# RESEARCH STATEMENT

CHRIS LOMONT

**Primary Interests: Quantum computation, algebraic geometry, computational complexity**

I am interested in the interplay between mathematics, physics, and computer science, an interplay exhibited clearly in quantum information theory. Over the last decade, results in quantum computing and quantum information theory has rewritten the notions of computational complexity and the meaning of information.

Starting with three bachelor's degrees in math, physics, and computer science, and continuing with a PhD in algebraic geometry, I have been working on understanding the computational power of different physical systems. As information theory has grown from an area of applied math to a fundamental underpinning of physical theory, the sophistication of the mathematical methods required to understand and analyze these relations has also grown. Since the most inclusive physical theories, such as superstring theory and supersymmetry, require deep mathematics to patch relativity with quantum mechanics, I wanted to master as much of the mathematics as I could, so I could probe the limits of computability. This route led me to algebraic geometry for my PhD, and a job after graduation doing quantum computation research.

## 1. Background

Information theory was started around 1950 by Claude Shannon, who made a mathematical model of information, and who proved fundamental results in the field. Over the next 50 years information theory has grown to touch many areas of mathematics, including sphere packing, combinatorics, algebra, and topology. In the 1980's Goppa [5] introduced the use of algebraic curves for code construction, obtaining codes surpassing the 30 year-old Gilbert-Varshamov bound. However, information was still primarily thought of as a mathematical concept.

On another front Feynman noted that classical computers could not simulate quantum systems due to the exponential growth of the information needed to store a quantum state, and this observation was expanded by Deutsch, Jozsa, and others into the notion of "quantum computing", that is, using quantum entanglement as a information processing resource. In 1994, Shor [14] famously demonstrated such a quantum computer could factor integers exponentially faster than classical computers, and would easily break RSA. It was later shown that there are problems which *require* exponential time on a classical computer, but could be solved in polynomial time on a quantum computer.

Since then quantum information theory has grown tremendously, and many important classical results have been recast in the new formalism. Many scientists now take the view that "information is physical," and as such there is a great push to understand what computational limits physics presents. This is what interests me: it is now clear quantum effects significantly add computational power over classical ideas. Does adding relativity add more again? To answer this one needs an understanding of numerous areas of math, physics, and computer science.

There are many open theoretical problems, many of which require advances in mathematical theory. For example, a positive answer to a certain question about the Hidden Subgroup Problem [11] would imply a fast graph isomorphism algorithm, which is currently the holy grail of quantum algorithms.

All this theoretical computational power has attracted other eyes. At a recent conference an Army Program manager said he calculated that the US government has invested over $1 billion so far into quantum computing research. Given the possible payback if (when?) quantum computing becomes commonplace, it seems this interest will continue from many sectors.

## 2. Work to date

2.1. **Coding theory and algebraic geometry.** My PhD thesis, "Error correcting codes on algebraic surfaces," constructed some new explicit error-correcting codes on ruled surfaces. Since going from Reed-Solomon codes defined on the projective line $\mathbb{P}^1$ to codes defined on general curves allowed Goppa to make better codes (in effect allowing longer codes to be constructed), it seemed that generalizing to surfaces would again allow longer codes to be constructed. This was the basic idea of my thesis.

The first case I studied was repeated blowing up of points in $\mathbb{P}^2$, which led to poor codes. In effect, over a finite field $\mathbb{F}_q$ the codes resulting from such repeated blowing up behave like codes from products of $\mathbb{P}^1$ codes, which have poor parameters. For surfaces that are the product of two curves, $S = C_1 \times C_2$, the codes are also inferior to the Goppa codes.

Next I completely analyzed codes from ruled surfaces over $\mathbb{P}^1$. It turns out the best codes are precisely the product codes. For ruled surfaces resulting from a vector bundle that is a direct sum of twisting sheaves over a curve, the best codes also turn out to be the product codes.

Atiyah [2] classified vector bundles on an elliptic curve $C$ over algebraically closed fields, and Arason, Elman, and Jacob [1] extended the classification to finite fields, which I used to do the elliptic curve case. All ruled surfaces over an elliptic curve resulting from a nontrivial vector bundle fall into invariant 0 or 1 cases. I completely solved the invariant 0 case. How $S^n(\mathcal{F}_2)$ decomposes into indecomposable sheaves was needed, where $\mathcal{F}_r$ denotes the unique degree 0 rank $r$ sheaf with a global section over $C$. Over the complex numbers Atiyah had shown $S^n(\mathcal{F}_2) \cong \mathcal{F}_{n+1}$. In characteristic $p$, I showed $S^n(\mathcal{F}_r)$ decomposes into a direct sum of $\mathcal{F}_i$ in any characteristic (and even

can obtain exact decompositions in some cases), which is enough structure to answer all questions about the resulting codes. These codes have parameters slightly inferior to yet arbitrarily close to the product code parameters. In the invariant 1 case I obtained bounds on the code parameters. I recently was mailed a preprint solving this final case which shows that again these are no better than product codes.

These cases may be extended to give long codes over a curve of any genus. In particular, I would like to analyze codes over the curves of Garcia-Stichtentoth [4], which are explicit curves that meet the TVZ bound. Since vector bundles on higher genus curves are not as well understood, I doubt I can answer the question completely, but using results similar to the elliptic curve case I can obtain bounds, which should be tight enough to decide if these codes beat previously best bounds or not.

While studying codes on curves, I wrote a paper [8] exhibiting curves with record numbers of rational points. In it all plane curves with degree at most 7 and with coefficients in $\mathbb{F}_2$ are studied to find those with large numbers of $\mathbb{F}_{2^m}$ rational points, for $m = 3, 4, ..., 11$. Known lower bounds are improved for many genus and $\mathbb{F}_q$ combinations; in some cases it is shown the Serre and other known upper bounds are actually achieved. To do it I wrote about 5000 lines of C++ code to search through all polynomials, find irreducible curves unique up to isomorphism, select from each isomorphism class the polynomial with least work required to evaluate, and study any singularities. Then bounds on the genus were found, and for interesting curves the exact genus was computed from a variety of techniques. To obtain bounds on the number of $\mathbb{F}_q$-rational points, I derived some relations about the information gained from the computer search, and used it to find the best curves from each genus and $\mathbb{F}_q$ combination.

2.2. **Quantum Computation.** After graduation, I found a job at Cybernet doing research into quantum computing algorithms for image processing. I wanted this job to gain a detailed understanding of quantum computing and quantum information theory.

Most of the quantum algorithms that achieve exponential speedup over classical algorithms rely on the quantum version of the Fourier transform over a finite group. Since convolution and correlation are closely related to the Fourier transform and are also useful in image processing, I tried to make quantum versions, but obtained as an early result that convolution and correlation of quantum states are physically impossible [9].

Reviewing the literature, I found a fatal error in the published algorithms for the quantum Fourier transform over odd cyclic groups, an important case. I was able to correct these errors, and obtained better results in [10]. The detailed overview of the Hidden Subgroup Problem (HSP) is contained in [11].

The most recent problem I have been working on is trying to study if basis choice of irreducible representations allows enough information to solve the HSP over the symmetric group $S_n$. An efficient method to reconstruct these hidden subgroups

would yield an efficient algorithm for Graph Isomorphism, an elusive and important complexity problem for over 30 years. Failure to find such bases would at any rate give better insight to quantum algorithms. Success would derail one approach to show $\mathbf{P} \neq \mathbf{NP}$. To pursue this problem I have been writing software to perform rapid computations on irreducible representations of finite groups, so I can sample data and see if there is ample evidence in important cases. This is ongoing work.

## 3. Future Research Plans

3.1. **Extending coding results.** It took about 10 years after the discovery of good curve codes until practical algorithms were discovered to decode them. It would be non-trivial to extend these algorithms to ruled surfaces, then surfaces, and perhaps varieties in general, since they rely on an interplay of Riemann-Roch and Serre Duality that does not seem to generalize to higher dimensions. I want to work some on this computational side, and find algorithms for constructing and decoding these codes, based on generalizations of the decoding algorithms for curves. I also plan to continue to research codes on more general classes of algebraic surfaces, extending classification past ruled surfaces. Central to this work is an understanding of indecomposable vector bundles over curves over finite fields, a rich area with many unanswered questions. Given time I want to pursue a deeper understanding of indecomposable vector bundles at a level precise enough to answer questions suitable for code construction.

3.2. **Quantum algorithms.** Adding quantum ideas to classical computing resulted in a strictly stronger model of computing, and the last 10 years have added greatly to the theory of complexity in the quantum domain. I would like to pursue this understanding, especially in finding the limits of what can be done using the quantum Fourier transform. The limiting problem seems to be questions about representation theory, so there is where I will continue my work.

3.3. **Information theory.** Another question in this vein I have not had time to pursue is: does adding relativity allow any more computational power? I also want to recast information theory in a relativistic framework, since information needs to travel to be useful, and under even current technology there are relativistic effects. Not having time yet to pursue this, I am unaware of anyone working in this direction.

3.4. **Quantum error correction.** A third direction I want to pursue is quantum error correction, merging areas from my thesis with my work in quantum computing. A significant amount of work has been done in this area [3], and there are very good quantum error correction codes. These are very different than traditional methods, since one cannot measure the quantum state and correct as in classical error correcting codes. Again, I have some ideas I want to apply here, but have not had the time to do so yet.

3.5. **Other interests.** I have many other interests which I have not been able to pursue as of yet. A visit to my website `www.lomont.org` shows many of these interests. A brief list includes computer graphics, cryptography, compression, security, coding quality, novel computer architectures, and string theory. For example, I recently wrote a detailed article on using geometric algebras in computer graphics [12] which will be published in the spring in the book "Games Programming Gems V."

## References


[1] J.K. Arason, R. Elman, and B. Jacob, *On indecomposable vector bundles*, Comm. Algebra **20**, no. 5, pp. 1323-1351, (1992).

[2] M.F. Atiyah, *Vector bundles over an elliptic curve*, Proc. London Math. Soc., **7**, pp. 414-452, (1957).

[3] , A. R. Calderbank, E. M. Raines, P. W. Shor, and N. J. Sloane, *Quantum Error Correction and Orthogonal Geometry*, Physical Review Letters, (1997).

[4] A. Garcia and H. Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C. R. Acar. Sci. Paris Sér. I Math., **322**, pp. 1067-1070, (1996).

[5] V.D. Goppa, *Codes on algebraic curves*, Sov. Math.-Dokl., Vol. 24, pp. 170-172, (1981).

[6] S. H. Hanson, *The Geometry of Deligne-Lusztig Varieties; Higher dimensional AG codes*, Ph. D. Thesis, University of Aarhus, Department of Mathematical Sciences, University of Aarhus, DK-800 Aarhus C, Denmark, July 1999.

[7] J.H. van Lint, *Introduction to Coding Theory*, GTM#86, Springer-Verlag, (1982).

[8] Chris. Lomont, *Yet more projective curves over* $\mathbb{F}_2$, J. of Exp. Math., Volume 11, issue 4, (2002),`math.NT/0105262`.

[9] Chris Lomont, *Quantum convolution and quantum correlation algorithms are physically impossible*, (2003), `quant-ph/0309070`.

[10] Chris Lomont, *A quantum Fourier transform algorithm*, (2004), `quant-ph/0404060`.

[11] Chris Lomont, *The Hidden Subgroup Problem - Review and Open Problems*, (2004), `quant-ph/0411037`.

[12] Chris Lomont, *Using geometric algebra for computer graphics*, (2004), to be published spring 2005 in Games Programming Gems V, Charles River Media.

[13] S. Roman, *Coding Theory and Information Theory*, GTM#134, Springer-Verlag, (1992).

[14] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings, 35th Annual Symposium on Fundamentals of Comp. Science (FOCS), pp. 124–134, (1994).

[15] M.A. Tsfasman, S.G. Vlăduţ, and Th. Zink, *On Goppa codes which are better than the Varshamov-Gilbert bound*, Math Nachr, **109**, pp. 21-28, (1982).

[16] M. A. Tsfafman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht/Boston/London: Kluwer, (1991).



Chris Lomont, 584 Landings Blvd, Ann Arbor, MI, 48103
*Email address*: chris (at) lomont (dot) org

Written: December 2004