Kramers-Wannier Duality of Statistical Mechanics Applied to the Boolean Satisfiability Problem of Computer Science

Joe Mitchell,1 Benjamin Hsu,2 and Victor Galitski1

1Joint Quantum Institute and Condensed Matter Theory Center, Department of Physics, University of Maryland, College Park, Maryland 20742-4111, USA
2Department of Physics, Princeton University, Princeton, NJ 08544

(Dated: October 10, 2013)

We present a novel application of the Kramers-Wannier duality on one of the most important problems of computer science, the Boolean satisfiability problem (SAT). More specifically, we focus on sharp-SAT or equivalently #SAT – the problem of counting the number of solutions to a Boolean satisfaction formula. #SAT can be cast into a statistical-mechanical language, where it reduces to calculating the partition function of an Ising spin Hamiltonian with multi-spin interactions. We show that Kramers-Wannier duality can be generalized to apply to such multi-connected spin networks. We present an exact dual partner to #SAT and explicitly verify their equivalence with a few simple examples. It is shown that the NP-completeness of the original problem maps on the complexity of the dual problem of enumerating the number of non-negative solutions to a Diophantine system of equations. We discuss the implications of this duality and the prospects of similar dualities applied to computer science problems.

PACS numbers: 89.70.Eg, 12.40.Nn, 05.50.+q

Computationally intractable problems are ubiquitous and occur in many areas of the natural and computational sciences, with problems as diverse as spin glasses, optimization problems, and cryptography [1-4]. Generally speaking, they are problems whose solutions require a time that grows exponentially in the input size \( N \) of the problem. Understanding what sorts of problems have solutions that require exponential or polynomial time is an important issue that has many practical implications [5].

However, proving that a problem is indeed computationally intractable is by itself a difficult task. One tool utilized by theoretical computer scientists is mapping between problems with a known computational complexity. By mapping one problem into another, one can show their relative difficulty. In this work, we use for the first time the well-established statistical mechanics technique of Kramers-Wannier duality to analyze the famous Boolean satisfiability problem. We discover an a new and exact dual formulation of the counting problem #SAT, which maps it on an under-constrained system of Diophantine equations.

Kramers and Wannier’s work in 1941 [6] exactly related the partition function of the 2D square lattice Ising model to itself, deriving the exact transition temperature of the model. The method consists of introducing new link variables, summing out the original variables, and defining the link variables in terms of plaquette variables in order to satisfy constraints introduced by the summations. In this way, the plaquettes of the original lattice become the vertices of the dual lattice. The graphical dual of the square lattice is itself, so the square lattice Ising model is self-dual. With this relation, the knowledge that a phase transition must happen in the dual model when it happens in the regular model, and the assumption that there is only one phase transition in the square lattice Ising model, the transition temperature is easily derived. This value was later confirmed by Onsager’s exact solution for the model [7].

Since then, dualities of this sort have been generalized to a broad range of models [8,9]. Furthermore, the recently invented bond algebraic dualities [10-13] have not only grouped many of these classical and quantum dualities under a general framework, but also present methods to discover new dualities. The duality we use in this work is essentially the classic Kramers-Wannier duality for an Ising model in an external field. This additional field changes the constraints introduced so that the variables and interactions switch under duality, rather than the variables switching with the plaquettes. This is a lattice-independent transformation and allows us to apply duality not only for models with multi-spin interactions, but also for networks of spins, with no lattice structure required.

We will focus our attention on the Boolean satisfiability problem in computer science, known as SAT. Let \( \{ x_i \} \) be a set of \( N \) Boolean variables. Define a “clause” as the logical OR (\( \lor \)) of some combination of these variables, possibly with negation, e.g. \( (x_1 \lor \bar{x}_2 \lor x_5) \). A SAT problem asks whether some set of \( M \) clauses of the \( N \) Boolean variables may be simultaneously satisfied by some assignment of the variables. SAT problems that have the same number \( k \) of variables in each clause are known as \( k \)-SAT problems.

This problem is extremely important in computational complexity theory and computer science in general. It is in the non-deterministic polynomial time computational complexity class (NP), meaning it is verifiable, but not necessarily solvable, in polynomial time. It is in fact an
NP-complete problem, meaning that in addition to being in NP itself, it is also as difficult as all other problems in NP \cite{14,15}. A polynomial time solution for this problem would imply a polynomial time solution for all NP problems, answering the famous question P=NP. The SAT problem is actually the first proven example of an NP-complete problem, and many other NP-complete problems were proven so by reducing them to the SAT problem.

It is straightforward to examine the SAT problem from a statistical mechanics standpoint. Consider that the Boolean variables are equivalent to Ising variables and that the clauses can be expressed as Hamiltonian contributions that are zero if satisfied and positive otherwise, represented as a combination of multispin interactions. Many methods used to study sets of random SAT problems are also used to study disordered Ising models, including the replica method, belief propagation, and survey propagation \cite{5,10,17}.

Random $k$-SAT problems with a large number of variables and clauses have a variety of interesting behavior and have been a topic of study in statistical mechanics for some time. It was found for instance that in random 3-SAT problems there is a phase transition at the critical ratio $\alpha_c = M/N \approx 4.25$. The majority of 3-SAT instances are satisfiable below $\alpha_c$, and unsatisfiable above $\alpha_c$. Moreover, the time to find a solution is polynomial in $N$ below the transition and exponential above \cite{5,17}. At the threshold, there is an exponentially sharp peak in the median running time for the best known 3-SAT solvers to decide if there is a solution or not. From a statistical physics point of view, this exponential slow down corresponds to a spin glass transition in an equivalent disordered Ising model \cite{18,19}. One of the primary motivations for studying duality in $k$-SAT is because of the close connection between phase transitions and duality. We hope that the duality derived here and similar dualities for other computer science problems may help study the phases and phase transitions in these problems, particularly in establishing exact relations between the phases of seemingly unrelated problems.

To be specific, in this article we are concerned with calculating the number of assignments of the Boolean variables that make the set of clauses true. This problem is known as sharp-SAT, or $\#SAT$. While the “counting problem”, $\#SAT$, is closely related to the “decision problem”, SAT, they are distinct. SAT is in the class of NP-complete problems; it is in NP and is as difficult as any other problem in NP. $\#SAT$ is in the $\#P$-complete problems, where $\#P$ roughly is the class of counting problems associated with decision problems that are in NP. Because Kramers-Wannier duality is a relation between the partition functions of two problems and not, for example, between low energy states, we will be able to more easily investigate counting problems than decision problems.

A SAT instance can be mapped into a spin glass model. Define the Ising spin variable as $\sigma_s = (-1)^{x_s}$ where $x_s = 0, 1$ is the Boolean variable in a given clause, and define $c_{s,\mu}$ to be $-1$ if $x_s$ is involved in clause $\mu$ with a negation, $1$ if it is involved without a negation, and $0$ if it is not involved in the clause. One can define an energy cost for a violated clause as proportional to a number $X_{\mu} > 0$ with the Hamiltonian

$$\mathcal{H} = \sum_\mu X_{\mu} \left[ \prod_s (1 - c_{s,\mu} \sigma_s) \right].$$  \hspace{1cm} (1)

It is easy to see that $\mathcal{H} \geq 0$. The decision problem is equivalent to determining if this Hamiltonian has any ground states with zero energy. The counting problem is equivalent to calculating how many states have zero energy. This can be compactly described by calculating the associated partition function, $Z = \sum_{\{\sigma_s\}} e^{-\mathcal{H}}$, in the limit as each $X_{\mu} \to \infty$.

This Hamiltonian can be rearranged to suggest its nature as an Ising spin glass:

$$\mathcal{H} = \mathcal{H}_0 - \sum_s H_s \sigma_s - \sum_\mu T_l \prod_{s \in \partial l} \sigma_s.$$  \hspace{1cm} (2)

$$\mathcal{H}_0 = \sum_\mu X_{\mu}, \quad H_s = \sum_\mu X_{\mu} c_{s,\mu}. \quad T_l = -\sum_\mu X_{\mu} \prod_{s \in \partial l} (-c_{s,\mu}).$$  \hspace{1cm} (3)

Note that each of $\mathcal{H}_0$, $H_s$, and $T_l$ are linearly proportional to the large constants $X_{\mu}$. This is the model of a network of Ising spins with multispin interactions and a site-dependent magnetic field. E.g. in the case of 3-SAT, there are two- and three-body interactions. In this article, $s$ will signify the “sites” or locations of the variables $\sigma_s$, and $l$ will signify the “links” or locations of the multi-spin interactions $\prod_{s \in \partial l} \sigma_s$. $\partial l$ refers to the sites of spins involved in the interaction at $l$, and $\partial s$ refers to the links for interactions in which the spin $\sigma_s$ is involved.

![Diagram](image-url)

FIG. 1. A SAT instance, $F = (x_1 \lor x_2 \lor x_3) \land (x_3 \lor x_4 \lor x_5)$. Each circle represents a site, the location of a spin associated with a Boolean variable. Each square represents a link, the location of an interaction (constraint) between spins. In the dual picture, the spins are exchanged with interactions.
For any model of this type, there is a relatively simple Kramers-Wannier like duality [8, 20].

\[ Z = e^{-\mathcal{H}_0} \sum_{\{\sigma_s = \pm 1\}} e^{\sum_{s} H_s \sigma_s + \sum_{t} T_t \prod_{s \in t} \sigma_s} = Z_0 \tilde{Z}, \]  
\[ Z_0 = e^{-\mathcal{H}_0} \left( \prod_s 2 \sinh 2H_s \right)^{\frac{1}{2}} \left( \prod_l \frac{1}{2} \sinh 2T_l \right)^{\frac{1}{2}} \]  
\[ \tilde{Z} = \sum_{\{\nu_l = \pm 1\}} e^{\sum_{l} T_l \nu_l + \sum_{s} H_s \prod_{s \in \partial_l} \nu_l}, \]

\[ \tilde{H}_s = -\frac{1}{2} \ln \tanh H_s, \quad \tilde{T}_l = -\frac{1}{2} \ln \tanh T_l. \]  

In short, dual spins are introduced at the links of the original network and the original spins are summed out, leaving interactions for the dual spins in their places. I.e., the sites and links switch under duality. In addition, the dual couplings are monotonically decreasing functions of the original, and if the original couplings are negative then the dual couplings give a negative Boltzmann weight. The effect of a complex coupling in the Ising model [21] when dealing with duality could be of some interest, but the SAT problem has real couplings and we do not consider it here.

Now we will simplify using the specifics of the SAT model. We must take the limit \( X_\mu \to \infty \) prudently, Taylor expanding the partition function in terms of \( e^{X_\mu} \). With careful work, the partition function becomes:

\[ Z = \sum_{k_s, m_l \in \mathbb{Z}_+} e^{-S_{\{k, m\}}(\mathcal{Z}) k_s + \sum_{l} m_l \times z_{\{k, m\}}} \]  
\[ z_{\{k, m\}} = \sum_{\{\alpha_s\}} \left( \prod_{s} D_k^{sgnH_s \alpha_s} \right) \left( \prod_{l} D_m^{sgnT_l \prod_{s \in \partial l} \alpha_s} \right), \]  
\[ D_k^\alpha = \frac{1}{2} (1 + \alpha) - \frac{1}{2} (1 - \alpha) (1 - \delta_{k, 0}), \]  
\[ S_{\{k, m\}} = \sum_{\mu} X_\mu \left[ -\sum_{s} (1 - 2k_s) sgnH_s c_s^{\mu} - \sum_{l} (1 - 2m_l) sgnT_l \prod_{s \in \partial l} c_s^{\mu} \right]. \]

This does not seem a particularly enlightening form of the partition function, or of the #SAT problem. We have introduced extra summations over the natural numbers for each site and link. However, there are two points that should be considered.

First, consider the \( X_\mu \) independent part of the partition function, Eq. [4]. Given a set of \( \{k_s, m_l\} \), this calculation is much simpler than it appears. Because of the particular simplicity of \( D_k^\alpha \), an algorithm may be designed to calculate the \( \alpha \) summation in time polynomial in \( N \). Effectively, this is an unimportant calculation when compared to the full #SAT.

The second point to consider is that the limit \( X_\mu \to \infty \) will greatly restrict the summation over \( k_s \) and \( m_l \). Since we control each \( X_\mu \), we can set them so that \( X_\mu \) is much greater than \( X_{\mu+1} \). Given this, \( sgnH_s = e^{\mu} \) in the first clause where \( c_s^\mu \) is nonzero, and \( sgnT_l = -\prod_{s \in \partial l} (-c_s^\mu) \) in the first clause where the product is nonzero. Now consider \( S_{\{k, m\}} \), a sum of terms proportional to the \( X_\mu \). If this sum is positive, then the contribution to the partition function vanishes. If the sum is negative, then the sums must arrange to cancel this term or else the partition function would diverge. The only relevant sets of \( \{k, m\} \) in the summation are those that give \( S_{\{k, m\}} = 0 \).

Each \( X_\mu \) is controlled separately, so we can set each term of \( S \) to zero separately:

\[ A^\mu = \sum_{s} B_s^\mu k_s + \sum_{l} C_l^\mu m_l, \]

\[ B_s^\mu = sgnH_s c_s^\mu, \quad C_l^\mu = -sgnT_l \prod_{s \in \partial l} (-c_s^\mu), \]

\[ A^\mu = -\frac{1}{2} \left( 1 - \sum_{s} B_s^\mu - \sum_{l} C_l^\mu \right). \]

This is a system of linear Diophantine equations. Finding the nonnegative \( k_s \) and \( m_l \) that satisfy these equations gives exactly the \( \{k, m\} \) that should be summed over in the partition function, Eq. [8]. The complexity of calculating the number of solutions to a Boolean satisfaction instance has transformed into finding the nonnegative solutions of this (likely) underconstrained system of equations and summing an integer function over these solutions.

Eqs. [8]-[12] are the main results of this article. We have shown that a problem in #SAT is equivalent to listing the solutions to this system of integer equations. It would be useful to simplify these equations to also find an equivalent for the decision problem, i.e. whether \( Z = 0 \) or not. However, this is no trivial task. Any given solution to Eq. [12] could give a positive or negative contribution to the partition function. Knowing a portion of the solutions may give little information, as the rest may cancel the contribution to the partition function from the portion known, and so it will be difficult to say whether an instance is satisfiable or not. This may change if solutions can be categorized or if the important solutions can be singled out, but naively only #SAT is considered.

Now we will show simple examples of this duality. First, we take a look at a single clause of three variables:

\[ F = (x_1 \lor x_2 \lor x_3). \]

This equation is satisfiable, and has \( Z = 7 \) solutions that satisfy \( F = T \), all possible configurations except \( x_1 = \)

Now we will use (8) and (12) to calculate this number.

First, the sites are $s = 1, 2, 3$ and the links are $l = 12, 13, 23, 123$. Seeing that $c_{s}^{l} = 1$, we find $\text{sgn}Z_{s} = \text{sgn}T_{123} = 1$ and for all $l \neq 123$, $\text{sgn}T_{l} = -1$. This means the Diophantine system of equations is just

$$k_{1} + k_{2} + k_{3} + m_{12} + m_{13} + m_{23} + m_{123} = 3. \quad (15)$$

The partition function is

$$Z = \sum_{\{k_{s}, m_{l}: \text{s.t. } \delta_{(k_{s}, m_{l})} = 0\}} (-1)^{\sum_{k} k_{s} + \sum_{l} m_{l}} z_{(k_{s}, m_{l})}. \quad (16)$$

Using (9), $z_{(k_{s}, m_{l})}$ may be calculated with relative simplicity. There are eight configurations of $\{\delta_{k_{s}, 0}, \delta_{m_{l}, 0}\}$ that leave $z$ nonzero. One of these requires all seven of the $k$s and $m$s to be nonzero, while the others require exactly three nonzero and four zero. These each contribute 1 to the partition function, leaving us with $Z = 7$.

Now look at a very simple unsatisfiable case:

$$F = (x_{1} \lor x_{2} \lor x_{3}) \land (x_{1} \lor x_{2} \lor \bar{x}_{3}) \land (x_{1} \lor \bar{x}_{2} \lor \bar{x}_{3}) \land (\bar{x}_{1} \lor x_{2} \lor x_{3}) \land (\bar{x}_{1} \lor x_{2} \lor \bar{x}_{3}) \land (\bar{x}_{1} \lor \bar{x}_{2} \lor \bar{x}_{3})$$

First, note that the calculation of $z_{(k_{s}, m_{l})}$ is exactly the same. When calculating a new #SAT case, $z_{(k_{s}, m_{l})}$ need not be recalculated unless the sites or links are changed. A simple benefit from this is that it makes it easier to analyze all bit flips of a SAT instance. However, the $\{k_{s}, m_{l}\}$ that give $S = 0$ must be recalculated each time. In this case, the Diophantine system is overconstrained and unsatisfiable. This immediately gives $Z = 0$.

An overconstrained system is one way in which SAT instance may reveal its unsatisfiability. However, this is not the only way. As noted previously, the contributions to the partition function, $(-1)^{\sum_{k} k_{s} + \sum_{l} m_{l}} z_{(k_{s}, m_{l})}$, may be positive or negative, and it is possible for there to be many solutions to the Diophantine system that give contributions that cancel. For another example and more discussion on unsatisfiability, see section 2 of the supplement [20].

It is important to ask how difficult it is to find the solutions to Eq. (12). First, let us discuss the matrix size. Although the equations apply to any instance, let us restrict to interesting instances, with a large number of variables and clauses, roughly of the same order: $N \sim M > 1$. Let us also assume the clauses contain a small number of variables. Assuming the clauses are well distributed among the variables, the matrix is roughly of the size $N + kM \times M$, where $k$ is some small number related to the number of variables in the clauses. The matrix size is quadratic in input size $N$.

There is much research addressing algorithms for reducing a Diophantine system to useable forms, in particular the Hermite and Smith normal forms [22, 23]. The algorithms take more time than the analogous reduced row echelon algorithms for real matrices but the time is still polynomial in $N$. However, acquiring the nonnegative solutions to the system is not a polynomial task. Indeed, the number of nonnegative solutions need not be polynomial in $N$. For example, a collection of $M$ clauses with 3 variables where no clauses share variables will have $7^{M}$ solutions. Simply listing the solutions is #P-hard.

There is no doubt that there are instances where $Z$ is easier to calculate without using duality. However, it is quite possible that there are situations where it will be easier to use the dual equations, notably when the number of solutions to the Diophantine system is small or zero. This situation is likely to coincide to some extent with when the number of solutions to SAT instances is small or zero, the region of greatest interest in Boolean satisfiability research.

Beyond this, the particular form of the matrix (the fact that it is a $(-1, 0, 1)$ matrix and how the link columns are completely determined from the site columns) could lead to great simplification in algorithms for finding the nonnegative solutions. Also, by categorizing which solutions will give negative values, the equations could be simplified to describe the decision problem which is of more interest, SAT itself.

Combining duality with the cavity method, commonly used to study SAT problems as well as Ising problems, could be a promising research direction. Preliminary steps may be found in the supplement [20].

Other computer science problems could also have interesting dual problems. Many of these problems are easily stated as some limit of a statistical mechanics model, which likely has a simple duality relation to another model. Once the appropriate limit is taken, this dual problem will reduce to a problem very unlike the original. The $x - y$, $p$-clock, Coulomb gas, and vector Potts models are a small set of classical models with well studied, simple dualities relations [39].

The recent work with bond algebraic dualities [10, 13] opens up the number of models to study even further. With this new way to categorize and explore dualities, even quantum complexity classes could be accessible for study with duality [21, 25].

In this letter, we have presented an exact relation between problems in #SAT and solving a linear Diophantine system of equations, given from a modified version of the established Kramers-Wannier duality. This relation serves both as a novel avenue for study of #SAT and a glimpse at the power statistical mechanics dualities can bring to computer science. With the large number of duality relations and the ease of relating a computer science problem to the limit of a physical model, the study of duality could prove very fruitful.

This research was supported by NSF-CAREER award No. DMR-0847224 and Simons Foundation.
[1] D. Achlioptas, “Random satisfiability,” Chap. 8, pp. 245–270, vol. 185 of [26] (2009).
[2] F. Altarelli, R. Monasson, G. Semerjian, and F. Zamponi, CoRR abs/0802.1829 (2008).
[3] M. Mézard and A. Montanari, Information, physics, and computation (Oxford University Press Inc., New York, NY, USA, 2009).
[4] R. Sebastiani and A. Tacchella, “Sat techniques for modal and description logics,” Chap. 25, pp. 781–824, vol. 185 of [26] (2009).
[5] S. Arora and B. Barak, Complexity Theory: A Modern Approach (Cambridge University Press, 2009).
[6] H. A. Kramers and G. H. Wannier, Phys. Rev. 60, 252 (1941).
[7] L. Onsager, Phys. Rev. 65, 117 (1944).
[8] R. Savit, Rev. Mod. Phys. 52, 453 (1980).
[9] J. B. Kogut, Rev. Mod. Phys. 51, 659 (1979).
[10] Z. Nussinov and G. Ortiz, Phys. Rev. B 79, 214440 (2009).
[11] E. Cobanera, G. Ortiz, and Z. Nussinov, Phys. Rev. Lett. 104, 020402 (2010).
[12] E. Cobanera, G. Ortiz, and Z. Nussinov, Advances in Physics 60, 679 (2011).
[13] G. Ortiz, E. Cobanera, and Z. Nussinov, Nuclear Physics B 854, 780 (2012).
[14] S. A. Cook, in Proceedings of the third annual ACM symposium on Theory of computing, STOC ’71 (ACM, New York, NY, USA, 1971) pp. 151–158.
[15] L. A. Levin, Problemy Peredachi Informatsii 9, 115 (1973).
[16] M. Mézard and G. Parisi, EPL (Europhysics Letters) 3, 1067 (1987).
[17] M. Mézard, G. Parisi, and R. Zecchina, Science 297, 812 (2002).
[18] R. Monasson and R. Zecchina, Phys. Rev. E 56, 1357 (1997).
[19] A. Montanari, F. Ricci-Tersenghi, and G. Semerjian, J. Stat. Mech. 2008, 04004 (2008).
[20] http://terpconnect.umd.edu/~galitski/SATDual/.
[21] V. Matveev and R. Shrock, Journal of Physics A: Mathematical and Theoretical 41, 135002 (2008).
[22] T. Mulders and A. Storjohann, in Proceedings of the 1999 international symposium on Symbolic and algebraic computation, ISSAC ’99 (ACM, New York, NY, USA, 1999) pp. 181–188.
[23] G. Jäger and C. Wagner, Parallel Comput. 35, 345 (2009).
[24] C. R. Laumann, R. Moessner, A. Scardicchio, and S. L. Sondhi, Quant. Inf. and Comp. 10, 0001 (2010).
[25] B. Hsu, C. R. Laumann, A. M. Lauechli, R. Moessner, and S. L. Sondhi, Phys. Rev. A 87, 062334 (2013).
[26] A. Biere, M. J. H. Heule, H. van Maaren, and T. Walsh, eds., Handbook of Satisfiability, Frontiers in Artificial Intelligence and Applications, Vol. 185 (IOS Press, 2009) p. 980.