GRAPHS, COLORING IDEALS, AND GRÖBNER BASES

WITH AN APPLICATION IN SUDOKU PUZZLES

Rayaan Attari **Anna Bundy** **Mario Manalu**

May 25, 2021

1 Introduction

Many graph theoretic problems have benefited from the viewpoint of algebraic geometry. A not-insignificant portion of graph theory is concerned with coloring the vertices of graphs such that no two adjacent vertices get the same color. In this paper, we apply tools from algebraic geometry to understand the colorability of graphs using the theory of Gröbner bases which is a key computational tool for studying polynomial ideals.

In Section 2, we will explore the concept of a graph coloring and use algebraic techniques to determine possible colorings for a graph. Ideals will play a pivotal part in this exploration by enabling us to concisely encode information about a graph into a set of polynomials. Uncovering the structure of these ideals will then naturally lead us to the proof of three interesting algebraic characterizations of colorability.

In Section 3, we will consider the graph coloring problem presented by Sudoku and Shidoku puzzles. A Sudoku can be thought of as a graph with 81 vertices and a specially defined edge set. Assigning a variable to each of the vertices, we will find ideals which assign these variable values which are consistent with the rules of Sudoku. We will also explain the shape of the Gröbner basis given by a well-posed Sudoku puzzle.

2 Graphs, Coloring Ideals, and Gröbner Bases

In this section, we consider a well-known family of polynomial ideals encoding the problem of graph k-colorability. We begin by introducing the graph polynomial and associated terminology, followed by certain ideals we are interested in. Then, we reduce the decidability of k-colorability to an ideal membership problem, which we know how to solve from the tools of computational algebraic geometry. For instance, by expressing a given graph as a set of polynomials, we will use Gröbner bases to determine if a given graph is 3-colorable, and if so, determine all possible 3-colorings. Finally, we will briefly conclude with yet another characterization of k-colorability embedded in quotient ideals.

2.1 Introduction to Graph Colorings

Let's dive right into the problem we are interested in; we want to be able to color a graph. A graph coloring is essentially just an assignment of labels, called colors, to the vertices of a graph such that no two adjacent vertices share the same color. Clearly the intriguing quantity is the minimum number of colors required for a coloring. We provide the formal definition of a graph coloring and related concepts below.

Definition 2.1.1 (Colorability, Chromatic Number)**.** Let G be a graph with vertex set V. A *k-coloring* of G is a function f from V to a set S with k elements; a *proper k-coloring* is a k-coloring such that $f(v) \neq f(w)$ whenever (v, w) is an edge, otherwise we call it *improper*. A graph is said to be *k-colorable* if there exists a proper k-coloring. The *chromatic number* of G, denoted $\chi(G)$, is the smallest k such that G is k-colorable.

As an example, consider the cycle graph C_5 given below.[1]

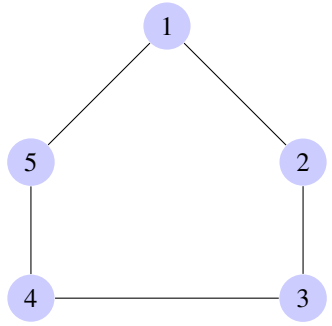

Figure 1: *The cycle graph on 5 vertices.*

One way to color this graph would be to color every vertex a different color; this would be a proper 5-coloring. But, we can do better. Let S be the set $\{\text{blue}, \text{green}, \text{red}\}$. Then, we could let $f(1)$ and $f(3)$ be blue, $f(2)$ and $f(4)$ be green and $f(5)$ be red. So, there is a proper 3-coloring.

[1] *Graph Theory Notes*, C. French

Notice, however, that there is not a proper 2-coloring. We could demonstrate this by contradiction. Suppose we had only two colors, say black and white, then once we decide what $f(1)$ is, this forces $f(2)$ to be the other color. In turn, we must have $f(3)$ be the first color so $f(3) = f(1)$. Similarly, we get $f(5) = f(3) = f(1)$, but we do not get a proper coloring, since vertices 1 and 5 are adjacent in C_5. Thus $\chi(C_5) = 3$.

The study of graph colorings from an algebraic perspective has introduced interesting techniques and algorithms into the field of computational algebra.[2] Given some k, the question that we are interested in answering is whether or not some graph G is k-colorable. In order to apply algebraic methods to problems about graphs, we must first transform graph-theoretic information into algebraic information. Particulary, we need to transform information about our graph into information about a set of polynomials; we work in $\mathbb{C}[x_1, ..., x_n]$, with a variable for each vertex of the graph.

2.2 Vertex Coloring Ideals

This motivates the following definition.

Definition 2.2.1 (Graph Polynomial)**.** Let G be an undirected graph with vertex set $V = \{1, ..., n\}$ and edge set E. The *graph polynomial*[3] of G is given by

$$f_G = \prod_{\substack{(i,j)\in E \\ i<j}} (x_i - x_j) \in \mathbb{C}[x_1, ..., x_n]$$

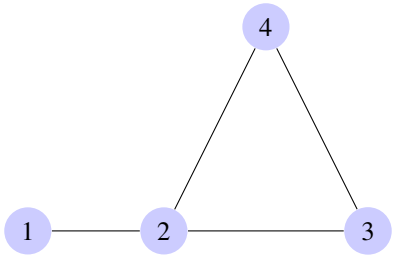

Figure 2: *Constructing the graph polynomial* f_G.

For instance, in the undirected graph G pictured above, we have four edges and should thus expect four expressions of the form $(x_i - x_j)$ in our product. It is easy to see that $f_G = (x_1 - x_2) \cdot (x_2 - x_3) \cdot (x_3 - x_4) \cdot (x_2 - x_4)$.

The graph polynomial has a lot of interesting properties related to the graph, but we're only interested in a few of them.[4] However, the graph polynomial by itself will not be enough to tell us much about whether a graph is k-colorable, so we turn to ideals to provide us some assistance. When looking at polynomial ideals, a problem that often arises is how to determine if an arbitrary polynomial is a member of the ideal. We now reduce the decidability of k-colorability to an ideal membership problem.

[2] *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, C. Hillar & T. Windfeldt
[3] Ibid
[4] *A Variety of Graph Coloring Problems*, D. Mehrle

Let $G = (V, E)$ be a graph with $V = \{1, ..., n\}$. Fix $k \in \mathbb{Z}^+$. Suppose we wish to check whether G is k-colorable. We define the vertex coloring ideal $I_{n,k} \subseteq \mathbb{C}[x_1, ..., x_n]$ (also denoted I_n if the number of colors is clear) to be the ideal generated by the vertex polynomials $v_i = x_i^k - 1$ for all $i \in V$. And so, we shift focus to the following ideal of $\mathbb{C}[x_1, ..., x_n]$.

$$I_{n,k} = \langle x_i^k - 1 : i \in V \rangle$$

The next theorem describes the reduction from the decidability of graph colorability to ideal membership.

Theorem 2.2.1. Fix k, a positive integer. The graph G is k-colorable if and only if $f_G \notin I_{n,k}$.

This criterion gives us a very testable algorithm to determine if a graph is k-colorable. But before we get into the proof, it is worth looking at a simple example. Consider the graph C_3 displayed below with vertices $\{1, 2, 3\}$.[5] This graph is clearly 3-colorable but not 2-colorable, but to test the feasibility of our algorithm let's apply Theorem 2.2.1.

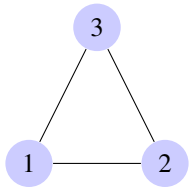

Figure 3: *Applying Theorem 2.2.1 to C_3.*

Let R be the ring $\mathbb{C}[x, y, z]$, and consider the ideal $I_{3,3} = \langle x^3 - 1, y^3 - 1, z^3 - 1 \rangle$. This is also a Gröbner basis for the ideal $I_{3,3}$. The graph polynomial of C_3 is easly determined to be $f_{C_3} = (x - y) \cdot (y - z) \cdot (x - z)$. Note that none of the terms of f_{C_3} are cubic in any of the variables, and hence f_{C_3} is not divisible by any of the elements of our Gröbner basis. Hence, $f_{C_3} \notin I_{3,3}$ and we conclude that C_3 is 3-colorable by the above theorem. But, it is not 2-colorable because

$$f_{C_3} = (y - z) \cdot (x^2 - 1) + (z - x) \cdot (y^2 - 1) + (x - y) \cdot (z^2 - 1) \in I_{3,2}$$

Notice that implicit in the discussion above is the use of the following proposition which will be central to our exploration.

Proposition 2.2.1. Let $\mathcal{G} = \{g_1, ..., g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is nonzero.[6]

Okay, so our algorithm for determining k-colorability seems to be accurate. That's great! But, why exactly does it work? Imagine taking the colors to be k^{th} roots of unity. Recall that an n^{th} root of unity, where n is a positive integer, is a number x satisfying the equation $x^n - 1 = 0$.[7] Coloring our vertices with roots of unity? That's absurd! However, remember that a coloring is simply an assignment of labels to the vertices, whatever those labels may be. Taking the colors to be roots of unity, specifically the k^{th} roots of unity, allows us to numerically deal with them using algebraic

[5] Ibid
[6] *Ideals, Varieties, and Algorithms*, Cox et al.
[7] *Root of Unity*, Wikipedia

tools. It is important to note that we are using the result that there are exactly k distinct k^{th} roots of unity in $\mathbb{C}$. In fact, any algebraically closed field of characteristic not diving k contains k distinct k^{th} roots of unity.[8] We could generalize our results to these fields but we stick to $\mathbb{C}$ for simplicity. Thus for each vertex in a graph G, we assign a "color", which corresponds to setting each variable to a k^{th} root of unity. Then, the points in $\mathbf{V}(I_{n,k})$ are all n-tuples of k^{th} roots of unity and therefore naturally correspond to all k-colorings of G. However, if two adjacent vertices are assigned the same color, f_G will vanish. Consequently, we get the following lemma.

Lemma 2.2.2. Let G be a graph and fix $k \in \mathbb{Z}^+$. The variety $\mathbf{V}(I_{n,k})$ is in bijection with all k-colorings of G.[9]

In order to prove Theorem 2.2.1, we will require the Nullstellensatz, a classical theorem of algebraic geometry, stated below.

Theorem 2.2.3 (Hilbert's Nullstellensatz)**.** Let k be an algebraically closed field. If $f, f_1, ..., f_s \in k[x_1, ..., x_n]$, then $f \in \mathbf{I}(\mathbf{V}(f_1, ..., f_s))$ if and only if $f^m \in \langle f_1, ..., f_s \rangle$ for some integer $m \geq 1$.[10]

Additionally, we will also need to demonstrate that $I_{n,k}$ is radical. But to do so we must first illustrate the following result.

Lemma 2.2.4. Let $f \in \mathbb{C}[x_1, ..., x_n]$, and let M be the largest power of any variable that appears in f. Fix $k > M$, k a positive integer, and let K^n denote the set of points of $\mathbb{C}^n$, where each coordinate is a k^{th} root of unity. If f vanishes at all points of K^n, then f is the zero polynomial.[11]

Proof. We proceed by induction on n.

For the base case, let $n = 1$. Then $f \in \mathbb{C}[x]$, where $\deg(f) = M$, has at most M roots. Notice that the set $K \subseteq \mathbb{C}$ contains k distinct k^{th} roots of unity. Since $k > M$, K contains at least $M + 1$ distinct points. But then f vanishes on at least $M + 1$ distinct points by hypothesis, and we arrive at a contradiction. Therefore, f is the zero polynomial.

Now assume this holds true up to $n - 1$.

Let $f \in \mathbb{C}[x_1, ..., x_n]$ be a polynomial that vanishes at all points of $K^n \subseteq \mathbb{C}^n$. Notice that we can write f as a function of x_n as follows.

$$f = \sum_{i=0}^{N} g_i(x_1, ..., x_{n-1}) {x_n}^i$$

Let $(a_1, ..., a_{n-1}) \in K^{n-1}$ be arbitrary. Then $f(a_1, ..., a_{n-1}, x_n)$ is a polynomial in one variable with finite degree. Since $f(a_1, ..., a_{n-1}, x_n)$ vanishes whenever $x_n \in K$, we know that $f(a_1, ..., a_{n-1}, x_n)$ is the zero-polynomial in $\mathbb{C}[x]$ from the base case. Hence, we must have $g_i(a_1, ..., a_{n-1}) = 0$ for all i. Now because $(a_1, ..., a_{n-1})$ is an arbitrary element in K^{n-1}, we conclude that each $g_i \in \mathbb{C}[x_1, ..., x_{n-1}]$ is the zero polynomial. Therefore, f is the zero polynomial in $\mathbb{C}[x_1, ..., x_n]$. □

[8] *Graph-coloring Ideals: Nullstellensatz Certificates, Gröbner Bases for Chordal Graphs, and Hardness of Gröbner Bases*, De Loera et al.

[9] *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, C. Hillar & T. Windfeldt

[10] *Ideals, Varieties, and Algorithms*, Cox et al.

[11] Ibid

We use this result to show that $I_{n,k}$ is radical.

Lemma 2.2.5. $I_{n,k}$ is a radical ideal.

Proof. It suffices to show that $\mathbf{I}(\mathbf{V}(I_{n,k})) = I_{n,k}$ because $\mathbf{I}(V)$ is always a radical ideal for any variety V. One direction of the containment is trivial since we always have that $J \subseteq \mathbf{I}(\mathbf{V}(J))$, where J is an ideal. Specifically, we already have that $I_{n,k} \subseteq \mathbf{I}(\mathbf{V}(I_{n,k}))$. Thus it remains to show that $\mathbf{I}(\mathbf{V}(I_{n,k})) \subseteq I_{n,k}$.

Let f be an arbitrary element of $\mathbf{I}(\mathbf{V}(I_{n,k}))$. Then f vanishes on $\mathbf{V}(I_{n,k})$, which is the set of all n-tuples $(a_1, ..., a_n)$ where each a_i is a k^{th} root of unity. To show that f is in $I_{n,k}$, we will use division with remainder on the generators of $I_{n,k}$. Using lex order with $x_1 > x_2 > \cdots > x_n$, we have that f can be written as

$$f = q_1 \cdot ({x_1}^k - 1) + q_2 \cdot ({x_2}^k - 1) + \cdots + q_n \cdot ({x_n}^k - 1) + r$$

where $q_i, r \in \mathbb{C}[x_1, ..., x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in $\mathbb{C}$, of monomials, none of which is divisible by any of leading terms ${x_1}^k, {x_2}^k, ..., {x_n}^k$. Suppose that $r \neq 0$. It follows that every power of an x_i that appears in the remainder r is strictly less than k. Now notice that since f vanishes on $\mathbf{V}(I_{n,k})$ and $q_i \cdot ({x_i}^k - 1)$ vanishes on $\mathbf{V}(I_{n,k})$ for all i, r must also vanish on $\mathbf{V}(I_{n,k})$. Then Lemma 0.4 allows us to conclude that r is the zero polynomial and, since f can now be written as a linear combination of elements in $I_{n,k}$, $f \in I_{n,k}$. Therefore, $\mathbf{I}(\mathbf{V}(I_{n,k})) \subseteq I_{n,k}$ so $I_{n,k}$ is radical.[12] □

We are now ready to prove Theorem 2.2.1, stated once again for reference.

Theorem 2.2.1. Fix k, a positive integer. The graph G is k-colorable if and only if $f_G \notin I_{n,k}$.[13]

Proof. We first prove the forward direction. Suppose G is k-colorable. Then, there is an assignment of k colors to vertices such that no two adjacent vertices have the same color. By Lemma 0.2, this corresponds to a point $a \in \mathbf{V}(I_{n,k})$ such that $f_G(a) \neq 0$. Since any linear combination of the generators of $I_{n,k}$ will vanish at a, but f_G does not, it follows that f_G cannot be in the ideal $I_{n,k}$.

Conversely, if G is not k-colorable, then every assignment of k colors to the vertices of G must have two adjacent vertices sharing a color. This means that f_G vanishes for any assignment of k colors. In particular, this implies that f_G vanishes on $\mathbf{V}(I_{n,k})$. Hence, by the Nullstellensatz, there is some $m \geq 1$ such that ${f_G}^m \in I_{n,k}$. But $I_{n,k}$ is a radical ideal, so therefore $f_G \in I_{n,k}$. □

[12] Proof idea provided by Prof. Mileti

[13] *A Variety of Graph Coloring Problems*, D. Mehrle

2.3 Graph Coloring Ideals

For the next segment of this section we will illustrate how one can apply the technique of Gröbner bases to determine whether a given graph can be 3-colored (in fact the same technique would work for any coloring). We then arrive at an equivalent theorem for deciding k-colorability. This material is based on a portion of D. Bayer's thesis.[14]

Let us first state the problem precisely. We are given a graph G with n vertices with at most one edge between any two vertices. We want to color the vertices in such a way that only 3 colors are used, and no two vertices connected by an edge are colored the same way. That is, we want to demonstrate a 3-coloring.

First, we let $\omega \in \mathbb{C}$ be a cube root of unity (i.e. $\omega^3 = 1$). We represent the 3-colors by $1, \omega, \omega^2$, the 3 distinct cube roots of unity. Now, we let $x_1, .., x_n$ be variables representing the distinct vertices of the graph G. Each vertex is to be assigned one of the 3 colors $1, \omega, \omega^2$. This can be represented by the following n equations

$$x_i{}^3 - 1 = 0, \quad 1 \leq i \leq n \tag{1}$$

Note that this constraint would be encoded in the ideal $I_{n,3}$ that was presented earlier. Now, if the vertices x_i and x_j are connected by an edge, they need to have a different color. Since $x_i{}^3 = x_j{}^3$, we have $(x_i - x_j) \cdot (x_i{}^2 + x_i x_j + x_j{}^2) = 0$. Therefore, x_i and x_j will have different colors if and only if

$$x_i{}^2 + x_i x_j + x_j{}^2 = 0 \tag{2}$$

Note that this constraint would be encoded in the graph polynomial f_G that was defined earlier. Let $I_{G,3}$ be the ideal of $\mathbb{C}[x_1, ..., x_n]$ generated by the polynomials in Equation (1) and for each pair of vertices x_i, x_j connected by an edge by the polynomials in Equation (2). We call $I_{G,3}$ the 3-coloring ideal of G. More generally, we have the following definition.[15]

Definition 2.3.1 (Coloring Ideal)**.** The *k-coloring ideal* of a graph $G = (V, E)$ is the ideal $I_{G,k} \subseteq \mathbb{C}[x_i \ : \ i \in V]$ generated by

$$x_i{}^k - 1, \text{for all } i \in V$$

$$x_i{}^{k-1} + x_i{}^{k-2} x_j + \cdots + x_i x_j{}^{k-2} + x_j{}^{k-1}, \text{for all } (i, j) \in E$$

In considering the variety $\mathbf{V}(I_{G,3})$ in $\mathbb{C}^n$, the following two results follow immediately.[16]

Lemma 2.3.1. Let G be a graph and fix $k \in \mathbb{Z}^+$. The variety $\mathbf{V}(I_{G,k})$ is in bijection with all of the proper k-colorings of G.

Theorem 2.3.2. The graph G is k-colorable if and only if $\mathbf{V}(I_{G,k}) \neq \emptyset$.

[14] *The Division Algorithm and the Hilbert Scheme*, D. Bayer
[15] *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, C. Hillar & T. Windfeldt
[16] Ibid

We can now use Gröbner bases to determine if $\mathbf{V}(I_{G,3}) = \emptyset$. Of course, we first need to compute a (reduced) Gröbner basis $\mathcal{G}$ for $I_{G,3}$. If $1 \in \mathcal{G}$, $\mathbf{V}(I_{G,3}) = \emptyset$, otherwise $\mathbf{V}(I_{G,3}) \neq \emptyset$. The latter result is a consequence of the Weak Nullstellensatz.

Theorem 2.3.3 (Weak Nullstellensatz)**.** Let k be an algebraically closed field and let $I \subseteq k[x_1, ..., x_n]$ be an ideal satisfying $\mathbf{V}(I) = \emptyset$. Then $I = k[x_1, ..., x_n]$.[17]

Consider the graph G shown below.

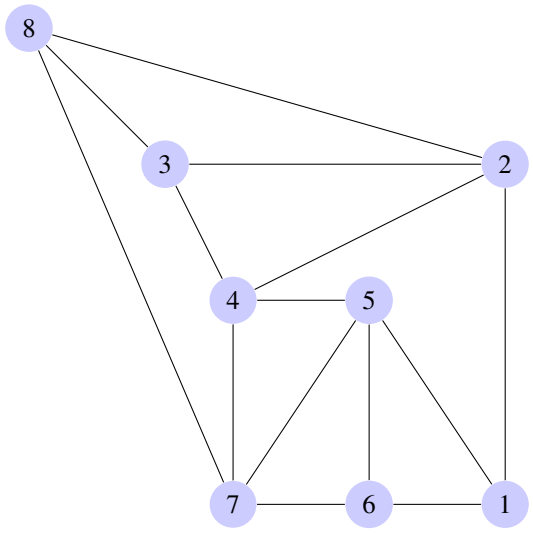

Figure 4: *Demonstrating a 3-coloring.*

The polynomials corresponding to G are

$$x_i{}^3 - 1 = 0, \text{ for } i = 1, ..., 8$$

and

$$x_i{}^2 + x_i x_j + x_j{}^2, \text{ for the pairs } (i,j) \in \{(1,2), (1,5), (1,6), (2,3), (2,4),$$

$$(2,8), (3,4), (3,8), (4,5), (4,7), (5,6), (5,7), (6,7), (7,8)\}$$

We compute a reduced Gröbner basis for the ideal $I_{G,3}$ corresponding to the above polynomials. We use the lex term ordering with $x_1 > x_2 > \cdots > x_8$. Using Sage, we obtain

[17] *Ideals, Varieties, and Algorithms*, Cox et al.

$$\mathcal{G} = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8,$$

$$x_5 + x_7 + x_8, x_6 - x_8, {x_7}^2 + x_7x_8 + {x_8}^2, {x_8}^3 - 1\}$$

Since $1 \notin \mathcal{G}$, we have that $\mathbf{V}(I_{G,3}) \neq \emptyset$, and hence, by Theorem 2.3.2, G is 3-colorable.

We can use the Gröbner basis $\mathcal{G}$ to give an explicit coloring, since the system of equations represented by $\mathcal{G}$ turns out to be easy to solve. Let us assume that the 3 colors we are using are blue, red, and green. We must first choose a color for x_8, say red, since the only polynomial in one variable in $\mathcal{G}$ is ${x_8}^3 - 1$. We then must choose a different color for x_7, say blue, because of the polynomial ${x_7}^2 + x_7x_8 + {x_8}^2 \in \mathcal{G}$. Then we have that x_1 and x_3 must be blue because of the polynomials $x_1 - x_7, x_3 - x_7 \in \mathcal{G}$, and x_4, x_6 must be red because of the polynomials $x_4 - x_8, x_6 - x_8 \in \mathcal{G}$. Finally x_2 and x_5 have the same color, which is a different color from the colors assigned to x_7 and x_8, so x_2 and x_5 are green; this is because the polynomials $x_2 + x_7 + x_8$, and $x_5 + x_7 + x_8$ are in $\mathcal{G}$.

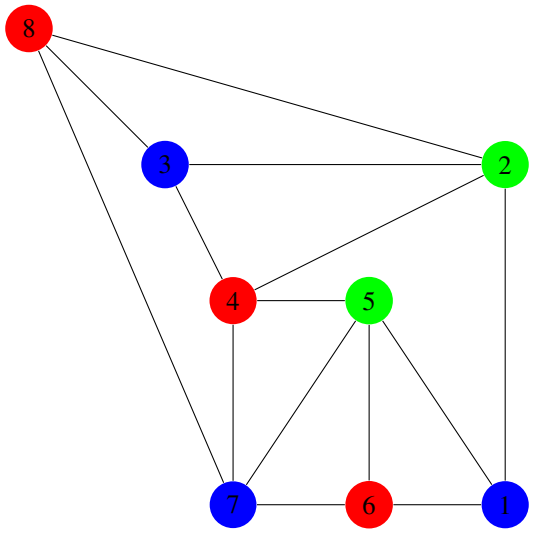

Figure 5: *A unique 3-coloring.*

It is evident from the Gröbner basis in the previous example that there is only one way to color the graph G, up to permuting the colors, and so it should not be too surprising that solving the equations determined by the Gröbner basis is easy. However, if there is more than one possible coloring, the Gröbner basis may look considerably more complicated. We say that a graph is uniquely k-colorable if there is a unique proper k-coloring up to permutation of the colors. In fact, Hillar and Windfeldt showed that unique k-colorability is fairly straightforward to detect using Gröbner bases, but that is the topic of another discussion.[18]

[18] *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, C. Hillar & T. Windfeldt

2.4 Quotient Coloring Ideals

The final characterization of k-colorability that we will provide is to do with quotient ideals.[19] The following two facts prove useful in this regard.

Lemma 2.4.1. Let $I \subseteq k[x_1, ..., x_n]$ be an ideal such that $\mathbf{V}(I)$ is finite. The vector space dimension of $k[x_1, ..., x_n]/I$ over k is greater than or equal to the number of points in the variety $\mathbf{V}(I)$. Furthermore, equality occurs if and only if I is a radical ideal.[20]

Proof. See [*Ideals, Varieties, and Algorithms*, p. 253, Proposition 5.3.7] □

Lemma 2.4.2. $I_{G,k}$ is a radical ideal.

Proof. The proof is similar to the proof of Lemma 2.2.5. □

We define the quotient coloring ideal of a graph G to be the ideal $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$. The following theorem is now immediate.

Theorem 2.4.3. Let G be a graph and fix $k \in \mathbb{Z}^+$. The vector space dimension of $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$ over $\mathbb{C}$ equals the number of proper k-colorings of G.

Proof. According to Lemma 2.4.1, the vector space dimension of $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$ over $\mathbb{C}$ equals the number of points in the variety $\mathbf{V}(I_{G,k})$ since $I_{G,k}$ is a radical ideal. The result now follows since $\mathbf{V}(I_{G,k})$ is the set of all proper k-colorings of G as a result of Lemma 2.3.1. □

And now, the final result.

Theorem 2.4.4. Let G be a graph and fix $k \in \mathbb{Z}^+$. Then G is k-colorable if and only if the vector space dimension of $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$ over $\mathbb{C}$ is nonzero.

Proof. The graph G is not k-colorable if and only if the number of proper k-colorings of G is zero. Theorem 2.4.3 shows that this happens if and only if the vector space dimension of $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$ over $\mathbb{C}$ is zero. □

2.5 Summary and Conclusion

We can summarize the various characterizations of k-colorability presented in this section with the following theorem.

Theorem 2.5.1 (Characterizations of k-colorability)**.** Let G be a graph and fix $k \in \mathbb{Z}^+$.
The following statements are equivalent:

[19] *Algebraic Characterization of Uniquely Vertex Colorable Graphs*, C. Hillar & T. Windfeldt
[20] *Ideals, Varieties, and Algorithms*, Cox et al.

(1) The graph G is not k-colorable.

(2) The graph polynomial f_G belongs to the ideal $I_{n,k}$.

(3) The constant polynomial 1 belongs to the k-coloring ideal $I_{G,k}$.

(4) The vector space dimension of $\mathbb{C}[x_1, ..., x_n]/I_{G,k}$ over $\mathbb{C}$ is zero.

There are many interesting ways to apply techniques from algebraic geometry to learn about the structure of a graph and there are certainly other ways to reduce k-colorability to a problem which can be solved via Gröbner bases. For instance, the edge ideal which is the ideal generated by $x_i x_j$ for all $\{i, j\} \in E$, provides yet another useful approach to capturing the intricacies of a graph.

In the next section we use Gröbner bases to explore the inherent structure of Sudoku puzzles and boards as an application of the theory developed above. The Gröbner basis representations of these boards can then be used to find puzzle solutions or even count the numbers of boards.

3 Sudoku Puzzles

3.1 The Graph of a Sudoku Puzzle

In this section, we will explore the graph coloring problem presented by Sudoku puzzles.

Definition 3.1.1. A *Sudoku board* is a Latin square of order 9, that is a 9×9 grid, in which each square of the grid is filled with an integer from 1 to 9 with no integers repeating in any row or column. A Sudoku board also has the additional condition that the integers 1 through 9 may not repeat in each of the nine 3×3 subgrids that compose the grid.

Definition 3.1.2. A *Sudoku puzzle* is a Sudoku board with given values in some squares. A Sudoku puzzle is *well-posed* if it determines exactly one unique set of values for the Sudoku board.

8							6	4
	9		8		6			5
6	7			9				
1	2		4			6		
	6		2		8		4	
					7		8	1
				5			9	8
9			3		1		5	
2	5							7

Figure 6: An example of a Sudoku puzzle

For example, the Sudoku puzzle in Figure 1 is well-posed.

We can think of the Sudoku board as a graph coloring problem where the graph $S = (V, E)$ of the Sudoku board has 81 vertices corresponding to each square, so $V = \{x_1, ..., x_{81}\}$ (See Figure 7), and the edge set

$$E = \{(i, j) : 1 \leq i < j \leq 81, \text{ and } x_i \text{ and } x_j \text{ are in the same row, column, or block}\}$$

Solutions to the Sudoku will be proper 9-colorings of this graph.

In section 2, we showed that we can use ideals, varieties, and Gröbner bases to find a coloring of a graph. If the graph can be represented by an ideal, I, then the points corresponding to the set of vertices that are contained in $\mathbf{V}(I)$ are the ways we can value or color each of the vertices. We will take this approach when trying to solve the Sudoku Graph coloring problem.

3.2 Ideal Representation of a 9×9 Sudoku Puzzle

We wish to find an ideal which represents the possible solutions to a Sudoku board within the given rules.[21] As in section 2, we can determine the ideal in $\mathbb{C}[x_1, ...x_{81}]$ of the Sudoku graph to be the ideal generated by

$$x_i{}^9 - 1, \text{for all } i \in V$$

$$x_i{}^8 + x_i{}^7 x_j + \cdots + x_i x_j{}^7 + x_j{}^8, \text{for all } (i,j) \in E$$

In the case of a Sudoku board, the "colors" or values of each vertex are the integers 1 through 9. If we consider the colors of our graph to literally be these integers, there are more enlightening ways to determine the ideal which represents the graph of a Sudoku board.

First, assign variables to each of the squares of the Sudoku board, as shown in Figure 7.

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}
x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{27}
x_{28}	x_{29}	x_{30}	x_{31}	x_{32}	x_{33}	x_{34}	x_{35}	x_{36}
x_{37}	x_{38}	x_{39}	x_{40}	x_{41}	x_{42}	x_{43}	x_{44}	x_{45}
x_{46}	x_{47}	x_{48}	x_{49}	x_{50}	x_{51}	x_{52}	x_{53}	x_{54}
x_{55}	x_{56}	x_{57}	x_{58}	x_{59}	x_{60}	x_{61}	x_{62}	x_{63}
x_{64}	x_{65}	x_{66}	x_{67}	x_{68}	x_{69}	x_{70}	x_{71}	x_{72}
x_{73}	x_{74}	x_{75}	x_{76}	x_{77}	x_{78}	x_{79}	x_{80}	x_{81}

Figure 7: Sudoku puzzle variable-assignment

We want to find a set of polynomials in $\mathbb{C}[x_1, \ldots, x_{81}]$ that represents the condition that each of these variables $x_1, \ldots x_{81}$ will have a value in the set of integers $\{1, \ldots, 9\}$. Consider the polynomial:

$$F(z) = \prod_{k=1}^{9} (z - k) \tag{3}$$

[21] This section draws heavily on ideas from Decker and Pfister *A First Course in Algebraic Geometry*, and Gago-Vargas et al. *Sudokus and Gröbner bases: not only a Divertimento*

Plugging in each variable $x_1, \ldots, x_{81}$ into $F(z)$ for z results in a set of 81 distinct polynomials.

$$\{F(x_i) : 1 \leq i \leq 81\} \tag{4}$$

We will call the ideal generated by the polynomials in (4) I_F. Note that F is not a function, it simply represents a set of polynomials. Notice that we can extend the one-variable polynomials $F(x_i)$ given by each x_i to the polynomials, $F_1(x) = \prod_{k=1}^{9}(x_1 - k), F_2(x) = \prod_{k=1}^{9}(x_2 - k), \ldots, F_{81}(x) = \prod_{k=1}^{9}(x_{81} - k) \in \mathbb{C}[x_1, \ldots x_{81}]$ where $x = (x_1, \ldots, x_{81})$. I_F represents the requirement that every vertex in the graph, represented by an x_i must be assigned a value in the set $\{1, \ldots, 9\}$ We have the following proposition:

Proposition 3.2.1. Let I_F be the ideal generated by the 81 $F(x_i)$ polynomials, and let $a = (a_1, a_2, \ldots, a_{81})$. Then $a \in \mathbf{V}(I_F)$ if and only if $a_i \in \{1, \ldots, 9\}$ for all $1 \leq i \leq 81$.

Proof. The proof is relatively straightforward. First, let $a \in \mathbf{V}(I_F)$. Then every polynomial $F_i(x)$ vanishes on a, and every polynomial $F(x_i)$ vanishes on its respective a_i. We know that each $F(x_i)$ has nine distinct roots, namely the integers 1 through 9. So $a_i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for all $1 \leq i \leq 81$. Now, suppose $a_i \in \{1, \ldots, 9\}$ for all $1 \leq i \leq 81$. Since each $F(x_i)$ has the integer roots 1 through 9, $F(a_i)$ vanishes for all a_i. □

Now that we have found a set of polynomials that requires our variables (or vertices) be values with the integers 1 through 9, we must find a set of polynomials that confines our solutions within the row, column, and block conditions of Sudoku.

Let x_i, x_j be two variables in the same row, column, or 3×3 block of the Sudoku, with $1 \leq i < j \leq 81$. We could equivalently say that $(i, j) \in E$. We know x_i and x_j must not have equal values, so $x_i - x_j \neq 0$. Furthermore, if we expand the polynomial $F_i(x_i) - F_j(x_j)$, it turns out $x_i - x_j$ is a factor. So, the polynomials

$$G(x_i, x_j) = (F_i(x_i) - F_j(x_j))/(x_i - x_j), 1 \leq i < j \leq 81 \tag{5}$$

are well defined for x_i and x_j not in the same column, row, or 3×3 block. We will call the ideal generated by the G polynomials I_G. This ideal represents the condition that values 1 through 9 do not repeat in any column, row, or 3×3 block, which we will prove in Proposition 3.2.5. The $G(x_i, x_j)$ polynomials can be extended to polynomials $G_{i,j}(x, y)$ where $x = (x_1, \ldots, x_{81})$ and $y = (y_1, \ldots, y_{81})$ in a similar manner as we extended the F polynomials.

We are well on our way to finding an ideal which represents the set of solutions to a Sudoku board with no given values. Before we prove that the ideals generated by the F and G polynomials does in fact represent a solution to the Sudoku within the given rules, there are some helpful propositions we should know.

Proposition 3.2.2. If A and B are ideals, then $A + B$ is an ideal, and furthermore, if $A = \langle f_1, ..., f_r \rangle$ and $B = \langle g_1, \ldots, g_s \rangle$ then $A + B = \langle f_1, ..., f_r, g_1, \ldots, g_s \rangle$

Proof. The proof can be found in *Ideals, Varieties and Algorithms*, Prop 4.3.2. [22] □

Proposition 3.2.3. If A and B are ideals, then $\mathbf{V}(A+B) = \mathbf{V}(A) \cap \mathbf{V}(B)$.

Proof. The proof can be found in *Ideals, Varieties and Algorithms*, Theorem 4.3.4[23] □

Proposition 3.2.4. Given I_F and I_G as described above, $I_F + I_G$ is an ideal generated by the terms $\langle \{F(x_i) : 1 \leq i \leq 81\}, \{G(x_i, x_j) : 1 \leq i < j \leq 81, \text{ and } x_i, x_j \text{ are in the same row, column, or 3x3 block}\}\rangle$

Proof. The result follows directly from Proposition 3.2.2. □

Now we can prove the following proposition, which shows that I_F and I_G give us an ideal that represents all of the rules of Sudoku, and solves the blank grid.

Proposition 3.2.5. Let I be the ideal $I_F + I_G$, let $\mathbf{V}(I)$ be the variety defined by I, and let $a = (a_1, a_2, \ldots, a_8 1)$ be a point. Then $a \in \mathbf{V}(I)$ if and only if $a_i \in 1, \ldots, 9$, for all $1 \leq i \leq 81$ and $a_i \neq a_j$ for $(i,j) \in E$.[24]

Proof. Suppose $a \in \mathbf{V}(I)$. By Proposition 3.2.3, we have that $\mathbf{V}(I) \subseteq \mathbf{V}(I_F)$. So, by Proposition 3.2.1, every a_i must be in the set $\{1, \ldots, 9\}$. Now, assume a_i and a_j are in the same row, column, or block. We wish to show that $a_i \neq a_j$. Assume for contradiction that $a_i = a_j = b$. We know from (5) that $F(x_i) = (x_i - x_j)G(x_i, x_j) + F(x_j)$. Substituting b for x_j gives $F(b) = (b - x_j)G(b, x_j) + F(x_j) = (b - x_j)G(b, x_j) = 0$, since F vanishes in $\mathbf{V}(I)$. Since $G(b,b) = 0$, this implies that b is a zero of F of order at least two, which is impossible due to the form of F. In the other direction, if the conditions on the right hand side are fulfilled, we know from Prop. 3.2.1 that the F polynomials vanish on a. Furthermore, since $G(x_i, x_j) = (F_i(x_i) - F_j(x_j))/(x_i - x_j)$, every G polynomial vanishes on a as well. So any linear combination of F and G polynomials will also vanish on a, so $a \in \mathbf{V}(I)$. □

We have proved that our ideal holds for determining the possible values of a Sudoku board. But what if instead of a blank Sudoku board, we are instead given a well-posed Sudoku puzzle? Suppose we have a set of given values $\{a_i\}_{i \in L}$ with $L \subset \{1, \ldots, 81\}$. Let I_L be the ideal generated by the terms $\{x_i - a_i\}_{i \in L}$ The sum of two ideals is also an ideal, so the Sudoku puzzle is represented by the ideal

$$I_S = I + I_L = I_F + I_G + I_L \tag{6}$$

which, by Prop 3.2.2, is equivalent to the ideal generated by all of the $F(x_i)$ polynomials, $G(x_i, x_j)$ polynomials, and the appropriate $x_i - a_i$ polynomials.

Now that we have the terms which generate an ideal that represents the Sudoku, we can find a Gröbner basis of the ideal, then find the unique point at which that Gröbner basis vanishes to solve the Sudoku. However, in the 9×9 case

[22] *Ideals, Varieties, and Alogoritms*, Cox, Little, and O'Shea
[23] Ibid.
[24] *A First Course In Algebraic Geometry* Wolfram Decker and Gerhard Pfister.

we have more than 800 polynomials that generate our ideal. We will instead determine the form of a Gröbner basis for a given Sudoku Puzzle.

Proposition 3.2.6. Let S be a well-posed Sudoku with a set of given values $\{a_i\}_{i\in L}$ for a subset $L \subset \{1,\dots,81\}$. With respect to any global monomial ordering, the reduced Gröbner basis of I_S has the shape $x_1 - a_1, ..., x_{81} - a_{81}$.[25]

Proof. We know S has a unique solution $a = (a_1,\dots,a_{81})$ with $a_i \in 1,\dots,9$, for all $1 \leq i \leq 81$ because it is well-posed. By Prop. 3.2.5, $a \in \mathbf{V}(I)$. Additionally, I_L vanishes at points $\{b : b_i = a_i \text{ when } i \in L\}$. Clearly, a is contained in this set, so I_L vanishes on a. Using Prop. 3.2.3, $a \in \mathbf{V}(I_S) = \mathbf{V}(I) \cap \mathbf{V}(I_L)$, and in fact, a is the only element in this intersection, because it is a the Sudoku is well-posed and thus a is a unique solution. Since $a_i \neq 0$ for all $1 \leq i \leq 81$, no constant will vanish on a, i.e. for any constant c, $c \notin \mathbf{I}(\mathbf{V}(I_S))$ However, it is obvious that the polynomials $x_1 - a_1,\dots,x_{81} - a_{81}$ will vanish on a. This set of polynomials contains every variable, and every term has degree 1. Thus, every term of $\mathbf{I}(\mathbf{V}(I_S)$ with higher degree is divisible by some subset of these terms, and can be written as a linear combination of them. So $\mathbf{I}(\mathbf{V}(I_S) = \langle x_1 - a_1,\dots,x_{81} - a_{81}\rangle$. The Nullstellensatz then implies that $\sqrt{I_S} = \langle x_1 - a_1,\dots,x_{81} - a_{81}\rangle$. Thus, I_S contains a power of $(x_i - a_i)$ for each i. Now, choose an arbitrary $a_i \in \{1,\dots,9\}$. Since I_S contains the polynomials $F(x_i)$ we know that the elimination ideal $I_S \cap \mathbb{C}[x_i]$ contains $F(x_i)$ and the appropriate $(x_i - a_i)^m$ contained in I_S. I_S is an ideal in the PID $\mathbb{C}[x_i]$, so it will also contain the gcd of $F(x_i)$ and $(x_i - a_i)^m$, namely $x_i - a_i$. Since $\mathbb{C}[x_i]$ is a PID, and the ideal $I_S \cap \mathbb{C}[x_i]$ does not contain any units, $x_i - a_i$ must be a generator. Since a_i was arbitrary, every elimination ideal $I_S \cap \mathbb{C}[x_i]$ is generated by the corresponding $x_i - a_i$. Since the elimination ideals are generated by the $x_i - a_i$ terms, we know that $x_i - a_i \in I_S$ for all i. It follows that $\langle x_1 - a_1,\dots,x_{81} - a_{81}\rangle \subset I_S$. We also know that $I_S \subset \sqrt{I_S} = \langle x_1 - a_1,\dots,x_{81} - a_{81}\rangle$. Thus, $I_S = \langle x_1 - a_1, ..., x_{81} - a_{81}\rangle$ and the shape of the reduced Gröbner basis is as claimed. □

We can then find the unique point at which this Gröbner basis vanishes. This point $(a_1,\dots a_{81})$ effectively assigns a value 1 through 9 to each variable, and gives a 9-coloring of the Sudoku graph.

3.3 Ideal representation of 4×4 Shidoku Puzzles

In section 4, we will implement a Shidoku solver to solve Shidoku Puzzles. This section examines the theory used in the Shidoku solver

Definition 3.3.1. A *Shidoku Board* is a Latin square of order 4, that is a 4×4 grid, in which each square of the grid is filled with an integer 1, 2, 3, or 4 with no integers repeating in any row or column. A Shidoku board also has the additional condition that the integers 1 through 4 may not repeat in each of the four 2×2 blocks that compose the grid.

The graph of the Shidoku puzzle has a vertex set of 16 vertices, $V = \{x_1,\dots,x_{16}\}$, and an edge set,

$$E = \{x_i x_j : 1 \leq i < j \leq 16, \text{ and } x_i \text{ and } x_j \text{ are in the same row, column, or block}\}$$

[25] *A First Course In Algebraic Geometry*, Wolfram Decker and Gerhard Pfister.

We wish to find 4-colorings of this graph. We assign a variables $x_1, x_2, \ldots, x_{16}$ to each of these squares, or vertices, as illustrated in Figure 8.

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

Figure 8: Shidoku puzzle variable-assignment

Similar to the 9×9 case, we wish to find a set of polynomials which represents the condition that $x_i \in \{1, 2, 3, 4\}$. We can use a similar polynomial to the F polynomials in Section 3.2.

$$f(z) = (z-1)(z-2)(z-3)(z-4) \tag{7}$$

Plugging in our variables gives us 16 polynomials $f(x_i)$ that set the value of each x_i as some integer from 1 to 4. We can rephrase Prop. 3.2.1 for the 4×4 case as follows:

Proposition 3.3.1. Let I_f be the ideal generated by the 16 $f(x_i)$ polynomials, and let $a = (a_1, a_2, \ldots, a_{16})$. Then $a \in \mathbf{V}(I_f)$ if and only if $a_i \in \{1, 2, 3, 4\}$ for all $1 \leq i \leq 16$

Proof. The proof is very similar to the proof of Prop 3.2.1. □

Now, we need to find an ideal which represents the condition that no two squares in the same row, column or 2×2 block have the same number, or "color." This is actually simpler in the 4×4 case, due to the following fact

Fact 3.3.1. The only way to choose 4 numbers from the set {1, 2, 3, 4} which sum to 10 and multiply to 24 is to choose each number 1, 2, 3, and 4 exactly once.[26]

Consider the following polynomials

$$x_k + x_l + x_m + x_n - 10 \tag{8}$$

[26] *Gröbner Basis Representations of Sudoku*, Arnold, Lucas, and Taalman.

$$(x_k \cdot x_) \cdot x_n \cdot x_m) - 24 \tag{9}$$

Where x_k, x_l, x_m, x_n are in the same row, column, or 2×2 block.

Proposition 3.3.2. Let I_g be the ideal generated by the polynomials in (8) and (9), and let $a = (a_1, a_2, a_3, a_4)$ be a point. $a \in \mathbf{V}(I_g)$ if and only if $a_i \neq a_j$ for all $(i, j) \in E$

Proof. The proof is very simple and uses Fact 3.3.1. □

Propositions 3.3.1 and 3.3.2 in mind, the ideal $I = I_f + I_g$ represents the constraints of the Shidoku board with no given values. By Proposition 3.2.3, $\mathbf{V}(I) = \mathbf{V}(I_f) \cap \mathbf{V}(I_g)$, so Proposition 3.3.1 and Proposition 3.3.2 hold for $a \in \mathbf{V}(I)$. So $\mathbf{V}(I)$ gives an appropriate set of solutions for the Shidoku board, or, equivalently, an appropriate coloring of the board.

As in the 9×9 Sudoku case, we may have some values already given. This set can be written as $\{a_i\}_{i \in L}$ for some $L \subset \{1, \ldots, 16\}$. Let I_L be the ideal generated by the polynomials

$$\{x_i - a_i\}_{i \in L} \tag{10}$$

Our ideal I_S which represents the Shidoku puzzle is

$$I_S = I_f + I_g + I_L \tag{11}$$

and is generated by the polynomials $\{f(x_i) : 1 \leq i \leq 16\}$, the polynomials in (8) and (9), and the appropriate $\{x_i - a_i\}_{i \in L}$ for the given puzzle.

The reduced Gröbner basis for a Shidoku board with no given values is given in Arnold, Lucas and Taalman, and contains 17 terms. An example of a Gröbner basis for a given Shidoku Puzzle is given in Section 4, and is used to determine the solutions to a given Shidoku puzzle.

3.4 Conclusion

We have found ideals which represent the valid solutions of a Sudoku board, Sudoku puzzle, and Shidoku puzzle. These ideals can then be used to find a reduced Gröbner basis for a given puzzle. Finding the points at which every term of Gröbner basis vanishes gives us a set of solutions to the Shidoku or Sudoku board. If the Sudoku or Shidoku is well-posed, there will only be one point at which the Gröbner basis vanishes. If we then fill in the Sudoku grid with the values of x_i given by this point, we will have a completed Sudoku puzzle.

There are other applications of Gröbner bases to Sudoku. For instance, it turns out there are approximately 6.671×10^{21} valid Sudoku boards. [27] Arnold, Lucas, and Taalman (2010) use the reduced Gröbner basis of the Shidoku board with no given values to determine that there are 288 possible Shidoku boards.

[27] *Mathematics of Sudoku I*, Felgenhauer and Jarvis.

Another application of Gröbner Bases in Sudoku is discussed in Gagos-Vargas et al. who determine polynomial representations for several popular variations on the Sudoku puzzle.

In section 4, we will apply the polynomial representation of Shidoku found in section 3.3 to solve given Shidoku puzzles.

4 Shidoku Solver

4.1 Overview

Many computer programs have been developed to solve Sudoku puzzles using various strategies. In this section, we will exploit the concept of Gröbner bases to implement a solver for the 4×4 Sudoku variant called Shidoku. Our Shidoku solver will take a Shidoku board with some number of clues and return the board with each cell filled with the correct number.

Recall that the rules of Shidoku are:

1. Each row can only contain each number from 1 to 4 once.
2. Each column can only contain each number from 1 to 4 once.
3. Each 2×2 square can only contain each number from 1 to 4 once.

To solve a Shidoku puzzle with the solver, one can store an incomplete Shidoku puzzle as a one-dimensional array in the source code. For simplicity, empty cells are assumed to contain zero. The `check_shidoku` function in the `shidoku.py` file will check whether the length of the array is 16 or not. It will also check whether the number of clues are sufficient to solve the puzzle or not. The minimum number of clues such that a Shidoku puzzle has a unique solution is determined to be four. We refer the reader to read *Some Results on Su Doku* by Gupta for the proof.

The solver will model the constraints in the Shidoku board as a system of polynomials. It assigns one variable to each cell in the following way.

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

Figure 9: Assign one variable to one cell

Once the Shidoku is determined to have a solution, the solver will call the `encode_shidoku()` function to create a copy of the board with empty cells filled in by the corresponding variables. The first rule of Shidoku shows that the sum and product of cells in the same row must be equal to 10 and 24. Thus, we need to derive eight equations:

1. $a + b + c + d - 10 = 0$
2. $a \cdot b \cdot c \cdot d - 24 = 0$
3. $e + f + g + h - 10 = 0$
4. $e \cdot f \cdot g \cdot h - 24 = 0$
5. $i + j + k + l - 10 = 0$
6. $i \cdot j \cdot k \cdot l - 24 = 0$
7. $m + n + o + p - 10 = 0$
8. $m \cdot n \cdot o \cdot p - 24 = 0$

The solver forms these equations by calling the `generate_row_equations()` function. Similarly, it forms 16 other equations that encode the constraints on the columns and squares by calling the `generate_column_equations()` and `generate_square_equations()`.

After that, the solver will compute the Gröbner bases for the system of constraint equations. We know that the Gröbner bases is a simplification of the constraint equations. Thus, they are easier to solve and have the same solution as the constraint equations. Finally, the solver will solve the polynomials in the Gröbner bases to obtain a number to fill in each of the empty cells.

4.2 An Example

We present an example of how our Shidoku solver solves a Shidoku board with the minimum number of clues. Suppose that we want to solve the following Shidoku board.

0	0	0	1
4	0	0	0
0	0	0	0
0	3	2	0

Figure 10: Assigning zeroes to the empty cells

We will need to represent the Shidoku above in the form of a one-dimensional array. Thus, we code

$$\texttt{initial\_shidoku\_board} = [0, 0, 0, 1, 4, 0, 0, 0, 0, 0, 0, 0, 0, 3, 2, 0] \tag{12}$$

Then, we call `answer = solve_shidoku(initial_shidoku_board)`. Under the hood, the algorithm solves the Shidoku in the following way:

1. It calls `check_shidoku_board(initial_shidoku_board)`, checking whether the Shidoku array has 16 elements and has at least 4 clues. The input passes the test. Thus, it can be solved.

2. Then, it calls `shidoku = encode_shidoku(initial_shidoku_board)` to fill in the empty cells with some variables. The result is as follows.

a	b	c	1
4	f	g	h
i	j	k	l
m	3	2	p

Figure 11: Assigning variables to the empty cells

3. After that, it calls `generate_row_equations(shidoku)`, `generate_column_equations(shidoku)`, and `generate_square_equations(shidoku)` to generate the 24 equations that constraints the Shidoku board:

(a) $a + b + c - 9 = 0$
(b) $a \cdot b \cdot c - 24 = 0$
(c) $f + g + h - 6 = 0$
(d) $4 \cdot f \cdot g \cdot h - 24 = 0$
(e) $i + j + k + l - 10 = 0$
(f) $i \cdot j \cdot k \cdot l - 24 = 0$
(g) $m + p - 5 = 0$
(h) $6 \cdot m \cdot p - 24 = 0$
(i) $a + i + m - 6 = 0$
(j) $4 \cdot a \cdot i \cdot m - 24 = 0$
(k) $b + f + j - 7 = 0$
(l) $3 \cdot b \cdot f \cdot j - 24 = 0$
(m) $c + g + k - 8 = 0$
(n) $2 \cdot c \cdot g \cdot k - 24 = 0$
(o) $h + l + p - 9 = 0$
(p) $h \cdot l \cdot p - 24 = 0$
(q) $a + b + f - 6 = 0$
(r) $4 \cdot a \cdot b \cdot f - 24 = 0$
(s) $i + j + m - 7 = 0$
(t) $3 \cdot i \cdot j \cdot m - 24 = 0$
(u) $c + g + h - 9 = 0$
(v) $c \cdot g \cdot h - 24 = 0$
(w) $k + l + p - 8 = 0$
(x) $2 \cdot k \cdot l \cdot p - 24 = 0$

4. Next, the algorithm will compute the Gröbner bases for the ideal generated by the 24 equations above. The Gröbner function from `sympy` uses the lexicographic ordering with $a > b > c > ... > p$. It returns the following Gröbner bases:

(a) $a - 3$
(b) $b - 2$
(c) $c - 4$
(d) $f - 1$
(e) $g - 3$
(f) $h - 2$
(g) $i - 2$
(h) $j - 4$
(i) $k - 1$
(j) $l - 3$
(k) $m - 1$
(l) $p - 4$

5. Finally, the algorithm equates every element of the Gröbner bases to zero, solve for the corresponding variables, and store the result in the corresponding cells. The complete Shidoku puzzle is as follows.

3	2	4	1
4	1	3	2
2	4	1	3
1	3	2	4

Figure 12: A complete solution

4.3 Conclusion

There are many ways to solve Shidoku puzzles computationally. One could use the backtracking approach or if available, use the power of GPUs and multithreading to accelerate the "guessing" method. In this section, we explored the power of Gröbner bases to simplify the polynomials that constrain the input puzzle. A natural followup to our Shidoku solver discussion is to think about how we can we build a Sudoku solver from the Shidoku solver. Despite of the simplicity of the Shidoku solver's algorithm, extending the algorithm to solve Sudoku puzzles is difficult. One factor to consider is the minimum number of clues needed for a Sudoku puzzle to have a solution. We do not yet know what the number is. It is conjectured that there needs to be 17 clues at least, but no formal proof has been written. The algorithm needs to know the minimum number of clues to determine whether a given Sudoku has a solution or not before it does all the hard work.

References

[1] Arnold, Elizabeth, et al. (2010). Gröbner Basis Representations of Sudoku. *College Math, 41*(2), 101-111.

[2] Cox, David, Little, John, and O'Shea, Donal. (2018) *Ideals, Varieties, and Algorithms*. Springer.

[3] Decker, Wolfram, and Pfister, Gerhard (2013). Sudoku. *A First Course In Algebraic Geometry* (pp. 104-110). Cambridge University Press.

[4] Felgenhauer, Bertram, and Frazer, Jarvis (2006). Mathematics of Sudoku 1.

[5] Gago-Vargas, Jesús, et al. (2006). Sudokus and Gröbner Bases: Not only a Divertimento. *Computer Algebra in Scientific Computing*. (pp. 155-165) Springer.

[6] Mehrle. (2015). A Variety Of Graph Coloring Problems. *Department of Mathematical Sciences*. Carnegie Mellon University.

[7] De Loera, Margulies, et al. (2014). Graph-coloring ideals: Nullstellensatz certificates, Gröbner bases for chordal graphs, and hardness of Gröbner bases. arXiv.

[8] Hillar, Windfeldt. (2007). Algebraic Characterization of Uniquely Vertex Colorable Graphs. arXiv.

[9] Bayer. (1982). The Division Algorithm and the Hilbert Scheme. Harvard University.