Eidgenössische Technische Hochschule Zürich
Ecole polytechnique fédérale de Zurich
Politecnico federale di Zurigo
Swiss Federal Institute of Technology Zurich

Institut für Theoretische Informatik
Emo Welzl, Jiří Matoušek

24.06.2004

Theoretische Informatik (Kernfach) *SS 2004*
Exercise Set 13

Exercise 1

Complete the proof of Proposition 5.3.3 in the lecture notes (a 2 out of n scheme with contrast close to $1/4$ and with $m = O(\log n)$).

Exercise 2

Let E be a set of two-element subsets of $V = \{1, 2, \ldots, n\}$. In other words, $G = (V, E)$ is a simple undirected graph. The goal is to construct basis matrices for a visual cryptography scheme with n shares where the qualified sets are the edges of G, while every subset of V not containing any edge as a subset is forbidden. (So 2 out of n schemes are a special case with $G = K_n$.)

(a) Find a construction with $m = 2$ for G being a star (one vertex is connected to all others).

(b) Generalize (a) to G being a star plus some number of isolated vertices.

(c) Supposing that basis matrices can be constructed for $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, how can we construct basis matrices for $G = (V, E_1 \cup E_2)$?

(d) Use (b) and (c) to construct suitable basis matrices for every G. What is the smallest m you can get?

Exercise 3

Now we want to encode a secret image into two shares, but we do not want the shares to look random. We are given two "innocent" images 1 and 2, and we want that share 1 alone shows image 1, share 2 alone shows image 2, and the overlay shows the secret image, with no trace of either image 1 or image 2. To this end, construct eight $2 \times m$ basis matrices B_{c,c_1,c_2} for a suitable m. Given a pixel of the secret image of color c, such that the corresponding pixel in image 1 has color c_1 and the pixel in image 2 has color c_2, the pixel is encoded using a random permutation of the columns of B_{c,c_1,c_2}.

(a) Formulate the conditions on these matrices guaranteeing the desired behavior.

(b) Construct such matrices.

Due-date: 01.07.04 in the lecture