

## RESEARCH STATEMENT

CARL A. MILLER

My research specialization is in the field of **algebraic geometry**. I am interested in both pure and applied research in this subject. My current focus is on applications of algebraic geometry to computer science.

Algebraic geometry involves finding information about polynomial equations by studying their zero-sets. Let  $K$  be an algebraically closed field, and suppose that  $S = \{f_1, \dots, f_m\}$  is a set of polynomials in  $n$  variables over  $K$ . Then the set of solutions to  $S$  in  $K^{\oplus n}$  forms a geometric object, often denoted  $Z(S)$ . This set can be studied using geometric methods, including methods from algebraic topology and differential geometry. Geometric insight obtained into  $Z(S)$  can then be translated back into information about the polynomials  $\{f_1, \dots, f_m\}$ . This approach often yields interesting results. (A simple geometric proof of the Fundamental Theorem of Algebra is an example.)

I studied algebraic geometry in a purely mathematical context when I was in graduate school. My interests took an applied turn while I was working as an assistant professor at the University of Michigan, and I became interested in the topic of quantum information theory. This statement gives a short summary of my work, in reverse chronological order. Section 1 discusses quantum information theory, and Section 2 discusses my work in arithmetic geometry.

### 1. RESEARCH IN QUANTUM INFORMATION THEORY

Quantum information theory is concerned with quantum systems, i.e., sets of particles that are in an undetermined state. One of the distinctive features of quantum systems—one thing that makes quantum information theory different from classical information theory—is the possibility of **quantum entanglement**. This concept is the focus of my research.

Suppose that a quantum system is shared by two parties, Alice and Bob. A natural question is whether there exists a linear measurement of the “entanglement” in the shared system. A good numerical measurement of entanglement would be one that is decreased, or that remains constant, whenever Alice or Bob applies a local operation to his or her system. In the case of a two-party system, a good numerical entanglement measure does exist, based on the notion of tensor rank. (See the introduction to [5] for a discussion.)

My research work in [6], with Eric Chitambar and Yaoyun Shi, addresses the same problem at the next level of complexity. Suppose that a quantum system is shared between three parties, Alice, Bob, and Charlie. Suppose that Alice’s share of the system consists only of a single “qubit.” (A qubit is the simplest nontrivial quantum system—it is a particle that has only two basic states.) In this three-party case, it turns out that a strictly linear measurement of entanglement is impossible. There are states of this quantum system which are incomparable under local operations (meaning neither one can be converted into the other).

Although the state-space of this three-party system can’t be linearized, it can be understood from a different perspective. Local operations by Alice, Bob, and Charlie decompose the state-space of the system into equivalence classes (where we consider two states to be equivalent if one can be reversibly converted to the other via local operations). The following problem can then be posed:

- **Problem:** Classify all equivalence classes of states of the system shared by Alice, Bob, and Charlie.

States of this system can be represented by vectors in a vector space of the form  $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ . Once appropriately translated, the above problem is seen to be equivalent to the following mathematical problem:

- **Problem:** Let  $m$  and  $n$  be positive integers. Classify all orbits in the vector space

$$\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^n$$

under the action of the group

$$GL_2(\mathbb{C}) \times GL_m(\mathbb{C}) \times GL_n(\mathbb{C}).$$

My work with Chitambar and Shi addresses this problem using primitive elements of algebraic geometry. To illustrate the approach, let us assume for simplicity that we are dealing with the case where  $n = m$ . Any element  $v \in \mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^m$  can be expressed as a sum

$$v = \sum_{i,j,k} c_{ijk} \mathbf{e}_i \otimes \mathbf{f}_j \otimes \mathbf{f}_k,$$

where  $\{\mathbf{e}_i\}$  and  $\{\mathbf{f}_i\}$  are the standard bases for the spaces  $\mathbb{C}^2$  and  $\mathbb{C}^m$ . For each such  $v$ , we can define a polynomial

$$P_v(\mu, \lambda) = \det(\mu[c_{1jk}]_{j,k} + \lambda[c_{2jk}]_{j,k}),$$

which is homogeneous of degree  $m$  in the indeterminates  $\mu$  and  $\lambda$ .

If two vectors  $v$  and  $w$  are in the same GL-orbit, then there is a linear operation on the coordinates  $\{\mu, \lambda\}$  which carries  $P_v(\mu, \lambda)$  to  $P_w(\mu, \lambda)$ . So  $v$  and  $w$  can lie in the same orbit only if such a linear operation on coordinates exists. In geometric terms, this means that the zero sets of  $P_v(\mu, \lambda)$  and  $P_w(\mu, \lambda)$  on the projective line  $\mathbb{P}_{\mathbb{C}}^1$  must be related by some linear fractional transformation.

The question of classifying equivalence classes of quantum states is thus related to a much-studied object in algebraic geometry: the set of isomorphism classes of genus-zero curves with marked points. Using this relationship, as well as some additional theory from linear algebra, Chitambar and Shi and I came up with a complete classification of states of a  $(2, m, n)$ -dimensional three-party system ([6]). We showed in particular that an infinite number of equivalence classes exist iff  $\min\{m, n\} \geq 4$ .

Here is a significant result which is a consequence of our classification:

**Theorem 1.1** (Miller, Chitambar, and Shi). *Let  $v, w$  be vectors in  $\mathbb{C}^2 \otimes \mathbb{C}^m \otimes \mathbb{C}^m$ . Suppose that the polynomials  $P_v(\mu, \lambda)$  and  $P_w(\mu, \lambda)$  both have  $m$  distinct zeroes in  $\mathbb{P}_{\mathbb{C}}^1$ . Then  $v$  and  $w$  are GL-equivalent (meaning that the quantum states they represent can be related by local operations) if and only if there is a linear fractional transformation of  $\mathbb{P}_{\mathbb{C}}^1$  which maps the zero set of  $P_v(\mu, \lambda)$  to the zero set of  $P_w(\mu, \lambda)$ .*

Our project invites a number of extensions which I hope to explore. When an infinite number of equivalence classes exist, the geometric formulation discussed above suggests a natural way to parametrize the classes. I'm interested in finding out what these parametrizations reveal about the topology of the classes. This approach could be important for answering questions about approximation in the quantum setting.

Also, it's natural to consider how our approach could be extended to higher dimensions. Consider, for example, equivalence classes of states of a  $(3, m, m)$ -dimensional quantum system. A vector in  $\mathbb{C}^3 \otimes \mathbb{C}^m \otimes \mathbb{C}^m$  determines a three-variable homogeneous polynomial, whose zero set (typically) is a curve in the projective plane  $\mathbb{P}_{\mathbb{C}}^2$ . Two states can be equivalent only if their respective plane curves are isomorphic. The study of  $(3, m, m)$ -quantum systems is thus related to the study of complex curves. Could this approach lead to some further classification?

## 2. RESEARCH IN ARITHMETIC GEOMETRY

I'm interested in characteristic- $p$  arithmetic geometry, which is to say that I study number systems in which  $p \cdot 1 = 0$  for some prime number  $p$ . The central concept in my work on this subject is the concept of **sheaf cohomology**, which is a tool borrowed from algebraic topology.

Let  $k$  be an algebraically closed field of characteristic  $p > 0$ . Let  $Z$  be a  $k$ -variety, and let  $\mathcal{F}$  be a constructible étale sheaf of abelian groups of  $Z$ . Then one can construct the cohomology groups

$$H^i(Z, \mathcal{F}),$$

for  $i = 0, 1, 2, \dots$ . These groups encode information about the space  $Z$  and the sheaf of coefficients  $\mathcal{F}$ . Sheaf cohomology is a powerful tool in algebraic geometry. Andre Weil conjectured a formula for the number of rational points on a variety over a finite field, and this conjecture was ultimately proven using étale sheaf cohomology (see [4]).

So there is some interest in expanding the knowledge base for sheaf cohomology in algebraic geometry. One natural goal is to find general formulas for the sizes of cohomology groups.

Let us consider this goal first in a purely geometric setting. Let  $\bar{X}$  be a compact orientable 2-manifold. Let  $X \subseteq \bar{X}$  be the complement of a finite subset of  $\bar{X}$ . Let  $F$  be a field, and  $\mathcal{M}$  be a locally constant sheaf of finite-dimensional  $F$ -vector spaces on  $X$ . Then the following relationship holds:

$$(1) \quad \sum_{i=0}^2 (-1)^i \dim_F H^i(X, \mathcal{M}) = (\text{rank } \mathcal{M}) \sum_{i=0}^2 (-1)^i \dim_F H^i(X, F)$$

If we let  $\chi(\cdot, \cdot)$  denote the Euler characteristic of a sheaf-pair, then the formula can be written succinctly as:

$$(2) \quad \chi(X, \mathcal{M}) = (\text{rank } \mathcal{M}) \chi(X, F).$$

The sizes of the cohomology groups of  $(X, \mathcal{M})$  are readily computable from this formula.

My research is concerned with constructing a similar statement in the setting of characteristic- $p$  curves. This goal is somewhat difficult to achieve because of the complexity of characteristic- $p$  geometry. In the first place, a formula as simple as (2) is not possible, because two sheaves of the same rank on a characteristic- $p$  curve may have different Euler characteristics. So additional data is needed to find an Euler characteristic formula on characteristic- $p$  curves.

Here are two theorems which summarize the known results.

**Theorem 2.1** (Grothendieck, et. al.). *Let  $Y$  be a smooth  $k$ -curve. Let  $\bar{Y}$  be a projective closure of  $Y$ . Let  $F_0$  be a finite field, and let  $\mathcal{G}$  be a locally constant constructible sheaf of  $F_0$ -vector spaces on  $Y$ .*

*If the characteristics of  $k$  and  $F_0$  are different, then*

$$(3) \quad \chi(Y, \mathcal{G}) = (\text{rank } \mathcal{G}) \chi(Y, F_0) - \sum_{y \in \bar{Y} \setminus Y} \text{Sw}_y(\mathcal{G}).$$

**Theorem 2.2** (Miller). *Let  $Y$ ,  $\bar{Y}$ ,  $F_0$ , and  $\mathcal{G}$  be as in the previous theorem.*

*If the characteristics of  $k$  and  $F_0$  are the same, then*

$$(4) \quad \chi(Y, \mathcal{G}) \geq (\text{rank } \mathcal{G}) \chi(Y, \mathcal{O}_Y) - \sum_{y \in \bar{Y} \setminus Y} \mathfrak{C}_y(\mathcal{G}).$$

Above, the expressions  $\text{Sw}_y(\mathcal{G})$  and  $\mathfrak{C}_y(\mathcal{G})$  both denote numerical invariants which depend on the local behavior of the sheaf  $\mathcal{G}$  near a point. (The invariant  $\text{Sw}_y(\mathcal{G})$  is called the ‘‘Swan conductor’’ and the invariant  $\mathfrak{C}_y(\mathcal{G})$  is called the ‘‘minimal root index.’’) Formula (3) is an old result known

as the “Grothendieck-Ogg-Shafarevich formula”.<sup>1</sup> Formula (4) is the outcome of my work in [3], extending work of R. Pink in [2]. The inequality (4) is known to be an equality in some cases (see [2]).

Using notation from the above theorems: let  $y$  be point in the set  $\bar{Y} \setminus Y$ , and let  $t \in \mathcal{O}_{Y,y}$  be a local parameter. Then the sheaf  $\mathcal{G}$  determines a Galois representation

$$(5) \quad \text{Gal} \left( \overline{k((t))} / k((t)) \right) \circlearrowleft V,$$

where  $V$  denotes a vector space over the field  $F_0$ . In geometric terms, this is the “local monodromy” representation of  $\mathcal{G}$  at  $y$ . The terms  $\text{Sw}_y \mathcal{G}$  and  $\mathfrak{C}_y \mathcal{G}$  are numerical invariants associated to these representations. Essentially what Theorems 2.1 and 2.2 tell us is that any extra co-cycles of the sheaf  $\mathcal{G}$  can be detected in these local monodromy representations.

What I would like to do next is to illuminate formula (4) by introducing some more concepts from geometry. I suspect this might lead to interesting results. For example: in the theory of vector bundles with connections, there is a notion of the “irregularity” of a pole. This concept is similar in nature to the invariant  $\mathfrak{C}_y(\mathcal{G})$ . I would like to see if I can find a connection between those two invariants.

Additionally, ideas from representation theory might help to illuminate formula (4). The local monodromy representation (5) is an  $F_0$ -representation of some finite quotient of the group  $\text{Gal}(\overline{k((t))}/k((t)))$ . In the case where  $(\text{char } F_0) = (\text{char } k)$ , it can be shown that (5) is equivalent to an upper-triangular representation (after possible base change). What can this fact tell us about the invariant  $\mathfrak{C}_y(\mathcal{G})$ ?

These lines of investigation might give insight into some of the unique features of characteristic- $p$  geometry.

#### REFERENCES

- [1] A. Grothendieck et. al., Séminaire de Géométrie Algébrique du Bois-Marie (SGA 5), Lecture Notes in Mathematics, Vol. 589, Springer-Verlag, 1977.
- [2] R. Pink, Euler-Poincaré formula in equal characteristic under ordinarity assumptions, *Manuscripta Math.* 102 (2000), no. 1, pp. 1–24.
- [3] C. Miller, Equicharacteristic étale cohomology in dimension one. <http://arxiv.org/abs/0906.4093> . Submitted to *Algebra & Number Theory*.
- [4] E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjectures*, Springer-Verlag, Berlin, 1988.
- [5] E. Chitambar, R. Duan, and Y. Shi, Tripartite entanglement transformations and tensor rank. <http://arxiv.org/abs/0805.2977>
- [6] E. Chitambar, C. Miller, and Y. Shi, Matrix pencils and entanglement classification. <http://arxiv.org/abs/0911.1803>

---

<sup>1</sup>See Theorem 7.1, Exposé X in [1].