桁数) とおけば、この条件は以下の式と同値である

$$n = 2^c - 1 \tag{7.4}$$

$k = n - c = 2^c - c$ なので、n 及び k のとりうる値は次のようになる。

$$\begin{array}{ccccccc} c & = & 1 & 2 & 3 & 4 & 5 & \cdots \\ n & = & 1 & 3 & 7 & 15 & 31 & \cdots \\ k & = & 0 & 1 & 4 & 11 & 26 & \cdots \end{array}$$

ハミング符号の構成

このようなパラメータに対して符号を構成しよう。
$t = 1$ とおき、系 7.31 からそのような符号 $\mathcal{C}$ が存在することは

- 階数 c
- すべての 2 つの列の組が線形独立となっている

なる $c \times n$ 行列 H が $\mathbf{F}_2$ 上に存在することと同値で、$\mathbf{F} = \mathbf{F}_2 = \{0, 1\}$ より、

- H の任意の列 $\mathbf{c}_i$ が非零
- H のすべての列が互いに異なっている

つまり H は互いに異なる $n = 2^c - 1$ 個の非零な長さ c の列ベクトルからなる。
このとき、2^c 個の相異なる長さ c の 2 元ベクトルのみが存在し、列 $\mathbf{c}_i$ の選択は存在しない。これらは何らかの順の非零な長さ c の列すべて ($2^c - 1$ 個) になる。
($c = 3$ の場合については例 7.3 を見よ)