Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Conversion of element representations in Galois rings

Juan Carlos Ku-Cauich[1], Guillermo Morales-Luna[2]

A Galois ring is a finite ring with unity such that the divisors of zero, together with zero itself, form a principal ideal, generated by an element of the form pe, where e is the ring unit and p is a prime number. For any prime p and two integers s, m, the map

$$\pi_p : \mathbb{Z}_{p^s}[X] \to \mathbb{F}_p[X]\ ,\ g(X) = \sum_{j=0}^{m-1} a_j X^j \mapsto g(X) \bmod p = \sum_{j=0}^{m-1} (a_j \bmod p) X^j,$$

is a ring homomorphism. An irreducible polynomial $h(X) \in \mathbb{Z}_{p^s}[X]$ is basic if $\pi_p(h(X))$ is irreducible in $\mathbb{F}_p[X]$ and in this case $\mathbb{Z}_{p^s}/\langle h(X)\rangle$ is a Galois ring, denoted $GR(p^s, m)$. Let $\eta = X + \langle h(X)\rangle \in GR(p^s, m)$, then $h(\eta) = 0$ and $\mathbb{F}_{p^m} \approx [\mathbb{Z}_p[X]/\langle \pi_p(h(X))\rangle]$. Hence, $GR(p^s, m) = \mathbb{Z}_{p^s}[\eta]$ and each element in the Galois ring can be written in an additive form: $\sum_{j=0}^{m-1} a_j \eta^j$, with $a_j \in \mathbb{Z}_{p^s}$.

A polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ is basic primitive if $\pi_p(g(X))$ is primitive in $\mathbb{F}_p[X]$. It is well known [4] that there is an element $\xi \in GR(p^s, m)$ and a basic primitive polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ of degree m such that $o(\xi) = p^m - 1$, $g(\xi) = 0$, $g(X)|(X^{p^m-1} - 1)$ in $\mathbb{Z}_{p^s}[X]$ and the following two properties hold:

- $GR(p^s, m) = \mathbb{Z}_{p^s}[\xi]$
- Each element in $GR(p^s, m)$ can be written uniquely in a p-adic form: $\sum_{k=0}^{s-1} b_k p^k$, with $b_k \in \mathcal{T}(g(X))$, where $\mathcal{T}(g(X)) = \{0\} \cup \left(\xi^i\right)_{i=0}^{p^m-2}$ is a Teichmüller set.

Each primitive polynomial in $\mathbb{F}_p[X]$ characterizes a set of basic primitive polynomials in $\mathbb{Z}_{p^s}[X]$, namely its inverse image under the projection π_p. The p-adic representation depends on the chosen basic primitive polynomial.

We have developed a series of programs, basically in `sage`, to find monic basic primitive polynomials and convert additive representations into p-adic representations of the Galois ring elements, and conversely.

For any $m \in \mathbb{Z}^+$ there is [2] a monic primitive polynomial $f_{pm}(X) \in \mathbb{F}_p[X]$ dividing $P_{pm}(X) = X^{p^m-1} - 1$ in $\mathbb{F}_p[X]$. Then, by Hensel Lift [3] there is a monic basic primitive polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ dividing $P_{pm}(X)$ in $\mathbb{Z}_{p^s}[X]$ with projection $f_{pm}(X)$. Since $f_{pm}(X) \in \mathbb{F}_p[X]$ is irreducible with no multiple roots, the polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ is unique [4]. Hence, a natural correspondence $f_{pm}(X) \leftrightarrow f_{psm}(X)$ arises, and in most cases it is not the identity, namely $f_{pm}(X) \neq f_{psm}(X)$ in $\mathbb{Z}_{p^s}[X]$.

In the worst case, for small values of m and s the search of the Hensel lift polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ can be done exhaustively. Alternatively, a list [2] of monic primitive polynomials in the ring $\mathbb{F}_p[X]$ may be provided in order to consider the inverse images of those polynomials under the projection modulus p.

The interest in finding effective and efficient representation conversions is due to the implementation of authentication codes based on the Gray transform [1].

Keywords: Galois rings, Teichmüller elements, symbolic computation

References

[1] Juan Carlos Ku-Cauich and Horacio Tapia-Recillas. Systematic authentication codes based on a class of bent functions and the Gray map on a Galois ring. *SIAM J. Discrete Math.*, 27(2):1159–1170, 2013.

[2] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[3] B.R. McDonald. *Finite Rings With Identity*. Pure and Applied Mathematics Series. Marcel Dekker Incorporated, 1974.

[4] Z.X. Wan. *Lectures on Finite Fields and Galois Rings*. World Scientific, 2003.

[1]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
jckc35@hotmail.com

[2]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
gmorales@cs.cinvestav.mx