Classification of all the minimal bilinear algorithms for computing the coefficients of the product of two polynomials modulo a polynomial,

Part II: The algebra $G[u]/ < u^n >$

Amir Averbuch

Tel-Aviv University

Zvi Galil

Columbia University and Tel-Aviv University

Shmuel Winograd

IBM T.J. Watson Research Center

ABSTRACT

In this paper we will classify all the minimal bilinear algorithms for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \mathrm{mod} Q(u)^l$ where $\deg Q(u) = j$, $jl = n$ and $Q(u)$ is irreducible (over G) is studied. The case where $l = 1$ was studied in [1]. For $l > 1$ the main results are that we have to distinguish between two cases: $j > 1$ and $j = 1$. The case where $j > 1$ was studied in [5].

For $j = 1$ it is shown that up to equivalence every minimal ($2n-1$ multiplications) bilinear algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \mathrm{mod} u^n$ is done either by first computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ and then reduce them modulo u^n or by first computing the coefficients $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ and then reduce them modulo u^n and add $x_{n-1} y_0 u^{n-1}$ or by first computing the coefficients $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ and then reduce them modulo u^n and add $(x_{n-1} y_0 + x_0 y_{n-1}) u^{n-1}$

I. Introduction

Let G be a field, $G[u]$ be the polynomial ring in u over the field G, $\{x_0, x_1, \cdots, x_{n-1}\}$ and $\{y_0, y_1, \cdots, y_{n-1}\}$ are two sets of indeterminates, and let $P(u) = Q(u)^l = u^n + \sum_{i=0}^{n-1} a_i u^i$ be a monic polynomial, $a_i \in G$ and $Q(u)$ is irreducible (over G) $\deg Q(u) = j$ $(jl = n)$. Denote by $R(u)$ the polynomial $\sum_{i=0}^{n-1} x_i u^i$ by $S(u)$ the polynomial $S(u) = \sum_{i=0}^{n-1} y_i u^i$ whose coefficients are indeterminates, and by T_p the set of coefficients of the polynomial $\sum_{i=0}^{n-1} \psi_i u^i = R(u)S(u) \bmod P(u)$ where $\{\psi_0, \psi_1, \cdots, \psi_{n-1}\} \subset G(x_0, \cdots, x_{n-1}, y_0, \cdots, y_{n-1})$

This paper continues the flow of general results on the problem of classification of all the minimal algorithms for computing T_p begun in [1] and continued in [2], [3], [4] and [5] and on different type of bilinear forms as in [7], [8] and [9]. [1], [2], [3] and [4] are fully classified all the minimal algorithms for computing the T_p in algebraic extension field, i.e. $l = 1$ while in [5] and in this paper we are classifying all the minimal $(2n-1$ multiplications) bilinear algorithms for computing T_p when $l > 1$ $(P(u) = Q(u)^l)$. The case $l > 1$ and $j = \deg Q(u) > 1$ was investigated in [5]. There we laid up the technical foundations for classifying the minimal bilinear algorithms for computing T_p when $l > 1$ and $j \geq 1$. Therefore we will consult [5] closely and very often.

In this paper we will classify all the minimal bilinear algorithms for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod $P(u)$ where $P(u) = Q(u)^l$, $Q(u) = u - \xi$, $\xi \in G$ $(j = 1, l = n)$. Since the algebra $G[u]/ < u^n >$ is isomorphic to the algebra $G[v]/ < (v-\xi)^n >$ by the isomorphism σ such that $\sigma(u) = v + \xi$ then computation of $\underline{x} \times \underline{y}$ where $\times$ is the multiplication in $G[u]/ < u^n >$ and $\underline{x} = (x_0, \cdots, x_{n-1})^T$ $\underline{y} = (y_0, \cdots, y_{n-1})^T$ is equivalent to the algorithm which computes $\underline{x} o \underline{y}$ where o is the multiplication in $G[v]/ < (v-\xi)^n >$. Thus, for $j = 1$, the classification in this paper will be performed in the algebra $G[u]/ < u^n >$.

Since Theorem II.3 ([5]) will be the basis for our new algorithms we will repeat the lengthy discussion of this theorem here; Let $F = G(x_0, \cdots, x_l)$, $H = F(y_0, \cdots, y_m)$ where $x_0, \cdots, x_l$, $y_0, \cdots, y_m, u$ are distinct indeterminates over G. Let $R_l(u) = \sum_{i=0}^{l} x_i u^i, S_m(u) = \sum_{i=0}^{m} y_i u^i$ be two polynomials with indeterminates as coefficients. $T(u) = R_l(u)S_m(u)$ form a system of bilinear forms which are denoted by $T(u) = \sum_{i=0}^{l+m} \psi_i u^i$. We aim at classifying all the minimal $(l + m + 1$ multiplications [2]) algorithms for computing $\{\psi_0, \cdots, \psi_{l+m}\} \subset H$ over $B = G \cup \{x_0, \cdots, x_l\} \cup \{y_0, \cdots, y_m\}$. There are two ways for computing $R_l(u)S_m(u)$ using $l + m + 1$ multiplications. The first one uses the following identity:

$$R_l(u)S_m(u) = R_l(u)S_m(u) \bmod \prod_{i=0}^{m+l} (u - \alpha_i) \tag{1}$$

where $\alpha_i \in G \quad i = 0, \cdots, m + l$ are distinct. Therefore, choose $m + l + 1$ distinct elements of G. By using the Chinese Remainder Theorem (CRT) $R_l(u)S_m(u) \bmod \prod_{i=0}^{m+l}(u - \alpha_i)$ can be obtained by computing $R_l(u)S_m(u) \bmod (u - \alpha_i) = R_l(\alpha_i)S_m(\alpha_i)$ $i = 0, \cdots m + l$ and then using only multiplications by elements of G we obtain $R_l(u)S_m(u) \bmod \prod_{i=0}^{m+l}(u - \alpha_i)$.

The second way uses the identity:

$$R_l(u)S_m(u) = R_l(u)S_m(u) \bmod \prod_{i=1}^{m+l}(u-\beta_i) + x_l y_m \prod_{i=1}^{m+l}(u-\beta_i) \tag{2}$$

where $\beta_i \in G$ $i = 1, \cdots m+l$ are distinct. Therefore, $R_l(u)S_m(u) \bmod \prod_{i=1}^{m+l}(u-\beta_i)$ is computed by using the CRT. We get $l+m$ multiplications $R_l(\beta_i)S_m(\beta_i)$ $i = 1, \cdots, m+l$ and the $(l+m+1)$ - st multiplication is $x_l y_m$.

Theorem I.1 [2]: Every algorithm for computing the coefficients of $R_l(u)S_m(u)$ in $l+m+1$ multiplications uses either (1) or (2).

For $l > 1$ and $j = 1$ it is shown in this paper that up to equivalence every minimal ($2n-1$ multiplications) bilinear algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ is done either by first computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ (using Theorem I.1) and then reduce them modulo u^n or by first computing the coefficients $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ and then reduce them modulo u^n (using Theorem I.1) and add $x_{n-1}y_0u^{n-1}$ or by first computing the coefficients $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ (using Theorem I.1) and then reduce them modulo u^n and add $(x_{n-1}y_0 + x_0 y_{n-1})u^{n-1}$.

The paper is organized as follows. In the next section we present some necessary short background. Afterwards we will give detailed examples for each of the three types of algorithms. The detailed examples up-front will illustrate the technical aspects of the rest of the paper. In section IV we define the concept of equivalence relation on the class of algorithms we are about to classify. This class of transformations will be larger than the one mentioned in [5] but there will be some overlapping transformations. In section V we will analyze the structure of the matrix W where W is $n \times n$ G-matrix such that $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$. This analysis will be the main starting point for deriving all the algorithms. In sections VII-VIII we will do the detailed classification based on the results of section V.

II. Some background

From now on we will use the following notation: $\underline{x}^T, \underline{y}^T$ will denote a row vectors $\underline{x}^T = (x_0, \cdots, x_{n-1})$ $\underline{y}^T = (y_0, \cdots, y_{n-1})$. Computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ is the same as computing the coordinates values of $\underline{x} \times \underline{y}$ where $\times$ stands for multiplication in $G[u]/ < u^n >$.

For $G[u]/ < u^n >$, the comapnion matrix of u, denoted by U, is:

$$U = \begin{bmatrix} 00\ldots00 \\ 10\ldots00 \\ 01\ldots00 \\ \cdot\cdot \quad \cdot\cdot \\ \cdot\cdot \quad \cdot\cdot \\ \cdot\cdot \quad \cdot\cdot \\ 00\ldots10 \end{bmatrix} \tag{1}$$

then

$$(U)^j = j+1 \begin{bmatrix} 00\ldots00 \\ \cdot\cdot \quad \cdot\cdot \\ \cdot\cdot \quad \cdot\cdot \\ \cdot\cdot \quad \cdot\cdot \\ 10\ldots00 \\ 01\ldots00 \\ \cdot\cdot \quad \cdot\cdot \\ \cdot\cdot \quad \cdot\cdot \\ 00\ldots10 \end{bmatrix} \tag{2}$$

Therefore we obtain that the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$mod u^n, (i.e. the regular matrix representation determined by the basis $\{1, u, \cdots u^{n-1}\}$) are given by:

$$\begin{bmatrix} x_0 & 0 & \ldots & 0 & 0 \\ x_1 & x_0 & \ldots & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ x_{n-2} & x_{n-3} & \cdots & x_0 & 0 \\ x_{n-1} & x_{n-2} & \cdots & x_1 & x_0 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \cdot \\ \cdot \\ y_{n-2} \\ y_{n-1} \end{bmatrix} \tag{3}$$

Since $U^T = K^{-1}UK$ then

$$K = \begin{bmatrix} 00\cdots001 \\ 00\cdots010 \\ \cdot\cdot \quad \cdots \\ \cdot\cdot \quad \cdots \\ \cdot\cdot \quad \cdots \\ 01 \quad 000 \\ 10 \quad 000 \end{bmatrix} \tag{4}$$

Let A be a minimal bilinear algorithm for computing the coefficients of $\underline{x} \times \underline{y}$ then $\underline{\psi} = \underline{x} \times \underline{y} = A(\underline{x})(\underline{y}) = M\underline{m}$ where $\underline{\psi} = (\psi_0 \cdots, \psi_{n-1})^T$, M is $n \times 2n-1$ G-matrix, $m_{i,j} \in M$ $i = 1\cdots, n$ $j = 1\cdots, 2n-1$, $\underline{m} = (m_1 \cdots, m_{2n-1})^T, m_i = L_i(\underline{x})M_i(\underline{y})$ $i = 1\cdots, 2n-1$ $, L_i(\underline{x}) = \sum_{j=0}^{n-1} u_{ij}x_j = u_i^T\underline{x},\ u_{ij},\ t_{ij} \in G,\ M_i(\underline{y}) = \sum_{j=0}^{n-1} t_{ij}y_j = t_i^T\underline{y},\ u_i^T = (u_{i,0}\cdots, u_{i,n-1}),\ t_i^T = (t_{i,0}\cdots, t_{i,n-1}),\ i = 1\cdots, 2n-1$ and U is the companion matrix of $P(u) = u^n((1))$. From Lemma IV.1 ([5]) we have that if $A(\underline{x})\underline{y} = M\underline{m}$ then *rank* $M = n$ and there exist a non-singular $n \times n$ G-matrix W such that $M = (W^{-1}|W^{-1}\alpha)$.

Denote each row of W by $w_i^T = (w_{i,0}\cdots, w_{i,n-1})$ then from (4) we have that

$$\overline{w}_i^T = w_i^T K = (w_{i,n-1}\cdots, w_{i,0}) \ \ i = 1, \cdots, n \tag{5}$$

If $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ then the matrix α has the form

$$\alpha = \begin{bmatrix} \alpha_{1,1}\cdots & \alpha_{1,n-1} \\ \cdot & \cdot \\ \cdot & \cdot \\ \alpha_{n,1}\cdots & \alpha_{n,n-1} \end{bmatrix}$$

From Lemma IV.2 ([5]) and from (2) and (4) we get that the regular matrix representation of $U_{\overline{w}_i} = \sum_{k=0}^{n-1} \overline{w}_{i,k} U^k$ has the form:

$$U_{\overline{w}_i} = \begin{bmatrix} w_{i,n-1} & 0 & \cdots & 0 & 0 \\ w_{i,n-2} & w_{i,n-1} & \cdots & 0 & 0 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ w_{i,1} & w_{i,2} & \cdots & w_{i,n-1} & 0 \\ w_{i,0} & w_{i,1} & \cdots & w_{i,n-2} & w_{i,n-1} \end{bmatrix} \qquad (6)$$

Since $j = 1$ then from Lemma IV.3 ([5]) there is at least one invertible row in $\overline{W}$. As mentioned in Remark IV.1 ([5]) we assume that always $\overline{w}_n$ is invertible, then the following are equivalent

$$w_{n,n-1} \neq 0,\ U_{\overline{w}_n} \text{ is non-singular},\ \delta(\overline{w}_n) = 0 \qquad (7)$$

where if $a = \sum_{k=0}^{n-1} g_k u^k$, $(j = 1)$ $a \in G[u]/ < u^n >$, $g_k \in G$ $k = 0 \cdots, n-1$ then $\delta(a)$, which is the dimension of the null space of the polynomial a, is defined as

$$\delta = \delta(a) = \begin{bmatrix} 0 \text{ if } g_0 \neq 0 \\ 1 \text{ if } g_0 = 0, g_1 \neq 0 \\ 2 \text{ if } g_0 = 0, g_1 = 0, g_2 \neq 0 \\ \cdot \\ \cdot \\ n-1 \text{ if } g_{n-1} \neq 0, \text{ and for all i } 0 \leq i \leq n-2 \ \ g_i = 0 \\ n \text{ if } g_i = 0 \text{ for all i } 0 \leq i \leq n-1 \end{bmatrix} \qquad (8)$$

Let $a, b \in G[u]/ < u^n >$ then $\delta(a \times b) = \min(n, \delta(a) + \delta(b))$ where $\times$ is the multiplication in

$G[u]/ < u^n >$ and $\delta(a) < n$ when $a \neq 0$.

We will need also some notations and facts from Corollarys IV.2-IV.2" ([5]): In the matrix α we can have that the entries of the last row are $\alpha_{n,1} = \cdots = \alpha_{n,n-1} = 1$ and $t_i = \sum_{j=0}^{n-1} b_{ij} t_{n+j}$ $u_i = \sum_{j=0}^{n-1} a_{ij} u_{n+j}$, a_{ij}, $b_{ij} \in G$, $i = 1, \cdots, n-1$. Since $j = 1$ then $\{u_n, u_{n+1} \cdots, u_{2n-1}\}$, $\{t_n, t_{n+1} \cdots, t_{2n-1}\}$, are linearly independent and finally there exist n-dimensional vectors $S_0, \cdots, S_{n-1}$ and n-dimensional vectors $V_0, \cdots, V_{n-1}$ such that $t_{n+j}^T S_l = \delta_{jl}$, $\delta(S_0) = 0$ (Lemma IV.5 ([5])) and $u_{n+j}^T V_l = \delta_{jl}$ $j, l = 0, \cdots, n-1$.

We are going to use $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b_{il}^* \overline{w}_i \times S_0$ $i, l = 1, \cdots, n-1$, which was proved in Lemma IV.7 (v) ([5]), very often in this section without mentioning the Lemma it was derived from.

Remark II.1: If for some i, $i \in \{1, \cdots n-1\}$, $\delta(\overline{w}_i) = t$ then at least $n - t$ multiplications are needed to compute $w_i^T A(\underline{x})\underline{y}$ and at least $n - t - 1$ terms of $\alpha_{il}, \cdots, \alpha_{i,n-1}$ are equal to 0 (Lemma IV.6 ([5])). We can assume $\alpha_{i1}, \cdots, \alpha_{i,n-t-1} \neq 0$. If this is not the case we can apply a permutation matrix (transformation 1 from section IV) and obtain an equivalent algorithm in the following way: Let N be an $(2n-1) \times (2n-1)$ G-permutation matrix such that the first n rows and n columns of N is the identity matrix and $WA(\underline{x})\underline{y} = (I|\alpha)NN^{-1}\underline{m}$. Then $\alpha_{i1}, \cdots, \alpha_{i,n-t-1}$ are not equal to 0.

The procedure above, which reorder the non-zero elements of a row, can successfully applied to at least one row in W, however it is not guaranteed that this transformation can be applied successfully to more than one.

III. Examples

Since the paper is technically involved we prefer in the beginning to look at some intuitively *obvious* methods for computing the coefficients of $\sum_{i=0}^{n-1} x_i u^i)\sum_{i=0}^{n-1} y_i u^i)\mathrm{mod}\ u^n$ by giving a detailed list of examples how to compute the coefficients of $\sum_{i=0}^{n-1} x_i u^i)\sum_{i=0}^{n-1} y_i u^i)\mathrm{mod}\ u^n$ for $n = 4$ in 7 multiplications and demonstrates some concepts which are defined in the previous section. This bilinear system has the following matrix representation:

$$A(\underline{x})\underline{y} = \begin{bmatrix} x_0 & 0 & 0 & 0 \\ x_1 & x_0 & 0 & 0 \\ x_2 & x_1 & x_0 & 0 \\ x_3 & x_2 & x_1 & x_0 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

In addition we will compute the matrices W and α such that $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ and for $i = 0, \cdots, 3$ the 4-dimensional vectors S_i and V_i such that $t_{n+j}^T S_l = \delta_{jl}$, $u_{n+j}^T V_l = \delta_{jl}$, $t_i = \sum_{i=0}^{3} b_{ij} t_{n+j}$ and $u_i = \sum_{i=0}^{3} a_{ij} u_{n+j}$ for $i, j = 0, \cdots, 3$.

Example III.1:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1/3 & 1 & -1/2 & -1/4 & 1/20 & 1/30 & -12 \\ -5/4 & 2/3 & 2/3 & -1/24 & -1/24 & 0 & 4 \\ 5/12 & -7/12 & -1/24 & 7/24 & -1/24 & -1/24 & 15 \end{bmatrix} \times \tag{1a}$$

$$\begin{bmatrix} x_0 y_0 \\ (x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) \\ (x_0 - x_1 + x_2 - x_3)(y_0 - y_1 + y_2 - y_3) \\ (x_0 + 2x_1 + 4x_2 + 8x_3)(y_0 + 2y_1 + 4y_2 + 8y_3) \\ (x_0 - 2x_1 + 4x_2 - 8x_3)(y_0 - 2y_1 + 4y_2 - 8y_3) \\ (x_0 + 3x_1 + 9x_2 + 27x_3)(y_0 + 3y_1 + 9y_2 + 27y_3) \\ x_3 y_3 \end{bmatrix}$$

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 209/216 & 37/36 & 5/6 & 1 \\ 307/324 & -49/54 & 7/9 & -2/3 \\ 52/81 & 52/27 & 16/9 & 16/3 \end{bmatrix} \quad \alpha = \begin{bmatrix} 0 & 0 & 0 \\ -1/40 & -1/135 & 6 \\ -1/20 & -1/405 & 4 \\ -1/5 & -64/405 & 64 \end{bmatrix} \tag{1a'}$$

and

$$V_0 = S_0 = (3/2, 1/4, -1/4, 0) \ \ V_1 = S_1 = (3/10, -1/4, 1/20, 0) \tag{1aa'}$$

$$V_2 = S_2 = (-4/5, 0, 1/5, 0) \ \ V_3 = S_3 = (12, -4, -3, 1)$$

Here for all $i = 0, \cdots, 3$ V_i and S_i are invertible while $\delta(\overline{w}_i) = 0$ for $i = 2, 3, 4$ and $\delta(\overline{w}_1) = 3$. Then

$$b_{10} = 27/19 \quad b_{11} = 6/19 \quad b_{12} = -14/19 \quad b_{13} = 262/19 \tag{1aaa'}$$

$$b_{20} = 36/23 \quad b_{21} = 2/13 \quad b_{22} = -15/23 \quad b_{23} = 216/23$$

and $a_{ij} = b_{ij}$.

$$b_{30} = 1 \quad b_{31} = 3/5 \quad b_{32} = -3/5 \quad b_{33} = 14$$

We get this algorithm by computing the coefficients of $(\sum_{i=0}^{3} x_i u^i)(\sum_{i=0}^{3} y_i u^i)$ using Theorem I.1 with the scalars 0,1,-1,2,-2,3 and reducing them modulo u^4. In general, this type of algorithms we get by computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ with $2n-2$ distinct scalars from the field G by using Theorem I.1 and reducing them modulo u^n.

Another algorithm in this category:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 3/4 & 3/4 & -3/10 & -3/10 & 1/20 & 1/20 & -36 \\ 3/4 & -3/4 & -3/20 & 3/20 & 1/60 & -1/60 & 0 \\ -13/48 & -13/48 & 1/3 & 1/3 & -1/16 & -1/16 & 49 \\ -13/48 & 13/48 & 1/6 & -1/6 & -1/48 & 1/48 & 0 \end{bmatrix} \times \qquad (1b)$$

$$\begin{bmatrix} (x_0+x_1+x_2+x_3)(y_0+y_1+y_2+y_3) \\ (x_0-x_1+x_2-x_3)(y_0-y_1+y_2-y_3) \\ (x_0+2x_1+4x_2+8x_3)(y_0+2y_1+4y_2+8y_3) \\ (x_0-2x_1+4x_2-8x_3)(y_0-2y_1+4y_2-8y_3) \\ (x_0+3x_1+9x_2+27x_3)(y_0+3y_1+9y_2+27y_3) \\ (x_0-3x_1+9x_2-27x_3)(y_0-3y_1+9y_2-27y_3) \\ x_3y_3 \end{bmatrix}$$

$$W = \begin{bmatrix} 80/81 & 80/81 & 8/9 & 8/9 \\ 80/81 & -80/81 & 8/9 & -8/9 \\ 65/81 & 130/81 & 20/9 & 40/9 \\ 65/81 & -130/81 & 20/9 & -40/9 \end{bmatrix} \quad \alpha = \begin{bmatrix} -2/243 & -1/243 & 8 \\ -1/243 & -2/243 & 8 \\ -40/243 & -8/243 & 80 \\ -8/243 & -40/243 & 80 \end{bmatrix} \qquad (1b')$$

and

$$V_0 = S_0 = (9/5, 0, -1/5, 0) \; V_1 = S_1 = (1/5, 1/6, 1/30, 0) \; V_2 = S_2 = (-1, -1/6, 1/6, 0) \qquad (1bb')$$

$$V_3 = S_3 = (-18, -9, -2, 1)$$

Here for all $i = 0, \cdots, 3$ V_i, S_i and $\overline{w}_i$ are invertible.

We get this algorithm by computing the coefficients of $(\sum_{i=0}^{3} x_i u^i)(\sum_{i=0}^{3} y_i u^i)$ using Theorem I.1 with the scalars 1,-1,2,-2,3,-3.

Example III.2:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2/3 & -2/3 & 0 & -1/12 & 1/12 & 0 \\ 0 & 2/3 & 2/3 & 0 & -1/24 & -1/24 & 0 \\ 0 & -1/6 & 1/6 & 1 & 1/2 & -1/12 & 1 \end{bmatrix} \begin{bmatrix} x_0y_0 \\ (x_0+x_1+x_2)(y_0+y_1+y_2) \\ (x_0-x_1+x_2)(y_0-y_1+y_2) \\ x_3y_0 \\ (x_0+2x_1+4x_2)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2)(y_0-2y_1+4y_2) \\ x_0y_3 \end{bmatrix} \qquad (2a)$$

and

$$W=\begin{bmatrix}1&0&0&0\\0&3/4&3/4&0\\0&-3/4&3/4&0\\0&-1/4&0&1\end{bmatrix}\quad \alpha=\begin{bmatrix}0&0&0\\-3/32&1/32&0\\1/32&-3/32&0\\1/16&-1/16&1\end{bmatrix} \tag{2a'}$$

and

$$S_0=(1,0,-1/4,0)\ \ S_1=(0,1/4,1/8,0)\ \ S_2=(0,-1/4,1/8,0)\ \ S_3=(0,0,0,1) \tag{2aa'}$$

$$V_0=(0,0,0,1)\ \ V_1=(0,1/4,1/8,0)\ \ V_2=(0,-1/4,1/8,0)\ \ V_3=(1,0,-1/4,0)$$

$\delta(\overline{w}_4)=0$ while $\delta(\overline{w}_1)=3$ and $\delta(\overline{w}_2)=\delta(\overline{w}_3)=1$. In addition, $\delta(S_0)=\delta(V_3)=0$, $\delta(V_0)=\delta(S_3)=3$ and for $i=2,3$ we have that $\delta(S_i)=\delta(V_i)=1$.

$$a_{10}=0\ a_{11}=0\ a_{12}=0\ a_{13}=1 \tag{2aaa'}$$

$$b_{10}=1\ b_{11}=0\ b_{12}=0\ b_{13}=0$$

$$a_{20}=0\ a_{21}=3/8\ a_{22}=-1/8\ a_{23}=6/8$$

$$b_{20}=6/8\ b_{21}=3/8\ b_{22}=-1/8\ b_{23}=0$$

$$a_{30}=0\ a_{31}=-1/8\ a_{32}=3/8\ a_{33}=6/8$$

$$b_{30}=6/8\ b_{31}=-1/8\ b_{32}=3/8\ b_{33}=0$$

We get this algorithm by computing the coefficients of $(\sum_{i=0}^{2}x_iu^i)(\sum_{i=0}^{2}y_iu^i)$ using Theorem I.1 with the scalars 0,1,-1,2,-2 and reducing them modulo u^4 and add $(x_3y_0+x_0y_3)u^3$. In general, this type of algorithms we get by using the identity $(\sum_{i=0}^{n-1}x_iu^i)(\sum_{i=0}^{n-1}y_iu^i)\text{mod } u^n=(\sum_{i=0}^{n-2}x_iu^i)(\sum_{i=0}^{n-2}y_iu^i)\text{mod } u^n+(x_0y_{n-1}+x_{n-1}y_0)u^{n-1}$. We compute the coefficients of $(\sum_{i=0}^{n-2}x_iu^i)(\sum_{i=0}^{n-2}y_iu^i)$ by Theorem I.1 using $2n-4$ distinct scalars from G and reducing them modulo u^n.

Since in (2a) $M_1(\underline{y})=M_4(\underline{y})$ then by linear combination we get an equivalent algorithm to (2a):

$$A(\underline{x})\underline{y}=\begin{bmatrix}1&0&0&-1&0&0&0\\0&2/3&-2/3&0&-1/12&1/12&0\\0&2/3&2/3&0&-1/24&-1/24&0\\0&-1/6&1/6&1&1/12&-1/12&1\end{bmatrix}\begin{bmatrix}(x_0+x_3)y_0\\(x_0+x_1+x_2)(y_0+y_1+y_2)\\(x_0-x_1+x_2)(y_0-y_1+y_2)\\x_3y_0\\(x_0+2x_1+4x_2)(y_0+2y_1+4y_2)\\(x_0-2x_1+4x_2)(y_0-2y_1+4y_2)\\x_0y_3\end{bmatrix} \tag{2b}$$

and

$$W=\begin{bmatrix}1&0&0&1\\0&3/4&3/4&0\\0&-3/4&3/4&0\\0&-1/4&0&1\end{bmatrix}\quad \alpha=\begin{bmatrix}0&0&0\\-3/32&1/32&0\\1/32&-3/32&0\\1/16&-1/16&1\end{bmatrix} \tag{2b'}$$

$\delta(\overline{w}_1) = \delta(\overline{w}_4) = 0 \quad \delta(\overline{w}_2) = \delta(\overline{w}_3) = 1.$

$$a_{10} = 1 \; a_{11} = 0 \; a_{12} = 0 \; a_{13} = 1 \tag{2bb'}$$

and the rest of a_{ij} and b_{ij} are the same in eq. 2aaa'.
Since in (2a) the multiplications p_4 and p_7 are referred only by the last row of M (where M appears in $A(\underline{x})y = M\underline{m}$) we can change them without affecting the other multiplications and we get the following algorithm which is equivalent to (2a) in the following way; Assume that

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \; A^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

then $(\overline{u}_4|\overline{u}_7) = (u_4|u_7)A$ and $\begin{bmatrix} \overline{t}_4^T \\ \overline{t}_7^T \end{bmatrix} = A^{-1}\begin{bmatrix} t_4^T \\ t_7^T \end{bmatrix}$ where $\overline{u}_4$, $\overline{u}_7$, $\overline{t}_4$ and $\overline{t}_7$ are the coordinates of the modified multiplications.
Then we get:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2/3 & -2/3 & 0 & -1/12 & 1/12 & 0 \\ 0 & 2/3 & 2/3 & 0 & -1/24 & -1/24 & 0 \\ 0 & -1/6 & 1/6 & 1 & 1/12 & -1/12 & 1 \end{bmatrix} \begin{bmatrix} x_0 y_0 \\ (x_0+x_1+x_2)(y_0+y_1+y_2) \\ (x_0-x_1+x_2)(y_0-y_1+y_2) \\ x_3(y_0+y_3) \\ (x_0+2x_1+4x_2)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2)(y_0-2y_1+4y_2) \\ (x_0-x_3)y_3 \end{bmatrix} \tag{2c}$$

α and W are the same as in eq. $2a'$.

$$S_0 = (1,0,-1/4,0) \; V_1 = S_1 = (0,1/4,1/8,0) \; V_2 = S_2 = (0,-1/4,1/8,0) \tag{2c'}$$

$$S_3 = (-1,0,1/4,1) \; V_0 = (1,0,-1/4,1) \; V_3 = (0,0,0,-1)$$

$$\delta(S_0) = \delta(S_3) = \delta(V_0) = 0$$

$$\delta(S_1) = \delta(S_2) = \delta(V_1) = \delta(V_2) = 1$$

$$\delta(V_3) = 3$$

$$a_{10} = -1 \; a_{11} = 0 \; a_{12} = 0 \; a_{13} = 1 \tag{2cc'}$$

$$b_{10} = 1 \; b_{11} = 0 \; b_{12} = 0 \; b_{13} = -1$$

$$a_{20} = -6/8 \; a_{21} = 3/8 \; a_{22} = -1/8 \; a_{23} = 6/8$$

$$b_{20} = 6/8 \; b_{21} = 3/8 \; b_{22} = -1/8 \; b_{23} = -6/8$$

$$a_{30} = -6/8 \; a_{31} = -1/8 \; a_{32} = 3/8 \; a_{33} = 6/8$$

$$b_{30} = 6/8 \; b_{31} = -1/8 \; b_{32} = 3/8 \; b_{33} = -6/8$$

Another type of algorithm related to (2a) is:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2/3 & -2/3 & 0 & -1/12 & 1/12 & 0 \\ 0 & 2/3 & 2/3 & 0 & -1/24 & -1/24 & 0 \\ -1 & -1/6 & 1/6 & 1 & 1/12 & -1/12 & -1 \end{bmatrix} \begin{bmatrix} x_0y_0 \\ (x_0+x_1+x_2)(y_0+y_1+y_2) \\ (x_0-x_1+x_2)(y_0-y_1+y_2) \\ (x_0+x_3)(y_0+y_3) \\ (x_0+2x_1+4x_2)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2)(y_0-2y_1+4y_2) \\ x_3y_3 \end{bmatrix} \tag{2d}$$

and

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3/4 & 3/4 & 0 \\ 0 & -3/4 & 3/4 & 0 \\ 1 & 1/4 & 0 & 1 \end{bmatrix} \quad \alpha = \begin{bmatrix} 0 & 0 & 0 \\ -3/32 & 1/32 & 0 \\ 1/32 & -3/32 & 0 \\ 1/16 & -1/16 & -1 \end{bmatrix} \tag{2d'}$$

$$\delta(\overline{w}_1) = 3 \ \delta(\overline{w}_2) = \delta(\overline{w}_3) = 1 \ \delta(\overline{w}_4) = 0$$

and

$$V_0 = S_0 = (1, 0, -1/4, 0) \ V_1 = S_1 = (0, 1/4, 1/8, 0) \ V_2 = S_2 = (0, -1/4, 1/8, 0)$$

$$V_3 = S_3 = (-1, 0, 1/4, 1) \tag{2dd'}$$

Example III.3:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2/3 & 4 & -2/3 & -1/12 & -1/12 & 0 \\ -5/4 & 2/3 & 0 & 2/3 & -1/24 & -1/24 & 0 \\ 0 & -1/6 & 5 & 1/6 & 1/2 & -1/12 & 1 \end{bmatrix} \begin{bmatrix} x_0y_0 \\ (x_0+x_1+x_2+x_3)(y_0+y_1+y_2) \\ x_3y_2 \\ (x_0-x_1+x_2+x_3)(y_0-y_1+y_2) \\ (x_0+2x_1+4x_2+8x_3)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2-8x_3)(y_0-2y_1+4y_2) \\ x_0y_3 \end{bmatrix} \tag{3a}$$

and

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 15/16 & 15/16 & 3/4 & 3/4 \\ 0 & -1/16 & 0 & -1/4 \\ 15/16 & -15/16 & 3/4 & -3/4 \end{bmatrix} \quad \alpha = \begin{bmatrix} 0 & 0 & 0 \\ -3/64 & -11/64 & 3/4 \\ -1/64 & 5/192 & -1/4 \\ -1/64 & 7/64 & -3/4 \end{bmatrix} \tag{3a'}$$

$$\delta(\overline{w}_1) = 3 \ \ \delta(\overline{w}_2) = \delta(\overline{w}_3) = 1 \ \ \delta(\overline{w}_4) = 0$$

and

$$S_0 = (4/3, 0, -1/3, 0) \ S_1 = (1/6, 1/4, 1/12, 0) \ S_2 = (-1/2, -1/4, 1/4, 0)$$
$$S_3 = (0, 0, 0, 1)$$
$$V_0 = (0, -4/3, 0, 1/3) \ V_1 = (0, 1/12, 1/8, 1/24) \ V_2 = (0, 1/4, 1/8, -1/8) \ V_3 = (1, 1, -1/4, -1/4) \tag{3aa'}$$

$$\delta(S_i) = 0 \ \ i = 0, 1, 2 \ \ \delta(S_3) = 3$$

$$\delta(V_i) = 1 \ \ i = 0, 1, 2 \ \ \delta(V_3) = 0$$

$$a_{10} = 0 \; a_{11} = 0 \; a_{12} = 0 \; a_{13} = 1$$

$$b_{10} = 8/6 \; b_{11} = 1/6 \; b_{12} = -3/6 \; b_{13} = 0$$

$$a_{20} = -1 \; a_{21} = 1/4 \; a_{22} = 1/4 \; a_{23} = 3/2$$

$$b_{20} = 1 \; b_{21} = 1/2 \; b_{22} = -1/2 \; b_{23} = 0$$

$$a_{30} = 0 \; a_{31} = 0 \; a_{32} = 0 \; a_{33} = 1$$

$$b_{30} = -1/3 \; b_{31} = 1/12 \; b_{32} = 1/4 \; b_{33} = 0$$

We get this algorithm by computing the coefficients of $(\sum_{i=0}^{3} x_i u^i)(\sum_{i=0}^{2} y_i u^i)$ using Theorem I.1 with the scalars 0,1,-1,2,-2 and reducing them modulo u^4 and add $x_0 y_3 u^3$. In general, this type of algorithms we get by using the identity $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n = (\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i) \bmod u^n$ $+ x_0 y_{n-1} u^{n-1}$. Thus, compute the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ by Theorem I.1 and reduce them modulo u^n . By interchanging the roles of u_i and t_i the following identity is valid: $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n = (\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n + x_{n-1} y_0 u^{n-1}$. Hence the following algorithm, where the roles of u_i and t_i where exchanged, is <u>equivalent to (3a)</u>
$A(\underline{x})\underline{y} =$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2/3 & 4 & 0 & -2/3 & -1/12 & 1/12 \\ -5/4 & 2/3 & 0 & 0 & 2/3 & -1/24 & -1/24 \\ 0 & -1/6 & -5 & 1 & 1/6 & 1/12 & -1/12 \end{bmatrix} \begin{bmatrix} x_0 y_0 \\ (x_0+x_1+x_2)(y_0+y_1+y_2+y_3) \\ x_2 y_3 \\ x_3 y_0 \\ (x_0-x_1+x_2)(y_0-y_1+y_2-y_3) \\ (x_0+2x_1+4x_2)(y_0+2y_1+4y_2+8y_3) \\ (x_0-2x_1+4x_2)(y_0-2y_1+4y_2-8y_3) \end{bmatrix} \tag{3b}$$

and

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 15/8 & 0 & 3/2 & 0 \\ -5/16 & 1/4 & -1/4 & 0 \\ -5/4 & 5/4 & -1 & 1 \end{bmatrix} \quad \alpha = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -1/16 & -1/16 \\ -1/3 & -1/96 & 1/32 \\ -4/3 & 1/48 & 1/16 \end{bmatrix} \tag{3b'}$$

and

$$S_0 = (1, 1, -1/4, -1/4) \; S_1 = (0, -4/3, 0, 1/3) \; S_2 = (0, 1/12, 1/8, 1/24) \; S_3 = (0, 1/4, 1/8, -1/8)$$
$$V_0 = (0, 0, 0, 1) \; V_1 = (4/3, 0, -1/3, 0) \; V_2 = (1/6, 1/4, 1/12, 0) \; V_3 = (-1/2, -1/4, 1/4, 0) \tag{3bbb'}$$

$$a_{10} = 0 \; a_{11} = 4/3 \; a_{12} = 1/6 \; a_{13} = -1/2$$
$$b_{10} = 1 \; b_{11} = 0 \; b_{12} = 0 \; b_{13} = 0$$
$$a_{20} = 0 \; a_{21} = 1 \; a_{22} = 1/2 \; a_{23} = -1/2$$
$$b_{20} = 5/4 \; b_{21} = -2/3 \; b_{22} = 7/24 \; b_{23} = 1/8$$
$$a_{30} = 0 \; a_{31} = -1/3 \; a_{32} = 1/12 \; a_{33} = 1/4$$
$$b_{30} = -1/4 \; b_{31} = 1/3 \; b_{32} = 1/24 \; b_{33} = -1/8$$

We will now present the same type of algorithm as in (3a) but it is performed with the scalars 1, -1, 2, -2, 3:

$$A(\underline{x})\underline{y} = \begin{bmatrix} 1 & 1/2 & -12 & -1/2 & -1/10 & 1/10 & 0 \\ 2/3 & -2/3 & -4 & -1/12 & 1/12 & 0 & 0 \\ -7/12 & 1/24 & 15 & 7/12 & 1/12 & -1/8 & 0 \\ -1/6 & 1/6 & -5 & 1/12 & -1/12 & 0 & 1 \end{bmatrix} \begin{bmatrix} (x_0+x_1+x_2+x_3)(y_0+y_1+y_2) \\ (x_0-x_1+x_2-x_3)(y_0-y_1+y_2) \\ x_3y_2 \\ (x_0+2x_1+4x_2+8x_3)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2-8x_3)(y_0-2y_1+4y_2) \\ (x_0+3x_1+9x_2+27x_3)(y_0+3y_1+9y_2) \\ x_0y_3 \end{bmatrix} \tag{3c}$$

$$W = \begin{bmatrix} 281/272 & 111/136 & 69/68 & -3/34 \\ 121/136 & -49/68 & 21/34 & 5/17 \\ 13/1632 & -7/272 & 3/136 & -9/68 \\ 13/17 & 26/17 & 36/17 & 56/17 \end{bmatrix} \quad \alpha = \begin{bmatrix} 77/1360 & -2/85 & -3/34 \\ -83/680 & 1/85 & 5/17 \\ 27/2720 & -1/510 & -9/68 \\ -4/85 & -16/85 & 56/17 \end{bmatrix} \tag{3c'}$$

$$\delta(\overline{w}_i) = 0 \;\; i = 1, ..., 4$$

and

$$S_0 = (3/2, 1/4, -1/4, 0) \quad S_1 = (3/10, -1/4, 1/20, 0) \quad S_2 = (-4/5, 0, 1/5, 0) \tag{3cc'}$$

$$S_3 = (0,0,0,1)$$

$$V_0 = (0, 3/4, 1/8, -1/8) \quad V_1 = (0, -3/20, 1/8, -1/40) \quad V_2 = (0, -4/15, 0, 1/15)$$

$$V_3 = (1, -1/3, -1/4, 1/12)$$

$$a_{10} = 3/4 \quad a_{11} = -1/20 \quad a_{12} = -1/5 \quad a_{13} = 1/2 \tag{3cc'}$$

$$b_{10} = 3/2 \quad b_{11} = 1/10 \quad b_{12} = -3/5 \quad b_{13} = 0$$

$$a_{20} = 7/20 \quad a_{21} = -1/20 \quad a_{22} = 1/15 \quad a_{23} = -1/10$$

$$b_{20} = 1 \quad b_{21} = 3/5 \quad b_{22} = -3/5 \quad b_{23} = 0$$

$$a_{30} = -5/44 \quad a_{31} = -1/44 \quad a_{32} = 2/33 \quad a_{33} = 55/726$$

$$b_{30} = -1/4 \quad b_{31} = 1/20 \quad b_{32} = 1/5 \quad b_{33} = 0$$

Since in (3a) $L_1(\underline{x}) = L_7(\underline{x})$ then we can use a linear combination to get the following equivalent algorithm to (3a):

$$A(\underline{x})\underline{y} = \tag{3d}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 2/3 & 4 & -2/3 & -1/12 & 1/12 & 0 \\ -5/4 & 2/3 & 0 & 2/3 & -1/24 & -1/24 & -5/4 \\ 0 & -1/6 & -5 & 1/6 & 1/12 & -1/12 & 1 \end{bmatrix} \begin{bmatrix} x_0(y_0+y_3) \\ (x_0+x_1+x_2+x_3)(y_0+y_1+y_2) \\ x_3y_2 \\ (x_0-x_1+x_2-x_3)(y_0-y_1+y_2) \\ (x_0+2x_1+4x_2+8x_3)(y_0+2y_1+4y_2) \\ (x_0-2x_1+4x_2-8x_3)(y_0-2y_1+4y_2) \\ x_0y_3 \end{bmatrix} \tag{3d}$$

and

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 15/16 & 15/16 & 3/4 & 3/4 \\ 0 & -1/16 & 0 & -1/4 \\ 15/16 & -15/16 & 3/4 & -3/4 \end{bmatrix} \quad \alpha = \begin{bmatrix} 0 & 0 & -1 \\ -3/64 & -1/64 & -9/8 \\ -1/64 & 1/64 & -1/4 \\ -1/64 & -3/64 & -21/8 \end{bmatrix} \qquad (3d')$$

and

$$S_0 = (4/3, 0, -1/3, 0) \quad S_1 = (1/6, 1/4, 1/12, 0) \quad S_2 = (-1/2, -1/4, 1/4, 0) \qquad (3dd')$$

$$S_3 = (0, 0, 0, 1)$$

$$V_0 = (0, -4/3, 0, 1/3) \quad V_1 = (0, 1/12, 1/8, 1/24) \quad V_2 = (0, 1/4, 1/8, -1/8)$$

$$V_3 = (1, 1, -1/4, -1/4)$$

All the algorithms presented in later sections will be derivable using one of the three methods described in the examples above. While we are in the process of developing these algorithms we will point out when we reach each method. At first glance it will be rather difficult to see the connection between the above methods and the formal description of each algorithm as it appeared in the coming theorems. Therefore, we will point after each theorem to a suitable detailed example which will give some insight how the above methods really exhaust all the possible minimal bilinear algorithms for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \mathrm{mod} u^n$. In addition, before analyzing each type of algorithm we will present a short outline of the approach we are taking in each case.

IV. The equivalence classes of minimal bilinear algorithms

In order to accommodate the new algorithms we have to enhance the class of equivalent algorithms that were mentioned in [5] section III. For the completeness of our description of equivalence classes, which will play a major role in collapsing together algorithms which at first glance look unrelated, we will repeat the description we gave in [5] and will add in the suitable places the additional transformations that identify algorithms in $G[u]/ < u^n >$ which are belonging to the same equivalence class.

If an algorithm A' is derived from an algorithm A by some transformation which does not use any m/d operations then the algorithms are related and we will identify them as belonging to the same equivalence class and thus we do not distinguish among them since they differ merely by these transformations.

We can divide these transformations into two types:

Type 1: Transformations applicable to any systems of bilinear forms.

Type 2: Transformations applicable only to systems of bilinear forms that were derived from $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) mod u^n$.

We will identify six types of transformations. Transformations (1),(2) and (5) have been used in [5]. In addition to those, we will see some new ones appearing in this section as (3), (4) and (6). Let A be a minimal algorithm for computing $\underline{\psi} = A(\underline{x})(\underline{y})$ then $\underline{\psi} = A(\underline{x})(\underline{y}) = M\underline{m}$ where $\underline{\psi} = (\psi_0, ..., \psi_{n-1})^T$,

$$A(\underline{x}) = \begin{bmatrix} R_{11} & \cdots & R_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ R_{n1} & \cdots & R_{nn} \end{bmatrix}$$

and $R_{kj} = \sum_{i=0}^{n-1} g_{ijk}x_i, \quad g_{ijk} \in G, \quad M$ is $n \times 2n-1$ G-matrix $m_{i,j} \in M \quad i = 1, ..., n \quad j = 1, ..., 2n-1, \quad \underline{m} = (p_1, ..., p_{2n-1})^T, p_i = L_i(\underline{x})M_i(\underline{y}), \quad L_i(\underline{x}) = \sum_{j=0}^{n-1} u_{ij}x_j = x^T u_i, \quad M_i(\underline{y}) = \sum_{j=0}^{n-1} t_{ij}y_j = y^T t_i, \quad u_{ij}, \quad t_{ij} \in G$ and $u_i = (u_{i,0}, ..., u_{i,n-1}), \quad t_i = (t_{i,0}, ..., t_{i,n-1}), \quad i = 1, ..., 2n-1, \quad \underline{x} = (x_0, ..., x_{n-1})^T \quad \underline{y} = (y_0, ..., y_{n-1})^T$.

Type 1 contains the following transformations: Another algorithm $A' \quad (\underline{\psi} = A(\underline{x})(\underline{y}) = M'\underline{m}')$ is equivalent to $A \quad (\underline{\psi} = A(\underline{x})(\underline{y}) = M\underline{m})$ if one of the following conditions is satisfied:

1. We can renumber the multiplication column and then rerrange the coefficients matrix to suit this permutation and get an equivalent algorithm. In other words, let Π be any $(2n-1) \times (2n-1)$ G-permutation matrix, then the relabeling will be done the following:

$$M' = M\Pi$$

$$m' = \Pi^{-1}\underline{m}$$

2. Replace $m_i = L_i(\underline{x})M_i(\underline{y})$ by $(a_iL_i(\underline{x}))(b_iM_i(\underline{y}))$ $a_i, b_i \in G \quad a_i, b_i \neq 0$ and multiplying the i-th column of M by $(a_ib_i)^{-1}$.

In other words, we can scale the multiplications by scalars from the base field G.

3. Assume WLG that $m_{1,1} = m_{1,2} = 1 \quad m_{i,1}, m_{i,2} = 0 \quad 2 \le i \le n$, otherwise use transformation (2) . Then $\psi_1 = \sum_{i=1}^{n} R_{1,i}(\underline{x})y_i = p_1 + p_2 + \sum_{i=3}^{2n-1} m_{1,i}p_i$ therefore $p_1 + p_2 = \sum_{i=1}^{n} R_{1,i}(\underline{x})y_i - \sum_{i=3}^{2n-1} m_{1,i}p_i$. Since $p_1 = x^Tu_1t_1^Ty$ and $p_2 = x^Tu_2t_2^Ty$ then

$$p_1 + p_2 = x^Tu_1t_1^Ty + x^Tu_2t_2^Ty = x^T(u_1|u_2)\begin{pmatrix} t_1^T \\ t_2^T \end{pmatrix} y$$

Choose a 2×2 non-singular G-matrix A. Denote: $(\overline{u}_1|\overline{u}_2) = (u_1|u_2)A$ and

$$\begin{pmatrix} \overline{t}_1^T \\ \overline{t}_2^T \end{pmatrix} = A^{-1}\begin{pmatrix} t_1^T \\ t_2^T \end{pmatrix}$$

then $\overline{p}_1 = x^T\overline{u}_1\overline{t}_1^Ty \quad \overline{p}_2 = x^T\overline{u}_2\overline{t}_2^Ty$ and we get $p_1 + p_2 = \overline{p}_1 + \overline{p}_2$. In words, since p_1 and p_2 are referred only by the first row of M we can modify p_1 and p_2 without affecting the other multiplications of the algorithm. See example (2c) in section III.

4. Let A be an algorithm where $M_1(\underline{y}) = M_2(\underline{y})$ then we can get an equivalent algorithm A' where $L_1'(\underline{x}) = L_1(\underline{x}) + gL_2(\underline{x}) \quad L_i'(\underline{x}) = L_i(\underline{x}) \quad i = 2, ..., 2n-1 \quad g \in G$ and $M_1'(\underline{y}) = M_2'(\underline{y}) = M_1(\underline{y})$ and $M_i'(\underline{y}) = M_i(\underline{y}) \quad i = 3, ..., 2n-1$ and $m_{i,2}' = m_{i,2} - gm_{i,1} \quad i = 1, ..., 2n-1 \quad g \in G$.
In words, if $M_i(\underline{y}) = M_j(\underline{y}) \;\; i \neq j$ we can perform any linear combination (with scalars from G) and get a new algorithm after adjusting the coefficients matrix M. See examples (2b) and (3d) in section III.
Type 2 contains the following transformations:
5. Choose two invertible elements α, β in the algebra $G[u]/ < u^n >$. Always $x \times y = (\alpha \times \beta)^{-1} \times ((\alpha \times x) \times (\beta \times y))$ where $\times$ is the multiplication in $G[u]/ < u^n >$. Each α is described by $\alpha = \sum_{i=0}^{n-1} \alpha_i u^i$. Its regular matrix representation is given by $U_\alpha = \sum_{i=0}^{n-1} \alpha_i U^i$ where U is the companion matrix of u^n . Similiarly, let $\beta = \sum_{i=0}^{n-1} \beta_i u^i, \quad U_\beta = \sum_{i=0}^{n-1} \beta_i U^i$. Then A' is given by $\underline{m}' = (p_1', ..., p_{2n-1}')^T$ where $p_i' = L_i(U_\alpha \underline{x}) M_i(U_\beta \underline{y}) \quad 1 \leq i \leq 2n-1$ and $M' = U_{(\alpha\beta)^{-1}} M$.
From $L_i(\underline{y}) = u_i^T \underline{x}, \quad M_i(\underline{y}) = t_i^T \underline{y}, \quad L_i(U_\alpha \underline{x}) = u_i^T U_\alpha \underline{x} = (u_i')^T \underline{y}$ and $M_i(U_\beta \underline{y}) = t_i^T U_\beta \underline{y} = (t_i')^T \underline{y}$ we obtain for all $i = 1, ..., 2n-1$ that: $u_i' = U_\alpha^T u_i$ and $t_i' = U_\beta^T t_i$. We should note that in $G[u]/ < u^n > \quad \alpha$ and β are invertible if and only if $\alpha_0, \; \beta_0 \neq 0$.
6. Replace each $L_i(\underline{x}) = \sum_{j=0}^{a_i} u_{i,j} x_j$ and $M_i(\underline{y}) = \sum_{j=0}^{b_i} t_{i,j} y_j \quad 0 \leq a_i, \; b_i \leq n-1 \quad i = 1, ..., 2n-1$ of an algorithm A by $L_i'(\underline{x}) = \sum_{j=0}^{b_i} t_{i,j} x_j$ and $M_i'(\underline{y}) = \sum_{j=0}^{a_i} u_{i,j} y_j \quad 0 \leq a_i, b_i \leq n-1 \quad i = 1, ..., 2n-1$ and get and equivalent algorithm A' since $A(\underline{x})(\underline{y}) = (\sum_{i=0}^{n-1} x_i U^i)\underline{y}$ (U is the companion matrix of $Q(u)^l$) and the polynomial multiplication in $G[u]/ < Q(u)^l >$ is commutative thus we also have $A(\underline{x})(\underline{y}) = (\sum_{i=0}^{n-1} y_i U^i)\underline{x}$.
See how example (3a) is related to example (3b) in section III (through the use of this transform).
Notation: Denote by $\mathcal{J}_{u^n}$ the class of all the algorithms for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in any algebra isomorphic to $G[u]/ < u^n >$.
How do we relate the computation among various algebras in $\mathcal{J}_{u^n}$?
Let σ be an isomorphism $\sigma : G[u]/ < u^n > \to G[v]/ < v^n >$. Therefore, in order to compute the coefficients of $R(u)S(u) \bmod u^n$ we compute $R'(v) = \sigma(R(u))$ and $S'(v) = \sigma(S(u))$. This part uses no m/d steps. Then to compute the coefficients of $R(u)S(u) \bmod u^n$ we compute the coefficients of $T'(v) = R'(v)S'(v) \bmod v^n$ and then compute $\sigma^{-1}(T'(v))$. The last part does not uses any m/d steps.

V. The structure of the matrix $\overline{W}$

In this section we will derive the structure of the matrix $\overline{W}$. The difficulty, which does not appear in [5], comes from the fact that there is at least one invertible row in $\overline{W}$ (Lemma IV.3 [5]) which does not guarantee that the rest of the rows in $\overline{W}$ are invertible. From Lemma IV.5 [5] it follows that if $\deg Q(u) = j > 1$ then there are at least two invertible rows in $\overline{W}$ and by Lemma IV.4 [5] all the rows in $\overline{W}$ are invertible. Lemmas V.1-V.3 are the results of case analysis of the rows of $\overline{W}$.

Lemma V.1: For all $i = 1, ..., n$ let $r_i = (r_{i0}, ..., r_{i,n-1})$. If $\{r_1, ..., r_n\}$ is a basis for $G[u]/ < u^n >$ then there are at most k, $1 \leq k \leq n$, r_i's such that $\delta(r_i) \geq n - k$.

Proof: Assume that there are $k+1$, $1 \leq k \leq n-1$, of r_i such that $\delta(r_i) \geq n-k$. Denote this $k+1$ distinct indices by Ω . Then $r_{i,l} = 0 \quad l = 0, ..., n-k-1$ while i is ranges over the set Ω . Then the $k+1$ vectors $r_i \quad i \in \Omega$ are linearly dependent contradiction to $\{r_1, ..., r_n\}$ being a basis. □

Remark V.1: Since $\{\overline{w}_1, ..., \overline{w}_n\}$ constitute a base then from Lemma V.1 it follows that in $\overline{W}$ there can be at most one row i such that $\delta(\overline{w}_i) = n-1$ (i.e. $\overline{w}_i = (0, ..., 0, \xi) \quad \xi \in G, \quad \xi \neq 0)$.

Lemma V.2: If there exists $\overline{w}_i \in \overline{W}$ so that $1 \leq \delta(\overline{w}_i) \leq n-2$ then there exists at least one $\overline{w}_j \in \overline{W}$ such that $\delta(\overline{w}_j) = 1$.

Proof: Assume

$$t = min\{\delta(\overline{w}_i) \;:\; 1 \leq \delta(\overline{w}_i) \leq n-2 \quad 1 \leq i \leq n-1\} \tag{1a}$$

and let j be such that

$$\delta(\overline{w}_j) = t \tag{1b}$$

From Lemma IV.6 [5], (1a) and (1b) at least $n-t$ multiplications are needed to compute $w_j^T A(\underline{x})\underline{y}$ then by Remark II.1:

$$\alpha_{j,1}, ..., \alpha_{j,n-t-1} \neq 0 \tag{2a}$$

and since $t < n-1$ ((1a)) we can assume that in (2a) there is at least one $\alpha_{j,l} \neq 0 \quad l \in \{1, ..., n-t-1\}$. Assume:

$$\alpha_{j,1} \neq 0 \tag{2b}$$

From (1b) and (2b) we obtain:

$$\delta(\overline{w}_j - \alpha_{j1}\overline{w}_n) = 0 \tag{2c}$$

But $(\overline{w}_j - \alpha_{j1}\overline{w}_n) \times S_1 = b^*_{j1}\overline{w}_j$ so from (1b) and (2c) we obtain:

$$b^*_{j1} \neq 0 \quad \delta(S_1) = \delta(\overline{w}_j) = t. \tag{3}$$

If $\delta(\overline{w}_i) = 0 \quad i \neq j$ then from $(\overline{w}_i - \alpha_{i1}\overline{w}_n) \times S_1 = b^*_{i1}\overline{w}_i$ and (3) we obtain:

$$b^*_{i1} = 0 \tag{4a}$$

and

$$\delta(\overline{w}_i - \alpha_{i,1}\overline{w}_n) \geq n-t > 1 \tag{4b}$$

Let

$$g_i = \begin{cases} \alpha_{i1} & \text{if} \quad \delta(\overline{w}_i) = 0 \\ 0 & \text{if} \quad \delta(\overline{w}_i) > 0 \end{cases} \tag{5}$$

By definition of t ((1a)) and (5) we have defined g_i for all $i = 1, ..., n-1$.
Consider $\{\overline{w}_1 - g_1\overline{w}_n, ..., \overline{w}_{n-1} - g_{n-1}\overline{w}_n, \overline{w}_n\}$. This is a basis for $G[u]/ < u^n >$. By the construction this basis has $n-1$ non-invertible elements. By Lemma V.1 there must be at least one element say $\overline{w}_k - g_k\overline{w}_n$ satisfying

$$\delta(\overline{w}_k - g_k\overline{w}_n) = 1 \tag{6}$$

But

$$\delta(\overline{w}_k) > 0 \tag{7}$$

because if $\delta(\overline{w}_k) = 0$ then from (4b) and (5) we obtain that $\delta(\overline{w}_k - \alpha_{k1}\overline{w}_n) \geq 2$ contradiction to (6). Therefore from (6) and (7) it follows that $g_k = 0$ and $\delta(\overline{w}_k) = \delta(\overline{w}_k - g_k\overline{w}_n) = 1$. $\square$

Lemma V.3: If there is one row i in $\overline{W}$ such that $\delta(\overline{w}_i) = 1$ then there are no two invertible rows in $\overline{W}$ in addition to $\overline{w}_n$.

Proof: Assume:

$$\delta(\overline{w}_1) = \delta(\overline{w}_2) = 0 \tag{1a}$$

and

$$\delta(\overline{w}_{n-1}) = 1 \tag{1b}$$

From Lemma IV.6 ([5]) and (1a) we have

$$\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 1, 2 \tag{2a}$$

From Lemma IV.6 ([5]) and (1b) at least $n-1$ multiplications needed to compute $w_{n-1}A(\underline{x})\underline{y}$ and at least $n-2$ terms of $\alpha_{n-1,1}, ..., \alpha_{n-1,n-2}$ are not zero then by Remark II.1 we can assume that

$$\alpha_{n-1,1}, ..., \alpha_{n-1,n-2} \neq 0 \tag{2b}$$

From (2b), $(\overline{w}_{n-1} - \alpha_{n-1,1}\overline{w}_n) \times S_1 = b^*_{n-1,1}\overline{w}_{n-1}$ and the fact that $\delta(\overline{w}_{n-1} - \alpha_{n-1,1}\overline{w}_n) = 0$ we get

$$b^*_{n-1,1} \neq 0, \quad \delta(S_1) = \delta(\overline{w}_{n-1}) = 1 \tag{3}$$

From $(\overline{w}_i - \alpha_{i1}\overline{w}_n) \times S_1 = b^*_{i1}\overline{w}_i \quad i = 1, 2$, (1a) ,(2a) and (3) we get: $b^*_{i1} = 0 \quad i = 1, 2$ and $\delta(\overline{w}_i - \alpha_{i1}\overline{w}_n) = n-1 \quad i = 1, 2$ contradiction to Lemma V.1 and Remark V.1 since $\{\overline{w}_1 - \alpha_{11}\overline{w}_n,\ \overline{w}_2 - \alpha_{21}\overline{w}_n, \overline{w}_3, ..., \overline{w}_n\}$ is a basis for $G[u]/ < u^n >$. $\square$

The following Corollary (which summarizes Lemmas V.1-V.3) will be very important in the following sections since it will be used as a starting point for a refined case analysis of the rows of $\overline{W}$. If one of the rows of $\overline{W}$ has a null dimension of $n-1$ we designate $\overline{w}_1$ as having $\delta(\overline{w}_1) = n-1$ just for ease of the notation for the rest of this paper without loss of the generality of the coming proofs.

Corollary V.1: The rows of $\overline{W}$ satisfy one of the following relationships:

(i) $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ (i.e. all the rows of $\overline{W}$ are invertible)

Or

(ii) $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$

Or

(iii) $\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-2 \quad \delta(\overline{w}_{n-1}) = 1$

Or

(iv) $\delta(\overline{w}_1) = 0 \quad \delta(\overline{w}_i) > 0 \quad i = 2, ..., n-2 \quad \delta(\overline{w}_{n-1}) = 1$

In (iii) and (iv) we assume $\delta(\overline{w}_n) = 0$

The main results of the paper (which are derived from on Corollary V.1):

Theorem V.1: An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} x_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$'s and $M_i(\underline{y})$'s are given by:

$$\overline{u}_i = \overline{t}_i = K^{-1}\left(1/(w-\beta_i)\right) \quad i = 1, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(1)$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}\left(1/(w-\alpha_{n-1,l})\right) \quad l = 0, ..., n-1$$

where $\delta(w) = 0 \quad w \in G[u]/ < u^n >$ and the minimal degree polynomial (over G) satisfied by w $(mod\ u^n)$ is of degree n, 1 is the unit vector in $G[u]/ < u^n >$ and the set $A = \{\beta_1, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-1}\}$ has $2n-2$ distinct elements . Conversely, for every $\delta(w) = 0 \quad w \in G[u]/ < u^n >$, and for every set $A = \{\beta_1, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-1}\}$ of $2n-2$ distinct elements of G there exist an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

Corollary V.1: Every bilinear algorithm A in $\mathcal{J}_{u^n}$, that is described by Theorem V.1, for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is done by first compute the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ (using Theorem I.1) and then reduce them modulo u^n.

In this algorithm all the distinct scalars from the base field G are not zero. This algorithm is demonstrated in example (1b) in section III.

Theorem V.1': An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$'s and $M_i(\underline{y})$'s are given by:

$$\overline{u}_1 = \overline{t}_1 = 1$$

$$\overline{u}_i = \overline{t}_i = K^{-1}\left(1/(w-\beta_i)\right) \qquad i = 2, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(1)$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}\left(1/(w-\alpha_{n-1,l})\right) \qquad l = 0, ..., n-1$$

where $\delta(w) = 0 \quad w \in G[u]/<u^n>$ and the minimal degree polynomial (over G) satisfied by w (mod u^n) is of degree n, 1 is the unit vector in $G[u]/<u^n>$ and the set $A = \{\beta_2, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-1}\}$ of $2n-3$ distinct elements. Conversely, for every $\delta(w) = 0$ $w \in G[u]/<u^n>$, and for every set $A = \{\beta_2, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-1}\}$ of $2n-3$ distinct elements of G there exist an algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

This is the same type of an algorithm presented in the Theorem V.1 but here one of the scalars which is chosen from the base field G is 0. See example (1a) in section III.

Theorem V.2: An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$s and $M_i(\underline{y})$s are given by:

$$\overline{u}_i = K^{-1}\left(1/(w-\beta_i)\right) \qquad \overline{t}_i = K^{-1}\left(V_0/(w-\beta_i)\right) \quad i = 1, ..., n-2$$

$$\overline{u}_{n-1} = K^{-1}(1) \qquad \overline{t}_{n-1} = K^{-1}(V_0)$$

$$\overline{u}_{n+l} = K^{-1}\left(1/(w-\alpha_{n-1,l})\right) \qquad \overline{t}_{n+l} = K^{-1}\left(V_0/(w-\alpha_{n-1,l})\right) \quad l = 0, ..., n-2$$

$$\overline{u}_{2n-1} = 1 \qquad \overline{t}_{2n-1} = K^{-1}(1)$$

where $\delta(w) = 0 \quad w \in G[u]/<u^n>$, the minimal degree polynomial (over G) satisfied by w (mod u^n) is of degree n, $\delta(V_0) = 1 \quad 1$ is the unit vector in $G[u]/<u^n>$, $\overline{u}_{n+l}^T V_0 = \delta_{l0} \quad l = 0, ...n-1$ and the set $A = \{\beta_1, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-3$ distinct elements. Conversely, for every $\delta(w) = 0 \quad w \in G[u]/<u^n>$, $\delta(V_0) = 1$, and for every set $A = \{\beta_1, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-3$ distinct elements of G there exist an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

Corollary V.2: Every bilinear algorithm A in $\mathcal{J}_{u^n}$, that is described by Theorem V.2, for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is done by first compute the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ (using Theorem I.1) and then reduce them modulo u^n and add $x_0 y_{n-1} u^{n-1}$.

Here all the distinct scalars from the base field G are non-zero. See example (3c) in section III.

Theorem V.2': An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$s and $M_i(\underline{y})$s are given by:

$$\overline{t}_1 = \overline{t}_1 = 1$$

$$\overline{u}_i = K^{-1}\left(1/(w-\beta_i)\right) \qquad \overline{t}_i = K^{-1}\left(V_0/(w-\beta_i)\right) \quad i = 2, ..., n-2$$

$$\overline{u}_{n-1} = K^{-1}(1) \qquad \overline{t}_{n-1} = K^{-1}(V_0)$$

$$\overline{u}_{n+l} = K^{-1}\left(1/(w-\alpha_{n-1,l})\right) \qquad \overline{t}_{n+l} = K^{-1}\left(V_0/(w-\alpha_{n-1,l})\right) \quad l = 0, ..., n-2$$

$$\overline{u}_{2n-1} = 1 \qquad \overline{t}_{2n-1} = K^{-1}(1)$$

where $\delta(w) = 0 \quad w \in G[u]/ < u^n >$, $\delta(V_0) = 1$, 1 is the unit vector in $G[u]/ < u^n > \quad \overline{u}_{n+l}^T V_0 = \delta_{l0} \quad l = 0, ...n-1$ and the set $A = \{\beta_2, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-4$ distinct elements. Conversely, for every $\delta(w) = 0 \quad w \in G[u]/ < u^n >$, $\delta(V_0) = 1$, and for every set $A = \{\beta_2, ..., \beta_{n-2}, 0, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-4$ distinct elements of G there exist an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem. This is the same type of an algorithm as presented in Theorem V.2 but here one of the distinct scalars which is chosen from the base field G is 0.

Theorem V.3: An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$s and $M_i(\underline{y})$s are given by:

$$\overline{u}_i = \overline{t}_i = K^{-1}\left(w/(w-\beta_i)\right) \qquad i = 1, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(w)$$

$$\overline{u}_n = K^{-1}(1) \quad \overline{t}_n = 1$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}\left(w/(w-\alpha_{n-1,l})\right) \qquad l = 1, ..., n-2$$

$$\overline{u}_{2n-1} = 1 \quad \overline{t}_{2n-1} = K^{-1}(1)$$

where $\delta(w) = 0 \quad w \in G[u]/ < u^n >$, $w \notin G$, 1 is the unit vector in $G[u]/ < u^n >$ and the set $A = \{\beta_1, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-4$ distinct elements. Conversely, for every $w \in G[u]/ < u^n >$, $w \notin G$, $\delta(w) = 1$ and for every set $A = \{\beta_1, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-4$ distinct elements of G there exist an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

Corollary V.3: Every bilinear algorithm A in $\mathcal{J}_{u^n}$, that is described by Theorem V.3, for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is done by first compute the coefficients of $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ (using Theorem I.1) and then reduce them modulo u^n and add $(x_0 y_{n-1} + x_{n-1} y_0) u^{n-1}$.

Here all the distinct scalars from the base field G are non-zero.

Theorem V.3': An algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$s and $M_i(\underline{y})$s are given by:

$$\overline{t}_1 = \overline{t}_1 = 1$$

$$\overline{u}_i = \overline{t}_i = K^{-1}\left(w/(w-\beta_i)\right) \qquad i = 2, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(w)$$

$$\overline{u}_n = K^{-1}(1) \quad \overline{t}_n = 1$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}\left(w/(w-\alpha_{n-1,l})\right) \qquad l = 1, ..., n-2$$

$$\overline{u}_{2n-1} = 1 \; \overline{t}_{2n-1} = K^{-1}(1)$$

where $\delta(w) = 1 \quad w \in G[u]/ < u^n >$, $w \notin G$ 1 is the unit vector in $G[u]/ < u^n >$ and the set $A = \{\beta_2, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-5$ distinct elements. Conversely, for every $w \in G[u]/ < u^n >$, $w \notin G$, $\delta(w) = 1$ and for every set $A = \{\beta_2, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-5$ distinct elements of G there exist an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $\quad i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

This is the same type of an algorithm as presented in Theorem V.3 but here one of the scalars that is chosen from the base field G is 0. See example (2a) in section III.

Corollary V.4: Every minimal bilinear algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ mod u^n in $2n-1$ multiplications is equivalent to an algorithm that is described in either Theorem V.1, or Theorem V.1', or Theorem V.2, or Theorem V.2', or Theorem V.3 or Theorem V.3'.

The rest of the paper is devoted to prove these theorems. We will proceed now to a more refined analysis of Corollary V.1. Therefore, in the rest of this paper we will analyze what Corollary V.1 says about the form of the algorithms and we will answer the following questions: In Corollary V.1 (iii) and (iv), what is the δ of the rest of the rows of $\overline{W}$? How does each condition of Corollary V.1 determine S_l, V_l, $\quad a^*_{il}$, b^*_{il} and $\quad \alpha_{il} \quad i, l = 1, ..., n-1$? Does each condition of Corollary V.1 describe an existing algorithm or a family of algorithms ? Do there exist any conditions in Corollary V.1 which are equivalent to each other in the sense of section IV ?

VI. Proof of Theorems V.1, V.1', V.2, V.2'

or

Analysis of the case where all the rows of $\overline{W}$
are invertible, i.e. analysis of Corollary V (i) and (ii).

We assume throughout this section that $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ (Corollary V.1 (i)) or $\delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ and $\delta(\overline{w}_1) = n-1$ (Corollary V.1 (ii)).

The lemmas we present here are technical in nature. The results are applicable to both Corollary V.1 (i) and (ii).

Here is a brief outline of the approach we are taking in this case. Corolloary V.1 (i) states that all the rows of $\overline{W}$ are invertible. But unlike Theorem V.1 ([5]) where all the rows in $\overline{W}$ as elements in $G[u]/ < Q(u)^l >$ $(\deg Q(u) > j)$ are invertible which causes $S_l \quad l = 0, ..., n-1 \quad (t^T_{n+j} S_l = \delta_{jl} \; j, l = 0, ..., n-1)$ to be invertible, here the fact that all the rows of $\overline{W}$ are invertible, as elements in $G[u]/ < u^n >$, do not necessarily yields that all $S_l \quad l = 0, ..., n-1$ are invertible. Thus we get two cases for Corollary V.1 (i) and (ii):

case 1: $\delta(S_l) = 0 \quad l = 0, ..., n-1 \quad \Rightarrow \quad \delta(V_l) = 0 \quad l = 0, ..., n-1$ (example (1b) in section III).

case 2: $\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$

Case 2 is splitted into two subcases:

case 2.1: $\delta(V_l) = 0 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = n-1$

case 2.2: $\delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0$ (example (3c) in section III).

As we will see there does not exist an algorithm which is described by case 2.1. This will limit the number of algorithms we are about to derive.

Lemma VI.1: If $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ or $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ then the following conditions are equivalent:

(i) $\delta(S_l) > 0$

(ii) For all i if $\delta(\overline{w}_i) = 0$ then $b^*_{il} = 0$ where $t_i = \sum_{j=0}^{n-1} b_{ij} t_{n+j}$

(iii) For all i if $\delta(\overline{w}_i) = 0$ then $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) > 0$

(iv) $\delta(S_l) = n-1$.

Proof: Assume

$$\delta(S_l) = t > 0. \tag{1a}$$

Recall that

$$(\overline{w}_i - \alpha_{i,l}\overline{w}_n) \times S_l = b^*_{i,l}\overline{w}_i \quad \delta(\overline{w}_i) = 0 \quad \alpha_{il} \neq 0 \quad l = 1, ..., n-1. \tag{1b}$$

From (1a) and (1b) we have that

$$0 \leq t = \delta(S_l) \leq \delta((\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l) = \delta(b^*_{il}\overline{w}_i). \tag{1c}$$

But

$$\delta(b^*_{il}\overline{w}_i) = \begin{cases} \delta(\overline{w}_i) & \text{if } b^*_{il} \neq 0 \\ n & \text{if } b^*_{il} = 0 \end{cases}$$

Therefore, if $\delta(\overline{w}_i) = 0$ then from (1d) and (2) we get that $b^*_{il} = 0$.
We proved (i) $\Rightarrow$ (ii) .
If $b^*_{il} = 0$ then from (1b) we have $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) \geq n - \delta(S_l) > 0$.
Thus we proved (ii) $\Rightarrow$ (iii) .
If $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) > 0$ then since $\delta(\overline{w}_i) = 0$ we get from (1b) that $\delta(S_l) \geq n - \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) > 0$.
Thus we proved (iii) $\Rightarrow$ (i) .
We will now prove that (i) $\Rightarrow$ (iv) .
For all $i,\ 1 \leq i \leq n-1$, let

$$\tilde{\alpha}_{i,l} = \begin{cases} \alpha_{il} & \text{if } \delta(\overline{w}_i) = 0 \\ 0 & \text{if } \delta(\overline{w}_i) \neq 0 \end{cases} \tag{3}$$

From $\delta(S_l) > 0$, (1b) and (3) if $\delta(\overline{w}_i) = 0$ then

$$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = \delta(\overline{w}_i - \tilde{\alpha}_{il}\overline{w}_n) = n - \delta(S_l) > 0. \tag{4a}$$

From the assumption of the Lemma if $\delta(\overline{w}_i) \neq 0$ then $\delta(\overline{w}_i) = n-1$ and from (3) we have

$$\delta(\overline{w}_i - \tilde{\alpha}_{il}\overline{w}_n) = \delta(\overline{w}_i) = n - 1. \tag{4b}$$

$B = \{\overline{w}_i - \tilde{\alpha}_{i,l}\overline{w}_n, ..., \overline{w}_i - \tilde{\alpha}_{i,l}\overline{w}_n, \overline{w}_n\}$ $(i = 1, \ldots, n)$ is a basis for $G[u]/ < u^n >$. From (3),(4a) and (4b) it follows that in B there are $n-1$ non-invertible elements. Then from Lemma V.1 we have that at least one k, $1 \leq k \leq n-1$, such that

$$\delta(\overline{w}_k - \tilde{\alpha}_{kl}\overline{w}_n) = 1 \tag{5}$$

In (5) $\delta(\overline{w}_k) \neq n-1$ since otherwise from (3) we obtain that $\delta(\overline{w}_k - \tilde{\alpha}_{kl}\overline{w}_n) = \delta(\overline{w}_k) = 1$, contradiction to the assumption of the Lemma. Therefore $\delta(\overline{w}_k) = 0$ and from (1b) and (5) we have that $1 = \delta(\overline{w}_k - \tilde{\alpha}_{kl}\overline{w}_n) \geq n - \delta(S_l)$, so $\delta(S_l) \geq n-1$. Since $S_l \neq 0$ we have $\delta(S_l) = n-1$.
(iv) $\Rightarrow$ (i) is clear. This proves the Lemma. $\Box$

Corollary VI.1: If $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ or $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ then either
(i) $\delta(S_l) = 0 \quad l = 0, ..., n-1$
or
(ii) $\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$

Proof: Assume that for some l, $1 \leq l \leq n-1, \quad \delta(S_l) > 0$ then from Lemma VI.1 we get $\delta(S_l) = n-1$. Since $\{S_0, ..., S_n - 1\}$ is a basis for $G[u]/ < u^n >$ then by Lemma V.1 at most one $S_l \quad l \in \{1, ..., n-1\}$ of this type can exist . $\Box$

For demonstrating Corollary VI.1(i) see examples (1a) and (1b) in section III.
For demonstrating Corollary VI.1(ii) see examples (3a) and (3c) in section III.
We designate S_{n-1} as having $\delta(S_{n-1}) = n-1$ just for ease of the notation in the remainder of this section without loss of generality of the coming proofs.

Corollary VI.2: If $\delta(\overline{w}_i)=0 \quad i=1,...,n$ and $\delta(S_l)=0 \quad l=0,...,n-1$ then $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad i,l=1,...,n-1$.

Corollary VI.2': If $\delta(\overline{w}_1)=n-1 \quad \delta(\overline{w}_i)=0 \quad i=2,...,n$ and $\delta(S_l)=0 \quad l=0,...,n-1$ then $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad i=2,...,n-1 \quad l=1,...,n-1$.

Lemma VI.2: If $\delta(\overline{w}_i)=0 \quad i=1,...,n$ or $\delta(\overline{w}_1)=n-1 \quad \delta(\overline{w}_i)=0 \quad i=2,...,n$ and $\delta(S_l)=0 \quad l=0,...,n-1$ then $\delta(V_l)=0 \quad l=0,...,n-1$.

Proof: From our assumption we can use Corollary VI.2' for some $i, 2\le i\le n-1$, such that $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad l=1,...,n-1$ and $\delta(\overline{w}_i)=0$. Since $\delta(\overline{w}_i)=0$ then $\alpha_{i1},...,\alpha_{i,n-1}\neq 0$. Thus from $(\overline{w}_i-\alpha_{il}\overline{w}_n)\times V_l=a^*_{il}\overline{w}_i\times V_0$ (Lemma IV.7' (iii) [5]) and the above we get $\delta(V_l)=\delta(V_0) \quad l=1,...,n-1$. Since $\{V_0,...,V_{n-1}\}$ is a basis for $G[u]/<u^n>$ then there is at least one invertible element in it, therefore $\delta(V_l)=0 \quad l=0,...,n-1$. $\square$

See examples (1a) or (1b) in section III.

Lemma VI.3: If $\delta(\overline{w}_i)=0 \quad i=1,...,n$ and $\delta(S_l)=0 \quad l=0,...,n-2 \quad \delta(S_{n-1})=n-1$ then $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad i=1,...,n-1 \quad l=1,...,n-2$ and $\delta(\overline{w}_i-\alpha_{i,n-1}\overline{w}_n)\ge 1 \qquad i=1,...,n-1$.

Proof: From Lemma VI.1 we get that for $l,\ 1\le l\le n-1, \quad \delta(S_l)=0$ and thus $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad i=1,...,n-1 \quad l=1,...,n-2$. Since $\delta(S_{n-1})=n-1$ then from Lemma VI.1 we get $b^*_{i,n-1}=0$ and from $(\overline{w}_i-\alpha_{i,n-1}\overline{w}_n)\times S_{n-1}=b^*_{i,n-1}\overline{w}_i$ we obtain: $b^*_{i,n-1}=0 \quad i=1,...,n-1$ and $\delta(\overline{w}_i-\alpha_{i,n-1}\overline{w}_n)\ge 1 \quad i=1,...,n-1$. $\square$

See example (3cc') in section III.

Lemma VI.3': If $\delta(\overline{w}_1)=n-1$ or $\delta(\overline{w}_i)=0 \quad i=1,...,n$ and $\delta(S_l)=0 \quad l=0,...,n-2 \quad \delta(S_{n-1})=n-1$ then $\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad i=2,...,n-1 \quad l=1,...,n-2$ and $\delta(\overline{w}_i-\alpha_{i,n-1}\overline{w}_n)\ge 1 \qquad i=2,...,n-1$.

Proof: The proof is the same as in Lemma VI.3 but i starts from 2 . $\square$

Lemma VI.4: If $\delta(\overline{w}_i)=0 \quad i=1,...,n$ or $\delta(\overline{w}_1)=n-1 \quad \delta(\overline{w}_i)=0 \quad i=2,...,n$, and $\delta(S_l)=0 \quad l=0,...,n-2 \quad \delta(S_{n-1})=n-1$ then either

(i) $\delta(V_l)=0 \quad l=0,...,n-2 \quad \delta(V_{n-1})=n-1$

or

(ii) $\delta(V_l)=1 \quad l=0,...,n-2 \quad \delta(V_{n-1})=0$

Proof: From Lemma VI.3' we can assume that there exists some $i,\ 2\le i\le n-1$, such that

$$\delta(\overline{w}_i)=0 \quad \alpha_{il}\neq 0 \quad i=2,...,n-1 \quad l=1,...,n-2 \tag{1a}$$

and

$$\delta(\overline{w}_i-\alpha_{il}\overline{w}_n)=0 \quad \delta(\overline{w}_i-\alpha_{i,n-1}\overline{w}_n)\ge 1 \quad i=2,\ldots,n-1 \quad l=1,\ldots,n-2. \tag{1b}$$

From $(\overline{w}_i-\alpha_{il}\overline{w}_n)\times V_l=a^*_{il}\overline{w}_i\times V_0$ (Lemma IV.7' (iii) [5]) and (1a) we have that

$$\delta(V_l)=\delta(V_0) \quad l=1,...,n-2 \tag{2}$$

Claim: From (2) we get either

$$\delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0 \tag{3a}$$

or

$$\delta(V_l) = 0 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = n-1 \tag{3b}$$

We will prove that (3a) and (3b) are the only two possibilities that are derivable from (2).
Since $\{V_0, ..., V_{n-1}\}$ are a basis for $G[u]/ < u^n >$ and $\delta(V_0) = \delta(V_1) = ... = \delta(V_{n-2})$ then if for some $l, \quad 0 \leq l \leq n-2, \quad \delta(V_l) > 0$ then from Lemma V.1 there is at least one $k, \quad 0 \leq k \leq n-2$, such that $\delta(V_k) = 1$ therefore for $l, \quad 0 \leq l \leq n-2$, $\delta(V_l) = 1$. In each basis for $G[u]/ < u^n >$ there is at least one invertible element therefore $\delta(V_{n-1}) = 0$. This proves (3a).
Assume that $\delta(V_l) = 0 \quad l = 0, ..., n-2$. If $\delta(V_{n-1}) = 0$ as well, then from $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times V_{n-1} = a^*_{i,n-1}\overline{w}_i \times V_0 \quad i = 2, ..., n-1$ we get that $\delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = \delta(V_0) = 0$ contradiction to (1b) ($\delta(S_{n-1}) \neq 0$ and therefore $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) \neq 0$). Therefore, the only possibility that left is $\delta(V_{n-1}) \neq 0$. Assume

$$\delta(V_{n-1}) = t \neq 0 \tag{4}$$

then from $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times V_{n-1} = a^*_{i,n-1}\overline{w}_i \times V_0$, (1a), (1b) and $\delta(V_0) = 0$ we get:

$$a^*_{i,n-1} = 0 \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq n-t \quad i = 2, ..., n-1. \tag{5}$$

Follow, by now familiar argument, we let

$$\tilde{\alpha}_{i,n-1} = \begin{cases} \alpha_{i,n-1} & \text{if} \quad \delta(\overline{w}_i) = 0 \\ 0 & \text{if} \quad \delta(\overline{w}_i) \neq 0 \end{cases} \tag{6}$$

$B = \{\overline{w}_1 - \tilde{\alpha}_{1,n-1}\overline{w}_n, ..., \overline{w}_{n-1} - \tilde{\alpha}_{n-1,n-1}\overline{w}_n, \overline{w}_n\}$ is a basis for $G[u]/ < u^n >$. From (5) and (6) it follows that in B there are $n-1$ non-invertible elements. Then from Lemma V.1 we have that at least one k, $1 \leq k \leq n-1$

$$\delta(\overline{w}_k - \tilde{\alpha}_{k,n-1}\overline{w}_n) = 1$$

Then from (5) we get $t = n-1$. Therefore, from (4) it follows $\delta(V_{n-1}) = n-1$. This proves (3b) . $\square$

To demonstrate (ii) see examples (3a') or (3cc') in section III.
Lemma VI.5: It cannot happen that both $\delta(S_l) = n-1$ and $\delta(V_l) = n-1$.
Proof: From Lemma IV.7' (ii) ([5]) we get $t_{n+l} = K^{-1}(\overline{w}_n \times V_l)$. $\delta(V_l) = n-1$ then $t_{n+l} = (\xi, 0, ..., 0) \quad \xi \neq 0 \quad \xi \in G$. Since $\delta(S_l) = n-1$, i.e. $S_l = (0, ..., 0, \eta) \quad \eta \neq 0 \quad \eta \in G$, we get $t^T_{n+l}S_l = 0$ contradiction to Corollary IV.2" ([5]) $\square$
Corollary VI.4:
There does not exist an algorithm described by Corollary VI.1 (ii) ($\delta(S_{n-1}) = n-1$) and Lemma VI.4 (i) ($\delta(V_{n-1}) = n-1$).

If we picture, in a diagram format, the relationships among the $\delta(\overline{w}_i)$, $\delta(S_l)$, $\delta(V_l)$ and $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n)$, as derived from our starting point that the rows of $\overline{W}$ are either given by $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ or by $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$, then we get the following diagrams which demonstrate the relationships among these entities.

Notation: The symbol $\downarrow$ means the upper term implies the lower one.

diagram 1:

Start with $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ then

$$\begin{array}{cc} Path1: & Path2: \\ \downarrow & \downarrow \\ \delta(S_l) = 0 \quad l = 0, ..., n-1 & \delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1 \\ \downarrow & \downarrow \\ \delta(V_l) = 0 \quad l = 0, ..., n-1 & \delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0 \\ \downarrow & \downarrow \\ \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 & \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq 1 \\ i, l = 1, ..., n-1 & l = 1, ..., n-2 \quad i = 1, ..., n-1 \end{array}$$

diagram 1':

Start with $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ then:

$$\begin{array}{cc} Path1: & Path2: \\ \downarrow & \downarrow \\ \delta(S_l) = 0 \quad l = 0, ..., n-1 & \delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1 \\ \downarrow & \downarrow \\ \delta(V_l) = 0 \quad l = 0, ..., n-1 & \delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0 \\ \downarrow & \downarrow \\ \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 & \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq 1 \\ i = 2, ..., n-1 \quad l = 1, ..., n-1 & l = 1, ..., n-2 \quad i = 2, ..., n-1 \end{array}$$

So far we have seen the complete relationship among $\delta(\overline{w}_i)$, $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n)$, $\delta(S_l)$ and $\delta(V_l)$ $i, l = 1, ..., n-1$ based on Corollary V.1 (i) and (ii). We will now derive the values of b^*_{il}, a^*_{il}, α_{il} $i, l = 1, ..., n-1$ based on these corollaries.

Lemma VI.6: If $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ and $\delta(S_l) = 0 \quad l = 0, ..., n-1$ then $b^*_{il} \neq 0 \quad a^*_{il} \neq 0 \quad \alpha_{i,l} \neq 0 \quad i, l = 1, ..., n-1$

Proof: From Lemma IV.6 ([5]) we obtain $\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 1, ..., n-1$. From Lemma VI.1 we have $b^*_{il} \neq 0 \quad i, l = 1, ..., n-1$. Then from Corollary VI.2 ($\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad i, l = 1, ..., n-1$) and $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a^*_{il}\overline{w}_i \times V_0$: we have $a^*_{il} \neq 0 \quad i, l = 1, ..., n-1$. $\square$

See example (1b) in section III.

Lemma VI.6': If $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1$ and $\delta(S_l) = 0 \quad l = 0, ..., n-1$ then a^*_{il}, $b^*_{il} \neq 0 \quad i, l = 1, ..., n-1$ and $\alpha_{1l} = 0$, $\alpha_{i,l} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$.

Proof: $\delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1$ then from Lemma IV.6 ([5]) we have that $\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 2, ..., n-1$. From $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i$, and $\delta(S_l) = 0 \quad l = 1, ..., n-1$ we get $b^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$. From $(\overline{w}_1 - \alpha_{1l}\overline{w}_n) \times S_l = b^*_{1l}\overline{w}_1, \quad \delta(\overline{w}_1) = n-1$ and $\delta(S_l) = 0 \quad l = 0, ..., n-1$ we obtain $b^*_{1l} \neq 0 \quad l = 1, ..., n-1$ and $\alpha_{1l} = 0 \quad l = 1, ..., n-1$. From $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a^*_{il}\overline{w}_i \times V_0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$, and $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$ (Corollary VI.2') we get that $a^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$. From $\alpha_{1l} = 0 \quad l = 1, ..., n-1$ we have $\overline{w}_1 \times V_l = a^*_{1l}\overline{w}_1 \times V_0$ then from $\delta(V_l) = 0 \quad l = 0, ..., n-1$ (Lemma VI.2) we get $a^*_{1l} \neq 0 \quad l = 1, ..., n-1$. $\square$

See example (1a) in section III.

Lemma VI.7: If $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n-1$ and $\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$ then $b^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \quad b^*_{i,n-1} = 0 \quad i = 1, ..., n-1, \quad a^*_{il} \neq 0 \quad i, l = 1, ..., n-1$ and $\alpha_{il} \neq 0 \quad i, l = 1, ..., n-1$

Proof: From Lemma IV.6 ([5]) and $\delta(\overline{w}_i) = 0$ we have that $\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 1, ..., n-1$. Since $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i$ then $b^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2$. Since $\delta(S_{n-1}) = n-1, \quad \delta(\overline{w}_i) = 0 \quad i = 1, ..., n-1$ and $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i$ we obtain that $b^*_{i,n-1} = 0 \quad i = 1, ..., n-1$. From Lemma VI.3 ($\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2$) and $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a^*_{il}\overline{w}_i \times V_0$ we have $a^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2$. Since $\delta(V_{n-1}) = 0$ (Lemma VI.2) then from $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times V_{n-1} = a^*_{i,n-1}\overline{w}_i \times V_0$ we have $a^*_{i,n-1} \neq 0 \quad i = 1, ..., n-1$ $\square$

See example (3c) in section III.

Lemma VI.7': If $\delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1, \quad \delta(\overline{w}_1) = n-1$ and $\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$ then $b^*_{il} \neq 0 \qquad b^*_{i,n-1} = 0 \qquad i = 2, ..., n-1 \quad l = 1, ..., n-2$ and either

(i) $\quad \alpha_{1l} = 0 \quad l = 1, ..., n-1, \quad b^*_{1l} \neq 0 \quad l = 1, ..., n-2 \quad b^*_{1,n-1} = 0$ (see example (3c))

or

(ii) $\quad \alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0 \quad b^*_{1l} \neq 0 \quad l = 1, ..., n-1$ (see example (3d))

Proof: From $\delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1$ and Lemma IV.6 ([5]) we get:

$$\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 2, ..., n-1. \tag{1}$$

Since $\delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1$ then $\{u_i, u_{n+1}, ..., u_{2n-1}\} \quad \{t_i, t_{n+1}, ..., t_{2n-1}\} \quad i = 2, ..., n-1$ are two sets of linearly independent n-dimensional vectors (Lemma IV.4 ([5])) then we have

$$a_{i0}, \quad b_{i0} \neq 0 \quad i = 2, ..., n-1 \tag{2}$$

From $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i, \quad \delta(S_l) = 0 \quad l = 0, ..., n-2$, (1) and (2) we have that

$$b^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-2. \tag{3a}$$

Since $\delta(S_{n-1}) = n-1$ and $\delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq 1 \quad i = 2,...,n-1$ (Lemma V.3') then from $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i$ we obtain

$$b^*_{i,n-1} = 0 \quad i = 2,...,n-1 \tag{3b}$$

and $\delta(S_l) = 0 \quad l = 0,...,n-2$ then from $(\overline{w}_1 - \alpha_{1l}\overline{w}_n) \times S_l = b^*_{1l}\overline{w}_1$ it follows that $b^*_{1l} \neq 0 \quad l = 1,...,n-2$. If for some l, $1 \leq l \leq n-1$, $\alpha_{1l} \neq 0$ then $\delta(\overline{w}_1 - \alpha_{1l}\overline{w}_n) = 0$. Therefore, from $(\overline{w}_1 - \alpha_{1l}\overline{w}_n) \times S_l = b^*_{1l}\overline{w}_1$ we get

$$\delta(S_l) = \delta(\overline{w}_1) = n-1 \quad b^*_{1l} \neq 0 \tag{4}$$

Since $\{S_0,...,S_{n-1}\}$ is a basis then Lemma V.1 yields that (4) can appear at most once and we already know that $\delta(S_{n-1}) = n-1$. Thus $\alpha_{1l} = 0 \quad l = 1,...,n-2$.
Therefore, either $\alpha_{1l} = 0, \quad l = 1,...,n-1 \quad b^*_{1,n-1} = 0$ or $\alpha_{1l} = 0 \quad l = 1,...,n-2 \quad \alpha_{1,n-1} \neq 0 \quad b^*_{1l} \neq 0 \quad l = 1,...,n-1$. $\square$

Lemma VI.7": If $\delta(\overline{w}_1) = 1 \quad \delta(\overline{w}_i) = 0 \quad i = 2,...,n$ and $\delta(S_l) = 0 \quad l = 0,...,n-2 \quad \delta(S_{n-1}) = n-1$ then for all $i = 2,...,n-1$ and $l = 1,...,n-1$, $\alpha_{il} \neq 0$ and $a^*_{il} \neq 0$.

Proof: From our assumption and Lemma IV.6 ([5]) we have that $\alpha_{il} \neq 0 \quad i = 2,...n-1 \quad l = 1,...,n-1$. From $(\overline{w}_i - \alpha_{i,l}\overline{w}_n) \times V_l = a^*_{i,l}\overline{w}_i \times V_0$ and for all $i = 2,...,n-1 \quad l = 1,...,n-2 \quad \delta(\overline{w}_i - \alpha_{i,l}\overline{w}_n) = 0$ (Lemma VI.3') we get $a^*_{il} \neq 0 \quad i = 2,...,n-1 \quad l = 1,...,n-2$. From $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times V_{n-1} = a^*_{i,n-1}\overline{w}_i \times V_0$ and $\delta(V_{n-1}) = 0$ we obtain $a^*_{i,n-1} \neq 0 \quad i = 2,...,n-1$. $\square$

In the next Lemma we will prove that under the assumptions of Corollary V.1 (i) and (ii), regardless Lemma VI.7', $a^*_{1l} \triangleq a_{1l}/a_{10}$ is not defined.

Lemma VI.8: If $\delta(\overline{w}_1) = 1 \quad \delta(\overline{w}_i) = 0 \quad i = 2,...,n, \quad \delta(S_l) = 0 \quad l = 0,...,n-2 \quad \delta(S_{n-1}) = n-1$ and if Lemma VI.7' (i) ($\alpha_{1l} = 0 \quad l = 1,...,n-1$) is given or by Lemma V.7' (ii) ($\alpha_{1l} = 0 \quad l = 1,...,n-2, \quad \alpha_{1,n-1} \neq 0$) is given then $a_{10} = 0$.

Proof: From $Ku_{2n-1} = \overline{w}_n \times S_{n-1}$ and using $\delta(S_{n-1}) = n-1$ we obtain that $\overline{u}_{2n-1} = (1,0,...,0)$. But $b_{10}Ku_1 = \overline{w}_1$ then from $\delta(\overline{w}_{n-1}) = n-1$ we get (assume $b_{10} = 1$) that $\overline{u}_1 = (1,0,...,0)$. For all $i, 1 \leq i \leq n-1$, $u_i = \sum_{j=0}^{n-1} a_{ij}u_{n+j}$ (Corollary IV.2' ([5])) then we have that $\{u_1, u_{n+1},...,u_{2n-1}\}$ are linearly dependent therefore $a_{1,0} = 0$. $\square$
See example (3a) in section III.

By incorporating results of Lemmas VI.6-VI.8 into diagram 1 and diagram 1' respectively we get the following diagrams which show the complete dependency among $\delta(\overline{w}_i)$, α_{il}, $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n)$, b^*_{il} and a^*_{il} for all i and $l, 1 \leq i,l \leq n-1$.

diagram 2:

Start with $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ then:

$Path1:$	$Path2:$
$\downarrow$	$\downarrow$
$\delta(S_l) = 0 \quad l = 0, ..., n-1$	$\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$
$\downarrow$	$\downarrow$
$\delta(V_l) = 0 \quad l = 0, ..., n-1$	$\delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0$
$\downarrow$	$\downarrow$
$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$	$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq 1$
$i, l = 1, ..., n-1$	$l = 1, ..., n-2 \quad i = 1, ..., n-1$
$\downarrow$	$\downarrow$
$b^*_{il} \neq 0$	$b^*_{il} \neq 0 \ b^*_{i,n-1} = 0$
$i, l = 1, ..., n-1$	$l = 1, ..., n-2 \quad i = 1, ..., n-1$
$\downarrow$	$\downarrow$
$a^*_{il} \neq 0$	$a^*_{il} \neq 0$
$i, l = 1, ..., n-1$	$i, l = 1, ..., n-1$
$\downarrow$	$\downarrow$
$a_{il} \neq 0$	$a_{il} \neq 0$
$i, l = 1, ..., n-1$	$i, l = 1, ..., n-1$

Path 1 is demonstrated by example (1b) and Path 2 by example (3c) in section III.

diagram 2':

Start with $\delta(\overline{w}_1) = n-1 \ \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ then:

$Path1:$	$Path2:$	
$\downarrow$	$\downarrow$	
$\delta(S_l) = 0 \quad l = 0, ..., n-1$	$\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$	
$\downarrow$	$\downarrow$	
$\delta(V_l) = 0 \quad l = 0, ..., n-1$	$\delta(V_l) = 1 \quad l = 0, ..., n-2 \quad \delta(V_{n-1}) = 0$	
$\downarrow$	$\downarrow$	
$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$	$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \geq 1$	
$i = 2, ..., n-1 \quad l = 1, ..., n-1$	$l = 1, ..., n-2 \quad i = 2, ..., n-1$	
$\downarrow$	$\downarrow$	
$b^*_{il} \neq 0$	$b^*_{il} \neq 0 \ b^*_{i,n-l} = 0$	
$i, l = 1, ..., n-1$	$l = 1, ..., n-2 \quad i = 2, ..., n-1$	
$\downarrow$	$\downarrow$	
$a^*_{il} \neq 0$	$a^*_{il} \neq 0, \quad a_{10} = 0$	
$i, l = 1, ..., n-1$	$l = 1, ..., n-1 \quad i = 2, ..., n-1$	
$\downarrow$	$\downarrow$	
$\alpha_{il} \neq 0 \quad \alpha_{1l} = 0$	$\alpha_{il} \neq 0$	
$i = 2, ..., n-1 \quad l = 1, ..., n-1$	$l = 1, ..., n-1 \quad i = 2, ..., n-1$	
	$\downarrow$	$\downarrow$
	$\alpha_{il} = 0$	$\alpha_{il} = 0 \ \alpha_{1,n-1} \neq 0$
	$l = 1, ..., n-1$	$l = 1, ..., n-2$
	$\downarrow$	$\downarrow$
	$b^*_{1l} \neq 0 \ b^*_{1,n-1} = 0$	$b^*_{1l} = 0$
	$l = 1, ..., n-2$	$l = 1, ..., n-1$

Path 1 is demonstrated by example (1a) and the left most path of Path 2 by example (3a) in section III.

We have made all the (exhausting) technical preparation for derivation of all the minimal bilinear algorithms which are based on $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ (Corollary V.1 (i)) and $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ (Corollary V.1 (ii)).

Our classification is based on Diagrams 2 and 2'.

By scanning Diagrams 2 and 2' it seems that we might have here five different algorithms since we have five different paths to follow in Diagrams 2 and 2'. Here is a description of the paths we have to follow and the algorithms they generate:

Algorithm 1: Use Path 1 of Diagram 2. The algorithm it generates is given by Theorem V.1.

Algorithm 2: Use Path 1 of Diagram 2'. The algorithm it generates is given by Theorem V.1'. This algorithm is a variation of algorithm 1 but it is not equivalent to him.

Algorithm 3: Use path 2 of Diagram 2. The algorithm it generates is given by Theorem V.2.

Algorithm 4: Use Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-1$ of Diagram 2'. This algorithm is given by Theorem V.2' . This algorithm is a variation of algorithm 3 but it is not equivalent to him.

Algorithm that is based on Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0$ of Diagram 2' is equivalent to the algorithm which have already been described by Theorem V.2'. This will be shown in Corollary VI.5.

Therefore we get two new algorithms and two unrelated algorithms which are variations of these two.

Remark: All the theorems in this section and the coming ones are of the 'if and only if' types. We will prove the 'if' parts; proofs of the converses are essentially the same as the one for Theorem V.1' ([5]) . In proving our results, we will exhibit the explicit forms of the multiplications, i.e. if the algorithm is given in the form $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ where $\underline{m} = (m_1, ..., m_{2n-1})^T, \quad m_i = L_i(\underline{x})M_i(\underline{y}) \quad i = 1, ..., 2n-1$, then we will present for all $i, \quad 1 \leq i \leq 2n-1$, the form of $L_i(\underline{x})$ and $M_i(\underline{y})$. Once we determine the multiplications, the algorithm is completely determined.

We would like to make some general remarks concerning proofs of the converses which we are omitting. The 'only if' direction will be proved in general as the following: Given some vectors in $G[u]/ < u^n >$, distinct scalars from the field G and the multiplications, which have already been derived in the 'if' direction, we can construct the algorithm by using the identities of Lemma IV.8, Lemma IV.8' and Corollary IV.4 (all from [5]). Therefore in each case, the identities of Lemma IV.8, Lemma IV.8' and Corollary IV.4 can be verified from the assumption made in the hypothesis. Once these have been validated we can use the same argumentation and technique as the one in Theorem V.1' ([5]) to construct specific algorithms.

Algorithm 1: The algorithm that is based on Path 1 of Diagram 2:

Proof of Theorem V.1: If the algorithm is described by $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$ (Corollary V.1(i)) and by $\delta(S_l) = 0 \quad l = 0, ..., n-1$ then we can use Path 1 of Diagram 2. The conditions of the Theorem are the same as in the Theorem V.1 ([5]) but the computation is performed in $G[u]/ < u^n >$.

Since for all i and l, $1 \leq i, l \leq n-1$, $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$ (Path 1 of Diagram 2) then from the identities $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i \times S_0$ and $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a^*_{il}\overline{w}_i \times V_0$ we have:

$$S_l = b^*_{n-1,l}w/(w - \alpha_{n-1,l}) \qquad V_l = a^*_{n-1,l}w \times V_0/(w - \alpha_{n-1,l}) \qquad l = 1, ..., n-1 \tag{1}$$

where $w = \overline{w}_{n-1}/\overline{w}_n$, $b^*_{il} = b_{il}/b_{i,0}$ and the same for a^*_{il}.

Since for all i and l, $1 \leq i, l \leq n-1$, $b^*_{i,l} \neq 0$, $a^*_{il} \neq 0$, $\alpha_{il} \neq 0$ and $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$ (Path 1 of Diagram 2) then it follows that Lemmas IV.8,IV.8' and Corollary IV.4 (all from ([5])) are valid for $t = 0$ and for all $i = 1, ..., n-1 \quad \Omega_i = \{1, ..., n-1\}$. Therefore we can substitute $\overline{w}_i = \gamma_i\overline{w}_{n-1}/(w - \beta_i) \quad i = 1, ..., n-2$ (Corollary IV.4 ([5])) into $b_{i0}Ku_i = \overline{w}_i \quad i = 1, ..., n-2$ (Lemma IV.7 (iii) ([5])) and from (1) substitute $S_l \quad l = 1, ..., n-1$ into $Ku_{n+l} = \overline{w}_n \times S_l$ (Lemma IV.7 (i) ([5])) and get

$$u_i = \frac{\gamma_i}{b_{i0}}K^{-1}(\overline{w}_{n-1}/(w - \beta_i)) \qquad i = 1, ..., n-2 \tag{2a}$$

$$u_{n-1} = \frac{1}{b_{n-1,0}}K^{-1}\overline{w}_{n-1} \tag{2b}$$

$$u_n = K^{-1}\overline{w}_n = K^{-1}(\overline{w}_{n-1}/(w - \alpha_{n-1,0})) \qquad \alpha_{n-1,0} = 0 \tag{2c}$$

$$u_{n+l} = b^*_{n-1,l}K^{-1}(\overline{w}_{n-1}/(w - \alpha_{n-1,l})) \qquad l = 1, ..., n-1 \tag{2d}$$

Substitute $\overline{w}_i = \gamma_i\overline{w}_{n-1}/(w - \beta_i) \quad i = 1, ..., n-2$ (Corollary IV.4 ([5])) into $a_{i0}Kt_i = \overline{w}_i \times V_0 \quad i = 1, ..., n-2$ (Lemma IV.7' (i) ([5])) and substitute $V_l \quad l = 1, ..., n-1$ ((1)) into $Kt_{n+l} = \overline{w}_n \times V_l$ (Lemma IV.7' (ii) ([5])) and get:

$$t_i = \frac{\gamma_i}{a_{i0}}K^{-1}(\overline{w}_{n-1} \times V_0/(w - \beta_i)) \qquad i = 1, ..., n-2 \tag{3a}$$

$$t_{n-1} = \frac{1}{a_{n-1,0}}K^{-1}(\overline{w}_{n-1} \times V_0) \tag{3b}$$

$$t_n = K^{-1}(\overline{w}_n \times V_0) = K^{-1}(\overline{w}_{n-1} \times V_0/(w - \alpha_{n-1,0})) \qquad \alpha_{n-1,0} = 0 \tag{3c}$$

$$t_{n+l} = a^*_{n-1,l}K^{-1}(\overline{w}_{n-1} \times V_0/(w - \alpha_{n-1,l})) \qquad l = 1, ..., n-1 \tag{3d}$$

$\overline{w}_{n-1}/\overline{w}_n = w$.

Since $\{\overline{u}_n, ..., \overline{u}_{2n-1}\}$ are linearly independent (Lemma IV.4 ([5])) then $\{1/(w-\alpha_{n-1,0}), ..., 1/(w-\alpha_{n-1,n-1})\}$ are also linearly independent. Therefore $\alpha_{n-1,l} \quad l = 0, ..., n-1$ are distinct and since

$\alpha_{n-1,l} \neq \beta_i \quad l = 1, ..., n-1 \quad i = 1, ..., n-2$ (Lemma IV.8 (ii) ([5])) it follows that all the scalars we choose from G must be distinct. In addition, from Lemma IV.10 ([5])) we get that $\{1, w, ..., w^{n-1}\}$ are linearly independent, hence if there is a polynomial $P'(u)$ such that $P'(w) = 0 \bmod u^n$ then $\deg P'(u) = n$.

As in Theorem V.1 ([5]) we get rid of the constants and the invertible elements, $\overline{w}_{n-1}$ and $\overline{w}_{n-1} \times V_0$, and get the first half of the theorem. $\square$

If we compare the interpretation of section VI in [5] we see that this is the same type of algorithm which has been derived in Theorem VI.1 ([5]) but it is computed in the algebra $G[u]/ < u^n >$. Thus, this algorithm is computed, as explained in Theorem VI.1 ([5]) , by first computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ using Theorem I.1 and then reducing them modulo u^n.

This is the algorithm which is demonstrated in example (1b) in section III.

Algorithm 2: The algorithm that is based on Path 1 of Diagram 2':

Proof of Theorem V.1': If the algorithm is described by $\delta(\overline{w}_1) = n-1, \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$ (Corollary V.1(ii)) and by $\delta(S_l) = 0 \quad l = 0, ..., n-1$, i.e. it is based on Path 1 of Diagram 2' then u_i and $t_i \quad i = 2, ..., 2n-1$ are the same as in Theorem V.1 but since $\delta(\overline{W}_1) = n-1$ we get from $b_{i0}Ku_1 = \overline{w}_1$ (Lemma IV.7 (iii) ([5])) and $a_{i0}Kt_1 = \overline{w}_1 \times V_0$ (Lemma IV.7' (i) ([5])) that $\overline{u}_1 = \overline{t}_1 = 1$. $\square$

This type of algorithm is demonstrated in example (1a) in section III. Here one of the scalars that is chosen from the base field is 0. Hence, the multiplcation p_1 is x_0y_0. If we choose non-zero distinct scalars then we get the algorithm which is described in Theorem V.1.

Algorithm 3: The algorithm that is based on Path 2 of Diagram 2:

Proof of Theorem V.2: Assume the algorithm is described by $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n-1$ (Corollary V.1 (i)) and $\delta(S_l) = 0 \quad l = 0, ..., n-2 \quad \delta(S_{n-1}) = n-1$ i.e. the algorithm is described by Path 2 of Diagram 2. Since for all i and l, $1 \leq i \leq n-1 \quad 1 \leq l \leq n-2, \quad \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$ (Path 2 of Diagram 2) then, as in the proof of Theorem V.1, we have:

$$S_l = b^*_{n-1,l} w/(w - \alpha_{n-1,l}) \qquad V_l = a^*_{n-1,l} w \times V_0/(w - \alpha_{n-1,l}) \qquad l = 1, ..., n-2 \qquad (1)$$

where $w = \overline{w}_{n-1}/\overline{w}_n$.

Since for all i and l, $\quad 1 \leq i, l \leq n-1, \quad a^*_{il} \neq 0, \quad \alpha_{il} \neq 0, \quad \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$ and for all i and l, $1 \leq i \leq n-1 \quad 1 \leq l \leq n-2, \quad b^*_{il} \neq 0$ (Path 2 of Diagram 2) then follows that Lemmas IV.8,IV.8' and Corollary IV.4 (all from [5]) are valid for $t = 0$ and for all $i = 1, ..., n-1 \quad \Omega_i = \{1, ..., n-2\}$. Therefore we can substitute $\overline{w}_i = \gamma_i \overline{w}_{n-1}/(w - \beta_i) \quad i = 1, ..., n-2$ (Corollary IV.4 ([5])) into

$b_{i0}Ku_i = \overline{w}_i \quad i = 1, ..., n-2$ (Lemma IV.7 (iii) ([5])) and substitute $S_l \quad l = 1, ..., n-2$ ((1)) into $Ku_{n+l} = \overline{w}_n \times S_l$ (Lemma IV.7 (i) ([5])) and get:

$$u_i = \frac{\gamma_i}{b_{i0}} K^{-1}(\overline{w}_{n-1} \times S_0/(w - \beta_i)) \quad i = 1, ..., n-2 \tag{2a}$$

$$u_{n-1} = \frac{1}{b_{n-1,0}} K^{-1}(\overline{w}_{n-1} \times S_0) \tag{2b}$$

$$u_n = K^{-1}(\overline{w}_{n-1} \times S_0) = K^{-1}(\overline{w}_{n-1} \times S_0/(w - \alpha_{n-1,0})) \qquad \alpha_{n-1,0} = 0 \tag{2c}$$

$$u_{n+l} = b^*_{n-1,l} K^{-1}(\overline{w}_{n-1} \times S_0/(w - \alpha_{n-1,l})) \qquad l = 1, ..., n-2 \tag{2d}$$

$$u_{2n-1} = K^{-1}\overline{w}_n \times S_n - 1 \tag{2e}$$

Substitute $\overline{w}_i = \gamma_i \overline{w}_{n-1}/(w - \beta_i) \quad i = 1, ..., n-2$ (Corollary IV.4 ([5])) into $a_{i0}Kt_i = \overline{w}_i \times V_0 \quad i = 1, ..., n-2$ (Lemma IV.7' (i) ([5])) and substitute $V_l \quad l = 1, ..., n-2$ ((1)) into $Kt_{n+l} = \overline{w}_n \times V_l$ (Lemma IV.7' (ii) ([5])) and get:

$$t_i = \frac{\gamma_i}{a_{i0}} K^{-1}(\overline{w}_{n-1} \times V_0/(w - \beta_i)) \qquad i = 1, ..., n-2 \tag{3a}$$

$$t_{n-1} = \frac{1}{a_{n-1,0}} K^{-1}(\overline{w}_{n-1} \times V_0) \tag{3b}$$

$$t_n = K^{-1}(\overline{w}_n \times V_0) = K^{-1}(\overline{w}_{n-1} \times V_0/(w - \alpha_{n-1,0})) \qquad \alpha_{n-1,0} = 0 \tag{3c}$$

$$t_{n+l} = a^*_{n-1,l} K^{-1}(\overline{w}_{n-1} \times V_0/(w - \alpha_{n-1,l})) \qquad l = 1, ..., n-2 \tag{3d}$$

$$t_{2n-1} = K^{-1}\overline{w}_n \times V_{n-1} \tag{3e}$$

$\delta(S_{n-1}) = n-1$ then from (2e) we get $u_{2n-1} = (\xi, 0, ..., 0) \quad \xi \neq 0 \quad \xi \in G \quad (\delta(u_{2n-1}) = 0)$. $\delta(V_{n-1}) = 0$ then by the same method we use in Lemma IV.5 ([5]) (see Remark IV.2 ([5])) we can get for V_{n-1} that

$$V_{n-1} = \overline{w}_n = (1, 0, ..., 0) \tag{4}$$

$(\delta(S_0) = 0)$. As we did in Theorem V.1 ([5]), make the constants unity. $\delta(\overline{w}_{n-1}) = \delta(S_0) = 0$ then we can get rid of $\overline{w}_{n-1} \times S_0$ and by using $\delta(S_{n-1}) = n-1$ and (4) $(w = \overline{w}_{n-1})$ we get the multiplications which are stated in the theorem and $\alpha_{n-1,0} = 0 \quad \delta(w) = 0, \quad \delta(V_0) = 1, \quad w \in G[u]/ < u^n >$, 1 is the unit vector in $G[u]/ < u^n > \quad \overline{u}^T_{n+l}V_0 = \delta_{l0} \quad l = 0, ..., n-1$. Since $\delta(S_{n-1}) = n-1$ then after getting rid of $\overline{w}_{n-1} \times S_0, \quad u_{2n-1}$ still stays $(\xi, 0, ..., 0) \quad 0 \neq \xi \in G$.

Since $\{\overline{u}_n, ..., \overline{u}_{2n-1}\}$ are linearly independent (Lemma IV.4 ([5])) then $\{1/(w-\alpha_{n-1,0}), ..., 1/(w-\alpha_{n-1,n-2})\}$ are also linearly independent. Therefore $\alpha_{n-1,l} \quad l = 0, ..., n-2$ are distinct and since $\alpha_{n-1,l} \neq \beta_i \quad l = 1, ..., n-2 \quad i = 1, ..., n-2$ (Lemma IV.8 (ii) ([5])) it follows that all the scalars we choose from G must be distinct. □

Based on the same type of arguments given in Section VI ([5]), the algorithm which is presented in Theorem V.2 is the algorithm that in order to compute the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$

in $2n-1$ multiplications we have to compute the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i) \bmod u^n + x_0 y_{n-1} u^{n-1}$. This is done by first computing the coefficients $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ (using Theorem I.1) and then reducing them modulo u^n .

This type of algorithm is presented in example (3c) in section III.

Later on we will see an algorithm that is equivalent to this type.

Algorithm 4: The algorithm that is based on Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-1$ of Diagram 2':

Proof of Theorem V.2': Assume the algorithm is described by Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-1$ of Diagram 2' then we have that $\delta(\overline{w}_1) = n-1, \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n-1, \quad \delta(S_l) = 0 \quad l = 0, ..., n-2, \quad \delta(S_{n-1}) = n-1$. Since for all i and l, $2 \le i \le n-1 \quad 1 \le l \le n-2, \quad \delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0, \quad b^*_{il} \ne 0, \quad a^*_{il} \ne 0, \quad \alpha_{il} \ne 0$ and $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0$ (Path 2 of Diagram 2') then it follows that Lemmas IV.8,IV.8' and Corollary IV.4 (all from [5]) are valid for $t = 0$ and for all $i = 2, ..., n-1 \quad \Omega_i = \{1, ..., n-2\}$.

From $Ku_{2n-1} = \overline{w}_{n-1} \times S_{n-1}$ using $\delta(S_{n-1}) = n-1$ we obtain:

$$\overline{u}_{2n-1} = (1, 0, ..., 0) \tag{1a}$$

$b_{10}Ku_1 = \overline{w}_1$ then from $\delta(\overline{w}_1) = n-1$ we get (assume $b_{10} = 1$)

$$\overline{u}_1 = (1, 0, ..., 0)\,. \tag{1b}$$

We have already shown that

$$a_{10} = 0 \quad \alpha_{1l} = 0 \quad l = 1, ..., n-1\,. \tag{2}$$

Recall $U_{\overline{w}_i} = Kt_i u_i^T + \sum_{j=1}^{n-1} \alpha_{ij} K t_{n+j} u_{n+j}^T$ (Corollary IV.1 ([5])), $\quad u_i = \sum_{j=0}^{n-1} a_{ij} u_{n+j}$ (Corollary IV.2' ([5])). From (2) we have

$$U_{\overline{w}_1} = Kt_1 u_1^T = Kt_1(\sum_{j=0}^{n-1} a_{1j} u_{n+j})^T \tag{3a}$$

Multiply (3a) by V_{n-1} then (using $u_{n+j}^T \nu_{n-1} = \delta_{j,n-1}, \quad U_{\overline{w}_1}\nu_{n-1} = \overline{w}_1 \times \nu_{n-1}$):

$$a_{1,n-1}Kt_1 = \overline{w}_1 \times V_{n-1} \tag{3b}$$

Since $\delta(V_{n-1}) = 0$ then $\overline{w}_1 \times V_{n-1} \ne 0$ and from $\delta(\overline{w}_1) = n-1$ we get:

$$a_{1,n-1} \ne 0 \qquad \overline{t}_1 = (1, 0, ..., 0) \tag{3c}$$

Theorem V.2 is based on Path 2 of Diagram 2 while this Theorem is based on Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-1$. Thus, the difference between the two is in the first multiplication and the rest of the multiplications , u_i and $t_i \quad i = 2, ..., n-1$ are the same one as in Theorem V.2 and $\overline{u}_1 = \overline{t}_1 = 1$. Since $\{\overline{u}_n, ..., \overline{u}_{2n-2}\}$ are linearly independent (Lemma IV.4 ([5])) then $\{1/(w - \alpha_{n-1,0}), ..., 1/(w - \alpha_{n-1,n-2})\}$ are also linearly independent. Therefore $\alpha_{n-1,l} \quad l = 0, ..., n-2$ are distinct and since $\alpha_{n-1,l} \neq \beta_i \quad l = 2, ..., n-2 \quad l = 0, ..., n-2$ (Lemma IV.8 (ii) ([5])) it follows that all the scalars we choose from G must be distinct. □

The difference between this algorithm and the algorithm presented in Theorem V.2 is lies in the fact that here one of the distinct scalars we choose is 0. This type of algorithm is demonstrated in example (3a) in section III.

Analyzing Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0$ of Diagram 2':

Since in Theorem V.2' $\overline{u}_1 = \overline{u}_{2n-1}$ then by using tranformation 4 of IV, which is a linear combination of $\overline{t}_1$ and $\overline{t}_{2n-1}$, we can get an equivalent algorithm (see example (3d) in section III). In Corollary VI.5 we will prove that algorithm which is based on Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0$ of Diagram 2' is equivalent to the algorithm which have already been derived in Theorem V.2'.

Corollary VI.5: If an algorithm is described by Path 2 and $\alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0$ of Diagram 2' then it is equivalent to the algorithm that is described in Theorem V.2'.

Proof: The only difference in Lemma VI.7' between (i) and (ii) is that $\alpha_{1,n-1} \neq 0$. From $U_{\overline{w}_1} = Kt_1 u_1^T + \sum_{j=1}^{n-1} \alpha_{1j} K t_{n+j} u_{n+j}^T$ (Corollary IV.1 ([5])) and $\alpha_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{1,n-1} \neq 0$ (Path 2 of Diagram 2') we get:

$$U_{\overline{w}_1} = Kt_1 u_1^T + \alpha_{1,n-1} K t_{2n-1} u_{2n-1}^T \tag{1a}$$

Multiply (1a) by V_{n-1} using $u_1 = \sum_{j=1}^{n-1} a_{1j} u_{n+j}$ and we get $\overline{w}_1 \times V_{n-1} = a_{1,n-1} K t_1 + \alpha_{1,n-1} k t_{2n-1}$. Using $\delta(V_{n-1}) = 0, \quad \delta(\overline{w}_1) = n-1$ we get $t_1 = (1, 0, ...0) + \xi t_{2n-1} \quad \xi \neq 0 \quad \xi \in G$ and by using transformation 4 of IV this algorithm is equivalent to the algorithm which is described in Theorem V.2'. □

To demonstrate the equivalence between this algorithm and Theorem V.2' consult example (3d) in section III.

So far we got two types of unrelated algorithms. Although we have to go quite a bit in our classification to analyze Corollary V.1 (iii) and (iv), the lengthy discussions in the next sections will yield only one new type of algorithm and the rest of the algorithms will be equivalent to those which we have already derived in this section.

VII. Proof of Theorems V.3, V.3' or Analysis of Corollary V.1 (iii)

In this section we assume that in the matrix $\overline{W}$ we have $\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-2 \quad \delta(\overline{w}_{n-1}) = 1$ (Corollary V.1 (iii)).

In order to classify all the algorithms that are based on Corollary V.1 (iii) we have to know, as it was done before, the exact structure of the matrix $\overline{W}$ and the values of $\alpha_{il}, \quad a^*_{il}, \quad b^*_{il}, \quad S_l$ and $V_l \quad i, l = 1, ..., n-1$.

We will start by getting a more refined structure of the matrix $\overline{W}$. The main idea here is that since $\delta(\overline{w}_{n-1}) = 1$ then at least $n-1$ multiplications are needed to compute $\overline{w}_{n-1}A(\underline{x})\underline{y}$ and we can assume that for at least one row of the matrix α we have that $\alpha_{n-1,1}, ..., \alpha_{n-1,n-1} \neq 0$ and this will yield that $\alpha_{ij} \neq 0 \quad i = 1, ..., n-1, \quad j = 1, ..., n-2$.

Lemma VII.1: If $\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-2 \quad \delta(\overline{w}_{n-1}) = 1 \quad \delta(\overline{w}_n) = 0$ then either

(i) $\delta(\overline{w}_i) = 1 \quad i = 1, ..., n-1 \quad \alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \quad \delta(S_i) = 1 \quad i = 1, ..., n-2$

or

(ii) $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1 \quad \alpha_{1l}, \quad b^*_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 2, ..., n-1$ (example (2a)) $\quad l = 1, ..., n-2, \quad \delta(S_i) = 1 \quad i = 1, ..., n-2$

Proof: Since $\delta(\overline{w}_{n-1}) = 1$ then from Lemma IV.6 ([5]) at least $n-1$ multiplications are needed to compute $w_{n-1}A(\underline{x})\underline{y}$ then we can assume that the first $n-2$ elements of the $n-1$th row in the matrix α are not zero,

$$\alpha_{n-1,1}, ..., \alpha_{n-1,n-2} \neq 0 \ . \tag{1a}$$

From $\delta(\overline{w}_{n-1}) = 1$ and (1a) we have that

$$\delta(\overline{w}_{n-1} - \alpha_{n-1,l}\overline{w}_n) = \delta(w - \alpha_{n-1,l}) = 0 \quad l = 1, ..., n-2 \quad w = \overline{w}_{n-1}/\overline{w}_n \tag{1b}$$

From $(\overline{w}_{n-1} - \alpha_{n-1,l}\overline{w}_n) \times S_l = b^*_{n-1,l}\overline{w}_{n-1}$ and (1b) we have that

$$b^*_{n-1,l} \neq 0 \qquad \delta(S_l) = \delta(\overline{w}_{n-1}) = 1 \qquad l = 1, ..., n-2 \tag{1c}$$

For all $i = 1, ..., n-2 \quad l = 1, ..., n-1$ recall Corollary IV.3 ([5])

$$\frac{\overline{w}_i}{\overline{w}_n} \times (b^*_{n-1,l}w - b^*_{i,l}(w - \alpha_{n-1,l})) = \alpha_{il}b^*_{n-1,l}w \qquad w = \frac{\overline{w}_{n-1}}{\overline{w}_n} \tag{2}$$

. If for some $i, l \in \{1, ..., n-2\}$ we assume that $\alpha_{il} = 0$ then from (2) we get:

$$\overline{w}_i \times (b^*_{n-1,l}w - b^*_{il}(w - \alpha_{n-1,l})) = 0, \quad w = \overline{w}_{n-1}/\overline{w}_n, \quad \delta(w) = 1 \tag{3a}$$

If in (3a) $b^*_{n-1,l} = b^*_{il}$ then $\overline{w}_i \times (b^*_{il}\alpha_{n-1,l}) = 0$ and from (1a) and the fact that $\overline{w}_i \neq 0$ we get $b^*_{il} = 0$ thus $b^*_{n-1,l} = 0$ contradiction to (1c), hence $b^*_{n-1,l} \neq b^*_{il}$.

From (1b) and (1c) we get:

$$\delta(b^*_{n-1,l}w - b^*_{il}(w - \alpha_{n-1,l})) = 0 \tag{3b}$$

(3b) is contradiction to (3a) therefore

$$b^*_{il} = 0 \tag{4}$$

From (1c),(3a) and (4) we get:

$$\overline{w}_i \times b^*_{n-1,l}w = 0 \tag{5a}$$

From (1c) and (5a) it follows:

$$\delta(\overline{w}_i) + \delta(w) \geq n \tag{5b}$$

Since $\delta(w) = \delta(\overline{w}_{n-1}) = 1$ ((1c)) we obtain that

$$\delta(\overline{w}_i) = n - 1 \tag{5c}$$

or equivalently $w_i^T = (\xi, 0, ..., 0) \quad \xi \in G \qquad \xi \neq 0$. Only one row of this type ((5d)) can be in W. Since i and l are arbitrary , we have just proved that for all i and l, $\quad 1 \leq i, l \leq n-2$,

$$\text{If} \quad \alpha_{il} = 0 \quad \Rightarrow \quad b^*_{il} = 0, \quad w_i^T = (\xi, 0, ..., 0) \quad \xi \in G \quad \xi \neq 0 \tag{6}$$

Assume for some $i, l \in \{1, ..., n-2\}$ that

$$b^*_{il} = 0 \tag{7a}$$

then from (2) using (1c) we obtain:

$$w \times \left(\frac{\overline{w}_i}{\overline{w}_n} - \alpha_{il}\right) = 0 \tag{7b}$$

Because of the non-singularity of $\overline{W}$ then $\overline{w}_i$ and $\overline{w}_n$ are linearly independent so that $(\overline{w}_i/\overline{w}_n) \neq \alpha_{il}$. By our assumption

$$\delta(\overline{w}_i/\overline{w}_n) \neq 0 \qquad i = 1, ..., n-1 \tag{7c}$$

From (7c), if $\alpha_{il} \neq 0$, it follows that $\delta(\overline{w}_i/\overline{w}_n - \alpha_{il}) = 0$ contradiction to (7b), hence

$$\alpha_{il} = 0 \tag{8a}$$

Since $\delta(w) = 1$, then (7b) and (8a) yield $\delta(\overline{w}_i) = n - 1$.
Since i and l are arbitrary , we have just proved that for all i and l, $\quad 1 \leq i, l \leq n-2$,

$$\text{If} \quad b^*_{il} = 0 \quad \Rightarrow \quad \alpha_{il} = 0, \quad w_i^T = (\xi, 0, ..., 0) \quad \xi \in G \quad \xi \neq 0 \tag{9}$$

and only one row of that type $((\delta(\overline{w}_i) = n - 1))$ can exist in $\overline{W}$.
We proved in (6) and (9) that for all $i, l \in \{1, ..., n-2\}$:

$$\alpha_{il} = 0 \Leftrightarrow b^*_{il} = 0, \qquad w_i^T = (\xi_i, 0, ..., 0) \quad \xi_i \neq 0, \quad \xi_i \in G\ . \tag{10}$$

Assume that in (10) $i = l = 1$ then:

$$\alpha_{11} = 0 \quad \Leftrightarrow b^*_{11} = 0, \qquad \delta(\overline{w}_1) = n - 1 \tag{11}$$

What are the values of $\alpha_{1l}, \quad b^*_{1l} \quad l = 2, ..., n-2$?
From (11):

$$\alpha_{1l} \neq 0 \quad \Leftrightarrow b^*_{1l} \neq 0 \quad l = 2, ..., n-2 \tag{12a}$$

For all $l = 2, ..., n-2$ using (12a) if $b^*_{n-1,l} = b^*_{1l}$ then from (2) we get $\overline{w}_1 = \frac{\alpha_{1l} b^*_{n-1,l}}{b^*_{1l}\alpha_{n-1,l}} \overline{w}_{n-1}$ i.e. $\overline{w}_1$ and $\overline{w}_{n-1}$ are linearly dependent, contradiction to the non-singularity of $\overline{W}$. Hence

$$b^*_{n-1,l} \neq b^*_{1l} \quad l = 2, ..., n-2 \tag{12b}$$

From (1b),(1c), (2), (12a),(12b) and using $\delta(w) = 1$ we obtain:

$$\delta(b^*_{n-1,l} w - b^*_{il}(w - \alpha_{n-1,l})) = 0 \tag{12c}$$

From (2) and (12c) we obtain:

$$\delta(\overline{w}_1) = \delta(\overline{w}_{n-1}) = n - 1 \tag{12d}$$

Since $\delta(\overline{w}_{n-1}) = 1$ then from (12d) $n - 1 = 1$ and $n = 2$.

For $n > 2$:

$$\alpha_{1l} = 0 \quad \Leftrightarrow b^*_{1l} = 0 \quad l = 1, ..., n-2, \qquad \delta(\overline{w}_1) = n - 1 \tag{13}$$

and (13) can occur only once in $\overline{W}$.
So if (13) does not occur in $\overline{W}$ then

$$\alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \tag{14a}$$

This proves (i) of the Lemma.
Since $\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-1$ (given) then from (14a) we get:

$$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \tag{14b}$$

For all $i = 1, ..., n-1 \quad l = 1, ..., n-2$ in $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i$ and (14b) we get:

$$\delta(\overline{w}_i) = \delta(S_l) \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \tag{14c}$$

From (1c) and (14c) we get $\delta(\overline{w}_i) = 1 \quad i = 1, ..., n-2$. If (13) does occur then $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-2$ and $\alpha_{1l} = 0, \quad b^*_{1l} = 0, \quad \alpha_{il} \neq 0, \quad b^*_{il} \neq 0, \quad i = 2, ..., n-1 \quad l = 1, ..., n-2.$
□

If we summarize the results of the Lemma VII.1 then from the fact that one row is $\delta(\overline{w}) = 1$ then all the elements of the matrix A are non-zero.

$$\alpha = \left[\begin{array}{c|c} A & \begin{array}{c} \alpha_{1,n-1} \\ \vdots \\ \alpha_{n-1,n-1} \\ 1 \end{array} \end{array}\right] \qquad A = \begin{bmatrix} \alpha_{11} & \cdot & \cdot & \alpha_{1,n-2} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n-1,1} & \cdot & \cdot & \alpha_{n-1,n-2} \\ 1 & \cdot & \cdot & 1 \end{bmatrix}$$

In other words we can derive analytically the structure of the matrix A. Remain to find the values of $\delta(S_{n-1})$, $\alpha_{i,n-1}$ (which is the last column of the matrix α) and $b^*_{i,n-1} \quad i = 1, ..., n-1$. This will be done in Lemmas VII.2-VII.2"' by case analysis.

Lemma VII.2: Under the assumptions of Lemma VII.1 (i) or Lemma VII.1 (ii), if $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} = 0$ then $\alpha_{i,n-1} = 0$, $b^*_{i,n-1} = 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = n-1$.

Proof: Consider $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i \quad i = 1, ..., n-1$. Since $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} = 0$ then we obtain $\overline{w}_{n-1} \times S_{n-1} = 0$. $\delta(\overline{w}_{n-1}) = 1$ hence $\delta(S_{n-1}) = n-1$, $\quad b^*_{i,n-1} = 0$ and $\alpha_{i,n-1} = 0 \quad i = 1, ..., n-2$. □

See example (2a) in section III.

Lemma VII.2': Under the assumptions of Lemma VII.1 (i) or Lemma VII.1 (ii), if $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} \neq 0$ then $\alpha_{i,n-1} = 0$, $b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = 0$.

Proof: Consider $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i \quad i = 1, ..., n-1$. Since $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} \neq 0$ then $\overline{w}_{n-1} \times S_{n-1} = b^*_{n-1,n-1}\overline{w}_{n-1}$, hence $\delta(S_{n-1}) = 0$. If for some i, $1 \leq i \leq n-2$, $\alpha_{i,n-1} \neq 0$ then from $\delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 0$ we get $\delta(S_{n-1}) = \delta(\overline{w}_i) = 1$ contradiction to S_{n-1} being invertible. Therefore , for all i, $1 \leq i \leq n-2$, $\alpha_{i,n-1} = 0$. From $\overline{w}_i \times S_{n-1} = b^*_{i,n-1}\overline{w}_i$ and the fact that $\delta(S_{n-1}) = 0$ we get $b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-2$. □

See example (2c) in section III.

Analysis of the last case, $\alpha_{n-1,n-1} \neq 0$, will be done separately to Lemma VII.1 (i) ($\delta(\overline{w}_i) = 1 \quad i = 1, ..., n-1$) and then to Lemma VII.1 (ii) ($\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1$).

Lemma VII.2": Under the assumptions of Lemma VII.1 (i) , if $\alpha_{n-1,n-1} \neq 0$ then $\alpha_{i,n-1} \neq 0$, $b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-1$ and $\delta(S_{n-1}) = 1$.

Proof: Consider $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i \quad i = 1, ..., n-1$. Since $\alpha_{n-1,n-1} \neq 0$ then $\delta(\overline{w}_{n-1} - \alpha_{n-1,n-1}\overline{w}_n) = 0$. Then $\delta(S_{n-1}) = \delta(\overline{w}_{n-1}) = 1$ and $b^*_{n-1,n-1} \neq 0$. Assume for some i, $1 \leq i \leq n-2$, $\alpha_{i,n-1} = 0$ then from $\delta(S_{n-1}) = 1$, $\quad \delta(\overline{w}_i) = 1$ we get $\delta(\overline{w}_i \times S_{n-1}) = 2$ and if $n > 2$ then $\delta(\overline{w}_i \times S_{n-1}) \neq 0$, contradicts $\delta(\overline{w}_i) = 1$. Hence, $\alpha_{i,n-1} \neq 0 \quad i = 1, ..., n-2$. Therefore $\delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 0 \quad i = 1, ..., n-1$ and we obtain $b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-1$. □

Lemma VII.2"': Under the assumptions of Lemma VII.1 (ii), if $\alpha_{n-1,n-1} \neq 0$ then $\alpha_{i,n-1} \neq 0, \quad b^*_{i,n-1} \neq 0 \quad i = 2, ..., n-1, \quad \alpha_{1,n-1} = 0, \quad b^*_{1,n-1} = 0$ and $\delta(S_{n-1}) = 1$.

Proof: The proof is the same as in Lemma VII.2" for proving $\delta(S_{n-1}) = 1$ and $\alpha_{i,n-1} \quad b^*_{i,n-1} \quad i = 2, ..., n-1$. Let $\alpha_{1,n-1} \neq 0$. Then from $(\overline{w}_1 - \alpha_{1,n-1}\overline{w}_n) \times S_{n-1} = b^*_{1,n-1}\overline{w}_1$ we have $\delta(S_{n-1}) = \delta(\overline{w}_1) = n-1$, contradiction. Hence $\alpha_{1,n-1} = 0$ and from $\overline{w}_1 \times S_{n-1} = b^*_{1,n-1}\overline{w}_1$ we have $b^*_{1,n-1} = 0$. □

The following Corollary, which summarize the previous results, will describe the complete relationship among $\alpha_{il}, \quad \overline{w}_i, \quad b^*_{il}, \quad S_l \quad i, l = 1, ..., n-1$.

Corollary VII.1: If an algorithm is described by Corollary V.1 (iii) ($\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-1 \quad \delta(\overline{w}_{n-1}) = 1$) then the rows of $\overline{W}$ must satisfy one of the following conditions, either

Condition 1: If $\delta(\overline{w}_i) = 1 \quad i = 1, ..., n-1$ and therefore $\alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2, \quad \delta(S_i) = 1 \quad i = 1, ..., n-2$. Then either

- **(1a)** If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} = 0$ then: $\alpha_{i,n-1} = 0, \quad b^*_{i,n-1} = 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = n-1$

  or

- **(1b)** If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} \neq 0$ then: $\alpha_{i,n-1} = 0, \quad b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = 0$

  or

- **(1c)** If $\alpha_{n-1,n-1} \neq 0$ then: $\alpha_{i,n-1} \neq 0, \quad b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-1$ and $\delta(S_{n-1}) = 1$,

or

Condition 2: If $\delta(\overline{w}_1) = n-1$ and $\delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1$ and therefore $\alpha_{1l} = 0, \quad b^*_{1l} = 0 \quad l = 1, ..., n-2 \quad \alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-2, \quad \delta(S_i) = 1 \quad i = 1, ..., n-2$. Then either

- **(2a)** If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} = 0$ then: $\alpha_{i,n-1} = 0, \quad b^*_{i,n-1} = 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = n-1$

  or

- **(2b)** If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} \neq 0$ then: $\alpha_{i,n-1} = 0, \quad b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = 0$

  or

- **(2c)** If $\alpha_{n-1,n-1} \neq 0$ then: $\alpha_{i,n-1} \neq 0, \quad b^*_{i,n-1} \neq 0 \quad i = 2, ..., n-1, \quad \alpha_{1,n-1} = 0, \quad b^*_{1,n-1} = 0$ and $\delta(S_{n-1}) = 1$

In conditions (1) and (2) we assume $\delta(\overline{w}_n) = 0$.

Proof: Summary of Lemma VII.1 and Lemmas VII.2-2"'. $\square$

Corollary VII.1 states that the following sets $\{(1a)\}$, $\{(1b)\}$, $\{(1c)\}$, $\{(2a)\}$, $\{(2b)\}$ and $\{(2c)\}$ separately give complete description of the relations among $\alpha_{il}, b^*_{il}, \overline{w}_i, S_l \quad i,l = 1,...,n-1$. In the rest of this section we are going to answer the following questions: How can the above sets determine the values of $a^*_{il}, V_l \quad i,l = 1,...,n-1$? Do there exist any sets which are equivalent to each other in the sense of section IV ? Is each set described an existing algorithm or a new one ?

At first glance, Corollary VII.1 hints that this may be a source for many non-related algorithms. But after some more analysis we will prove that some of the entries in Corollary VII.1 are equivalent to each other and some are equivalent to previous algorithms and we are about *to get only one new type of algorithm.*

So at first we show that there exists equivalence relations among the conditions of Corollary VII.1. Corollary VII.1 (1a) states that if the algorithm is described by $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ then

$$\alpha = \begin{bmatrix} \alpha_{11} & \cdot & \cdot & \alpha_{1,n-2} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{n-1,1} & \cdot & \cdot & \alpha_{n-1,n-2} & 0 \\ 1 & \cdot & \cdot & 1 & 1 \end{bmatrix}$$

the δ of the first $n-1$ rows of $\overline{W}$ is 1 and the entries of the first $n-2$ columns of α are not zero. This particular structure of α enables us to change two multiplications of $\underline{m}$ (transformation 3 of section IV) and get an equivalent algorithm which is described by Corollary VII.1 (1b) (see examples (2a) and (2c) in Section III). The difference between Corollary VII.1 (1a) and (2a) is that in (2a) we have one row, $\overline{w}_1$, such that $\delta(\overline{w}_1) = n-1$, hence the entries of the first row in α are zero and the rest is the same as Corollary VII.1 (1a). Therefore the same technique we used to analyze Corollary VII.1 (1a) can be used to analyze Corollary VII.1 (2a). The above is described in the next Lemma.

Lemma VII.3: If an algorithm is described by Corollary VII.1 (1a) then it is equivalent to an algorithm which is described by Corollary VII.1 (1b). The same is true for Corollary VII.1 (2a) and (2b).

Proof: Recall Lemma IV.2 ([5]) that $U_{\overline{w}_i} = Ku_it_i^T + \sum_{j=1}^{n-1} \alpha_{ij}Ku_{n+j}t_{n+j}^T$. From Corollary VII.1 since $\delta(\overline{w}_i) = 1 \quad i = 1,...,n-1$ or $\delta(\overline{w}_1) = n-1, \quad \delta(\overline{w}_i) = 1 \quad i = 2,...,n-1$ then $w_{i,n-1} = 0 \quad i = 1,...,n-1$ therefore from the regular matrix representation of $U_{\overline{w}_i}$ (given as (6) in the section II) we get:

$$\underline{0}^T = (U_{\overline{w}_i})_1 = (Ku_i)_1t_i^T + \sum_{j=1}^{n-1} \alpha_{ij}(Ku_{n+j})_1t_{n+j}^T \tag{1}$$

where the subscript 1 means the first row of the matrix. We know that $\alpha_{il} \neq 0 \quad i = 1,...,n-1 \quad l = 1,...,n-2, \quad \{t_n,...,t_{2n-1}\} \quad (j=1)$ are linearly independent (Lemma IV.4 ([5])),

$$K = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot \\ 0 & 1 & & 0 & 0 & 0 \\ 1 & 0 & & 0 & 0 & 0 \end{bmatrix}$$

and from (1) we get:

$$x_{n-1} \notin L_i(\underline{x}) \qquad i = 1,...,n-1 \quad i = n+1,...,2n-2 \tag{2a}$$

i.e. x_{n-1} does not appear in $2n-3$ multiplications. Since $\delta(\overline{w}_n) = 0$ and $u_n = K^{-1}\overline{w}_n$ (Lemma IV.7 (i) ([5])) we get:

$$x_{n-1} \in L_n(\underline{x}) \tag{2b}$$

Since $\alpha_{i,n-1} = 0 \quad i = 1,...,n-1$ (the last column of the matrix α) from Corollary VII.1 (1a) and (2a) we can apply transformation 3 of section IV to get an equivalent algorithm. Choose $a \quad 2 \times 2$ non-singular G-matrix A; then

$$K^{-1}U_{\overline{w}_n} - (u_{n+1}|...|u_{2n-2}) \begin{bmatrix} t_{n+1}^T \\ \cdot \\ \cdot \\ t_{2n-2}^T \end{bmatrix} = (u_n|u_{2n-1})AA^{-1} \begin{bmatrix} t_n^T \\ t_{2n-1}^T \end{bmatrix} \tag{3}$$

Choose $\alpha = 1 + \xi u^{n-1} \quad \xi \in G \quad \xi \neq 0$. α is an invertible element in $G[u]/<u^n>$ where

$$U_\alpha = \begin{bmatrix} 1...0 \\ 01..0 \\ ..... \\ ..... \\ \xi...1 \end{bmatrix}$$

is its regular matrix representation in $G[u]/<u^n>$. Multiply (3) by U_α^T

$$U_\alpha^T K^{-1}U_{\overline{w}_n} - (u_{n+1}|...|u_{2n-2}) \begin{bmatrix} t_{n+1}^T \\ \cdot \\ \cdot \\ t_{2n-2}^T \end{bmatrix} = U_\alpha^T(u_n|u_{2n-1})AA^{-1} \begin{bmatrix} t_n^T \\ t_{2n-1}^T \end{bmatrix} \tag{4}$$

From (2a) and the form of U_α^T it follows that $(u_{n+1}|...|u_{2n-2})$ stays invariant under multiplication by U_α^T.

$$U_\alpha^T K^{-1} = K^{-1}U_\alpha \tag{5}$$

From (4) and (5) it follows:

$$K^{-1}\overline{U}_{\overline{w}_n} = (\overline{u}_n|u_{n+1}...|u_{2n-2}|\overline{u}_{2n-1})\begin{bmatrix} \overline{t}_n^T \\ t_{n+1}^T \\ \cdot \\ \cdot \\ \overline{t}_{2n-1}^T \end{bmatrix} \tag{6}$$

where

$$(\overline{u}_n|\overline{u}_{2n-1}) = U_\alpha^T(u_n|u_{2n-1})A \qquad \begin{bmatrix} \overline{t}_n^T \\ \overline{t}_{2n-1}^T \end{bmatrix} = A^{-1}\begin{bmatrix} t_n^T \\ t_{2n-1}^T \end{bmatrix} \qquad \overline{U}_{\overline{w}_n} = U_\alpha U_{\overline{w}_n}$$

Assume we choose

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad ad - bc = 1 \qquad A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

If $a \neq 0$ and since $x_{n-1} \in L_n(\underline{x})$ it follows:

$$x_0, x_{n-1} \in \overline{L}_n(\underline{x})\ , \quad x_{n-1} \in \overline{L}_{2n-1}(\underline{x}) \quad \overline{L}_n(\underline{x}) = \overline{u}_n^T\underline{x}\ , \quad \overline{L}_{2n-1}(\underline{x}) = \overline{u}_{2n-1}^T\underline{x} \tag{7a}$$

$$y_0, \quad y_{n-1} \in \overline{M}_n(\underline{y}), \quad y_{n-1} \in \overline{M}_{2n-1}(\underline{y}) \quad \overline{M}_n(\underline{y}) = \overline{t}_n^T\underline{y}\ , \quad \overline{M}_{2n-1}(\underline{y}) = \overline{t}_{2n-1}^T\underline{y} \tag{7b}$$

From $Ku_{2n-1} = \overline{w}_n \times S_{n-1}$ (Lemma IV.7 (i) ([5])), $\delta(\overline{w}_n) = 0$ and (7a) we get:

$$\delta(S_{n-1}) = 0 \tag{8}$$

From $(\overline{w}_i - \alpha_{i,n-1}) \times S_{n-1} = b_{i,n-1}^*\overline{w}_i, \quad \alpha_{i,n-1} = 0 \quad i = 1, ..., n-1,$ and (8) we get

$$b_{i,n-1}^* \neq 0 \quad i = 1, ..., n-1\ . \tag{9}$$

(8) and (9) are the same as is described in Corollary VII.1 (1b) and Corollary VII.1 (2b). We will continue to denote $\overline{u}_n, \overline{u}_{2n-1}...$ by $u_n, u_{2n-1}...$ $\square$

Example (2c) in section III demonstrates how transformation 3 is used in Lemma VII.3.

Remark VII.1: Under the assumption of Corollary VII.1 (1b) or under the assumption of Corollary VII.1 (2b) we can assume from the proof of Lemma VII.3 (7b) that $y_{n-1} \in \overline{M}_n(\underline{y})$ and $y_{n-1} \in \overline{M}_{2n-1}(\underline{y})$.

Lemma VII.4: If for some i $\delta(\overline{w}_i) = 1, \quad \alpha_{i1}, ..., \alpha_{i,n-1} \neq 0, \quad \alpha_{i,n-1} = 0$ and $y_{n-1} \in \overline{M}_n(\underline{y})$ and $y_{n-1} \in \overline{M}_{2n-1}(\underline{y})$ then $V_0 = (1, 0, ..., 0), \quad \delta(V_i) = 1 \quad i = 1, ..., n-2, \quad \delta(V_{n-1}) = 0$ and $a_{il}^* \neq 0 \quad l = 1, ..., n-1$.

Proof: Since $y_{n-1} \in M_n(\underline{y})$ then from the structure of K, $Kt_n = \overline{w}_n \times V_0$ (Lemma IV.7' (ii) ([5])) and $\delta(\overline{w}_n) = 0$ we have

$$\delta(V_0) = 0 \tag{1a}$$

From Lemma IV.5, Remark IV.2 (both from [5]) and (1a) we have

$$V_0 = (1, 0, ..., 0). \tag{1b}$$

Since $t_i \neq 0$ then from $a_{i0}Kt_i = \overline{w}_i \times V_0$ (Lemma IV.7' (i) ([5])) and (1a) we have

$$a_{i0} \neq 0. \tag{2}$$

From our assumption $\alpha_{i1}, ..., \alpha_{i,n-1} \neq 0$ then

$$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad \delta(w - \alpha_{n-1,l}) = 0 \quad l = 1, ..., n-2 \tag{3}$$

From $(\overline{w}_i - \alpha_{i,l}\overline{w}_n) \times V_l = a^*_{i,l}\overline{w}_i \times V_0$ (Lemma IV.7' (iii) ([5])), (1a) ,(2) and (3) we get:

$$\delta(V_l) = \delta(\overline{w}_{n-1}) = 1 \quad l = 1, ..., n-2 \tag{4a}$$

From $y_{n-1} \in M_{2n-1}(\underline{y})$, $\quad Kt_{2n-1} = \overline{w}_n \times V_{n-1}$ (Lemma IV.7' (ii) ([5])) we get:

$$\delta(V_{n-1}) = 0. \tag{4b}$$

From $(\overline{w}_i - \alpha_{i,l}\overline{w}_n) \times V_l = a^*_{i,l}\overline{w}_i \times V_0$, (1a),(3)and (4a) we get:

$$a^*_{il} \neq 0 \quad l = 1, ..., n-2$$

Since $\alpha_{i,n-1} = 0$ then from $\overline{w}_i \times V_l = a^*_{i,l}\overline{w}_i \times V_0$ and (4b) we have $a^*_{i,n-1} \neq 0$. □

Corollary VII.2: Under the assumptions of Corollary VII.1 (1b) $V_0 = (1, 0, ..., 0)$, $\delta(V_i) = 1 \quad i = 1, ..., n-2$, $\delta(V_{n-1}) = 0$ and $a^*_{il} \neq 0 \quad i, l = 1, ..., n-1$.

Proof: From Corollary VII.1 (1b) and from Remark VII.1 the conditions of Lemma VII.4 hold for all $i = 1, ..., n-1$. □

Corollary VII.2': Under the assumptions of Corollary VII.1 (2b) $V_0 = (1, 0, ..., 0)$, $\delta(V_i) = 1 \quad i = 1, ..., n-2$, $\delta(V_{n-1}) = 0$, $a^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$, $a_{10} \neq 0$, $a^*_{1l} = 0 \quad l = 1, ..., n-2$ and $a^*_{1,n-1} \neq 0$.

Proof: From Corollary VII.1 (2b) and from Remark VII.1 the conditions of Lemma VII.4 hold for all $i = 2, ..., n-1$. From $a_{10}Kt_1 = \overline{w}_1 \times V_0$ and the fact that $\delta(V_0) = 0$ we have $a_{10} \neq 0$. Since $\alpha_{1,1}, ..., \alpha_{1,n-1} = 0$ and $V_0 = (1, 0, ..., 0)$, $\delta(V_i) = 1 \quad i = 1, ..., n-2$, $\delta(V_{n-1}) = 0$, then from $\overline{w}_1 \times V_l = a^*_{1l}\overline{w}_1 \times V_0$ we obtain $a^*_{1l} = 0 \quad l = 1, ..., n-2$ and $a^*_{1,n-1} \neq 0$. □

We are ready now to derive the algorithms which are based on Corollary VII.1 (1b) and the algorithms which are based on Corollary VII.1 (2b).

The algorithm we state next is described as a lemma and not as a theorem since we are going to give it in a different form later which will be the final version. Therefore, the proof is omitted.

Lemma VII.5: Under the assumptions of Corollary VII.1 (1b), every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$'s and $M_i(\underline{y})$'s are given by:

$$\overline{u}_i = \overline{t}_i = K^{-1}(\overline{w}_{n-1}/(w-\beta_i)) \quad i = 1, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(\overline{w}_{n-1})$$

$$\overline{u}_n = \overline{t}_n = K^{-1}(\overline{w}_n)$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}(\overline{w}_{n-1}/(w-\alpha_{n-1,l})) \quad l = 1, ..., n-2$$

$$\overline{u}_{2n-1} = \overline{t}_{2n-1} = (0, \overline{u}_{n,1}, ..., \overline{u}_{n,n-1})$$

where $\overline{u}_i = (\overline{u}_{i0}, ..., \overline{u}_{i,n-1})$ $i = 1, ..., 2n-1$, $\delta(\overline{w}_n) = 0$, $\delta(\overline{w}_{n-1}) = 1$, $\overline{w}_n$, $\overline{w}_{n-1} \in G[u]/\langle u^n\rangle$, and the set $A = \{\beta_1, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-4$ distinct elements . Conversely, for every $\overline{w}_{n-1}, \overline{w}_n$ $G[u]/\langle u^n\rangle$, $\delta(\overline{w}_{n-1}) = 1$ $\delta(\overline{w}_n) = 0$ and for every set
$A = \{\beta_1, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-4$ distinct elements of G there exists an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$, using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.
The proof is given in [6].
The algorithm presented in Lemma VII.5 is the algorithm which is given by example (2d) in Section III.

By using Corollary VII.1 (2b) we obtain the following Lemma.

Lemma VII.5': Under the assumptions of Corollary VII.1 (2b), every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications is equivalent to the algorithm whose $L_i(\underline{x})$s and $M_i(\underline{y})$s are given by:

$$\overline{u}_1 = \overline{t}_1 = 1$$

$$\overline{u}_i = \overline{t}_i = K^{-1}(\overline{w}_{n-1}/(w-\beta_i)) \qquad i = 2, ..., n-2$$

$$\overline{u}_{n-1} = \overline{t}_{n-1} = K^{-1}(\overline{w}_{n-1})$$

$$\overline{u}_n = \overline{t}_n = K^{-1}(\overline{w}_n)$$

$$\overline{u}_{n+l} = \overline{t}_{n+l} = K^{-1}(\overline{w}_{n-1}/(w-\alpha_{n-1,l})) \qquad l = 1, ..., n-2$$

$$\overline{u}_{2n-1} = \overline{t}_{2n-1} = (0, \overline{u}_{n,1}, ..., \overline{u}_{n,n-1})$$

where $\overline{u}_i = (\overline{u}_{i0}, ..., \overline{u}_{i,n-1})$ $i = 1, ..., 2n-1$ $\delta(\overline{w}_n) = 0$, $\delta(\overline{w}_{n-1}) = 1$, $\overline{w}_n$, $\overline{w}_{n-1} \in G[u]/\langle u^n\rangle$, 1 is the unit vector in $G[u]/\langle u^n\rangle$ and the set $A = \{\beta_2, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ has $2n-5$ distinct elements . Conversely, for every $\overline{w}_{n-1}, \overline{w}_n \in G[u]/\langle u^n\rangle$, $\delta(\overline{w}_{n-1}) = 1$ $\delta(\overline{w}_n) = 0$ and for every set $A = \{\beta_2, ..., \beta_{n-2}, \alpha_{n-1,1}, ..., \alpha_{n-1,n-2}\}$ of $2n-5$ distinct elements of G there exists an algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$, using $2n-1$ multiplications whose $L_i(\underline{x})$s and $M_i(\underline{y})$s $i = 1, ..., 2n-1$ are given by the form in the first half of the theorem.

Proof: If the algorithm is described by Corollary VII.1 (2a) then the proof is the same as Lemma VII.5 for u_i, t_i $i = 2, ..., 2n-1$. For u_1 and t_1 we get from $w_1^T = (\xi, 0, ..., 0)$ $\xi \neq 0$ $\xi \in G$, Lemma IV.7 (iii) ([5]) $(b_{10}Ku_1 = \overline{w}_1)$ and Lemma IV.7' (i) ([5]) $(a_{10}Kt_1 = \overline{w}_1)$ that $\overline{u}_1 = \overline{t}_1 = 1$. $\square$

Summary: Lemma VII.5 classifies all the algorithms which are described by Corollary VII.1 (1b) and Lemma VII.5' classifies all the algorithms which are described Corollary VII.1 (2b). We aim at classifying all the algorithms described by Corollary VII.1 (1a) and Corollary VII.1 (2a). If the algorithm is given by $A(\underline{x})\underline{y} = M\underline{m}$ then by Lemma VII.3 the difference between algorithm described by Corollary VII.1 (1a) and Corollary VII.1 (1b) is in the nth and the $2n-1$th entries of $\underline{m}$. The same is true for Corollary VII.1 (2a) and Corollary VII.1 (2b). Thus u_i and t_i $i = 1, ..., n-1, n+1, ..., 2n-2$ are the same as they appear in Lemmas VII 5-5'. In order to retrieve u_n, u_{2n-1}, t_n and t_{2n-1} we need to know S_0, S_{n-1}, V_0 and V_{n-1}. S_0 and S_{n-1} are given, and V_0 and V_{n-1} we will be derived in Lemma VII.6. By using Lemma VII.5, Lemma VII.5' and Lemma VII.6 we will derive the algorithms which are described in Theorems V.3-3'.

Lemma VII.6: If an algorithm is described by Corollary VII.1 (1a) then: (i) $a_{i0} = 0$ $i = 1, ..., n-1$ (ii) $\delta(V_0) = n-1$ (iii) $\delta(V_{n-1}) = 0$.

Proof: From Corollary VII.1 (1a) we have:

$$\delta(S_l) = 1 \quad l = 1, ..., n-2, \quad \delta(S_0) = 0, \quad \delta(S_{n-1}) = n-1 \tag{1a}$$

$$\delta(\overline{w}_i) = 1 \quad \alpha_{il} \neq 0, \quad \alpha_{i,n-1} = 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2 \tag{1b}$$

From $Ku_{n+l} = \overline{w}_n \times S_l$ (Lemma IV.7 (i) ([5])), $\delta(\overline{w}_n) = 0$ and (1a) we obtain:

$$x_{n-1} \notin L_i(\underline{x}) \quad i = n+1, ..., 2n-1 \tag{2a}$$

From $b_{i0}Ku_i = \overline{w}_i \times S_0$ (Lemma IV.7 (ii) ([5])), (1a) and (1b) we obtain:

$$x_{n-1} \notin L_i(\underline{x}) \quad i = 1, ..., n-1 \tag{2b}$$

(2a) and (2b) yield that for all $i = 1, ..., n-1$ $\{u_i, u_{n+1}, ..., u_{2n-1}\}$ are linearly dependent. Hence, $a_{i0} = 0$ $i = 1, ..., n-1$. This proves (i) of the Lemma. From $U_{\overline{w}_i} = Kt_i u_i^T + \sum_{j=1}^{n-2} \alpha_{ij} K t_{n+j} u_{n+j}^T$ $i =$

$1,...,n-1$ (Corollary IV.1 ([5])), $\alpha_{i,n-1}=0$ ((1b)), $u_i=\sum_{j=1}^{n-1}a_{ij}u_{n+j}$ $i=1,...,n-1$ (Corollary IV.2' ([5])) and $a_{i0}=0$ we obtain:

$$U_{\overline{w}_i}=Kt_i(\sum_{j=1}^{n-1}a_{ij}u_{n+j})^T+\sum_{j=1}^{n-2}\alpha_{ij}Kt_{n+j}u_{n+j}^T \quad i=1,...,n-1 \tag{3a}$$

Multiply (3a) by V_0 using Corollary IV.2" ([5]) then we obtain:

$$\overline{w}_i\times V_0=0 \quad i=1,...,n-1 \tag{3b}$$

From (1b) and (3b) we get that $\delta(V_0)=n-1$. This proves (ii) of the Lemma. From $Ku_{2n-1}=\overline{w}_n\times S_{n-1}$ (Lemma IV.7 (i) ([5])) and (1a) we get $u_{2n-1}=(\xi,0,...,0)$ $\xi\in G$ $\xi\neq 0$. From Corollary IV.2" ([5]) we get $\delta(V_{n-1})=0$. □

Proof of Theorem V.3: In Lemma VII.3 we proved by applying transformation 4 of III that Corollary VII.1 (1a) and (1b) are describing equivalent algorithms. Since the transformation in Lemma VII.3 change only the n-th and the $2n-1$th multiplication then u_i and t_i $i=1,...,n-1,n+1,...,2n-2$ are the same as derived in Lemma VI.5, therefore we have:

$$u_i=K^{-1}(\overline{w}_{n-1}\times S_0/(w-\beta_i)) \qquad t_i=K^{-1}(\overline{w}_{n-1}/(w-\beta_i)) \quad i=1,...,n-2 \tag{1a}$$

$$u_{n-1}=K^{-1}(\overline{w}_{n-1}\times S_0) \qquad t_{n-1}=K^{-1}(\overline{w}_{n-1}) \tag{1b}$$

$$u_n=K^{-1}(\overline{w}_n\times S_0) \qquad t_n=K^{-1}(\overline{w}_n\times V_0) \tag{1c}$$

$$u_{n+l}=K^{-1}(\overline{w}_{n-1}\times S_0/(w-\alpha_{n-1,l})) \qquad t_{n+l}=K^{-1}(\overline{w}_{n-1}/(w-\alpha_{n-1,l})) \quad l=1,...,n-2 \tag{1d}$$

$$u_{2n-1}=K^{-1}(\overline{w}_n\times S_{n-1}) \qquad t_{2n-1}=K^{-1}(\overline{w}_n\times V_{n-1}) \tag{1e}$$

$\overline{w}_{n-1}/\overline{w}_n=w$. We assume here that $\delta(S_0)=0$ but not necessarily $(1,0,...,0)$. Since $\delta(V_{n-1})=0$ (Lemma VI.6 (iii)) then apply Lemma IV.5 ([5]) on V_{n-1} and we get:

$$\overline{w}_n=V_{n-1}=(1,0,...,0) \quad w=\overline{w}_{n-1} \tag{2}$$

Using (2) and the facts that $\delta(S_{n-1})=n-1$ (Corollary VII.1 (1a)) and $\delta(V_0)=n-1$ (Lemma VII.6 (ii)) in (1c) and (1e) completes the proof. By already familiar argument, since $\{\overline{u}_{n+1},...,\overline{u}_{2n-2}\}$ are linearly independent then $\alpha_{n-1,l}$, β_i $i,l=1,...,n-2$ are distinct scalars from the field G. □

To demonstrate this Theorem see example (2a) in section III.

Proof of Theorem V.3': If the algorithm is described by Corollary VII.1 (2a) then we use the same proof as in Theorem V.3 for u_i and $t_i \quad i = 2, ..., 2n-1$. $\quad \overline{w}_1 = (0, ..., 0, 1)$, $\quad \delta(S_0) = 0$, and $b_{10} \neq 0$ then from $b_{10}Ku_1 = \overline{w}_1 \times S_0$ (Lemma IV.7 (iii) ([5])) we get $\overline{u}_1 = 1$. From $t_1 = \sum_{j=0}^{n-1} b_{1j}t_{n+j}$ (Corollary IV.2' ([5])) and $b_{1l} = 0 \quad l = 1, ..., n-1$ (Corollary VII.1 (2a)) then $t_1 = b_{10}t_n$ and since $t_n = 1$ we get $\overline{u}_1 = \overline{t}_1 = 1$. $\quad \square$

Remain to analyze Corollary VII.1 (1c). There the δ of $n-1$ rows of $\overline{W}$ is 1 and all the entries in α are not zero (include the last column). Therefore we can not apply any more transformation 3 of section IV on the algorithm. This situation yields that $\{u_i, u_{n+1}, ..., u_{2n-1}\}$ are linearly dependent, $V_l \quad l = 1, ..., n-1$ are invertible and $\delta(V_0) = n-1$ (Lemma VII.7). We already know that $\delta(S_0) = 0, \quad \delta(S_l) = 1 \quad l = 1, ..., n-1$. The above is sufficient to give a description of the algorithm described in Corollary VII.1 (1c). It is difficult now to see that it is equivalent to another algorithm in the previous chapter. But we prefer to go one step further and transform the algorithm into an equivalent one. There all the rows of $\overline{W}$ are invertible but the algorithm will not be in the form $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$. In order to get back to this form we interchange rows n and $2n-1$ of $\underline{m}$ and columns n of I and $n-1$ of α. Because of this interchange we get that V_0 has been interchanged with with V_{n-1} and the same is true for S_0 and S_{n-1}. This transformation has been described in Lemma VII.8.

The same technique will be used for analyzing Corollary VII.1 (2c).

Lemma VII.7: Under the assumption of Corollary VII.1 (1c) we have that $\{u_i, u_{n+1}, ..., u_{2n-1}\} \quad i = 1, ..., n-1$ are linearly dependent $(a_{i0} = 0 \quad i = 1, ..., n-1)$ $\delta(V_0) = n-1$ and $\delta(V_l) = 0 \quad l = 1, ..., n-1$.

The same is true under the assumption of Corollary VII.1 (2c).

Proof: From Lemma IV.2 ([5]) we have that

$$\underline{0}^T = (U_{\overline{w}_i})_1 = (Ku_i)_1 t_i^T + \sum_{j=1}^{n-1} \alpha_{ij}(Ku_{n+j})_1 t_{n+j}^T \tag{1}$$

$\{t_i, t_{n+1}, ..., t_{2n-1}\} \quad i = 1, ..., n-1$ are linearly independent (Lemma IV.7 (ii) ([5])), then from Corollary VII.1 (1c), $\delta(\overline{w}_i) = 1 \quad \alpha_{i1}, ..., \alpha_{i,n-1} \neq 0 \quad i = 1, ..., n-1$ and (1) we get $x_{n-1} \notin L_i(\underline{x}) \qquad i = 1, ..., n-1, n+1, ..., 2n-1$ which yields that $\{u_i, u_{n+1}, ..., u_{2n-1}\} \quad i = 1, ..., n-1$ are linearly dependent , then:

$$a_{i0} = 0 \quad i = 1, ..., n-1. \tag{2}$$

From (2), Lemma IV.7' (i) ([5]) and $\delta(\overline{w}_i) = 1 \quad i = 1, ..., n-1$ we get

$$\delta(V_0) = n-1. \tag{3}$$

Recall Corollary IV.1([5])

$$U_{\overline{w}_i} = Kt_i u_i^T + \sum_{j=1}^{n-1} \alpha_{ij} Kt_{n+j} u_{n+j}^T \qquad i = 1, ..., n-1 \tag{4}$$

Substitute $u_i = \sum_{j=0}^{n-1} a_{ij} u_{n+j} \quad i = 1, ..., n-1$ in (4) where $a_{i0} = 0$ using $u_{n+j}^T V_l = \delta_{jl} \quad j, l = 0, ..., n-1$ and we get:

$$(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a_{il} Kt_i \quad i, l = 1, ..., n-1 \tag{5}$$

From Corollary VII.1 (1c) and $\delta(\overline{w}_i) = 1 \quad \alpha_{il} \neq 0 \quad i, l = 1, ..., n-1$ we get $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad i, l = 1, ..., n-1$ therefore

$$a_{il} \neq 0 \quad i, l = 1, ..., n-1. \tag{6}$$

From (5) and (6)

$$Kt_i = \frac{1}{a_{il}}(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l \quad i, l = 1, ..., n-1. \tag{7}$$

Corollary VI.2" ([5]) and (3) implies that there must be at least one $V_l \quad l \in \{1, ..., n-1\}$ such that $\delta(V_l) = 0$. Assume $l = n-1$ then

$$\delta(V_{n-1}) = 0. \tag{8}$$

For $i = n-1$ in (7):

$$Kt_{n-1} = \frac{1}{a_{n-1,l}}(\overline{w}_{n-1} - \alpha_{n,1,l}\overline{w}_n) \times V_l = \frac{1}{a_{n-1,n-1}}(\overline{w}_{n-1} - \alpha_{n-1,n-1}\overline{w}_n) \times V_{n-1} \tag{9}$$

$$l = 1, ..., n-2$$

$\alpha_{n-1,l} \neq 0 \quad l = 1, ..., n-1$ (Corollary VII.1 (1c)) then

$$\delta(\overline{w}_{n-1} - \alpha_{n-1,l}\overline{w}_n) = 0 \quad l = 1, ..., n-1 \tag{10}$$

From Corollary VII.1 (1c), (8) and (10) we get $\delta(V_l) = \delta(V_{n-1}) = 0 \quad l = 1, ..., n-2. \qquad \square$

Lemma VII.8: If an algorithm is described by Corollary VII.1 (1c) then it is equivalent to an algorithm where (i) $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n-1$ (ii) $\delta(S_l) = 1 \quad l = 0, ..., n-2, \quad \delta(S_{n-1}) = 0$ (iii) $\delta(V_l) = 0 \quad l = 0, ..., n-2, \quad \delta(V_{n-1}) = n-1$ (iv) $b_{il}^* \neq 0 \quad i, l = 1, ..., n-1$ (v) $a_{i0} \neq 0, \quad a_{i,n-1} = 0 \quad i = 1, ..., n-1, \qquad a_{il}^* \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2$ (vi) $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0, \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 1 \qquad i = 1, ..., n-1 \quad l = 1, ..., n-2$

Proof: Assume the algorithm is described by Corollary VII.1 (1c) is: $WA(\underline{x})\underline{y} = B\underline{m}$ where $B = (I|\alpha)$. Let M be the matrix:

$$M = \begin{bmatrix} 1 & 0 & . & . & 0 & -\alpha_{1,n-1} \\ 0 & 1 & . & . & 0 & -\alpha_{2,n-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & 1 & -\alpha_{n-1,n-1} \\ 0 & 0 & . & . & 0 & 1 \end{bmatrix} \tag{1}$$

Apply M on $WA(\underline{x})\underline{y} = B\underline{m}$ and we get $W'A(\underline{x})\underline{y} = B'\underline{m}'$ where $MW = W'$. In $B' = (I|\alpha')$ columns n and $2n-1$ of B were interchanged and in $\underline{m}'$ rows n and $2n-1$ of $\underline{m}$ were interchanged. $\alpha_{i,n-1} \neq 0 \quad i = 1,...,n-1, \quad \delta(\overline{w}_i) = 1 \quad i = 1,...,n-1$ then $\delta(\overline{w}'_i) = \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 0$ $i = 1,...,n-1$ where $\overline{w}'_i$ is the i -th row of $M\overline{W}$. Continue to denote $W', \quad \underline{m}', \quad \alpha'$ as $W, \quad \underline{m}, \quad \alpha$. Since the rows n and $2n-1$ of $\underline{m}$ were interchanged then from Corollary VII.1 (1c) and (1) we get:

$$\delta(\overline{w}_i) = 0 \quad i = 1,...,n-1, \quad \delta(S_l) = 1 \quad l = 0,...,n-2 \quad \delta(S_{n-1}) = 0. \tag{2}$$

From Lemma VII.7, by interchanging V_0 with V_{n-1} we obtain:

$$\delta(V_l) = 0 \quad l = 0,...,n-2 \quad \delta(V_{n-1}) = n-1. \tag{3}$$

From $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times V_l = a^*_{il}\overline{w}_i \times V_0 \quad i,l = 1,...,n-1$ using (2) and (3) we obtain:

$$\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0 \quad a^*_{il} \neq 0 \quad i = 1,...,n-1 \quad l = 1,...,n-2. \tag{4}$$

From (4) using $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i \times S_0 \quad i,l = 1,...,n-1$ we get $b^*_{il} \neq 0 \quad i = 1,...,n-1 \quad l = 1,...,n-2$. From (2), $\alpha_{i,n-1} \neq 0 \quad i = 1,...,n-1$ using $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times S_{n-1} = b^*_{i,n-1}\overline{w}_i \times S_0 \quad i = 1,...,n-1$ we get

$$\delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 1 \quad b^*_{i,n-1} \neq 0 \quad i = 1,...,n-1, \quad b^*_{il} \neq 0 \quad i,l = 1,...,n-1 \tag{5}$$

and from (3) and (5) using $(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) \times V_{n-1} = a^*_{i,n-1}\overline{w}_i \times V_0 \quad i = 1,...,n-1$ we have $a^*_{i,n-1} = 0 \quad i = 1,...,n-1.$ □

Lemma VII.7 and Lemma VII.8 enable us to show that the algorithm which is described by Corollary VII.1 (1c) is equivalent to the algorithm which have already been described in Theorem V.2.

Corollary VII.3: Every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications which is described by Corollary VII.1 (1c), (i.e. $\delta(\overline{w}_i) = 1 \quad i = 1,...,n-1, \quad \delta(S_{n-1}) = 0, \quad \delta(S_l) = 1 \quad l = 1,...,n-2 \quad (t^T_{n+j}S_l = \delta_{jl} \quad j,l = 0,...,n-1)$, $\alpha_{il} \neq 0$ and $b^*_{il} \neq 0 \quad i,l = 1,...,n-1$) is equivalent to the algorithm that is given by Theorem V.2.

Proof: If the algorithm is described by Corollary VII.1 (1c) then from Lemma IV.7 (v) ([5]), Lemma IV.7' (iii) ([5]), Lemma VI.8 (iv) , (v) and (vi) we get:

$$S_l = b^*_{n-1,l}w \times S_0/(w - \alpha_{n-1,l}) \qquad V_l = a^*_{n-1,l}w \times V_0/(w - \alpha_{n-1,l}) \quad l = 1,...,n-2 \tag{1}$$

where $w = \overline{w}_{n-1}/\overline{w}_n$.

$$\overline{w}_i = \gamma_i \overline{w}_{n-1}/(w-\beta_i) \quad i = 1, ..., n-2 \tag{2}$$

Substitute (1) and (2) in Lemma IV.7 (iii) and (iv) ([5]) and (1) and (2) in Lemma IV.7' (i) (ii) ([5])

$$u_i = \frac{\gamma_i}{b_{i0}} K^{-1}(\overline{w}_{n-1} \times S_0/(w-\beta_i)) \qquad t_i = \frac{\gamma_i}{a_{i0}} K^{-1}(\overline{w}_{n-1} \times V_0/(w-\beta_i)) \quad i = 1, ..., n-2 \tag{3a}$$

$$u_{n-1} = \frac{1}{b_{n-1,0}} K^{-1}(\overline{w}_{n-1} \times S_0) \qquad t_{n-1} = \frac{1}{a_{n-1,0}} K^{-1}(\overline{w}_{n-1} \times V_0) \tag{3b}$$

$$u_n = K^{-1}(\overline{w}_n \times S_0) \quad t_n = K^{-1}(\overline{w}_n \times V_0) = K^{-1}(\overline{w}_{n-1} \times V_0/(w-\alpha_{n-1,0})) \quad \alpha_{n-1,0} = 0 \tag{3c}$$

$$u_{n+l} = b^*_{n-1,l} K^{-1}(\overline{w}_{n-1} \times S_0/(w-\alpha_{n-1,l})) \quad t_{n+l} = a^*_{n-1,l} K^{-1}(\overline{w}_{n-1} \times V_0/(w-\alpha_{n-1,l})) \quad l = 1, ..., n-2 \tag{3d}$$

$$u_{2n-1} = K^{-1}\overline{w}_n \times S_{n-1} \qquad t_{2n-1} = K^{-1}\overline{w}_n \times V_{n-1} \tag{3e}$$

$\delta(V_{n-1}) = n-1$ (Lemma VII.8 (iii)) then from (3e) we get $t_{2n-1} = (\xi, 0, ..., 0)$ $\xi \neq 0$ $\xi \in G$. $\delta(S_{n-1}) = 0$ (Lemma VII.8 (ii)) then we can apply Lemma IV.5 ([5]) not for S_0 but for S_{n-1} therefore:

$$S_{n-1} = (1, 0, ..., 0) \qquad \overline{w}_n^T = (1, 0, ..., 0) \qquad w = \overline{w}_{n-1} \tag{4}$$

Substitute (4) into (3e). As we did in Theorem V.1 ([5]) , make the constants unity. $\delta(\overline{w}_{n-1}) = \delta(V_0) = 0$ then we can get rid of $\overline{w}_{n-1} \times V_0$ in (3a)-(3d) and since $\delta(V_{n-1}) = n-1$ then after getting rid of $\overline{w}_{n-1} \times V_0$ t_{2n-1} still stays $(\xi, 0, ..., 0)$, $\xi \neq 0$, $\xi \in G$. Hence we get the following multiplications:

$$\overline{u}_i = K^{-1}(S_0/(w-\beta_i))\overline{t}_i = K^{-1}(1/(w-\beta_i)) \qquad i = 1, ..., n-2 \tag{6a}$$

$$\overline{u}_{n-1} = K^{-1}(S_0) \qquad \overline{t}_{n-1} = K^{-1}(1) \tag{6b}$$

$$\overline{u}_{n+l} = K^{-1}(S_0/(w-\alpha_{n-1,l})) \qquad \overline{t}_{n+l} = K^{-1}(1/(w-\alpha_{n-1,l})) \quad l = 0, ..., n-2 \tag{6c}$$

$$\overline{u}_{2n-1} = K^{-1}(1) \qquad \overline{t}_{2n-1} = 1 \tag{6d}$$

Apply transformation 6 of section IV, i.e. interchange the roles of $\overline{u}_i$ and $\overline{t}_i$, on (6a)-(6d) and we get an algorithm which is equivalent to the algorithm which has been described in Theorem V.2. $\square$

The algorithm which is presented in Corollary VII.3 is the algorithm which is based on the following identity: $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n = (\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n + x_{n-1}y_0u^{n-1}$. And this algorithm first compute the coefficients of $(\sum_{i=0}^{n-2} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$ using Theorem I.1 and then reduce them modulo u^n. By using tranformation 6 of IV this type of algorithm can be transformed to an algorithm which first computes $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-2} y_i u^i)$ using Theorem I.1 and then reducing them modulo u^n and adding $x_0y_{n-1}u^{n-1}$. For demonstrating this equivalence relationship see example (3b) which is equivalent to (3a) in section III.

Lemma VII.8': If an algorithm is described by Corollary VII.1 (2c) then it is equivalent to an algorithm where

(i) $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n$

(ii) $\delta(S_l) = 1 \quad l = 0, ..., n-2, \quad \delta(S_{n-1}) = 0$

(iii) $\delta(V_l) = 0 \quad l = 0, ..., n-2, \quad \delta(V_{n-1}) = n-1$

(iv) $b_{1l} = 0 \quad l = 0, ..., n-2 \quad b_{1,n-1} \neq 0 \quad b^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-1$

(v) $t_1 = (\xi, 0, ..., 0) \quad \xi \neq 0 \quad \xi \in G, \quad M_1(\underline{y}) = M_{2n-1}(\underline{y})$

(vi) $a_{i0} \neq 0, \quad a_{i,n-1} = 0 \quad i = 1, ..., n-1, \qquad a^*_{il} \neq 0 \quad i = 1, ..., n-1 \quad l = 1, ..., n-2$

(vii) $\delta(\overline{w}_i - \alpha_{il}\overline{w}_n) = 0, \quad \delta(\overline{w}_i - \alpha_{i,n-1}\overline{w}_n) = 1 \qquad i = 2, ..., n-1 \quad l = 1, ..., n-2$

Proof: Assume the algorithm which is described by Corollary VII.1 (2c) is: $WA(\underline{x})\underline{y} = B\underline{m}$ where $B = (I|\alpha)$.

Let M be the matrix:

$$M = \begin{bmatrix} 1 & 0 & . & . & 0 & 0 \\ 0 & 1 & . & . & 0 & -\alpha_{2,n-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & 1 & -\alpha_{n-1,n-1} \\ 0 & 0 & . & . & 0 & 1 \end{bmatrix} \tag{1}$$

Apply M on $WA(\underline{x})\underline{y} = B\underline{m}$ and we get: $W'A(\underline{x})\underline{y} = B'\underline{m}'$ where $MW = W'$. In $B' = (I|\alpha')$ columns n and $2n-1$ of B were interchanged and in $\underline{m}'$ rows n and $2n-1$ of $\underline{m}$ were interchanged. Continue to denote W', $\underline{m}'$, α' as W, $\underline{m}$, α.

(i), (ii), (iii),(vi) and (VI) are derived as in Lemma VII.8.

From Lemma IV.7 (iii) ([5]) $\quad b_{10}Ku_1 = \overline{w}_1 \times S_0, \quad \delta(\overline{w}_1) = n-1$ and $\delta(S_0) = 1$ we get $b_{10} = 0$.

From Lemma IV.7' (i) ([5]) $\quad a_{10}kt_1 = \overline{w}_1 \times V_0, \quad \delta(\overline{w}_1) = n-1$ and $\delta(V_0) = 0$ we get $a_{10} \neq 0$.

$\delta(S_l) = 1 \quad l = 0, ..., n-2, \quad b_{10} = 0,$ and $t_1 = \sum_{l=1}^{n-1} b_{1l}t_{n+l}$ (Corollary IV.2' ([5])) then $t_1 S_l = 0 \quad l = 0, ..., n-2$. Therefore $b_{1l} = 0 \quad l = 1, ..., n-2$. $\quad \delta(S_{n-1}) = 0$ i.e $S_{n-1,0} \neq 0$, $t_1 = (\xi, 0, ..., 0) \quad \xi \in G \quad \xi \neq 0$ therefore $t_1 S_{n-1} = b_{1,n-1} \neq 0$. Then $t_1 = b_{1,n-1}t_{2n-1}$, i.e. $M_1(\underline{y}) = b_{1,n-1}M_{2n-1}(\underline{y})$. We can assume $b_{1,n-1} = 1$. $\square$

Corollary VII.3': Every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications, which is described by Corollary VII.1 (2c), (i.e. $\delta(\overline{w}_1) = n-1, \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1, \quad \delta(S_{n-1}) = 0, \quad \delta(S_l) = 1 \quad l = 1, ..., n-2 \quad (t_{n+j}^T S_l = \delta_{jl} \quad j, l = 0, ..., n-1)$, $\alpha_{il} \neq 0, \quad b_{il}^* \neq 0, \quad \alpha_{i,n-1} \neq 0, \quad b_{i,n-1}^* \neq 0, \quad i = 2, ..., n-1 \quad l = 1, ..., n-2$ and $\alpha_{1l}, b_{1l}^* = 0 \quad l = 1, ..., n-1$), is equivalent to the algorithm that is given by Theorem V.2'.

Proof: If the algorithm is described by Corollary VII.1 (2c) then by Lemma VII.8' we get that u_i and $t_i \quad i = 2, ..., 2n-1$ are the same as in Corollary VII.3.

From substituting $\alpha_{1,l} = 0 \quad l = 1, ..., n-1$ (Corollary VII.1 (2c)) and $b_{1,l} = 0 \quad l = 1, ..., n-2 \quad b_{1,n-1} \neq 0$ (Lemma VII.8' (iv)) into $U_{\overline{w}_1} = K u_1 t_1^T + \sum_{j=1}^{n-1} \alpha_{1j} K u_{n+j} t_{n+j}^T$ (Lemma IV.2 ([5])) we have that

$$U_{\overline{w}_1} = K u_1 t_1^T. \tag{1}$$

Multiply (1) by $S_{n-1} \quad (\delta(S_{n-1}) = 0)$ Lemma VII.8' (ii) then

$$\overline{w}_1 \times S_{n-1} = b_{1,n-1} K u_1. \tag{2}$$

$\delta(\overline{w}_1) = n-1$ then from (2) we get $u_1 = (\xi, 0, ..., 0) \quad \xi \neq 0 \quad \xi \in G$ and from Lemma VII.8' (v) $t_1 = (1, 0, ..., 0)$. Hence the multiplications have the following form:

$$\overline{u}_1 = \overline{t}_1 = 1$$

$$\overline{u}_i = K^{-1}(S_0/(w - \beta_i)) \quad \overline{t}_i = K^{-1}(1/(w - \beta_i)) \quad i = 2, ..., n-2$$

$$\overline{u}_{n-1} = K^{-1}(S_0) \qquad \overline{t}_{n-1} = K^{-1}(1)$$

$$\overline{u}_{n+l} = K^{-1}(S_0/(w - \alpha_{n-1,l})) \quad \overline{t}_{n+l} = K^{-1}(1/(w - \alpha_{n-1,l})) \quad l = 0, ..., n-2$$

$$\overline{u}_{2n-1} = K^{-1}(1) \qquad \overline{t}_{2n-1} = 1$$

Apply transformation 6 of IV, i.e. interchange the roles of $\overline{u}_i$ and $\overline{t}_i$ and we get an algorithm which is equivalent to the algorithm which has been described in Theorem V.2'. □

Remark VII.1: In Lemma VII.8'(v) we have $M_1(\underline{y}) = M_{2n-1}(\underline{y})$, hence we can derive an equivalent algorithm by using transformation 4 of IV. We will utilize this fact later on to show that a potential candidate for a new algorithm is in fact equivalent to an exising one.

We completed the derivation of all the algorithms described by Condition 1 and 2 of Corollary VII.1.

VIII. No new algorithm or Analysis of Corollary V.1 (iv)

Corollary V.1 (iv) states that the matrix $\overline{W}$ has the following structure: $\delta(\overline{w}_1)=0, \quad \delta(\overline{w}_i)>0 \quad i=2,...,n-2, \quad \delta(\overline{w}_{n-1})=1$ and $\delta(\overline{w}_n)=0$. We will see that no new algorithm will be generated by Corollary V.1 (iv). By a series of transformations we will prove that all the algorithms appearing in this section are equivalent to the algorithnms which have already been previously discovered in sections VI-VII.

As usual, we will start with analyzing the structure of the matrix $\overline{W}$ and the values of $\alpha_{i,l}, \quad b^*_{i,l}, \quad S_l \quad i,l=1,...,n-1$.

Lemma VIII.1: It is impossible to have $\overline{W}$ such that $\delta(\overline{w}_1)=0, \quad \delta(\overline{w}_2)=n-1, \quad \delta(\overline{w}_i)>0 \quad i=3,...,n-2, \quad \delta(\overline{w}_{n-1})=1, \quad \delta(\overline{w}_n)=0$.

Proof: Assume there is an algorithm whose $\overline{W}$ has the following structure: $\delta(\overline{w}_1)=0, \quad \delta(\overline{w}_2)=n-1, \quad \delta(\overline{w}_i)>0 \quad i=3,...,n-2, \quad \delta(\overline{w}_{n-1})=1$. From $\delta(\overline{w}_{n-1})=1$ it follows that at least $n-2$ terms of $\alpha_{n-1,1},...,\alpha_{n-1,n-1}\neq 0$ and by Remark IV.6 ([5]) we can assume

$$\alpha_{n-1,1},...,\alpha_{n-1,n-2}\neq 0 \quad \delta(\overline{w}_{n-1}-\alpha_{n-1,l}\overline{w}_n)=\delta(w-\alpha_{n-1,l})=0 \quad l=1,...,n-2 \tag{1a}$$

where $w=\overline{w}_{n-1}/\overline{w}_n$. From $(\overline{w}_{n-1}-\alpha_{n-1,1}\overline{w}_n)\times S_1=b^*_{n-1,1}\overline{w}_{n-1}$ and (1a) we have

$$\delta(S_1)=\delta(\overline{w}_{n-1})=1 \tag{1b}$$

Since $\delta(\overline{w}_1)=0$ then we obtain from Lemma IV.6 ([5]) that at least n multiplications are needed to compute $w_1^T A(\underline{x})\underline{y}$ therefore

$$\alpha_{11},...,\alpha_{1,n-1}\neq 0. \tag{2a}$$

From $(\overline{w}_1-\alpha_{11}\overline{w}_n)\times S_1=b^*_{11}\overline{w}_1$, (1b) and (2a) we obtain:

$$b^*_{11}=0 \quad \delta(\overline{w}_1-\alpha_{11}\overline{w}_n)=n-1 \tag{2b}$$

Let $B=\{\overline{w}_1-\alpha_{11}\overline{w}_n, \quad \overline{w}_2, \quad \overline{w}_3,...,\overline{w}_n\}$. B is base for $G[u]/\langle u^n\rangle$ that by Lemma V.1 contradicts the assumption $\delta(\overline{w}_2)=n-1$ and (2b). $\square$

Lemma VIII.2: If $\delta(\overline{w}_1)=0, \quad \delta(\overline{w}_i)>0 \quad i=2,...,n-2, \quad \delta(\overline{w}_{n-1})=1, \quad \delta(\overline{w}_n)=0$ then: $\alpha_{1l}\neq 0 \quad l=1,...,n-1, \quad b^*_{1l}=0 \quad l=1,...,n-2 \qquad \delta(\overline{w}_i)=1, \quad \alpha_{il}, \quad b^*_{il}\neq 0, \quad \delta(\overline{w}_1-\alpha_{1l}\overline{w}_n)=n-1, \quad i=2,...,n-1 \quad l=1,...,n-2 \qquad \delta(S_i)=1 \quad i=1,...,n-2$

Proof: Apply the same proof as in Lemma VII.1 for $i=2,...,n-1$ and we obtain: $\delta(\overline{w}_i)=1, \quad \alpha_{il}, \quad b^*_{il}\neq 0 \quad \delta(S_l)=1 \quad i=2,...,n-1 \quad l=1,...,n-2$. $\delta(\overline{w}_1)=0$ then $\alpha_{11},...,\alpha_{1,n-1}\neq 0$ (Lemma IV.6 ([5])), then from $(\overline{w}_1-\alpha_{1l}\overline{w}_n)\times S_l=b^*_{1l}\overline{w}_1$ and from $\delta(\overline{w}_1)=0, \quad \delta(S_l)=1 \quad l=1,...,n-2$ we get $b^*_{1l}=0$ and $\delta(\overline{w}_1-\alpha_{1l}\overline{w}_n)=n-1 \quad l=1,...,n-2$. $\square$

The values of $\alpha_{i,n-1}, \quad b^*_{i,n-1}$ and $\delta(S_{n-1}) \quad i=2,...,n-1$ are the result of case analysis as it was carried out in Lemmas VII.2-VII.2"'. We are not repeating this identical procedure but we will suumarize it in the following corollary.

Corollary VIII.1: If an algorithm is described by Corollary V.1 (iv) (i.e. $\delta(\overline{w}_1) = 0, \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1, \quad \delta(\overline{w}_n) = 0$) and therefore $\alpha_{1l} \neq 0 \quad l = 1, ..., n-1, b^*_{1l} = 0 \quad l = 1, ..., n-2$ $\alpha_{il}, \quad b^*_{il} \neq 0 \quad i = 2, ..., n-1 \quad l = 1, ..., n-2, \quad \delta(S_i) = 1 \quad i = 1, ..., n-2.$
Then either

(1a) If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} = 0$ then $\alpha_{i,n-1} = 0 \quad i = 2, ..., n-2, \qquad b^*_{i,n-1} = 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = n-1$

or

(1b) If $\alpha_{n-1,n-1} = 0$ and $b^*_{n-1,n-1} \neq 0$ then $\alpha_{i,n-1} = 0 \quad i = 2, ..., n-1, \quad b^*_{i,n-1} \neq 0 \quad i = 1, ..., n-2$ and $\delta(S_{n-1}) = 0$

or

(1c) If $\alpha_{n-1,n-1} \neq 0$ then $\alpha_{i,n-1} \neq 0, \quad b^*_{i,n-1} \neq 0 \quad i = 2, ..., n-1, \quad b^*_{1,n-1} = 0$ and $\delta(S_{n-1}) = 1$.

The difference between Corollary VII.1 Condition 1, 2 and Corollary VIII.1 is that here we have one extra invertible row, $\overline{w}_1$, and $\delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1$. Thus $\alpha_{1,1}, ..., \alpha_{1,n-1} \neq 0$ and we can not use transformation 3 of IV but we will see that $\alpha_{1,1} = \cdots = \alpha_{1,n-1}$. Hence we can get an equivalent algorithm where the entries of the first row of α are all zero, $M_1(\underline{y}) = M_n(\underline{y})$ and $\delta(\overline{w}_1) = n-1$. From $M_1(\underline{y}) = M_n(\underline{y})$ it follows that we can apply transformation 4 of IV on the new algorithm. Then we get that the new algorithm is the one which already have been introduced in Corollary VII.1 (2a). Therefore, an algorithm which is descirbed by Corollary VIII.1 (1a) can be reduced to an algorithm that is decribed by Corollary VII.1 (2a) and therefore it is equivalent to an algorithm described by Corollary VII.1 (2b) (Lemma VII.3). Algorithm that is based on Corollary VII.1 (2a) is equivalent to the algorithm which have been described in Theorem V.3'.

The above results were taken from the following lemma:

Lemma VIII.3: Every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications which is described by Corollary VIII.1 (1a), (i.e. $\delta(\overline{w}_1) = 0, \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1, \quad \delta(S_0) = 0, \quad \delta(S_l) = 1 \quad l = 1, ..., n-2 \quad \delta(S_{n-1}) = n-1 \quad t^T_{n+j} S_l = \delta_{jl} \quad j, l = 0, ..., n-1$), is equivalent to the algorithm that is given by Theorem V.3'.

Proof: Since Theorem V.3' is based on Corollary VII.1 (2a) then we will prove that if an algorithm is described by Corollary VIII.1 (1a) then it is equivalent to an algorithm that is described by Corollary VIII.1 (2a).

From $\delta(\overline{w}_1) = 0$ and $(\overline{w}_i - \alpha_{il}\overline{w}_n) \times S_l = b^*_{il}\overline{w}_i, \quad \delta(S_l) = 1 \quad l = 1, ..., n-2$ (Corollary VIII.1 (1a)) we get for $i = 1$

$$\delta(\overline{w}_1 - \alpha_{1l}\overline{w}_n) = n-1 \quad l = 1, ..., n-2 \tag{1a}$$

$b^*_{1,n-1} = 0$ and $\delta(S_{n-1}) = n-1$ then from $(\overline{w}_1 - \alpha_{1,n-1}\overline{w}_n) \times S_{n-1} = b^*_{1,n-1}\overline{w}_1$

$$\delta(\overline{w}_1 - \alpha_{1,n-1}\overline{w}_n) \geq 1 \tag{1b}$$

Assume that $1 \leq \delta(\overline{w}_1 - \alpha_{1,n-1}\overline{w}_n) < n-1$ then from (1a) and (1b) we get $\delta(\overline{w}_n) \neq 0$ contradiction , therefore:

$$\delta(\overline{w}_1 - \alpha_{1,n-1}\overline{w}_n) = n-1 \tag{1c}$$

Then from (1a) and (1c) we get:

$$\alpha_{11} = \alpha_{12} = \ldots = \alpha_{1,n-1} = \theta \tag{2}$$

Multiply $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ by

$$M = \begin{bmatrix} 1 & . & . & . & -\theta \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & . & . & . & 1 \end{bmatrix}$$

then $w_1 A(\underline{x})\underline{y} = m_1 - \theta m_n$ where w_1 is the first row in MW. $\quad b^*_{1l} = 0 \quad l = 1, \ldots, n-1$ (Corollary VIII.1 (1a)) then from $t_1 = \sum_{l=0}^{n-1} b_{1l} t_{n+l}$ (Corollary IV.2' ([5])) we get (assume $b_{10} = 1$)

$$M_1(\underline{y}) = M_n(\underline{y}) \tag{3}$$

Apply on (3) transformation 4 of IV and we get an equivalent algorithm where

$$m_1 = (L_1(\underline{x}) - \theta L_n(\underline{x}))M_1(\underline{y}) \tag{4a}$$

and from (1a),(1c) (2)

$$w_1 = (\xi, 0, \ldots, 0) \quad \xi \neq 0 \quad \xi \in G. \tag{4b}$$

From (2),(4a) and (4b) we have

$$\alpha_{1,l} = 0 \quad l = 1, \ldots, n-1 \tag{4c}$$

The new equivalent algorithm, which is described by $\overline{w}_i \quad \alpha_{il}$ and $b^*_{il} \quad i, l = 1, \ldots, n-1$, where $\overline{w}_i \quad i = 2, \ldots, n$ and $\overline{w}_1$ are described in (4b), is exactly the one that have been described in Corollary VII.1 (2a) therefore it is equivalent to Corollary VII.1 (2b). $\square$

Lemma VIII.3 implies that in order to construct an algorithm that is described by Corollary VIII.1 (1a) it can be done in two steps:

1. Construct the algorithm as in Theorem V.3'.

2. Since in Theorem V.3' $M_1(\underline{y}) = M_n(\underline{y})$ then by linear combination of $L_1(\underline{x})$ and $L_n(\underline{x})$ we get the algorithm that is described by Corollary VIII.1 (1a).

Remain to examine Corollary VIII.1 (3c). Here all the entries of the matrix α are not equal to zero, $\delta(\overline{w}_1) = 0, \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1$. We get, as before, that all the entries of the first row of the matrix α are equal to each other. Hence we can get an equivalent algorithm $WA(\underline{x}) = (I|\alpha)\underline{m}$ with the following properties: $\delta(\overline{w}_1) = n-1$, all the entries in the first row of the matrix α are zero and $M_1(\underline{y}) = M_n(\underline{y})$. This is the algorithm which have already been described by Corollary VII.1 (2c). Therefore, we can apply Lemma VII.8' and get $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n$, interchange entries n and $2n-1$ of $\underline{m}$ then $M_1(\underline{y}) = M_{2n-1}(\underline{y})$. By Corollary VII.3', algorithm that is based on Corollary VII.1 (2c) is equivalent to the algorithm which is defined in Theorem V.2' . In Theorem V.2' $L_1(\underline{x}) = L_{2n-1}(\underline{x})$. Thus we can apply transformation 4 of IV and we will get an equivalent algorithm to the algorithm that is described by Corollary VIII.1 (1c).

Lemma VIII.4: Every algorithm A for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod u^n$ in $2n-1$ multiplications which is described by Corollary VIII.1 (1c), (i.e. $\delta(\overline{w}_1) = 0, \quad \delta(\overline{w}_i) = 1 \quad i = 2, ..., n-1, \quad \delta(S_0) = 0, \quad \delta(S_l) = 1 \quad l = 1, ..., n-1 \quad t_{n+j}^T S_l = \delta_{jl} \quad j, l = 0, ..., n-1$), is equivalent to the algorithm that is given by Theorem V.2'.

Proof: We will prove that if an algorithm is described by Corollary VIII.1 (1c) then it is equivalent to an algorithm that is described by Corollary VII.1 (2c). And since Theorem V.2' is based on Corollary VII.10 (2c) it will proves the Lemma.
From Corollary VIII.1 (1c)

$$\delta(S_l) = 1 \quad l = 1, ..., n-1 \quad \delta(S_0) = 0 \tag{1}$$

and since $\delta(\overline{w}_1) = 0$ then

$$\alpha_{11}, ..., \alpha_{1,n-1} \neq 0. \tag{2}$$

From $(\overline{w}_1 - \alpha_{1l}\overline{w}_n) \times S_l = b_{1l}^*\overline{w}_1$, (1) and (2)

$$b_{1l}^* = 0 \quad l = 1, ..., n-1 \tag{3}$$

From (1) and (3) using $(\overline{w}_1 - \alpha_{1l}\overline{w}_n) \times S_l = b_{1l}^*\overline{w}_1$,

$$\delta(\overline{w}_1 - \alpha_{1l}\overline{w}_n) = n-1 \quad l = 1, ..., n-1 \tag{4}$$

From (4)

$$\alpha_{11} = \cdots = \alpha_{1,n-1} = \theta \tag{5}$$

Since $b_{10} \neq 0$ then from (3) using $t_1 = \sum_{j=0}^{n-1} b_{1j}t_{n+j}$ (Corollary IV.2' ([5])) we get:

$$M_1(\underline{y}) = M_n(\underline{y}) \quad (b_{10} = 1) \tag{6}$$

Multiply $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ by

$$M = \begin{bmatrix} 1 & . & . & . & -\theta \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & . & . & . & 1 \end{bmatrix}$$

and from (5) we get:

$$w_1 A(\underline{x})\underline{y} = m_1 - \theta m_n. \tag{7}$$

where w_1 is the first row in MW. By transformation 4 of IV using (4),(6) and (7) we get an equivalent algorithm where:

$$w_1 = (\xi, 0, ..., 0) \quad \xi \neq 0 \quad \xi \in G \quad \alpha_{1l} = 0 \quad b^*_{1l} = 0 \quad l = 1, ..., n-1 \tag{8}$$

From (8) we get that the algorithm described by Corollary VIII.1 (1c) is equivalent to an algorithm described by Corollary VII.1 (2c). □

Lemma VIII.4 implies that in order to construct an algorithms that is described by Corollary VIII.1 (1c) we have to do it in two steps:

1. Construct the algorithm as in Theorem V.2'.
2. Since in Theorem V.2' $L_1(\underline{x}) = L_{2n-1}(\underline{x})$ then by linear combination of $M_1(\underline{y})$ and $M_{2n-1}(\underline{y})$ we get the algorithm that is equivalent to the algorithm that is described by Corollary VIII.1 (1c).

Or we can construct the algorithm that is described by Corollary VIII.1 (1c) differently:

1. Construct the algorithm as in Theorem V.2'.
2. By transformation 6 of IV, for all $i = 1, ..., 2n-1$, interchange the roles of $\overline{u}_i$ and $\overline{t}_i$.
3. Here $M_1(\underline{y}) = M_{2n-1}(\underline{y})$ then by linear combination of $L_1(\underline{x})$ and $L_{2n-1}(\underline{x})$ we get the algorithm that is equivalent to the algorithm that is described by Corollary VIII.1 (1c).

Summary

Our main starting point was Corollary V.1; There we proved that if the algorithm is given by $WA(\underline{x})\underline{y} = (I|\alpha)\underline{m}$ then the rows of W must satisfy one of the following conditions:

(i) $\delta(\overline{w}_i) = 0 \quad i = 1, ..., n.$

From (i) we derived the algorithms which are described in Theorems V.1 and V.2.

or

(ii) $\delta(\overline{w}_1) = n-1 \quad \delta(\overline{w}_i) = 0 \quad i = 2, ..., n.$

From (ii) we derived the algorithms which are described in Theorems V.1' and V.2'.

or

(iii) $\delta(\overline{w}_i) > 0 \quad i = 1, ..., n-2, \quad \delta(\overline{w}_{n-1}) = 1 \quad \delta(\overline{w}_n) = 0.$

From (iii) we derived the algorithms which are described in Theorems V.3 and V.3'.

or

(iv) $\delta(\overline{w}_1) = 0, \quad \delta(\overline{w}_i) > 0 \quad i = 2, ..., n-2, \quad \delta(\overline{w}_{n-1}) = 1 \quad \delta(\overline{w}_n) = 0.$

From (iv) we do not get any new algorithms but only these that are equivalent to Theorems V.2' of (ii) and to Theorem V.3' of (iii).

Conclusion

If we combine together the results of this paper and the previous ones ([1],[5]) we see that basically every bilinear algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod Q(u)^l$ where $Q(u)$ is irreducible (over G) $\deg Q(u) \geq 1$ is equivalent to an algorithm that is based on computing the coeffcients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i)$, hence it necessitates large coefficients. Therefore, future study of sub-minimal algorithms should be considered. In addition, we conjecture that as in the case of [3] and [4] every minimal algorithm for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod Q(u)^l$ where $Q(u)$ is irreducible (over G), $l > 1, \quad \deg Q(u) > 1$ is bilinear. While for the algorithm in this paper where $l > 1$ and $\deg Q(u) = 1$ we can not claim the validty of the above conjecture since we have the following example which shows a minimal quadratic algorithm for computing the coefficients of $(\sum_{i=0}^{2} x_i u^i)(\sum_{i=0}^{2} y_i u^i) \bmod u^3$.

$$\begin{bmatrix} x_0 & 0 & \\ x_1 & x_0 & 0 \\ x_2 & x_1 & x_0 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} x_0 y_0 \\ (x_0 + x_1)(y_0 + y_1) \\ x_1 y_1 \\ (x_0 + y_0)(x_2 + y_2) \\ (-x_0 + y_0)(x_2 - y_2) \end{bmatrix}$$

The problem of classifying all the minimal algorithms for computing the coefficients of $(\sum_{i=0}^{n-1} x_i u^i)(\sum_{i=0}^{n-1} y_i u^i) \bmod Q(u)^l$ where $Q(u)$ is irreducible (over G) $l > 1$ is still open.

References

1. S. Winograd, "On multiplication in algebraic extension fields", *Theoret. Comput. Sci., 8 (1979), pp. 359-377.*

2. S. Winograd, "Some linear forms whose multiplicative complexity depends on the field of constants". *Math. Syst. Theory, Vol 10 (1977), pp. 169-180.*

3. E. Feig, "On systems of bilinear forms whose minimal division-free algorithms are all bilinear", *J. of Algorithms 2, 261-281 (1981).*

4. E. Feig, "Certain systems of bilinear forms whose minimal algorithms are all quadratic", *J. of Algorithms 4, 137-149 (1983).*

5. A. Averbuch, Z. Galil, S. Winograd,"Classification of all the minimal bilinear algorithms for computing the coefficients of the product of two polynomials modulo a polynomial, Part I: The algebra $G[u]/\langle Q(u)^l \rangle \quad l > 1$", *Theoret. Comput. Sci., vol. 58, no 1-3 (1988), pp. 17-56.*

6. A. Averbuch, Z. Galil, S. Winograd,"Classification of all the minimal bilinear algorithms for computing the coefficients of the product of two polynomials modulo a polynomial, Part II: The algebra $G[u]/\langle u^n \rangle$", *Technical Report 82/87, Dept. of Computer Science, Tel-Aviv University, 1987.*

7. H.F. de Groote, "On varieties of optimal algorithms for the computation of bilinear mappings. I. The isotropy group of bilinear mapping", *Theoret. Comput. Sci., 7 (1978), pp. 1-24.*

8. H.F. de Groote, "On varieties of optimal algorithms for the computation of bilinear mappings. II. Optimal algorithms for 2×2 matrix multiplication", *Theoret. Comput. Sci., 7 (1978), pp. 124-148.*

9. H.F. de Groote, "On varieties of optimal algorithms for the computation of bilinear mappings. III. Optimal algorithms for the computation of xy and yx where $x, y \in M_2(K)$", *Theoret. Comput. Sci., 7 (1978), pp. 239-249.*