WORDBOX: A case study in SAT Encodings

Victor S. Miller

SRI, Computer Science Laboratory, Menlo Park, CA 94025 *

March 1, 2024

Abstract

The great effectiveness of SAT solvers for large, difficult, SAT problems is a recent welcome development. It is well know to practitioners in that field that the encoding of a problem can have a significant and radical effect on the practical solution time.

In particular, many combinatorial problems have a straightforward "easy" encoding which is logically sufficient to specify the problem. However, SAT solvers are very poor at inferring "global" knowledge about the problem. In fact, with some problems, such as the "Pigeon Hole Principal", in which global knowledge makes the problem trivial, branching SAT solvers must take exponential time. Examples of global knowledge are graph connectedness and parity. Therefore, in order to find an improved encoding global knowledge should be used.

In this note we consider the encoding a recreational Mathematics problem known as *Wordbox*. One is given a list of words, and an $m \times n$ rectangular grid. The object of the problem is to label the grid points with letters so that one can trace out all of the words in the list by moving adjacent grid points (using up/down, right/left moves). We show that this problem is an instance of the *labeled graph homomorphism* problem, in which we're given two finite undirected graphs G and H, along with labels $\ell(v)$ for every node of G. The object of the problem is to find a map $f : V(G) \to V(H)$ such that if $(v, v') \in E(G)$ then $(f(v), f(v')) \in E(H)$ (this is a *graph homomorphism*), and a labeling $\ell(w)$ of $w \in V(H)$ such that, for all $v \in V(G)$ we have $\ell(f(v)) = \ell(v)$. In turn, we show that the labeled graph homomorphism problem is a subset of the *colored graph homomorhphism problem*.

We investigate a number of different encodings of the global knowledge and their effect on solving times for various SAT solvers.

*Much of the this work performed at the IDA Center for Communications Research, Princeton, NJ 08540 USA

1 A recreational problem

In the GCHQ *Kryptos Kristmas Kwiz* of 2006 `https://theintercept.com/2015/12/25/gchq-play-a-british-spy-game/` [1] describes a problem called "wordbox":

> A wordbox is a rectangle of letters in which a series of words can be read by starting at one letter and moving to an adjacent letter in a row or column, but not diagonally. Retracing steps and reusing letters is allowed. Thus a wordbox might be
>
> | | | | |
> |---|---|---|---|
> | D | O | R | F |
> | I | G | E | S |
> | T | A | O | T |
>
> which contains `DODO, DOG, FROG, STOAT TIGER` and `TIT`, but doesn't contain `GOAT` or `GEESE`. This wordbox contains 12 letter cells, so its area is 12. What is the smallest (in area) wordbox that includes the planets: `MERCURY, VENUS, EARTH, MARS, JUPITER, URANUS, NEPTUNE, PLUTO`?

The answer given (without any proof of minimality) is:

V	E	A	M
A	N	R	T
R	U	S	H
N	T	A	
E	P	I	M
L	U	T	E
P	J	O	R
Y	R	U	C

2 A logical statement

To solve the original recreational problem, we pose it as a problem of *Labeled graph homomomorphism*:

Definition 1 (Graph Homomorphism)**.** *Let G, H be graphs. A* graph homomorphism *from G to H is a map $\phi : V(G) \to V(H)$ such that, for all $(v, w) \in E(G)$, we have $(\phi(v), \phi(w)) \in E(H)$.*

Definition 2 (Labeled Graph)**.** *Let G be a graph. A* labeling *of G is a map $\ell : V(G) \to C$, for some set C.*

Definition 3 (Labeled homomorphism)**.** *Let G be a labeled graph, with a* labeling *$\ell : V(G) \to C$, and H be a graph. A* labeled homomorphism *is a homomorphism $\phi : V(G) \to V(H)$, and a labeling $\ell' : V(H) \to C$, such that $\ell'(\phi(v)) = \ell(v)$ for all $v \in V(G)$.*

[1] Solutions at `https://theintercept.com/2016/01/01/gchq-play-a-british-spy-game-the-solutions/`

For the original problem, the graph G is a disjoint union of simple paths: for each word, of length k, there is a path $v_1, \ldots, v_k$, where the edges are (v_i, v_{i+1}) for $i = 1, \ldots, k-1$, and $\ell(v_i)$ is the i-th letter in the word. The graph H is an $m \times n$ *grid graph*: its vertices are pairs $(i,j), 0 \le i < m, 0 < j < n$, with $((i,j),(i',j'))$ an edge if and only if $|i-i'| + |j-j'| = 1$.

We may state the problem as follows: We are given two undirected graphs G, H, and a *labeling* $\ell : V(G) \to C$. We want to know if there exists a graph homomorphism $f : V(G) \to V(H)$, and a labeling $\ell' : V(H) \to C$ such that $\ell'(f(v)) = \ell(v)$ for all $v \in V(G)$.

For the original problem, the graph G is a disjoint union of paths, H is the *grid graph*

$$\begin{aligned} &\exists f : V(G) \to V(H), \ell' : V(H) \to C \\ &\forall (v,v') \in E(G), (f(v), f(v')) \in E(H) \\ \wedge &\forall v \in V(G), \ell'(f(v)) = \ell(v). \end{aligned} \tag{1}$$

where f is a function. However, in order to encode this in quantifier normal form we need to encode f as a binary relation.

So $w = f(x)$ means

$$\forall x \exists w R(x,w) \wedge \forall x, w, w'((w = w') \vee \neg R(w,x) \vee \neg R(x,w')).$$

3 The colored homomorphism problem

Definition 4 (Edge Colored Graph). *An* edge colored graph *is a finite undirected graph $G = (V(G), E(G))$ a set, C of colors and a map $\phi : E(G) \to C$, which assigns a color to each edge.*

Definition 5 (Edge Colored Homomorphism). *Let G and H be two edge colored graphs with the same set of colors. An* edge colored homomorphism *is a homomorphism $f : G \to H$, such that, for all edges $e \in E(G)$, the color of the edge $f(e) \in E(H)$ is the same as that of e.*

We now reduce the vertex colored homomorphism problem to the 2-colored edge homomorphism problem. Given a vertex colored graph G, construct the edge colored graph G' with two colors, red and green. The edges of G' will be a copy of the edges of G colored green. For each $v \neq v' \in V(G)$ such that $\ell(v) \neq \ell(v')$, and $(v,v') \notin E(G)$, we add an edge (v,v') colored red. For the target graph H, we construct a 2-colored graph H', whose green edges are a copy of the edges of H, and whose red edges are $(v,v') \notin H$, for $v \neq v'$.

Proposition 1. *There is a vertex colored homomorphism from G to H if and only if there is an edge colored homomorphism from G' to H'.*

4 Automorphisms of edge colored graphs

Programs such as `nauty` can calculate the automorphism group of a vertex colored graph. That is, if G is a vertex colored graph, with color function c, and *automorphism* $\phi : G \Rightarrow G$ is a one-to-one map $\phi : V(G) \to V(G)$ such that, for each edge $\{v_1, v_2\} \in E(G)$, we have $\{\phi(v_1), \phi(v_2)\} \in E(G)$ and for each $v \in V(G)$ we have $c(v) = c(\phi(v))$.

Given an edge two colored graph, G, we form a new vertex colored graph G' whose vertices are the disjoint union of two copies of $V(G)$: $V(G) \times \{0, 1\}$. The edges of G' are as follows: for each $v \in V(G)$ there is an edge $\{(v, 0), (v, 1)\}$. If an edge $\{v, w\} \in E(G)$ has color c, there is an edge $\{(v, c), (w, c)\} \in E(G')$. Vertices of the form (v, c) have color c. If ϕ is an automorphism of G', then necessarily $\phi((v, c)) = (w, c)$ for some w, by preserving colors. If $\phi((v, 0)) = (w, 0)$ then we must have $\phi((v, 1)) = (w, 1)$ for the same w because the only edges going from $(G, 0)$ to $(G, 1)$ are the vertical edges.

5 Fractional Homomorphism

Let G and H be undirected graphs. The *incidence matrix* for G (resp. H) is a matrix whose rows are indexed by $V(G)$ and columns by $E(G)$, with $M^G_{v,e} = [v \in e]$. We define two matrices X and Y which will encode a homomorphism. Given $v \in V(G), w \in V(H)$, define $X_{w,v} = 1$ if v maps to w and 0 otherwise. Similarly, given $e \in E(G)$ and $f \in E(H)$ define $Y_{f,e} = 1$ if e maps to f and 0 otherwise.

Proposition 2. *Given G, H simple undirected graphs, there is a homomorphism from G to H, if and only if there are 0/1 matrices $X_{w,v}$ for $v \in V(G), w \in V(H)$, and $Y_{f,e}$ for $e \in E(G), f \in E(H)$ with $\sum_{w \in V(H)} X_{w,v} = 1$ and $\sum_{f \in E(H)} Y_{f,e} = 1$ and $XM^G = M^H Y$.*

Proof. Note that □

$$(XM^G)_{w,e} = \sum_{v \in V(G)} X_{w,v} M^G_{v,e} = \sum_{v \in e} X_{w,v}, \tag{2}$$

and

$$(M^H Y)_{w,e} = \sum_{f \in E(H)} M^H_{w,f} Y_{f,e} = \sum_{f \in E(H), w \in f} Y_{f,e}. \tag{3}$$

We can interpret equation (2) as saying that $(XM^G)_{w,e}$ is the number of endpoints of edge e that map to w, which is 0, 1 or 2. We can also interpret equation (3) as saying that $(M^H Y)_{w,e}$ is the number of endpoints of e that map to w. However, this quantity is 0 or 1, since the graphs are simple. Thus, if the two sides are equal there is a homomorphism. The converse is clear.

We can express homomorphism in terms of these matrices: $XM^G = M^H Y$. Note that where $w \in V(H)$, and

The first equation encodes mapping on vertices $v \to w$, and the second encodes mapping on edges $e \to f$. If we require that the X and Y are left stochastic (row sum = 1, nonnegative entries), this is a relaxation.

More specifically, we would like X to have the property that $X_{w,v} = 1$ if v maps to w and 0 otherwise. In addition, we would like $Y_{f,e} = 1$ if e maps to f and 0 otherwise.

If this is the case then $(XM^G)_{w,e}$ is the number of vertices of G incident to e that map to w, which is the number of endpoints of e that map to w. Notice that for a simple graph this is 0, 1 or 2. However, as we shall see in the next paragraph. The entry on the right hand side must be 0 or 1.

We also have $(M^H Y)_{w,e}$ is 1 if e maps to an edge incident to w and 0 otherwise. Thus, the two sides are equal if and only if there is a homomorphism from G to H. If the edges of G and H are colored, and we require that colors map to like colors, we can enforce this by restricting elements of the matrix Y.

We have an LP (linear programming) relaxation by requiring that the matrices be left stochastic. That is $1 \geq Y_{f,e} \geq 0$ and $\sum_{e \in E(G)} Y_{f,e} = 1$. We can then interpret the value $Y_{f,e}$ as the probability that the edge e is mapped to the edge f. Similarly, we require that X is left stochastic. In this case we can interpret $X_{w,v}$ as the probability that v maps to w.