1020-14-117 **Dieter S Schmidt*** (dieter.schmidt@uc.edu), Department of Computer Science, Cincinnati, OH 45221-0030. *Zhuang-Zi: A new algorithm for solving multivariable polynomial equations over a finite field.* Preliminary report.

The Zhuang-Zi algorithm was proposed by Jintai Ding for solving polynomial equations

$$f_i(x_1, \ldots, x_n) = 0, \qquad i = 1, \ldots, n \tag{1}$$

when the coefficients come from a finite field G of size q and the solutions $x_1, \ldots, x_n$ have to be found in the same field. With the help of an extension field the set of polynomials can be written as a single polynomial $F(X) = 0$. The solution X has to be found in a field of size q^n and it will correspond to the solutions of (1).

In practical examples the degree of $F(X)$ will be very high. We will present methods for reducing the degree of $F(X)$, so that the roots of the polynomial can be found by one of the standard methods. We will discuss our experience in implementing this algorithm on a computer. Since solving (1) is known to be NP-hard we can not expect that the Zhuang-Zi algorithm will always succeed. Nevertheless, it will succeed in some cases where the Gröbner bases method fails and vice versa. (Received August 22, 2006)