AAECC 6, 171–173 (1995)

AAECC
Applicable Algebra in Engineering, Communication and Computing

Fast Evaluation of Rédei Functions*

Willi More

Department of Mathematics, University of Klagenfurt, A-9020 Klagenfurt, Austria
willi.more@uni-klu.ac.at

Received November 3, 1993; revised version March 15, 1994

Abstract. We introduce a fast evaluation algorithm for Rédei functions of complexity $O(\log_2 n)$. Rédei functions are of interest in cryptographic applications and primality testing.

Keywords: Rational functions, Finite Fields, Integers mod m, Primality testing, Public key cryptography, Key distribution systems

Introduction

Let R an arbitrary commutative unitary finite Ring and let $t(x) = x^2 - ax - b$ denote a polynomial over R with the two different roots $\alpha, \bar{\alpha}$. It can easily be shown that there always exist unique elements $r_k, s_k \in R$ such that

$$\alpha^k = r_k + \alpha s_k \quad \text{and} \quad \bar{\alpha}^k = r_k + \bar{\alpha} s_k \quad \text{for all } k \in \mathbb{N}.$$

So for $n \geqq 1$ by the binomial theorem we have

$$\begin{aligned}(x+\alpha)^n &= \sum_{k=0}^{n} \binom{n}{k} \alpha^k x^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} r_k x^{n-k} + \alpha \sum_{k=0}^{n} \binom{n}{k} s_k x^{n-k} \\ &= g_n(x) + \alpha h_n(x)\end{aligned}$$

where $g_n(x), h_n(x) \in R[x]$ are coprime over R.

The rational function

$$R_n(x) = \frac{g_n(x)}{h_n(x)}$$

is called *Rédei function of degree n with respect to* $t(x)$.

---

* This paper was partially supported by the *Österreichischen Fonds zur Förderung der wissenschaftlichen Forschung* under FWF project P9272

Rédei functions $R_n(x)$ over finite fields with respect to $t(x) = x^2 - b$ and b not a square were introduced by Rédei [14], with slight modifications in the definition as moving to $\mathbb{Z}_m$ and using arbitrary quadratic polynomials $t(x)$ by R. Nöbauer [8], [9] and W. Nöbauer [10], [11] as well as moving to arbitrary commutative unitary finite rings by Pieper [13]. The results by Pieper still hold using arbitrary quadratic polynomials $t(x)$ since the extension ring $R[x]/(t(x))$ is R-isomorphic to the quadratic R-algebra $R[\sqrt{\eta}], \eta \in R^\times$ (cf. [12]).

Rédei functions $R_n(x)$ over R are closed with respect to composition and satisfy the commuting property

$$R_{n_1}(x) \circ R_{n_2}(x) = R_{n_1 n_2}(x) = R_{n_2 n_1}(x) = R_{n_2}(x) \circ R_{n_1}(x).$$

The commuting property is one of the main reasons why Rédei functions are of interest in cryptographic applications for secret-key and public-key cryptosystems as proposed by Lidl and Müller [2] and investigated by R. Nöbauer [5], [6], for key distribution systems as proposed by R. Nöbauer [7] and for primality testing as proposed by Lidl and Müller [3]. A comprehensive up-to-date collection of results concerning Rédei functions and their relations to Dickson polynomials is given by Lidl, Mullen and Turnwald [1].

All these applications require a fast evaluation algorithm. The algorithms proposed by Lidl, Mullen and Turnwald [1, Lemma 2.29] and by More [4] are restricted to Rédei functions invented by Rèdei and the first one is also restricted to calculations in the extension ring $R[x]/(t(x))$. These restrictions can be dropped by the following algorithm maintaining same complexity $O(\log_2 n)$.

Recurring Sequences

The following Lemma can be obtained easily by induction on n from the defining equation $(x + \alpha)^n = g_n(x) + \alpha h_n(x)$ of Rédei functions.

Lemma. *The polynomials $g_n(x)$ and $h_n(x)$ satisfy the recurrence relations*

$$g_n(x) = x g_{n-1}(x) + b h_{n-1}(x)$$
$$h_n(x) = g_{n-1}(x) + (x + a) h_{n-1}(x)$$

for all $n > 1$ with initial values $g_1(x) = x$ and $h_1(x) = 1$.

As an immediate consequence follows

Corollary. *$R_n(x)$ satisfy the recurrence relation*

$$R_n(x) = \frac{x R_{n-1}(x) + b}{R_{n-1}(x) + (x + a)}$$

for all $n > 1$ with initial value $R_1(x) = x$.

Substituting $2n + 1$ for n and combining with the commuting property for $n_1 = 2$, $n_2 = n$ leads to a fast evaluation algorithm of complexity $O(\log_2 n)$ with respect to addition, subtraction and multiplication in R using

$$R_{2n+1}(x) = \frac{x R_{2n}(x) + b}{R_{2n}(x) + (x + a)} \quad R_{2n}(x) = R_2(x) \circ R_n(x) = \frac{R_n^2(x) + b}{2R_n(x) + a}.$$

Fast Evaluation Algorithm

This algorithm evaluates the Rédei function $R_n(x)$ of degree $n \geqq 1$ with respect to $t(x) = x^2 - ax - b$.

A1. [Initialize.] Let $\sum_{k=0}^{l} b_k 2^k$ the binary representation of $n \geqq 1$ with $b_k \in \{0, 1\}$. Set $i \leftarrow l - 1$ and $R(x) \leftarrow x$.

A2. [$i < 0$?] If $i < 0$, the algorithm terminates, with $R(x)$ as the answer.

A3. [Evaluate.] Set $R(x) \leftarrow \dfrac{R^2(x) + b}{2R(x) + a}$.

If $b_i = 1$, set $R(x) \leftarrow \dfrac{xR(x) + b}{R(x) + (x + a)}$.

Set $i \leftarrow i - 1$ and return to step A2.

References

1. Lidl, R., Mullen, G. L., Turnwald, G.: Dickson Polynomials. Pitman Monographs and Surveys in Pure and Applied Mathematics vol. **65**. Harlow: Longman 1993
2. Lidl, R., Müller, W. B.: Permutation polynomials in RSA-cryptosystems. In: Advances in Cryptology. Proceedings of the Crypto '83, pp. 293–301. New York: Plenum Press 1984
3. Lidl, R., Müller, W. B.: Generalization of the Fibonacci pseudoprime test. Discrete Math. **92**, 211–220 (1991)
4. More, W.: Rasches Auswerten von Rédei-Funktionen. Anz. Österreich. Akad. Wiss. Math.-Natur. Kl. **128**, 69–72 (1991)
5. Nöbauer, R.: Cryptoanalysis of the Rédei-scheme. In: Contributions to General Algebra vol. **3**, pp. 255–264. Vienna: Hölder-Pichier-Tempsky 1985
6. Nöbauer, R.: Rédei-Funktionen und ihre Anwendungen in der Kryptographie. Acta Sci. Math. (Szeged) **50**, 287–298 (1986)
7. Nöbauer, R.: Key distribution systems, based on polynomial functions and Rédei functions. Problems Control Inform. Theory **15**, 91–100 (1986)
8. Nöbauer, R.: Rédei-Permutationen endlicher Körper. In: Contributions to General Algebra vol. **5**, pp. 235–246. Vienna: Hölder-Pichler-Tempsky 1987
9. Nöbauer, R.: Rédei-Permutationen auf Restklassenringen $Z/(m)$. Monatshefle. Math. **106**, 41–56 (1988)
10. Nöbauer, W.: Über die Zyklenlänge der Rédei-Permutationen. Anz. Österreich. Akad. Wiss. Math.-Natur. Kl. **121**, 121–123 (1984)
11. Nöbauer, W.: Rèdei-Funktionen für Zweierpotenzen. Period. Math. Hungar. **17**, 37–44 (1986)
12. Pieper, R.: Kryptoanalytische Untersuchungen rationaler Permutationen von kommutativen unitären Ringen. Dissertation, Universität Dortmund 1990
13. Pieper, R.: Cryptanalysis of Rédei- and Dickson Permutations on Arbitrary Finite Rings. AAECC **4**, 59–76 (1993)
14. Rédei, L.: Über eindeutig umkehrbare Polynome in endlichen Körpern. Acta Sci. Math. (Szeged) **11**, 85–92 (1946)