A VARIETY OF GRAPH COLORING PROBLEMS

DAVID MEHRLE

Gröbner Bases and the Ideal Membership Problem

Let k be a field and let $A = \mathbb{C}[x_1, \dots, x_n]$. For the set of common zeros of elements of an ideal $I \subseteq A$, we write $\mathbf{V}(I)$. For the ideal of polynomials which vanish on a set $V \subseteq k^n$, we write $\mathbf{I}(V)$.

Given an ideal $I \subseteq A$, the ideal membership problem is the problem of determining whether or not a given $f \in A$ is an element of the ideal I. This is difficult because the division algorithm can badly fail in this ring. The next example demonstrates that we cannot determine if f is in I by simply dividing by the generators of this ideal.

Example 1. *Consider $A = \mathbb{C}[x, y, z]$. Let us fix a monomial order $<$ on elements of A wherein $x^\alpha > x^\beta$ if and only if the first nonzero entry in $\alpha - \beta$ is positive. Let $I = (g_1, g_2)$ where $g_1 = x^2y - z$ and $g_2 = xy - 1$, and let $f = x^3 - x^2y - x^2z + x$. Note that*

$$f = x^2 g_1 + (-x^3 - x) g_2 \ ,$$

so $f \in I$. Yet, long-dividing f by g_1 we find a remainder of $x^3 - x^2z + x - z$, which is not divisible by g_2, and likewise when long-dividing f by g_2 we find a remainder of $x^3 - x^2z$, which is not divisible by g_1.

This problem can be solved by finding a special kind of generating set for the ideal I. These generating sets are known as Gröbner Bases. Let $\mathrm{LT}(f)$ for $f \in A$ denote the leading term under a monomial order $<$, and let $\mathrm{LT}(I)$ denote the ideal generated by $\{\mathrm{LT}(f) \mid f \in I\}$.

Definition 1 (Gröbner Basis)**.** *Let $I \subseteq A$ be an ideal. Given a monomial ordering $<$, a subset $G = \{g_1, g_2, \dots, g_t\} \subseteq I$ is a Gröbner Basis for I if and only if*

(1) *G generates I, and*
(2) *$(LT(g_1), LT(g_2), \dots, LT(g_t)) = LT(I)$.*

We are guaranteed that a Gröbner basis always exists for any ideal by the Hilbert Basis Theorem. Why do Gröbner bases fix the issue we had before?

Fact 1. *Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq A$ and let $f \in A$. Then there is a unique $r, g \in A$ such that*

(1) *No term of r is divisible by any of $LT(g_1), \dots, LT(g_t)$, and*
(2) *There is $g \in I$ such that $f = g + r$.*

Proof. When dividing by G, we are guaranteed that each term of the remainder r is not divisible by anything in the ideal I, because the leading terms of the g_i generate $\mathrm{LT}(I)$. This also gives us the existence of some $g \in I$. To show uniqueness, note that for any two such remainders r_1 and r_2, their difference satisfies $r_1 - r_2 \in I$. But no term of either r_1 or r_2 is divisible by any element of I, so $r = 0$. $\square$

This fact can be restated as: $f \in I$ if and only if f vanishes when divided by a Gröbner basis for I.

Example 2. *In the situation of example 1, a Gröbner basis for the ideal* $I = (g_1, g_2)$ *is given by* $h_1 = yz - 1$ *and* $h_2 = x - z$*. Note that* $h_1 = g_1 - xg_2$ *and* $h_2 = -yg_1 + (1 + xy)g_2$*, so* $I \subseteq (h_1, h_2)$*, but also* $g_1 = xh_1 + (1 + xy)h_2$ *and* $g_2 = h_1 + yh_2$*. So* $(h_1, h_2) = (g_1, g_2) = I$*. Furthermore, it can be checked that the leading terms ideal* $LT(h_1, h_2) = (LT(h_1), LT(h_2))$*, so it is indeed a Gröbner basis. Upon long dividing* f *by* h_1 *and* h_2*, we find no remainder, so* $f \in I$*.*

There are several algorithms for computing Gröbner bases, such as Buchberger's algorithm, but they are quite technical and the proofs of correctness are none too enlightening. See, for instance, [E$^+$95] or [CLO07]. Next, we illustrate some neat applications of Gröbner bases to graph coloring.

Graph Coloring via Ideal Membership

Let $G = (V, E)$ be a graph. 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. Essentially, we reduce decidability of k-colorability to an ideal membership problem, which we know how to solve from the above. First, some basic definitions; for more, visit [Die00].

Definition 2 (Colorability, Chromatic Number)**.** *A graph* G *is* k*-colorable if there is an assignment of* k *distinct colors to each of the vertices such that no two adjacent vertices have the same color. The chromatic number* $\chi = \chi(G)$ *is the smallest number such that the graph can be colored with* χ *colors.*

Given some k, the question that we are interested in answering is whether or not the graph G is k-colorable. So we want to transform information about our graph into information about a set of polynomials; we work in $\mathbb{C}[V]$, with a variable for each vertex of the graph. This also motivates the following definition.

Definition 3 (Graph Polynomial)**.** *The graph polynomial* f_G *associated to the graph* $G = (V, E)$ *is an element of the ring* $\mathbb{C}[V]$*, given by:*

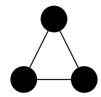
$$f_G \;:=\; \prod_{\{u,v\}\in E} (u - v)$$

The graph polynomial has a lot of interesting properties related to the graph, but we're only interested in a few of them. The next theorem describes the reduction from graph colorability decidability to ideal membership.

Theorem 1. *Fix* k *a positive integer. Let* I *be the ideal generated by the polynomials* $v^k - 1$ *for* $v \in V$*. The graph* G *is* k*-colorable if and only if* $f_G \notin I$*.*

This criterion gives us a very testable algorithm to determine if a graph is k-colorable: simply compute a Gröbner basis for I, and then divide f by this basis. Some intuition: imagine taking the colors to be k-th roots of unity. So for each vertex, we to assign a color, which corresponds to setting each variable to a k-th root of unity. However, if two adjacent are assigned the same color, f_G will vanish.

Example 3. *Consider the graph* G *displayed below, with nodes* u*,* v*,* w*. This graph is clearly three-colorable but not two colorable, but to test the feasibility of* *our algorithm let's apply Theorem 1.*



Let R be the ring $\mathbb{C}[u, v, w]$, and consider the ideal $I = (u^3 - 1, v^3 - 1, w^3 - 1)$. This is also a Gröbner basis for the ideal I. The graph polynomial of G is $f_G = (u - v)(u - w)(v - w)$. Note that none of the terms of f_G are cubic in any of the variables, and hence f_G is not divisible by any of the elements of our Gröbner basis. Hence, G is three-colorable. But it is not two-colorable, because

$$f_G = (v - w)(u^2 - 1) + (w - u)(v^2 - 1) + (u - v)(w^2 - 1) \ .$$

To prove Theorem 1, we will use the Nullstellensatz, a classical theorem of algebraic geometry, stated below:

Theorem 2 (Hilbert's Nullstellensatz)**.** *Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal, and let $f \in k[x_1, \ldots, x_n]$. If the polynomial f vanishes on $\mathbf{V}(I)$, then there is some integer m such that $f^m \in I$.*

Now we present the proof of Theorem 1, following [AT99].

Proof of Theorem 1. If G is k-colorable, there is an assignment of colors to vertices such that no two adjacent vertices have the same color. This corresponds to a point $a \in \mathbf{V}(I)$ such that $f(a) \neq 0$. Since any linear combination of the generators of I will vanish at a, but f does not, then f cannot be in the ideal I.

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

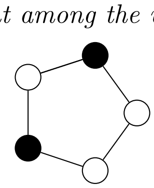
Finding the chromatic number

Here, we will discuss the covering ideal of a graph and its connection to the chromatic number of a graph. Before we do anything else that is interesting, we must introduce a few new definitions.

Definition 4 (Independent Set, Vertex Cover)**.** *For a graph $G = (V, E)$, an independent set is a subset of vertices $U \subseteq V$ such that there are no edges between any two vertices in U. The independence number $\alpha = \alpha(G)$ is the size of the largest independent set. A subset $W \subseteq V$ is a vertex cover if $W \cap e \neq \emptyset$ for all $e \in E$.*

Note that a vertex cover is the compliment of an independent set. So a maximal independent set corresponds to a minimal vertex cover. Furthermore, when coloring a graph, all vertices in an independent set may be assigned the same color.

Example 4. *Consider the graph C_5 depicted below. The black nodes are an independent set because they share no edges, and the white ones are a vertex cover because every edge has an endpoint among the white vertices.*



As before, we will transform graph-theoretic information into algebraic information. Again, we make a variable for each vertex by adjoining V to $\mathbb{C}$. But this time, we consider an ideal related to the graph instead of a polynomial.

Definition 5 (Cover Ideal)**.** *For a graph G, the cover ideal $\mathbf{J}(G)$ is the monomial ideal*

$$\mathbf{J}(G) := \bigcap_{\{u,v\}\in E} (u, v)$$

It turns out that the minimal generators for $\mathbf{J}(G)$ correspond to minimal vertex covers for G. Since minimal vertex covers are the compliments of maximal independent sets, then it is no surprise that $\mathbf{J}(G)$ is somehow related to the independence number of G.

Fact 2. *Let G be a graph with cover ideal $J = \mathbf{J}(G)$. Then J is generated by monomials of the form $\prod\{w \in W : W \text{ is a minimal vertex cover}\}$.*

Proof. Let x_W denote the product of variables in W, for any $W \subseteq V$. Let I be the ideal generated by $\{x_W \mid W \text{ a minimal vertex cover}\}$.

Suppose W is a minimal vertex cover. Then for any edge $\{u, v\} \in E$, either $u \in W$, or $v \in W$, and consequently either $u|x_W$ or $v|x_W$, and so $x_W \in (u, v)$. Therefore, $x_W \in J$ (see definition of J above), so $I \subseteq J$.

Conversely, let $f \in J$ be any monomial generator. Let W be the set of variables which divide f. Since $f \in J$, then $f \in (u, v)$ for each edge $\{u, v\} \in E$, then either $u|f$ or $v|f$, so either $u \in W$ or $v \in W$. Hence W is a vertex cover. Let $W' \subseteq W$ be a minimal vertex cover, and note that $x_{W'} \mid f$, so $f \in I$. Hence, $J \subseteq I$. □

Example 5. *Continuing the example of the graph C_5 from before, label the vertices (in order) u, v, w, x, y. Then $\mathbf{J}(C_5) = (u, v) \cap (v, w) \cap (w, x) \cap (x, y) \cap (y, u)$. Using Sage, we determine that $J(C_5) = (vxy, vwy, uwy, uwx, uvx)$, and each of these is a minimal vertex cover for C_5.*

Since minimal vertex covers are compliments of maximal independent sets, the generators of J also correspond to the maximal independent sets of G. We will use this fact to prove the following theorem.

Theorem 3. *Let G be a graph with vertex set $V = \{x_1, \ldots, x_n\}$. Let d be the smallest integer such that $x_1^{d-1}x_2^{d-1}\cdots x_n^{d-1} \in \mathbf{J}(G)^d$. Then $d = \chi(G)$.*

Example 6. *Again consider the graph C_5, as in the previous two examples. Clearly C_5 has chromatic number 3. Previously we showed that*

$$J(C_5) = (vxy, vwy, uwy, uwx, uvx).$$

We want to determine the minimal d such that $(uvwxy)^{d-1} \in J^d$. For $d = 1$, $1 \notin J$, so it is not 1-colorable. For $d = 2$, J^2 is generated by pairwise products of generators of J, so J^2 is generated by monomials of degree 6. Hence, $uvwxy \notin J^2$. Finally, J^3 is generated by the products of any three of the monomial generators of J, which in particular includes $uv^2w^2x^2y^2 = (vxy)(vwy)(uwx)$. In particular J^3 contains $u^2v^2w^2x^2y^2$.

Proof of Theorem 3. We first show that if $\chi(G) = d$, then $x_1^{d-1}x_2^{d-1}\cdots x_n^{d-1} \in J^d$. We partition V into its color classes, $V = U_1 \cup U_2 \cup \ldots \cup U_d$. Note that C_i is an independent set for all i, so $W_i = V \setminus U_i$ is a vertex cover. Hence, $x_{W_i} \in$

J for all i, by fact 2. Multiplying all of these monomials together, we see that $x_{W_1}x_{W_2}\cdots x_{W_d} \in J^d$. But because U_i are the color classes, they are disjoint. So if a vertex $x_i \in U_j$, then $x_i \in W_k$ for all $k \neq j$, so each vertex appears $d-1$ times in $x_{W_2}\cdots x_{W_d}$. Hence, $x_{W_2}\cdots x_{W_d} = x_1^{d-1}x_2^{d-1}\cdots x_n^{d-1} \in J^d$. So $\chi(G) \geq d$.

Conversely, let $x_1^{d-1}x_2^{d-1}\cdots x_n^{d-1} \in J^d$. We find minimal vertex covers $W_1, \dots, W_d$ such that $x_1^{d-1}x_2^{d-1}\cdots x_n^{d-1} = fx_{W_2}\cdots x_{W_d}$ for some $f \in \mathbb{C}[V]$. Forming compliments, this gives d disjoint independent sets $C_1, \dots, C_d$. For each of these sets, we assign a color, and see that $\chi(G) \leq d$. □

More fun facts

There are many other interesting ways to apply techniques from algebraic geometry to learn about the structure of a graph. There are at least two other ways to reduce k-colorability to a problem which can be solved via Gröbner bases. There are other ideals which encode information about the graph in interesting ways, such as the *edge ideal*, which is the ideal generated by uv for all $\{u, v\} \in E$. This ideal can tell us a great deal about the graph. For example:

Theorem 4. *For any graph G with edge ideal I, $\dim(\mathbf{V}(I)) = \alpha(G)$.*

Note that $\mathbf{I}(G)$ is an ideal generated by monomials. The dimension of a variety associated with a monomial ideal is relatively easy to compute using Gröbner bases, which makes this an effective algorithm for finding the independence number of the graph. For the proof of this theorem, see [VT13]. Some other facts about this ideal are stated below.

Theorem 5. *If G is a connected graph and I its edge ideal, then I is an ideal of linear type if and only if G is a tree or has a unique cycle of odd length.*

Theorem 6. *A graph G is bipartite if and only if I is normally torsion free.*

For proofs of these theorems, see [Vil90] and [SVV94], respectively.

References

[AT99] Noga Alon and M Tarsi. Combinatorial nullstellensatz. *Combinatorics Probability and Computing*, 8(1):7–30, 1999.

[CLO07] David A Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 2007.

[Die00] Reinhard Diestel. *Graph Theory* {*Graduate Texts in Mathematics; 173*}. Springer-Verlag Berlin and Heidelberg GmbH & Company KG, 2000.

[E$^+$95] David Eisenbud et al. *Commutative algebra with a view toward algebraic geometry*, volume 27. Springer New York, 1995.

[SVV94] Aron Simis, Wolmer V Vasconcelos, and Rafael H Villarreal. On the ideal theory of graphs. *Journal of Algebra*, 167(2):389–416, 1994.

[Vil90] Rafael H Villarreal. Cohen-macaulay graphs. *manuscripta mathematica*, 66(1):277–293, 1990.

[VT13] Adam Van Tuyl. A beginner's guide to edge and cover ideals. In *Monomial Ideals, Computations and Applications*, pages 63–94. Springer, 2013.

E-mail address: `dmehrle@cmu.edu`

Department of Mathematical Sciences, Wean Hall, Carnegie Mellon University, Pittsburgh, PA 15289