MEMO NUMBER: GFAU SRS
DATE: January 31, 2018
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: URCAD Abstract Draft

1 Introduction

A Galois Field is a field with a finite number of elements. The nomenclature $GF(q)$ is used to indicate a Galois Field with q elements. In $GF(q)$, the parameter q must be a power of a prime. For each prime power there exists exactly one finite field. The binary field $GF(2)$ is the most frequently used Galois field (**?**).

The Galois Field Arithmetic Unit will handle irreducible polynomials in $GF(2^n)$, where $2 \leq n \leq 16$. The arithmetic logic unit (ALU) will generate all the terms in the field of the polynomial, and allow the user to view and apply the following Galois operations: addition, subtraction, multiplication, division and logarithm.