Grid Colorings in Steganography

Jessica Fridrich and Petr Lisoněk

***Abstract*— A proper vertex coloring of a graph is called rainbow if, for each vertex v, all neighbors of v receive distinct colors. A k-regular graph G is called rainbow (or domatically full) if it admits a rainbow $(k+1)$-coloring. The d-dimensional grid graph G_d is the graph whose vertices are the points of $\mathbb{Z}^d$ and two vertices are adjacent if and only if their l_1-distance is 1. We use a simple construction to prove that G_d is rainbow for all $d \geq 1$. We discuss an important application of this result in steganography.**

***Index Terms*— steganography, domatically full graph, syndrome coding, pixel pooling, embedding efficiency, Hamming code**

I. Rainbow graphs

We use the standard terminology of graph theory. Let G be a simple graph. By $V(G)$ and $E(G)$ we denote the *vertex set* of G and the *edge set* of G, respectively. For a vertex v let $d(v)$ be the *degree* of v (the number of edges incident with v). We say that G is *k-regular* if $d(v) = k$ for all $v \in V(G)$. For the purpose of the application pursued in Section II below it is sufficient to restrict our attention to regular graphs.

A *proper vertex t-coloring* (or just "t-coloring") of G is a mapping $c : V(G) \to C$ with the property that $|C| = t$ and $c(u) \neq c(v)$ whenever $\{u, v\} \in E(G)$. Let $N(v) = \{x \in V(G) : \{x, v\} \in E(G)\}$ be the neighborhood of v in G. A proper vertex coloring c is called *rainbow* if, for each $v \in V(G)$, the set $\{c(u) : u \in N(v)\}$ consists of $d(v)$ distinct colors, that is, all neighbors of v receive distinct colors. We say that G is a *rainbow graph* if there exists an integer k such that G is k-regular and G admits a rainbow $(k+1)$-coloring.

By this definition, each rainbow graph belongs to the class of so-called *domatically full* graphs [3, page 251]. There exist results that can be used to prove that certain graphs are domatically full. One such result is a theorem due to Berge [1, Theorem 2], originally stated in the context of balanced hypergraphs. In order to apply Berge's theorem to proving that G is domatically full, one takes the closed neighborhoods $N[v] := N(v) \cup \{v\}$ ($v \in V(G)$) as the hyperedges of a hypergraph, which is then shown to be balanced. Interestingly, Theorem 1 stated below can not be proved in this way, since for $d \geq 3$ the resulting hypergraph is easily seen to be not balanced by looking at a small finite subgraph of G_d.

We will now establish a class of rainbow graphs. Let $\mathbb{Z}$ and $\mathbb{Z}_n$ denote the integers and the integers modulo n, respectively. Let d be a positive integer throughout. Let $\{e_1, \ldots, e_d\}$ be the standard basis of $\mathbb{Z}^d$, that is, $(e_i)_j$ equals 1 if $i = j$ and 0 otherwise. Let the d-dimensional grid graph G_d be defined as follows. The vertex set of G_d is $\mathbb{Z}^d$, and $\{u, v\} \in E(G_d)$ if and only if $u - v$ equals e_i or $-e_i$ for some $i \in \{1, \ldots, d\}$.

Theorem 1: For each positive integer d the graph G_d is rainbow.

Proof: Let $c : \mathbb{Z}^d \to \mathbb{Z}_{2d+1}$ be defined by

$$c(x_1, \ldots, x_d) := \left(\sum_{i=1}^{d} i x_i \right) \bmod (2d+1). \qquad (1)$$

G_d is $(2d)$-regular, and c is a rainbow $(2d+1)$-coloring of G_d. ■

We would like to point out that Theorem 1 generalizes the result by van Dijk and Willems [4] who proposed rainbow coloring of 2-dimensional lattices in the context of data hiding. The existence of rainbow colorings of higher dimensional lattices is posed as an open question in the last sentence of [4].

II. Application in Steganography

A. Background

Steganography is the science of information hiding. The sender starts with a *cover object*, such as for example a digital multimedia file, and (s)he embeds a hidden message into the cover object by slightly distorting it in a way that enables the intended recipient to retrieve the hidden message from the distorted cover object; at the same time the very existence of the hidden message should be impossible to detect by any third party.

We assume that the cover object is a sequence of elements of D, where $D = \{0, \ldots, m-1\}$, $m = 2^e$, where typically $e \in \{8, 12, 16\}$. For example, $e = 8$ for grayscale digital images and $e = 16$ for CD quality audio.

In most steganographic schemes, the sender and the recipient agree on a *symbol-assignment function*

$$v : D \to S. \qquad (2)$$

In this correspondence we use $S = \mathbb{F}_q$, the finite field with q elements, where q is a prime power. The message undetectability condition limits $|S|$ to relatively small values; thus the condition that $|S|$ is a prime power is not very restrictive and it allows introducing linear codes as ingredients for the message hiding process, as we will see shortly. To embed a given message symbol $z \in \mathbb{F}_q$ in a given element $x \in D$, the sender modifies x to x' so that $v(x') = z$ and $|x - x'|$ is as small as possible.

One of the goals of Steganography is to design schemes with high embedding efficiency, which can be broadly defined as the ratio between the amount of the communicated information and the amount of introduced distortion [5]. We will be measuring the total amount of distortion simply by counting the number of embedding changes.

J. Fridrich is with the Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY 13902-6000, USA.

Corresponding author: P. Lisoněk, Department of Mathematics, Simon Fraser University, Burnaby, BC, V5A 1S6, Canada.

It has been established in [2], [6] that the embedding efficiency can be increased by applying covering codes. Let us now briefly describe this method. The hidden message is retrieved by the receiver as the syndrome of the received (distorted) cover object with respect to a fixed parity check matrix. Consequently, this steganography method is sometimes called "*syndrome coding.*" We use the standard terminology of coding theory that can be found for example in [7].

We will assume that the cover object is a sequence of n elements of D and use $p = (p_1, \dots, p_n)$ to denote the sequence of their symbols obtained using v. The sender and the recipient agree in advance on an $r \times n$ parity check matrix H over $\mathbb{F}_q$. The embedded message is then a vector in $\mathbb{F}_q^r$, retrieved by the recipient as Hs^T, where $s = (s_1, \dots, s_n)$ is the symbol sequence of the modified elements of D communicated by the sender. If $z \in \mathbb{F}_q^r$ is the message to be communicated, then the sender modifies the cover object so that $s = p + y$ where y is a coset leader for the coset corresponding to the syndrome $z - Hp^T$. Assuming that *any required change in any single coordinate of* p *can be realized by one embedding change*, the number of required embedding changes equals the Hamming weight of the coset leader and is bounded from above by the covering radius R of the code.

Because the sender communicates r q-ary symbols in n elements of D, and because the sender needs to do at most R embedding changes, we say that this embedding scheme has *change rate*

$$\rho = \frac{R}{n}$$

and *information rate*

$$\alpha = \frac{r}{n} \log_2 q.$$

In other words, the change rate is the (upper bound on) the probability that an arbitrary element of D will be subjected to an embedding change, and the information rate is measured in bits per element of D. We will call the pair (ρ, α) the *CI rate.* Steganographers' goal is to design schemes with a high information rate but low change rate. A tight upper bound on the information rate for codes of a given change rate ρ was given in [2]

$$\alpha \leq \; H_q(\rho), \tag{3}$$

where H_q is the q-ary entropy function $H_q(x) = -x \log_2(x) - (1-x)\log_2(1-x) + x \log_2(q-1)$.

The most popular codes used in steganography are q-ary Hamming codes [7, p. 193], since the problem solved by the message sender (the coset leader problem) is trivial for them, as all these codes have covering radius $R = 1$. The q-ary Hamming code with codimension r will be denoted by $H(q, r)$ and its CI rate will be denoted

$$(\rho(q,r), \alpha(q,r)) = \left(\frac{q-1}{q^r - 1}, \frac{(q-1)r}{q^r-1} \log_2 q \right). \tag{4}$$

To cover the range of change and information rates more densely, one can use the direct sum of codes [7, Chapter 2, §9]. The following lemma is immediate; we record it here for later use.

Lemma 1: For $i = 1, 2$, let C_i be a q-ary linear code with block length n_i, redundancy r_i and covering radius R_i. Then for any two non-negative integers a, b, the code obtained as the direct sum of a copies of C_1 and b copies of C_2 has the CI rate

$$u\left(\frac{R_1}{n_1}, \frac{r_1}{n_1}\log_2 q\right) + (1-u)\left(\frac{R_2}{n_2}, \frac{r_2}{n_2}\log_2 q\right), \tag{5}$$

where $u = an_1/(an_1 + bn_2)$.

Thus we see from (5) that the direct sum of codes produces codes whose CI rates are convex combinations of CI rates of both codes.

The CI rates (4) for all Hamming codes $H(q, r)$ satisfy a useful relation. From $\rho = (q-1)/(q^r-1)$ we have

$$q^r = 1 + \frac{q-1}{\rho}$$

and thus

$$\alpha = \frac{q-1}{q^r-1} r \log_2 q = \rho \log_2 \left(1 + \frac{q-1}{\rho}\right). \tag{6}$$

Viewing α as a continuous function of $\rho \in (0, 1]$ in (6), we have $\alpha''(\rho) = -(q-1)^2/(\rho(\rho+q-1)^2)$ and so α is strictly concave for $\rho > 0$. Thus, for any $0 < \rho \leq \rho(q, 1)$ the code with the largest information rate (among all codes obtained as direct sums of Hamming codes) is obtained as the sum of the appropriate number of copies of $H(q, s)$ and $H(q, s+1)$, where $\rho(q, s+1) < \rho \leq \rho(q, s)$. In particular, we do not need to consider sums of more than two types of Hamming codes as they cannot have higher information rates.

B. A scheme based on rainbow colorings

According to [8], the impact of embedding becomes statistically detectable rather quickly with the increasing amplitude of embedding changes. Thus, from now on we limit ourselves to so-called *± 1 embedding changes* in which the sender modifies each element of D by at most one, which is the smallest possible modification[1]. Taking $q = 3$ and $v(x) = x \bmod 3$ ($x \in D$) as the symbol-assignment function and applying Hamming codes results in the following CI rates:

$$(\rho(3,r), \alpha(3,r)) = \left(\frac{2}{3^r-1}, \frac{2r}{3^r-1}\log_2 3\right) \tag{7}$$

We now show that pooling pixels combined with rainbow coloring and Hamming codes leads to embedding schemes with CI rates better than those obtainable using convex combinations of (7).

For the purpose of the hidden message embedding we will partition the cover object into disjoint segments, each of which consists of d elements of D. That is, we will partition the cover object into elements of D^d, which we will call *cells.* The details of partitioning into cells are immaterial for our study. The symbol-assignment function will now be a mapping

$$v_c : D^d \to \mathbb{F}_q.$$

[1] We note that a problem will arise in the rare case when the sender is required to apply the $+1$ change to the value $m - 1$ or the -1 change to the value 0. Then the sender can choose a different cover object, or the sender can perform a change of a magnitude greater than 1 to achieve the same effect.

Since both the change rate and the information rate were defined relative to one element of D, for embedding schemes that embed into cells of d elements of D, we define these concepts as

$$\rho = \frac{R}{nd}$$

and

$$\alpha = \frac{r}{nd}\log_2 q.$$

Let us assume that d is chosen such that $q = 2d+1$ is a prime power. Assume that the symbol-assignment function v_c is the function c defined in (1), where we introduce some bijection between $\mathbb{Z}_q$ and $\mathbb{F}_q$ if q is not a prime. Then Theorem 1 guarantees that any symbol in $\mathbb{F}_q$ can be embedded into any cell $x \in D^d$ by changing at most one D-coordinate of x by one. Additionally, suppose that the $H(q,r)$ Hamming code is used as described in the previous section. We have thus defined a scheme that embeds $r\log_2 q$ bits in $\frac{q^r-1}{q-1}d = \frac{q^r-1}{2}$ elements of D by changing at most one element of D by one, leading to the CI rate

$$(\rho_c(q,r), \alpha_c(q,r)) = \left(\frac{2}{q^r-1}, \frac{2r\log_2 q}{q^r-1}\right). \qquad (8)$$

We will now establish that the information rate achieved this way is larger than or equal to the information rate of the corresponding direct sum of ternary Hamming codes with the very same change rate.

Theorem 2: Let $q = 2d+1$ be a prime power, r a positive integer, and $(\rho_c(q,r), \alpha_c(q,r))$ the CI rate (8). Let s be the unique positive integer such that

$$\rho(3, s+1) < \rho_c(q,r) \leq \rho(3,s). \qquad (9)$$

Let C be the direct sum of a copies of $H(3,s)$ and b copies of $H(3,s+1)$, where a, b are chosen such that the CI rate $(\bar{\rho}, \bar{\alpha})$ of C satisfies $\bar{\rho} = \rho_c(q,r)$. Then

$$\alpha_c(q,r) \geq \bar{\alpha}, \qquad (10)$$

and equality occurs if and only if q is a power of 3.

Proof: For ternary Hamming codes, the relation (6) takes the form

$$\alpha = \rho\log_2\left(1 + \frac{2}{\rho}\right). \qquad (11)$$

The CI rates $(\rho_c(q,r), \alpha_c(q,r))$ computed in (8) also satisfy the relation (11). The inequality (10) then follows from the strict concavity of (11) (in which we again consider α as a function of ρ), applied to the triple (9), taking into account Lemma 1. The equality occurs exactly when $\rho_c(q,r) = \rho(3,s)$ for some s. This is, however, equivalent to $q = 3^k$ for some positive integer k. ■

We close this section with a note on how the proposed codes may be used in practice. Because the choice of the code (e.g., the parameters q, d, r) must be communicated to the recipient, a common practice is to select the code parameters to obtain a finite set of M codes with rates $\alpha_1 < \ldots < \alpha_M$ distributed approximately evenly in $[0,1]$. For a given information rate α, the encoder first finds the smallest α_i such that $\alpha \leq \alpha_i$. Then, a small portion of the cover object is selected using a secret shared stego key and the code choice is embedded there using some other embedding scheme, such as LSB embedding. Note that we only need $\log_2 M$ bits to uniquely specify the code choice. The rest of the cover object is used to embed the message using the selected code.

III. Conclusion

We have shown that all integer lattices can be rainbow colored. Under the assumption of limiting the embedding modifications of elements of D to ± 1, we have shown the following: The scheme that pools elements of D into cells of size d, then rainbow colors the cells, and then applies a $(2d+1)$-ary Hamming code has an information rate that is never worse than the information rate of the scheme that changes individual elements of D independently (without pooling) at the very same change rate, and then applies the ternary Hamming code. Both schemes enjoy the same ease of implementation and low computational complexity.

We fully acknowledge at this point that other code families, such as those discussed in [2], can be used to further increase the information rate at the expense of increased embedding and extraction complexity.

Acknowledgments

The work of Jessica Fridrich was supported by Air Force Research Laboratory, Air Force Material Command, USAF, under the research grant number FA8750-04-1-0112. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Air Force Research Laboratory, or the U.S. Government.

Research of Petr Lisoněk was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] C. Berge, Balanced matrices. *Math. Programming* **2** (1972), 19–31.

[2] J. Bierbrauer, Personal communication, available from `http://www.ws.binghamton.edu/fridrich/covcodes.pdf`, 1998.

[3] E.J. Cockayne and S.T. Hedetniemi, Towards a theory of domination in graphs. *Networks* **7** (1977), 247–261.

[4] M. van Dijk and F. Willems, Embedding information in grayscale images. In *Proceedings of the 22nd Symposium on Information Theory in the Benelux,* Enschede, The Netherlands, May 15–16, 2001, pp. 147–154.

[5] J. Fridrich, P. Lisoněk, and D. Soukal, On steganographic embedding efficiency, In *Proceedings of the 8th Information Hiding Workshop,* Alexandria, VA, July 10–12, 2006. To appear in Lecture Notes in Computer Science, Springer.

[6] F. Galand and G. Kabatiansky, Information hiding by coverings. In *Proceedings of the 2003 IEEE Information Theory Workshop,* Paris, France, pp. 151–154.

[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[8] D. Soukal, J. Fridrich, and M. Goljan, Maximum likelihood estimation of secret message length embedded using PMK Steganography in spatial domain, In *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII,* vol. 5681, San Jose, CA, January 16–20, 2005, pp. 595–606.