RESEARCH STATEMENT

CHRIS HURLBURT

My research interests lie in the areas of number theory and coding theory. The connection between these is my background arithmetic algebraic geometry. In particular my past research has been in a rather new area created when algebraic geometry is expanded in a meaningful way to include algebraic differential equations and in coding theory. To date in coding theory I have been interested in nonlinear algebraic-geometric codes. My future research interests are to continue working on the many questions related to nonlinear algebraic geometric codes, applications of arithmetic difference geometry, the random number theory problem that is accessible to undergraduates, and a few knotty problems in differential algebraic geometry.

The nonlinear algebraic-geometric codes in my research stem from a new construction of error-correcting codes from algebraic curves over finite fields introduced by N. Elkies in [Elkies1] that extends Goppa codes. In [HJ], J. Thunder and I show that Elkies' nonlinear codes are examples of a larger family of error-correcting codes. Currently Elkies' codes have the highest asymptotic transmission rates known for certain ranges of alphabet size and error rate. Our extension allows us to see Elkies' codes in the context of a larger family of codes that among other things have connections to linear equations. There is hope that more exploration of the larger family of error correcting codes will lead to codes with even better asymptotic transmission rates or could allow the construction of codes with the same alphabet size and error rate that are significantly longer than Elkies' codes for the same asymptotic transmission rate.

Just as Goppa codes generalize Reed-Soloman codes, codes constructed from points of bounded twisted height generalize the codes introduced by Elkies in [Elkies1]. Let us fix a finite field k with $q = p^l$ elements for p a prime number. Over this field let C be a projective, smooth, irreducible algebraic curve of genus g. Recall that this is equivalent to fixing an algebraic function field K over $\mathcal{F}_p$, namely a finite algebraic extension of $\mathcal{F}_p(T)$ where $\mathcal{F}_p$ is the finite field of p elements. Let N be the number of k-rational points on C. To construct a geometric Goppa code [Stichtenoth1], also known as an algebraic geometric code [Tsfasman-Vladut1], choose a set $S = \{P_1, ..., P_n\}$ of n distinct k-rational points and a divisor D such that $S \cap \text{supp}D = \emptyset$. Then the Goppa code is

$$\mathcal{C}(S, D) := \{(x(P_1), \ldots, x(P_n)) : x \in \mathcal{L}(D)\}$$

whereby $x(P_i)$ we mean the residue class of x at P_i and $\mathcal{L}(D) = \{x \in K : \text{div}(x) \geq -D\}$. Simply put a Goppa code is constructed by associating codewords to sections in the complete linear system associated to a divisor D over C. In the case of $C = \mathbb{P}^1$, each section of the linear system can be identified with a polynomial of degree at most $\deg D$.

Elkies introduces a new method for constructing nonlinear codes in [Elkies1] where he adds the following new idea to the construction of Goppa codes. In the simplest case where C is the projective line $\mathbb{P}^1$, Elkies replaces the polynomials used for Goppa codes with rational functions whose degree is $\leq h$ for h a positive integer. Each rational function f is then associated with the code word created by enumerating the rational function at the k-rational points on the curve C. Explicitly, f is identified with the N-tuple

$$(f(P_1), f(P_2), \ldots, f(P_N))$$

of values of f at points of C. Since f may have poles on some P_i, some $f(P_i)$ values may be ∞.

More generally, Elkies lets D be a divisor of degree 0 on the curve C. Then for each $h < N/2$, he defines $C_D(h)$ to be the set of rational sections of degree $\leq h$ on the line bundle L_D associated to D. We can describe the set $C_D(h)$ explicitly if for any $a \in K$, we let (a) denote the divisor of a and if we let E^+ and E^- denote the positive and negative parts of a divisor E then

$$C_D(h) = \{a \in K\backslash\{0\} : (a) = E - D \text{ where } \deg E^+ = \deg E^- \leq h\} \cup \{0\}.$$

Then to associate a code word to each element of $f \in C_D(h)$, Elkies fixes for each point P_i a rational function φ_i whose divisor as the same order at P_i as D and identifies f with the N-tuple

$$((\varphi_1 f)(P_1), (\varphi_2 f)(P_2), \ldots, \varphi_N f(P_N)) \in (\mathbb{P}^1(k))^N.$$

In order to generalize Elkies' code, we switch our language slightly to that of adeles. Let $M(K)$ be the set of places of K and for any $v \in M(K)$ we denote by K_v the completion of K at v. For any element $x \in K_v$, by $\mathrm{ord}_v(x)$ we will simply mean the valuation of x with repect to v. The adele ring, $K_{\mathbb{A}}$, consists of the product over all valuations of K_v where for any $x \in K_{\mathbb{A}}$, the entries for all but a finite number of places have valuation $\mathrm{ord}_v(x) = \mathrm{ord}_v(x_v) \geq 0$. There is a natural embedding of K into K_v for any $v \in M(K)$ and hence a natural embedding of K into $K_{\mathbb{A}}$.

For any $\mathbf{x} = (x_1, \ldots, x_n) \in K_v^n$, we define the order of $\mathbf{x}$ at v to be

$$\mathrm{ord}_v(x_1, \ldots, x_n) = \min_{1 \leq i \leq n} \{\mathrm{ord}_v(x_i)\}.$$

If $\mathbf{x} \in K_{\mathbb{A}}^n$, then $\mathbf{x}$ consists of an element in K_v^n at each place v and the order of $\mathbf{x}$ at a place v is just the order of the n-tuple of entries in the v place. For any $\mathbf{x} = (x_1, \ldots, x_n) \in K_{\mathbb{A}}^n$ the divisor of $\mathbf{x}$ is

$$\mathrm{div}(x_1, \ldots, x_n) = \sum_v \mathrm{ord}_v(x_1, \ldots x_n) \cdot v.$$

The degree of the divisor of $\mathbf{x}$ is

$$\deg(\mathrm{div}(\mathbf{x})) = \sum_v \mathrm{ord}_v(x_1, \ldots x_n) \cdot \deg v$$

where $\deg v$ is the degree of the place. For any $\mathbf{x} \in K^n$ or $\mathbf{x} \in K_{\mathbb{A}}^n$, we define the height of $\mathbf{x}$ to be

$$H(x_1, \ldots, x_n) = q^{-\deg(\mathrm{div}(x_1, \ldots, x_n))}.$$

The height of any $\mathbf{x}$ is unchanged by scaler multiplication of an element from K.

For any $A \in \mathrm{GL}_n(K_{\mathbb{A}})$, the twisted height with respect to A is the function

$$H_A(\mathbf{x}) = H(A\mathbf{x})$$

where $\mathbf{x}$ is a n-tuple in K^n. Just as the height of $\mathbf{x}$ is invariant under scaler multiplication, so is the twisted height of $\mathbf{x}$. Namely for all $a \in K$, $H_A(a\mathbf{x}) = H_A(\mathbf{x})$ and so we can view twisted heights as functions on the space of one-dimensional linear subspaces of K^n. For any $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ and h an integer, we define

$$C_A(h) = \left\{ \begin{matrix} \text{one-dimensional linear subspaces of} \\ K^n \text{ determined by } \mathbf{x} \in K^n \end{matrix} : H_A(\mathbf{x}) \leq q^h \right\}.$$

Namely $C_A(h)$ is the set of all points ξ in projective $(n-1)$-space over K whose twisted height is less than or equal to q^h. The general idea is to associate codewords to representatives of elements in $C_A(h)$. To do this we must describe what we mean by the evaluation of an adele at a point.

Suppose P is a k-rational point on the curve C and $\alpha \in K_{\mathbb{A}}$. The point P has an associated place in $M(K)$ which we will refer to as v_P and α has an entry at the v_P place, α_{v_P}, that is an element in K_{v_P}. By $\alpha(P)$ we will mean the residue of α_{v_P} in k if $v_P(\alpha) \geq 0$ and we will mean ∞ if $v_P(\alpha) < 0$. We note that the residue of v_P in k is well defined because P is a k-rational point and hence the residue field of K_{v_P} is k. Note that for any such α and P there are $q+1$ possibilities for $\alpha(P)$, namely the elements in k and ∞.

Let $A \in G_2$ be an upper triangular matrix of the form

$$A = \begin{bmatrix} \alpha & * \\ 0 & 1 \end{bmatrix}.$$

The generalization is to construct a code by choosing for each element in $C_A(h)/[1,0]^T$ the representative $\mathbf{x} = \begin{bmatrix} x \\ 1 \end{bmatrix} \in K^2$ and then to this representative associating the codeword $(\phi_1(P_1), \ldots, \phi_1(P_N))$ for $\phi = A\mathbf{x}$. Elkies' codes are the case when $* = 0$ and $\mathrm{div}(\alpha) = D$.

In this context it is easy to see how longer codes, desirable for error-correcting codes, might be constructed. Simply increasing n from 2 and evaluating more than one of the ϕ_i where $\phi = A\mathbf{x}$ would increase the length of the codewords. The immediate difficulty arises from the fact that the current argument for the minimal distance givens a minimal distance that is independent of n, the size of the matrix, and is at most $N+g-2h$ where g is the genus of the curve. Without better minimal distance bounds, the resulting decrease in the error detection rate means that the longer codes no longer even approach the same parameters as Goppa codes let alone improve them. It might be possible to exploit the geometry of the curve to come up with a more detailed minimal distance bound that could improve the minimal distance bound for larger n. Because the number of codewords will increase with an increase in n, this will require some finesse. For example a minimal distance bound $(n-1)N - 2h$ is impossible because the resulting code would violate the Singleton bound.

An improvement that we are working on is decreasing the alphabet size from $q+1$ to q. This has already been done in the case of Elkies' codes in [Elkies2] where he develops an idea introduced by Xing in [Xing1]. This improvement is possible here as well once some technical issues are resolved. Another related question is the relationship between a matrix $A \in \mathrm{GL}_n(K_{\mathbb{A}})$ and the minimum value for the twisted height H_A. There is constant λ_A in the minimal distance bound that is based on the minimum value for the twisted height H_A and this constant is on average $1-g$ where g is the genus of the curve. The constant λ_A also has a lower bound of $-g$.

We are working to construct matrices A where λ_A is either $1-g$ or $-g$, the latter of which may not exist. Our goal is to establish an effective criterion for generating a matrix A such that the associated constant λ_A in the minimal distance is either $1-g$ or $-g$ because these matrices would provide the best possible error-detection rates for the generalized codes.

Beyond this immediate work, a future avenue of inquiry is to work with the relation to linear equations in order to try and find a partial solution to the error detection or recognition problem: is a given word in the code? Realistically the solution from this avenue would be able to identify that an N-tuple was *not* a codeword, but would allow false positives. The reasons for this are two-fold. First the connection to linear equations depends on a choice of basis for a two dimensional subspace of K^3. Second we are trying to test whether or not an N-tuple of numbers could possible have resulted from the evaluation of an adele at the places of degree one where the adele is of the form Ax for $x \in K$ and A related to the choice of basis of the two dimensional subspace of K^3 determined by the homogeneous linear equation.

Another area of my research is that of differential algebraic geometry, specifically in the cases of arithmetic operators. A. Buium over a series of papers [BuiumAmJ], [BuiumAmJ2], [BuiumDuke], and [BuiumInv] introduced a new field called differential algebraic geometry. This field is created by expanding algebraic geometry to include algebraic differential equations and their arithmetic analogs. In particular, there are four classes of operators that can be used to "enlarge usual algebraic geometry" by "adjoining" an operator δ [BuiumOp]. One component of this expanded algebraic geometry is the expansion of modular forms to include differential modular forms. My earlier work involved computational aspects of these differential modular forms. My most recent work in differential algebraic geometry is in the case when the adjoined operator is an arithmetic difference operator, arithmetic difference geometry is the result. The basic theory of arithmetic difference geometry is detailed in [Hurlburt1]. The motivation for these "enlarged" geometries is the new approaches to arithmetic problems they provide. To date the theory of arithmetic analogs of derivations has been applied quite successfully to a variety of arithmetic problems. At this time, there are no significant applications of arithmetic difference geometry. However, the success of arithmetic analogs of derivations indicates that a search for applications of arithmetic difference geometry that will both motivate arithmetic difference geometry and give it context is worthwhile.

Among the various approaches to defining objects in these new geometries, we consider the constructive approach to the basic definitions of arithmetic difference geometry. Let L a field of characteristic zero, complete under discrete valuation, with an algebraically closed residue field k of characteristic $p > 0$. Furthermore assume L is a separable extension of $\mathbf{Q_p}$ with R the valuation ring of L and fix $\pi \in R$ a prime element. For R-algebras A and B with $f : A \to B$ an R-algebra homomorphsim, a π-difference operator of f is a map $\delta : A \to B$ that satisfies

$$\begin{aligned} \delta(x+y) &= \delta x + \delta y \\ \delta(xy) &= f(y)\delta x + f(x)\delta y + \pi\delta x\delta y \\ \delta(1) &= 0 \end{aligned}$$

for all $x, y \in A$. From now on we will assume that f is either the identity or a natural embedding of A into B and therefore can replace $f(x)$ with x. In the case

when $A = B = R$, if $\delta : R \to R$ is a π-difference operator then $\phi(x) = x + \pi\delta x$ is a ring homomorphism. Moreover the unique extension of ϕ to a homomorphism from L to L also denoted ϕ is a Galois automorpism of L over $\mathbf{Q_p}$ that operates trivially on k. As a result the set of π-difference operators from R to R is in bijective correspondence with the set of Galois automorphisms of L over $\mathbf{Q_p}$ that operate trivially on k. This set is called the first inertia group G_0. For what follows we fix a choice of $\delta : R \to R$ from the possibly many candidates.

Let X/R be a scheme of finite type. To construct π-jet spaces we proceed as follows. First we cover X with affine open subsets U_i. Then for any given i, $\mathcal{O}(U_i) = R[T]/(f)$ for T an n-tuple of indeterminates and f an m-tuple of polynomials. We extend $\delta : R \to R$ to a π-difference operator $\delta : R[T] \to R[T, T']$ where T' is another n-tuple of indeterminates by defining $\delta(T_i) = T_i'$. We let $\mathcal{O}(U_i^1) = R[T, T']/(f, f')\hat{}$ where $f' = \delta(f)$ and $\hat{}$ represents the π-adic completion. We then construct the first jet space by, X^1, gluing together the U_i^1. To obtain the nth jet space, X^n, this procedure is essentially iterated n times and by X_m^n we will simply mean $X^n \otimes R/(\pi^{m+1})$. In turn the π-jet spaces form a sequence

$$\ldots \to X^n \to X^{n-1} \to \ldots \to X^1 \to X^0$$

where $X^0 = \hat{X}$. By X^∞ we simply mean the inverse limit of this sequence. Then there also exists a natural map $\nabla^n : X(R) \to X^n(R)$ where $X(R)$ denotes the R rational points of X. Passing to the projective limit, we have $\nabla : X(R) \to X^\infty(R)$.

A *δ-formal function of order $\leq n$* on $X(R)$ is an R-valued function $\varphi : X(R) \to R$ such that any point in X has an affine open neighborhood $U \subset X$ where φ can be written as

$$\varphi(P) = \Phi(u(P), \delta u(P), \delta^2 u(P), \ldots, \delta^n u(P)), \qquad P \in U(R)$$

with $u = (u_1, \ldots, u_N)$ an N-tuple of regular functions on U and Φ an element in the π-adic completetion of the ring of polynomials with coefficients in R and $N(n+1)$ variables. There is a natural map $\mathcal{O}(X^n) \to \mathcal{O}^n(X)$ where the latter refers to the ring of δ formal functions of order $\leq n$ which is *not* necessarily injective.

An obvious application of π-difference geometry is to apply it in a similar fashion to the application of the geometry of p-jets to proving quantitative bounds for $\#(X(R) \cap J(R)_{tors}$ where X/R is a smooth projective curve of genus $g \geq 2$ and J/R is the Jacobian of X. The result of applying π-difference geometry requires that X/R have a non-trivial Kodaira-Spencer class and is a bound of

$$\#(X(R) \cap J(R)_{tors}) \leq p^{(3+N)g}(3^g)[8g-2]g!$$

where N is the smallest integer such that $\frac{\nu(p)}{p^{N+1}-p^N} < 1$ for ν the valuation on R. The requirement that X/R have a non-trivial Kodaira-Spencer class means that $\nu(p) > 1$. However, a special case of a theorem of Coleman is that if X is a curve of genus g over $\mathbf{Q_p}$ with good reduction and $p > 2g$, then $X \cap J_{tors}$ is unramified, i.e., contained in $J({\mathbf{Q_p}}^{unr})_{tors}$ [Poonen1], [Coleman1]. As a consequence the bound from π-difference geometry is seldom applicable.

As this example demonstrates, useful applications of π-difference geometry will differ from the applications of the geometry of p-jets. The intrinsic connection between the Galois automorphisms in the first inertia group and π-difference operators and role of the Kodaira-Spencer class in π-difference geometry are guides to a search for applications. For example, in [CV] Coleman and Voloch use Kodaira-Spencer theory to study companion forms. That Kodaira-Spencer theory can be used to

study companion forms suggests that there might be a relation between companion forms and π-difference geometry. Other places to look for connections include the large areas of geometry where Galois actions of varieties are used and questions about varieties over ramified fields. In addition to the relatively unexplored arithmetic difference geometry, there are numerous unresolved questions related to differential algebraic geometry in the case the arithmetic analog of the derivative as well. While I am not actively working on these types of questions at present, I still ponder some of them occasionally.

Finally an area of research interest to me, slightly apart from the areas of research discussed so far, is various basic number theory problems. My interest in these types of problems stems from two sources, one being my own entertainment and the other being their accessibility to undergraduates. A sample of this type of problem is the non-existence of Fibonacci triangles. Simply put, a Fibonacci triangle is triangle whose side lengths are Fibonacci numbers and whose area is an integer. It is conjectured that there is precisely one Fibonacci triangle, namely the triangle whose sides are $(5, 5, 8)$. It is fairly simple to show that any possible Fibonacci triangle must be isosceles and hence of the form (F_{n+k}, F_{n+k}, F_k) where F_i is the ith Fibonacci number. During a recent undergraduate research semester, a student working with me proved the non-existence of Fibonacci triangles in cases of $k = 7, \ldots, 12$ which were not previously known. These types of problems, while peripheral to my main research foci in coding theory and other applications of arithmetic algebraic geometry, remain part of my research interests simply because of the opportunity for collaboration with undergraduates in research that these types of problems provide.

[BuiumAmJ] A.Buium, Geometry of differential polynomial functions I: algebraic groups, Amer J. Math. 115, 6 (1993), 1385-1444.

[BuiumAmJ2] A.Buium, Geometry of differential polynomial functions II : algebraic curves, Amer. J. Math., 116, 4, (1994), 785-819.

[BuiumDuke] A.Buium, Geometry of $p-$adic jets, Duke Math. J., 82, 2, (1996), 349-367.

[BuiumInv] A.Buium, Differential characters of abelian varieties over p-adic fields, Invent. Math., 122, 2, (1995), 309-340.

[BuiumOp] A.Buium, Arithmetic analogues of derivations, J. Algebra, 198, (1997), 290-299.

[Coleman1] R. F. Coleman, Ramified torsion points on curves, Duke Math J. 57, 2, (1987), 615-640.

[CV] R. F. Coleman and J. F. Voloch, Companion forms and Kodaira-Spencer theory, Invent. Math., 110, 2, (1992), 263-281.

[Elkies1] N. Elkies, Excellent nonlinear codes from modular curves, STOC'01: Proceedings of the 33rd Annual ACM Symposium on the Theory of Computing, Hersonissos, Crete, Greece, (2001), 200-208.

[Elkies2] N. Elkies, Still better nonlinear codes from modular curves, arXiv:math.NT, (2003).

[HJ] C. Hurlburt and J. Thunder, Non-linear codes from points of bounded height, Preprint 2004.

[Hurlburt1] C. Hurlburt, Geometry of Arithmetic Difference Operators, Preprint 2004.

[Poonen1] B. Poonen, Computing torsion points on curves, Experiment. Math. 10, 3, (2001), 449-465.

[Stichtenoth1] H. Stichtenoth, Algebraic function fields and codes, Universitext, Springer Verlag, 1993.

[TsfasmanVladut1] M. A. Tsfasman and S. G. Vlăduţ, Algebraic-geometric codes, Mathematics and its applications (Soviet Series), 58, Kluwer Academic Publishers, 1992.

[Xing1] C. Xing, Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound, IEEE Trans. Inform. Theory, 49, (2003), 432-437.