

Robert N. Talbert, Ph.D.
Statement of Scholarship

My overall approach to scholarship is centered on a dual commitment to both teaching and learning. I take a broad view of scholarship that includes any creative, substantive intellectual activity that contributes to my discipline and the ways it is taught and used. I pursue scholarship with an eye towards using it to teach students both in the classroom (for example, through examples, group activities, or labs) and out of the classroom (for example, through undergraduate research, independent studies, or blogging). In my view, the ideal line of research always ends in the classroom or the lab as something students can examine and learn from for themselves, regardless of how or where the research originates or what form it takes.

My early research was concentrated in algebra and topology, making use of classical ring and module theory along with universal algebra and category theory to study certain constructions in geometric topology. My Ph.D. dissertation ([5]) used a category-theoretic construction called a *homotopy colimit* to establish an isomorphism between the stratified or “Quinn” homology groups $H_*(X/G; \pi_k \mathcal{S}(p))$ and the better-understood equivariant homology groups $H_*^G(X; M)$ in the case where G is a discrete group acting cellularly on a simplicial complex. A version of my dissertation ([4]) appeared in an international mathematics journal. My results have been useful in further work on the Isomorphism Conjecture of Farrell and Jones as well as in understanding the somewhat mysterious spectral sequence constructions of Frank Quinn.

In more recent years, I have aligned my scholarly work with the model proposed by Ernest Boyer ([1]), pursuing scholarship of *discovery*, *teaching*, *integration*, and *application*. Each of these four kinds of scholarship are present in the specific avenues of study I describe below. I have found this multifaceted approach to scholarship to be productive, realistic, student-centered, and conducive to a well-balanced professional life.

My primary area of mathematical research for the last several years has been *cryptology*. Cryptology is defined as the study of communication in the presence of an adversary and is more popularly known as the mathematics behind codemaking and codebreaking. I was first exposed to the subject through a student whose independent study on the subject I oversaw. In 2002, I attended an American Mathematical Society short course on cryptology where I studied some current issues in the field and interacted with some of its most famous researchers. After this minicourse, I began to make cryptology my primary area of study through a program of reading and through the design and teaching of a topics course in the subject.

In 2006, I published a paper ([3]) that grew out of a computer lab assignment on the rail fence cipher, given in my Modern Algebra class. The rail fence cipher is a columnar transposition cipher using just two columns. Since the rail fence cipher is a permutation on the plaintext characters, group-theoretic results imply that a message enciphered with the rail fence may be deciphered by repeated re-encipherment. The results of my paper revolve around calculations of the minimal number of encipherments it takes to accomplish this, a number known as the *order* of the permutation. In the process, I discovered some interesting number-theoretic properties of the rail fence cipher. For example, the order of the rail fence cipher is a prime number p if and only if the length of the plaintext divides the Mersenne number $M_p = 2^p - 1$.

I have extended my work in cryptology beyond the scholarship of discovery in several ways. I designed and taught (on two different occasions) an upper-division special topics course on cryptology. The course has featured student expository research on such topics as digital steganography, quantum computing, and wi-fi encryption protocols as well as a collaborative student wiki on cryptology during World War II (<http://enigma.wikispaces.com>). I have also built cryptology-flavored components into my course on Methods of Problem Solving, and I give an annual two-week minicourse on cryptology to students in the freshman course Introduction to the Mathematical Sciences. I designed and taught an interdisciplinary liberal arts course titled “Cryptology, Privacy, and Leadership” for students with no mathematics or computing backgrounds which deals with cryptography in the context of privacy, identity theft, and civil liberties issues.

Regarding my near-term goals for continued involvement with cryptology, I intend to continue my reading, and perhaps take coursework, in cryptology and allied areas (such as number theory, probability, information

theory, and programming languages) to develop my overall breadth of knowledge. I would also like to bolster my knowledge in cryptanalysis (codebreaking) to complement my knowledge of cryptography (codemaking), with my eventual goal being to work through Bruce Schneier’s self-study course on block cipher cryptanalysis ([2]). Finally, to add depth to my breadth, I intend to continue a reading program of technical research papers on areas of cryptology that are particularly amenable to my background, such as the discrete logarithm problem and multivariate public-key cryptography.

My long-term goals for cryptology are twofold. First, I want to create and maintain a wide variety of opportunities for student involvement in the field. These would include the design and offering of liberal arts or interdisciplinary courses for nonmajors, similar to the “Cryptology, Privacy, and Leadership” course; curricular units in cryptology for existing courses; the design and regular offering of an upper-level cryptology course; and ongoing individual work with students via independent studies and undergraduate research. Second, to ensure that I can support this level of student activity, I want to attain a depth of knowledge in an active sub-area of cryptology to the extent that I can produce original research in the field, ideally through collaboration with experts in a primarily research-oriented environment.

Another area of scholarship has been the use of technology in collegiate mathematics teaching. I am interested in how the use of technology – including but not limited to computer algebra systems, computer programming, dynamic geometry software, wikis, and spreadsheets – can help students solve problems and do creative work in different mathematical subjects. Most recently, I wrote a paper ([6]) on the use of wikis as tools for collaborative upper-division course projects, highlighting wikis that students created in my Cryptology and Modern Algebra courses. Another area of interest is how best to incorporate computer programming in the college mathematics major. I am currently developing a one-hour course that would teach the fundamentals of MATLAB programming and then design programming experiences throughout the curriculum.

I enjoy working with educational technology and intend to continue trying new things in this area and disseminating the results. My future plans for this area include expanding my technological repertoire to learn more about numerically-oriented computer algebra systems such as MATLAB, advanced uses of spreadsheets, and computer programming and scripting languages. I also want to continue to use Web 2.0 software, such as wikis and blogs, to enhance students’ creative work in all my courses, building on what I have already done with my upper-level courses. As the technology develops rapidly, I want to stay fluent in the best of current technology, deepen my understanding of its workings, and contribute to our knowledge of its social and educational implications.

My scholarship in cryptology and in educational technology has been enjoyable and fruitful for both me and my students, and I look forward to continuing this work throughout my career.

References

- [1] E. Boyer. *Scholarship Reconsidered: Priorities of the Professoriate*. New York: Jossey-Bass, 2000.
- [2] B. Schneier. “A self-study course in block-cipher cryptanalysis.” *Cryptologia*, **24**(1): 18–34, 2000.
- [3] R. Talbert. “The cycle structure and order of the rail fence cipher.” *Cryptologia*, **30**(2):159–172, 2006.
- [4] R. Talbert. “An isomorphism between Bredon and Quinn homology via homotopy colimits.” *Forum Mathematicum*, **11**:591–616, 1999.
- [5] R. Talbert. “Stratified and equivariant homology via homotopy colimits”. Ph.D. dissertation, Vanderbilt University, August 1997.
- [6] R. Talbert. “A tale of two wikis: Upper-level mathematics meets Web 2.0.” To appear in *Electronic Proceedings of the ICTCM 2008*.