1014-12-1541 **Gadiel Seroussi*** (gadiel@msri.org). *Word-oriented PN sequence generation and polynomials of special forms over* $\mathbb{F}_{2^m}$. Preliminary report.

There has been recent increased interest in word-oriented linear feedback shift registers (LFSRs) that process a vector of bits (typically, a computer word of, say, 8, 16, 32, or 64 bits) at each clock cycle. The interest stems from the need to generate long-period binary pseudo-noise (PN) sequences at very high speed. In 2002, Tsaban and Vishne proposed *linear transformation shift registers* (TSRs) as a design methodology for this purpose, and studied the conditions under which these circuits generate maximal period sequences. We show that (TSRs) of maximal period for m-bit words are essentially equivalent to conventional LFSRs over $\mathbb{F}_{2^m}$. Furthermore, by carefully choosing the parameters and field representations employed, the complexity of the designed circuits can be significantly reduced. Minimal complexity circuits hinge on the availability of irreducible and primitive polynomials of certain forms over $\mathbb{F}_{2^m}$. We discuss facts and conjectures regarding the existence of such polynomials. (Received September 28, 2005)