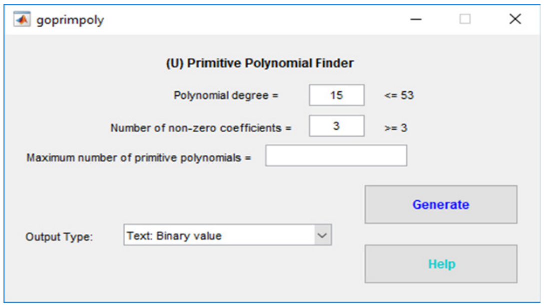
GOPRIMPOLY

SCR#
2494

MATLAB

MAC,
WINDOWS,
LINUX

GOPRIMPOLY is an application for efficiently finding binary primitive polynomials from order 16 to 53



goprimpoly

(U) Primitive Polynomial Finder

Polynomial degree = 15 <= 53

Number of non-zero coefficients = 3 >= 3

Maximum number of primitive polynomials =

Output Type: Text: Binary value

Robust error detection techniques are vital for reliable and efficient digital communication. Commonly occurring digital communication errors and changes are often a result of factors such as noise and interference. Cyclic redundancy check (CRC) is an error detection method for finding burst errors up to the length of the CRC used. CRC generator polynomials using the factor (x+1) times the primitive polynomial can detect up to 3 errors for messages up to a length of approximately 2^d bits where d is the degree of the polynomial. Using larger generator polynomials creates very low probability of undetected errors for short message lengths. The factoring of polynomials has been a well-known and researched problem, particularly for degree $m \le 16$.

Sandia researchers have developed the GOPRIMPOLY application and primitive polynomial search algorithm to efficiently determine primitive binary polynomials from order 16 to 53. Using GOPRIMPOLY, the user can select the number of non-zero coefficients of the primitive polynomial in order to find binary primitive polynomials with the desired characteristic. GOPRIMPOLY is a self-contained Matlab executable and requires the Matlab Compile Runtime (MCR) to execute in a target machine without the need for the full Matlab application. If the user has the full Matlab application, the application can run from the command line. In addition, if the user has the application with the parallel toolbox enabled, the application can exploit multi-core processors. With this tool, many different generator polynomials can be examined and various output options are possible, including results similar to those from Matlab's "primpoly" function.

TECHNICAL BENEFITS

- Efficiently determines primitive polynomials up to order 53 or larger if a separate method is available
- Billions of candidate polynomials for high degrees can be treated using subsets of the polynomials and limit memory requirements
- Nearly eightfold increase in speed and efficiency using 8-core processor
- Ease of use. Includes GUI interface and user manual

INDUSTRIES & APPLICATIONS

- Cyclic Redundancy Check (CRC)
- Random number generators using linear feedback shift registers (LFSR)
- Digital communications companies
- Digital content generation
- Mathematical toolboxes

ip.sandia.gov
ip@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2020-9635 M