Legitimate Coloring of Finite Projective Planes via Entropy Compression

Luís Doin - IME-USP
luis.pogrebinschi@usp.br

Rodrigo Bissacot - IME-USP
rodrigo.bissacot@gmail.com

1. Introduction

"The Probabilistic Method has now become one of the most important and indispensable tools for the Combinatorist. There have been several hundred papers written which employ probabilistic ideas and some wonderful monographs. ... Over the past two decades, the explosion of research material, along with the wide array of very impressive results demonstrates another important aspect of the Probabilistic method; some of the techniques involved are subtle, one needs to know how to use those tools, more so than simply understand the theoretical underpinnings.". Nirajan Balachandran's words ([5]) give us an idea of the dimensions that this method has now reached. The method, which became popular after several contributions of Paul Erdős, can be summarized as follows: to prove the existence of an object (a graph with certain properties, for example) one builds a probability space in which our object has positive probability. So, even though we don't know how to build it, we know it exists. Noga Alon and Zoltan Füredi published, in 1989, a result on legitimate colorings of projective planes [1] in which this method is applied via the Local Lovász Lemma (LLL). In [4], Moser and Tardos, for a special case of the LLL called variable version, showed an constructive algorithm that finds the object which the LLL proves existence . In order to analyze this algorithm, Moser and Tardos developed the so-called entropy compression method (this name was given by Terrence Tao in [6]) . Roughly speaking, the method consists in two main stages: first, we provide some way to encode an execution process of the algorithm so that the outcomes of all random choices performed by the algorithm can be uniquely recovered from the resulting encoding. On the second stage we use the structure of this encoding to show that if the expected runtime of the algorithm were unbounded then this encoding would losslessly compress the original random data while reducing its Shannon entropy, which is impossible. It was discovered lately (and somewhat unexpectedly), by Grytczuk, Kozik and Micek in [8], that one can obtain better combinatorial results by a direct application of the entropy compression method rather than simply appealing to the LLL. The idea is to construct a randomized procedure that solves a particular combinatorial problem (instead of proving the LLL in general) and then apply an entropy compression argument to show that this procedure has expected finite runtime. Examples can be found in [2], [7], [3], etc.. In our research [9], we use this method to improve the result obtained by Noga Alon and Zoltan Füredi in [1].

2. Definitions

Let P and L be sets whose elements are called "points and "lines", respectively and $R : P \to L$ a relation. Then (P, L, R) is a projective plane if:

Axiom 1 Given $b, c \in P$, $b \neq c$, there is an only one element $a \in L$ such that (a, b), $(a, c) \in R$.

Axiom 2 Given $b, c \in L$, $b \neq c$, there is an only one element $a \in P$ such that (a, b), $(a, c) \in R$.

Axiom 3 There are $a_1, a_2, a_3, a_4 \in P$ such that there are no $b \in L$ and $i, j, k \in \{1, 2, 3, 4\}$ such that $(a_i, b), (a_j, b)(a_k, b) \in R$, where $k \neq i \neq j \neq k$.

If P and L are finite sets then (P, L, R) is called a finite projective plane and:

Result 1 There is $n \in \mathbb{N}$ such that $\sharp P = \sharp L = n^2 + n + 1$ (and n is the order of the finite projective plane)

Result 2 If $l \in L$ then there are only $p_1, \dots, p_{n+1} \in P$ such that $(p_i, l) \in R$, for all $i \in \{1, ..., n + 1\}$ (for n fixed in the Result 1)

Result 3 If $p \in P$ then there are only $l_1, \dots, l_{n+1} \in L$ such that $(l_i, l) \in R$, for all $i \in \{1, ..., n + 1\}$ (for n fixed in the Result 1)

The next figure shows the projective plane of order 2 - The Fano Plane:

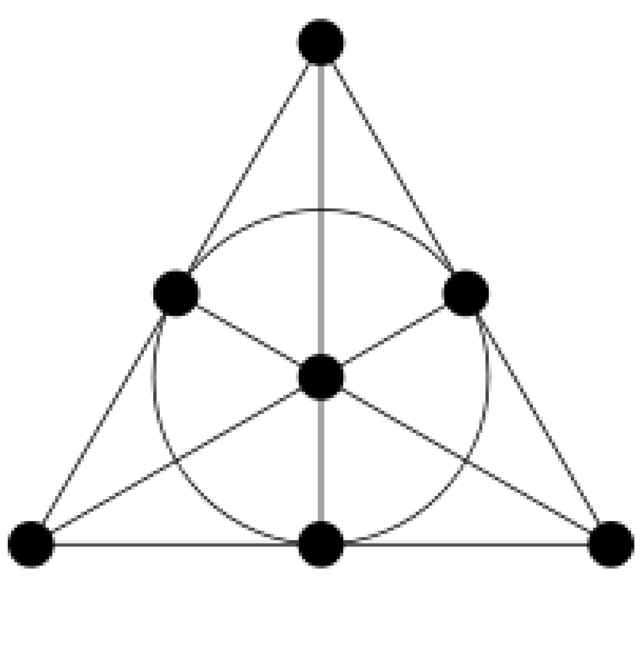

Figure 1: The Fano Plane.

Definition 1 *$f\colon P \to \{1, \dots, \chi\}$ is a χ-coloring of (P, L, R).*

Definition 2 *The type of a line l is the vector $t_{l,f} = (|l \cap f^{-1}(1)|, \dots, |l \cap f^{-1}(\chi)|)$.*

Definition 3 *If, for some χ-coloring, all the lines of a (P, L, R) have different types , this coloring is called legitimate.*

Definition 4 *$\chi(P, L, R)$ is the minimum number of colors necessary in oder to exist a legitimate χ-coloring of (P, L, R).*

3. Results

In [1] is shown that every projective plane of order greater than $3 \cdot 10^{36}$ can be legitimate colored with 8 colors. In our research we concluded that this is true for projective planes of order greater than 10^{10}. We also conclude that with 9 colors one can legitimate color projective plane of order greater than $3 \cdot 10^6$, with 10 colors greater than 60, etc..

We now show a sketch of our proof. First we need some results used in [1]

Lemma 1 *There is $S \subset P$ such that, for all $l \in L$, $\ln n \leqslant |l \cap S| \leqslant 20 \ln n$.*

Now we fix a 8-coloring f for $P \setminus S$. For all $l_i, l_j \in L$, we define $\{l_i, l_j\}$ as a dangerous pair if $d_1(t_{li,f}, t_{lj,f}) \leqslant 40 \ln n$.

Lemma 2 *There is a 8-coloring $f\colon\ P \setminus S \to \{1, \dots, 8\}$ in which there is no $p \in P$ that belongs to more than 4 dangerous pairs.*

Making little changes in the lemmas presented in [1] it is not hard to show that there is a f-coloring of $P \setminus S$ in which none of the points $p \in P$ belong to more than b_n dangerous pairs and there is no line that forms a dangerous pair with more than a_n (or more) lines, given that n is large enough.

Now we use the entropy compression method described in [7] and explained in [6]. We will use a simple algorithm define as follows:

From now on $[n]$ will denote the set $\{1, \dots, n\}$. let P_n be a projective plane of order n with set of points $P = [n^2 + n + 1]$. let S and $f : P \setminus S \to [c]$ be the set and the partial coloring defined above. let $K = \lceil \frac{m}{m-1}(m!\delta(m-1))^{(1/m)} \rceil$ for $m, \delta > 0$ to be defined and $F \in [K]^t$, for $t > 0$. the vector F will provide the entries for the algorithm. We must show that there is a vector F for which the algorithm finds a legitimate coloring of P_n. The algorithm follows:

At step i, assign F_i (the i-th entry of F) to the uncolored point p_j of smallest index of S . Suppose that, after p_j is colored, the distance between two lines becomes zero with all points colored. In this case, it is possible to define a vector R such that lemmas 3 and 4 holds.

Let X_i be the set of points not colored at step i and ϕ_i the partial coloring of P_n at step i. We will show that the pair $(\phi_i, (R_j)_{j \leq i})$ is produced by exactly one vector $(F_j)_{j \leq i}$. But first we need the following lemma:

Lemma 3 At each step i, X_i is uniquely determined by $(R_j)_{j \leq i}$.

Lemma 4 At each step i, the application that associates to each $(F_j)_{j \leq i}$ the pair $((R_j)_{j \leq i}, \phi_i)$ is injective.

Let $\mathcal{F}_t$ be the set of vectors F for which the projective plane is not completely colored at step t of the algorithm. Clearly $|\mathcal{F}_t| \leq K^t$ and if this inequality is strict then there is a vector F for which the projective plane is completely colored (in a legitimate fashion) at step t. Let $\mathcal{R}_t$ be the set of registers R that can be produced by vectors from $\mathcal{F}_t$. Since there are $(K + 1)^{|S|}$ possible partial colorings of P_n at step t the next lemma is a direct consequence of lemma 4.

Lemma 5 $|\mathcal{F}_t| \leq (K + 1)^{|S|}|\mathcal{R}_t|$.

We now need to compute $|\mathcal{R}_t|$ and show that for t large enough, $|\mathcal{F}_t|$ is smaller than the set of all possible vectors, meaning that there is a vector F for which the algorithm terminates.

Let $w = w_1 \dots w_m$ be a word on the alphabet $\mathcal{A} = [(a \cdot b)^{1/m}]$ and $\theta(w) = 1 + \sum_{i=1}^{m}(w_i - 1)(a \cdot b)^{i-1/m}$. One can easily check that θ is injective and has range in $[a \cdot b]$.

Let $R \in \mathcal{R}_t$. We define $R^* = (R^*_i)_{i \leq t}$ as the sequence of words on the alphabet $\mathcal{A}^* = \mathcal{A} \cup \{0\}$ as follows: for $1 \leq i \leq t$, if $R_i = \emptyset$ then $R^*_i = 0$. If $R_i = (u, v)$ then R^*_i is the concatenation of 0 and $\theta^{-1}(v)$. Now, let $R^\bullet$ be the word obtained from R^* by concatenating all its entries and R° on the alphabet $\{0, 1\}$ obtained from $R^\bullet$ changing its non-zero letters into 1.

Let $\mathcal{R}^*_t = \{R^* | R \in \mathcal{R}_t$. It is possible to show that $|\mathcal{R}_t| \leq (m!)^{t/m}|\mathcal{R}^*_t|$. Clearly $R^* \mapsto R^\bullet$ is an injection. We will have to work a little harder to analyse $R^\bullet \mapsto R^\circ$.

Definition 5 A partial Dyck word is word w on the alphabet $\{0, 1\}$ such that any prefix of w contains at least as many 0's as 1's. A Dyck word of length $2t$ is a partial Dyck word with t 0's and t 1's. A descent in a (partial) Dyck word is a maximal sequence of consecutive 1's.

Lemma 6 For any $R \in \mathcal{R}_t$, the word R° is a partial Dyck word with t 0's and $t - r$ 1's, where r is the number of points after t steps of the algorithm. Moreover, all descents in R° have length m.

The proof of the first part of lemma 6 can be find in [7]. The second part comes from de fact that in a word R°, each 1 represents a point that was uncolored and each 0 a point that was colored.

Let $\mathcal{R}^\circ_t = \{R^\circ | R \in \mathcal{R}_t\}$. The fact that in a word R° the number of 1's does not exceed the number of 0's (lemma 6) implies that $|\mathcal{R}^\bullet| \leq ((a \cdot b)^{1/m})^t |\mathcal{R}^\circ_t|$. Therefore, by lemma 5:

Lemma 7 $|\mathcal{F}_t| \leq (K + 1)^{|S|}((m!a \cdot b)^{1/m})^t |\mathcal{R}^\circ_t|$.

We now aim to count partial Dyck words having the properties described in lemma 5. To make the computation easier, we will in fact count Dyck words with these properties. The next lemma, proven in [7] shows that counting these two objects is almost equivalent, provided that r (the difference between the number of 0 s and 1 s in the partial Dyck word) is not too large.

Lemma 8 Let t and $r \leq t$ be integers, and let $E \neq \{1\}$ be a non-empty set of non-negative integers. Let $C_{t,r,E}$ (resp. $C_{t,E}$) be the number of partial Dyck words with t 0's, $t - r$ 1's (resp. Dyck words with length $2t$) and all descents having length in E. Then $C_{t,r,E} \leq C_{t+r(s-1),E}$, where $s = min(E \setminus \{1\})$.

As mentioned in [7], if $E = \{m\}$ then

$$C_{t,E} = \frac{1}{t+1}\binom{t+1}{\frac{t}{m}}.$$

Using Stirling's formula, we find its asymptotic value $ct^{3/2}C^t_m$, where c is a constant and $C_m = m(m-1)^{1/m-1}$.

We are now able to prove the main result of our research:

Theorem 8. Let P_n be a projective plane of order n. There is a legitimate coloring of P_n with $max(c(n, a, b), \lceil \frac{m}{m-1}(m!\delta(m-1))^{1/m} \rceil)$ colors, with m as defined above, $\delta = a \cdot b$ for a e b defined above and $c(n)$ the number of colors needed in order to exist a $f : P \setminus S \to [c(n)]$ with the properties previously mentioned.

Proof: To prove the theorem, we need to show that there is a vector $F \in [\frac{m}{m-1}(m!\delta(m-1))^{1/m}]^t$ such that the algorithm with P_n and F as entries, returns a legitimate coloring of P_n. By lemma 7, $|\mathcal{F}_t| \leq (K + 1)^{|S|}((m!a \cdot b)^{1/m})^t |\mathcal{R}^\circ_t|$. Note that, for each $R \in \mathcal{R}_t$, the number of zeros and ones in each prefix of R° differs by at most $|S| - 1$ since at most $|S| - 1$ points are colored in each step of the algorithm. Now, lemmas 6 and 8 implies that $|\mathcal{R}^\circ_t| \leq \sum_{r=0}^{|S|} C_{t+r,E} \leq c^{'} C^t_m t^{-\frac{3}{2}}$, where $c^{'}$ is a constant. Therefore $|\mathcal{F}_t| \leq c^{'}((m!a \cdot b)^{1/m})^t |C^t_m t^{-\frac{3}{2}}$, and $|\mathcal{F}_t| / (\frac{m}{m-1}(m!\delta(m-1))^{1/m})^t$ goes to as t goes to infinity. In particular, for t large enough, $|\mathcal{F}_t| < [\frac{m}{m-1}(m!\delta(m-1))^{1/m})]^t$, hence there is a vector F for which the algorithm halts in less than t steps and returns a legitimate coloring of P_n using at most $\lceil \frac{m}{m-1}(m!\delta(m-1))^{1/m} \rceil$ colors in S. Since we had used $c(n, a, b)$ colors in $P \setminus S$, the result follows.

References

[1] N. Alon e Z. Füredi: Legitimate colorings of projective planes, Graphs and Combinatorics 5 (1989), 95 - 106.

[2] V. Dujmović, G. Joret, J. Kozik, and D.R. Wood. Nonrepetitive Colouring via Entropy Compression. arXiv:1112.5524. 17

[3] D. Gonçalves, M. Montassier, and A. Pinlou. Entropy compression method applied to graph colorings. arXiv:1406.4380.

[4] Moser, R., Tardos, G.: A constructive proof of the general LovÃ¡sz Local Lemma. Journal of the ACM 572, pp. 11:1-11:15 (2010)

[5] Niranjan Balachandran, The Probabilistic Method in Combinatorics, Lectures by Niranjan Balachandran, Caltech

[6] T. Tao. Moser's entropy compression argument, What's New, 2009.

[7] Louis Esperet, Aline Parreau, Acyclic edge-coloring using entropy compression, European Journal of Combinatorics Volume 34, Issue 6, August 2013, Pages 1019-1027

[8] J. Grytczuk, J. Kozik, and P. Micek. New approach to nonrepetitive sequences. Random Structures & Algorithms, Volume 42, Issue 2, 2013. Pages 214-225.

[9] R. Bissacot, L. Doin. Legitimate Coloring of Finite Projective Planes via Entropy Compression. (preprint)