INFORMATIQUE THÉORIQUE ET APPLICATIONS

ST. WAACK

On the parallel complexity of linear groups

Informatique théorique et applications, tome 25, n° 4 (1991), p. 323-354

<http://www.numdam.org/item?id=ITA_1991__25_4_323_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 25, n° 4, 1991, p. 323 à 354)

ON THE PARALLEL COMPLEXITY OF LINEAR GROUPS (*)

by St. WAACK (1)

Communicated by J. BERSTEL

Abstract. – *The parallel complexity of the word problem of finitely generated (f.g.) linear groups over an arbitrary field is investigated. The computation model of Boolean circuits with fan-in bound 2 is used. It is shown that a f.g. linear group over a field of prime characteristic has a word problem solvable within depth* $\log n . \log\log n$ *using* $n^{O(1)}$ *gates. In the case of characteristic zero the somewhat weaker depth bound* $\log n . \log\log n . \log\log\log n$ *is shown. The word problem of a f.g. solvable-by-finite linear group is shown to belong to* NC^1. *Using a famous theorem due to Tits we get that each f.g. linear group which does not contain a noncyclic free group has an* NC^1 *word problem.*

Résumé. – *On étudie la complexité parallèle du problème des mots des groupes linéaires sur un corps arbitraire admettant un système de générateurs fini. Pour cela, on utilise des circuits booléens comme modèle de calcul. Il est démontré que les groupes linéaires sur un corps de caractéristique p possèdent un problème des mots résoluble en profondeur* $\log n . \log\log n$ *et un nombre* $n^{O(1)}$ *des portes. En caractéristique* 0, *on montre la profondeur* $\log n . \log\log n . \log\log\log n$, *qui est un peu plus faible. En outre, il est prouvé que le problème des mots d'une extension d'un groupe linéaire soluble admettant un système fini de générateurs par un groupe fini appartient à la classe* NC^1. *D'après un théorème célèbre de Tits, on obtient que chaque groupe linéaire admettant un système fini de générateurs et qui ne contient pas de sous-groupe libre non cyclique admet un problème des mots appartenant à* NC^1.

1. INTRODUCTION

Much effort has been done in the last years to study the complexity of word problems of finitely generated groups.

It was shown that there exist finitely presented groups where the word problems have any preassigned space complexity [29 to 32] improving an analogous result concerning so-called admissible complexity classes [2].

(*) Received April 1989, revised December 1990.
(1) Karl-Weierstraß-Institut für Mathematik, Postfach 1304, 0-1086 Berlin, Germany.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/91/04 323 32/$5.20/

In 1961, G. Higman proved the following remarkable theorem. A finitely generated group G can be embedded in some finitely presented group H if and only if G can be recursively presented. In [32] it is shown, that if G is recursively presented, the finitely presented extension group H of G can be choosen in such a way that the space complexity of the word problem is not enlarged. This improves the result obtained in [3].

In [17, 18] exponential lower bounds on the complexity of the word problem of free groups of finite rank are derived for restricted computation models.

Finite groups play an important role when studying small parallel complexity classes. Barrington proved, that the word problem of the symmetric group S_5 is p-complete for NC^1 [6].

Avenhaus and Madlener discussed several decision problems, for example the so-called Intersection Problem, and Nielsen reduction algorithms in free groups. It turns out that these problems are logspace complete for $\mathbb{P}$ [4, 5].

Lipton and Zalcstein proved that the word problem of a finitely generated linear group over a field of characteristic zero is solvable in logspace [21]. Simon proved an analogous result for fields of prime characteristic [26]. These results imply that the word problem of a finitely generated linear group over an arbitrary field belongs to NC^2.

In [33] the parallel complexity of some important constructions in combinatorial group theory is studied.

We show for a finitely generated linear group G over a field of prime-characteristic, that the word problem $W(G)$ of G belongs to U-SIZE, DEPTH $(n^{O(1)}, \log n . \log\log n)$. In the case of characteristic zero the depth bound is only $\log n . \log\log n . \log\log\log n$. This improves the above analogous result to some extend. If, moreover, G is solvable-by-finite, then $W(G) \in NC^1$. Using Tits' famous alternative [28] we obtain that the word problem of any finitely generated linear group has a word problem solvable in logdepth provided that it has no noncyclic free subgroup.

As corollaries we get, for example, that the word problem of a finitely generated free group belongs to U-SIZE, DEPTH $(n^{O(1)}, \log n . \log\log n)$, whereas the word problem of a finitely generated polycyclic group belongs to NC^1. This improves the result due to Lipton and Zalcstein in the case of polycyclic groups.

Although the word problem of a f.g. free group can be solved within logarithmic bounded parallel time by parallel random access machines, it is

unlikely because of Barringtons result [6] that it belongs to NC^1. Consequently, the word problem of a f. g. linear group which is not solvable-by-finite is probably not contained in NC^1.

Muller and Schupp gave a very interesting characterization of those groups which have context-free word problems [24]. In general it is known that context-free languages belong to NC^2. As to context-free word problems we show using the result of [24] and [13] that they are NC^1-equivalent to the word problem of a f. g. free group and consequently belong to U-SIZE, DEPTH $(n^{O(1)}, \log n . \log\log n)$.

2. PARALLEL COMPUTATION MODELL, WORD PROBLEMS

We assume familiarity with what might be termed "standard" complexity theory such as can be found in [16] and [34]. In particular, an $O(\log n)$ space-bounded deterministic Turing machine will be referred to as a logspace transducer having only inputs of the type 1^n in the context of circuits.

We adopt the usual definition of a fan-in two Boolean circuit family in which the n-th circuit has n inputs and $h(n)$ outputs where $h(n)$ is a nondecreasing polynomially bounded function. Observe, that with this definition depth $O(\log n)$ implies polynomial size.

We use the logspace uniformity of circuits, namely we require a logspace transducer be able to compute the description of the circuit family $\langle \alpha_n \rangle_{n \in \mathbb{N}}$ in the following way. Given the input 1^n it computes a description of the circuit α_n.

DEFINITION: (i) U-SIZE, DEPTH $(n^{O(1)}, d(n))$ is the set of all functions $f: \{0, 1\}^* \to \{0, 1\}^*$ computable by a uniform Boolean circuit family $\langle \alpha_n \rangle$ in which α_n has size polynomial in n and depth $O(d(n))$.

(ii) $NC^k = U$-SIZE, DEPTH $(n^{O(1)}, (\log n)^k)$,

$$NC = \bigcup_k NC^k.$$

We say that a function f is computable in logdepth if $f \in NC^1$.

Intuitively, NC is the set of functions computable superfast on a parallel computer of feasible size. The correspondence between uniform circuit size

and Turing machine classes is among others given by the inclusions

$$NC^1 \subseteq \mathbb{L}^* = DSPACE(\log n)^* \subseteq NC^2 \subseteq \ldots \subseteq NC \subseteq \mathbb{P}^*.$$

For details *see* [9 to 12].

For each problem we assume reasonably binary encoding of the problem instances. The letter n stands for the length of this encoding. Since we shall consider identities

$$T_1 . T_2 \cdot \ldots \cdot T_N - T_{N+1} . T_{N+2} \cdot \ldots \cdot T_{2N} = 0$$

in matrix rings (*see* Paragraph 4) and

$$w_1 w_2 \ldots w_N = 1$$

in groups, we have the number N as well. Obviously, n and N are polynomially related.

Following [12] in the context of a particular problem instance of binary length n, we say that an integer m is *tiny* if $|m| \leqq n^c$ where c is a constant. As to inputs, we assume that integers are specified in binary notations, except when an integer is tiny, in which unary notation is used. As to outputs, integers are represented in binary.

DEFINITION: The function $f: \{0, 1\}^* \to \{0, 1\}^*$ is NC^1 *reducible* to the function $g: \{0, 1\}^* \to \{0, 1\}^*$ if and only if there exists a logspace uniform circuit family $\langle \alpha_n \rangle$ which computes f with $\text{depth}(\alpha_n) = O(\log n)$ where, in addition to the usual gates, oracle nodes for g are allowed. An oracle node is a node which has some sequence $y_1, \ldots, y_u$ of input edges and some sequence $z_1, \ldots, z_v$ of output edges with associated function

$$(z_1, \ldots, z_v) = g(y_1, \ldots, y_u).$$

For the purpose of defining depth, the oracle node counts as depth $[\log(u+v)]$.

Now we mention some results concerning the parallel complexity of arithmetic operations, some of them we need later.

2.1. THEOREM (iterated addition) [8]: *Finding the sum of m integers of k bits each can be done by uniform circuits of size $(m.k)^{O(1)}$ and depth $O(\log m + \log k)$.* ■

2.2. THEOREM (multiplication, division) [8, 25]: *Let a and b be two m-bit integers.* NC^1 *contains the problem of computing $a \cdot b$, whereas computing $[a/b]$*

is contained in

$$U\text{-SIZE, DEPTH}(n^{O(1)}, \log n . \log\log n).$$

2.3. PROPOSITION [7]: *Let a be a any integer and let m be a tiny (relative to the problem size n of the encoding) integer. Computing $a \bmod m$ is contained in* NC^1.

2.4. THEOREM [7]: *Let $a_1, \ldots, a_r$ be any integers, and let m be a tiny integer.* NC^1 *contains the problem of computing $a_1 \cdot \ldots \cdot a_r \bmod m$.*

Now we turn to the algebraic backround of word problems. First we consider free groups. Let $A = \{a_1, \ldots, a_m\}$, $m \geqq 2$. Assume that $\langle A \rangle$ is the free group on A. Each element of $\langle A \rangle$ can be represented as word over the alphabet

$$A = A \,\square\, \{a_1^{-1}, \ldots, a_m^{-1}\}.$$

(The symbol "$\square$" denotes the disjoint union.) Given two words w_1 and w_2 over A. It is well-known that w_1 is freely equal to w_2, *i.e.* w_1 and w_2 define one and the same element in the group $\langle A \rangle$ iff w_1 can be transformed into w_2 by a finite sequence of the following rules:

(i) replace $a_i a_i^{-1}$ by 1; (ii) replace $a_i^{-1} a_i$ by 1; (iii) the inverse of (i); (iv) the inverse of (ii), where 1 denotes the empty word, which equals the neutral element of $\langle A \rangle$.

A word w is called *freely reduced* iff neither rule (i) nor rule (ii) can be applied to w. Each group element of $\langle A \rangle$ has a unique freely reduced representation over A.

In general, *a* group G is called recursively presented iff there are *a* finite set A and *a* recursive enumerable set $R = \{r_1, r_2, r_3, \ldots\} \subseteq A^*$ such that $G \cong \langle A \rangle / \mathrm{cl}(R)$, where $\mathrm{cl}(R)$ denotes the smallest normal subgroup containing the set R. We say that G has a recursive presentation $\langle A \mid R \rangle$ and we also write $G = \langle A \mid R \rangle$.

The word problem of $G = \langle A \mid R \rangle$ is the following language $W(\langle A \mid R \rangle) = \{w \in A^* \mid w = 1 \text{ in } G\}$. We remark that the complexity of $W(\langle A \mid R \rangle)$ does not depend an a special recursive presentation if only complexity classes are considered which are closed under NC^1 reductions. This follows from the fact that a homomorphism of finitely generated monoids can be computed within logdepth. Thus we are justified to speak about the complexity of the word problem of a group.

Let $G=\{x_1, x_2, \ldots, x_r \mid R\}$ be a recursive group presentation, let $H<G$ be a subgroup. Assume $1=g_1, g_2, g_3, \ldots$ be a representative system for right cosets modulo H in G, *i.e.* $G=\bigcup_i H.g_i$. Then for each element $g\in G$ there is a representative $\bar{g}\in\{g_1, g_2, g_3, \ldots\}$ such that $g=h.\bar{g}$, $h\in H$. The following theorem due to K. Reidemeister [22] is well-known.

2.5. THEOREM: (i) *The subgroup H is generated by words set*

$$\{g_i x_j (\overline{g_i x_j})^{-1} \mid i=1, 2, \ldots, j=1, 2, \ldots, r\}.$$

Especially it holds that

$$g_i x_j^{-1} (\overline{g_i x_j^{-1}})^{-1} = (\overline{g_i x_j^{-1}} x_j (\overline{g_i x_j^{-1}} x_j)^{-1})^{-1}.$$

(ii) *Let $w=x_{i_1}^{e_1}\cdot x_{i_2}^{e_2}\cdot \ldots \cdot x_{i_N}^{e_N}$, $e_j\in\{1, -1\}$ a word, which belongs to the subgroup H. Then w is equal to $\tilde{w}_1\cdot \ldots \cdot \tilde{w}_N$, where*

$$\tilde{w}_j = \overline{x_{i_1}^{e_1}\cdot x_{i_2}^{e_2}\cdot \ldots \cdot x_{i_{j-1}}^{e_{j-1}}}\cdot x_{i_j}^{e_j}\cdot \overline{x_{i_1}^{e_1}\cdot x_{i_2}^{e_2}\cdot \ldots \cdot x_{i_j}^{e_j}}^{-1}.$$ ■

It follows from 2.5 that if the subgroup H is of finite index in G, then H is finitely generated, too.

2.6. THEOREM (M. Hall [14]): *Let G be a finitely generated group. If H is a subgroup of finite index in G, then H contains a subgroup K characteristic (and consequently normal) in G with finite index in G.* ■

A group G is called *nilpotent* iff $G_d=1$, for some d. ($G_1=G$, $G_{i+1}=[G_i, G]$, where $[A, B]$ is the subgroup in a common extension of A and B generated by the commutators $[a, b]$, $a\in A$, $b\in B$.)

A group is called *solvable* iff there is a finite tower of groups $G=G_1>G_2>\ldots>G_d=1$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian. If G_i/G_{i+1} is cyclic, for each i, then G is called *polycyclic*.

A group is called *solvable-by-finite* iff it contains a solvable subgroup of finite index.

It is well-known that finitely generated nilpotent groups are polycyclic.

The following theorem was independently proved by Auslander [1] and Swan [27].

2.7. THEOREM: *Each polycyclic group has a faithful representation of finite degree over the ring of integers $\mathbb{Z}$.* ■

Let K be a field. $\mathrm{GL}(k, K)$ is the group of all invertible $k\times k$ matrices over K. Moreover, we consider the subgroup $T(k, K)$ of all upper triangular invertible matrices.

A group $G \leqq \mathrm{GL}(k, K)$ is called *triangularizable*, iff it is conjugate in $\mathrm{GL}(k, K)$ to a subgroup of $T(k, K)$.

It is an easy exercise to show that $T(k, K)$ is solvable. The following theorem due to Mal'cev [23] supplies an important information on the structure of solvable linear groups.

2.8. THEOREM: *A solvable linear group over an algebraic closed field K contains a triangularizable normal subgroup of finite index.* ■

2.9. REMARK: Let $A_1, A_2, \ldots, A_N \in \mathrm{GL}(k, K)$ be matrices, such that $A_i = (a_{j,l}^{(i)})_{j,l \in \{1, \ldots, k\}}$, and $A = (a_{j,l}) = A_1 \cdot A_2 \cdot \ldots \cdot A_N$. Then

$$a_{j,l} = \sum_{\mu} a_{j,\mu_1}^{(1)} a_{\mu_1,\mu_2}^{(2)} \ldots a_{\mu_{N-1},l}^{(N)}$$

where the sum ranges over all sequences

$$\mu = (\mu_1, \ldots, \mu_{N-1}) \in \{1, 2, \ldots, k\}^{N-1}.$$

If all A_i are upper triangular matrices, it is sufficient to take nondecreasing sequences μ only. The number of nondecreasing sequences belonging to $\{1, 2, \ldots, k\}^{N-1}$ is equal to $\binom{k+N-2}{N-1} = \binom{k+N-2}{k-1}$.

Now let us turn to a theorem which allows us to apply Mal'cev's Theorem in our context.

2.10. THEOREM: *Let G be a finitely generated group, and let $H < G$ be a subgroup of finite index.*

The word problem of G *is* NC^1*-equivalent to the word problem of H.*

Proof: The assertion $W(H) \leqq_{\mathrm{NC}^1} W(G)$ is clear. Let us turn to prove $W(G) \leqq_{\mathrm{NC}^1} W(H)$. By M. Hall's Theorem we may assume that H is a normal subgroup of the group G. Since our considerations do not depend on a special recursive presentation, we may select an appropriate one. We shall use the notations and assertions of Theorem 2.5.

Let $\langle x_1, x_2, \ldots, x_r \mid R \rangle$ be a recursive presentation of H. Let K be the finite quotient group G/H. K has a presentation given by the multiplication table, namely

$$\langle k_1, k_2, \ldots, k_s \mid k_i \cdot k_j = k_{l(i,j)}, k_1 = 1 \rangle.$$

Moreover, there is a homomorphism $\eta : G \to K$, $\ker \eta = H$. We fix elements $g_i \in G$, $i = 1, 2, \ldots, s$, such that $\eta(g_i) = k_i$, for $i = 1, 2, \ldots, l$, and $g_1 = 1$. The

set

$$\{g_1, g_2, \ldots, g_s\}$$

forms a representative system for the right cosets modulo H in G.

If $g \in G$, then $\bar{g}$ is the unique element g_i such that $\eta(g_i) = \eta(g)$.

The following relations are fulfilled in G.

$$g_i x_j g_i^{-1} = y_{i,j}, \qquad i = 1, \ldots, s, \qquad j = 1, \ldots, r$$
$$g_i g_j = z_{i,j} g_{l(i,j)}, \qquad i = 1, \ldots, s, \qquad j = 1, \ldots, r$$

where $y_{i,j}$ and $z_{i,j}$ belong to H, *i.e.* can be represented as words over $\{x_1, x_2, \ldots, x_r, x_1^{-1}, x_2^{-1}, \ldots, x_r^{-1}\}$. Now it is no problem to verify that G has the following presentation

$$\langle x_1, \ldots, x_r, g_1, \ldots, g_s \mid R, g_i x_j g_i^{-1} = y_{i,j}, g_i g_j = z_{i,j} g_{l(i,j)} \rangle.$$

We define the projection

$$\pi: \quad (\{x_1^{\pm 1}, \ldots, x_r^{\pm 1}\} \square \{g_1, \ldots, g_s\})^* \to \{g_1, \ldots, g_s\}^*$$

by

$$x_i^{\pm 1} \to g_1 \qquad \text{for} \quad i = 1, \ldots, r,$$
$$g_i \to g_i \qquad \text{for} \quad i = 1, \ldots, r,$$

and the bijection

$$\beta: \quad \{g_1, g_2, \ldots, g_s\}^* \to \{k_1, k_2, \ldots, k_s\}^*$$

by

$$g_i \to k_i \qquad \text{for} \quad i = 1, \ldots, r.$$

We observe that $\beta \circ \pi$ defines the group homomorphism η. Moreover, we have the multiplication map

$$\mu: \quad \{g_1, g_2, \ldots, g_s\}^* \to \{g_1, g_2, \ldots, g_s\}$$

defined by

$$\mu(g_{i_1} \cdot g_{i_2} \cdot \ldots \cdot g_{i_t}) = g_l \qquad \text{iff} \quad \eta(g_{i_1} \cdot g_{i_2} \cdot \ldots \cdot g_{i_t}) = k_l.$$

If $w \in (\{x_1^{\pm 1}, \ldots, x_r^{\pm 1}\} \square \{g_1, \ldots, g_s\})^*$, we get $\bar{w} = \mu \circ \pi(w)$.

We consider the input word

$$w = w_1 w_2 \ldots w_N \in (\{x_1^{\pm 1}, \ldots, x_r^{\pm 1}\} \square \{g_1, \ldots, g_s\})^N$$

of length N. We shall describe an NC^1-circuit using oracle nodes for the word problem of H which decides whether $w = 1$ in G. Before doing so we observe that

$$\tilde{w}_i = \begin{cases} \mu \circ \pi(w_1 \cdot \ldots \cdot w_{i-1})\, w_i\, (\mu \circ \pi(w_1 \cdot \ldots \cdot w_{i-1}))^{-1} & \text{if } w_i = x_i^{\pm 1} \\ z_{j_{i-1}, j_i} \quad \text{if } w_i = g_{j_i} \quad \text{and} \quad \mu \circ \pi(w_1 \cdot \ldots \cdot w_{i-1}) = g_{j_{i-1}}. \end{cases}$$

Step 1: We check whether w belongs to H. The method is to check the identity $(\beta \circ \pi)(w) = 1$ in K.

This can be done by iterated finite table look-up since the multiplication table of K is finite. Consequently $O(\log N) = O(\log n)$ depth is sufficient.

Step 2: We compute $\tilde{w}_i$, for all $i = 1, 2, \ldots, N$, in parallel. More precisely, computing $\tilde{w}_i$ means:

(i) checking whether or not $w_i \in \{x_1^{\pm 1}, \ldots, x_r^{\pm 1}\}$;

(ii) computing $\mu \circ \pi(w_1 \cdot \ldots \cdot w_{i-1}) = g_{j_{i-1}}$;

(iii) applying one of the relations $g_j x_k g_j^{-1} = y_{j,k}$ in the case of $w_i \in \{x_1^{\pm 1}, \ldots, x_r^{\pm 1}\}$, or applying one of the relations $g_i g_j = z_{i,j} \cdot g_{l(i,j)}$ in the case of $w_i \in \{g_1, \ldots, g_s\}$.

(i) can be done by a finite table look-up. Consequently, constant depth is enough. As to (ii) we remark, that it is similar to Step 1. Step 2 (iii) is again a finite table look-up.

Step 3: We take an oracle node for the word problem of H and check whether $\tilde{w}_1 \tilde{w}_2 \ldots \tilde{w}_N = 1$ in H.

Step 4: We accept iff the computations of Step 1 and Step 3 are accepting computations. ■

2.11. REMARK: We make use of finite tables in the proof of 2.10. For example, we have the multiplication table $\{k_i \cdot k_j = k_{l(i,j)}\}$ of the finite group K. Clearly, a logspace transducer can compute this table. Moreover, the transducer can describe a circuit which "looks up in the table" to find the element k_l corresponding to (k_i, k_j). If the table is finite, the look-up computation can be carried out in constant depth (finite table look-up).

The "look-up" process is a proper NC^1 computation in the more general case that for each input length n we have a table tab_n such that there is a

logspace transducer which computes the function $1^n \to \text{tab}_n$ (*see* [12]). Again we make use of this principle in 4.1.

Finally we mention finitely generated context-free group languages in this paragraph. A formal language L is called a *finitely generated context-free group language* if and only if $L = W(G)$ is a context-free word problem of a recursive presentation $G = \langle X \mid R \rangle$.

2.12. THEOREM: *A finitely generated group has a context-free word problem if and only if the group has a free subgroup of finite index.*

Proof: See [24] in connection with [13]. ■

2.13. THEOREM [34]: *A finitely generated free group is $\mathbb{Z}$-linear of degree two. Moreover, it has a faithful representation over a field of prime characteristic.*

2.14. THEOREM [28]: *A finitely generated linear group is either solvable-by-finite or contains a noncyclic free subgroup.*

3. SOMETHING FROM COMMUTATIVE ALGEBRA

The proofs in this paragraph which are not carried out can be found in [19]. A ring is always a commutative one if there is no different specification made.

NOTATIONS: We use the following nonstandard notations. If $X = (X_1, \ldots, X_m)$ is a vector of independent variables, Y another variable which is independent from the vector X, then $\mathbb{A}$ denotes the polynomial ring $\mathbb{Z}[X] = \mathbb{Z}[X_1, \ldots, X_m]$.

If p is a prime, and if as usual $\mathbb{F}_p$ is the prime field of characteristic p, then $\mathbb{A}_p$ denotes the ring $\mathbb{F}_p[X]$.

σ_p denotes the canonical ring homomorphism $\mathbb{A} \to \mathbb{A}_p$ resulting from the canonical projection $\mathbb{Z} \to \mathbb{F}_p$. This map can be extended to $\hat{\sigma}_p : \mathbb{A}[Y] \to \mathbb{A}_p[Y]$ in the natural way. The image of a polynomial $G(Y) \in \mathbb{A}[Y]$ under the homomorphism $\hat{\sigma}_p$ is frequently denoted by G^{σ_p}.

Let $\mathbb{F}_{p^r}$ be the finite field of characteristic p with p^r elements. Let $\zeta = (\zeta_1, \ldots, \zeta_m) \in \mathbb{F}_{p^r}^m$. Then we assign to each polynomial $G(X) \in \mathbb{A}$ an element $G(\zeta)$ of the finite field $\mathbb{F}_{p^r}$ which is obtained by substituting $(\zeta_1, \ldots, \zeta_m)$ for $(X_1, \ldots, X_m)$. We denote the resulting ring homomorphism $\mathbb{A}_p \to \mathbb{F}_{p^r}$ by ρ_ζ.

This map can again be extended to $\mathbb{A}_p[Y] \to \mathbb{F}_{p^r}[Y]$ which we denote by $\hat{\rho}_\zeta$.

3.1. On polynomials I

3.1.1. Let $\mathbf{R}$ be a ring. Then $M(k, \mathbf{R})$ is the ring of all $k \times k$ matrices over $\mathbf{R}$. $\mathrm{GL}(k, \mathbf{R})$ is the group of units of $M(k, \mathbf{R})$. If $\mathfrak{a}$ is an ideal of the ring $\mathbf{R}$, the radical $r(\mathfrak{a})$ of the ideal $\mathfrak{a}$ is defined to be $\{x \in \mathbf{R} \mid x^k \in \mathfrak{a}, \text{ for some } k \geqq 1\}$. The radical of an ideal is again an ideal in the ring $\mathbf{R}$. Obviously, we have a ring homomorphism $\mathbf{R}/\mathfrak{a} \to \mathbf{R}/r(\mathfrak{a})$.

Let $\psi : \mathbf{R} \to \mathbf{S}$ be a ring homomorphism. Then we have a homomorphism of noncommutative rings $M(k, \mathbf{R}) \to M(k, \mathbf{S})$ defined by $(r_{i,j}) \to (\psi(r_{i,j}))$. If we restrict this homomorphism to $\mathrm{GL}(k, \mathbf{R})$, we get a group homomorphism $\mathrm{GL}(k, \mathbf{R}) \to \mathrm{GL}(k, \mathbf{S})$.

If $\mathfrak{a}$ is an ideal in $\mathbf{R}$, the extension $\mathfrak{a}^e$ of $\mathfrak{a}$ is defined to be the ideal in $\mathbf{S}$ generated by $\psi(\mathfrak{a})$. Obviously, ψ induces a ring homomorphism $\bar{\psi} : \mathbf{R}/\mathfrak{a} \to \mathbf{S}/\mathfrak{a}^e$. The extension of a principle ideal generated by an element $r \in \mathbf{R}$ is again a principle ideal generated by $\psi(r)$.

Let $\mathbf{K}$ be a field,

$$F(Y) \in \mathbf{K}[Y], \qquad F(Y) = Y^{\delta} + \sum_{i=0}^{\delta-1} f_i . Y^i$$

be a polynomial. Let $\mathfrak{a} = F(Y).\mathbf{K}[Y]$. Since $\mathbf{K}[Y]$ is a principle ideal domain, $r(\mathfrak{a})$ is a principle ideal. Let $\bar{F}(Y)$ be the uniquely determined generator of $r(\mathfrak{a})$ with leading coefficient 1. Assume that $\mathbf{K}$ is the splitting field of F, *i.e.* F is assumed to split over $\mathbf{K}$ into linear factors. Then $\bar{F}(Y)$ is determined by the following two properties,

(i) If α is a root of $F(Y)$, then α is a root of $F(Y)$ and vice versa.

(ii) $\bar{F}(Y)$ is a separable polynomial, *i.e.* it has no multiple roots. Obviously, if $F(Y)$ is separable, then $r(\mathfrak{a}) = \mathfrak{a}$.

3.1.2. Let $\mathbf{R}$ and $\mathbf{S}$ be entire rings, and let $\psi : \mathbf{R} \to \mathbf{S}$ be a ring homomorphism. Let $F(Y) = Y^{\delta} + \sum_{i=0}^{\delta-1} f_i . Y^i$ be an element of $\mathbf{R}[Y]$. The discriminant is defined to be

$$\mathscr{D}(F) = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \ldots, \alpha_{\delta}$ are the not necessarily distinct roots of the polynomial F in an algebraic closure of the quotient field of R. Obviously, the polynomial F is separable iff $\mathscr{D}(F)$ is different from O. $\mathscr{F}(F)$ is a symmetric function in the roots $\alpha_1, \ldots, \alpha_{\delta}$. Consequently, $\mathscr{D}(F)$ can be expressed as a polynomial

in the elementary symmetric functions which are up to sign the coefficients of the polynomial F. We get that $\mathcal{D}(F)$ can be represented as a polynomial in $f_0, \ldots, f_{\delta-1}$ with integer coefficients, and consequently $\mathcal{D}(F^{\psi}(Y)) = \psi(\mathcal{D}(F))$.

3.1.3. *The Euclidean Algorithm:* Let $G[Y] \in \mathbf{R}(Y)$ be another polynomial. Then there are unique polynomials $\mathbf{Q}(Y), \mathbf{R}(Y) \in \mathbf{R}[\mathbf{Y}]$ such that $G = F \cdot Q + R$ and the degree of R is less than δ.

3.1.4. LEMMA: *Let* $\mathfrak{a} = F(Y) \cdot \mathbf{R}[Y]$ *be the principle ideal generated by* $F(Y)$. *Define the matrix* $B(F)$ *to be*

$$\begin{pmatrix} 0 & 0 \ldots 0 & -f_0 \\ 1 & 0 \ldots 0 & -f_1 \\ 0 & 1 \ldots 0 & -f_2 \\ \vdots & \vdots \quad \vdots & \vdots \\ 0 & 0 \ldots 1 & -f_{\delta-1} \end{pmatrix}$$

Let $R(Y), P(Y) \in \mathbf{R}[Y]$ *be polynomials such that*

(i) $P(Y) = \sum_{i=0}^{M} p_i \cdot Y^i, \qquad M \geqq \delta - 1$

(ii) $R(Y) = \sum_{i=0}^{\delta-1} r_i \cdot Y^i = P(Y) \bmod F(Y).$

Then

$$\begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{\delta-2} \\ r_{\delta-1} \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{\delta-2} \\ p_{\delta-1} \end{pmatrix} + \sum_{i=1}^{M-\delta+1} [B(F)]^i \cdot \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ p_{\delta+i-1} \end{pmatrix}.$$

Proof: By 3.1.3 $\mathbf{R}[Y]/\mathfrak{a}$ is a free $\mathbf{R}$-module of rank δ. The sequence $1, Y, Y^2, \ldots, Y^{\delta-1}$ forms a basis. The element Y supplies an $\mathbf{R}$-endomorphism φ of the R-module $\mathbf{R}[Y]/\mathfrak{a}$. The matrix $B(F)$ represents this endomorphism with respect to the basis $1, Y, Y^2, \ldots, Y^{\delta-1}$. It remains to remark that $\varphi^i(p_{\delta+i-1} \cdot Y^{\delta-1}) = p_{\delta+i-1} \cdot Y^{\delta+i-1}$. ■

3.1.5. LEMMA (Lipton's Interpolation Lemma [20]): *Let* $\mathbf{K}$ *be a field, and let* $g(X_1, X_2, \ldots, X_m) \in \mathbf{K}[X_1, X_2, \ldots, X_m]$. *Assume that the degree of* g *in each variable* X_i *is bounded by* τ_i. *Let, for* $i = 1, \ldots, m$, $T_i \subseteq \mathbf{K}$, *such that*

$|T_i| > \tau_i$. *Define* $T = T_1 \times T_2 \times \ldots \times T_m \subseteq \mathbf{K}^m$. *Then* g *is identical to* 0 *if and only if* $g(t) = 0$, *for all* $t \in T$.

3.2. Separable field extensions

3.2.1. THEOREM: *If* k *is a perfect field, any finitely generated field extension* K *of* k *contains a separating transcendence base which can be selected from any set of generators of* K *over* k.

Proof: See [36], Chap II, Theorem 30 and Theorem 31. ■

Remark: It is well-known that prime fields are perfect. Remember that if we have an extension $k \subseteq K$ of a field k, a transcendence base $\{X_i\}$ of K/k is called a *separating transcendence base* iff K is a separable algebraic extension of $k(\{X_i\})$.

3.2.2. THEOREM (Theorem of the Primitive Element): *Let* K *be a finite separable extension field of the field* k. *Then there is an element* $\alpha \in K$ *which generates* K *as an extension field of* k, i.e. $K = k(\alpha)$. ■

3.2.3. PROPOSITION: *Let* α *be algebraic over* k, *and let* $F(Y)$ *be the irreducible polynomial (with leading coefficient* 1*) of* α *over* k. $k(\alpha)$ *is a separable algebraic extension of* k *if and only if* $F(Y)$ *has no multiple roots* (i.e. F *is a separable polynomial*). ■

3.2.4. Let P be a prime field, K be a finitely generated extension field of P. We use 3.2.1 up to 3.2.3. There is a transcendence base $X = (X_1, X_2, \ldots, X_m)$ and an element y such that

$$K = P(X_1, X_2, \ldots, X_m)[y].$$

If $F(Y) = Y^\delta + \sum_{i=0}^{\delta-1} f_i . Y^i$ is the minimal polynomial of y over $P(X)$, then F is separable. Define

$$\mathbf{B} = \begin{cases} \mathbb{A} = \mathbb{Z}[X] & \text{if } \chi(K) = 0 \\ \mathbb{A}_p = \mathbb{F}_p[X] & \text{if } \chi(K) = p. \end{cases}$$

We may choose the primitive element y in such a way that its minimal polynomial $F(Y)$ has coefficients belonging to $\mathbf{B}$.

Define $\mathfrak{b} = F(Y) \cdot \mathbf{B}[Y]$, which is an ideal in $\mathbf{B}[Y]$. Then K is the quotient field of $\mathbf{B}[y] = \mathbf{B}[Y]/\mathfrak{b}$. More precisely, we get using the Euclidean Algorithm the following. Each element from K can be represented as a fraction $G(Y)/g$,

where $G(Y) \in \mathbf{B}[Y]$, $g \in \mathbf{B}$, the degree of $G(Y)$ in Y is less than δ, and since $\mathbf{B}$ is factorial the coefficients of G and g are coprime. This representation is unique up to multiplications by units of $\mathbf{B}$.

3.3. Finite fields

3.3.1. Let p be a prime number. Let $\mathbb{F}_p = \mathbb{Z}/p \cdot \mathbb{Z}$. In a fixed algebraic closure of $\mathbb{F}_p$ there is exactly one Galois field $\mathbb{F}_{p^r}$, for each natural number r, which has exactly p^r elements. It is the splitting field of the polynomial $Z^{p^r} - Z$. Hence $\mathbb{F}_{p^r}$ is a normal extension of $\mathbb{F}_p$. Moreover, it is separable. The multiplicative group $(\mathbb{F}_{p^r})^*$ is cyclic.

If $\mathbb{F}_{p^s}$ is another Galois field of characteristic p, then we have a tower of finite extensions

$$\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$$

if and only if r divides s.

The Galois field $\mathbb{F}_{p^r}$ can be represented as follows. Since $\mathbb{F}_{p^r}$ is the unique extension of $\mathbb{F}_p$ of degree r, for any irreducible polynomial $\Phi_{p,r}(Z) \in \mathbb{F}_p[Z]$ of degree r we have

$$\mathbb{F}_{p^r} = \mathbb{F}_p[Z]/(\Phi_{p,r}(Z) \cdot \mathbb{F}_p[Z]).$$

Moreover, all these polynomials $\Phi_{p,r}(Z)$ are separable ones. Because of the fact that the extension $\mathbb{F}_p \subset \mathbb{F}_{p^r}$ is normal, each irreducible polynomial $\Psi(Z) \in \mathbb{F}_p[Z]$ the degree of which divides r splits over $\mathbb{F}_{p_r}$ into linear factors.

Let δ be a positive natural number. Define $\delta^* = \text{l. c. m. } (1, \ldots, \delta)$. It follows from the above considerations that $\mathbb{F}_{p^{\delta^*}}$ is the splitting field of all polynomials of degree less than or equal to δ with coefficients in $\mathbb{F}_p$.

By the Euclidean Algorithm each element of $\mathbb{F}_{p^r}$ can be uniquely represented by a polynomial with coefficients in $\mathbb{F}_p$ of degree less than r.

3.3.2. Addition in $\mathbb{F}_{p^r}$ can be carried out by componentwise addition of the (natural) coefficients modulo the prime p.

3.3.3. As to multiplication in $\mathbb{F}_{p^r}$ we have the following situation. Let ω be a generator of the cyclic group $(\mathbb{F}_{p^r})^*$. To each nonzero element α of $\mathbb{F}_{p^r}$ we assign a discrete logarithm $l_\omega(\alpha)$ with respect to ω such that $\omega^{l_\omega(\alpha)} = \alpha$.

If we consider a product $\alpha_1 \cdot \ldots \cdot \alpha_N$, and if all factors α_i are different from 0, we can compute the product as follows.

(i) Compute the discrete logarithm $l_\omega(\alpha_i)$ for all factors.

(ii) Compute $\sum l_\omega(\alpha_i) \bmod p^r - 1$.

(iii) Compute the element of $\mathbb{F}_{p^r}$ which belongs to the number resulting from Step (ii).

3.3.4. LEMMA: *Let $D(X_1, X_2, \ldots, X_m) \in \mathbb{A}_p$ be a nonzero polynomial. Assume that the degree of D in any variable X_j is bounded above by θ. Let $M \in \mathbb{N}$. Assume that $p^r \geqq M^{m-1} \cdot \theta + M$.*

Then there are subsets $T_i \subseteqq \mathbb{F}_{p^r}$, $|T_i| \geqq M$, $i = 1, 2, \ldots, m$, such that the polynomial $D(X)$ has no root belonging to $T_1 \times \ldots \times T_m$.

Proof. – We prove the claim by induction on the number of variables.

Case: $m = 1$.

Let $D(X_1)$ be a polynomial of degree $\leqq \theta$. Hence D has in $\mathbb{F}_{p^r}$ at most θ roots. Since $|\mathbb{F}_{p^r}| = p^r \geqq M + \theta$, the claim follows.

Case $m \nearrow m+1$.

Consider $D(X_1, X_2, \ldots, X_m, X_{m+1}) = \sum_{i=0}^{\theta} d_i(X_1, \ldots, X_m) \cdot X_{m+1}^i$. There is an index i_0 with $d_{i_0}(X_1, \ldots, X_m)$ different from 0. Since

$$p^r \geqq M^m \circ \theta + M > M^{m-1} \cdot \theta + M,$$

there are subsets $T_1, T_2, \ldots, T_m \subseteqq \mathbb{F}_{p^r}$, $|T_i| = M$, such that

$$D(t_1, t_2, \ldots, t_m, X_{m+1})$$

is not the zero polynomial, for all $t_i \in T_i$. Each of these M^m polynomials has at most θ roots in $\mathbb{F}_{p^r}$. Hence $\mathbb{F}_{p^r}$ has at least M elements which are not such a root. Define T_{m+1} to be this set. ■

3.3.5. Let $F(Y) = Y^\delta + \sum_{i=0}^{\delta-1} f_i \cdot Y^i \in \mathbb{F}_p[Y]$ be a polynomial. Define δ^* to be l.c.m. $(1, 2, \ldots, \delta)$, and assume that δ^* divides r. Then $F(Y)$ splits over $\mathbb{F}_{p^r}$ into linear factors. Define α to be $F(Y) \cdot \mathbb{F}_{p^r}[Y]$. Let $\bar{F}[Y]$ be the polynomial with leading coefficient 1 (*see* 3.1.1) such that $r(\alpha) = \bar{F}[Y] \cdot \mathbb{F}_{p^r}[Y]$.

In particular, we have that if F is separable, F equals $\bar{F}$.

LEMMA (Evaluation-Interpolation): *Assume* $\alpha_1, \alpha_2, \ldots, \alpha_\Delta \in \mathbb{F}_{p^r}$ *to be the pairwise different roots of the polynomial* $\bar{F}$. *Define* $A(\bar{F})$ *to be*

$$\begin{pmatrix} 1, & \alpha_1, & \alpha_1^2, & \ldots, & \alpha_1^{\Delta-1} \\ 1, & \alpha_2, & \alpha_2^2, & \ldots, & \alpha_2^{\Delta-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1, & \alpha_\Delta, & \alpha_\Delta^2, & \ldots, & \alpha_\Delta^{\Delta-1} \end{pmatrix}.$$

Then:

(i) $\det(A(\bar{F})) = \prod_{i<j} (\alpha_j - \alpha_i)$, *and consequently* $A(\bar{F})$ *is invertible.*

(ii) *Let* $G(Y) \in \mathbb{F}_{p^r}[Y]$ *be another polynomial. By the Euclidean Algorithm there are unique polynomials* $Q(Y)$, $R(Y) \in \mathbb{F}_{p^r}[Y]$ *such that* $G = \bar{F}.Q + R$, *and the degree of* R *is less than* Δ.

If

$$R(Y) = \sum_{i=0}^{\Delta-1} r_i . Y^i$$

then

$$\begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{\Delta-2} \\ r_{\Delta-1} \end{pmatrix} = [A(\bar{F})]^{-1} . \begin{pmatrix} G(\alpha_1) \\ G(\alpha_2) \\ \vdots \\ G(\alpha_{\Delta-1}) \\ G(\alpha_\Delta) \end{pmatrix} = [A(\bar{F})]^{-1} . \begin{pmatrix} R(\alpha_1) \\ R(\alpha_2) \\ \vdots \\ R(\alpha_{\Delta-1}) \\ R(\alpha_\Delta) \end{pmatrix}$$

(Interpolation-Formula)

and

$$\begin{pmatrix} R(\alpha_1) \\ R(\alpha_2) \\ \vdots \\ R(\alpha_{\Delta-1}) \\ R(\alpha_\Delta) \end{pmatrix} = A(\bar{F}) . \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{\Delta-2} \\ r_{\Delta-1} \end{pmatrix}$$

(Evaluation-Formula)

(iii) *The map* $\mathbb{F}_{p^r}[Y]/(\bar{F}(Y).\mathbb{F}_{p^r}[Y]) \to (\mathbb{F}_{p^r})^{\Delta}$ *defined by*

$$R(Y) \to \begin{pmatrix} R(\alpha_1) \\ R(\alpha_2) \\ \vdots \\ R(\alpha_{\Delta-1}) \\ R(\alpha_{\Delta}) \end{pmatrix}$$

is an isomorphism of rings.

Proof: Claim (i) is standard. Claim (ii) follows from claim (i), the Euclidean Algorithm, and the well-known fact that a polynomial over an entire ring of degree less than Δ is uniquely determined by its values on a set of cardinality Δ. Claim (iii) follows from (i) and (ii). ■

3.4. On polynomials II

In addition to the general agreement of this paragraph let us introduce the following notation. Let $\mathbf{B}$ be either $\mathbb{A}$ or $\mathbb{A}_p$.

As usual let $F(Y) \in \mathbf{B}[Y]$ be the following polynomial

$$F(Y) = Y^{\delta} + \sum_{i=0}^{\delta-1} f_i \cdot Y^i.$$

The coefficients of F are polynomials $f_i = f_i(X_1, \ldots, X_m)$ either with integer coefficients or with coefficients in $\mathbb{F}_p$.

Define the ideal $\mathfrak{b}$ in $\mathbf{B}[Y]$ to be $F(Y) \cdot \mathbf{B}[Y]$. If we consider an element of the ring $\mathbf{B}[Y]/\mathfrak{b}$, we shall always assume that it is given by its unique representative $\sum_{i=0}^{\delta-1} g_i . Y^i$ of degree less than δ (*see* 3.1.3, 3.2.4).

3.4.1. LEMMA: *Let* $A_1, A_2, \ldots, A_N \in \mathrm{GL}(k, \mathbf{B}[Y]/\mathfrak{b})$. *Let* $F(Y) \in \mathbf{B}[Y]$ *as before.*

(*i*) *If for all entries*

$$P(Y) = \sum_{i=0}^{\delta-1} p_i(X) . Y^i$$

of the matrices $A_1, A_2, \ldots, A_N$ *the degree of* $p_i(X)$ *as well as of* $f_i(X)$ *in* X_j *is bounded by* τ, *for* $i=1, 2, \ldots, \delta-1, j=1, 2, \ldots, m$, *then for all entries*

$$Q(Y)=\sum_{i=0}^{\delta-1} q_i(X)\cdot Y^i$$

of the product $A_1\cdot A_2\cdot \ldots \cdot A_N$ *in* $\mathrm{GL}(k, \mathbf{B}[Y]/\mathfrak{b})$ *the degree of* $q_i(X)$ *in* X_j *is bounded by* $\tau\cdot\delta\cdot N$, *for all* i, j *under consideration.*

(ii) *If, moreover,* $\mathbf{B}=\mathbb{A}$, *and if the integer coefficients of* $p_i(X)$, $i=1, 2, \ldots, \delta-1$, *are bounded in absolute value by* γ, *the coefficients of* $q_i(X)$ *are bounded in absolute value by* $2^{\chi\cdot N}$, *where* χ *is a number which does not depend on* N.

Proof: The proof is pure routine. It proceeds in two steps. In the first step we consider the matrices A_i to be over $\mathbf{B}[Y]$ and multiply them. Secondly we apply 3.1.4 to compute the representative mod $F(Y)$. The details are omitted. ■

3.4.2. Lemma: *Let* $\mu(M)=\prod p$, *where the product ranges over all primes* $p \leqq M$.

There is a constant λ *such that* $\mu(M) \geqq 2^{\lambda\cdot M}$.

Proof: See [15]. ■

3.5. The correctness Lemmas

The aim of this section is to prove two lemmas which ensure the correctness of the algorithms of Paragraph 4. Let

$$\Psi_N(T_1, T_2, \ldots, T_{2N})=T_1\cdot T_2\cdot \ldots \cdot T_N - T_{N+1}\cdot T_{N+2}\cdot \ldots \cdot T_{2N},$$

$N\in\mathbb{N}$, a sequence of polynomials belonging to $\mathbb{Z}[\{T_i \mid i\in\mathbb{N}\}]$.

Let us turn to the first lemma. Let $F(Y)\in\mathbb{A}[Y]$

$$F(Y)=Y^{\delta}+\sum_{i=0}^{\delta-1} f_i(X)\cdot Y^i$$

be a *separable polynomial.* Let $\mathscr{D}(F)\in\mathbb{A}$ be the nonzero discriminant of F. Let $co(\mathscr{D}(F))$ be the least common multiple of the integer coefficients of $\mathscr{D}(F)$ regarded as a polynomial in X.

If $\mathfrak{b} = F(Y) \cdot \mathbb{A}[Y]$ is the ideal in $\mathbb{A}[Y]$ generated by $F(Y)$, if p is a prime, and if $\sigma_p : \mathbb{A}[Y] \to \mathbb{A}_p[Y]$ is the canonical projection, then we define $\mathfrak{b}_p$ to be $\mathfrak{b}^e = F^{\sigma_p}(Y) \cdot \mathbb{A}_p[Y]$, and we have $\bar{\sigma}_p : \mathbb{A}[Y]/\mathfrak{b} \to \mathbb{A}_p[Y]/\mathfrak{b}_p$ (*see* 3.1.1).

NOTATION: The image of a matrix $A \in \mathrm{GL}(k, \mathbb{A}[Y]/\mathfrak{b})$ under the canonical map $\mathrm{GL}(k, \mathbb{A}[Y]/\mathfrak{b}) \to \mathrm{GL}(k, \mathbb{A}_p[Y]/\mathfrak{b}_p)$ resulting from $\bar{\sigma}_p$ (*see* 3.3.1) is denoted by $A^{(p)}$.

3.5.1. LEMMA: *Let* $A_1, A_2, \ldots, A_{2N} \in \mathrm{GL}(k, \mathbb{A}[Y]/\mathfrak{b})$ *be matrices such that the assumptions of* 3.4.1 *are fulfilled.*

Then (i) $\Psi_N(A_1, A_2, \ldots, A_{2N}) = 0$ *iff* $\Psi_N(A_1^{(p)}, A_2^{(p)}, \ldots, A_{2N}^{(p)}) = 0$, *for all primes* p, *where* p *does not divide* $co(\mathscr{D}(F))$, *and* p *is less than or equal to* $[((\chi+1) \cdot N + \log_2 co(\mathscr{D}(F)))/\lambda]$, *where* χ *and* λ *are the constants from* 3.4.1 *and* 3.4.2.

(ii) *If* p *does not divide* $co(\mathscr{D}(F))$, *then* $F^{\sigma_p}(Y) \in \mathbb{A}_p[Y]$ *is separable.*

Proof: (i) The only-if-part follows from the fact that the canonical map $M(k, \mathbb{A}[Y]/\mathfrak{b}) \to M(k, \mathbb{A}_p[Y]/\mathfrak{b}_p)$ is a homomorphism of noncommutative rings.

Let us turn to the if-part. For $\iota_1, \iota_2 \in \{1, 2, \ldots, k\}$, let

$$Q(Y) = \sum_{i=0}^{\delta-1} q_i(X) \cdot Y^i$$

be the unique representative $\bmod F(Y)$ of the (ι_1, ι_2)-entry of $\Psi_N(A_1, A_2, \ldots, A_{2N})$. By 3.4.1 the absolute values of the integer coefficients of $q_i(X)$, $i = 0, 1, \ldots, \delta - 1$, are bounded by $2^{\chi \cdot N}$. By 3.1.3

$$Q^{\sigma_p}(Y) = \sum_{i=0}^{\delta-1} \sigma_p(q_i(X)) \cdot Y^i$$

is the unique representative $\bmod F^{\sigma_p}(Y)$ of the (ι_1, ι_2)-entry of $\Psi_N(A_1^{(p)}, A_2^{(p)}, \ldots, A_{2N}^{(p)})$ the degree of which is less than δ. By the assumption, $Q^{\sigma_p}(Y) = 0$, for all primes p under consideration. Consequently, the integer coefficients of the polynomials $q_i(X)$, $i = 0, 1, \ldots, \delta - 1$, are equal to zero $\bmod p$. Using the well-known Chinese-Remainder-Theorem claim (i) follows.

(ii) By 3.1.2. $\mathscr{D}(F^{\sigma_p}(Y)) = \sigma_p(\mathscr{D}(F))$. Since p does not divide $co(\mathscr{D}(F))$, no coefficient of $\mathscr{D}(F)$ vanishes under the reduction. ■

We turn to the second lemma. We assume that

$$F(Y)=Y^{\delta}+\sum_{i=0}^{\delta-1} f_i(X).\,Y^i\in\mathbb{A}_p[Y]$$

is *separable*. Let θ be a natural number such that the degree of $\mathcal{D}(F)$ in any variable X_j is less than θ.

If $\mathfrak{b}=F(Y)\cdot\mathbb{A}_p[Y]$, $\zeta=(\zeta_1, \zeta_2, \ldots, \zeta_m)\in\mathbb{F}_{p^r}^m$,

$$\hat{\rho}_\zeta:\quad \mathbb{A}_p[Y]\to\mathbb{F}_{p^r}[Y],$$

then we define the ideal $\mathfrak{b}(\zeta)$ to be

$$\mathfrak{b}^e=F^{\rho_\zeta}(Y)\cdot\mathbb{F}_{p^r}[Y]=\left(Y^{\delta}+\sum_{i=0}^{\delta-1} f_i(\zeta)\cdot Y^i\right)\cdot\mathbb{F}_{p^r}[Y]$$

(*see* 3.1.1).

Furthermore we have (*see* 3.1.1 and 3.3.5)

$$r(\mathfrak{b}(\zeta))=\bar{F}[Y]\cdot\mathbb{F}_{p^r}[Y],$$

and

$$\bar{\rho}_\zeta:\quad \mathbb{A}_p[Y]/\mathfrak{b}\to\mathbb{F}_{p^r}[Y]/r(\mathfrak{b}(\zeta)).$$

NOTATION: The image of the matrix $A\in\mathrm{GL}(k, \mathbb{A}_p[Y]/\mathfrak{b})$ under the canonical map

$$\mathrm{GL}(k, \mathbb{A}_p[Y]/\mathfrak{b})\to\mathrm{GL}(k, \mathbb{F}_{p^r}[Y]/r(\mathfrak{b}(\zeta)))$$

resulting from $\bar{\rho}_\zeta$ is denoted by $A(\zeta)$.

3.5.2. LEMMA: *Let* $A_1, A_2, \ldots, A_{2N}\in\mathrm{GL}(k, \mathbb{A}_p[Y]/\mathfrak{b})$ *be matrices such that the assumptions of* 3.4.1 *are fulfilled. Let r be a natural number such that l. c. m.* $(1, 2, \ldots, \delta)$ *divides r and* p^r *is greater than* $(\tau\cdot\delta\cdot N+1)^{m-1}+\tau\cdot\delta\cdot N+1$.

Then

$$\Psi_N(A_1, \ldots, A_{2N})=0$$

iff $\Psi_N(A_1(\zeta), \ldots, A_{2N}(\zeta))=0$ *in* $\mathrm{GL}(k, \mathbb{F}_{p^r}[Y]/r(\mathfrak{b}(\zeta)))$ *for all* $\zeta\in\mathbb{F}_{p^r}^m$.

Proof: The only-if-part is clear since there are homomorphisms of matrix rings under consideration.

Since $p^r \geqq (\tau \cdot \delta \cdot N+1)^{m-1}+\tau \cdot \delta \cdot N+1$, there are subsets

$$T_i \subseteqq F_{p^r}, \qquad |T_i| \geqq \tau \cdot \delta \cdot N+1,$$

such that the discriminant $\mathscr{D}(F)$ has no root belonging to $T=T_1 \times T_2 \times \ldots \times T_m$ (*see* 3.3.4). Since $\mathscr{D}(F^{\rho_\zeta})=\rho_\zeta(\mathscr{D}(F)$ (*see* 3.1.2), it follows that $\mathscr{D}(F^{\rho_\zeta})$ is different from 0. We have by 3.1.1 that

$$r(\mathfrak{b}(\zeta))=\mathfrak{b}(\zeta)=F^{\rho_\zeta}(Y)\cdot \mathbb{F}_{p^r}[Y], \qquad \text{for all} \quad \zeta \in T.$$

Let

$$Q(Y)=\sum_{i=0}^{\delta-1} q_i(X)\cdot Y^i$$

be any entry of $\Psi_N(A_1, \ldots, A_{2N})$. By 3.4.1 the degree of all $q_i(X)$ in any variable X_j is bounded by $\tau \cdot \delta \cdot N$. By 3.1.3 the unique representative of degree less than δ mod $F^{\rho_\zeta}(Y)$ of the corresponding entry $\Psi_N(A_1(\zeta), \ldots, A_{2N}(\zeta))$ is

$$Q^{\rho_\zeta}(Y)=\sum_{i=0}^{\delta-1} q_i(\zeta)\cdot Y^i,$$

for all $\zeta \in T$. For all $\zeta \in T$, $Q^{\rho_\zeta}(Y)$ is known to be zero. This is the case iff $q_i(\zeta)=0$, $i=0, 1, \ldots, \delta-1$. It follows from 3.1.5 that $q_i(X)=0$, for $i=0, 1, \ldots, \delta-1$. Consequently, $Q(Y)=0$. ■

4. THE MAIN LEMMA

4.1. We make use of the notations of Paragraph 3. Let again **B** be either the ring $\mathbb{A}$ or the ring $\mathbb{A}_p$, and let

$$F(Y)=Y^\delta+\sum_{i=0}^{\delta-1} f_i(X).\, Y^i \in \mathbf{B}[Y]$$

be a separable polynomial which is irreducible over the quotient field of **B**.

Define the ideal $\mathfrak{b}$ in $\mathbf{B}[Y]$ to be $F(Y).\mathbf{B}[Y]$. For each natural number we assume $\Psi_N(T_1, \ldots, T_{2N})$ to be the polynomial

$$\Psi_N(T_1, T_2, \ldots, T_{2N})=T_1\cdot T_2\cdot \ldots \cdot T_N-T_{N+1}\cdot T_{N+2}\cdot \ldots \cdot T_{2N}$$

in the variables T_i (*see* 3.5). Let us denote by Ψ the whole sequence $(\Psi_N \mid N \in \mathbb{N})$. Let $co(\mathscr{D}(F))$ be the least common multiple of the integer coefficients of the dicriminant $\mathscr{D}(F)$ (*see* 3.5).

Suppose $\mathscr{M}at$ to be a finite subset of $\mathrm{GL}(k, \mathbf{B}[Y]/\mathfrak{b})$. In line with Paragraph 3 we assume.

– If $P(Y) = \sum_{i=0}^{\delta-1} p_i(X) \cdot Y^i$ is an entry of an element of $\mathscr{M}at$, then the degree of the polynomials $f_i(X)$ and $p_i(X)$ in X_j is bounded by a natural number τ, for $i = 1, \ldots, \delta - 1, j = 1, \ldots, m$.

– If $\mathbf{B} = \mathbb{A}$, moreover the integer coefficients of p_i and of f_i are bounded in absolute value by γ, $i = 1, 2, \ldots, \delta - 1$.

In this paragraph we consider the parallel complexity of the following evaluation problem $\mathscr{EV}(\Psi, \mathscr{M}at)$ with its problem instances $\mathscr{EV}_N(\Psi, \mathscr{M}at)$, $N \in \mathbb{N}$.

INPUT: A sequence $(A_1, A_2, \ldots, A_{2N}) \in \mathscr{M}at^{2N}$

OUTPUT: $\begin{cases} 1, & \text{if } \Psi_N(A_1, A_2, \ldots, A_{2N}) = 0 \\ 0, & \textit{otherwise.} \end{cases}$

4.2. Main lemma

(I) If $\mathbf{B} = \mathbb{A}_p$, then $\mathscr{EV}(\Psi, \mathscr{M}at)$ belongs to

$$U\text{-SIZE, DEPTH}\,(n^{O(1)}, \log n \cdot \log\log n).$$

(II) If $\mathbf{B} = \mathbb{A}$, then $\mathscr{EV}(\Psi, \mathscr{M}at)$ belongs to

$$U\text{-SIZE, DEPTH}\,(n^{O(1)}, \log n \cdot \log\log n \cdot \log\log\log n).$$

(III) If $\mathscr{M}at \subseteq T(k, \mathbf{B}[Y]/\mathfrak{b})$, then $\mathscr{EV}(\Psi, \mathscr{M}at)$ belongs to NC^1.

Proof.

4.2.1. *The method:* If $\mathbf{B} = \mathbb{A}$, let PRIME_N be the set of all primes not dividing $co(\mathscr{D}(F))$ which are less than or equal to

$$\left\lceil \frac{(\chi + 1) \cdot N + \log_2 co(\mathscr{D}(F))}{\lambda} \right\rceil$$

where χ and λ are the constants from 3.4.1 and 3.4.2 (*see* 3.5.1). If $\mathbf{B} = \mathbb{A}_p$, then $\mathrm{PRIME}_N = \{p\}$.

For all primes $p \in \mathrm{PRIME}_N$, let r be the minimal natural number such that, $p^r \geqq (\tau \cdot \delta \cdot N+1)^{m-1}+\tau \cdot \delta \cdot N+1$ and the l.c.m. $(1, 2, \ldots, \delta)$ divides r. For all vectors $\zeta=(\zeta_1, \ldots, \zeta_m) \in \mathbb{F}_{p^r}^m$, let $\mathscr{F}_{p,\zeta}$ be the canonical isomorphism $\mathbb{F}_{p^r}[Y]/(\bar{F}_{p,\zeta}(Y) \cdot \mathbb{F}_{p^r}[Y]) \to (\mathbb{F}_{p^r})^{\Delta}$ defined in 3.3.5. We compute

$$\Psi_N(\mathscr{F}_{p,\zeta}(A_1^{(p)}(\zeta)), \ldots, \mathscr{F}_{p,\zeta}(A_{2^N}^{(p)}(\zeta))).$$

We agree that $A_i^{(p)}=A_i$ in the case of $\mathbf{B}=\mathbb{A}_p$.

We accept iff $\Psi_N(\mathscr{F}_{p,\zeta}(A_1^{(p)}(\zeta)), \ldots, \mathscr{F}_{p,\zeta}(A_{2^N}^{(p)}(\zeta)))=0$, for all p, and for all ζ under consideration.

The correctness of the method follows from 3.5.1 in connection with 3.5.2 or from 3.5.2 in the case of characteristic p.

Elements from the field $\mathbb{F}_{p^r}$ are represented as vectors of dimension r over $\mathbb{F}_p$ (*see* 3.3). Scalars from $\mathbb{F}_p$ are always given in binary representation of their canonical representative belonging to $\{0, \ldots, p-1\}$. Since $p^r=N^{O(1)}$, any element of $\mathbb{F}_{p^r}$ can be written down on a Turing tape within space $O(\log N)$. Clearly, the same is valid for any polynomial over $\mathbb{F}_p$ of degree $O(r)$.

4.2.2. *Logspace Tables:* The following information ((i)-(vii)) are computed by a logspace Turing transducer having input 1^n and are hardwired in the circuit.

(i) Compute the set PRIME_N, and for each prime $p \in \mathrm{PRIME}_N$ the natural number r defined above.

(ii) Compute an irreducible polynomial $\Phi_{p,r}(Z) \in \mathbb{F}_p[Z]$ with leading coefficient 1 (*see* 3.3.1) by the brute force method. Moreover, if

$$\Phi_{p,r}(Z)=\sum_{i=0}^{r-1} \varphi_i^{p,r} \cdot Z^i + Z^r,$$

we compute the matrices $[B(\Phi_{p,r})]^i$ (*see* 3.1.4), for $i=1, 2, \ldots, r-1$, and hardwire their coefficients in the circuit. Let us denote these coefficients by $\chi_{k,l}^{p;r,i}$.

Remark: We observe that addition in $\mathbb{F}_{p^r}$ can be performed on a logspace bounded working tape of a transducer. To do the same for multiplication, we proceed as follows. We carry out ordinary multiplication of two polynomials over $\mathbb{F}_p$ of degree less than r by brute force withing $\log n$-space since the number p^r is tiny. We get a polynomial $\pi(Z)$ of degree less than or equal to $2(r-1)$. In order to compute the representative $\bmod \Phi_{p,r}(Z)$ of $\pi(Z)$ we

check for all polynomials $\alpha(Z)$, $\beta(Z) \in \mathbb{F}_p[Z]$ of degree less than r whether

$$\pi(Z) - \alpha(Z) = \beta(Z) \cdot \Phi_{p,r}(Z) \text{ in } \mathbb{F}_p[Z].$$

We shall succeed for exactly one polynomial $\alpha(Z)$ which is the representative we are looking for.

In that way it is also possible to do the following.

(iii) Compute a generator ω_p, $p \in \mathrm{PRIME}_N$, of the cyclic group $(\mathbb{F}_{p^r})^*$ by brute force and compute a table for the assignments

$$\beta \to l_{\omega_p}(\beta) = l_p(\beta),$$

(Log-Table)

where $\beta \in (\mathbb{F}_{p^r})^*$, and a table for the assignment

$$\{0, 1, \ldots, p^r - 1\} \ni i \to \omega_p^i.$$

(Exp-Table)

(iv) Compute all different roots $\alpha_{p,\zeta,j}$ of the polynomial $F_{p,\zeta}(Y)$, for all $\zeta \in \mathbb{F}_{p^r}^m$, for $j = 1, 2, \ldots, \Delta \leqq \delta$, where

$$F_{p,\zeta}(Y) = Y^\delta + \sum_{i=0}^{\delta-1} f_i^{\sigma_p}(\zeta) \cdot Y^i \in \mathbb{F}_{p^r}[Y],$$

provided that $\mathbf{B} = \mathbb{A}$, and

$$F_{p,\zeta}(Y) = Y^\delta + \sum_{i=0}^{\delta-1} f_i(\zeta) \cdot Y^i \in \mathbb{F}_{p^r}[Y]$$

im the case of $\mathbf{B} = \mathbb{A}_p$.

NOTATION : $\bar{F}_{p,\zeta}(Y) = \prod_{j=1}^{\Delta} (Y - \alpha_{p,\zeta,j})$ (*see* 3.3.5).

(v) Compute for all entries $P(Y) = \sum_{i=0}^{\delta-1} p_i(X) \cdot Y^i$ of elements of $\mathcal{M}at$, for all primes $p \in \mathrm{PRIME}_N$, for all $\zeta \in \mathbb{F}_{p^r}^m$, and for all roots of $\alpha_{p,\zeta,j}$ of $\bar{F}_{p,\zeta}(Y)$

$$\sum_{i=0}^{\delta-1} p_i^{\sigma_p}(\zeta) \cdot Y^i.$$

Remark: We have to construct uniform subcircuits to handle with the arithmetic operations in the rings $\mathbb{F}_{p^r}[Y]/(\bar{F}_{p,\zeta}(Y)\cdot\mathbb{F}_{p^r}[Y])$. By 3.1.3 there are isomorphisms

$$\mathscr{F}_{p,\zeta}\colon\quad \mathbb{F}_{p^r}[Y]/(\bar{F}_{p,\zeta}(Y).\mathbb{F}_{p^r}[Y]) \to (\mathbb{F}_{p^r})^{\Delta}$$

which algebraically reduce this problem to the corresponding one in the fields $\mathbb{F}_{p^r}$. We need evaluation tables in order to effectively compute these isomorphisms.

(vi) Compute for all primes $p \in \mathrm{PRIME}_N$, for all $\zeta \in \mathbb{F}_{p^r}^m$, and for all elements

$$H(Y)=\sum_{i=0}^{\Delta-1} h_i\cdot Y^i \in \mathbb{F}_{p^r}[Y]/(\bar{F}_{p,\zeta}(Y)\cdot\mathbb{F}_{p^r}[Y])$$

[which are represented as vectors $(h_0, \ldots, h_{\Delta-1}) \in \mathbb{F}_{p^r}^{\Delta}$] the vector

$$(H(\alpha_{p,\zeta,1}), H(\alpha_{p,\zeta,2}), \ldots, H(\alpha_{p,\zeta,\Delta})) \in \mathbb{F}_{p^r}^{\Delta}.$$

(Evaluation-Table)

This is nothing else than multiplication of vectors of dimension Δ over $\mathbb{F}_{p^r}$ with the matrix $A(\bar{F}_{p.\zeta})$ (*see* 3.3.5). Obviously, the computations which are necessary can be carried out on a Turing tape within tape $O(\log n)$, and the table can be generated within $O(\log n)$ space.

Remark: In the case of claim (III) we need all monotone nondecreasing sequences $\mu \in \{1, 2, \ldots, k\}^{N-1}$ (*see* 2.9).

(vii) Compute all monotone sequences $\mu \in \{1, 2, \ldots, k\}^{N-1}$. The following facts ensure that this can be done in $O(\log N)$ space.

- The number of such sequences equals $\binom{k+N-2}{N-1} = N^{O(1)}$.
- Each such sequence has a unique representation

$$1^{f_1}2^{f_2}\ldots k^{f_k}, \qquad \sum_{j=1}^{k} f_j = N-1, \quad f_j \geqq 0.$$

Consequently, it can be written down on a Turing tape encoded as a sequence of length k of integers less than N in binary representation.

- The successor of any such sequence in the lexicografic ordering can be computed within space $O(\log N)$.

4.2.3. *Addition in* $\mathbb{F}_{p^r}$: For all primes $p \in \mathrm{PRIME}_N$, we construct a uniform circuit having the following input-output behaviour.

INPUT: $\beta_1, \beta_2, \quad , \beta_M \in \mathbb{F}_{p^r}$

OUTPUT: $\beta_1 + \beta_2 + \quad + \beta_M \in \mathbb{F}_{p^r}$

DEPTH: $O(\log M + \log\log p)$.

Do for all r components in parallel.

Step 1: Iterated addition of M log p-bit integers by 2.1.

Step 2: Substracting off in parallel the multiples of $p-0, p, \ldots, (M-1)\cdot p$- from the results of step 1 and choosing the appropriate difference.

In the case of $M = r^{O(1)}$ we have depth $O(\log\log N)$. If $M = 0(N)$, the depth is bounded by $O(\log N)$.

4.2.4. *Multiplication in* $\mathbb{F}_{p^r}$: For all primes $p \in \mathrm{PRIME}_N$, we construct a uniform circuit having the following input-output behaviour.

INPUT: $\beta'_1, \beta'' \in \mathbb{F}_{p^r}$

OUTPUT: $\beta'_1 \cdot \beta'' \in \mathbb{F}_{p^r}$

DEPTH: $O(\log r + \log(\log r + \log p) \,.\, \log\log(\log r + \log p))$.

If $\beta' = (\beta'_0, \ldots, \beta'_{r-1})$, $\beta = (\beta''_0, \ldots, \beta''_{r-1})$ and $\beta = (\beta_0, \ldots, \beta_{r-1})$, then it is easy to see that

$$\beta_k = \sum_{j=0}^{r-1} \sum_{l=0}^{r-1} \chi_{k,l}^{p,r,j} \cdot \beta'_j \cdot \beta''_1 \qquad \text{for} \quad k = 0, \ldots, r-1.$$

Remember, that the constants $\chi_{k,l}^{p,r,j}$ are hardwired in the circuit [*see* 3.1.4, 4.2.2 (ii)].

Step 1: Compute in parallel all products

$$\chi_{k,l}^{p,r,j} \cdot \beta'_j \cdot \beta''_l$$

as natural numbers using 2.2.

Step 2: Carry out the r-fold iterated addition of $(r-1)^2$ summands in parallel by theorem 2.1.

Step 3: Reduce in parallel the r results of step 2 mod p by the help of integer division, multiplication and subtraction.

In the case of p a prime not depending on the input length, the depth is bounded by $O(\log\log N)$, otherwise only by $O(\log\log N \,.\, \log\log\log N)$.

4.2.5. *Iterated Multiplication in* $\mathbb{F}_{p^r}$: For all primes $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$ we construct a uniform circuit such that

INPUT: A sequence of elements $(\beta_1, \beta_2, \ldots, \beta_M) \in \mathbb{F}_{p^r}^M$,

OUTPUT: The product $\beta = \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_M$.

DEPTH: $O(\log N)$, provided that $M = O(N)$.

Step 1: Check whether one of the inputs equals zero in $\mathbb{F}_{p^r}$. If this is the case, the output equals zero. Otherwise turn to Step 2.

Step 2: Compute, for all $i = 1, \ldots, M$, $l_p(\beta_i)$ using the log-table of (iii).

Step 3: Compute for all $j = 1, 2, \ldots, \Delta$

$$\lambda = \sum_{i=1}^{M} l_p(\beta_i) \bmod p^r - 1$$

using Theorem 2.1 and Proposition 2.3.

Step 4: Compute β from λ by using the exp-table of (iii).

4.2.6. *The Proof of Claim I and II:* There is, for each prime $p \in \mathrm{PRIME}_N$, and for each $\zeta \in \mathbb{F}_{p^r}^m$ a circuit $\mathrm{Cir}_{p,\zeta}$ such that

INPUT: $C_1, C_2 \in \mathrm{GL}(k, \mathbb{F}_{p^r}^{\Delta})$.

OUTPUT: The product $C_1 . C_2$.

DEPTH: If $\mathbf{B} = \mathbb{A}$, then $O(\log\log N . \log\log\log N)$.

If $\mathbf{B} = \mathbb{A}_p$, then $O(\log\log N)$.

This follows directly from 4.2.3 and 4.2.4.

Now let us construct the desired circuit. Let $(A_1, A_2, \ldots, A_{2^N}) \in \mathcal{M}at^{2^N}$ be an input sequence. We assume that $N = 2^{N'}$, $N' \in \mathbb{N}$.

Step 1: Compute for all $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$ the matrices $A_i^{(p)}(\zeta)$, $i = 1, 2, \ldots, 2N$, by using table (v).

Step 2: Compute for all $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$ the matrices $\mathscr{F}_{p,r}(A_i^{(p)}(\zeta))$, $i = 1, 2, \ldots, 2N$, by using table (vi).

Step 3 *a:* Divide for all $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$ the word $\mathscr{F}_{p,r}(A_1^{(p)}(\zeta)) \cdot \ldots \cdot \mathscr{F}_{p,r}(A_N^{(p)}(\zeta))$ into $N/2$ subwords of length 2. Of course, this subdivision is hardwired in the circuit. Then

$$\mathscr{F}_{p,\zeta}(A_1^{(p)}(\zeta)) \cdot \ldots \cdot \mathscr{F}_{p,\zeta}(A_N^{(p)}(\zeta)) = B_1 \cdot \ldots \cdot B_{N/2},$$

where

$$B_j = \mathscr{F}_{p,\zeta}(A_{2j-1}^{(p)}(\zeta)) \cdot \mathscr{F}_{p,\zeta}(A_{2j}^{(p)}(\zeta)).$$

Compute all matrices B_j in parallel by the help of circuits $\mathrm{Cir}_{p,\zeta}$. The resulting word of matrices $B_1 \cdot \ldots \cdot B_{N/2}$ is again divided into words of length 2, and the process iterates.

We can do so N' times. What we get is the product $\mathscr{F}_{p,\zeta}(A_1^{(p)}(\zeta)) \cdot \ldots \cdot \mathscr{F}_{p,\zeta}(A_N^{(p)}(\zeta))$ within size $n^{O(1)}$. If $B = \mathbb{A}$, then the depth is bounded by $O(\log n \cdot \log\log n \cdot \log\log\log n)$. Otherwise the depth bound is $O(\log n \cdot \log\log n)$.

Step 3 *b:* Do the same as in Step 3 *a* with $A_{N+1} \cdot \ldots \cdot A_{2N}$. Observe that Step 3 *a* and *b* can be carried out in parallel.

Step 4*:* Compare the results of Step 3 *a* and *b* with each other. Accept iff they are identical, for all $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$.

4.2.7. *The Proof of Claim (III)*

Step 1 and *step* 2 are the same as in 4.2.6.

Step 3 *a:* Compute the products

$$\mathscr{F}_{p,\zeta}(A_1^{(p)}(\zeta)) \cdot \ldots \cdot \mathscr{F}_{p,\zeta}(A_N^{(p)}(\zeta))$$

in parallel, for all primes $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}$ using the formula of remark 2.9, the table of 4.2.2 (vii), and the circuits from 4.2.5 and 4.2.3.

Step 3 *b:* Do the same as in Step 3 *a* with $A_{N+1} \cdot \ldots \cdot A_{2N}$. Observe that Step 3 *a* and *b* can be carried out in parallel.

Step 4*:* Compare the results of Step 3 *a* and *b* with each other. Accept iff they are identical, for all $p \in \mathrm{PRIME}_N$, and for all $\zeta \in \mathbb{F}_{p^r}^m$.

5. THE RESULTS

5.1. THEOREM: *Let G be a finitely generated K-linear group, where K is any field.*

If $\chi(K) = 0$, *then*

$$W(G) \in U\text{-SIZE, DEPTH}(n^{O(1)}, \log n \,.\, \log\log n \,.\, \log\log\log n).$$

If $\chi(K)=p$, *for some prime* p, *then*

$$W(G)\in U\text{-SIZE, DEPTH}\,(n^{O(1)}, \log n.\log\log n).$$

Proof: Since the group G is finitely generated, we assume that G is a subgroup of $\mathrm{GL}(k, P(X_1, \ldots, X_m)\,[y])$, where P is a prime field, $X=(X_1, \ldots, X_m)$ is a separating trancendence base, and y is algebraic over $P(X_1, \ldots, X_m)$. If

$$F(Y)=Y^{\delta}+\sum_{i=0}^{\delta-1} f_i(X)\cdot Y^i$$

is the minimal polynomial of y over $P(X)$, F is separable. Moreover, y can be choosen in such a way, that the coefficients $f_i(X)$ of the polynomial F belong to $\mathbb{Z}[X]$ if $\chi(K)=0$, and to $\mathbb{F}_p[X]$ if $\kappa(K)=p$ (*see* 3.2).

As in in 3.2 let

$$\mathbf{B}=\begin{cases}\mathbb{A}=\mathbb{Z}[X] & \text{if } \chi(K)=0\\ \mathbb{A}_p=\mathbb{F}_p[X] & \text{if } \chi(K)=p.\end{cases}$$

Then for each entry of a generator or the inverse of a generator of the group G we take its unique representation as a fraction $G(Y)/g(X)$, where $G(Y)\in\mathbf{B}[Y]$, $g(X)\in\mathbf{B}$. Let $q(X)$ be the least common multiple of all such elements $g(X)$. Define the set of matrices $\mathcal{M}at$ contained in $\mathrm{GL}(k, \mathbf{B}[Y]/b)$ (*see* 4.1) as follows. $\mathcal{M}at=\{q.A \mid A^{\pm 1}$ is a generator of $G\}\cup\{q\cdot E\}$, where E is the identity matrix. Obviously,

$$A_1\cdot\ldots\cdot A_N=E \quad \text{iff} \quad \Psi_N(q\cdot A_1, \ldots, q\cdot E, \ldots, q\cdot E)=0.$$

We may apply the Main Lemma. ■

5.2. COROLLARY: *The word problem of a finitely generated free group belongs to* U-SIZE, DEPTH $(n^{O(1)}, \log n\cdot\log\log n)$.

Proof: We apply 2.13. ■

5.3. THEOREM: *A finitely generated context-free group language is* NC^1-*equivalent to the word problem of an arbitrary finitely generated free group.*

Proof: Obviously, the word problems of two f.g. free groups are NC^1-equivalent. Let G be a f.g. group having a context-free word problem. By 2.12 the group G has a free subgroup F of finite index, which is, of course, finitely generated, too. Using Theorem 2.10 we get that $W(G)$ is NC^1-equivalent to $W(F)$. ■

5.4. COROLLARY: *A finitely generated context-free group language belongs to U*-SIZE, DEPTH ($n^{O(1)}$, $\log n \cdot \log\log$).

Proof: The claim follows from 5.1, 2.10, 2.12, and 2.13. ■

5.5. THEOREM: *Let G be a finitely generated solvable-by-finite K-linear group, where K is any field. Then the word problem of G is solvable in logdepth.*

Proof: By definition G has a finitely generated subgroup G' of finite index which is solvable. By 2.8 G' has a finitely generated normal subgroup H which is triangularizable over the algebraic closure of K. We proceed analogously as in 5.1 to prove that the word problem of H is contained in NC^1. Applying 2.10 twice we are done. ■

5.6. COROLLARY: *Each finitely generated linear group which does not contain a noncyclic free group has a word problem solvable in logdepth.*

Proof: The result follows from 5.5 and 2.14. ■

5.7. COROLLARY: *Each finitely generated polycylic group has a word problem belonging to* NC^1.

Proof: The assertion follows from 5.5 and 2.7. ■

5.8. COROLLARY: *Each finitely generated nilpotent group has a word problem solvable in logdepth.* ■

REFERENCES

1. L. AUSLANDER, On a problem of Philip Hall, *Ann. of Math.*, 1967, **86**(2), pp. 112-116.
2. J. AVENHAUS, K. MADLENER, Subrekursive Komplexität bei Gruppen, I. Gruppen mit vorgeschriebener Komplexität, *Acta Inform.*, 1977, **9**, pp. 87-104.
3. J. AVENHAUS, K. MADLENER, Subrekursive Komplexität bei Gruppen, II. Der Einbettungssatz von Higman für entscheidbare Gruppen, *Acta Inform.*, 1978, **9**, pp. 183-193.
4. J. AVENHAUS, K. MADLENER, The Nielson reduction and P-complete problems in free groups, *Theoret. Comput. Sci.*, 1984, **32**, pp. 61-76.
5. J. AVENHAUS, K. MADLENER, On the complexity of intersection and conjugacy problems in free groups, *Theoret. Comput. Sci.*, 1984, pp. 279-295.
6. D. A. BARRINGTON, Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1, in: *Proc. 18th A.C.M. S.T.O.C.*, 1986, pp. 1-5.
7. P. W. BEAME, S. A. COOK, H. J. HOOVER, Logdepth circuits for division and related problems, *S.I.A.M. J. Comput.*, 1986, **15**(4), pp. 993-1003.

8. A. BORODIN, S. A. COOK, N. PIPPENGER, Parallel computation for well-endowed rings and space bounded probabilistic machines, TR # 162/83, University of Toronto.
9. S. A. COOK, The classification of problems which have fast parallel algorithms, in: *Lecture Notes in Comput. Sci.*, 158, Springer-Verlag, Berlin, 1983.
10. S. A. COOK, A Taxonomy of problems with fast parallel algorithms, *Inform. and Control*, 1985, **64**, pp. 2-22.
11. S. A. COOK, P. MCKENZIE, Problems complete for deterministic logarithmic space, *J. Algorithms*, 1987, **8**, pp. 385-394.
12. S. A. COOK, P. MCKENZIE, The parallel complexity of abelian permutation group problems, *S.I.A.M. J. Comput.*, 1987, **16** (2), pp. 880-909.
13. M. J. DUNWOODY, The accessibility of finitely presented groups, *Invent. Math.*, 1985, **81**, pp. 449-457.
14. M. HALL, Subgroups of finite index in free groups, *Canad. J. Math.*, 1949, **1**, pp. 187-190.
15. G. H. HARDY, E. M. WRIGHT, An introduction to the theory of numbers, Oxford U. Press, London, 1957.
16. J. E. HOPCROFT, J. D. ULLMAN, Introduction to automata theory, languages, and computation, Addison-Wesley, Reading, 1979.
17. M. KRAUSE, S. WAACK, On oblivious branching programs of linear length, to appear in *Inform. and Comput.*
18. K. KRIEGEL, S. WAACK, Lower bounds on the complexity of real-time branching programs, *RAIRO Inform. Théor. Appl.*, 1988, **22** (4), pp. 447-459.
19. S. LANG, *Algebra*, Addison-Wesley, Reading 1965.
20. R. J. LIPTON, Polynomials with 0-1 coefficients that are hard to evaluate, in: Proc. 16*th Ann. I.E.E.E. Symp. on Foundations of Comp. Sci.*, 1975, pp. 6-10.
21. R. J. LIPTON, Y. ZALCSTEIN, Word problems solvable in logspace, *J. of the A.C.M.*, 1977, **24 (3)**, pp. 322-526.
22. W. MAGNUS, A. KARASS, D. SOLITAR, Combinatorial group theory, Interscience Publishers, 1966.
23. A. I. MAL'CEV, On certain classes of infinite solvable groups, *Mat. Sb.*, 1951, **28**, pp. 567-598.
24. D. MULLER, P. SCHUPP, Groups, the theory of ends, and context-free languages, *J. Comput. System Sci.*, 1983, **26**, pp. 295-310.
25. J. E. SAVAGE, The complexity of computing, John Wiley, New York, 1976.
26. H. U. SIMON, Word problems for groups and contextfree recognition, in: *Proc. FCT'79*, Akademie-Verlag, Berlin, 1979.
27. R. G. SWAN, Representations of polycyclic groups, *Proc. Amer. Math. Soc.*, 1967, **18**, pp. 573-574.
28. TITS, Free subgroups in linear groups, *J. Algebra*, 1972, **20**, pp. 250-270.
29. C. TRETKOFF, Complexity, combinatorial group theory and the language of pulatators, *Theoret. Comput. Sci.*, **56**, 1988, pp. 253-275.
30. S. WAACK, Tape complexity of word problems, in: *Proc. FCT'81*, *Lecture Notes in Comput. Sci.*, 1981, **117**, Springer-Verlag, Berlin, pp. 467-471.
31. S. WAACK, Tape complexity of word problems, TR IMATH der AdW der DDR, Berlin 1981.
32. S. WAACK, Raumkomplexität von Wortproblemen endlicher Gruppenpräsentationen, Dissertation A, Berlin 1983.

33. S. WAACK, The parallel complexity of some constructions in combinatorial group theory, *J. Inf. Process. Cybern.*, 1990, **26**, 5/6, pp. 265-281.
34. I. WEGENER, The complexity of boolean functions, Wiley-Teubner Series in Comput. Sci., 1987.
35. B. A. F. WEHRFRITZ, Infinite linear groups, Springer-Verlag, New York, 1973.
36. O. ZARISKI, P. SAMUEL, Commutative algebra I, II, Van Nostrand, Princton, 1958, 1960.