On random satisfiability and optimization problems

Joel Larsson
The cover illustrates a key piece of the proof of Theorem 9 in paper III: how the satisfiability of a 3-SAT formula can be affected by changing the signs with which a single variable occurs. The white squares correspond to 3-clauses, the large circles corresponds to variables, and the $d$-hypercube within each circle corresponds to the $2^d$ ways a variable $x$ can be assigned signs ($x$ or $\neg x$) in its $d$ occurrences.

The colours of the hypercubes describe the satisfiability of the entire formula: Green (blue) for when the formula can be satisfied if and only if the variable is set to true (false), and white if its satisfiability does not depend on the value of $x$. 
ACKNOWLEDGEMENTS

This thesis would not have been possible were it not for the help and encouragement from advisors and colleagues, and the love and support from friends and family.

To my advisor Klas Markström, thank you for your patience and for always having time for discussions, mathematical and otherwise. To my co-advisors Victor Falgas-Ravry and Roland Häggkvist, thank you for reminding me to see the bigger picture, and be deliberate in my choice of research problems. To my academic sibling and office mate Lan Anh Pham, thank you for being good company and a friend.

I would also like to thank Jakub Sliacan for his help with proof-reading, my mentor Anneli Dyrvold for her good advice, and Anna Ivarsson and the administrators for answering countless questions.

To Ester, Rebecka, Sofie, Linn, Petter, Monica, Linnea, Kristian, Linnéa, Willeke, and many others, thank you for providing some much needed distractions from mathematics. Anyone would be lucky to have such great friends.

To my family – my parents Kjell & Berit, my sister Mimmi, and my brother-in-law Carl-Johan – thank you for your unwavering support throughout the years.

Finally, I would like to express my gratitude to Lina for being in my life.
This thesis consists of the following papers.

I J. Larsson, *The Minimum Matching in Pseudo-dimension* $0 < q < 1$, to appear in *Combinatorics, Probability and Computing*

II V. Falgas-Ravry, J. Larsson, K. Markström, *Speed and concentration of the covering time for structured coupon collectors*, submitted for publication

III J. Larsson, K. Markström, *Biased random $k$-SAT*, preprint

IV J. Larsson, K. Markström, *Polarized random $k$-SAT*, preprint

In Paper I, we study the following optimization problem: in the complete bipartite graph where edges are given i.i.d. weights of *pseudo-dimension* $q > 0$, find a perfect matching with minimal total weight. The generalized Mézard-Parisi conjecture states that the limit of this minimum exists and is given by the solution to a certain functional equation. This conjecture has been confirmed for $q = 1$ [1] and for $q > 1$ [27]. We prove it for the last remaining case $0 < q < 1$.

In Paper II, we study generalizations of the coupon collector problem. Versions of this problem shows up naturally in various context and has been studied since the 18th century. Our focus is on using existing methods in greater generality in a unified way, so that others can avoid ad-hoc solutions.

Papers III & IV concerns the satisfiability of random Boolean formulas. The classic model is to pick a $k$-CNF with $m$ clauses on $n$ variables uniformly at random from all such formulas. As the ratio $m/n$ increases, the formulas undergo a sharp transition from satisfiable (w.h.p.) to unsatisfiable (w.h.p.). The critical ratio for which this occurs is called the satisfiability *threshold*.

We study two variations where the signs of variables in clauses are not chosen uniformly. In paper III, variables are biased towards occurring pure rather than negated. In paper IV, there are two types of clauses, with variables in them biased in opposite directions. We relate the thresholds of these models to the threshold of the classical model.
SAMMANFATTNING

Denna doktorsavhandling består av följande artiklar.

I J. Larsson, *The Minimum Matching in Pseudo-dimension*  
$0 < q < 1$

II V. Falgas-Ravry, J. Larsson, K. Markström, *Speed and concentration of the covering time for structured coupon collectors*

III J. Larsson, K. Markström, *Biased random k-SAT*

IV J. Larsson, K. Markström, *Polarized random k-SAT*

I artikel I studerar vi följande problem: i den kompletta bipartita grafen med $n + n$ hörn där kanterna ges oberoende och likafördelade vikter enligt pseudo-dimension $q > 0$, hitta en perfekt matchning med minimal total vikt. Enligt den generaliserade Mézard-Parisi-förmodan existerar gränsvärdet av detta minimum och ges av lösningen till en viss funktionalekvation. Detta har bekräftats för $q = 1$ [1] och för $q > 1$ [27]. Vi visar att förmodan även är sann i det sista kvarvarande fallet, $0 < q < 1$.


Artiklar III och IV handlar om lösbarnheten av slumpmässiga Booliska formler. Den klassiska modellen är att dra formler av typen $k$-CNF med $m$ klausuler och $n$ variables enligt det uniforma sannolikhetsmåttet. När kvoten $\alpha := m/n$ ökar genomgår dessa formler en skarp övergång från att vara lösbara med hög sannolikhet till olösbara med hög sannolikhet. Det kritiska $\alpha$ kallas för löslighetströskeln.

Vi studerar två varianter av denna modell. I artikel III har är alla klausuler *skeva*: variabler har högre sannolikhet att finnas med rena än negerade. I artikel IV finns det två typer av klausuler, skeva i varsir riktning. Vi finner samband mellan trösklarna för dessa modeller och tröskeln för den klassiska modellen.
Minimum Perfect Matchings

Background

Graphs

A graph \( G = G(V, E) \) is defined by a vertex set \( V \) and an edge set \( E \), where each \( e \in E \) is a 2-subset of \( V \), i.e. \( e = \{u, v\} \) for some \( u, v \in V \). We think of the edges as connections or bridges between vertices, and often abbreviate \( \{u, v\} \) to \( uv \). We say that \( G' \) is a subgraph of the graph \( G = (V, E) \) if \( G' = (V', E') \) is a graph, \( V' \subseteq V \), and \( E' \subseteq E \). The complete bipartite graph \( K_{n,m} \) is the graph consisting of a vertex set \( U \cup V \), where \( U \) and \( V \) are disjoint sets of cardinality \( n \) and \( m \) respectively, and the edge set \( E := U \times V \).

A subset \( M \subseteq E \) is called a matching if there are no distinct edges \( e, e' \in M \) such that \( e \) and \( e' \) share a vertex (i.e. there is a \( v \in V \) such that \( e \cap e' = \{v\} \)). A matching \( M \) is called perfect if every vertex belongs to some edge in \( M \). An equivalent definition is that \( M \) is a perfect matching if and only if \( |M| = \frac{1}{2}|V| \).

A weighted graph is a graph \( G \) together with a function from the set of edges to the positive real numbers, assigning each edge a weight. The weight of any subgraph of \( G \) is the sum of all the weights of the edges in the subgraph.

The Minimum Perfect Matching Problem

Given any weighted graph \( G \), we can ask (i) whether it has a perfect matching, and if it does, (ii) what the minimum weight of a perfect matching is. We will be especially interested in this problem on the complete bipartite graph \( K_{n,n} \). Here, the answer to (i) is trivially yes; but since there are \( n! \) perfect matchings it might be computationally expensive to answer (ii).

With the development of linear programming in the ’30s and ’40s, in particular the simplex method, it became possible to answer (ii). But while the simplex method is often efficient in practice, its worst-case performance is exponential. The first guaranteed polynomial-time algorithm for finding this minimum was given by Kuhn [16] in ’55. He dubbed it the Hungarian Method, since his work was based on earlier work by Hungarian mathematicians Egerváry and König, predating the theory of linear programming. While still a primal-dual algorithm, it exploits some of the structure specific to matchings to achieve \( O(n^3) \) time complexity.
In an effort to understand the *typical* behavior of this problem, random instances have been studied. In ’69, Donath [6] assigned edges weights uniformly at random from [0, 1], and used the Hungarian Method to find the answer to (ii). More formally, let \((c_{ij})_{i,j=1}^n\) be an \(n \times n\) random matrix with independent entries chosen uniformly at random from \([0, 1]\) and define \(M_n\) by

\[
M_n = \min_{\pi \in S_n} \sum_{i=1}^{n} c_{i\pi(i)},
\]

where the minimum is taken over the set of all \(n\)-permutations. This is often called the *random assignment problem* or the *minimum matching problem*\(^{[7]}\). Donath’s numerical evidence suggested that \(M_n \approx 1.6\) for large \(n\). Ten years later, Walkup [26] proved that \(1 \leq E M_n \leq 3\).

Around the same time, physicists noticed similarities between random combinatorial optimization problems and certain models in statistical physics. This connection enabled them to employ a new set of tools, most notably the replica symmetry heuristic and the cavity method.

While it has proven very challenging to make these methods rigorous, they have been rich sources of interesting conjectures. M´ezard and Parisi [21] applied replica symmetry heuristics to the random assignment problem, which led to the beautiful prediction that the limit (in probability) of \(M_n\) is \(\zeta(2) = \pi^2/6 \approx 1.64\). This became known as the M´ezard-Parisi conjecture and remained open for nearly two decades until it was confirmed by Aldous [1] in ’00.

A natural variation on the M´ezard-Parisi conjecture is to change the edge weight distribution. It turns out that only the behavior of the distribution for edge weights near 0 matters and distributions can thus be classified by the behavior of their cumulative distribution functions (cdf) near 0. If a cdf \(F\) scales like \(F(z) \sim z^q\) near 0 for some \(q > 0\), \(F\) is said to be of *pseudo-dimension*\(^{[2]}q\). This generalized conjecture was confirmed for \(q > 1\) in ’11 (W¨astlund [27]).

\(^{[1]}\)While the latter has become the standard term in recent years, it can cause confusion. The *maximum matching* problem is well-known, and concerns finding a matching with the maximum number of edges, so the term minimum matching suggests we are looking for a matching with the minimum number of edges – i.e. the empty set. Since what we are looking for is a perfect matching of minimal weight, the author prefers the term *minimum perfect matching*.

\(^{[2]}\)The motivation behind this terminology is that the cdf of the distance between two points, chosen uniformly at random from the \(d\)-dimensional hypercube \([0,1]^d\), scales like \(z^d\).
Let $M_{n,q}$ be the minimum weight of a perfect matching on $K_{n,n}$ equipped with i.i.d. edge weights between 0 and 1, with cdf $z^q$. In this paper we prove the Mézard-Parisi conjecture in the last remaining applicable case: $0 < q < 1$. More precisely, we prove that $n^{1-1/q}M_{n,q}$ converges in probability to some positive constant $\beta(q)$ as $n \to \infty$. Our proof uses a game theory approach, based on the work in [27], but introducing some functional analysis to estimate the size of a certain tree.

By thinning the graph and taking the Benjamini-Schramm limit, we can work with an infinite tree instead of $K_{n,n}$. On this tree we play the game Exploration. It consists of two players taking turns choosing the next edge of a self-avoiding walk according to some rules. It can be shown that the limit of $n^{1-1/q}M_{n,q}$ exists if the game will (almost surely) end after a finite number of moves.

In the proof of the conjecture for $q > 1$ in [27], the argument involves estimating the size of the tree of so-called reasonable moves, which are certain near-optimal moves. This random tree contains the game path, and they show that its expected branching number will eventually fall below 1. Hence the game will end after a finite time, almost surely. This argument fails for $q < 1$, however, because the branching number may not decrease uniformly.

We solve this by (i) pruning the tree a little, and (ii) bounding its size recursively.

(i) Instead of the tree of all near-optimal moves, we work with the (strictly smaller) tree which is the union of all near-optimal paths starting at an arbitrary vertex $v$.

(ii) Consider the expected size of such a tree, conditioned on the game theoretical valuation of the position $v$ being equal to $z$. This turns out to be a continuous function of $z$, and we get one such function $R_k$ for each turn $k$ of the game. We show that there exists a linear operator $L$ such that $LR_{k-1} = R_k$, and that $L \circ L$ is a contraction.

This enables us to show that a tree guaranteed to include the actual game path is finite (a.s.), which implies that the limit exists.
STRUCTURED COUPON COLLECTORS

BACKGROUND

The classical coupon collector problem is as follows: At integer times, a coupon collector draws elements (‘coupons’) uniformly at random from \{1, 2 \ldots n\} with replacement. How many coupons will she need to draw before she has seen each element at least once? This problem has a rich history, and can be traced back to de Moivre [20] in the 18th century.

The classical problem has been generalized in various ways, such as the coupons occurring with different probabilities [13, 23], coupons being drawn in sets of \(k\) [11, 25, 8, 19, 2, 15, 18], or that the coupon collector has \(m\) younger siblings that she gives her leftover coupons to [22, 9]. There is a certain amount of overlap here, as some authors have dealt with models generalized in several ways simultaneously.

The probability of a complete collection has a sharp threshold at time \(n \log n\), and a classical result by Erdős & Rényi [9] gives the precise shape of the threshold.

**Theorem 1 (Erdős–Rényi):** Let \(V = [n]\), and let \(X_i\) be a random coupon obtained by selecting a singleton from \(V\) uniformly at random. Denote by \(T^m\) the least \(t\) such that every point of \(V\) has been covered by at least \(m\) of the coupons \(X_1, \ldots, X_t\). Then for every \(x \in \mathbb{R}\),

\[
\lim_{n \to \infty} \mathbb{P}(T^m < n \log n + (m - 1)n \log \log n + xn) = e^{-e^{-x}}.
\]

In particular, \(T^m\) is sharply concentrated around \(n \log n + (m-1)n \log \log n\).

We will focus on a wider generalization where the coupon collector draws a random subset \(X_i \subseteq V\) at each integer time, and different subsets occur with different probabilities. The coupon collector have finished when \(\bigcup X_i = V\). We call these structured coupon collector problems. An easy example of this would be if each 2-set is drawn with equal probability, and sets of other sizes are never drawn. This is equivalent to the Erdős-Rényi random graph model, and having collected all elements corresponds to having minimum degree 1 in the graph. Another interesting (but far harder) example of a structured coupon collector is the random \(k\)-SAT problem, which we will discuss in the next section.
Variations on the structured coupon collector show up in numerous contexts. The aim of this paper is to apply standard methods in greater generality, so that mathematicians encountering a coupon collector problem can use ready-made theorems, instead of solving the problem with ad hoc methods. In this way, we hope this paper will be very useful.

A large number of theorems are given, dealing with a variety of cases. Let \( F \) be the family of subsets of \( V \) that are picked with positive probability. The main message of the paper is that typically, the larger the sets in \( F \), the more structure or symmetry of \( F \) is needed in order to have a sharp concentration of the covering time. In one extreme, if no structure of \( F \) is known, we can only guarantee concentration if the sets have maximal size \( n^{o(1)} \), whereas on the other extreme, if \( F \) is invariant under any permutation of \( V \), maximal set size \( o(n) \) works. If we have some intermediate structure, we typically get concentration for coupon collector problems with maximum coupon size up to some \( K \) between those two extremes.

One property that guarantees concentration is negative association between elements of \( V \). For instance, the coupon collector problem in which one tries to cover the edges of a complete graph by drawing random spanning trees has sharp concentration of the covering time.

**Random \( k \)-SAT**

**Background**

Let \( x_1, \ldots, x_n \) be \( n \) Boolean variables. We say that \( z \) is literal on \( x_i \) if \( z := x_i \) or \( z := \neg x_i \). A \( k \)-clause is a logical formula of the form \( z_1 \lor \ldots \lor z_k \), where each \( z_j \) is a literal on some \( x_i \). (We usually require the \( z_j \)'s to be literal on distinct variables.) A \( k \)-CNF is a Boolean formula of the form \( C_1 \land C_2 \land \ldots \land C_m \), where each \( C_j \) is a \( k \)-clause.

Given a \( k \)-CNF \( \Phi = \Phi(x_1, \ldots, x_n) \), the satisfiability problem is to assign each \( x_i \) a value of TRUE or FALSE, such that \( \Phi \) evaluates to TRUE. This is NP-complete for \( k \geq 3 \), and in fact often serves as the prototypical example of an NP-complete problem. In an effort to understand average-case complexity rather than worst-case complexity, random in-
stances of $k$-SAT have been studied. The classic model is to let $\varphi_k(m,n)$ be a $k$-CNF in which $m$ clauses are picked uniformly at random from the set of $2^k \binom{n}{2}$ possible $k$-clauses on $n$ variables.

Working on the case $k = 2$, Chvátal & Reed [3] proved in ’92 that a random 2-SAT formula with $\alpha n$ clauses on $n$ variables is satisfiable w.h.p. whenever $\alpha < 1$, and unsatisfiable w.h.p. whenever $\alpha > 1$. They conjectured that random $k$-SAT should exhibit similar threshold behavior for any $k \geq 3$.

**Conjecture 2 (The Satisfiability Conjecture):** There exist limiting densities $\alpha_k$ such that for any $\varepsilon > 0$, 

$$
\mathbb{P}(\varphi_k(m,n) \text{ is satisfiable}) = \begin{cases} 
1 - o(1), & m < (\alpha_k - \varepsilon)n \\
o(1), & m > (\alpha_k + \varepsilon)n.
\end{cases}
$$

There are two aspects to this conjecture. First, the transition from satisfiable w.h.p. to unsatisfiable w.h.p. should be sharp. Second, there should be some critical density, not depending on $n$, where the transition occurs.

The first part was proven in ’99 by Friedgut [10], i.e. that the conjecture holds if we replace the constants $\alpha_k$ with some functions $\alpha_k(n)$. Coja-Oghlan [4] showed that these functions are constrained to a small interval for large $k$: there exists a sequence $\varepsilon_k = o_k(1)$ such that $|\alpha_k(n) - 2^k \log 2 + \frac{1+\log 2}{2}| \leq \varepsilon_k$ for all sufficiently large $n$.

The conjecture was confirmed for all $k \geq k_0$ in ’14 by Ding, Sly & Sun [5], for some absolute $k_0$. Their proof employs the replica symmetry method (more specifically, one-step replica symmetry breaking), a method which has also been used to give non-rigorous predictions and some rigorous upper bounds of the threshold values. For instance, it gives the prediction of $\alpha_3 \approx 4.26675$, while recent empirical studies [17] suggest $\alpha_3 < 4.262$.

While the exact value (or indeed, the existence) of $\alpha_3$ is not known, a series of upper and lower bounds have been proven rigorously. The best known upper bound [7] is 4.506, while the best known lower bound [12, 14] is 3.52. For comparison, a standard application of the first moment method gives an upper bound of $-1 / \log_2(1 - 2^{-k}) = 2^k \log 2 + o_k(1)$, which is approximately 5.19 for $k = 3$. Meanwhile, an equally straightforward application of the second moment method fails to give a lower bound within a constant factor of the conjectured threshold unless $k = \Omega(\log n)$. 

vi
Paper III: Biased random $k$-SAT

We work with a variation on the random $k$-SAT problem that has received far less attention: the biased random $k$-SAT problem. It was introduced in [24], aiming to interpolate between easy and hard instances. In this model there is a bias parameter $0 \leq b < \frac{1}{2}$, and variables in clauses occur (independently) pure with probability $\frac{1}{2} + b$, and negated with probability $\frac{1}{2} - b$. Setting $b$ to 0 recovers the classic random $k$-SAT model.

We gain some understanding of how the threshold depends on the parameter $b$. For $b$ near $\frac{1}{2}$, we prove that the threshold scales like $|b - \frac{1}{2}|^{1-k}$, confirming what the heuristics in [24] suggested. For $b$ near 0, we prove that it scales like $\alpha_k + \Theta(b^2)$ (where the implied constant is positive).

Paper IV: Polarized random $k$-SAT

In paper IV, we introduce a new random $k$-SAT model closely related to the biased model in paper III. While all clauses in biased $k$-SAT were biased toward having pure variables, in polarized random $k$-SAT we flip a fair coin for every clause to determine the direction of the bias. More precisely, we have a polarization parameter $p$ and for each clause where the coin came up head we have variables occur pure w.p. $p$ and negated with probability $1 - p$, while for the clauses where the coin came up tails these probabilities are interchanged.

In contrast to the biased model, the threshold does not grow unbounded when $p$ approaches 0, but stays beneath $2^k \log 2$. We prove that the threshold is non-decreasing as $p$ decreases. Hence any upper bound on the threshold for polarized $k$-SAT is automatically an upper bound on $\alpha_k$. We also conjecture that the threshold is identical for any polarization $p$.

The model becomes simpler when $p = 0$, where there are only two types of clauses, each occurring with probability $\frac{1}{2}$: clauses where all variables are pure, and clauses where all variables are negated. Given that some of the difficulties encountered while proving upper bounds on the threshold for classical random $k$-SAT is due to formulas becoming unbalanced in various ways, analyzing the fully polarized model might be more tractable.

\[3\] A much earlier version of paper III was included in the author’s Licentiate thesis. Each section of the current paper is either new or improved. For instance, in the earlier version we proved that the satisfiability threshold was increasing with $b$, while in the current version we find the scaling behavior as $b \to 0$ or $\frac{1}{2}$. 

vii
References


