SOLVING QUADRATIC EQUATIONS
OVER POLYNOMIAL RINGS
OF CHARACTERISTIC TWO

JØRGEN CHERLY, LUIS GALLARDO,
LEONID VASERSTEIN AND ÉTHEL WHELAND

Abstract

We are concerned with solving polynomial equations over rings. More precisely, given a commutative domain $A$ with 1 and a polynomial equation $a_n t^n + \cdots + a_0 = 0$ with coefficients $a_i$ in $A$, our problem is to find its roots in $A$.

We show that when $A = B[x]$ is a polynomial ring, our problem can be reduced to solving a finite sequence of polynomial equations over $B$. As an application of this reduction, we obtain a finite algorithm for solving a polynomial equation over $A$ when $A$ is $F[x_1, \ldots, x_N]$ or $F(x_1, \ldots, x_N)$ for any finite field $F$ and any number $N$ of variables.

The case of quadratic equations in characteristic two is studied in detail.