1046-68-1837 **Daniel S. Roche*** (droche@cs.uwaterloo.ca), School of Computer Science, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 6P7, Canada. *Fast Multiplication with Low Space Complexity.* Preliminary report.

The multiplication of arbitrary-precision integers and univariate polynomials over finite fields is one of the fundamental components of any computer algebra system. The classical algorithm has time complexity $O(n^2)$, but this has been improved on many times, first by Karatsuba/Ofman, and later by Toom/Cook, Schönhage/Strassen, Cantor/Kaltofen, and others. However, all of the "faster" multiplication algorithms require at least $O(n)$ auxiliary storage space for their implementation, whereas the classical algorithm can be implemented with $O(\log n)$ space.

We present new algorithms with the same time complexity as Karatsuba multiplication, that is, $O(n^{1.59})$, but with only $O(\log^2 n)$ auxiliary storage space required, as well as the space for the result. This is achieved by following the general divide-and-conquer scheme of Karatsuba, but with extra restrictions on the recursive calls, so that at each recursive step only a constant amount of extra words of memory are needed. We also present an FFT-based algorithm for multiplication which uses just $O(\log n)$ extra space, but unfortunately works only when the size of the output is a power of 2. (Received September 16, 2008)