LOW AUTO-CORRELATION BINARY SEQUENCES EXPLORED USING SURVEY PROPAGATION

ABSTRACT. TODO

1. INTRODUCTION

The Low Auto-correlation Binary Sequence (LABS) problem consists in finding a binary sequence $S = \{S_1, S_2, ..., S_N\}$ where $S_i \in \{1, -1\}$ for $1 \leq i \leq N$ that minimizes the function

$$E(S) = \sum_{k=1}^{N-1} C_k(S)^2 \tag{1}$$

where $C_k(S)$ are the aperiodic auto-correlation coefficients:

$$C_k(S) = \sum_{i=1}^{N-k} S_i S_{i+k}, \text{ for } 1 \leq k \leq N-1. \tag{2}$$

Finding such optimal sequences is a notoriously hard problem, for increasing values of N[**?**].

To build these low auto-correlation binary sequences is of fundamental interest in many practical applications. In radars, for example, LABS are required for modulation in the process of pulse compression to enhance range resolution and long range detection capabilities [**?**]. Also for the measurement of space-time curvatures between high precision radars [**?**]. In Mathematics it is known as the Littlewood problem, that consists in finding the coefficients of a polynomial around the unit circle in the complex plane. In Statistical Physics, these are the ground states of the Bernasconi's model [**?**], that implies the energy minimization of an Ising spin system with long range interacting variables with four-fold antiferromagnetic interactions. Morover, it also appears in digital signaling processing [**?**], and in Artificial Inteligence [**?**].

The problem has been largely studied using exact and heuristic methods. Exhaustive search is currently the only available way to obtain exact LABS solutions. Golay published in [**?**] optimal solutions for values up to $N = 32$. Since then, due the computational complexity of the problem, all the new

Date: March 18, 2019.

optimal solutions have been obtained using Branch and Bound [?] methods with different parallel implementations, resulting in algorithms with cost of order $O(k^N)$ with $k < 2$.

For example, Mertens found the solution of the LABS problem up to $N \leq 48$ with a computational cost of $O(1.85^N)$ in 1996 [?]. Later in 2004 with an improved implementation Mertens and Bauke computed the solution up to $N \leq 60$ [?]. Wiggenbrock expanded this approach to $N \leq 64$ using a better bound and reported a cost of order $O(1.79^N)$ [?]. More recently in 2016, Packebusch and Mertens obtained exact solutions for two more values $N = 65$ and $N = 66$, employing the combined bounds of Prestwich and Wiggenbrock $O(1.729^N)$ [?]. Despite these sophisticated implementations and improvements it is clear that this approach is not viable in the search of optimal sequences with larger lengths, for example, $N > 100$.

A readable summary of the application of different heuristic and stochastic algorithms to LABS appears in [?] and [?]. More specifically, in [?] the authors used Evolutionary Search (ES) taking a special care on processes to generate the offsprings without a recombination strategy and with a mutation operator flipping more than one bit at once, the authors found solutions, for odd system sizes, as large as $N = 201$. In [?] the authors presents empirical evidence showing that evolutionary pure algorithms are not capable of facing the complexity of the problem, but also that evolutionary methods assisted by local-search operators (memetic algorithms) provide optimal or near-optimal results. In [?] the authors improved the Tabu Search Method previously developed in [?] getting better results than memetic algorithms and they explore the solution space for systems size between $[61 - 77]$ and report the best values that they obtain with TSv7 algorithm which has an expected run time of $\mathcal{O}(1.03\text{e}{-5} \cdot 1.34^N)$, according to these authors the improvement came from a deep study of the searched trajectories and a better diversification process. The state of the art of heuristic algorithms according to [?] seems to be the work [?] where the authors combined a random self-avoiding walk and Hasse graph. However, like with exact algorithms these complex and advanced heuristics fail in systems of relative high dimensions [?] leaving room for further improvements.

Here we first introduce Warning Propagation and compare it to Greedy Monte Carlo, to show that indeed, it is a better candidate to look for low energy configurations of the LABS problem. Then we try WP on the disordered versions of LABS in order to shed light on the relevance of the structure for the underlying graph of interactions on the space of available configurations of the problem.

2. Physically inspired algorithms

The minimization of the energy $E(S)$ (cost function) can be obtained by specific methods tailored for this very problem, as those that are the state of the art for LABS, or conversely by general standard techniques. While the former are currently more efficient the later are easier to interpret and may open the way to important new ideas in the treatment of the problem. The simplest of these algorithms is the greedy minimization of the cost function. A simple greedy approach corresponds in the statistical mechanics community to the Monte Carlo method at $T = 0$, where variables are iteratively altered only when the proposed changes reduce the energy. Typically greedy algorithms are simple to program and guaranteed to converge, but are prone to get stuck on non-optimal solutions.

On the other hand, since the beginning of the century, Message Passing algorithms have found their way in the realm of the statistical physics community. The turning point was the realization that message passing algorithms can be viewed as fixed point equations derived from variational approximations to the free energy of Ising-like models [**?**]. This inspired researchers to look for novel applications of these algorithms in the field of Combinatorial Optimization [**?**, **?**, **?**] and to explore new extensions [**?**, **?**, **?**].

3. Survey Propagation

$$u_{a\to i} = sgn(-h_j h_k h_l) min(|-1|, |h_j|, |h_k|, |h_l|) \tag{3}$$

$$P(h_i) = \int_u \prod_{a\in V(i)} Q(u_{a\to i}) \delta(h_i - \sum_{i=1}^{m} u_i) d(u_i) \tag{4}$$

$$\begin{aligned} Q(u_{a\to i}) = \int_{h_j}\int_{h_k}\int_{h_l} & P(h_j)P(h_k)P(h_l) \\ & \delta(u - sgn(-h_j h_k h_l) min(1, |h_j|, |h_k|, |h_l|)) dh_j dh_k dh_l \end{aligned} \tag{5}$$

Debido a que estamos lidiando con valores discretos de u y h es util asumir que:

$$Q(u_{a\to i}) = \eta_0 \delta(u_{a\to i}) + \eta_1 \delta(u_{a\to i} - 1) + \eta_{-1} \delta(u_{a\to i} + 1) \tag{6}$$

y por ende

$$\begin{aligned}(7)\quad P(h_i) = \rho_0\delta(h_i) + \rho_1\delta(h_i-1) + \rho_{-1}\delta(h_i+1) + ...\\ \rho_n\delta(h_i-n) + \rho_{-n}\delta(h_i+n)\end{aligned}$$

en este punto resulta necesario encontrar una relacion entre η y ρ. Empecemos por η_0, η_0 en principio significa la probabilidad de que $u_{a\to i}$ tome valor 0, para que esto ocurra es necesario que el producto del sgn sea 0 o que el min de los valores absolutos sea 0. Estas dos condiciones necesitan que una, dos o las tres h involucradas tomen valor cero y esto puede suceder de distintas combinaciones.

$$\begin{aligned}(8)\quad \eta_0^{a\to i} = \rho_0^j\rho_0^k\rho_0^l + \rho_0^j\rho_0^k[\sum_{\alpha\in[-n,n]/0}\rho_\alpha^l]+\\ \rho_0^j[\sum_{\alpha\in[-n,n]/0}\rho_\alpha^k]\rho_0^l + [\sum_{\alpha\in[-n,n]/0}\rho_\alpha^j]\rho_0^k\rho_0^l+\\ \rho_0^j[\sum_{\alpha\in[-n,n]/0}\rho_\alpha^k][\sum_{\beta\in[-n,n]/0}\rho_\beta^l]+\\ [\sum_{\alpha\in[-n,n]/0}\rho_\alpha^j]\rho_0^k[\sum_{\beta\in[-n,n]/0}\rho_\beta^l]+\\ [\sum_{\alpha\in[-n,n]/0}\rho_\alpha^j][\sum_{\beta\in[-n,n]/0}\rho_\beta^k]\rho_0^l\end{aligned}$$

apoyandonos en que

$$(9)\qquad \sum_{\alpha\in[-n,n]/0}\rho_\alpha^j = 1-\rho_0^j$$

razonando de forma similar para k, l y aplicando cierto trabajo algebraico es posible simplificar la expresion anterior hasta obtener:

$$\begin{aligned}(10)\quad \eta_0^{a\to i} = \rho_0^j\rho_0^k\rho_0^l - (\rho_0^j\rho_0^k + \rho_0^k\rho_0^l + \rho_0^j\rho_0^l)+\\ \rho_0^j + \rho_0^k + \rho_0^l\end{aligned}$$

para obtener η_1 es necesario notar que $sgn(-h_j h_k h_l) = 1$, si y solo si $h_j h_k h_l < 0$. Es decir los tres valores de h deben ser negativos o solo uno de estos puede serlo. Por ende:

$$\begin{aligned}\eta_1^{a\to i} = &\sum_{\alpha\in[-n,-1]} \rho_\alpha^j \sum_{\beta\in[-n,-1]} \rho_\beta^k \sum_{\gamma\in[-n,-1]} \rho_\gamma^k + \\ &\sum_{\alpha\in[-n,-1]} \rho_\alpha^j \sum_{\beta\in[1,n]} \rho_\beta^k \sum_{\gamma\in[1,n]} \rho_\gamma^k + \\ &\sum_{\alpha\in[1,n]} \rho_\alpha^j \sum_{\beta\in[-n,-1]} \rho_\beta^k \sum_{\gamma\in[1,n]} \rho_\gamma^k + \\ &\sum_{\alpha\in[1,n]} \rho_\alpha^j \sum_{\beta\in[1,n]} \rho_\beta^k \sum_{\gamma\in[-n,-1]} \rho_\gamma^k\end{aligned} \tag{11}$$

la expresion anterior luce complicada, pero sugiere que es posible expresarla como un funcion comulativa de los valores de ρ. Sea $C_{-1}^j = \sum_{\alpha\in[-n,-1]} \rho_\alpha^j$, sin tener en cuenta los valores individuales de ρ.

$$\begin{aligned}\eta_1^{a\to i} = &C_{-1}^j C_{-1}^k C_{-1}^l + C_{-1}^j C_1^k C_1^l + \\ &C_1^j C_{-1}^k C_1^l + C_1^j C_1^k C_{-1}^l\end{aligned} \tag{12}$$

y por ende:

$$\begin{aligned}\eta_{-1}^{a\to i} = &C_1^j C_1^k C_1^l + C_1^j C_{-1}^k C_{-1}^l + \\ &C_{-1}^j C_1^k C_{-1}^l + C_{-1}^j C_{-1}^k C_1^l\end{aligned} \tag{13}$$

Aplicando el mismo razonamiento anterior podemos derivar las ecuaciones para el modelo de 2-Spin antiferromagnetico.

$$\eta_0^{a\to i} = \rho_0^j \tag{14}$$

$$\eta_1^{a\to i} = \sum_{\alpha\in[-n,-1]} \rho_\alpha^j \tag{15}$$

$$\eta_{-1}^{a\to i} = \sum_{\alpha\in[1,n]} \rho_\alpha^j \tag{16}$$

Queda pendiente el problema de la obtencion de los valores de C_{-1}, dado que el computo de este valor depende de un número largo de términos $\sum_{\alpha\in[-n,-1]} \rho_\alpha^j$ que crece con la dimensión del problema es necesario la obtencion de un método para la computacion de este. Estudiaremos dos métodos a continuación.

4. Results

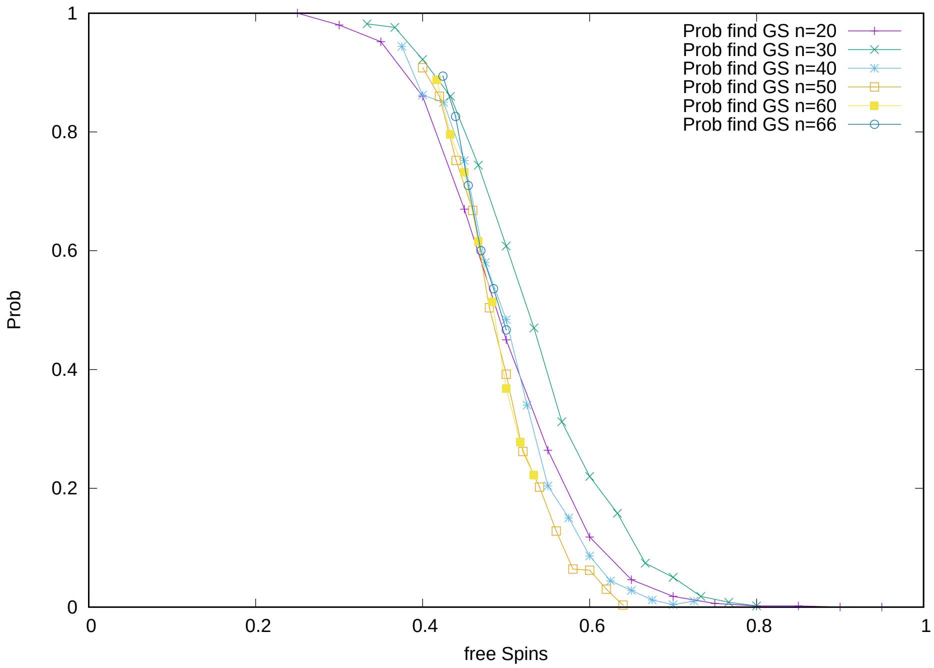

Figure 1. Probability of found the ground state given partial information. The Y axis is the probability, and X axis is the inverse of the information of the ground state. The Graphic show that, a transition occur around the middle of partial information.

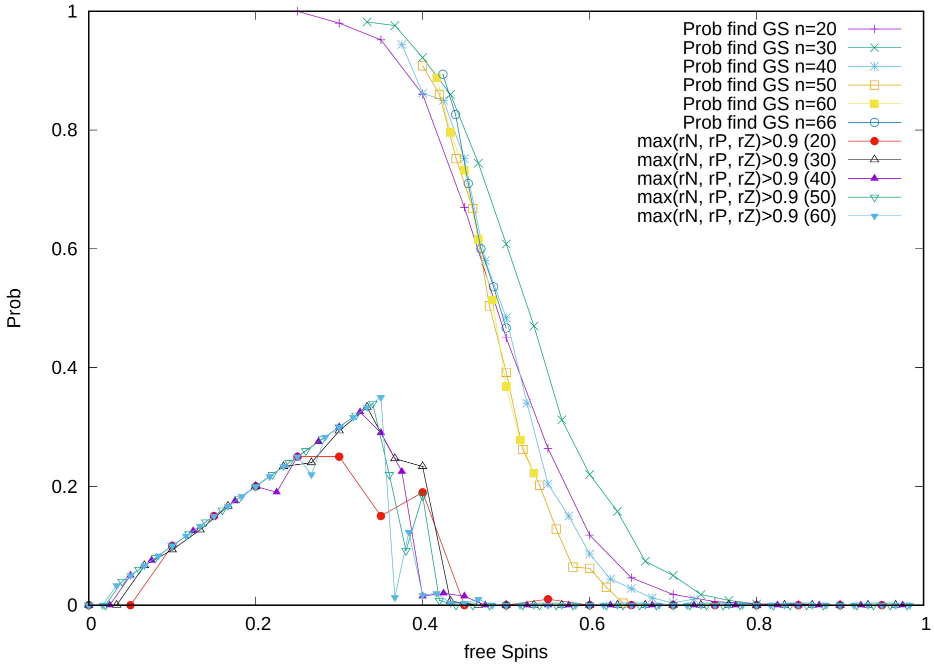

FIGURE 2. Amount of decimate variable with bias values greater than 0.9 . The Y axis a normalization for the lowers curves of system sizes where the bias has a value greater than .9. The graphic show that the amount of spin with no initial set of value, increasing in the same region where the probability of founding the GS decreasing is 1, and when the amount of this spins decreasing the probability decrease at the same rate.

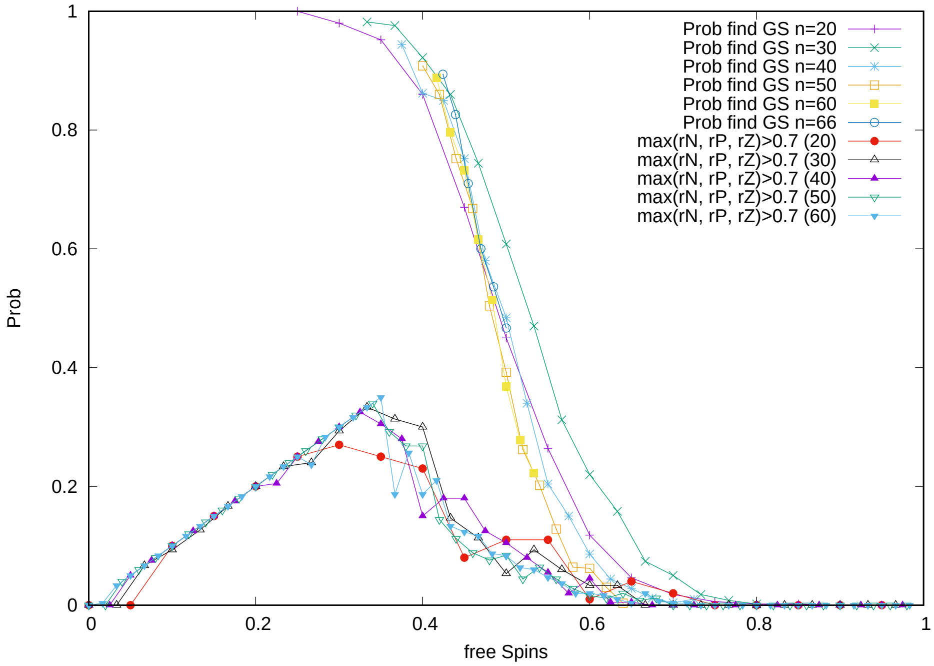

Figure 3. Equal to the second graph, but with the .7 threshold.

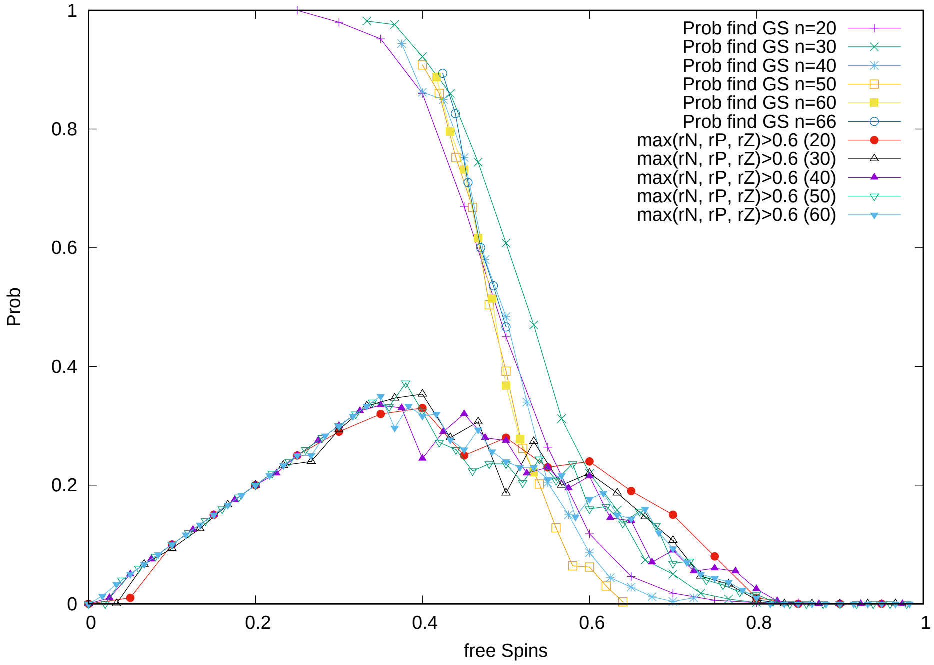

Figure 4. Equal to the second graph, but with the .6 threshold.

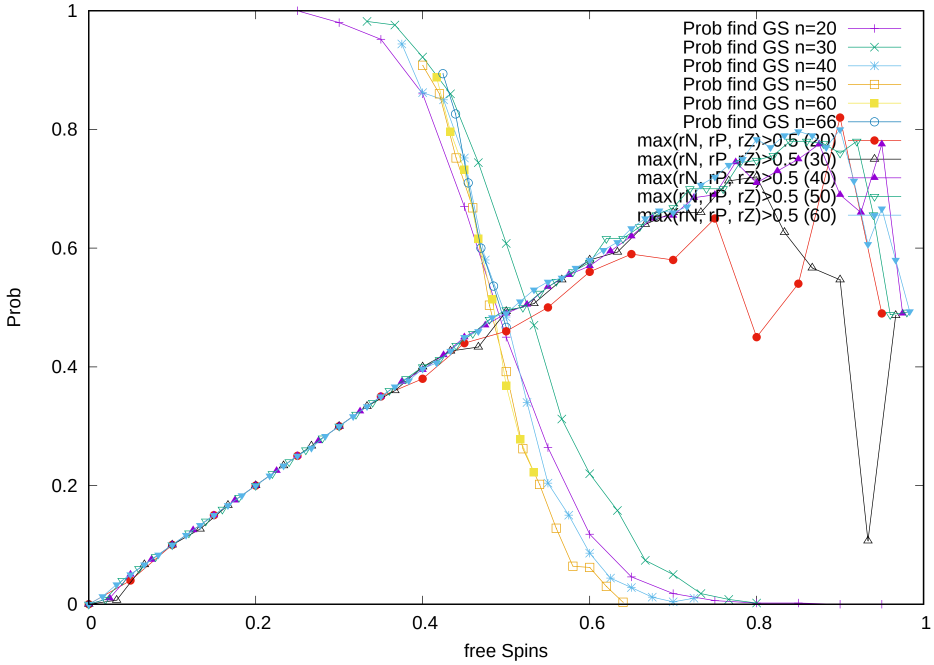

Figure 5. Equal to the second graph, but with the .5 threshold.

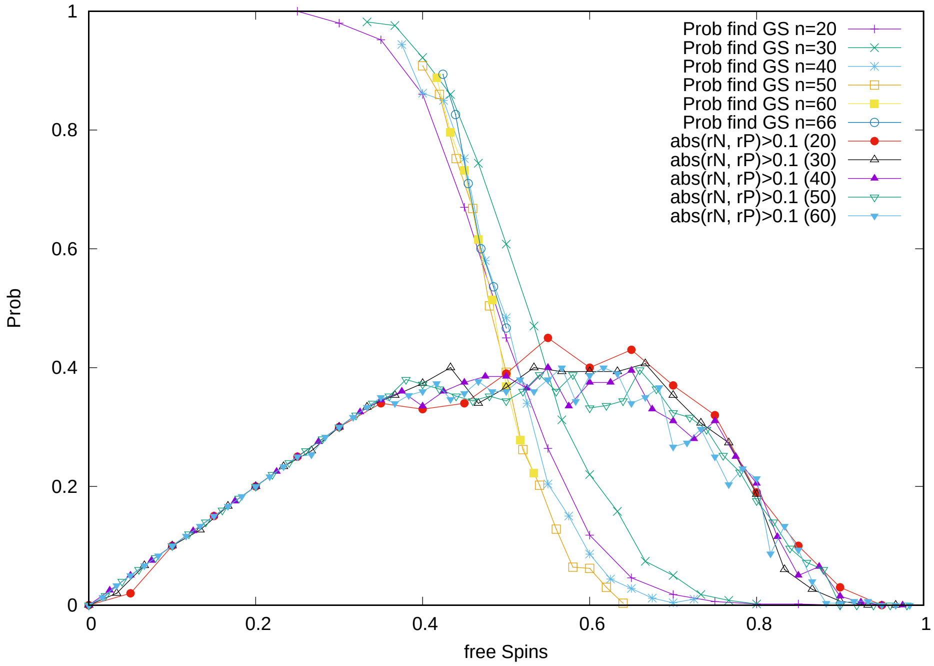

FIGURE 6. Equal to the second graph, but when the difference between Rho Positive and Rho Negative is bigger than .1