Theoretical Computer Science 19 (1982) 39–67
North-Holland Publishing Company

ADDITIVE COMPLEXITY IN DIRECTED COMPUTATIONS

D.Yu. GRIGOR'EV

Leningrad Branch of Mathematical V.A. Steklov Institute of Academy of Sciences of the USSR, Leningrad, 191011, U.S.S.R.

Communicated by A. Ershov

Abstract. A straight-line additive computation which computes a set $\mathscr{A}$ of linear forms can be presented as a product of elementary matrices (one instruction of such a computation corresponds to a multiplication by an elementary matrix). For the general complexity measure no methods for obtaining nonlinear lower bounds for concrete natural sets of linear forms are known at the moment (under the general complexity measure of $\mathscr{A}$ we mean the minimal number of multipliers in products computing $\mathscr{A}$). In the paper three complexity measures (triangular, directed and a modification of the latter—reduced directed complexity) close in spirit each to others are defined and investigated. For these measures some nonlinear lower bounds are obtained. Moreover, the problem of the exact explicit calculation of the directed complexity is solved for which a suitable algebraic apparatus (the generalized Bruhat decomposition) is developed. Apparatus is exposed in the appendix to the paper.

1. Introduction and basic notions

Development of methods for obtaining nonlinear lower bounds in the algebraic computational complexity still remains an unsolved problem for the present. In the paper two models of computation (triangular and directed) are introduced, and nonlinear lower bounds of complexity are obtained for these models. Connections of the general model with the models under consideration are also discussed. There may be some independent interest in the technique of obtaining lower bounds of complexity in the considered restricted models bearing in mind the approach of obtaining lower bounds of complexity in the general model.

In the paper the complexity of computing of a set of linear forms by an additive straight-line computation is investigated. Additive computation (or simply computation—other kinds of computations are not considered in the paper) is defined as usual with some modifications, convenient for our aims, in the following way:

(1) a set of input variables $x_1, \ldots, x_n$ is fixed;

(2) there are registers $y_1, \ldots, y_N$, among which the registers $y_{i_1}, \ldots, y_{i_n}$ are distinguished;

(3) at the initial moment the value of a register y_{i_j} $(1 \leq j \leq n)$ is equal to x_j, the value of any other register is equal to zero;

0304-3975/82/0000–0000/$02.75 © 1982 North-Holland

(4) the computation itself is a sequence of instructions of the form

$$y_k := \alpha y_i + \beta y_j \quad (1 \leq i, j, k \leq N)$$

where $\alpha, \beta \in F$ and F is some field fixed henceforth;

(5) the result of the computation is the set of n linear forms that are the values of the registers $y_{i_1}, \ldots, y_{i_n}$ at the end of computing (the value of a register at any moment is defined by the natural induction).

The last condition (5) being not a serious restriction for the general complexity measure (charging to any instruction from (4) the unity weight), is very essential for the aims of the present paper. If some complexity measure of an additive computation is fixed then, as usually, the complexity of a set of n linear forms over n variables is defined as the minimal complexity of additive computations computing this set of linear forms.

Additive computations were researched earlier in a more common manner in [2, 4, 7, 11], for instance. It would be fair to admit that additive computations were investigated far less than, for example, bilinear programs, although the difficulties in obtaining lower bounds are the same for the former, and on the other hand the additive computations are more clear and treating them is more simple than for many other models of computation.

It is assumed in [2] and [4] that F is the field of real or complex numbers and that the coefficients of an instruction (see (4) above) satisfy the inequalities $|\alpha| \leq 1, |\beta| \leq 1$. Under this assumption on computations it is not difficult to produce an example of a set of linear forms with the coefficients ± 1 with nonlinear complexity (in [4] the nonlinearity of complexity is proved for the matrix of Fourier transform—its coefficients are the roots of unity). Let us write these forms as the rows of some square matrix. Namely, set $A_1 = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$, further define by induction

$$A_{n+1} = \begin{pmatrix} A_n & A_n \\ -A_n & A_n \end{pmatrix}.$$

Then $\det A_{n+1} = \det(2A_n^2) = 2^{2^n}(\det A_n)^2$ so $\det A_n = 2^{n \cdot 2^{n-1}}$. [4] and the last equality entail, under the assumption $|\alpha| \leq 1$, $|\beta| \leq 1$, that the complexity of the set of forms, defined as rows of the matrice A_n, is not less than $\log_2 |\det A_n| = n \cdot 2^{n-1}$.

It is convenient to change the instructions from (4) by the instructions of the following kind which we call elementary:

$$y_i := y_i + \alpha y_j \quad (i \neq j) \quad \text{and} \quad y_i := \alpha y_j \qquad \text{where } \alpha \in F$$

(the transfer to the elementary instructions, as will be shown further, increases the estimates of complexity no more than triple and on the other hand creates some technical advantages). Namely, instead of one instruction from (4), consider the following sequence of the elementary instructions:

(a) $y_k := 0 \cdot y_k$

$y_k := y_k + \alpha y_i$ if $i \neq k, j \neq k$;

$y_k := y_k + \beta y_j$

(b) $y_k := \alpha y_k$

$y_k := y_k + \beta y_j$ if $i = k, j \neq k$;

(c) $y_k := (\alpha + \beta) y_k$ if $i = j = k$.

After this change the problem of estimating of the general complexity $c(\mathbf{A})$ of computing of the set of n linear forms (over n variables) which are the rows of $n \times n$ matrix A accepts the following matrix form: find some integer $N \geq n$, indices $1 \leq i_1 < \cdots < i_n \leq N$ and the minimal integer $c = c(A)$ such that there exists some $N \times N$ matrix which can be presented as a product of c elementary matrices (in other words the matrices corresponding to the elementary instructions) and an $n \times n$ submatrix of this $N \times N$ matrix which is situated at the intersection of rows and columns with the indices $i_1, \ldots, i_n$ is equal to A. Further we shall make use of this reformulation and use the matrix terms. Some more elegant form the problem under discussion accept in the case $N = n$ (the absence of auxiliary memory) but even in this particular case there is no success in obtaining nonlinear lower bounds for the general complexity measure. Meanwhile, the author conjectures that a solution of the problem under discussion in the case $N = n$ would give a possibility for solving the problem in the general case.

Also remark (actually it was made in [7]) that the complexity $c(A)$ of an $n \times n$ matrix A is equal to n^2 almost everywhere in the case of an infinite field F and is equal to $n^2/\ln n$ (within a constant factor) in the case of a finite field. So the problem of obtaining a lower bound can be interpreted informally as the problem of producing a 'concrete' matrix from the 'great' set of matrices (filling in almost the whole space of all matrices) of the large complexity.

Say briefly about further content of the paper. In Section 2 so-called triangular computations will be introduced, for them a method for obtaining nonlinear lower bounds of (triangular) complexity will be described and a concrete implicit example of a matrix with non-linear triangular complexity will be produced. Notice at once that in proving its name the result of any triangular computation is an uppertriangular matrix.

In Section 3 the directed computations will be defined by which (distinguished from the triangular computations) already every matrix can be computed but the considerable restriction (compared with the measure $c(A)$) consists in the definition of the complexity (the directed complexity). A simple criterion in the terms of minors of a matrix will be formulated on satisfying of which the directed complexity of a matrix is quadratic in the size of the matrix.

Although it is very easy to produce a matrix with the large directed complexity, it may be interesting that there is a success in the explicit calculation of the directed complexity (this will be done in Section 4). In order to calculate the directed complexity sharply (and effectively) the author was compelled to prove many algebraic assertions which is done in the appendix. The appendix itself probably presents special interest and can be entered into the immediate subject of the paper by a stretch but the author couldn't find the basic results of the appendix in literature

(interrogation of acquainted specialists in Chevalley groups was also unsuccessful). Besides that and the major thing, the results of the appendix are really necessary for explicit calculation of the directed complexity and moreover this calculation itself presents the curious application of the algebraic methods to the computational complexity. By all of these reasons the author has decided to include the appendix into the paper. The author tried to write the appendix so that one can read it without any preliminary knowledge on Chevalley groups (all the necessary definitions are adduced and if a known result is used reference is made to where this result can be found). On the other hand in order to understand the main result (Theorem 4 in Section 4) one can only read definitions and formulations in the appendix not going deep into the proofs. Remark for the completeness that the author has generalized the results of the appendix to the classical Chevalley groups [12].

It turns out that the directed complexity of a nonsingular matrix can be expressed as the length of the substitution from Bruhat decomposition of this matrix (all the necessary definitions can be found in Section A.1 of the appendix). In order to express the directed complexity of an arbitrary matrix, the author has constructed the generalized Bruhat decomposition (see Theorem 16 in Section A.2 of the appendix) and in its terms calculation of the directed complexity has been a success. Technically difficult is the proof of the elimination of the auxiliary memory in the directed computations (see Theorems 13 and 19 in the appendix), from which the explicit expression for the directed complexity can be already obtained relatively simply (see Theorem 4 in Section 4).

In Section 5 the reduced directed complexity (which is more close to the general complexity measure than the directed complexity) will be introduced. For this measure too a criterion in terms of minors of a matrix can be formulated on satisfying of which the reduced directed complexity of the matrix is quadratic in the size of the matrix. The examples of the matrices with the quadratic reduced directed complexity will be produced (over the field of rational numbers and also over finite fields). Making use of the existence of the linear superconcentrators it will be shown that the quadratic lower bound of the reduced directed complexity of a matrix A does not guarantee a nonlinear lower bound on the general complexity measure $c(A)$.

As conclusion of the main text it is noticed that a weak answer to the problem due to Valiant [11] can be deduced from the method of [2, Section 1].

2. Triangular computations

By the observation made in Section 1, consider computations containing only elementary instructions. The condition of the triangularity of a computation is in fact that in the computation only instructions of the following kind are used:

$$y_k := \alpha y_k \quad \text{or} \quad v_k := y_k + \alpha y_i \quad \text{where } i > k.$$

The result of a triangular computation is an uppertriangular matrix (i.e. a matrix with

zeroes below the diagonal). The triangular complexity $c_\triangle(A)$ of an uppertriangular matrix A is defined (in the usual manner) as the minimal complexity of the triangular computations (the complexity of a triangular computation is equal to a number of its instructions) computing A.

Adopt the following notations: $z_{ij}^{(\alpha)}$ is a matrix with the (i, j)-entry equal to α and with the other entries equal to zero. Further, $e_{ij}^{(\alpha)} = E + z_{ij}^{(\alpha)}$, where E is the unity matrix.

Using the matrix language and taking into account that the computations under consideration satisfy condition (5) in Section 1, we see that $c_\triangle(A)$ for an upper-triangular $n \times n$ matrix A is equal to the minimal c for which there exists an upper-triangular $N \times N$ matrix B such that, for some indices $1 \leq k_1 < \cdots < k_n \leq N$, the equality $(B)_{k_1,\ldots,k_n} = A$ is fulfilled, where $(B)_{k_1,\ldots,k_n}$ denotes the submatrix of the matrix B situated at the intersection of the rows and the columns with the indices $k_1, \ldots, k_n$ (a submatrix of such a kind we call the main submatrix), and moreover the matrix B can be presented as a product of c elementary uppertriangular matrices, i.e. $B = e_{i_1 j_1}^{(\alpha_1)} \cdots e_{i_c j_c}^{(\alpha_c)}$ where $i_1 \leq j_1, \ldots, i_c \leq j_c$.

Theorem 1. *Let an uppertriangular matrix* $A = \begin{pmatrix} U & W \\ 0 & V \end{pmatrix}$ *where* U, V *are, obviously, also uppertriangular matrices. Then*

$$c_\triangle(A) \geq c_\triangle(U) + c_\triangle(V) + \operatorname{rg} W.$$

Proof. Let U be $m \times m$ matrix. Using the notations introduced earlier $B = e_{i_1 j_1}^{(\alpha_1)} \cdots e_{i_c j_c}^{(\alpha_c)}$. Let $B = \begin{pmatrix} B_1 & D \\ 0 & B_2 \end{pmatrix}$ where B_1, B_2 are uppertriangular matrices and B_1 is of the size $k_m \times k_m$.

For each pair of indices $1 \leq i, j \leq N$ the (i, j)-entry of matrix B is

$$b_{ij} = \sum \alpha_{q_1} \cdots \alpha_{q_s} + \delta_{ij} \tag{1}$$

where the sum runs over such sets of indices $1 \leq q_1 < \cdots < q_s \leq c$ for which $i_{q_1} = i$, $j_{q_s} = j$ and $i_{q_{t+1}} = j_{q_t}$ for all $1 \leq t < s$ (δ_{ij} is Kronecker symbol).

Set $J = \{u : 1 \leq u \leq c, j_u \leq k_m\}$, $I = \{v : 1 \leq v \leq c, i_v > k_m\}$. Certainly, $I \cap J = \emptyset$. In the case when $j \leq k_m$ (or $i > k_m$) only $q \in J$ (resp. $q \in I$) can occur in the right part of equality (1). Hence for the subproducts (with order preservation) over indices from I and from J, the equalities $\prod_{u \in J} e_{i_u j_u}^{(\alpha_u)} = B_1$ and analogously $\prod_{v \in I} e_{i_v - k_m, j_v - k_m}^{(\alpha_v)} = B_2$ are fulfilled. Taking into account that $(B_1)_{k_1,\ldots,k_m} = U$ and $(B_2)_{k_{m+1}-k_m,\ldots,k_n-k_m} = V$ we obtain the inequalities

$$|J| \geq c_\triangle(U) \quad \text{and} \quad |I| \geq c_\triangle(V) \tag{2}$$

($|J|$ denotes the cardinality of the set J).

Let $\{p_1, \ldots, p_r\} = \{1, \ldots, c\} \setminus (I \cup J)$, where $r = c - |I| - |J|$.

Consider now a pair of indices i, j such that $i \leq k_m < j$. One and only one index q_l $(1 \leq l \leq s)$ equal to some p_f $(1 \leq f \leq r)$ occurs in each product in the right part of (1).

Therefore b_{ij} can be expressed as a sum

$$b_{ij} = \sum_{1 \leq f \leq r} \Big(\sum_{u_1, \ldots, u_g} \alpha_{u_1} \cdots \alpha_{u_g} \Big) \alpha_{p_f} \Big(\sum_{v_1, \ldots, v_h} \alpha_{v_1} \cdots \alpha_{v_h} \Big) \tag{3}$$

where the inner sums run over all sets of indices $u_1 < \cdots < u_g$ and $v_1 < \cdots < v_h$ satisfying the conditions:

(a) $u_1, \ldots, u_g$ $(u_g < p_f)$ are such elements of J that $i_{u_1} = i$, $j_{u_g} = i_{p_f}$ and $i_{u_{t+1}} = j_{u_t}$ for all $1 \leq t < g$;

(b) $v_1, \ldots, v_h$ $(v_1 > p_f)$ are such elements of I that $i_{v_1} = j_{p_f}$, $j_{v_h} = j$ and $i_{v_{t+1}} = j_{v_t}$ for all $1 \leq t < h$.

Denote in (3) the sum $\sum_{u_1, \ldots, u_g} \alpha_{u_1} \cdots \alpha_{u_g}$ by $b^J(i, f)$ and $\sum_{v_1, \ldots, v_h} \alpha_{v_1} \cdots \alpha_{v_h}$ by $b^I(f, j)$. Further by $B(f)$ we denote the $N \times N$ matrix of rank 1 defined as the product of the column with the ith coordinate equal to $b^J(i, f)$ $(1 \leq i \leq N)$ by the row with the jth coordinate equal to $b^I(f, j)$. Adopt the consent that the empty sum is equal to zero.

Hence the uppertriangular $N \times N$ matrix $\left(\begin{smallmatrix} 0 & D \\ 0 & 0 \end{smallmatrix}\right) = \sum_{1 \leq f \leq r} \alpha_{p_f} B(f)$ and taking into account that D contains W as a submatrix, we deduce the inequalities $r \geq \operatorname{rg} D \geq \operatorname{rg} W$. Together with (2) this completes the proof of the theorem.

We now produce a concrete example of an uppertriangular matrix with nonlinear triangular complexity.

Corollary 2. *Define by induction the following sequence of uppertriangular matrices:* $A_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \ldots, A_{n+1} = \left(\begin{smallmatrix} A_n & E \\ 0 & A_n \end{smallmatrix}\right)$. *Then* $c_\triangle(A_n) = n \cdot 2^{n-1}$.

Proof. The lower bound can be deduced from Theorem 1 by induction on n. For proving the upper bound we construct by induction on n the natural triangular computation (which computes A_{n+1}). In the first stage the upper copy of A_n is computed (by the induction hypothesis), in the second stage the unity matrix from the right upper corner of A_{n+1} and in the third stage the lower copy of A_n (also by the induction hypothesis).

Observe that the function $c_\triangle$ is equal to $\frac{1}{2}n(n+1)$ almost everywhere on the variety of all $n \times n$ uppertriangular matrices in the case of an infinite field F and $c_\triangle$ is equal to $n^2/\ln n$ within a constant factor almost everywhere in the case of a finite field F (the upper bound in the latter case can be proved by induction on n basing on the method suggested in [7]).

We turn ourselves in conclusion of this section to one circumstance being a surprise at first sight. Obviously $c_\triangle(A) \geq c(A)$ for every uppertriangular matrix A. It is natural to ask "is the converse valid?" It turns out that the answer on this question is negative. For example, define a 6×6 matrix $A = e_{54}^{(-1)} e_{15}^{(1)} e_{25}^{(1)} e_{56}^{(1)} e_{35}^{(1)} e_{54}^{(1)}$, then $c(A) \leq 6$. On the other hand using the method suggested in the proof of Theorem 1 and partitioning matrix A in four blocks such that the upper left block is of the size 4×4

and the lower right one is of the size 2×2, one can deduce that $c_{\Delta}(A)\geqslant 7$ (remark that the immediate application of Theorem 1 does not yet entail this lower bound, one needs some additional speculations).

3. Directed computations

A directed computation contains by definition instructions of the following three kinds:

(a) $y_{i+1} := y_{i+1}+\alpha y_i$;

(b) $y_k := y_k+\alpha y_i$ where $k<i$;

(c) $y_k := \alpha y_k$

and set a measure of complexity of a directed computation, in other words the directed complexity (denote it by c_d), equal to a number of instructions of kind (a). Denote by $\mathrm{el}_d(A)$ the minimal number of elementary matrices of the kind $e^{(\alpha)}_{i+1,i}$ in all the products $A=\prod_k e^{(\alpha_k)}_{i_k,j_k}$ containing the elementary matrices of the kinds $e^{(\alpha)}_{i+1,i}$, $e^{(\alpha)}_{i,k}$ $(k\geqslant i)$. The directed complexity $c_d(A)$ for a matrix A is defined in the usual manner as the minimal complexity of all directed computations computing A. Certainly $c_d(A)\leqslant \mathrm{el}_d(A)$ (the inverse inequality will be proved in Section 4). Taking into account that the computations under consideration satisfy condition (5) from Section 1, we obtain that $c_d(A)=\min \mathrm{el}_d(C)$ where the minimum is taken over all C containing A as a main submatrix (see Section 2). Notice that $c_d(A)=0$ iff A is an uppertriangular matrix.

We show that the directed complexity coincides with its following modification: instead of the instructions of kind (a) any instructions of the kind $y_k := y_k+\alpha y_i$ for $k>i$ are allowed, and the weight $2(k-i)-1$ is attached to such an instruction. For checking of the coincidence it is convenient to use the matrix language. Denote further by $s_i\in S_N$ $(1\leqslant i<N)$ the matrix of transposition of the neighbouring indices i and $(i+1)$ (S_N is the group of all substitutions of N elements). The equality $s_i=e^{(-2)}_{i+1,i+1}\,e^{(1)}_{i,i+1}\,e^{(-1)}_{i+1,i}\,e^{(1)}_{i,i+1}$ entails that $c_d(s_i)=1$. Using the equality $e^{(\alpha)}_{k,i}=s_is_{i+1}\cdots s_{k-2}\,e^{(\alpha)}_{k,k-1}s_{k-2}\cdots s_{i+1}s_i$ for $k>i$, we obtain that $c_d(e^{(\alpha)}_{k,i})\leqslant 2(k-i)-1$ $(k>i)$. One can easily deduce the desired coincidence from this inequality.

We now formulate the simple criterion on fulfillment of which for an $n\times n$ matrix A the directed complexity $c_d(A)$ is equal to n^2 within a constant factor. On the other hand the inequality $c_d(A)\leqslant \frac{1}{2}n(n-1)$ follows from the results of Section 4.

Lemma 3. *Let a matrix* $A=\begin{pmatrix} U & W\\ D & V\end{pmatrix}$ *where* U *and* V *are some square matrices. Then* $c_d(A)\geqslant (\mathrm{rg}\,D)^2$.

Proof. The lemma can be simply proved with the help of the results of Section 4 and of the method suggested in the proof of Theorem 1. We expose here the more immediate proof.

Correspond in the usual manner to a directed computation of the complexity $c_d(A)$ computing A the oriented acyclic graph G with the number of vertices equal to the number of all instructions of the kinds (a), (b) and (c) in the computation under consideration (see e.g. [10, 11]). Mark a vertex corresponding to an instruction $y_k := y_k + \alpha y_i$ (or to an instruction $y_k := \alpha y_k$) by the label k. Choose some $r \times r$ ($r = \operatorname{rg} D$) nonsingular submatrix of the matrix D and let it be situated at the intersection of the rows with the indices $l_1, \ldots, l_r$ and the columns with the indices $j_1, \ldots, j_r$.

The results of [10] (see also [9]) entail that r paths in the graph G without mutual intersections in vertices can be drawn from the input vertices of the graph G marked by the labels $i_{j_1}, \ldots, i_{j_r}$ to the output vertices with the labels $i_{l_1}, \ldots, i_{l_r}$ (remember the consents adopted in the items (3) and (5) from Section 1: the set of the input variables is put in the registers $y_{i_1}, \ldots, y_{i_n}$ at the beginning of computing, the result of the computation is put in these registers at the end of computing). Without loss of generality we can suppose that kth path passes from the vertex with the label i_{j_k} to the vertex with the label i_{l_k}. Consider the labels along the kth path. The label either does not increase along one edge or increases with one, therefore the contribution to $c_d(A)$ of the weights of the instructions corresponding to the vertices on kth path is no less than $i_{l_k} - i_{j_k}$. On the other hand $\max_{1 \leq k \leq r}\{i_{j_k}\} < \min_{1 \leq k \leq r}\{i_{l_k}\}$ (because the matrix D is situated in A below the diagonal), hence $c_d(A) \geq \sum_{1 \leq k \leq r}(i_{l_k} - i_{j_k}) \geq r^2$. This completes the proof of the lemma.

Consider the $n \times n$ matrix $V = \sum_{1 \leq i \leq n} z^{(1)}_{i,n+1-i}$. The equality $c_d(V) = \frac{1}{2}n(n-1)$ can be deduced from Theorem 4 in Section 4 (the inequality $c_d(V) \geq \frac{1}{4}(n-1)^2$ follows already from Lemma 3). On the other hand $V = (1\ n)(2\ n-1) \cdots ([\frac{1}{2}n]\ n+1-[\frac{1}{2}n])$ is the product of $[\frac{1}{2}n]$ transpositions. A transposition $(i\ j)$ equals to $e^{(-2)}_{ij}\, e^{(1)}_{ij}\, e^{(-1)}_{ji}\, e^{(1)}_{ij}$. Hence $c(V) \leq 2n$, i.e., the general complexity can be far less than the directed one.

4. Explicit calculation of the directed complexity by means of the generalized Bruhat decomposition

In the present section we obtain (basing on the results of the appendix) the explicit calculation of the directed complexity of a set of linear forms (speaking in the matrix language we deal with the coefficient matrix of a set). In the formulations and proofs we use the notations introduced in the appendix.

Let A be an $n \times n$ matrix, the substitution $w_A \in S_n$ be its completion constructed in Theorem 16 of Section A.2 of the appendix. Further let T_1, $T_2 \in \mathcal{T}$—the space of all uppertriangular matrices (i.e. not necessary nonsingular matrices with zeroes below the diagonal), $w \in S_n$. For the function l see the beginning of Section A.1 of the appendix and also the definition immediately after Theorem 16 of Section A.2 of the appendix.

Theorem 4. $c_d(A) = l(A) = l(w_A) = \min_{A \in \mathcal{T} w \mathcal{T}} l(w)$.

Proof. The equality $l(A) = l(w_A)$ is valid by definition from Section A.2 of the appendix, the equality $l(w_A) = \min_{A \in \mathcal{T} w \mathcal{T}} l(w)$ follows from Theorem 16.

Let $A = T_1 w_A T_2$ be a generalized Bruhat decomposition of A (see Theorem 16 and the definition after it). Present $w_A = s_{i_1} \cdots s_{i_l}$ where $l = l(A)$ (see the beginning of Section A.1 of the appendix). It is shown in Section 3 that $c_d(s_i) = 1$ therefore $c_d(A) \leq l(A)$.

Obviously, it is sufficient to prove the inverse inequality under the assumption that the field F is algebraically closed. Further we apply the auxiliary function $\mathrm{el}_d(A)$ introduced in Section 3.

Lemma 5. $\mathrm{el}_d(A) = l(A)$.

Proof. The inequality $\mathrm{el}_d(A) \leq l(A)$ can be proved with the help of the equality $c_d(s_i) = 1$ (cf. the above proof of the inequality $c_d(A) \leq l(A)$).

Conversely, let

$$A = \prod_k e_{i_k j_k}^{(\alpha_k)}, \tag{*}$$

where a number of the elementary multipliers of the kind $e_{i+1,i}^{(\alpha)}$ is equal to $t = \mathrm{el}_d(A)$. Let ε be a parameter. Change in the decomposition (*) each singular elementary multiplier (which is necessary of the kind $e_{i,i}^{(-1)}$) by the elementary matrix $e_{i,i}^{(-1+\varepsilon)}$. As a result we obtain the decomposition of the matrix A_ε for every $\varepsilon \in F$ (remark that $A_0 = A$) instead of the decomposition (*). Moreover all the elementary matrices from the right part of this decomposition are nonsingular when $\varepsilon \neq 0$, so A_ε is also nonsingular for $\varepsilon \neq 0$. If $A = A_0 \in \overline{\{A_\varepsilon : \varepsilon \neq 0\}}$ (the bar over a set denotes its closure in Zarisky topology in the variety $\mathcal{M}_n$ of all $n \times n$ matrices), then $l(A) \leq \max_{\varepsilon \neq 0} l(A_\varepsilon)$, according to (b) of Corollary 18 of Section A.2 of the appendix.

We now ascertain the inequality $l(A_\varepsilon) \leq t$ for $\varepsilon \neq 0$. Let $\mathcal{B} \subset \mathcal{T}$ be the space of all nonsingular uppertriangular matrices. We make use of the following well-known result (see e.g. [1, Ch. 4, Section 2], or [3, Lemma 12.7] or [8, Lemma 25, Section 3]): for every substitution $w \in S_n$ and each $1 \leq i < n$,

$$\mathcal{B} w \mathcal{B} \cdot \mathcal{B} s_i \mathcal{B} \subset \mathcal{B} w \mathcal{B} \cup \mathcal{B} w s_i \mathcal{B}. \tag{4}$$

Fix $\varepsilon \neq 0$. Let

$$C = A_\varepsilon = e_{i_1} \cdots e_{i_{f_1}} e_{j_1} e_{i_{f_1+1}} \cdots e_{i_{f_2}} e_{j_2} e_{i_{f_2+1}} \cdots e_{i_{f_t}} e_{j_t} e_{i_{f_t+1}} \cdots e_{i_{f_{t+1}}} \tag{**}$$

be the above constructed decomposition of A_ε into a product of nonsingular elementary matrices (denoted by e with some indices). Among them $e_{j_1}, \ldots, e_{j_t}$ are all the matrices of the kind $e_{i+1,i}^{(\alpha)}$ occuring in the decomposition (**) (remmber that $t = \mathrm{el}_d(A)$). Let $C^{(k)} = e_{i_1} \cdots e_{i_{f_1}} e_{j_1} e_{i_{f_1+1}} \cdots e_{i_{f_k}} e_{j_k} e_{i_{f_k+1}} \cdots e_{i_{f_{k+1}}}$ $(1 \leq k \leq t)$ be a subproduct (from the left and without gaps) of the above constructed product (**).

The decomposition under consideration of $C^{(k)}$ contains k matrices $e_{j_1}, \ldots, e_{j_k}$ of the kind $e^{(\alpha)}_{i+1,i}$ among the matrices $e_{j_1}, \ldots, e_{j_k}$ of the same kind in (**).

Deduce by the induction on k that $l(C^{(k)}) \leq k$ (of course $C^{(1)} = C = A_\varepsilon$). Let $C^{(k)} = B_1 w_k B_2$ be the Bruhat decomposition (see Proposition 11 from Section A.1 of the appendix), where $w_k \in S_n$, $B_1, B_2 \in \mathcal{B}$ and $l(C^{(k)}) = l(w_k) \leq k$ by the induction hypothesis. Then according to (4)

$$C^{(k+1)} \in \mathcal{B} w_k \mathcal{B}\, e^{(\alpha)}_{i+1,i} \mathcal{B} \subset \mathcal{B} w_k \mathcal{B} s_i \mathcal{B} s_i \mathcal{B}$$

$$\subset (\mathcal{B} w_k \mathcal{B} \cup \mathcal{B} w_k s_i \mathcal{B}) \cdot (s_i \mathcal{B}) \subset \mathcal{B} w_k s_i \mathcal{B} \cup \mathcal{B} w_k \mathcal{B}$$

for some $1 \leq i < n$ (here we use the equality $e^{(\alpha)}_{i+1,i} = s_i e^{(\alpha)}_{i,i+1} s_i$). Hence $l(C^{(k+1)}) \leq k+1$ (see the definition of the function in Section A.1 of the appendix).

Thus $l(A_\varepsilon) = l(C^{(t)}) \leq t = \mathrm{el}_d(A)$ for $\varepsilon \neq 0$. Recalling that $l(A) \leq \max_{\varepsilon \neq 0} l(A_\varepsilon)$ as proved earlier we have $l(A) \leq \mathrm{el}_d(A)$. The lemma is proved.

To complete the proof of the theorem, remember that $c_d(A) = \min \mathrm{el}_d(C)$ where the minimum is taken over all C containing A as a main submatrix. The inequality $l(A) \leq l(C)$ is fulfilled by Theorem 19 from the appendix, Lemma 5 entails that $l(C) = \mathrm{el}_d(C)$ and finally we obtain $l(A) \leq c_d(A)$ which was to be proved.

Corollary 6. (a) *If A is a main submatrix of a matrix C, then $c_d(A) \leq c_d(C)$;*

(b) *$c_d(A)$ does not depend on a field F (i.e. $c_d(A)$ is preserved if one considers a matrix A over an extension of F);*

(c) *$c_d(A)$ is semicontinuous as a function of A, i.e. $c_d(A) \leq \max_{C \in \mathcal{U} \subset \mathcal{M}_n} c_d(C)$ if $A \in \bar{\mathcal{U}}$;*

(d) *$\max_{A \in \mathcal{M}_n} c_d(A) = \frac{1}{2}n(n-1)$ and $c_d(A)$ is quadratic in n without a constant factor almost everywhere for any field F ($c_d(A) = \frac{1}{2}n(n-1)$ almost everywhere in the case of an infinite field);*

(e) *$c_d(A)$ can be calculated in polynomial time for a matrix A with rational entries (in fact n^3 operations over the entries are sufficient).*

A sketch of the proof. (a) Use Theorem 19 of Section A.2 of the appendix.

(b) Apply Lemma 10 of Section A.1 of the appendix and the equality $c_d(A) = l(w_A)$.

(c) Follows from (b) of Corollary 18 of Section A.2 of the appendix.

(d) The first part can be deduced from Proposition 12 of Section A.1 of the appendix; for the proof of the second part use Lemma 3 of Section 3 (the assertion in parenthesis follows from the Chevalley theorem—see Proposition 12).

(e) One can check it basing on the constructing of w_A in the proof of Theorem 16 of Section A.2 of the appendix and on the constructing of the incomplete sample u_A in the proof of (c) of Proposition 14 from Section A.2 of the appendix.

5. Reduced directed complexity

There is shown at the end of Section 3 that it is very simply to produce an $n \times n$ matrix A with the directed complexity $c_d(A)$ quadratic in n and with the general complexity $c(A)$ linear in n. One of the reasons of this phenomenon consists in the fact that the directed complexity of a set of linear forms depends essentially on the order in which these forms are numerated. The reduced directed complexity considered in the present section is deprived of this drawback.

The reduced directed complexity of $n \times n$ matrix A is defined as

$$c_d^*(A) = \min_{w_1, w_2 \in S_n} c_d(w_1 A w_2).$$

The value of $c_d^*(A)$ does not depend on the choice of a field F (this follows from Corollary 6(b) in Section 4).

Lemma 7. *If the rank of each* $[\frac{1}{2}n] \times [\frac{1}{2}n]$ *submatrix of a matrix* A *is no less than* r, *then* $c_d^*(A) \geq r^2$.

This lemma can be easily deduced from Lemma 3 in Section 3.

A matrix A satisfying the condition formulated in Lemma 7 for $r = [\frac{1}{2}n]$ can be produced without great difficulties over an infinite (or with a sufficiently large cardinality compared with n) field F.

Check for example that an $n \times n$ matrix $\Phi_n = (2^{ij})$ for $F = \mathbb{Q}$ satisfies the condition under consideration from Lemma 7. Moreover show that any minor of the matrix Φ_n does not vanish. Consider some $k \times k$ submatrix D of the matrix Φ_n situated at the intersection of the rows with the indices $i_1 < \cdots < i_k$ and the columns with the indices $j_1 < \cdots < j_k$. Then

$$M = \sum_{1 \leq l \leq k} i_l j_{k+1-l} < \sum_{1 \leq l \leq k} i_l j_{\pi(k+1-l)}$$

where $\pi \in S_k$ is any nonidentical substitution. This can be deduced, for instance, by presenting $\pi = s_{i_1} \cdots s_{i_l}$ where $l = l(\pi)$ is the length of π (see Section A.1 of the appendix). Lemma 10 of Section A.1 of the appendix then entails that each transposition s_{i_m} $(1 \leq m \leq l)$ increases the number of inversions of a substitution $s_{i_1} \cdots s_{i_{m-1}}$ (i.e. its length) by one. It is not difficult to deduce from this, by the induction on m, that each multiplier s_{i_m} increases the expression in the right part of the desired inequality. The proved inequality entails that $\det D = (-1)^{k(k-1)/2} 2^M + q \cdot 2^{M+1}$ for some integer q, so $\deg D \neq 0$.

A more difficult thing is the production of examples in the case of a finite field F. Considerations exposed above are not applicable here as for instance there does not exist a $2n \times 2n$ matrix (for $n > 3$) over the field consisting of two elements in which every $n \times n$ minor does not vanish (there does not even exist an $n \times 2n$ matrix with this property). That is why for producing a matrix with the large reduced directed complexity over a finite field we are compelled to make use of some constructions from the coding theory. We restrict ourselves to the case of the field of two elements.

Let C be a $k \times n$ matrix. The minimal number of unities in all nonzero linear combinations of the rows of C is called the *coding distance* of C (see [6, Chapter 1]). Set $k(n, d)$ be the largest possible values of k when n and d are fixed. Utilize the following estimation (see [6, Chapter 4]): if $d/n < \frac{1}{2}$, then $k(n, d) \sim n(1 - H(d/n))$ for large n, where $H(q) = -q \log_2 q - (1-q)\log_2(1-q)$ is the entropy $(0 \leq q \leq 1)$.

The function H increases on the interval $[0, \frac{1}{2}]$. Obviously $H(0) = 0$ and $H(\frac{1}{4}) > \frac{1}{2}$ hence $H(\gamma) = \frac{1}{2}$ for some unique $0 < \gamma < \frac{1}{4}$. Set $d \sim \gamma n$, $k = k(n, d) \sim \frac{1}{2}n$ for some sufficiently large even n and let C_n be some $\frac{1}{2}n \times n$ matrix with coding distance d. Define A_n as an $n \times n$ matrix consisting of two $\frac{1}{2}n \times n$ submatrices situated at the first $\frac{1}{2}n$ and last $\frac{1}{2}n$ rows both equal to C_n, i.e. $A_n = \binom{C_n}{C_n}$.

Proposition 8. *$C_d^*(A_n) > \varepsilon n^2$ for some $\varepsilon > 0$ independent of n.*

Proof. Fix $D = w_1 A_n w_2 (w_1, w_2 \in S_n)$. Let $I = w_1(\{1, \ldots, \frac{1}{2}n\}), J = w_1(\{\frac{1}{2}n + 1, \ldots, n\})$. Either

$$|I \cap \{\tfrac{1}{2}n + 1, \ldots, n\}| \geq \tfrac{1}{4}n \text{ or } |J \cap \{\tfrac{1}{2}n + 1, \ldots, n\}| \geq \tfrac{1}{4}n.$$

In the following we assume that $|I \cap \{\frac{1}{2}n + 1, \ldots, n\}| \geq \frac{1}{4}n$. Let $t = |I \cap \{\frac{1}{2}n + 1, \ldots, n\}|$.

We let D' denote a $t \times n$ submatrix of the matrix D situated at the rows of D with indices from the set $I \cap \{\frac{1}{2}n + 1, \ldots, n\}$. Let D_1 be a $t \times \frac{1}{2}n$ submatrix of matrix D' situated at the columns of D' with indices from the set $\{1, \ldots, \frac{1}{2}n\}$ and let D_2 be a $t \times \frac{1}{2}n$ submatrix of matrix D' situated at the columns with indices from the set $\{\frac{1}{2}n + 1, \ldots, n\}$. Estimate $r = \operatorname{rg} D_1$.

Consider some $(t - r) \times t$ matrix V with linear independent rows and $VD_1 = 0$. Then the coding distance of the $(t - r) \times \frac{1}{2}n$ matrix VD_2 is no less than d. As $d/\frac{1}{2}n \sim 2\gamma < \frac{1}{2}$, $(t - r) \leq k(\frac{1}{2}n, d) \sim \frac{1}{2}n(1 - H(2\gamma))$. Therefore $r \geq \frac{1}{2}n(H(2\gamma) - \frac{1}{2}) = \gamma_1 n$ ($\gamma_1 > 0$ because $H(2\gamma) > H(\gamma) = \frac{1}{2}$).

Using Lemma 7 and the fact that matrix D_1 is situated in D below the diagonal, we obtain that $c_d^*(A_n) \geq r^2 > \varepsilon n^2$.

Certainly $c_d^*(A) \leq \frac{1}{2}n(n-1)$ for an $n \times n$ matrix A. If a field F is infinite, then $c_d^*(A) = \frac{1}{2}n(n-1)$ almost everywhere (cf. Corollary 6(d) in Section 4). If a field F is finite, then $c_d^*(A)$ is quadratic in n almost everywhere; this can be deduced by proving that for almost every $n \times n$ matrix over a finite field the rank of each $[\frac{1}{2}n] \times [\frac{1}{2}n]$ submatrix is greater than $\frac{1}{4}n$ and application of Lemma 7).

Proposition 9. *If a field F is infinite, then there exists a sequence of matrices $\{V_n\}_{n \geq 1}$ (V_n is an $n \times n$ matrix) such that the general complexity $c(V_n)$ is linear in n and $c_d^*(V_n)$ is quadratic in n.*

Proof. Let $\{G_n\}_{n \geq 1}$ be a sequence of superconcentrators (G_n *is an* n-superconcentrator) with the number of edges linear in n (see e.g. [10]). Fix n and supply the ith

edge (in some fixed numeration) of the graph G_n with a parameter β_i. Correspond to the input vertices of G_n the variables $x_1, \ldots, x_n$. If some values from the field F are attached to the parameters $\{\beta_i\}$, then the linear form over the variables $x_1, \ldots, x_n$ with the coefficients from F can be corresponded naturally to each vertex of the graph G_n. By this the linear forms $v_1, \ldots, v_n$ are corresponded to the output vertices.

We show that the values from F can be attached to $\{\beta_i\}$ so that in $n \times n$ matrix V_n with rows $v_1, \ldots, v_n$ each of its minors is distinguished from zero. Suppose contrarily that some $k \times k$ submatrix situated at the intersection of the rows with the indices $j_1, \ldots, j_k$ (corresponding to the forms $v_{j_1}, \ldots, v_{j_k}$) and the columns with the indices $l_1, \ldots, l_k$ (corresponding to the variables $x_{l_1}, \ldots, x_{l_k}$) is singular for any attaching the values to the parameters $\{\beta_i\}$. As G_n is a superconcentrator, k paths from the input vertices $l_1, \ldots, l_k$ to the output vertices $j_1, \ldots, j_k$ can be passed such that these paths have no common vertices. Attach to the parameters, corresponding to the edges belonging to the considered k paths, the value one and attach the value zero to the other parameters. By this attaching the $k \times k$ minor under consideration is equal to ± 1 which contradicts the accepted assumption.

Now it is not difficult to check that for some attaching values to the parameters $\{\beta_i\}$ all the minors of the matrix V_n do not vanish. Each minor is a polynomial over variables $\{\beta_i\}$ not vanishing identically as it was proved above. Hence such values from F can be attached to the parameters $\{\beta_i\}$ that all these polynomials (minors) are distinguished from zero implying that the field F is infinite.

The general complexity $c(V_n)$ is linear in n (it is no greater than the number of edges in G_n) and $c_{\mathrm{d}}^{*}(V_n) \geq \frac{1}{4}n^2$ according to Lemma 7 which completes the proof of the proposition.

In conclusion, without any connection with the preceding text but with a connection to the subject under investigation, we give, based on the method from [2, Section 1], an incomplete answer to the problem due to Valiant (see problem 2 in [11]). The question of Valiant is informally the following: Is the nonlinearity of the general complexity $c(A)$ of an $n \times n$ matrix A guaranteed by the fulfilment of the following condition: if $A = D + C$ for some matrices D, C, then either $\operatorname{rg} D > \varepsilon n$ or the number of nonzero entries in the matrix C is greater than εn^2 (for some $\varepsilon > 0$ independent of n)?

The incompleteness of the answer consists in the assumption that a straight-line computation (additive computation), computing a set of linear forms $a_1, \ldots, a_n$ being the rows of a matrix A, satisfies the following restriction (condition (**) in [2]): Correspond the oriented below acyclic graph G to a straight-line computation in the usual manner and let $G^{(i)}$ $(1 \leq i \leq n)$ denote the subgraph of graph G generated by the vertices of G situated above the vertex u_i, to which a linear form a_i is attached (in other words from each vertex of the graph $G^{(i)}$ the oriented below path can be passed to the vertex u_i, and conversely each vertex with this property is in $G^{(i)}$). The considered restriction consists in assuming that every $G^{(i)}$ $(1 \leq i \leq n)$ is a tree.

The method suggested in [2, Section 1] entails in particular that if an $n \times n$ matrix A satisfies the condition due to Valiant, then the complexity (i.e. the number of instructions) of every straight-line computation computing A and satisfying the formulated restriction is greater than $n \lg n/\lg \lg n$ within a constant factor.

Appendix. Monotony of the length of a substitution in the generalized Bruhat decomposition

A.1. Bruhat decomposition and the monotony of the length of a substitution in nonsingular case

In this section information (necessary for proving Theorem 4 of Section 4) about the length of a substitution, Bruhat decomposition (see [1, 8]), is exposed and also the monotony of the length of a substitution in the nonsingular case is proved.

For any substitution $w \in S_n$ its *length* $l(w)$ is defined as the least l such that w can be presented as a product of l transpositions of neighbouring indices, i.e. $w = s_{i_1} \cdots s_{i_l}$ where s_i is the transposition of the indices i and $(i+1)$ $(1 \leq i < n)$. Any presentation of w in a product of $l = l(w)$ transpositions of the kind s_i is called a *reduced presentation* (some properties of the function l can be found in [1, Chapter 4, Section 1]). The following lemma is well known but, as the author was not able to give a corresponding reference, we give its proof.

Lemma 10. *The length $l(w)$ is equal to the number $I(w)$ of inversions in w, i.e. the number of pairs $i < j$ such that $w(i) > w(j)$.*

Proof. As $I(s_i u) \leq I(u) + 1$ $(1 \leq i < n)$ for every $u \in S_n$, we obtain inequality $I(w) \leq l(w)$ by induction on $l(w)$.

Proof of the inverse inequality by induction on $I(w)$. If $I(w) > 0$, then there exists $1 \leq i < n$ such that $w(i) > w(i+1)$. Therefore $I(s_i w) = I(w) - 1$ and by the induction hypothesis, $l(s_i w) = I(w) - 1$. On the other hand $l(w) \leq l(s_i w) + 1 = I(w)$.

The lemma is proved.

It follows from the proof of this lemma that $\max_{w \in S_n} l(w) = \frac{1}{2}n(n-1)$ is achieved by the substitution $v = (1 \;\; n)(2 \;\; n-1) \cdots ([\frac{1}{2}n] \;\; n+1-[\frac{1}{2}n])$ (cf. the end of Section 3).

The relation of the partial order on S_n is introduced in the following manner (see [8, Section 8, Lemma 53]). Define $w' \leq w$ iff w' is equal to a product of some subsequence (preserving the order of the multipliers) of transpositions of the neighbouring indices chosen from some reduced presentation $w = s_{i_1} \cdots s_{i_l}$ where $l = l(w)$. It turns out that the definition of the partial order does not depend on a choice of a reduced presentation (see [8, Section 8, Lemma 53]), i.e. if $w = s_{i_1} \cdots s_{i_l}$ is another reduced presentation and $w' \leq w$, then w' is equal to a product of some subsequence of transpositions from the presentation $w = s_{i_1} \cdots s_{i_l}$. Obviously $l(w') \leq$

$l(w)$ when $w' \leqslant w$ and if moreover $w' \neq w$, then $l(w') < l(w)$. This entails that $w' = w$ implying that $w' \leqslant w$ and $w \leqslant w'$. Put $w' < w$ if $w' \leqslant w$ and $w' \neq w$.

The substitution v satisfies the condition $w \leqslant v$ for every $w \in S_n$. For proving this, suppose the contrary and let $w \neq v$ be some substitution relatively maximal to the order $\leqslant$. Consider any reduced presentation $w = s_{i_1} \cdots s_{i_l}$ $(l = l(w))$. There exists $1 \leqslant i < n$ such that $w(i) < w(i+1)$ because $w \neq v$. By Lemma 10, $l(s_i w) = l(w) + 1$ and hence $s_i w = s_i s_{i_1} \cdots s_{i_l}$ is a reduced presentation of $s_i w$. This entails $w < s_i w$ which contradicts with the assumption.

Denote by $\mathcal{B}$ the variety of all nonsingular uppertriangular matrices (i.e. matrices with zeroes below the diagonal and nonzero entries on the diagonal).

Proposition 11 (see [8, Section 3, Theorem 4], or [1, Chapter 4, Section 2], or [3, Lemma 12.6]). *Every nonsingular $n \times n$ matrix A can be presented in a form $A = B_1 w_A B_2$ (Bruhat decomposition) for some $B_1, B_2 \in \mathcal{B}$ and unique $w_A \in S_n$.*

Proof. One can find a proof of the uniqueness of w_A in the referred literature; besides that the more general statement will be proved in Section A.2 of the present appendix (see Proposition 14). This leaves only the effective construction of the substitution $w = w_A$ proceeding from a matrix A (see [8, Section 3]).

Execute some elementary uppertriangular transformations over the rows of the matrix A, i.e. a transformation consists in adding to a row some other row (multiplied by an element of F) with a greater index, according to the following rule. If, for instance, the first from the left nonzero entry in ith row for some i is situated in the same kth column as the first from the left nonzero entry in jth row for some j and $i < j$, then we add to ith row the jth row multiplied by a suitable coefficient from F in order to let the (i, k)-entry vanish. Use this rule as long as it is applicable (the choice of a pair i, j at step of the described process is not necessary unique). As a result we obtain a matrix $A' = B_1 A$ satisfying the following property. Let the first from the left nonzero entry of ith row $(1 \leqslant i \leqslant n)$ be situated in a cell with the coordinates $(i, w(i))$, then $w(i) \neq w(j)$ implying that $i \neq j$. It is not difficult to check that $w \in S_n$ is the desired substitution. The described process contains less than n^2 elementary transformations.

The proposition is proved.

One can deduce from the construction in the proof of Proposition 11 that the matrices B_1 and B_2 are defined over the same field F as a matrix A, and that the substitution w_A does not depend on the field, i.e. w_A is preserved on its extension. Therefore extending the field F we can assume (without loss of generality) in the formulation of Proposition 12 and in the proofs of Proposition 12 and Theorem 13 that the field F is algebraically closed.

Introduce the notation $l(A) = l(w_A)$ for every nonsingular $n \times n$ matrix A where $w_A \in S_n$ can be found by Bruhat decomposition of A (the function l does not depend on the field F by the above observation).

Proposition 12. $l(A) = \dim \mathcal{B}A\mathcal{B} - \dim \mathcal{B}$ (*certainly* $\dim \mathcal{B} = \frac{1}{2}n(n+1)$) *where* dim *is understood in the sense of the algebraic geometry* (*see* [5, *Chapter* 1]).

Proof. The proof is essentially based on the following theorem of Chevalley (see [8, Section 8, Theorem 23]):

$$\overline{\mathcal{B}w\mathcal{B}} = \bigcup_{w' \leq w} \mathcal{B}w'\mathcal{B}$$

where the bar denotes the closure in Zariski topology in the variety $\mathrm{GL}_n = \mathrm{GL}_n(F)$ of all nonsingular $n \times n$ matrices. The proof is by induction on $l(A)$. We can assume that $A = w = w_A \in S_n$ because $\mathcal{B}A\mathcal{B} = \mathcal{B}w_A\mathcal{B}$.

Each element of the Boolean algebra with the operations of union, intersection and supplement, generated by the sets closed in Zarisky topology is called a *constructive set* in the algebraic geometry (see [5, Chapter 1]). The set $\mathcal{B}w\mathcal{B}$ is constructive by the theorem of Chevalley about the constructivity of the image of a constructive set under a regular morphism (see [5, Chapter 1]) as $\mathcal{B}w\mathcal{B}$ is the image of the constructive set $\mathcal{B} \times \mathcal{B} \subset \mathrm{GL}_n \times \mathrm{GL}_n$ under the regular morphism $(C_1, C_2) \to C_1wC_2$ to the variety GL_n. Therefore $\mathcal{B}w\mathcal{B}$ can be presented as a finite union $\bigcup_i (\mathcal{U}_i \setminus \mathcal{V}_i)$ where $\mathcal{U}_i$, $\mathcal{V}_i$ are closed in GL_n, $\mathcal{U}_i$ is irreducible, $\mathcal{V}_i \subset \mathcal{U}_i$ and $\mathcal{U}_i \setminus \mathcal{V}_i \neq \varnothing$ for all i. Hence $\overline{\mathcal{B}w\mathcal{B}} = \bigcup_i \mathcal{U}_i$ and $\mathcal{B}w'\mathcal{B} \subset \bigcup_i \mathcal{V}_i$ for every $w' < w$ by the theorem of Chevalley about the structure of $\overline{\mathcal{B}w\mathcal{B}}$. So

$$\dim \mathcal{B}w'\mathcal{B} \leq \dim \bigcup_i \mathcal{V}_i$$

$$= \max_i \dim \mathcal{V}_i < \max_i \dim \mathcal{U}_i = \dim \mathcal{B}w\mathcal{B}.$$

From this inequality we obtain the inequality $l(w) \leq \dim \mathcal{B}w\mathcal{B} - \dim \mathcal{B}$ for every $w \in S_n$ by induction on $l(w)$. Suppose that the strict inequality $l(w') < \dim \mathcal{B}w'\mathcal{B} - \dim \mathcal{B}$ is fulfilled for some $w' \in S_n$, then $l(w) < \dim \mathcal{B}w\mathcal{B} - \dim \mathcal{B}$ for every $w = s_iw'$ where index i is such that $w'(i) < w'(i+1)$ (such i exists when $w' \neq v$), obviously $w' < w$. Thus $l(v) < \dim \mathcal{B}v\mathcal{B} - \dim \mathcal{B}$ under the supposed inequality because v is the unique maximal element of S_n relatively to the order $\leq$ as it was shown earlier. On the other hand the theorem of Chevalley about the structure of $\overline{\mathcal{B}w\mathcal{B}}$ entails that $\overline{\mathcal{B}v\mathcal{B}} = \mathrm{GL}_n$ (taking into account that $v \geq w$ for each $w \in \mathbf{S}_n$), therefore $\dim \mathcal{B}v\mathcal{B} = n^2$. This contradicts with the assumed inequality because $l(v) = \frac{1}{2}n(n-1)$, which completes the proof of the proposition.

Remember (see Section 2) that an $n \times n$ submatrix A of an $N \times N$ matrix C is called a main submatrix if $A = (C)_{k_1,\ldots,k_n}$ for some $1 \leq k_1 < \cdots < k_n \leq N$, i.e. A is situated in C at the intersection of the rows and the columns with the indices $k_1, \ldots, k_n$.

We turn ourselves to the main theorem of the present section.

Theorem 13. *Let A be a main submatrix of a matrix C and A, C be nonsingular. Then $l(A) \leq l(C)$.*

Proof. The general plan: compare $\dim \mathscr{B}^{(n)}A\mathscr{B}^{(n)}$ and $\dim \mathscr{B}^{(N)}C\mathscr{B}^{(N)}$ and make use of Proposition 12 ($\mathscr{B}^{(n)}$ is the variety of all nonsingular uppertriangular $n \times n$ matrices).

Set $I = \{k_1, \ldots, k_n\}, J = \{1, \ldots, N\} \backslash I$. For the convenience of notation (in order to represent a partitioning of a matrix in blocks) renumerate indices $1, \ldots, N$ (by some uniquely defined substitution $\pi \in S_N$) in order to put the indices from I at the beginning, the indices from J at the end of the new numeration with preserving the order in I and in J (i.e. $\pi(k_i) = i$ for $1 \leqslant i \leqslant n$ and $\pi(j_1) < \pi(j_2)$ for $j_1 < j_2$, $j_1 \in J$, $j_2 \in J$). Then represent $C' = \pi C \pi^{-1} = \left(\begin{smallmatrix} A & U \\ G & D \end{smallmatrix}\right)$. The matrix A is uppertriangular under the initial numeration iff it is uppertriangular under the new numeration after renumerating (the analogous is valid for D) but certainly the uppertriangularity of C' does not necessary entail the uppertriangularity of C and vice versa. Obtain $Y_0 A Q_0 = w_A = w \in S_n$ by Bruhat decomposition where $Y_0, Q_0 \in \mathscr{B}^{(n)}$ (see Proposition 11).

Estimate from below the dimension of the variety consisting of all the matrices H which can be presented in the following form:

$$H = \begin{pmatrix} X & 0 \\ Y & Z \end{pmatrix} \begin{pmatrix} Y_0 & 0 \\ 0 & E \end{pmatrix} C' \begin{pmatrix} Q_0 & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} P & Q \\ 0 & R \end{pmatrix} \in \pi \mathscr{B}^{(N)} C \mathscr{B}^{(N)} \pi^{-1} \tag{5}$$

where X, Y, Z, P, Q, R run over all the matrices (of corresponding sizes) satisfying the condition that the matrices $\left(\begin{smallmatrix} X & 0 \\ Y & Z \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} P & Q \\ 0 & R \end{smallmatrix}\right)$ are nonsingular uppertriangular under the initial numeration of the indices (i.e. $\pi^{-1}\left(\begin{smallmatrix} X & 0 \\ Y & Z \end{smallmatrix}\right)\pi$ and $\pi^{-1}\left(\begin{smallmatrix} P & Q \\ 0 & R \end{smallmatrix}\right)\pi$ are nonsingular uppertriangular). In particular X, Z, P, R, Y_0, Q_0 are nonsingular and uppertriangular under the initial and under the new numerations. Obviously

$$H = \begin{pmatrix} XY_0AQ_0P & XY_0(AQ_0Q + UR) \\ (YY_0A + ZG)Q_0P & (YY_0A + ZG)Q_0Q + (YY_0U + ZD)R \end{pmatrix}$$

$$= \begin{pmatrix} T & L_2 \\ L_1 & M \end{pmatrix}$$

where T, L_1, L_2, M denote the blocks in the middle matrix.

It can be deduced by direct calculation that

$$M = Z(D - GA^{-1}U)R + L_1 T^{-1} L_2. \tag{6}$$

Define the isomorphism (in the sense of the algebraic geometry) of the variety $\mathscr{A} = \{(T, L_1, L_2, M)\}$ (i.e. the variety of all 4-tuples with components defined by the formulas above—we utilize further the similar notations) onto some variety $\mathscr{D}$ by the formula

$$(T, L_1, L_2, M) \to (T, L_1, L_2, M - L_1 T^{-1} L_2).$$

Hence the dimension we are estimating satisfies (according to (5)) the inequality

$$\dim(\mathscr{B}^{(N)} C \mathscr{B}^{(N)}) \geqslant \dim\{(H)\} = \dim \mathscr{A} = \dim \mathscr{D}.$$

Consider the following sequence of two regular projections:

$$\mathscr{D} \xrightarrow{\varphi} \mathscr{C} = \{(T, M - L_1 T^{-1} L_2)\} \xrightarrow{\psi} \{(T)\}.$$

Proposition 12 entails that $\dim\{(T)\} = l(A) + \frac{1}{2}n(n+1)$. Estimate $\dim \mathscr{C}$ from the below. The further speculations are based on the theorem on dimensions of the layers (see [5, Chapter 1]). For application of this theorem the irreducibility of the varieties $\mathscr{D}$, $\mathscr{C}$, $\{(T)\}$ has to be ascertained. The irreducibility of $\{(T)\}$ follows from the fact that $\{(T)\}$ is the image of an irreducible variety $\mathscr{B}^{(n)} \times \mathscr{B}^{(n)}$ under the regular morphism $(B_1, B_2) \to B_1 w B_2$; analogously the irreducibility of $\mathscr{D}$ which is isomorphic to $\{(H)\}$ can be proved; the variety $\mathscr{C}$ is the image of $\mathscr{D}$ under the morphism φ and therefore $\mathscr{C}$ is also irreducible.

The matrix $D - GA^{-1}U$ is nonsingular because

$$\begin{pmatrix} E & 0 \\ -GA^{-1} & E \end{pmatrix}\begin{pmatrix} A & U \\ G & D \end{pmatrix} = \begin{pmatrix} A & U \\ 0 & D - GA^{-1}U \end{pmatrix}.$$

Hence for every fixed matrix T the dimension of its inverse image (layer) under the morphism ψ is equal to $l(D - GA^{-1}U) + \frac{1}{2}(N-n)(N-n+1)$ according to (6) and Proposition 12. Therefore

$$\begin{aligned} \dim \mathscr{C} &= \dim\{(T)\} + l(D - GA^{-1}U) + \tfrac{1}{2}(N-n)(N-n+1) \\ &\geqslant l(A) + \tfrac{1}{2}n(n+1) + \tfrac{1}{2}(N-n)(N-n+1) \end{aligned}$$

by the theorem on dimensions of the layers.

We turn ourselves to the estimation of the dimension of a layer of the morphism φ. We suppose the matrices X, Z, P, R to be fixed, hence the dimension of the layer under estimation is no less than the dimension of the variety $\{(XwQ,\ YwP)\} = \{(XY_0AQ_0Q,\ YY_0AQ_0P)\}$ with the running matrices Q, Y (satisfying of course the conditions of uppertriangularity of the matrices $\pi^{-1}\left(\begin{smallmatrix} X & 0 \\ Y & Z \end{smallmatrix}\right)\pi$ and $\pi^{-1}\left(\begin{smallmatrix} P & Q \\ 0 & R \end{smallmatrix}\right)\pi$ considered above).

Adopt the following convention on the notations. For example $A_{i,j}$ denotes the (i, j)-entry of matrix A (and so on). Return to the initial numeration preserving for the matrices the same notations, as under the new numeration, with the following modification evoking no misunderstandings: for instance Y_{j,k_η} denotes the (j, k_η)-entry of the matrix $\pi^{-1}\left(\begin{smallmatrix} X & 0 \\ Y & Z \end{smallmatrix}\right)\pi$; this cell is situated in fact, as it can be easily seen, in the submatrix Y (and so on).

Let $j \in J$, $k_i \in I$. Then we obtain from the expression for L_1 that

$$H_{j,k_i} = \sum_{k_\eta \in I} Y_{j,k_\eta} P_{k_{w(\eta)},k_i} + H^0_{j,k_i} \tag{7}$$

where $H^0_{j,k_i} = \sum_{\lambda,\mu,\tau} Z_{j,\lambda} G_{\lambda,\mu} Q^0_{\mu,\tau} P_{\tau,k_i}$ is fixed as the matrices Z, P are fixed.

It follows from (7) that $H_{j,k_1} - H^0_{j,k_1} = Y_{j,k_{w^{-1}(1)}} P_{k_1,k_1}$ because P is nonsingular uppertriangular. Hence for arbitrary value of $H_{j,k_1} (J \ni j < k_{w^{-1}(1)})$ we determine a unique $Y_{j,k_{w^{-1}(1)}}$ (if $j > k_{w^{-1}(1)}$, then $Y_{j,k_{w^{-1}(1)}} = 0$). The number of indices $j \in J$

satisfying the inequality $j < k_{w^{-1}(1)}$ is equal to $k_{w^{-1}(1)} - w^{-1}(1)$. Analogously we determine a unique $Y_{j,k_{w^{-1}(2)}}$ for $j < k_{w^{-1}(2)}$ for arbitrary value of H_{j,k_2} because in the expression $H_{j,k_2} - H^0_{j,k_2}$ from (7) only $Y_{j,k_{w^{-1}(1)}}$ (already defined) and $Y_{j,k_{w^{-1}(2)}}$ can occur. The number of indices $j \in J$ satisfying the inequality $j < k_{w^{-1}(2)}$ equals to $k_{w^{-1}}(2) - w^{-1}(2)$. Continuing like this we determine a unique $Y_{j,k_{w^{-1}(3)}}$ for arbitrary value of H_{j,k_3} for $j < k_{w^{-1}(3)}$ etc. At the end of this process we determine a unique $Y_{j,k_{w^{-1}(n)}}$ for arbitrary value of H_{j,k_n} for $j < k_{w^{-1}(n)}$.

We obtain from the expression for L_2 that

$$H_{k_i,j} = \sum_{k_\theta \in I} X_{k_i,k_\theta} Q_{k_{w(\theta)},j} + H^0_{k_i,j}$$

where $H^0_{k_i,j}$ is fixed as above. Speculating as earlier one can see that $H_{k_n,j} - H^0_{k_n,j} = X_{k_n,k_n} Q_{k_{w(n)},j}$ because X is non-singular uppertriangular. Therefore for arbitrary value of $H_{k_n,j}$ we determine a unique $Q_{k_{w(n)},j}$ for $j > k_{w(n)}$. The number of indices $j \in J$ satisfying the inequality $j > k_{w(n)}$ is equal to $(N-n) - (k_{w(n)} - w(n))$. After that we determine unique $Q_{k_{w(n-1)},j}$ for arbitrary value of $H_{k_{n-1},j}$ for $j > k_{w(n-1)}$. The number of indices $j \in J$ satisfying the inequality $j > k_{w(n-1)}$ is equal to $(N-n) - (k_{w(n-1)} - w(n-1))$ etc. At the end of this process we determine a uniquely $Q_{k_{w(1)},j}$ for arbitrary value of $H_{k_1,j}$ for $j > k_{w(1)}$.

As a result we deduce that the dimension of every layer of the morphism φ is no less than

$$\sum_{1 \leq i \leq n} (k_i - i) + \sum_{1 \leq i \leq n} ((N-n) - (k_i - i)) = n(N-n)$$

because the entries H_{j,k_i} $(j < k_{w^{-1}(i)})$ of the submatrix $\mathbf{L}_1$ and the entries $H_{k_i,j}$ $(j > k_{w(i)})$ of the submatrix L_2 run independently arbitrary values from the field F (when P, R, X, Z fixed).

Application of the theorem on dimensions of the layers to the morphism φ entails the estimations

$$\dim \mathscr{D} \geq n(N-n) + \dim \mathscr{C} \geq l(A) + \tfrac{1}{2}N(N+1).$$

Using this inequality and Proposition 12 we obtain that

$$l(C) = \dim(\mathscr{B}^{(N)} C \mathscr{B}^{(N)}) - \tfrac{1}{2}N(N+1) \geq \dim \mathscr{D} - \tfrac{1}{2}N(N+1) \geq l(A)$$

which was to be proved.

A.2. Generalized Bruhat decompositition and the monotony of the length of a substitution in the general case

We let $\mathscr{T}$ denote the variety of all not necessarily nonsingular uppertriangular matrices (i.e. the matrices with zeroes below the diagonal). Every $n \times n$ matrix A (not necessarily nonsingular) can be presented in the form $A = T_1 w T_2$ (see Proposition 14 below) where $w \in S_n$, T_1, $T_2 \in \mathscr{T}$. Unlike the nonsingular case (see Proposition 11 above) a substitution w is not necessarily unique. Nevertheless for every matrix A

there exists and can be effectively constructed (see Theorem 16 below) the unique substitution $w_A \in S_n$ such that $A \in \mathcal{T} w_A \mathcal{T}$ and $w_A \leq w$ (see Section A.1 of the appendix) for any $w \in S_n$ satisfying the condition $A \in \mathcal{T} w \mathcal{T}$. Set $l(A) = l(w_A)$. It will be shown in Theorem 19 based on Theorem 13 that $l(A) \leq l(C)$ for a main submatrix A of a matrix C.

For every $n_1 \times n_2$ matrix A we define the following auxiliary function $r_A(m, k)$ over the pairs of the natural numbers $0 \leq m \leq n_1$, $0 \leq k \leq n_2$. Set $r_A(m, k)$ (for $m, k \geq 1$) equal to the rank of the $m \times k$ submatrix $A^{(m,k)}$ (utilize this notation also further) of the matrix A situated in the lower left corner of A (i.e. $A^{(m,k)}$ is the submatrix of A situated at the intersection of the rows with the indices $n_1 - m + 1, \ldots, n_1$ and the columns with the indices $1, \ldots, k$). And set $r_A(0, k) = r_A(m, 0) = 0$. One can easily check the following properties of the function $r = r_A$:

(1) $0 \leq r(m, k) \leq \min\{m, k\}$;

(2) $r(m, k) \leq r(m+1, k) \leq r(m, k) + 1$, $r(m, k) \leq r(m, k+1) \leq r(m, k) + 1$;

(3) if $r(m+1, k) = r(m, k+1) = r(m, k) + 1$, then $r(m+1, k+1) = r(m, k) + 2$.

Definition. *An incomplete sample* is a matrix with the entries from the set $\{0, 1\}$; moreover each two unities stay in the different rows and in the different columns.

Proposition 14. (a) *For any function r satisfying the conditions* (1), (2) *and* (3) *formulated above, there exists the unique incomplete sample u such that $r = r_u$;*

(b) $r_{T_1 A T_2} \leq r_A$ *(inequality for the functions means inequality for all values of arguments) where $T_1, T_2 \in \mathcal{T}$, besides that $r_{B_1 A B_2} = r_A$ where $B_1, B_2 \in \mathcal{B}$;*

(c) *for every matrix A there exists (and can be easily constructed) the unique incomplete sample u_A such that $A = B_1 u_A B_2$ for some $B_1, B_2 \in \mathcal{B}$ (this entails in particular as a consequence the uniqueness of the substitution in Bruhat decomposition—see Proposition* 11 *in Section A.*1 *of the appendix*);

(d) *any $n \times n$ matrix A can be presented in the form $A = T_1 w T_2$ for some $w \in \mathbf{S}_n$ and $T_1, T_2 \in \mathcal{T}$.*

Proof. (a) Define the matrix u with the entries from $\{0, 1\}$ according to the following rules: set $u_{n_1 - m, k+1} = 1$ $(m, k \geq 0)$ iff $r(m, k) = r(m+1, k) = r(m, k+1) = r(m+1, k+1) - 1$.

We check at first that so defined matrix u is an incomplete sample. Observe that property (3) of the function r can be reformulated in the following manner: if $r(m+1, k) > r(m, k)$, then $r(m+1, k+1) > r(m, k+1)$; from this we deduce by induction on $(l - k)$ that $r(m+1, l) > r(m, l)$ when $l \geq k$ (or by analogous reformulation of property (3): if $r(m, k+1) > r(m, k)$, then $r(m+1, k+1) > r(m+1, k)$ and we obtain by induction that $r(l, k+1) > r(l, k)$ for $l \geq m$). Suppose that $u_{n_1 - m, k+1} = u_{n_1 - m, k'+1} = 1$ for some $k' > k$. Then according to the construction of u, the inequality $r(m+1, k+1) > r(m, k+1)$ is valid and hence property (3) of r entails the inequality $r(m+1, k') > r(m, k')$ but this contradicts to the equality

$u_{n_1-m,k'+1}=1$. Analogously, the assumption $u_{n_1-m,k+1}=u_{n_1-m',k+1}=1$ leads to a contradiction when $m'>m$. Thus the matrix u is an incomplete sample.

Now we deduce the equality $r_u(m,k)=r(m,k)$ by induction on m, k. Assume that the equalities $r_u(m',k')=r(m',k')$ are proved for all $m'\leq m+1$, $k'\leq k+1$ with the exception of the case $m'=m+1$, $k'=k+1$. Then check the equality $r_u(m+1, k+1)=r(m+1,k+1)$ by analysis of cases. As u is an incomplete sample, $r_u(m',k')$ is equal to the number of unities in the submatrix $u^{(m',k')}$.

(α) Let $r(m,k)=r(m+1,k)=r(m,k+1)$. As $r(m,k)=r_u(m,k)=r_u(m,k+1)=r_u(m+1,k)$ by the induction hypothesis, the last (the most right) column of the matrix $u^{(m,k+1)}$ is equal to zero; analogously the first (the most upper) row of this matrix is equal to zero. If $r(m+1,k+1)=r(m,k)$, then $u_{n_1-m,k+1}=0$ according to the construction of u and $r_u(m+1,k+1)=r_u(m,k)=r(m,k)=r(m+1,k+1)$, else if $r(m+1,k+1)=r(m,k)+1$, then $u_{n_1-m,k+1}=1$ according to the construction of u and $r_u(m+1,k+1)=r_u(m,k)+1=r(m,k)+1=r(m+1,k+1)$.

(β) Let $r(m,k+1)>r(m,k)$ or $r(m+1,k)>r(m,k)$. In any of these cases $u_{n_1-m,k+1}=0$ and the number of unities in the submatrix $u^{(m+1,k+1)}$ is equal to $r_u(m+1,k+1)=r_u(m,k)+(r_u(m+1,k)-r_u(m,k))+(r_u(m,k+1)-r_u(m,k))$.

The function r satisfies the same equality and so $r_u(m+1,k+1)=r(m+1,k+1)$ by the induction hypothesis.

The uniqueness of the incomplete sample u' satisfying the condition $r_{u'}=r$ follows from the above exposed construction of u and the fact that if $u'_{n_1-m,k+1}=1$ then $r_{u'}(m,k)=r_{u'}(m,k+1)=r_{u'}(m+1,k)=r_{u'}(m+1,k+1)-1$.

(b) The second part is obvious, the first part can be deduced from the second part taking into account that every matrix $T\in\mathcal{T}$ can be presented as a product of the matrices from $\mathcal{B}$ and of the singular diagonal matrices of the kind $e_{i,i}^{(-1)}=E-z_{i,i}^{(-1)}$ (remember the notations adopted in Section 2: $z_{ij}^{(\gamma)}$ is the matrix with the (i,j)-entry equal to γ and the other entries equal to zero, E is the unity matrix). It remains to observe that multiplication by the matrix $e_{i,i}^{(-1)}$ from the left or from the right does not increase the function r.

(c) The construction of the desired incomplete sample is close to the construction of the substitution in Proposition 11. Namely, execute elementary uppertriangular transformations over the rows of the matrix A according to the following rule as long as it is possible. If the first from the left nonzero entries of the ith and jth rows ($i<j$) are situated in the same kth column, then add to ith row the jth row multiplied by some suitable coefficient from the field F in order to let the (i,k)-entry vanish (a choice of a pair i,j is not necessarily unique). As a result of these transformations we obtain a matrix $A'=B_1A$ ($B_1\in\mathcal{B}$) in which the first nonzero entries of all nonzero rows are situated in mutually different columns. Define the incomplete sample $u=u_A$: we set $u_{i,j}=1$ iff the first from the left nonzero entry of the ith row is situated in the jth column. One can easily see that $u=A'B_2$ for some $B_2\in\mathcal{B}$.

If $A=B_1uB_2=B'_1u'B'_2$ for some incomplete samples u, u' and $B_1,B_2,B'_1,B'_2\in\mathcal{B}$, then (b) of the present proposition entails the equalities $r_A=r_u=r_{u'}$ from this and (a) of the present proposition the equality $u=u'$ can be deduced.

(d) Let $A = B_1 u B_2$ (see (c) of the present proposition). It is sufficient to present u in a form $u = T_1' w T_2'$. Complete arbitrarily the incomplete sample u by unities up to some substitution $w \in S_n$. Let $u = \sum_{1 \le l \le k} z^{(1)}_{i_l, j_l}$, then set $T_1' = \sum_{1 \le l \le k} z^{(1)}_{i_l, i_l}$, $T_2' = \sum_{1 \le l \le k} z^{(1)}_{j_l, j_l}$. The simple checking ends the proof of the proposition.

We assume in (a) of the following proposition that the field F is infinite. The formulation of the result of (b) of the following proposition does not depend on the choice of the field F, therefore this assumption is not essential for the result of (b).

Proposition 15. (a) *Let A be rectangular $n \times m$ matrix and $r_A \le r$ for some function r satisfying the above formulated conditions* (1), (2) *and* (3). *Then $A \in \overline{\{C : r_C = r\}}$ (as earlier the bar denotes the closure in Zariski topology in the space of all matrices)*;

(b) *For every pair of substitutions $w_1, w_2 \in S_n$ the relation $w_1 \le w_2$ (see Section A.1 of the appendix) is equivalent to the inequality $r_{w_1} \le r_{w_2}$.*

Proof. According to (a) and (c) of Proposition 14 one can assume that AS is equal to an incomplete sample u_A and besides that one can find the incomplete sample u such that $r_u = r$. Carry the proof by the induction on $m + n$.

We let $L = F[\varepsilon, \varepsilon^{-1}]$ denote the ring of Loran polynomials over one variable. Any $0 \ne p \in L$ can be uniquely presented in the form $p = \varepsilon^N p_1$ for some integer N and the usual polynomial p_1 over ε with nonvanished free term; the integer N is called the *degree* of p. The induction hypothesis consists in the following:

(α) Already the nonsingular uppertriangular $n \times n$ matrix B_1 and nonsingular uppertriangular $m \times m$ matrix B_2 (over the ring L), corresponding to $n \times m$ incomplete sample u_A and to the $n \times m$ incomplete sample u, are constructed;

(β) Each entry of the matrix $B_1 u B_2$ belongs to the ring $P = F[\varepsilon]$ of the usual polynomials;

(γ) the matrix $(B_1 u B_2)^{free}$, consisting of the free terms of the entries of the matrix $B_1 u B_2$, is equal to u_A.

The inductive step will consist in the construction of the matrices B_1', B_2' satisfying the conditions (α), (β) and (γ) and corresponding to the $(n+1) \times m$ incomplete sample u_A' obtained from u_A by adding of a first $1 \times m$ row d and to the $(n+1) \times m$ incomplete sample u' obtained from u by adding of a first $1 \times m$ row.

Let $s = r_A(n+1, m)$ be equal to the number of unities in the incomplete sample u_A', let $1 \le q_1 < \cdots < q_s \le m$ denote the indices of the columns containing these s unities. For every $1 \times m$ vector η we denote by $\eta^{(s)}$ the projection of the vector η on the space generated by the orts with the indices $q_1, \ldots, q_s$ (so $\eta^{(s)}$ is an $1 \times s$ vector). Let the unities of the incomplete sample u' be situated in the cells with the coordinates (t_1', t_1), $(t_2', t_2), \ldots$ where $1 \le t_1 < t_2 < \cdots$ and $1 \le t_i' \le n+1$, $1 \le t_i \le m$ for each i. The inequality $1 = r_A(n+1, q_1) \le r_{u'}(n+1, q_1)$ entails that $t_1 \le q_1$; then the inequality $2 = r_A(n+1, q_2) \le r_{u'}(n+1, q_2)$ entails that $t_2 \le q_2$; after that we obtain inequality $t_3 \le q_3$ etc.

We construct the matrix B_1' by adding some first row $(b_1, \ldots, b_m)$ (which will be defined below) to the matrix B_1; the matrix B_2' will be obtained from the matrix B_2 by some modification described below. Let θ_l $(1 \leqslant l \leqslant s)$ denote the row with the index t_l of the matrix B_2. Consider the $s \times s$ matrix G with the lth row equal to $\theta_l^{(s)}$ $(1 \leqslant l \leqslant s)$. So $G_{l,l}$ is equal to the (t_l, q_l)-entry of the matrix B_2. Consider also a matrix $G' = G + \varepsilon^M E$ for such a large natural number M that G' is nonsingular and besides that M is greater than the absolute value of the degree of each entry (with a negative degree) of the matrix B_1. Modify the matrix B_2 by adding the polynomial ε^M to any (t_l, q_l)-entry of B_2 for all $1 \leqslant l \leqslant s$ (so the modified matrix B_2 is uppertriangular as before because $t_l \leqslant q_l$; we preserve the same notation for the modified matrix B_2). Let $(\theta_l')^{(s)}$ denote the row with the index l $(1 \leqslant l \leqslant s)$ of the matrix G'.

For some natural number M_1 each entry of the matrix $G_1 = \varepsilon^{M_1} G'$ belongs to P. The matrix G_1 can be reduced by some sequence of elementary transformations over P to the diagonal form with nonzero entries at the diagonal. Therefore there exist $b_{t_1'}, \ldots, b_{t_s'} \in L$ such that

$$\left(\sum_{1 \leqslant l \leqslant s} b_{t_l'} (\theta_l')^{(s)} \right)^{\text{free}} = d^{(s)} \tag{8}$$

and moreover each coefficient of the vector $\sum_{1 \leqslant l \leqslant s} b_{t_l'} (\theta_l')^{(s)}$ belongs to P. We can assume that $b_{t_l'} \neq 0$ for all $1 \leqslant l \leqslant s$, adding if necessary to each $b_{t_l'}$ the polynomial ε^{M_2} for arbitrary natural number M_2 which is greater than the absolute value of the degree of every entry (with a negative degree) of the matrix B_2. Set all the other coefficients of the vector $(b_1, \ldots, b_m)$ equal to ε^{M_2}. Thus the matrix B_1' is defined.

Set each (t_i, j)-entry of the matrix B_2' equal to ε^{M_3} (when $t_i \leqslant j$, $1 \leqslant i \leqslant s$ and $j \neq q_l$ for all $1 \leqslant l \leqslant s$) where the natural number M_3 is greater than the absolute value of degree of every entry (with a negative degree) of the matrix B_1'. Preserve the other entries of the matrix B_2 without exchanging (remember that we consider the modified matrix B_2). This completes the description of the matrix B_2'.

According to the choice of the numbers M, M_3 the conditions (β), and (γ) are fulfilled for the submatrix $B_1 u B_2'$ of the matrix $B_1' u' B_2'$ (the polynomials containing only positive powers of ε have been added to the entries of the matrix $B_1 u B_2$ by the changes in the entries of the matrix B_2). Taking into account the choice of the vector $(b_1, \ldots, b_m)$ and of the numbers M_2, M_3, we obtain the conditions (β) and (γ) for the first row of the matrix $B_1' u' B_2'$ (the equality (8) and the choice of M_2 entail it for the coefficients of the first row with the coordinates $q_1, \ldots, q_s$; for all the other coefficients one can deduce this based on the choice of M_2 and M_3—these coefficients contain only positive powers of ε). That matrix B_1' is invertible, follows from non-vanishing of b_1.

Thus the conditions (α), (β) and (γ) are valid for the matrices B_1' and B_2' corresponding to the incomplete samples u_A', u'. We have considered the case when a row is added to each of the matrices u_A and u. Analogously the case of adding of a column can be considered.

The equality $r_{\mathbf{B}_1(\varepsilon)u\mathbf{B}_2(\varepsilon)} = r_u = r$ is fulfilled for almost arbitrarily fixed $\varepsilon \neq 0$ by the condition (α) and by (b) of Proposition 14, on the other hand the conditions (β) and (γ) entail that $u_A \in \overline{\{B_1(\varepsilon)uB_2(\varepsilon): \varepsilon \neq 0\}}$. This completes the proof of (a) of the present proposition.

(b) Consider the set $\mathcal{M} = \{A \in \mathrm{GL}_n: r_A \leq r_{w_2}\}$. It is closed in Zarisky topology in GL_n as the inequality $r_A \leq r_{w_2}$ is equivalent to the system $\mathcal{L}$ of vanishing of some minors of the matrix A (namely for every m, k, if $r_{w_2}(m, k) = g$, then insert into the system $\mathcal{L}$ all the minors of the sizes greater than g of the matrix $A^{(m,k)}$). (b) of Proposition 14 entails that $\overline{\mathcal{B}w_2\mathcal{B}} \subset \mathcal{M}$ and therefore $\overline{\mathcal{B}w_2\mathcal{B}} \subset \mathcal{M}$.

Conversely, the inclusion $\overline{\mathcal{B}w_2\mathcal{B}} \supset \mathcal{M}$ follows from (a) the present proposition.

The equality $\mathcal{M} = \overline{\mathcal{B}w_2\mathcal{B}} = \bigcup_{w \leq w_2} \mathcal{B}w_2\mathcal{B}$ is valid by the theorem of Chevalley on the structure of $\overline{\mathcal{B}w_2\mathcal{B}}$; from this equality one can easily deduce (b) of the present proposition.

Theorem 16 (Generalized Bruhat decomposition). *For arbitrary $n \times n$ matrix A there exists the unique substitution $w_A \in S_n$ such that $A \in \mathcal{T}w_A\mathcal{T}$, and for every $w \in S_n$ such that $A \in \mathcal{T}w\mathcal{T}$ the inequality $r_{w_A} \leq r_w$ is fulfilled (and so $w_A \leq w$ according to (b) of Proposition* 15).

Proof. Making use of (c) of Proposition 14, we can bound ourselves to the case that $A = u = \sum_{1 \leq l \leq m} z^{(1)}_{i_l j_l}$ is an $n \times n$ incomplete sample.

The construction of the substitution matrix w_u proceeds in two stages. The construction consists of finding of the cells in w_u in which entries equal to unities.

Stage 1: Construct the sequence of the incomplete samples $u_0 = u, u_1, \ldots$ such that for each q the matrix u_{q+1} is a submatrix of the matrix u_q (the matrix u_q is of the size $(n-q) \times (n-q)$). Assume that q steps of the first stage have proceeded and as a result of these steps the incomplete sample u_q has been constructed; and that in the not yet constructed to the end matrix w_u q unities are already put in some cells (at each step of the first stage one unity is put in some cell of w_u).

Before describing of $(q+1)$th step of the first stage we make a remark about the notations. If a matrix G is a submatrix of the matrix D, then each cell of the matrix G has coordinates in the matrix G and in the matrix D. So every time when misunderstandings can arise we define more precisely which coordinates are considered.

$(q+1)$th step of the first stage $(q \geq 0)$. Assume that $u_{ij} = 1$ (the choice of a cell (i, j) is not necessarily unique), moreover the cell (i, j) is situated also in the matrix u_q and has the coordinates $(i^{(q)}, j^{(q)})$ in u_q where $i^{(q)} \geq j^{(q)}$, in other words this cell is situated not above the diagonal in the matrix u_q. Then put unity at the cell (i, j) in the matrix w_u. The matrix u_{q+1} is obtained from the matrix u_q by eliminating its row with the index $i^{(q)}$ and its column with the index $j^{(q)}$. If there is no unity satisfying the formulated properties in the matrix u, then pass to the second stage of the construction of w_u not executing the $(q+1)$th step of the first stage. After execution of the $(q+1)$th step of the first stage we pass to the $(q+2)$th step.

Before describing the second stage, we observe the following useful property of the matrices u_q.

Lemma 17. *Let $l < q$. If a cell in the matrix u_q is situated not below the diagonal, then it is also in the matrix u_l situated not below the diagonal.*

It is sufficient to prove the lemma for the case $q = l+1$ (for the completion of the proof use the induction on $q-l$).

So let the matrix u_q be obtained from the matrix u_l by eliminating its row with index $i^{(l)}$ and its column with index $j^{(l)}$, where $(i^{(l)}, j^{(l)})$ are coordinates in the matrix u_l. Assume that a cell with the coordinates $(i_1^{(l)}, j_1^{(l)})$ of the matrix u_l is situated in the matrix u_q not below the diagonal. First we check that either $i_1^{(l)} < i^{(l)}$ or $j_1^{(l)} > j^{(l)}$. Suppose to the contrary that

$$i_1^{(l)} > i^{(l)}, \qquad j_1^{(l)} < j^{(l)}. \tag{9}$$

As $i^{(l)} \geqslant j^{(l)}$ according to construction at the first stage, $i_1^{(l)} \geqslant j_1^{(l)} + 2$. The cell with the coordinates $(i_1^{(l)}, j_1^{(l)})$ in the matrix u_l has the coordinates $(i_1^{(l)} - 1, j_1^{(l)})$ in the matrix u_q under the supposition (9). This contradicts the fact that this cell is situated in the matrix u_q not below the diagonal, i.e. $i_1^{(l)} - 1 \leqslant j_1^{(l)}$. Thus (9) is impossible.

The coordinates of the cell $(i_1^{(l)}, j_1^{(l)})$ under consideration are equal (in the matrix u_q) to

(α) $\quad (i_1^{(l)}, j_1^{(l)})$ if $i^{(l)} > i_1^{(l)}, j^{(l)} > j_1^{(l)}$

or

$$(\beta) \quad (i_1^{(l)}, j_1^{(l)} - 1) \quad \text{if} \quad i^{(l)} > i_1^{(l)}, j^{(l)} < j_1^{(l)} \tag{10}$$

or

(γ) $\quad (i_1^{(l)} - 1, j_1^{(l)} - 1)$ if $i^{(l)} < i_1^{(l)}, j^{(l)} < j_1^{(l)}$.

Based on the fact that this cell is situated in the matrix u_q not below the diagonal, we deduce that in each of these cases (α), (β) and (γ) this cell is situated in the matrix u_l also not below the diagonal. For instance $i_1^{(l)} \leqslant j_1^{(l)} - 1$ in case (β), consequently $i_1^{(l)} \leqslant j_1^{(l)}$. The lemma is proved.

We turn ourselves to the description of the second stage of the construction of w_u.

Stage 2: Let k steps of the first stage have proceeded and as a result an $(n-k) \times (n-k)$ incomplete sample u_k with all its unities situated above the diagonal has been constructed. Choose $(n-k)$ cells of the matrix u situated at the diagonal in the matrix u_k and complete the construction of the substitution w_u putting unities in these cells.

Let the unities put in w_u in the first stage successively be situated in the cells with the coordinates $(i_1, j_1), \ldots, (i_k, j_k)$ (one can easily see from the construction at the

first stage that the unities are situated in these cells in the matrix u, remember that $u = \sum_{1 \leq l \leq m} z^{(l)}_{i_l, j_l}$), i.e. the unity has been put in the cell with the coordinates (i_l, j_l) in the matrix w_u at the lth step. In the second stage the unities have been put in the cells with the coordinates $(p_1, t_1), \ldots, (p_{n-k}, t_{n-k})$ and moreover $p_1 < \cdots < p_{n-k}$, $t_1 < \cdots < t_{n-k}$ (here and further on, if the contrary is not specified, all the coordinates are understood as coordinates in the matrix w_u).

We show that $u = T_1 w_u T_2$ for some $T_1, T_2 \in \mathcal{T}$. If $m \geq l > k$, then the cell with the coordinates (i_l, j_l) is situated also in the matrix u_k, and as the entry of the matrix u (and therefore of the matrix u_k) in this cell is unity, the cell under consideration is situated in the matrix u_k above its diagonal (otherwise we should execute the $(k+1)$th step of the first stage not passing on to the second stage). Hence there exists a unique $1 \leq q_l \leq n-k$ such that $t_{q_l} = j_l$ and therefore the inequality $p_{q_l} > i_l$ is valid by force of the observed earlier. Introduce the matrix T_1 as the incomplete sample in which the unities are situated in the cells with the coordinates $(i_1, i_1), \ldots, (i_k, i_k)$ and in the cells with the the coordinates $(i_{k+1}, p_{q_{k+1}}), \ldots, (i_m, p_{q_m})$ (all the other entries are equal to zeros). Set T_2 equal to the unity matrix. The equality $u = T_1 w_u T_2$ can be checked immediately.

Now assume that $u \in \mathcal{T} w \mathcal{T}$ for some $w \in S_n$. Then (b) of Proposition 14 entails that $r_w \geq r_u$. Further on the inequality $r_{w_u} \leq r_w$ will be proved. Let $1 \leq f, g \leq n$. Prove the inequality $r_{w_u}(f, g) \leq r_w(f, g)$ by analysis of two cases.

Case 1: Suppose that an $f \times g$ submatrix $w_u^{(f,g)}$ of the matrix w_u contains only unities which have been put in the matrix w_u at the first stage of its construction.

Then the number of unities in the matrix $w_u^{(f,g)}$ is equal to $r_{w_u}(f, g) \leq r_u(f, g) \leq r_w(f, g)$ (the equality $r_{w_u}(f, g) = r_u(f, g)$ in fact in this case is fulfilled).

Case 2: Suppose that the incomplete sample $w_u^{(f,g)}$ contains $q > 0$ unities (situated in the cells with the coordinates $(p_{l+1}, t_{l+1}), \ldots, (p_{l+q}, t_{l+q})$ for some l) which have been put in w_u in the second stage of the construction and h unities which have been put in w_u in the first stage (consequently $r_{w_u}(f, g) = h + q$).

These assumptions entail the inequalities $p_l < n - f + 1 \leq p_{l+1}$ and $t_{l+q} \leq g < t_{l+q+1}$ (set $p_0 = 0$ and $t_{n-k+1} = n + 1$ by definition). There exist $p_{l+1} - (n - f + 1)$ unities in the matrix w_u situated in the cells with the values of the first coordinates between $(n - f + 1)$ and p_{l+1}; fix one of these unities situated in a cell with the coordinates (i, j), then $(n - f + 1) \leq i < p_{l+1}$. These $p_{l+1} - (n - f + 1)$ unities have been put in the first stage because the unities which have been put in the second stage cannot stay in the cells with the first coordinates strictly between p_l and p_{l+1}. Check the inequality $j < t_{l+1}$ for the pair (i, j) under consideration. Otherwise, as the cell with the coordinates (p_{l+1}, t_{l+1}) is situated at the diagonal in the matrix u_k, this cell is situated not below the diagonal in the matrix $u_{k'}$ by Lemma 17, where $(k' + 1)$ is the index of the step (of the first stage) at which the cell under consideration with the coordinates (i, j) has been eliminated. So this cell is situated above the diagonal in the matrix $u_{k'}$ which contradicts the construction in the first stage. Thus the considered $p_{l+1} - (n - f + 1)$ unities of the substitution w_u are situated in the matrix $w_u^{(f,g)}$ and obviously not in the matrix $C = w_u^{(n - p_{l+1} + 1, t_{l+q})}$.

Analogously $(g-t_{l+q})$ unities put in the matrix w_u in the first stage and situated in the cells with the values of the second coordinates greater than t_{l+q} and not greater than g are also situated in the matrix $w_u^{(f,g)}$ and not situated in the matrix C. So there are q unities in the matrix C put in w_u in the second stage and $h'=h-(p_{l+1}-(n-f+1))-(g-t_{l+q})$ unities put in the first stage.

The coordinates of the upper right cell of the matrix C are (p_{l+1}, t_{l+q}) and in the matrix u_k its coordinates are $(l+1, l+q)$. For each unity put in the matrix w_u in the first stage and situated in a cell with the coordinates (i_d, j_d) for some $1 \leq d \leq k$ either $i_d > p_{l+1}$ or $j_d < t_{l+q}$ is valid as the cell with the coordinates (p_{l+1}, t_{l+q}) is situated not below the diagonal in u_k and therefore this cell is situated not below the diagonal in the matrix u_{d-1} by Lemma 17. On the other hand the cell with the coordinates (i_d, j_d) is situated not above the diagonal in the matrix u_{d-1} (that contradicts to the conjunction of the inequalities $i_d < p_{l+1}, j_d > t_{l+q}$) according to the construction in the first stage. Observing $10(\alpha, \beta, \gamma)$ in the proof of Lemma 17, we obtain that for the cell with the coordinates (p_{l+1}, t_{l+q}) the difference between the values of its first and its second coordinate decreases by one, when transferring from the coordinates in the matrix u_{d-1} to the coordinates in the matrix u_d $(1 \leq d \leq k)$, only in case $10(\beta)$, i.e. when $i_d > p_{l+1}$ and $j_d < t_{l+q}$. This difference is not changed in the cases $10(\alpha, \gamma)$ (either $i_d > p_{l+1}$ or $j_d < t_{l+q}$ as has been proved earlier, therefore the difference under consideration cannot increase). The number of indices satisfying the conjunction of the inequalities $i_d > p_{l+1}, j_d < t_{l+q}$ is equal to the number of unities which have been put in the matrix w_u in the first stage and are situated in the matrix C. So this number is equal to h'.

As a result of these speculations we deduce the equality $q-1=(l+q)-(l+1)=(t_{l+q}-p_{l+1})-h'$, therefore $g+f-n=h+q$.

As $n=r_w(n,n) \leq r_w(f,g)+(n-f)+(n-g)$ by property (2) (just before Proposition 14) of the function r, $r_w(f,g) \geq f+g-n=h+q=r_{w_u}(f,g)$. This completes the analysis of the second case.

Thus we have shown that $r_{w_u} \leq r_w$ for every $w \in S_n$ such that $u \in \mathcal{T}w\mathcal{T}$ (this and (b) of Proposition 15 entail that $w_u \leq w$). The uniqueness of the substitution w_u is evident. Namely, if for some $w' \in S_n$ such that $u \in \mathcal{T}w'\mathcal{T}$ the inequality $r_{w'} \leq r_w$ is fulfilled for every $w \in S_n$ satisfying the condition $u \in \mathcal{T}w\mathcal{T}$, then $r_{w'}=r_{w_u}$ and hence $w'=w_u$ according to (a) of Proposition 14. This ends the proof of Theorem 16.

Remark. It can be deduced that $r_{w_A}(i,j)=\max\{i+j-n, r_A(i,j)\}$ (we shall not use this further). This equality determines uniquely the substitution w_A by (a) of Proposition 14.

Definition. The substitution w_A constructed in Theorem 16 will be called the *completion* of the matrix A; a decomposition $A=T_1 w_A T_2$ where $T_1, T_2 \in \mathcal{T}$ will be called *generalized Bruhat decomposition*. Set $l(A)=l(w_A)$. Then $l(A)=\min_{A \in \mathcal{T}w\mathcal{T}} l(w)$ by the preceding theorem.

It can be easily seen from the construction of w_A in the proof of Theorem 16 that w_A does not depend on the choice of a field F, i.e. w_A is preserved on its extension, and the matrices T_1, T_2 in the generalized Bruhat decomposition can be defined over the same field F as the matrix A. Therefore the function l does not depend on the field F. Assume an infiniteness of the field F in the following corollary.

Corollary 18.

(a) $$\overline{\mathcal{B}w\mathcal{B}} = \overline{\mathcal{T}w\mathcal{T}} = \bigcup_{w' \leq w} \mathcal{T}w'\mathcal{T} = \{A \in \mathcal{M}_n : r_A \leq r_w\}$$

for every $w \in S_n$ (remember that the bar over a set denotes its closure in Zariski topology in the variety $\mathcal{M}_n$ of all $n \times n$ matrices);

(b) *If* $\mathcal{Y} \subset \mathcal{M}_n$ *and* $A \in \bar{\mathcal{Y}}$, *then* $l(A) \leq \max_{Y \in \mathcal{Y}} l(Y)$ (*the semicontinuity of the function* l).

Proof. Consider, as in the proof of (b) of Proposition 15, the following closed subset: $\mathcal{M} = \{A \in \mathcal{M}_n : r_A \leq r_w\}$ of the variety $\mathcal{M}_n$. Obviously $\mathcal{M} \supset \mathcal{T}w\mathcal{T}$ (according to (b) of Proposition 14), consequently $\mathcal{M} \supset \overline{\mathcal{T}w\mathcal{T}}$.

If $A \in \mathcal{M}$, then Theorem 16 entails the inequality $r_{w_A} \leq r_w$ for the completion w_A of A. Therefore $w_A \leq w$ by (b) of Proposition 15 and $A \in \bigcup_{w' \leq w} \mathcal{T}w'\mathcal{T}$ as $A \in \mathcal{T}w_A\mathcal{T}$. Thus $\mathcal{M} \subset \bigcup_{w' \leq} \mathcal{T}w'\mathcal{T}$.

If $A \in \bigcup_{w' \leq w} \mathcal{T}w'\mathcal{T}$ and $A \in \mathcal{T}w'\mathcal{T}$ for some $w' \leq w$, then $r_A \leq r_{w'} \leq r_w$ according to (b) of Proposition 14 and to (b) of Proposition 15. Applying (a) of Proposition 15, we obtain that $\overline{\{C \in \mathcal{M}_n : r_C = r_w\}} \ni A$, and the equality $\{C \in \mathcal{M}_n : r_C = r_w\} = \mathcal{B}w\mathcal{B}$ follows from (a) and (b) of Proposition 14. Finally the inclusion $\bigcup_{w' \leq w} \mathcal{T}w'\mathcal{T} \subset \overline{\mathcal{B}w\mathcal{B}}$ completes the proof of (a) of the corollary.

(b) Theorem 16 entails that $\mathcal{Y} \subset \bigcup_{Y \in \mathcal{Y}} \mathcal{T}w_Y\mathcal{T}$. The equality $\overline{\bigcup_{Y \in \mathcal{Y}} \mathcal{T}w_Y\mathcal{T}} = \bigcup_{Y \in \mathcal{Y}} \overline{\mathcal{T}w_Y\mathcal{T}}$ is valid as there are in fact only a finite number of mutually distinguished sets among the sets $\{\mathcal{T}w_Y\mathcal{T}\}_{Y \in \mathcal{Y}}$. Based on this and on the (a) of the present corollary, we deduce the following chain:

$$A \in \bar{\mathcal{Y}} \subset \overline{\bigcup_{Y \in \mathcal{Y}} \mathcal{T}w_Y\mathcal{T}} = \bigcup_{Y \in \mathcal{Y}} \overline{\mathcal{T}w_Y\mathcal{T}} = \bigcup_{Y \in \mathcal{Y}} \bigcup_{w \leq w_Y} \mathcal{T}w\mathcal{T},$$

therefore $A \in \mathcal{T}w\mathcal{T}$ for some $w \leq w_Y$, $Y \in \mathcal{Y}$. Hence $w_A \leq w \leq w_Y$ and $l(A) = l(w_A) \leq l(w_Y) = l(Y)$ by Theorem 16.

As the formulation of the following theorem does not depend on the choice of the field F, we can, without loss of generality, assume that F is algebraically closed.

Theorem 19. *If* A *is a main submatrix of a matrix* C, *then* $l(A) \leq l(C)$.

Proof. Let A be an $n \times n$ matrix and C an $N \times N$ matrix. Denote by $\varphi : \mathcal{M}_N \to \mathcal{M}_n$ the natural projection 'obliging' the cells of an $N \times N$ matrix, which in the matrix C are situated outside its submatrix A (certainly $\varphi(C) = A$).

Let ψ denote the restriction of φ on the closed set $\overline{\mathcal{T}w_C\mathcal{T}}$ (φ is a regular morphism and so ψ is also a regular morphism, evidently $\psi(C) = A$). (a) of Corollary 18 entails that $E_N \in \overline{\mathcal{T}w_C\mathcal{T}}$ (we denote by E_N the unity $N \times N$ matrix). Of course $\psi(E_N) = E_n$, therefore the set $\mathcal{U} = \psi(\overline{\mathcal{T}w_C\mathcal{T}}) \cap \mathrm{GL}_n$ is not empty and open in Zariski topology of the constructive set $\psi(\overline{\mathcal{T}w_C\mathcal{T}})$.

The set $\mathcal{T}w_C\mathcal{T}$ is irreducible as the image of the irreducible set $\mathcal{T} \times \mathcal{T}$ (which is isomorphic to $F^{N(N+1)}$, under the regular morphism $(T_1, T_2) \to T_1 w_C T_2$, hence $\overline{\mathcal{T}w_C\mathcal{T}}$ is also irreducible (otherwise, if $\overline{\mathcal{T}w_C\mathcal{T}} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_d$ where each $\mathcal{V}_i$ is closed, then $\mathcal{V}_i \supset \overline{\mathcal{T}w_C\mathcal{T}}$ for some $1 \leq i_0 \leq d$ and consequently $\mathcal{V}_{i_0} = \overline{\mathcal{T}w_C\mathcal{T}}$).

As $\overline{\mathcal{T}w_C\mathcal{T}}$ is irreducible, $\mathcal{U}_1 = \psi^{-1}(\mathcal{U}) \cap \mathrm{GL}_N$ is an not empty, open and every where dense subset in $\overline{\mathcal{T}w_C\mathcal{T}}$. Check that $\psi(\mathcal{U}_1) \supset \psi(\overline{\mathcal{T}w_C\mathcal{T}})$. Otherwise the intersection $\mathcal{U}_1 \cap \psi^{-1}(\psi(\overline{\mathcal{T}w_C\mathcal{T}}) \setminus \overline{\psi(\mathcal{U}_1)})$ of two not empty open subsets of the set $\overline{\mathcal{T}w_C\mathcal{T}}$ is empty which contradicts the irreducibility of $\overline{\mathcal{T}w_C\mathcal{T}}$.

(a) of Corollary 18 entails that $l(C) \geq l(C')$ for any $C' \in \mathcal{U}_1 \subset \overline{\mathcal{T}w_C\mathcal{T}} = \bigcup_{w \leq w_C} \mathcal{T}w\mathcal{T}$. Then $C' \in \mathrm{GL}_N$, $\psi(C') \in \mathrm{GL}_n$ for every $C' \in \mathcal{U}_1$ and therefore $l(C') \geq l(\psi(C'))$ according to Theorem 13.

Based on the inclusion $A \in \overline{\psi(\mathcal{U}_1)} \cap \overline{\psi(\mathcal{T}w_C\mathcal{T})}$ shown above and the application of (b) of Corollary 18, we deduce that $l(A) \leq l(\psi(C'))$ for some $C' \in \mathcal{U}_1$ (actually this inequality is valid for almost all $C' \in \mathcal{U}_1$). Finally we obtain the inequality $l(A) = l(C)$, which was to be proved.

References

[1] N. Bourbaki, *Groupes et Algèbres de Lie. Deuxième Partie* (Hermanne, Paris, 1968).

[2] D.Yu. Grigor'ev, An application of separability and independence notions for proving lower bounds of circuit complexity, Notes of Scientific Seminars of Leningrad Branch of Mathematical Institute of Academy of Sciences of USSR **60** (1976) 38–48 (in Russian).

[3] J. Milnor, *Introduction to Algebraic K-theory* (Princeton University Press, Princeton NJ, 1971).

[4] J. Morgenstern, Note on a lower bound of the linear complexity of the fast Fourier transform, *J. ACM* **20** (2) (1973) 305–306.

[5] D. Mumford, *Introduction to Algebraic Geometry*, Harvard Lecture Notes, (Harvard University Press, Cambridge, MA, 1967).

[6] W.W. Peterson, *Error-Correcting Codes* (MIT Press and Wiley, New York/London, 1961).

[7] J.E. Savage, An algorithm for the computation of linear forms, *SIAM J. Comput.* **3** (2) (1974) 150–158.

[8] R. Steinberg, *Lectures on Chevalley Groups* (Yale University Press, New Haven, CT, 1967).

[9] M. Tompa, Time-space tradeoffs for computing functions using connectivity properties of their circuits, *Proc. 10th Annual ACM Symposium on Theory of Computing* (1978) 196–204.

[10] L.G. Valiant, On non-linear lower bounds in computational complexity, University of Leeds, Technical Report No. 61 (1975).

[11] L.G. Valiant, Some conjectures relating to super-linear complexity bounds, University of Leeds, Technical Report 85 (1976).

[12] D.Yu. Grigor'ev, An analogy of the Bruhat decomposition for the closure of the cone of a Chevalley group of the classical series, *Soviet Math. Dokl.* **23** (2) (1981) 393–397.