On the Hensel Lift of a Polynomial

Zhe-Xian Wan
Dept of Information Technology
Lund University
P.O. Box 118
SE-221 00 Lund, Sweden
e-mail: wan@it.lth.se

Abstract — **Denote by R the Galois ring of characteristic p^e and cardinality p^{em}, where p is a prime and e and m are positive integers. Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$. A polynomial $f(x)$ over R is defined to be a Hensel lift of $g(x)$ in $R[x]$ if $\overline{f}(x) = g(x)$, where $-$ is the natural homomorphism from R onto $\mathbb{F}_{p^m}$, and there is a positive integer n not divisible by p such that $f(x)$ divides $x^n - 1$ in $R[x]$. It is proved that $g(x)$ has a unique Hensel lift in $R[x]$ if and only if $g(x)$ has no multiple roots and $x \nmid g(x)$. An algorithm to compute the Hensel lift is also given.**

I. Definition

In 1995 the following definition of the Hensel lift of a polynomial appeared in [1].

Let $h_2 \in \mathbb{F}_2[x]$ be of degree $m > 0$ and assume that $h_2|(x^l - 1)$ and l is minimal subject to this property. There is a unique monic polynomial $h \in \mathbb{Z}_4[x]$ of degree m such that $\overline{h} = h_2$ and $h|(x^l - 1)$ in $\mathbb{Z}_4[x]$. This polynomial is called the Hensel lift of $h_2(x)$.

In the above definition the condition that l is odd should be added. A counter-example when l is even is: $h_2(x) = (x-1)^2(x^2+x+1)$, $h_2 \mid (x^6-1)$ in $\mathbb{F}_2[x]$, $h = (x^2-1)(x^2+x+1)$ and $h' = (x^2-1)(x^2-x+1)$.

The formulation of the above definition involves some statements which should be proved. Now we suggest a simpler definition which can be formulated for an arbitrary Galois ring. For Galois rings, see [2] and [3].

Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$. A monic polynomial $f(x)$ over R is called a **Hensel lift** of $g(x)$ if $\overline{f}(x) = g(x)$ and there is a positive integer n not divisible by p such that $f(x)|(x^n - 1)$ in $R[x]$.

II. Existence and Uniqueness

Proposition 1. A monic polynomial $g(x)$ over $\mathbb{F}_{p^m}$ has a Hensel lift $f(x)$ over R if and only if $g(x)$ has no multiple roots and $x \nmid g(x)$ in $\mathbb{F}_{p^m}[x]$.

Lemma 2. Let n_1 and n_2 be positive integers and $n = \gcd(n_1, n_2)$. Then $x^n - 1 = \gcd(x^{n_1} - 1, x^{n_2} - 1)$ in $\mathbb{F}_{p^m}[x]$, $(x^n - 1)|(x^{n_1} - 1)$ in $R[x]$, and $(x^n - 1)|(x^{n_2} - 1)$ in $R[x]$.

Proposition 3. Let $g(x)$ be a monic polynomial over $\mathbb{F}_{p^m}$ without multiple roots and $x \nmid g(x)$ in $\mathbb{F}_{p^m}[x]$. Then $g(x)$ has a unique Hensel lift in $R[x]$.

III. An Algorithm to Compute the Hensel Lift

Based on Propositions 1 and 3 of the proceeding section we formulate the following algorithm for computing the Hensel lift of a monic polynomial over $\mathbb{F}_{p^m}$ in $R[x]$.

Algorithm Given a monic polynomial $g(x)$ of degree > 0 over $\mathbb{F}_{p^m}$ to compute the Hensel lift of $g(x)$ in $R[x]$ we proceed in the following steps.

1. Test whether $x|g(x)$ in $\mathbb{F}_{p^m}[x]$.
   If yes, we are finished and $g(x)$ has no Hensel lift in $R[x]$.
   If no, go to step 2.
2. Compute $\gcd(g(x), g'(x))$ and let it be $d(x)$.
   If $\deg d(x) > 0$, we are finished and $g(x)$ has no Hensel lift in $R[x]$.
   If $\deg d(x) = 0$, go to step 3.
3. Factorize $g(x)$ into a product of distinct monic irreducible polynomials over $\mathbb{F}_{p^m}$ by Berlekamp's Algorithm. Let the result be
   $$g(x) = g_1(x)g_2(x)\dots g_r(x),$$
   where $g_1(x), g_2(x), \dots, g_r(x)$ are distinct monic irreducible polynomial over $\mathbb{F}_{p^m}$. Let $\deg g_i(x) = n_i, i = 1, 2, \dots, r$ and go to step 4.
4. Compute $\mathrm{lcm}[p^{mn_1} - 1, p^{mn_2} - 1, \dots, p^{mn_r} - 1]$. Let the result be n, then p does not divide n and $g(x)|(x^n - 1)$. Go to step 5.
5. Divide $x^n - 1$ by $g(x)$ by division algorithm. Let the quotient be $g_1(x)$. Then $x^n - 1 = g(x)g_1(x)$ and $\gcd(g(x), g_1(x)) = 1$. Go to step 6.
6. By the constructive proof of Hensel's Lemma construct two coprime monic polynomials $f(x)$, $f_1(x) \in R[x]$ such that $x^n - 1 = f(x)f_1(x)$ in $R[x]$ and $\overline{f}(x) = g(x), \overline{f}_1(x) = g_1(x)$. Then $f(x)$ is the Hensel lift of $g(x)$ in $R[x]$. □

When $\mathbb{F}_{p^m} = \mathbb{F}_2$ and $R = \mathbb{Z}_4$, the Hensel lift of a polynomial $g(x)$ over $\mathbb{F}_2$ without multiple roots and not divisible by x can be calculated by using Graeffe's method for finding a polynomial whose roots are the squares of the roots of $g(x)$, see [4] and [5].

References

[1] Bonnecaze, A., Sole, P, and Calderbank, A. R., "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory* **41**(1995), 366–377.

[2] Krull, W., "Algebraische Theorie der Ringe," *Math. Ann.* **92**(1924), 183–213.

[3] MacDonald, B. R., *Finite Rings with Identity*, Marcel Dekker, 1974.

[4] Uspensky, J. V., *Theory of Equations*, McGraw-Hill, 1948.

[5] Wan, Z.-X., *Quaternary Codes*, World Scientific, Singapore, 1997.