Rose-Hulman Undergraduate Mathematics Journal

Volume 21
Issue 1

Article 6

Colorings and Sudoku Puzzles

Katelyn D. May
Murray State University, kmay10@murraystate.edu

Recommended Citation
May, Katelyn D. (2020) "Colorings and Sudoku Puzzles," *Rose-Hulman Undergraduate Mathematics Journal*: Vol. 21 : Iss. 1 , Article 6.
Available at: https://scholar.rose-hulman.edu/rhumj/vol21/iss1/6

Cover Page Footnote

The author expresses a special thanks to Dr. Kelly Pearson for all her feedback and support throughout the research process.

ℝose-Hulman Undergraduate Mathematics Journal
VOLUME 21, ISSUE 1, 2020

Colorings and Sudoku Puzzles

By *Katelyn Danielle May*

Abstract. Map colorings refer to assigning colors to different regions of a map. In particular, a typical application is to assign colors so that no two adjacent regions are the same color. Map colorings are easily converted to graph coloring problems: regions correspond to vertices and edges between two vertices exist for adjacent regions. We extend these notions to 4x4 Sudoku puzzles, known as Shidoku puzzles, and standard 9x9 Sudoku puzzles by demanding unique entries in rows, columns, and regions. Motivated by our study of ring and field theory, we expand upon the standard division algorithm to study Gröbner bases in multivariate polynomial rings. We utilize Gröbner bases of an ideal of a multivariate polynomial ring over a finite field to solve coloring, Shidoku, and Sudoku problems. In the last section, we note Gröbner bases are also well-suited to hypergraph coloring problems.

1 Introduction

We implement the theory of Gröbner bases of ideals of multivariate polynomial rings over finite fields to determine permissible colorings of maps and various Sudoku puzzles. Section 2 delineates the principal notions of abstract algebra necessary to investigate our propositions. We begin this investigation in Section 3, by examining map and graph colorings. Regarding maps, we examine permissible colorings such that no two adjacent regions share identical colorings. There has been an extensive amount of work done in relation to this problem. In particular, the Four Color Theorem states that the regions of any simple planar map can be colored with only four colors in such a way that any two adjacent regions have different colors [3]. However, for this paper we will be concerned with exploring maps that can be colored with three colors.

We transform our maps to graphs in the canonical manner by associating each region with a node and connecting two adjacent regions with an edge. We are then able to show that the map of the counties of West Kentucky cannot be colored with only three colors. We accomplish this through considering a sequence of quadratic polynomials with coefficients in $\mathbb{Z}_3$.

Mathematics Subject Classification. 13P10,12Y05
Keywords. Sudoku, Shidoku, Gröbner Basis

We then extend these algebraic notions to study small Sudoku-type puzzles in Section 4. Elaborating on the idea of colorings, we consider n by n grids with unique entries $1, 2, ..., n$ in each row and column. We generalize the quadratic polynomial studied in the 3-color problem to a sequence of polynomials of degree $n-1$. Using these polynomials we consider Shidoku and Sudoku puzzles in Sections 5 and 6, with the added condition that unique entries must also occur in each region. For both of these cases, our Sage code successfully solves various puzzles that we implement. Previous work done to solve Sudoku puzzles by equations was not successful in that the calculations were not feasible on the computer [5]. However, our success is due to the use of a finite field, but unfortunately still has some limits on feasibility of computation. Finally, in Section 7, we note Gröbner bases are also well-suited to hypergraph coloring problems.

2 Terminology and Background

In this section, we establish and review the basic notions of abstract algebra necessary to study our coloring problems.

Recall that a field is a commutative ring with unity so that every nonzero element has a multiplicative inverse. Familiar examples include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Note that $\mathbb{Z}_p = \{0, ..., p-1\}$ with addition and multiplication modulo p, where p is a prime, is a finite field of order p. More generally, for every prime p and $n \geq 1$ there is a unique finite field, up to isomorphism, of order p^n.

For our intended purpose, we utilize a finite field of order four and a finite field of order nine. We will determine these explicitly but need to utilize the following definitions and theorems which can be found in Gallian [6].

Recall that an integral domain is a commutative ring with unity for which $ab = 0$ implies $a = 0$ or $b = 0$ for all a, b in the ring. In particular, fields are integral domains. We consider multivariate polynomial rings over fields.

Definition 2.1. Let R be a commutative ring with unity. We denote $R[x_1, ..., x_n]$ to be the polynomial ring of n indeterminants with coefficients in R.

Within polynomial rings there exist reducible and irreducible polynomials. In particular, we concern ourselves with irreducible polynomials.

Definition 2.2. [6] Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

The theory of irreducible polynomials is rich. For our purposes, we note that a polynomial $p(x)$ of degree two or three in $F[x]$ where F is a field is irreducible over F if and only if there is no $a \in \mathrm{F}$ for which $p(a) = 0$. Whether a polynomial is irreducible gives insight into the structure of ideals within the polynomial ring. In particular, the following definitions and theorems will allow us to construct a field as a factor ring.

Definition 2.3. [6] A maximal ideal A of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $\mathrm{A} \subseteq \mathrm{B} \subseteq \mathrm{R}$, then B = A or B = R.
In particular, R is a principal ideal domain if every ideal has the form $< a >= \{ra | r \in \mathrm{R}\}$ for some a in R.

A field is trivially a principal ideal domain and a univariate polynomial ring over a field is a principal ideal domain as well. We state the following theorem below and note its proof is an application of the Division Algorithm in $\mathrm{F}[x]$.

Theorem 2.4. *[6] Let* F *be a field. Then* $\mathrm{F}[x]$ *is a principal ideal domain. Indeed, any nonzero proper ideal is generated by any polynomial of minimal degree in the ideal. Let* $p(x) \in \mathrm{F}[x]$. *Then* $< p(x) >$ *is a maximal ideal in* $\mathrm{F}[x]$ *if and only if* $p(x)$ *is irreducible over* F.

We can now construct a field as a factor ring by the following theorem.

Theorem 2.5. *[6] Let* R *be a commutative ring with unity and let* A *be an ideal of R. Then* R/A *is a field if and only if* A *is maximal.*

With the above tools, we are in a position to explicitly construct two fields we will be using.

Example 2.6. We determine a finite field of order four by first constructing an irreducible quadratic polynomial in $\mathbb{Z}_2[x]$. To be irreducible, we need only check that there are no roots in $\mathbb{Z}_2$. It is readily verified that x^2+x+1 is such a polynomial. Therefore, $< x^2+x+1 >$ is a maximal ideal in $\mathbb{Z}_2[x]$ and hence $\mathbb{Z}_2[x]/ < x^2+x+1 >$ is a field of order four. To be explicit, we may write the elements of this field as $\{0, 1, a, a+1\}$. The addition operation is obvious; the multiplication is given by $a^2 = a+1$, $a(a+1) = 1$, and $(a+1)^2 = a$.

Example 2.7. In a similar manner, we determine a finite field of order 9 to be $\mathbb{Z}_3[x]/ < x^2+1 >$, as x^2+1 is an irreducible polynomial over $\mathbb{Z}_3$. We explicitly list its elements as $\{0, 1, 2, a, a+1, a+2, 2a, 2a+1, 2a+2\}$. Again, the addition operation is obvious. We note the following multiplication to show the nonzero elements are units: $2 \cdot 2 = a \cdot 2a = (a+1)(a+2) = (2a+1)(2a+2) = 1$.

We now adjust our focus to generalizing familiar notions to multivariate polynomial rings over fields. Gröbner basis computation is a generalization of three familiar techniques: Gaussian elimination for solving linear systems of equations, the Euclidean algorithm for computing the greatest common divisor of two univariate polynomials, and the Simplex Algorithm for linear programming [11].

As mentioned Gröbner bases generalize the division algorithm for $\mathrm{F}[x]$ which we briefly recall with the following example.

Example 2.8. Let $f = 3x^4 - 5x^3 + 7x^2 + x + 1$ and $g = x^2 + x + 2$ be in $\mathbb{Q}[x]$. We divide f by g to get the quotient $3x^2 - 8x + 9$ and the remainder $8x - 17$ as follows:

$$\begin{array}{r}
3x^2 - 8x + 9 \\
x^2 + x + 2 \overline{)3x^4 - 5x^3 + 7x^2 + x + 1} \\
\underline{3x^4 + 3x^3 + 6x^2} \\
-8x^3 + x^2 + x + 1 \\
\underline{-8x^3 - 8x^2 - 16x} \\
9x^2 + 17x + 1 \\
\underline{9x^2 + 9x + 18} \\
8x - 17
\end{array}$$

and so we have $f = (3x^2 - 8x + 9)g + (8x - 17)$.

In general, given two polynomials $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ and $g = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$, such that $n = \deg(f) \geq m = \deg(g)$, the objective is to multiply g by a term, $\frac{a_n}{b_m}x^{n-m}$, such that the product of the leading term of g and this term cancels the leading term of f in subtraction. This results in a remainder, expressed as h. We call h a reduction of f by g and denote the process of computing h by

$$f \xrightarrow{g} h$$

Note that, in the reduction $f \xrightarrow{g} h$, the degree of the polynomial h is strictly less than the degree of f. We continue this process until the degree of g is greater than the degree of the remainder or the remainder is zero. The succeeding theorem follows.

Theorem 2.9. *[6] Let g be a non-zero polynomial in* $\mathrm{F}[x]$. *Then for any $f \in \mathrm{F}[x]$, there exists q and r in* $\mathrm{F}[x]$ *such that*

$$f = qg + r, \text{ with } r = 0 \text{ or } deg(r) < deg(g).$$

Moreover, r and q are unique (q is called the quotient and r the remainder).

We note that multivariate polynomial division is not as straightforward. Firstly, we need to create an order for the terms within polynomials. Although ordering single variable polynomials is obviously done by degree, there are many ways to order multivariate polynomials.

First recall that the set of power products is denoted by

$$\mathbb{T}^n = \{x_1^{\beta_1}...x_n^{\beta_n} | \beta_i \in \mathbb{N}, i = 1,..,n\}$$

Definition 2.10. A term ordering is a total order $<$ on $\mathbb{T}^n$ such that the following conditions are satisfied:

- $1 < x^\alpha$ for all $x^\alpha \in \mathbb{T}^n$, $x^\alpha \neq 1$
- If $x^\alpha < x^\beta$, then $x^\alpha x^\gamma < x^\beta x^\gamma$, for all $x^\gamma \in \mathbb{T}^n$.

Definition 2.11. We define the lexicographical order on $\mathbb{T}^n$ with $x_1 > x_2 > ... > x_n$ as follows: For

$$\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}^n$$

we define

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \text{the first coordinates } \alpha_i \text{ and } \beta_i \text{ in } \alpha \text{ and } \beta \text{ from} \\ \text{the left, which are different, satisfy } \alpha_i < \beta_i \end{cases}$$

So in the case of two variables x_1 and x_2, we have

$$1 < x_2 < x_2^2 < x_2^3 < ... < x_1 < x_1x_2 < x_1x_2^2 < ... < x_1^2 < ...$$

Definition 2.12. We define the degree lexicographical order (deglex) on $\mathbb{T}^n$ with $x_1 > x_2 > ... > x_n$ as follows: For

$$\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}^n$$

we define

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ and } x^\alpha < x^\beta \text{ with respect to lex} \end{cases}$$

So, with this order, we first order by total degree and we break ties by the lex order. In the case of two variables, we have:

$$1 < x_2 < x_1 < x_2^2 < x_1x_2 < x_1^2 < x_2^3 < x_1x_2^2 < x_1^2x_2 < x_1^3 < ...$$

We are now prepared to extend the Division Algorithm to multivariate polynomials and illustrate with an example.

Example 2.13. Let $f = y^2x + 4yx - 3x^2$, $g = 2y + x + 1 \in \mathbb{Q}[x, y]$. Also let the order be deglex with $y > x$. Then the reduction process in long division format is

$$\begin{array}{r l}
 & \frac{1}{2}yx - \frac{1}{4}x^2 + \frac{7}{4}x \\
2y + x + 1) & y^2x + 4yx - 3x^2 \\
 & y^2x + \frac{1}{2}yx^2 + \frac{1}{2}yx \\
\hline
 & -\frac{1}{2}yx^2 + \frac{7}{2}yx - 3x^2 \\
 & -\frac{1}{2}yx^2 - \frac{1}{4}x^3 - \frac{1}{4}x^2 \\
\hline
 & \frac{1}{4}x^3 + \frac{7}{2}yx - \frac{11}{4}x^2 \\
 & \frac{7}{2}yx + \frac{7}{4}x^2 + \frac{7}{4}x \\
\hline
 & \frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x
\end{array}$$

Note that in the last polynomial, namely $\frac{1}{4}x^3 - \frac{9}{2}x^2 - \frac{7}{4}x$, no term is divisible by the leading term of g and so this procedure cannot continue.

This gives rise to a “long division" or reduction of one polynomial by a list of polynomials by applying long division successively. Note that the order in the list matters.

Let I be the ideal generated by $\{f_1, ..., f_k\}$. An important aspect to note of a Gröbner basis is that it gives membership into the ideal such that $f \in \mathrm{I}$ if and only if the polynomial f reduced by the Gröbner basis of the ideal I produces 0. This extends the Division Algorithm for a single variable where we can use the generator of the ideal to long divide and the remainder determines membership into the ideal.

Buchberger's Algorithm [1] states that given any generating set for I, we can construct a Gröbner basis. This is typically done on a computer as it is computationally expensive.

Theorem 2.14. *[1] For a system of polynomials, $\{f_1, ..., f_k\}$, in $F[x_1, ..., x_n]$ if I is the ideal generated by $\{f_1, ..., f_k\}$ and G is the Gröbner basis of I, then a solution to the system $f_i = 0$ for all $1 \le i \le k$ is a solution to the system $g_i = 0$ for every $g_i \in \mathrm{G}$.*

We note that if $\{1\}$ is the Gröbner basis then there is no solution to the system. In particular, we refer to this as Hilbert's Weak Nullstellensatz [1].

3 Colorings

We implement the theory of Gröbner bases to determine permissible colorings of graphs. Permissible colorings occur when no two adjacent nodes, i.e. nodes that are connected by an edge, within the graph share identical colorings. The intention of the following coloring examples is to determine if the graphs can be colored with three colors under this condition. Working with the theory of Gröbner bases, the following notation will be utilized:

- The colors are labeled 0, 1, and 2.
  - Note that these colors are identified with the elements in $\mathbb{Z}_3$.
- Suppose there are n nodes. For $i = 1, 2, ..., n$, we choose an indeterminate x_i and create the polynomial ring $\mathrm{R} = \mathbb{Z}_3[x_1, ..., x_n]$.
- Colorings of the graph are identified with a point of $\mathbb{Z}_3^n$ such that the i^{th} coordinate of the point corresponds to the color of the i^{th} node.

Additionally, we provide the following lemmas which are adapted from exercises in Kreuzer and Robbiano [7].

Lemma 3.1. *For a 3-coloring, the set of zeros of the ideal $(x_1^3 - x_1, ..., x_n^3 - x_n)$ is the set of all possible colorings disregarding the defined condition that adjacent nodes cannot share identical colorings.*

Proof. Note that $x_i = 0, x_i = 1$, or $x_i = 2$ for $i = 1, 2, ..., n$.

Case 1: Suppose $x_i = 0$. Then $x_i^3 - x_i = 0 - 0 = 0 \in \mathbb{Z}_3$.
Case 2: Suppose $x_i = 1$ Then $x_i^3 - x_i = 1 - 1 = 0 \in \mathbb{Z}_3$.
Case 3: Suppose $x_i = 2$ Then $x_i^3 - x_i = 2 - 2 = 0 \in \mathbb{Z}_3$.
Thus the set of all possible colorings is the set of zeros of the ideal $(x_1^3 - x_1, ..., x_n^3 - x_n)$. □

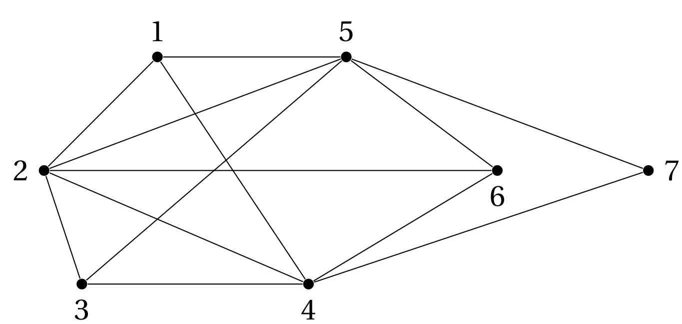
Lemma 3.2. *For a 3-coloring, the colors of the i^{th} and j^{th} node in the graph are different if and only if the coloring is a zero of the polynomial $x_i^2 + x_i x_j + x_j^2 + 2$.*

Proof. Assume the i^{th} and j^{th} node in the graph have different colors. Thus, $x_i \neq x_j$. We then consider the cases this generates to see that in each case, the coloring is a zero of the polynomial $x_i^2 + x_i x_j + x_j^2 + 2$:
Case 1: Suppose $x_i = 0$ and $x_j = 1$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 0 + 0 + 1 + 2 = 0 \in \mathbb{Z}_3$.
Case 2: Suppose $x_i = 0$ and $x_j = 2$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 0 + 0 + 1 + 2 = 0 \in \mathbb{Z}_3$.
Case 3: Suppose $x_i = 1$ and $x_j = 2$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 1 + 2 + 1 + 2 = 0 \in \mathbb{Z}_3$.

Conversely, we assume the coloring is a zero of the polynomial $x_i^2 + x_i x_j + x_j^2 + 2$. Thus $x_i^2 + x_i x_j + x_j^2 + 2 = 0$. Suppose the i^{th} and j^{th} node in the graph have the same color and consider the cases this generates.
Case 1: Suppose $x_i = 0$ and $x_j = 0$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 0 + 0 + 0 + 2 = 2 \neq 0 \in \mathbb{Z}_3$.
Case 2: Suppose $x_i = 1$ and $x_j = 1$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 1 + 1 + 1 + 2 = 2 \neq 0 \in \mathbb{Z}_3$.
Case 3: Suppose $x_i = 2$ and $x_j = 2$. Then $x_i^2 + x_i x_j + x_j^2 + 2 = 1 + 1 + 1 + 2 = 2 \neq 0 \in \mathbb{Z}_3$.
Hence, a contradiction occurs. Thus, the colors of the i^{th} and j^{th} node in the graph are different. □

For the following examples, to determine all the permissible 3-colorings,we implement the condition which states that an edge cannot connect nodes of identical colorings in accordance to the given graphs in Sage [10].

Example 3.3. [7] We are interested in the various possible colorings of the following graph when working with three different colors.



We begin by establishing that we are working within the realm of polynomial ring of seven indeterminants with coefficients in a finite field of order 3. We create a list of all edges of the graph so that if $\{i, j\}$ is an edge, we put the polynomial $x_i^2 + x_i x_j + x_j^2 + 2$ in the list L. Next, we attach the association of the first node being of color "0" and the second node being of color "1" to list L by appending x_1 and $x_2 - 1$ to the list L. Lastly, we define the ideal I to be generated by L and compute B to be the Gröbner bases with the ideal I. The code follows below:

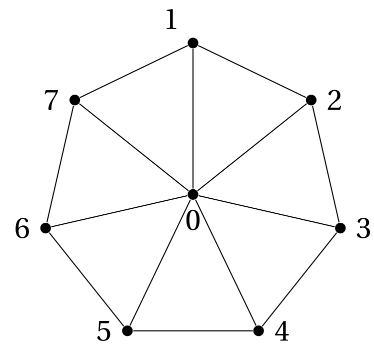
```
k=FiniteField(3)
R=PolynomialRing(k, 8,"x")
L=[]
var('i j')
assume(i, 'integer')
assume(j, 'integer')
def E(i,j):
return (R.gen(i))^2 + (R.gen(j))^2 + (R.gen(i))*(R.gen(j)) + 2
L.append(E(1,2))
L.append(E(1,4))
L.append(E(1,5))
L.append(E(2,3))
L.append(E(2,4))
L.append(E(2,5))
L.append(E(2,6))
L.append(E(3,4))
L.append(E(3,5))
L.append(E(4,6))
L.append(E(4,7))
L.append(E(5,6))
L.append(E(5,7))

p=R.gen(1)
L.append(p)
p=R.gen(2)-1
L.append(p)

I=Ideal(L)
B=I.groebner_basis(); B
```

From this code we find that the graph has two permissible colorings

- $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 2, x_5 = 2, x_6 = 0, x_7 = 0$
- $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 2, x_5 = 2, x_6 = 0, x_7 = 1$

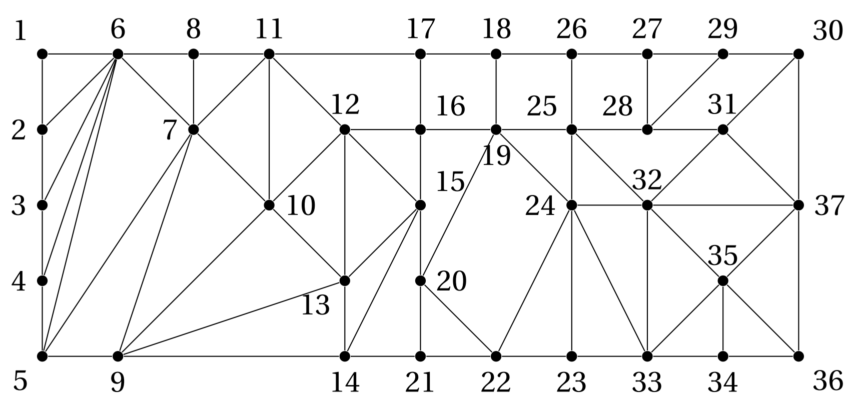
with the specified conditions.

Example 3.4. [7] We now consider the graph constructed by joining a center point of a regular 7-gon to each of its vertices. This specific graph has eight nodes and fourteen edges.



As in the preceding example, we are interested in finding all possible colorings with three different colors. In this case, our code tells us that the Gröbner basis is $\{1\}$ which implies the ideal is the full polynomial ring. By Hilbert's Weak Nullstellensatz, we conclude this graph cannot be colored with three colors. This conclusion can be readily confirmed visually. The center vertex, labeled 0, receives one of the colors. Then the outside vertices would need to alternate the remaining two colors. However, since there is an odd number of such vertices, one of the edges would connect nodes of identical colors.

Example 3.5. We now construct a graph that represents the connections between the counties in West Kentucky.



There are thirty-seven nodes, each representing a different county, and seventy-seven edges. We start labeling the counties with node 1 representing Fulton county through node 37 representing Hart county. Again we are interested in determining whether it is possible to color this graph with three colors and, if so, whether this coloring is unique. Thus, we implement coding in Sage with the conditions noted above. We again see the Gröbner basis is $\{1\}$ and apply the Weak Nullstellensatz to conclude that this graph has no possible colorings with such conditions.

4 Small Sudoku-type puzzles

We consider a 3 by 3 grid in which a permissible coloring occurs where each row and each column consists of three distinct "colors", or numbers. Firstly, we examine how many total permissible 3-colorings a 3 by 3 grid generates.

Theorem 4.1. *There are twelve permissible 3-colorings of the 3 by 3 grid.*

Proof. The first row is determined by a permutation of three objects. Hence, there are six distinct colorings of the first row. The second row must be a derangement of the top row. Therefore, there are two choices for a permissible coloring of the second row. Lastly, once the first two rows are determined, the bottom row is fixed. Thus, there are a total of twelve permissible colorings. □

Next, we investigate the conditions of 3 by 3 Sudoku puzzles which produce unique colorings.

Theorem 4.2. *Once three entries that are not on a diagonal nor existing on a common row or column are given, the* 3*-coloring is uniquely determined.*

Proof. Since any three entries not on a diagonal nor existing on a common row or column implies at least two of the entries are on a row or column together, we may assume, without loss of generality, that the first and second entry of the 3 by 3 grid are given. By utilizing Sage, we see the Gröbner basis is given by $\{x_9^2 - x_9, x_1, x_2 - 1, x_3 + 1, x_4 + x_9 + 1, x_5 + x_9, x_6 + x_9 - 1, x_7 - x_9 - 1, x_8 - x_9 + 1\}$. From this, it is known that any other element, not on the first row will uniquely determine the coloring.

□

The 3 by 3 grid can be generalized to a p^n by p^n grid for any prime p by utilizing Gröbner bases to study the different colorings. We note that it is necessary to have a finite field for the coefficient ring and thus restrict ourselves to powers of primes. Thus, we generalize our polynomial from the three color setting to a more general setting.

Theorem 4.3. *Consider a graph with p^n colors with p a prime and let $\mathbb{F}$ be a field of order p^n. The colors of the i^{th} and j^{th} node in the graph are different if and only if the coloring is a zero of the polynomial $\prod_{\alpha \in \mathbb{F} \setminus \{0\}} (x_i - x_j - \alpha)$.*

Similar to above, we investigate the conditions of p by p Sudoku puzzles which produce unique colorings. One may conjecture that if $\frac{p(p-1)}{2}$ entries are given with no p entries given in one row, column, or diagonal, then there is a unique permissible coloring of the p by p grid. However, we can provide ten entries in a 5 by 5 grid which yield more than one permissible coloring:

Example 4.4. We consider the following 5 by 5 puzzle:

0	1	2	3	
2	3	4		
3	4			
4				

Note that there is not a unique permissible coloring for the above puzzle with ten entries as determined by running Sage and calculating a Gröbner basis, which is given by

$x_{15}^2 - 2x_{15} - x_{20} - x_{25} - 1$
$x_{15}x_{19} - x_{15} - 2x_{19} + 2$
$x_{19}^2 - x_{19}$
$x_{15}x_{20} + 2x_{15} + x_{20} - 2x_{25} - 1$
$x_{19}x_{20} + 2x_{19} + 2x_{20} + 2x_{25} + 2$
$x_{20}^2 - x_{20} - 2x_{25} + 1$
$x_{15}x_{25} - x_{15} - 2x_{20} + x_{25}$
$x_{19}x_{25} - x_{19} + 2x_{20} + 2x_{25} + 2$
$x_{20}x_{25} + 2x_{20} + 2x_{25} - 1$
$x_{25}^2 + x_{25} - 2$
x_1
$x_2 - 1$
$x_3 - 2$
$x_4 + 2$
$x_5 + 1$
$x_6 - 1$
$x_7 + 2$
$x_8 + 1$
$x_9 - x_{15} - x_{20} - x_{25} - 1$
$x_{10} + x_{15} + x_{20} + x_{25} - 1$
$x_{11} + 2$
$x_{12} + 1$
$x_{13} - x_{19} - x_{20} - x_{25} - 1$
$x_{14} + x_{15} + x_{19} + x_{20} + x_{25} - 2$

$x_{16}+1$
$x_{17}-2$
$x_{18}+x_{19}+x_{20}+1$
$x_{21}-2$
x_{22}
$x_{23}+x_{25}+1$
$x_{24}+1$

However, adding a color to the x_{25} position yields a unique permissible coloring, also demonstrated by our Sage code.

Observe that the general coloring problem is applicable for any natural number n as well. Similarly to Theorem 4.1, we examine the number of permissible n-colorings that exist in a basic n by n grid.

Definition 4.5. For a natural number n, a derangement of n is a permutation of n which has no fixed point. We denote $\mathrm{D}(n)$ to be the number of derangements of n. It is known that $\mathrm{D}(n) = n!\sum_{i=0}^{n}\frac{(-1)^i}{i!}$.

Theorem 4.6. *The number of permissible n-colorings of the n by n grid, denoted $\mathrm{C}(n)$, is strictly less than $n!\prod_{i=0}^{n-3}[\mathrm{D}(n)-i]$ for $n>3$.*

Remark 4.7. In the case where $n=3$, $\mathrm{C}(n)$ is equal to the formula. See Theorem 4.1.

Proof. The first row is determined by a permutation of n objects. Hence, there are $n!$ distinct colorings of the first row. Subsequent rows must be distinct derangements of the first row. However, when $n>3$, these derangements result in an occurrence of identical colorings within one or more more columns in the following rows. Note, this formula precisely calculates the number of possible derangements for the second row, since a derangement has no fixed points. However, when moving on in the calculation, this formula calculates these same derangements, only discarding the exact derangement(s) above it. Although these derangements do not coincide in the positioning of any object with the first row, repetition amongst some derangements occur in subsequent rows. When $n>3$, there are at least $(n-1)(n-2)$ derangements that coincide in the positioning of an object within the first column. Note, the object in the second position cannot be the same as the object in the first position or the object located in the second position in the first row. Thus, the total number of permissible colorings is strictly less than $n!\prod_{i=0}^{n-3}[\mathrm{D}(n)-i]$ when $n>3$.

□

5 Shidoku

Next, we consider 4 by 4 Shidoku puzzles in which we additionally require each 2 by 2 region to have unique entries. We will denote each “color", or number, by an element from $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. Since we are switching from a 3-coloring to a 4-coloring it is important to redefine our equations. We note that two vertices x_i and x_j have different colors if and only if

$$E(i,j)=\prod_{\alpha\in F\setminus\{0\}}(x_i-x_j-\alpha)=0.$$

As with the p by p puzzles, we investigate the conditions of Shidoku puzzles which produce unique colorings.

Theorem 5.1. *If every element is represented and there is at least one entry in each region, column, and row, then the Shidoku puzzle has a unique solution.*

Proof. These conditions generate sixteen particular cases within the Shidoku grid. Without loss of generality, we consider the case in which x_1, x_7, x_{10}, x_{16} are given. Computing a Gröbner basis gives way to a system of linear equations. Thus, the puzzle is uniquely determined. Any other case is merely a renumbering. □

Example 5.2. We consider the following Shidoku puzzle:

1			
		2	
	3		
			4

Note that this puzzle meets the conditions in theorem 5.1. Logically, one can conclude that the solution to the puzzle is:

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

Nevertheless, it is important to note that our Sage code confirms these results. One may conjecture that a Shidoku puzzle only has unique solution with such conditions defined in Theorem 5.1. However, we can provide a Shidoku puzzle with different initial conditions that produces a unique solution.

Example 5.3. Consider the following Shidoku puzzle:

2			
		1	
	4		3

As in example 5.2, one can solve this Shidoku puzzle with logic. However, our Sage code works quickly to solve puzzles like this one, and exemplifies the application of an abstract concept to a familiar puzzle. The Gröbner basis is given by

$x_1 + a + 1$
x_2
$x_3 + a$
$x_4 + 1$
$x_5 + 1$
$x_6 + a$
$x_7 + a + 1$
x_8
$x_9 + a$
$x_{10} + 1$
x_{11}
$x_{12} + a + 1$
x_{13}
$x_{14} + a + 1$
$x_{15} + 1$
$x_{16} + a$

Thus, confirming the solution to the given puzzle is

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

Next, we examine how many total permissible 4-colorings a Shidoku puzzle generates. We provide an explicit, straightforward argument using a Gröbner basis. Another proof can be found in Arnold [2].

Theorem 5.4. *There are 288 permissible 4-colorings of Shidoku.*

Proof. The first row is determined by a permutation of four objects. Hence, there are twenty-four distinct colorings of the first row. We then fix the first row as $\{1,2,3,4\}$ and the second row beginning with a 3 and calculate the Gröbner basis which is a collection of polynomials:

$x_{14}^2 + ax_{14}$
$x_{12}^2 + x_{12} + (a+1)x_{14}$
$x_{14}x_{16} + ax_{14} + ax_{16} + (a+1)$
$x_{15}^2 + (a+1)x_{14} + ax_{15} + (a+1)x_{16} + (a)$
$x_{12}x_{15} + x_{15}x_{16} + (a+1)x_{12} + (a+1)x_{14} + ax_{15}$
$x_{14}x_{15} + x_{15}x_{16} + ax_{15}$

$x_{12}x_{14} + ax_{14}$
$x_{12}x_{16} + ax_{12} + ax_{16} + (a+1)$
$x_{16}^2 + (a+1)x_{14} + x_{16} + 1$
x_1
$x_2 + 1$
$x_3 + a$
$x_4 + (a+1)$
$x_5 + a$
$x_6 + (a+1)$
$x_7 + x_{12} + x_{16} + a$
$x_8 + x_{12} + x_{16} + a + 1$
$x_9 + x_{14} + x_{15} + x_{16} + a$
$x_{10} + x_{14} + a$
$x_{11} + x_{12} + x_{15} + x_{16}$
$x_{13} + x_{14} + x_{15} + x_{16}$

We are interested in setting these polynomials equal to zero and solving the system of equations.

First we consider $x_{14}^2 + ax_{14} = 0$, we see that x_{14} is either 0 or a. Then since $x_{12}^2 + x_{12} + (a+1)x_{14} = 0$, we consider our possible cases when x_{14} is 0 or a. If $x_{14} = 0$, then $x_{12} = 0$ or $x_{12} = 1$. If $x_{14} = a$, then $x_{12} = a$ or $x_{12} = a+1$. Next we consider the equation $x_{14}x_{16} + ax_{14} + ax_{16} + a + 1 = 0$ with the possible values of x_{14} again. If $x_{14} = 0$, this equation yields $x_{16} = a$. If $x_{14} = a$, then $x_{16} = 0$. Finally we consider $x_{15}^2 + (a+1)x_{14} + ax_{15} + (a+1)x_{16} + (a) = 0$ with our possible values for x_{14} and x_{16}. We conclude that x_{15} is either 1 or $a+1$.

We now have eight combinations that are possibles for $x_{12}, x_{14}, x_{15}, x_{16}$, as shown in Table 1. However, by considering the equation

Table 1:

x_{12}	x_{14}	x_{15}	x_{16}
0	0	1	a
0	0	a+1	a
a	a	1	0
a	a	a+1	0
a+1	a	1	0
a+1	a	a+1	0
1	0	1	a
1	0	a+1	a

$$x_{12}x_{15} + x_{15}x_{16} + (a+1)x_{12} + (a+1)x_{14} + ax_{15} = 0$$

we may may eliminate the cases in Table 2 since they are not solutions.

Table 2: Not solutions

x_{12}	x_{14}	x_{15}	x_{16}
1	0	1	a
1	0	a+1	a

In a similar fashion, we have six solutions possible when the first row is fixed at $\{1,2,3,4\}$ and the first entry of the second row is 4. We now count to see that there are $4! \cdot 2 \cdot 6 = 288$ possible Shidoku puzzles.

□

6 Sudoku

Classical Sudoku puzzles consist of a 9 by 9 grids with nine regions. We want to have unique entries within each row, column, and 3 by 3 region. We will be working over a finite field of order nine as discussed earlier. Recall the field will be isomorphic to $Z_3[x]/\langle x^2+1\rangle$, and we denote the elements by $\{0,1,2,a,a+1,a+2,2a,2a+1,2a+2\}$. As in Shidoku, we note that two vertices x_i and x_j have different colors if and only if

$$\mathrm{E}(i,j) = \prod_{\alpha \in \mathrm{F}\setminus\{0\}} (x_i - x_j - \alpha) = 0.$$

Continuing work with Gröbner bases, we want to conclude if our code in Sage is applicable to these 9 by 9 Sudoku puzzles.

Example 6.1. We first consider a randomly generated Sudoku puzzle

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

Using our code, we obtain a unique solution as follows:

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

Example 6.2. It has been shown in McGuire [8] that the minimal number of clues possible to yield a unique solution is seventeen. We found such a Sudoku puzzle and tried it in our Sage code. However, due to computational constraints, we were not able to produce a solution. Here is one such puzzle:

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

We then considered another type of question. What is the maximum number of clues that can be given which yield a unique solution but that removing any one of the clues results in multiple solutions to the Sudoku puzzle?

Example 6.3. It has been shown possible to provide forty clues for a Sudoku puzzle which yields a unique solution but that removing any one of the clues results in more than one solution to the puzzle in the High Clue Tamagotchis forum [4]. One such puzzle is:

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

We consider this puzzle and our Sage code verifies there is a unique solution. Moreover, removing any of these clues results in more than one solution to the puzzle as can be seen by looking at the Gröbner basis provided by the Sage output.

7 Further Studies

There are various higher dimensional Sudoku-style puzzles, for example 8 by 8 and 27 by 27 boards. Theoretically, the Gröbner basis technique would work on any of these types of boards. In particular, the 8 by 8 board would be more manageable than the standard 9 by 9 board.

We may also apply our techniques to hypergraph colorings.

Definition 7.1. A hypergraph is a pair (V, E) where V is a set of vertices and E is a set of nonempty subsets of V called hyperedges.

A hypergraph coloring is assigning $\{1,2,\ldots,k\}$ to each vertex of a hypergraph so that each hyperedge contains at least two vertices of distinct colors. In this case, the hypergraph is k-colorable.

Of particular interest are 2-colorable hypergraphs, first introduced in Miller [9]. To illustrate the effectiveness of our technique we consider the Fano plane and show it is not 2-colorable in the following example.

Example 7.2. In simplest terms, the Fano plane is the hypergraph on seven vertices $\{1,2,\ldots,7\}$ with the seven hyperedges given by

$$\{\{1,2,3\},\{1,6,5\},\{3,4,5\},\{1,7,4\},\{2,7,5\},\{3,7,6\},\{2,4,6\}\}.$$

For each hyperedge $\{i, j, k\}$ we know the following: $(x_i - x_j - 1)(x_i - x_k - 1)(x_j - x_k - 1) = 0$ if and only if there are at least two colors in $\{i, j, k\}$. By programming these seven polynomials into Sage and computing the Gröbner basis of $\{1\}$, we see that there is no solution; hence, there is no 2-coloring of the Fano plane.

Acknowledgments

The author expresses a special thanks to Dr. Kelly Pearson for all her feedback and support throughout the research process.

References

[1] Adams, Williams and Loustaunau, Philippe. *An Introduction to Gröbner Bases*. 1994. American Mathematical Society. Providence,RI.

[2] Arnold, Elizabeth, Lucas, Stephen, and Taalman, Laura. *Gröbner Basis Representations of Sudoku*. 2010. The College Mathematics Journal. vol. 41. pp. 101-112.

[3] Biggs, Norman, Lloyd, E. Keith, and Wilson, Robin. *Graph Theory 1736-1936*. 1976. Clarendon Press Publication. Oxford, United Kingdom.

[4] Dobrichev et al. *The New Sudoku Player's Forum*. 2014. Enjoy Sudoku. pp. 10. http://forum.enjoysudoku.com/high-clue-tamagotchis-t30020-135.html.

[5] Gago-Vargas, Jesús, Hartillo-Hermoso, Maria, Martín-Morales, Jorge, and Ucha-Enriquez, Jose. Sudokus and Gröbner Bases: Not only a Divertimento. 2006. *Computer Algebra in Scientific Computing* vol. 4194. pp. 155-165.

[6] Gallian, Joseph. *Contemporary Abstract Algebra*. 2010. Brooks/Cole. Belmont,CA. 7th edition.

[7] Kreuzer, Martin and Robbiano, Lorenzo. *Computational Commutative Algebra 1*. 2000. Springer. Berlin, Germany.

[8] McGuire, Gary, Civario,Gilles, and Tugemann, Bastian. There is no 16-Clue Sudoku: Solving the Sudoku Minimum Number of Clues Problem Via Hitting Set Enumeration. 2014. *Experimental Mathematics* vol. 23. pp. 190-217.

[9] Miller, E. On a Property of Families of Sets. 1937. *Comptes Rendus Varsovie* vol. 30. pp. 31-38.

[10] Stein, William. *Sage Mathematics Software*. (Version 8.6). 2019. The Sage Development Team. `http://www.sagemath.org`.

[11] Sturmfels, Bernd. What is a Gröbner Basis. 2005. *Notices of the American Mathematical Society* vol. 52. pp. 1199-1200.

Katelyn Danielle May
Murray State University
kmay10@murraystate.edu