1046-15-1959 **Gregory V Bard*** (bard@fordham.edu), Department of Mathematics, John Mulcahey Hall,
Room 421, Fordham University, The Bronx, NY 10458, and **Robert Miller** (rlm@rlmiller.org).

Ultra-Sparse Matrix Reduction to Reduced Row-Echelon Form for matrices over $GF(2)$.

Reducing matrices over $GF(2)$ to their Reduced Row-Echelon Form is a core part of the F4 algorithm for solving polynomial systems of equations over finite (or other) fields. This in turn is a crucial step in algebraic cryptanalysis. Furthermore, the matrices are often sparse.

Treating sparse matrices as if they were dense is unwise, because Gaussian Elimination will cause the matrix to become dense after a few small iterations. A long series of known techniques relating to graph theory exist for the identical problem over the real numbers, but require modification to work over $GF(2)$. In particular, the standard technique (the "min degree algorithm") works on positive semi-definite symmetric matrices. For matrices M that are not symmetric, or positive semi-definite, or even those that are rectangular, M^TM is used instead, which will be positive semi-definite and symmetric. But over characteristic two, this fails because the null-space of M^TM might be larger than the null-space of M—impossible in characteristic zero. We construct a new algorithm, using similar methods, but taking advantage of the properties of the relationships between matrices and graphs that remain unchanged when moving from characteristic zero to characteristic two. (Received September 16, 2008)