1. INTRODUCTION

Currently, it has become evident that solution of a wide class of applied problems requires combining symbolic, numerical, and graphical computer methods. Many of these problems reduce to the solution of systems of algebraic, differential, or even finite-difference equations. In the case of nonlinear problems (with few exceptions), the desired solution can be obtained only numerically. In many cases, however, computer algebra methods allow one to extract useful information from the system of equations without finding its exact solution. One of the most universal methods for obtaining such information relies on the use of Gröbner bases. An algorithm for construction of Gröbner bases in the case of algebraic systems of polynomial type was suggested by Buchberger [1, 2] a little more than 40 years ago. Since then, Gröbner bases have become a powerful tool for solving algebraic polynomial equations in many unknowns, which arise in various fields of mathematics and natural sciences. In addition to the Buchberger algorithm [2], other, more effective, algorithms for computation of Gröbner bases, such as the involutive algorithm [3, 4] and Faugère’s algorithms $F_4$ and $F_5$ [5, 6], were developed during last decade.

Moreover, by way of direct extending the Buchberger and involutive algorithms, Gröbner bases found useful applications in some noncommutative algebras [7] and in studies of linear differential and difference systems of equations [7–9]. In the general case of systems of equations with polynomial dependence on unknowns (functions) and algorithmically computable coefficients (for example, rational functions of parameters (independent variables in the case of differential systems) over the field of rational numbers), the Gröbner bases methods allow one to algorithmically

1. check compatibility of systems of equations;
2. find dimension of the solution space;
3. exclude some subset of variables, i.e., obtain consequences (if any) not containing variables from the given subset;
4. “split” the original system into a finite number of simpler systems, such that solutions of these systems altogether coincide with the solutions of the original system;
5. transform the system to the form convenient for solving and numerical analysis;
6. study symmetry and group properties of differential equations;
7. reveal existence of certain specific features, such as, for example, integrability in the sense of the inverse scattering problem for nonlinear differential equations of the evolutionary type for one spatial and one temporal variables.

It is important to note that, from the computer algebra point of view, analysis of very different mathematical objects, say, for example, differential or partial difference equations and polynomial algebraic ones, can be done by means of, basically, one and the same algorithm, namely, by means of the algorithm for construction of Gröbner bases for polynomial algebraic equations or its analogue for differential or difference equations.

However, the efficiencies of modern software products for computation of algebraic and differential (difference) Gröbner bases differ significantly. Great experience accumulated in optimizations of the algorithm
Input: a finite set \( F \in R(R') \setminus \{0\} \) of polynomials.

Output: an autoreduced Gröbner basis \( G \) for the ideal \( \text{Id}(F) \)

1: \( A := \emptyset \)
2: \textbf{for all} \( i = 1, \ldots, n \) \textbf{do}
3: \textbf{for all} \( f \in F \) \textbf{do}
4: \( A := A \cup \{ x_i \cdot f \} \)
5: \textbf{end for}
6: \textbf{end for}
7: \( G := \text{AutoReduce}(F \cup A) \)
8: \( k := \text{card}(G) \)
9: \( B := \{ [i, j] : 1 \leq i < j \leq k \} \)
10: \textbf{while} \( B \neq \emptyset \) \textbf{do}
11: \( [i, j] := \text{SelectPair}(B, G) \)
12: \( B := B \setminus \{ [i, j] \} \)
13: \textbf{if} \( \text{criterion1}([i, j], G) \) \textbf{and} \( \text{criterion2}([i, j], B, G) \) \textbf{then}
14: \( h := \text{NormalForm}((\text{Spoly}(G_i, G_j), G)) \)
15: \textbf{if} \( h \neq 0 \) \textbf{then}
16: \( G := G \cup \{ h \} \)
17: \( k := k + 1 \)
18: \( B := B \cup \{ [i, k] : 1 \leq i < k \} \)
19: \textbf{end if}
20: \textbf{end if}
21: \textbf{end while}
22: \( R := \{ g \in G \mid \exists q \in G \setminus \{0\}, \text{lt}(q) \not\subseteq \text{lt}(g) \} \)
23: \textbf{return} \( \text{AutoReduce}(G \setminus R) \)

Fig. 1. Algorithm Gröbner Basis\( (F) \).

for construction of Gröbner bases in commutative algebra has not yet been extended to the case of differential and difference equations. In addition to the fact that the algorithm generally does not stop for these equations, the basic problem consists in the detection of useless zero reductions and search for optimal strategies of selection of critical pairs (the Buchberger and Faugère algorithms) or nonmultiplicative prolongations (involutive algorithm).

In this paper, we consider specialized Buchberger and involutive algorithms designed for the case of systems of polynomials over the simplest finite field \( \mathbb{F}_2 \) with values of variables in \( \mathbb{F}_2 \). Such polynomial systems come to existence in quantum computation [10] when constructing unitary matrices for quantum circuits composed from Hadamard and Toffoli gates, which constitute a universal set of quantum gates, as well as in a number of cryptanalysis problems for cryptosystems with open key based on the difficulty of establishing isomorphism of polynomial systems over \( \mathbb{F}_2 \) [11–13].

2. BASIC DEFINITIONS AND NOTATION

We use the following notation:

\( \mathbb{N}_{\geq 0} \) is the set of nonnegative integers.

\( \mathbb{X} = \{ x_1, \ldots, x_n \} \) is a set of variables.

\( R = \mathbb{K}[\mathbb{X}] \) is a ring of polynomials over field \( \mathbb{K} \) of characteristic 0.

\( R' = \mathbb{F}_2[\mathbb{X}] \) is a ring of polynomials over field \( \mathbb{F}_2 \).

\( \tilde{R} = R'/(x_1^2 + x_1, \ldots, x_n^2 + x_n) \) is a quotient ring of ring \( R' \) over the ideal.

The greatest degree of variables in the polynomials of this ring is equal to one; i.e., they belong to the field \( \mathbb{F}_2 \). The multiplication of monomials in this ring is defined as follows:

\[
\begin{align*}
m_1 \cdot m_2 &= x_1^{i_1} \ldots x_n^{i_n} \cdot x_1^{j_1} \ldots x_n^{j_n} \\
&= x_1^{\max(i_1, j_1)} \ldots x_n^{\max(i_n, j_n)}.
\end{align*}
\]

Let us also define the least common multiple (LCM) and the greatest common divisor (GCD) in this field as

\[
\begin{align*}
\text{lcm}(m_1, m_2) &= \text{lcm}(x_1^{i_1} \ldots x_n^{i_n}, x_1^{j_1} \ldots x_n^{j_n}) \\
&= x_1^{\max(i_1, j_1)} \ldots x_n^{\max(i_n, j_n)},
\end{align*}
\]

\[
\begin{align*}
\text{gcd}(m_1, m_2) &= \text{gcd}(x_1^{i_1} \ldots x_n^{i_n}, x_1^{j_1} \ldots x_n^{j_n}) \\
&= x_1^{\min(i_1, j_1)} \ldots x_n^{\min(i_n, j_n)}.
\end{align*}
\]

\( \text{Id}(F) \) is an ideal in \( R \) generated by \( F \subset R \). Analogously, for the rings \( R' \) and \( \tilde{R} \).

\( \mathbb{M} = \{ x_1^{i_1} \ldots x_n^{i_n} \mid i_k \in \mathbb{N}_{\geq 0}, 1 \leq k \leq n \} \) is a monoid of monomials from \( R \). Analogously, for the ring \( R' \).