ゼミ 8 章-2　p83 8.2 ∼ p85 -L5　　5/1 B4 横溝尚也

8.2 BIBD による視覚暗号の構成

BIBD を使用して視覚暗号で用いる基底行列を構成していく。
$(\omega, b, r, k, \lambda) - BIBD$ を仮定する。v(点の個数) $\leftrightarrow \omega$(秘密を分散させる人数),b(ブロック数) $\leftrightarrow m$(ピクセルの拡大画素) に対応している。基底行列M_1 を BIBD の結合行列,M_0 をどの行もはじめ r 列が"1", 続く b-r 列が"0"である行列とする (左側 $\omega \times r$ 行列の要素がすべて"1"かつ右側$\omega \times b - r$ 列が零行列)。このときM_0 と M_1 はどの行もハミング重み r であるため、p82 式 13 の条件を満たしている。

ここで相対コントラスト γ を考える。$\mathbf{wt}(M_1[i]$ **or** $M_1[j]) = 2r - \lambda$ $(i \neq j)$ と $\mathbf{wt}(M_0[i]$ **or** $M_0[j]) = r$ $(i \neq j)$ に注意すると、

$$\gamma = \frac{2r - \lambda - r}{b} = \frac{r - \lambda}{b}$$

と表せる。

定理 8.1

$(\omega, b, r, k, \lambda) - BIBD$ が存在すると仮定する。このとき拡大画素が $m = b$ となるperfect $(2,\omega) - VTS$)(VTS は Visual Threshold Scheme の略) と、相対コントラスト $\gamma = \frac{r-\lambda}{b}$ が存在する。

実際、p83.Example8.2 は (4,6,3,2,1)-BIBD によって生成されている。

ここでアダマール行列の復習を行う。

アダマール行列 … 要素が 1 または -1 のいずれかであり、かつ各行が互いに直交である正方行列。次数 4t のアダマール行列が存在するとき、かつそのときに限り symmetric な (4t-1,2t-1,t-1)-BIBD が存在する (定理 2.10)。

系 8.2

次数 4t のアダマール行列が存在すると仮定すると、拡大数 m=4t-1, 相対コントラスト $\gamma = \frac{t}{4t-1}$ となる perfect$(2, 4t-1) - VTS$ が存在する。

t は自然数であることに注意すると、$\gamma > \frac{1}{4}$ であることがわかる。

8.3 VTS における最適なコントラスト

8 章の視覚暗号で最も大切なことは、拡大画素 m と相対コントラスト γ の最適な数値の選択である。安全性を保ちつつ視認性を挙げるために、拡大画素を最小化し、相対コントラスト最大化する必要がある。8 章 3 節では m と γ の最適な数値を求める方法について学習していく。

M_0, M_1 を拡大画素 m, 相対コントラスト γ である perfect$(2, \omega) - VTS$ の基底行列、$\omega_i = \mathbf{wt}(M_h[i])$ $(h = 0, 1$、$1 \leq i \leq \omega)$ とする。また a_hを $M_h(i, c) = M_h(j, c) = 1$ となる列の個数とする。このとき $\mathbf{wt}(M_h[i]$ **or** $M_h[j]) = \omega_i + \omega_j - a_h$ と $\mathbf{wt}(M_1[i]$ **or** $M_1[j]) = \mathbf{wt}(M_0[i]$ **or** $M_0[j])$ より、以下が成り立つ。

$$a_0 - a_1 \geq \gamma m \tag{1}$$

また、$M_1(i, c) = 1$ かつ $M_1(j, c) = 0$ となる M_1 の列数は

$$\begin{aligned} w_i - a_1 &\geq w_i - (a_0 - \gamma m) \quad (\because (1)) \\ &= w_i - a_0 + \gamma m \\ &\geq \gamma m \quad (\because a_0 \leq w_i) \end{aligned} \tag{2}$$

ここで T を以下のように定義する。

$$T = \{(i, j, c) : M_1(i, c) = 1, M_1(j, c) = 0\} \tag{3}$$

$(i, j, c) \neq (j, i, c)$ であることに注意すると、(2),(3) 式より以下が得られる。

$$|T| \geq \omega(\omega - 1)\gamma m \tag{4}$$

また、M_1 の列 c における"1"の個数を x とすると、$x(\omega - x)$ 組の $(i, j, c) \in T$ が存在する。この $x(\omega - x)$ を最大化する x は $\frac{\omega}{2}$ である。x が整数であることに注意すると以下が成り立つ。

$$|T| \leq m\lceil\frac{\omega}{2}\rceil\lfloor\frac{\omega}{2}\rfloor \tag{5}$$

式 (4),(5) より以下の定理が成り立つ。

定理 8.3

どの perfect(2,ω) $- VTS$ でも$\lambda \leq \lambda^*(\omega)$ が成立する。ただし$\lambda^*(\omega)$ は

$$\lambda^*(\omega) = \frac{\lceil\frac{\omega}{2}\rceil\lfloor\frac{\omega}{2}\rfloor}{\omega(\omega - 1)}$$

である。

定理 8.3 は最大化したい相対コントラストの最大値が $\lambda^*(\omega)$ であり、そのように設定することが良い視覚分散のパラメータであることを意味する。さらに、系 8.2 は以下のように計算できるため最適なコントラストであることがわかる。

$$\lambda^*(4t - 1) = \frac{2t(2t - 1)}{(4t - 1)(4t - 2)} = \frac{t}{4t - 1}$$