CSGT 2007
Combinatorica o.p.s.
Department of Applied Mathematics, VŠB – Technical University Ostrava

Invited lecture

GRAPH COLOURINGS IN STEGANOGRAPHY

Petr Lisoněk

Steganography is the science of information hiding. The sender embeds a secret message into the cover object (e.g., a multimedia file) by slightly distorting it in a way that enables the intended recipient to retrieve the hidden message; at the same time the very existence of the hidden message should be impossible to detect by any third party.
The main goal of Steganography is to design schemes with high embedding efficiency, which is the ratio between the amount of the communicated information and the amount of introduced distortion.
We will show that one class of steganography schemes can be described by graphs that admit a so-called "rainbow colouring." A rainbow colouring of a k-regular graph G is a proper vertex colouring of G with $k+1$ colours such that, for each $v \in V(G)$, all neighbours of v receive distinct colours. The Steganography application requires rainbow colouring functions that have a very low complexity, say $O((\log |V(G)|)^c)$ space and time.
As an explicit example we will note that the d-dimensional integer lattice graph $\mathbb{Z}^d$ admits a rainbow colouring for each d. In a combination with linear codes over finite fields this specific rainbow colouring can be extended to steganographic schemes that have a better embedding efficiency than the previously used schemes.