Electronic Colloquium on Computational Complexity
ECCC Technical Reports Series 1994 Report Nr: TR94–015

Symmetric Systems of Linear Equations modulo p

Miklós Ajtai[†]

Received *December 18, 1994*

Abstract. Suppose that p is a prime number A is a finite set with n elements and for each sequence $a = \langle a_1, ..., a_k \rangle$ of length k from the elements of A, x_a is a variable. (We may think that k and p are fixed an n is sufficiently large.) We will consider systems of linear equations modulo p of the form $\sum u_a^{(i)} x_a \equiv b_i \pmod p$, $i = 1, ..., l$. We will call such a system symmetric if for every permutation π of the set A and for every $i = 1, ..., l$ the equation $\sum u_{a\pi}^{(i)} x_a = b_i$ is also an equation of the system. We show that if such a system has a solution then it also has a solution which is definable by a first-order formula ϕ whose length depends only on k and p over the structure $\mathcal{A} = \langle A, \leq, R_1, ..., R_{p^j} \rangle$ defined in the following way. Let $\leq$ be a linear ordering of the universe and j a positive integer sufficiently large with respect to k and p. For each $i = 1, ..., p^j$, R_i is a unary relation on a, $R_i(x)$ holds iff x is the rth element of A and $r \equiv i \pmod p$. More precisely the expression that the solution t_a, $a \in A^k$ is first-order definable means that for each $c = 0, 1, ..., p-1$ the set $\{a \in A | t_a \equiv c \pmod p\}$ is definable by a first-order formula ϕ_c whose length remains below a bound depending only on k and p.

Keywords: propositional proof-systems, forcing, constant-depth circuits, representations of the symmetric group

[†] IBM Almaden Research Center

1. Introduction. The theorem described in the abstract (more precisely a somewhat stronger but more complicated form of it) was needed for proving that the modulo p counting principles are independent from each other in some sense. The modulo p counting principle (for the number n) is the following statement: a set with n elements cannot have two partitions: one with each classes having exactly p elements and an other where each class with one exception has exactly p elements and the exceptional class has 1 elements. This statement can be considered as a mod p analogue of the pigeonhole principle. If it holds on an arbitrary (not necessarily finite) structure in the sense that the universe has no two partitions of the described properties and there is linear ordering of the universe then we may assign a modulo p "cardinality" to each first-order definable subset of the universe in a way that the usual properties of the notion of cardinality remain valid (see [Ajt3]). It was known that the pigeonhole principle is in some sense weaker than the mod 2 counting principle (see [Ajt2], [Ajt1]). (In [Ajt2] the modulo 2 counting priniple was called the "parity principle".) The proof given there is using (in a hidden way) the analogue of the theorem given in the abstract over the fields of rationals. (The theorem is a much easier over the rationals; it can be proved by either an averaging argument or using some basic theorems about the representations of the symmetric groups over a field of characteristic 0. In this case the structure $\mathcal{A}$ contains only the eqaulity relation, the other relations are not needed.) In this paper we prove the theorem about linear equations for the mod p case. (The proof of the theorem concerning the modulo p counting principles is given in a separate paper (see [Ajt4])). In the present paper we do *not* suppose that reader is familiar with any of mentioned concepts or proofs related to the modulo p counting principles or the pigeonhole principle.

We give now a more rigorous formulation of the theorem mentioned in the abstract. Later we give an other form of the theorem using the concepts of the representation theory of the symmetric group. Actually all of the proofs will be using the terminology of representation theory. Apart from the terminology the representation theory of the symmetric group, particularly the so called "charactersic free" results of G. D. James (see [J]) have a crucial role in the proofs. For the sake of the reader who is not familiar with the terminology of representation theory, first we give all of our results in terms of symmetric systems of linear equations.

As we formulated the theorem in the abstract we used a structure $\mathcal{A} = \langle A, \leq, R_1, ..., R_{p^j} \rangle$ which depended on the parameters p and j. Throughout the paper the prime p will be fixed, however j will vary, that is, we get various structures $\mathcal{A}_j$. With the present formulation if $j' > j$ then the structure $\mathcal{A}_{j'}$ is not an extension of $\mathcal{A}_j$ since the relation symbols R_i, $i = 1, ..., j$ have different interpretations in the two structure. We will give a somewhat more complicated definition for the structures $\mathcal{A}_j$ so that $\mathcal{A}_{j'}$ is an extension of $\mathcal{A}_j$ if $j' > j$. In the structure $\mathcal{A}_j$ we will have relations $R_{i,s}$ for all $i = 1, ..., j$ and $s = 1, ..., p^i$. $R_{i,s}(x)$ will hold if x is the rth element of the structure according to the ordering and $r \equiv s \pmod{p^i}$.

Definitions. 1. Assume that p is a prime. For each positive integer j we define a first-order language L_j^p which (apart from the equality) has a single binary relation: $\leq$, and for each $i = 1, .., j$, $s = 1, \ldots, p^i$ a unary relations $R_{i,s}$. Let ϕ_j^p be the following first-order formula of L_j^p:

"$\leq$ is a linear ordering of the universe and

if z is the smallest element then $R_{i,1}(z)$ for all $i = 1, \ldots, j$ and

for each element x and each fixed $i = 1, \ldots, j$ there is exactly one $s = 1, \ldots, p^i$ with $R_{i,s}(x)$ and

for each x, y and $i = 1, \ldots, j$ if $1 \leq s, s' \leq p^i$ are integers, y is the successor of x, and $s' \equiv s + 1 \bmod p^i$ then $R_{i,s}(x)$ implies $R_{i,s'}(y)$."

Let T_j^p be the theory consisting of the single formula ϕ_j^p. If $\mathcal{A}$ is a model of T_j^p, then $\leq_{\mathcal{A}}$ will denote the interpretation of the relation symbol $\leq$ in $\mathcal{A}$. If the choice of $\mathcal{A}$ is clear from the context then we may omit the subscript.

Clearly, for each positive integer n any two models of T_j^p with a universe of size n are isomorphic. This is a consequence of the fact that $R_{i,s}(x)$ holds iff x is the s'-th element of the ordering "$\leq$" for some $s' \equiv s \pmod{p^i}$. Moreover if $\langle A, \leq \rangle$ is an ordered set then there is a single model $\mathcal{A}$ of T_j^p so that the universe of $\mathcal{A}$ is A and "$\leq$" = "$\leq_{\mathcal{A}}$". We will denote this model by $\mathcal{A}_{A,\leq,j,p}$. If $j > j'$ then the interpretation $\mathcal{A}_{A,\leq,j,p}$ is an extension of the interpretation $\mathcal{A}_{A,\leq,j',p}$, that is those relation symbols which occur in both L_j^p and $L_{j'}^p$ have identical interpretations in the two models.

4. Suppose that for each $a \in A_k$, x_a is a variable and for each $a \in A^k$, $i = 1, ..., l$, $u_a(i) \in Z_p$, $b_{i \in Z_p}$. If π is a permutation of A then π also acts in a natural way on A^k, namely $\langle a_1, ..., a_k \rangle \pi = \langle a_1 \pi, ..., a_k \pi \rangle$.

We say that the system of linear equations $\sum_{a\in A^k} u_a^{(i)} x_a = b_i$, $i = 1,...,l$ is symmetric if for each permutation π of the set A and $i = 1,...,l$ there is an $i' = 1,...,l$ so that for all $a \in A^k$ we have $u_{a\pi}^{(i)} = u_a^{i'}$.

Now we may formulate the theorem described in the abstract.

Theorem 1. *For all prime number p and natural number k there are natural numbers c, j so that for all natural number n the following holds:*

Suppose that A is a set with n elements, $\mathcal{A} = \langle A, \leq, ...\rangle$ is an interpretation of the theory T_j^p, l is a natural number, and for all $i = 1,...,l$, $a \in A^k$ we have $u_a^{(i)} \in Z_p$ and $b_i \in Z_p$. If the linear system $\sum_{a\in A^k} u_a^{(i)} x_a = b_i$, $i = 1,...,l$ is symmetric and it has a solution in Z_p then it also has a solution $x_a = t_a$ in Z_p so that for each fixed $d \in Z_p$ there is a first-order formula $\phi_d(y_1,...,y_k)$ of the language L_j^p so that the length of ϕ_d is at most c and for each $a = \langle a_1,...,a_k\rangle$ we have:

$t_a = d$ *iff* $\mathcal{A}_{A,\leq,j,p} \models \phi_d(a_1,...,a_k)$

For the applications we need the theorem in a somewhat stronger form. Namely, for each $a \in A^k$ there will be not only one variable x_a but a set of variables, altogether no more then c. More precisely let Γ be a finite set (we will assume in the theorem that $|\Gamma| \leq c$) and for each pair $a \in A^k$, $\gamma \in \Gamma$ let $x_{a,\gamma}$ be a variable. Now a system of linear equations will be of the form $\sum_{a\in A^k,\gamma\in\Gamma} u_{a,\gamma}^{(i)} x_{a,\gamma} = b_i$, $i = 1,...,l$. The system will be called symmetric if for all permutation π of A, $\gamma \in \Gamma$ and $i = 1,...,l$ there is an $i' = 1,...,l$ so that for all $a \in A^k$ we have $u_{a\pi,\gamma}^{(i)} = u_{a,\gamma}^{i'}$.

Theorem 2. *For all prime number p and natural number k there are natural numbers c, j so that for all natural number n the following holds:*

Suppose that A is a set with n elements, $\mathcal{A} = \langle A, \leq, ...\rangle$ is an interpretation of the theory T_j^p, Γ is a finite set with at most c elements, l is a natural number, and for all $i = 1,...,l$, $a \in A^k$, $\gamma \in \Gamma$ we have $u_{a,\gamma}^{(i)} \in Z_p$ and $b_i \in Z_p$. If the linear system $\sum_{a\in A^k,\gamma\in\Gamma} u_{a,\gamma}^{(i)} x_{a,\gamma} = b_i$, $i = 1,...,l$ is symmetric and it has a solution in Z_p then it also has a solution $x_{a,\gamma} = t_{a,\gamma}$ in Z_p so that for each fixed $d \in Z_p$ and $\gamma \in \Gamma$ there is a first-order formula $\phi_{d,\gamma}(y_1,...,y_k)$ of the language L_j^p so that the length of $\phi_{d,\gamma}$ is at most c and for each $a = \langle a_1,...,a_k\rangle$ we have:

$t_{a,\gamma} = d$ *iff* $\mathcal{A}_{A,\leq,j,p} \models \phi_{d,\gamma}(a_1, ..., a_k)$.

The theorem has a Corollary which is used in the mentioned applications. It was noticed on specific examples that if the symmetric system

(**3**) $\quad \sum_{a \in A^k, \gamma \in \Gamma} u^{(i)}_{a,\gamma} x_{a,\gamma} = b_i, \quad i = 1, ..., l$

can be given in a "uniform" way in n then the fact whether the system has a solution or not, depends only on the residue of n modulo p^ν, where ν depends only on k. (Here we used the world uniform in the general sense not as a mathematical concept.) To show an example of such a system we need the following definition. The *symmetric hull* of a system of linear equations is the smallest system of symmetric linear equations containing it. E.g. if $A = \{1, ..., n\}$ and $k = 2$ then the symmetric hull of the system consisting of the single equation $x_{\langle 1,2\rangle} - x_{\langle 2,1\rangle} = 0$ is the set of all equations $x_{\langle i,j\rangle} - x_{\langle j,i\rangle} = 0$ for $i, j \in \{1, ..., n\}$, $i \neq j$. Clearly this definition has some uniformity in n. In a similar way if we give a set equations each containing only variables of the type $x_{\langle i,j\rangle}$ where $i, j \in \{1, ..., c\}$, $i \neq j$, then for any n we may consider the symmetric hull of this set of equations. This defintion again seems to be uniform. An other type of defintions is illustrated by the following the following example: our system is the symmetric hull of the equation

(**4**) $\quad \sum_{i=2}^{n} x_{\langle 1,i\rangle} = 1.$

If $n = 3$ this equation is simply $x_{\langle 1,2\rangle} + x_{\langle 1,3\rangle} = 1$. We may get the general equation from this in the following way. Let $A_0 = \{1\}$, $A' = \{1, 2, 3\}$. Let $u'_{\langle i,j\rangle}$ be the coefficient of $x_{\langle i,j\rangle}$ in the equation $x_{\langle 1,2\rangle} + x_{\langle 1,3\rangle} = 1$. For each permutation π of $A = \{1, ..., n\}$ which fixes the elements of A_0 if $i\pi \in A'$, $j\pi \in A'$ then let $u_{\langle i,j\rangle} = u'_{i\pi,j\pi}$. The coefficients $u_{\langle i,j\rangle}$ define the equation (4). (That is the elements in A' serve as a model for determining the coefficients belongong to arbitrary elements of A.)

These examples motivate the following definition.

Defintions. 1. Let A' be a subset of A. Suppose that u' is a Z_p-valued function defined on $A^k \times \Gamma \times \{1, ..., l\}$, $A_0 \subseteq A'$, $|A' - A_0| > k$ and b is a Z_p valued function defined on $\{1, ..., l\}$. (The values of b will be denoted by $b_1, ..., b_l$). We will say that the system

(**5**) $\sum_{a\in A^k,\gamma\in\Gamma} u^{(i)}_{a,\gamma}x_{a,\gamma} = b_i, \quad i = 1,...,l$

is based on the quadruplet u', A', A_0, b if the following holds: for all $i = 1,...,l$ and $\langle a,\gamma\rangle \in A^k \times \Gamma$ if

(a) π is a permutation of A which fixes each element of A_0 and

(b) $a\pi \in (A')^k$,

then $u^{(i)}_{a,\gamma} = u'(\langle a\pi,\gamma,i\rangle)$.

2. We will say that a symmetric system E is induced by the quadruplet u', A_0, A', b (over A) if E is the symmetric hull of a system based on this quadruplet.

Remark. The $|A' - A_0| > k$ assumption implies that if a system based on a quadruplet then it is uniqaly determined by it. Indeed if $a \in A^k$ then because of this assumption there is always a permutation π fixing each element of A_0 so that $a\pi \in (A')^k$ and therefore the coefficients of the equations are determined by the identities $u^{(i)}_{a,\gamma} = u'(\langle a\pi,\gamma,i\rangle)$. Clearly this also implies there can be only a single linear system induced by a quadruplet.

Corollary 6 . *For all positive integers k, s and prime p there is a positive integer ν so that if $1 \le l \le s$, the sets $A_0 \subseteq A'$, Γ have at most s elements, $|A - A_0| > k$, u' is a Z_p valued function on $(A')^k \times \Gamma \times \{1,...,l\}$ and b is a Z_p valued function on $\{1,...,l\}$ then the following holds:*

There is a a subset Q of the residue classes modulo p^ν, so that for any sufficiently large n, if A is a set containing n elements, $A' \subseteq A$, and the symmetric system E is induced by the quadruplet u', A_0, A', b over A, then E has a solution iff $n \equiv d \pmod{p^\nu}$ for some $d \in Q$.

In the theorems and corollary described above the variables of the linear equations are assigned to sequences of length k formed from the elements of A. We may have used not sequences, but other type of structures formed from at most k elements of A, like e.g. subsets of size k or sequences of length k with different elements. In these and similar cases the theorem and corollary remain true. In section 4 we give a more general formulation of our results in this sense. This formulation (although

it is not more difficult to prove then the present one) is more convininet for the applications. From the point of view of representation theory the natural formulation is the following: first we fix a partition $\mu_1, ..., \mu_i$ of n, (that is, $n = \mu_1 + ... + \mu_i$) so that $\mu_1 = n - k$. The variables are assigned to the partitions of the set A into classes of sizes $\mu_1, ..., \mu_k$. We will prove our results in this form and show in section 4 that the other forms follow from this easily.

2. In this section we give a formulation of our results using the terminology of representation theory. We sketch the definitions of those concepts of the representation theory of the symmetric group which are needed to understand the statement of the theorem. (See also [J]).

If $\mu = \langle \mu_1, ..., \mu_i \rangle$ is a partition of the positive integer n then a μ tabloid is a partition of the set $\{1, ..., n\}$ into i numbered classes so that the jth class has μ_j elements for $j = 1, ..., i$. The classes will be also called the rows of the tabloid.

If π is a permutation of $\{1, ..., n\}$ and t is a μ tabloid then $t\pi$ will be the μ tabloid whose jth row is $\{x_1\pi, ..., x_{\mu_j}\pi\}$, where $\{x_1, ..., x_{\mu_j}\}$ is the jth row of t.

M^μ will be a vectorspce (in our case over Z_p) whose basis is the set of μ-tabloids, in other words the vectorspace of the formal sums $\sum_{t\in T} \alpha_t t$ where T is the set of μ tabloids. We define the action of a $\pi \in S_n$ by $(\sum_{t\in T} \alpha_t t)\pi = \sum_{t\in T} \alpha_t t\pi$. We may extend this oprartion in a natural way to the group algebra $Z_p\mathbf{S}_n$. Under this operation M^μ is a $Z_p\mathbf{S}_n$-module.

As we were able to use the notion of first-order definability for solutions of eqautions we will use this concept also for the elements of M^μ or more generally an element of a direct sum of finitely many modules M^μ. The following definitions are necessary for this purpose.

Definitions. 1. Assume that $\mu = \langle \mu_1, \ldots, \mu_i \rangle$, is a partition of n and of $\mu_1 = n-k$. Assume further that $x_1, \ldots, x_k$ are distinct elements of $\{1, ..., n\}$. We will denote by $\mathrm{td}^{(k)}(x_1, \ldots, x_k) = \mathrm{td}(x_1, \ldots, x_k)$ the μ-tabloid t that we get in the following way. The first row is $\{1, ..., n\} - \{x_1, \ldots, x_k\}$. If for each $j = 2, \ldots, i$, $\sum_{r=2}^{j-1} \mu_r = s_j$ then the $j+1$-th row consists of the elements $x_{s_j+1}, \ldots, x_{s_j+\mu_j}$. (In other words we put the elements $x_1, \ldots, x_k$ in row number 2,...,$j+1$ of t so that we are using the elements x_i in the given order and try to fill up those rows first wich have smaller row-numbers.)

If $l \geq k$, then let $\mathrm{td}^{(l,k)}(x_1, \ldots, x_k, \ldots, x_l) = \mathrm{td}^{(k)}(x_1, \ldots, x_k)$

2. Suppose that $\lambda^1 = \langle \lambda^1_1, ... \rangle, ..., \lambda^r = \langle \lambda^r_1 ... \rangle$ is a sequence of partitions of n so that $\lambda^i_1 \geq n - k$, $i = 1, ..., l$. If $u \in M = \bigoplus_{r=1}^{l} M^{\lambda^r}$ and $x \in Z_p$ and $1 \leq i \leq r$ then $\mathrm{set}(u, i, x)$ will be the set of all sequences $a = \langle a_1, ..., a_k \rangle$ so that if $u = u_1 + ... + u_l$ then the coefficient of u_i belonging to the tabloid $\mathrm{td}^{k, n-\lambda^i_1}(a_1, ..., a_k)$.

Theorem 7 . *For all positive integers k, l and prime p, there is a positive integer d so that for all positive integer n the following holds. Suppose that λ^r, $r = 1, \ldots, l$ is a sequence of partitions of n, and for each fixed r, $\lambda^r = \langle \lambda^r_1, \ldots \rangle$. If $\lambda^r_1 \geq n - k$ for $r = 1, \ldots, l$ and N is a $Z_p\mathbf{S}_n$submodule of the direct sum $\bigoplus_{r=1}^{l} M^{\lambda^r}$ then there is a subset G of N containing at most d elements so that G generates N (as a submodule) and for each fixed $g \in G$, $x \in Z_p$ and $j = 1, ..., l$ there is a first-order formula $\phi_{g,x,j}(y_1, ..., y_k)$ of the language L^p_j so that the length of $\phi_{g,x,j}$ is at most c and for each $a = \langle a_1, ..., a_k \rangle$ we have:*

$a \in \mathrm{set}(g, x, j)$ iff $\mathcal{A}_{A,\leq,j,p} \models \phi_d(a_1, ..., a_k)$.

Sketch of the proof. Assume that N is a submodule, for the sake of simplicity we assume that $N \subseteq M^\mu$. (The general case when S^μ is a submodule of a direct sum can be reduced to this with some kind of diagonalization procedure.) According to James's submodule theorem, either $N \supseteq S^\mu$ or $N \subseteq (S^\mu)^\perp$. If $N \supseteq S^\mu$ then N is isomorphic to a submodule of the factor-module M^μ / S^μ. In either case the modules containing N are of simpler structure then the original module M^μ (they do not contain the irreducible module D_μ as a factor), which makes possible the application of our inductive assumption. It creates however considerable difficulties that the property that we want to prove (the existence of a first-order definable system of generators) is not necessarily invariant under isomorphisms, while the simpler structures of the mentioned modules implies only that there are isomorphic modules where the induction hypothesis can be applied. (In principle e.g. it would be possible that N has two isomorphic copies in M^μ so that one has such a set of generator the other not). To resolve these type of problems we have to build up a detailed theory of submodules with first-order definable generators, and also use deep theorems (of the charactersitic free representation theory as given in [J]). This theory describes several

important properties of the factor module M^μ/S^μ which are valid independently of the characteristic of the field F.

3. Proof of Theorem 7. In this section we assume that the reader is familiar with some of the notions and theorems of the theory of the representations of the symmetric group as as it is developed in [J]. The following notions and theorems are essential for us:

μ tableaux , μ tabloids, the module M^μ, the module S^μ, the sumbmodule theorem, the standard basis of S^μ, pairs of permutations μ^*, μ, the module $S^{\mu^*,\mu}$, a basis for $S^{\mu^*,\mu}$

the notion of μ-tableaux, μ-tabloids

The following definitions will be helpful when we are speaking about first-order definability in the sense of Theorem 7.

Definitions. 1. Assume that $\langle A, \leq\rangle$ is a finite odered set, l is a positive integer, and A^l is the set of all l-tuples formed from A. If c is a positve integer we say that a $B \subseteq A^l$ is c, p, A-definable if there is a $j \leq c$ and an interpretation $\mathcal{A}$ of T_j^p on the universe A so that $\leq_{\mathcal{A}}$ and $\leq$ are identical and there is a formula $\phi(x_1, \ldots, x_l)$ of L_j^p of length at most c with l free variables, so that for all $b_1, \ldots, b_l \in A$ we have that $\langle b_1, \ldots, b_l\rangle \in B$ iff $\mathcal{A} \models \phi(b_1, \ldots, b_l)$. If the choice of p and A is clear from the context we will say that B is c-definable.

Suppose that p is a prime and l is a positive integer, and $\langle A, \leq\rangle$ is an ordered set. Assume further that f is a function defined on a subset of A^l with values in Z_p, where Z_p is a field with p elements. We say that f is c, p, A-regular if for each $a \in Z_p$ the set $f^{-1}(a)$ is c, p, A-definable. (Again we will use the expression c-regular if the choice of p and A is clear.)

We will use the following uniform version of the notions of $c$defianblity/regularity. Suppose that A_n is a finite set and $B_n \subseteq A_n^l$ for all but a finite number of integers n. We say that B_n is uniformly c, p, A-definable if each fixed B_n is c, p, A_n-definable and in the definiton of a, p, A_n definability $\mathcal{A} \models \phi(b_1, \ldots, b_l)$ holds with the same formula ϕ for all n. We will use this definition exclusively with $A_n = \{1, ..., n\}$.

It is a consequence of this definiton that the domains of a uniformly c-regular family of functions is uniformly c-definable.

Suppose that for all but a finite number of positive integers n f_n is a function defined on a subset of A_n^l. The family of functions f_n will be called uniformly c-regular if for each $a \in Z_p$ the family of sets $f_n^{-1}(a)$ is uniformly c-regular. (Again it is a consequence of this definiton that if f_n is uniformly c-regular then domain(f_n) is uniformly c-definable.)

2. Assume that n is a positive integer and $\mu = \langle \mu_1, \ldots, \mu_i \rangle$ is a sequence of nonnegative integers. We say that μ is a partition of n if $n = \mu_1 + \ldots + \mu_i$. μ is called a proper partition if $\mu_1 \geq \ldots \geq \mu_i$. tbld_μ will denote the set of all μ tabloid.

3. Assume that μ, n and k are the same as in the previous definiton and $x_1, \ldots, x_k \in I_n$. $\mathrm{tab}(x_1, \ldots, x_k)$ will denote the tableau that we get from the tabloid $\mathrm{td}^{(k)}(x_1, \ldots, x_k)$ by arranging the elements of each of its rows in an increasing order.

4. If l, i are a positive integers then I_l will denote the set $\{1, ..., l\}$ and $I_{l,i}$ will denote the set of all sequences of length i formed from the elements of $1, ..., l$.

5. Assume that, Γ is a finite set and for all $\gamma \in \Gamma$, $\mu^\gamma = \langle \mu_1^\gamma, \ldots \rangle$ is a partition of n and $\mu_1^\gamma \geq k$. Let M_Γ be the direct sum of all of the modules M^{μ^γ}, that is, $M_\Gamma = \bigoplus_{\gamma \in \Gamma} M^{\mu^\gamma}$. We get a linear basis of M_Γ by taking the union of the tabloid basis of each direct summand M^{μ^γ}. We may associate the elements of this basis in a natural way with the elements of T_Γ, where T_Γ is the set of all pairs $\langle \gamma, \{t\} \rangle$, where $\gamma \in \Gamma$ and $\{t\}$ is a μ^γ-tabloid. Assume now that $\Gamma = I_l$ for some $l \leq n$, where $I_l = \{1, ..., l\}$. If $a \in M_\Gamma$ then we define a function h on a subset of $I_{n,k+1}$ with values in T_Γ. (This will code the elemeents of the basis T_Γ by sequences of integers.) Let $r = n - \mu_1^{x_{k+1}}$. $h(x_1, \ldots, x_k, x_{k+1})$ will be defined iff $x_{k+1} \in I_l = \Gamma$ and $\mathrm{td}^{k,r}(x_1, ..., x_k)$ is defined. In this case let and $h(x_1, \ldots, x_{k+1}) = \langle x_{k+1}, \mathrm{td}^{k,r}(x_1, \ldots, x_k) \rangle$.

6. If $a \in M_\Gamma$ then we may define a function f_a on a subset of $I_{n,k+1}$ in the following way. $f_a(x_1, ..., x_{k+1})$ is defined iff $h(x_1, ..., x_{k+1})$ is defined and in this case $f_a(x_1, ..., x_{k+1})$ is the coefficient of the basis element $h(x_1, ..., x_{k+1})$ in the representation of a as a linear combination of the elements of T_Γ. We will say that the element a is c-regular if the function f_a is c-regular.

7. If $\mu = \langle \mu_1, \ldots \rangle$ is a partition of n and $\mu_1 = n - k$, then for an arbitrary Z_p-valued function f defined on the set of μ-tabloids we may define a function $\bar{f}$ on A^k

by $\bar{f}(x_1,\ldots,x_k) = f(\mathrm{td}(x_1,\ldots,x_k))$. ($\bar{f}$ is defined iff td is defined). We say that f is d-regular iff $\bar{f}$ is d-regular. (We will use later the fact that domain(td) is c-definable for some c depending only on k.)

Following [J] we say that μ^*, μ is a pair of partitions if $\mu = \langle \mu_1, ..., \mu_i \rangle$ is a partition of n, $\mu^* = \langle \mu_1^*, ..., \mu_i^* \rangle$ is a proper partition of some positive integer not greater than n, $\mu_1^* = \mu_1$ and for all $j = 1, ..., i$, $\mu_j^* \leq \mu_j$.

Definitions. 1. If t is a μ-tableau then let C_t be the group of coloumn permutations of t, that is the set of all permutations π so that for each $i \in I_n$, i and $i\pi$ are in the same coloumn of t. If μ^*, μ is a pair of partitions and t is a μ-tableau, then we say that an element of t is outside μ^* if it is in the j-th element of the i-th row and $\mu_i^* < j$. Let C_t^* be the set of those permutations of C_t which fix each element of t which are outside μ^*.

2. If μ^*, μ is a pair of partitions, t is a μ-tableau then let $e_t^{\mu^*,\mu} = \sum_{\pi \in C_t^*} \mathrm{sgn}(\pi)\{t\}\pi$, where $\mathrm{sgn}(\pi) = 1$ if π is even, otherwise $\mathrm{sgn}(\pi) = -1$. $S^{\mu^*,\mu}$ is the linear subspace of M_μ spanned by all of the elements $e_t^{\mu^*,\mu}$. $S^{\mu^*,\mu}$ is a submodule of M_μ. In [J] a linear basis of $S^{\mu^*,\mu}$ is given, Theorem 17.13, p. 69., we will refer to this basis as the standard basis of $S^{\mu^*,\mu}$. We will use only the following porperties of this basis:

(a) the standard basis of $S^{\mu^*,\mu}$ can be given in the form of $\{e_t^{\mu^*,\mu} | t \in T^{\mu^*,\mu}\}$, where $T^{\mu^*,\mu}$ is a subset of the set of μ-tableaux (depending on μ^*), and each $t \in T^{\mu^*,\mu}$ is standard inside μ^*, that is those elements of the tableau t which are not outside μ^* are increasing from left to right in each row and they are also increasing down in each coloumn.

(b) the set $\{\langle x_1,\ldots,x_k\rangle \in A^k | \mathrm{tab}(x_1,\ldots,x_k) \in T^{\mu^*,\mu}\}$ is c-definable, where c-depends only on k.

(c) if t, t' are distinct elements of the $T^{\mu^*,\mu}$, then the tabloids $\{t\}$ and $\{t'\}$ are also distinct

The facts listed in (a) are explicitely stated in section 17 of [J]. (b) and (c) are immediate consequences of Theorem 17.13, p. 69 of [J]. We do not formulate the theorem here since it involves definitions that we do not need in this paper.

3. Assume that μ^*, μ is a pair of partition for n and $\mu_1 = \mu_1^* = n - k$. Let $T = T^{\mu^*,\mu}$. Since $\{e_t^{\mu^*,\mu} | t \in T\}$ is a basis of $S^{\mu^*,\mu}$, each $a \in T$ can be written in a unique way in the form of $\sum_{t \in T} c_t e_t$. We will say that the element a is c-regular with respect to the standard basis of $S^{\mu^*,\mu}$ if the function $c_{\mathrm{tab}(x_1,\ldots,x_n)}$ is c-regular.

4. As in the case of μ-tabloids, we define the notion of d-regularity for an arbitrary function f defined on $T^{\mu^*,\mu}$. If f is an arbitrary function defined on $T^{\mu^*,\mu}$ with values in Z_p we say that f is d-regular iff $f(\mathrm{tab}(x_1,\ldots,x_k))$ is d-regular. (We will use later the fact that domain(tab) is c-definable, and (as we have remarked at the definition of $T^{\mu^*,\mu}$) $\{\langle x_1,\ldots,x_k\rangle | \mathrm{tab}(x_1,\ldots,x_k) \in T^{\mu^*,\mu}\}$ is also c-definable for some c depending only on k.)

Definiton. Suppose that $\mathcal{A}_1 = \langle A_1, \leq \ \ldots\rangle$ $\mathcal{A}_2 = \langle A_2, \leq \ \ldots\rangle$ are models of T_s^p. dist will denote the distance function on A_i, $i = 1, 2$, that is if $a, b \in A$ then $\mathrm{dist}(a,b) = |\{x \in A_i \mid \min(a,b) \leq x < \max(a,b)\}|$. Suppose that $a = \langle a_1, ..., a_l\rangle$ resp. $b = \langle b_1, ..., b_l\rangle$ are sequences from the elements of A_1 resp A_2 and m is a positive integer. We say that a and b are m isomorphic (with respect to $\mathcal{A}_1$, $\mathcal{A}_2$) iff for all $1 \leq i\ l$ and $1 \leq j \leq l$ the following four requiremnts are met.

(a) $a_i \leq a_j$ iff $b_i \leq b_j$

(b) if $\mathrm{dist}(a_i, a_j) \leq m$ then $\mathrm{dist}(a_i, a_j) = \mathrm{dist}(b_i, b_j)$

(c) if $\mathrm{dist}(b_i, b_j) \leq m$ then $\mathrm{dist}(a_i, a_j) = \mathrm{dist}(b_i, b_j)$

(d) $R_{r,r'}(a_i) = R_{r,r'}(b_i)$ for all $r = 1, ..., s$, $r' = 1, ..., p^s$.

We will say that a and b are strongly m-ismorphic (with respect to $\mathcal{A}_1, \mathcal{A}_2$) iff the sequnces $\langle a_1, ..., a_l, o_1, i_1\rangle$ $\langle b_1, ..., b_l, o_2, i_2\rangle$ are m-isomorphic, where o_r is the smallest and i_r is the greatest element of the ordered set $A_r, \leq$ for $r = 1, 2$.

Lemma 8. *For all positive integers d, l and prime p there is a positive integer m so that the following holds. If $\phi(x_1,\ldots,x_l)$ is a formula of L_d^p of length at most d and $\mathcal{A}_1 = \langle A_1, \leq, \ldots\rangle$ $\mathcal{A}_2 = \langle A_2, \leq, \ldots\rangle$ are models of T_d^p and $a = \langle a_1,\ldots,a_l\rangle$ resp. $b = \langle b_1,\ldots,b_l\rangle$ are strongly m-isomorphic sequences from the elements of A_1 resp. A_2, then $\mathcal{A}_1 \models \phi(a_1,\ldots,a_l)$ iff $\mathcal{A}_2 \models \phi(b_1,\ldots,b_l)$.*

Proof. In this proof we will assume that $A_1 = \{1, ..., n_1\}$ and $A_2 = \{1, ..., n_2\}$ for some positive integers n_1, n_2.

Assume that ϕ is in prenex form and the number of quantifiers in ϕ is r. We prove the Lemma by induction r. (We will denote by $m_{r,l,d}$ the value of m in the lemma belonging to the corresponding values of the parameters r, l, d.) If ϕ is a propositional formula then the statement is an immediate consequence of the definition of m-isomorphism. Assume now that ϕ is in prenex form with r-quantifiers starting with the quantifier $\exists$, and the lemma is true with $r \to r-1$ and with any values of the parameters d, l. (We will assume that both sequences contain the greatest and smallest element of the corresponding universe. Beacuse of this assumption we may speak about m isomorphism instead of strong m isomorphism.) Suppose that the sequences $a = \langle a_1, ..., a_l \rangle$, $b = \langle b_1, ..., b_l \rangle$ are $m_{r,l,d}$ if $m_{r,l,d} > 4m_{r-1,l+1,d}$. Assume further that $\mathcal{A}_1 \models \exists x,\ \phi'(x, a_1, ..., a_l)$. Let $x_0 \in A$ with $\mathcal{A}_1 \models \phi(x_0, a_1, ..., a_l)$. Let $1 \leq i \leq l$ so that $y = x_0 - a_i$ has minimal absolute value. We claim that if $|y| \leq 2m_{r-1,l+1,d}$ then the sequences $a' = \langle x_0, a_1, ..., a_l \rangle$ and $b'' = \langle b_i + y, b_1, ..., b_l \rangle$ are $m_{r-1,l+1,d}$ isomorphic and if $|y| > 2m_{r-1,l+1,d}$ then the sequences $a' = \langle x_0, a_1, ..., a_l \rangle$ and $b'' = \langle b_i + z, b_1, ..., b_l \rangle$ are $m_{r-1,l+1,d}$ isomorphic, where z is an integer with the properties

(9) $\quad y \equiv z \pmod{p^d}$ and

(10) $\quad |z - \frac{y}{|y|} 2m_{r-1,l+1,d}| < p^d + 1.$

Indeed if $y \leq 2m_{r-1,l+1,d} = m'$ then the $m_{r,l,d}$ isomorphisms of the sequences a, b and $m_{r-1,l+1,d} < 4m_{r,l,d}$ implies this. If $y > 2m'$ where $m' = m_{r-1,l+1,d} =$ then the distance of x_0 from any points of a is at least $2m'$. If $[a_j, a_{j'}]$ is the minimal interval formed from the elements of a that contains x_0 then $a_j - a_{j'} > 4m'$ and so by the $m_{r,l,d}$ isomorphism of a and b we have that $b_j - b_{j'} > 4m'$. Clearly the interval $[b_j, b_{j'}]$ contains $b_i + z$ and so according to 10 the distance of z from any elements of the sequence b is at least $\frac{3}{2}m'$, which together with (9) implies the m' isomorphism of a' and b''.

In either cases applying the inductive hypothesis with $r \to r-1$, $l \to l+1$ we get that $\mathcal{A}_2 \models \phi'(b_i + w, b_1, ..., b_l)$ for some integer w that is $\mathcal{A}_2 \models \phi(b_1, ..., b_l)$.

If ϕ starts with a $\forall$ quantifier then we apply the lemma for $\neg\phi \equiv \exists x \ldots$.

Corollary 11. *For all positive integers d, l and prime p there is a positive integer m so that the following holds. If $\phi(x, x_1, \ldots, x_l)$ is a formula of L_d^p of length at most d, $\mathcal{A}_1 = \langle A_1, \leq, \ldots\rangle$ $\mathcal{A}_2 = \langle A_2, \leq, \ldots\rangle$ are models of T_d^p and $a = \langle a_1, \ldots, a_l\rangle$, resp. $b = \langle b_1, \ldots, b_l\rangle$ are strongly m-isomorphic sequences from the elements of A_1 resp. A_2, then the number of elements in the following two sets are congruent modulo p:*

$X_a = \{x \in A_1 \mid \mathcal{A}_1 \models \phi(x, a_1, \ldots, a_l)\}$ *and*

$Y_b = \{x \in A_2 \mid \mathcal{A}_2 \models \phi(x, b_1, \ldots, b_l)\}$.

Proof. We assume again that $A_1 = \{1, ..., n_1\}$ and $A_2 = \{1, ..., n_2\}$. The strong m isomorphism of a and b implies that $n_1 \equiv n_2 \pmod{p^d}$. As in the previous proof we may assume that the smallest and

greatest elements of the universes are included in the correspomdimg sequences. Let $m_{l,d}$ be the number whose existence is guaranteed by Lemma 11 for some fixed l and d and let $m = 2lm_{l+1,d}$. Let S_a be the set of all elements of A whose distance from the set $\{a_i\}_{i=1}^l$ is at most $m_{l+1,d}$ and S_b defined in an anlogue way for the sequence b. Clearly the m-isomorphism a and b can be extended in a unique way into an $m_{l+1,d}$ isomorphism between a', b' where a', b' are extensions of the sequences a, b with elements from S_a resp. S_b so that each element of S_a resp. S_b is used. Let κ be the one-to-one map between S_a and S_b induced by this isomorphism. Clearly if $x \in S_a$ then the sequences $\langle x, a\rangle$, $\langle \kappa(x), b\rangle$ are $m_{l+1,d}$ isomorphic and therfore, by Lemma 8,

(**12**) $\quad |S_a \cap X_a| = |S_b \cap X_b|$.

For any $x \in A_1 - S_a$ and $y \in A_2 - S_b$ if $x \equiv y \pmod{p^d}$ then the sequences $\langle x, a\rangle$ and $\langle y, b\rangle$ are $m_{l+1,d}$-isomorphic and so by Lemma 8:

(**13**) $\quad$ for all $x \in A_1 - S_a$, $y \in A_2 - S_b$, $x \equiv y \pmod{p}$ we have $x \in X_a$ iff $y \in X_b$.

The $m_{l+1,d}$ isomorphism of $\langle x, a\rangle$ and $\langle \kappa(x), b\rangle$ imply that the number of elements of $S_a \cap X_a$ and $S_b \cap X_b$ which are in any fixed residue class c modulo p is the same. Therefore $n_1 \equiv n_2 \pmod{p^d}$ and (13) imply that $|\{x \in X_a | x \equiv c \pmod{p}\}| \equiv |\{y \in X_b | y \equiv c \pmod{p}\}|$, therefore according to (13) $|X_a - S_a| \equiv |X_b - S_b| \pmod{p}$ and so by (12) $|X_a| \equiv |X_b| \pmod{p}$.

Corollary 14. *For all positive integers l, d and prime p there is a d' so that if $\phi(x, y_1, ..., y_l)$ is a first-order formula of L_d^p of length at most d with the free variables $x, y_1, ..., y_l$ then there exists a d' so that the following holds: For each positive integer n we define a function f_n on $I_{n,l} = (I_n)^l$ with values in Z_p in the following way. If $a_1, ..., a_n \in I_n$ then $f_n(a_1, ..., a_n)$ is the residue class of the number of elements of the set $\{x \in I_n \mid \mathcal{A}_{I_n, \leq, d, p} \models \phi(x, a_1, ..., a_l)\}$ modulo p.*

Then the family of functions f_n is uniformly d'-regular

Proof. We divide the sequences $\langle a_1, ..., a_l, n\rangle$, $a_i \in I_n, i = 1, ..., l$ into equivalence classes in the following way: $\langle a_1, ..., a_l, n_1\rangle$ and $\langle b_1, ..., b_l, n_2\rangle$ are in the same class if the sequences $\langle a_1, ..., a_l\rangle$ and $b_1, ..., b_l$ are strongly m isomorphic with respect to I_{n_1}, I_{n_2}, where m is the positive integer whose existence was guaranteed by Corollary 11.

According to the definiton of m-isomorphism the number of equivalence classes depends only on p, d, l and m and so, by Corollary 11 only on p, d and l. Therefore there is an n_0 depending only on p, d and l so that each equivalence class contains an element $\langle a_0, ..., a_l, n_0\rangle$. Therefore $f_n(b_1, ..., b_l) = c$ iff

(**15**) "there is a sequence $a = \langle a_0, ..., a_l\rangle$, $a_i \leq n_0$, $i = 1, ..., n_0$ so that the sequences a and $\langle b_1, ..., b_l\rangle$ are m isomorphic and $f_c(a_1, ..., a_l) = c$."

It is easy to see that there is a first-order formula ψ depending only on p, d, l and ϕ (form the uniform definition of the family f_n) so that (15) holds iff $\mathcal{A}_{I_n, \leq, d', p} \models \psi(a_1, ..., a_2)$ which completes the proof of Lemma (14).

Lemma 16 . *For all positive integers d, l and prime p there is a positive integer d' so that the following holds. Assume that $c_1, c_2 \in Z_p$*

(**17**) *If f, g are d regular functions on A^l then $c_1 f + c_2 g$ and fg are d' regular.*

(**18**) *If f_n, g_n are uniformly d regular families of functions, then $c_1 f_n + c_2 g_n$ and $f_n g_n$ are uniformly d' regular.*

Proof. We prove only (17), the other statement can be proved in an analogue way. It is clear that $f' = c_1 f$ is d regular since if $c_1 \neq 0$ the $f'^{-1}(c) = f^{-1}(c_1^{-1} c)$. So

we have to prove only that $f' = f + g$ is d' regular provided that both f and g are d regular.

$f'^{-1}(c) = \bigcup_{a \in Z_p}(f^{-1}(a) \cap g^{-1}(c-a))$. Since the sets $f^{-1}(a)$ and $f^{-1}(c-a)$ are d definable and the number of terms in the union depends only on p we have that $f'^{-1}(c)$ is d'-definable which completes the proof of the d' regularity of $c_1 f_1 + c_2 f_2$. The d' regularity of fg can be proved in a similar way.

Lemma 19. *For all positive integers d, l and prime p there is a positive integer d' so that the following holds.*

Assume that $\langle A^l, \leq \rangle$ is an ordered set, f is a d-regular function defined on A^l with values in Z_p, $0 \leq k \leq l$ and f' is a function defined on A^k by $f'(a_1, \ldots, a_k) = \sum\{f(a_1, \ldots, a_k, b_1, \ldots, b_{l-k}) |\ \langle b_1, \ldots, b_{l-k} \rangle \in A^{l-k}\}$. Then f' is d'-regular.

Moreover if the family of functions f_n is uniformly d-regular then the family of functions $f'_n(a_1, \ldots, a_k) = \sum\{f_n(a_1, \ldots, a_k, b_1, \ldots, b_{l-k}) |\ \langle b_1, \ldots, b_{l-k} \rangle \in A^{l-k}\}$ is uniformly d'-regular.

We prove only the non-uniform version of the lemma. The proof can be easily modified for the uniformity.

Assume first that $l = 1$. For each $c \in Z_p$ let f_c the function that we get from f by changing all it's non-c values into zero and let f'_c

$f'_c(a_1, \ldots, a_k) = \sum\{f_c(a_1, \ldots, a_k, b_1, \ldots, b_{l-k}) |\ \langle b_1, \ldots, b_{l-k} \rangle \in A^{l-k}\}$.

Clearly $f' = \sum_{c \in Z_p} f'_c$. According to Lemma 16 it is enough to show that each f'_c is d' regular. (The $c = 0$ case is trivial since $f'_c \equiv$).) Let $c, u \in Z_p$, $c \neq 0$ be fixed. $f'_c(a_1, ..., a_k) = u$ iff the number of elements in the set $\{b \in A | f_c(b, a_1, ..., a_l) = c\}$ is congruent to $c^{-1}u$ modulo p. Therefore d regularity of f_c and Corollary 14 implies that $(f')_c^{-1}(u)$ is d' regular which completes the proof of the $l = 1$ case.

We prove the general case by induction on l. Assume that the lemma is true with $l \to l - 1$. Let

$\bar{f}(a_1, \ldots, a_k, b_{l-k}) = \sum\{f(a_1, \ldots, a_k, b_1, \ldots, b_{l-k}) |\ \langle b_1, \ldots, b_{l-k-1} \rangle \in A^{l-k-1}\}$.

According to the inductive assumption the function $\bar{f}$ is d'-regular. Since $f'(a_1, \ldots, a_k) = \sum\{\bar{f}(a_1, \ldots, a_k, b) |\ b \in A\}$, the $l = 1$ case implies the d'' regularity of f'.

Lemma 20. *For all positive integers k_1, k_2, d and prime p there is a positive integer d' so that the following holds.*

Assume that ϕ is a linear transformation from M^μ to M^λ where $\mu = \langle \mu_1, \ldots \rangle$, $\lambda = \langle \lambda_1, \ldots \rangle$, $\mu_1 = k_1$, $\lambda_1 \leq k_2$. Suppose that for each μ tabloid τ we have $\tau\phi = \sum_{\tau' \in \mathrm{tbld}_\lambda} c_{\tau,\tau'}\tau'$. If the function $f(x_1, ..., x_{k_1, y_1, ..., y_{k_2}}) = c_{\mathrm{td}(x_1,...,x_{k_1}),\mathrm{td}(y_1,...,y_{k_2})}$ is d-regular and $a \in M^\mu$ is d-regular with respect to the tabloid basis of M^μ then $a\phi$ is d' regular with respect to the tabloid basis of M^λ.

Proof. Assume that $a = \sum_{\tau \in \mathrm{tbld}_\mu} \gamma_\tau \tau$. The d regularity of a implies that the function γ_τ is d regular. Let $\leq_{k_1}$ be the lexicographic ordering on I_{n,k_1} We define a function g on I_{n,k_1} by $g(x_1, ..., x_{k_1}) = \gamma_\tau$ if $\langle x_1, ..., x_{k_1} \rangle$ is the smallest element of A^{k_1} under the ordering $\leq_{k_1}$ so that $\mathrm{td}(x_1, ..., x_{k_1}) = \tau$. If there is no such $\tau \in \mathrm{tbld}_\mu$ then $g(x_1, ..., x_{k_1}) = 0$. It is easy to see that g is d_1 regular where d_1 depends only on d, k_1, l and p.

In a similar way starting from the function $c_{\tau,\tau'}$ we define a function $h(x_1, ..., x_{k_1}, y_1, ..., y_{k_2})$. Namely $h(x_1, ...x_{k_1}, y_1, ..., y_{k_2}) = c(\tau, \tau')$ if $\mathrm{td}(y_1, ..., y_{k_2}) = \tau'$ and $\langle x_1, ..., x_{k_1} \rangle$ is the smallest element of A^{k_1} under the $\leq_{k_1}$ ordering so that $\tau = \mathrm{td}(x_1, ..., x_k)$. If there are no τ, τ' with these properties, then $h(x_1, ..., x_k, y_1, ..., y_{k_2}) = 0$.

If $a\phi = \sum_{\tau' \in \mathrm{tbld}_\lambda} \delta_{\tau'}\tau'$ then we have to show that the function $q(y_1, ..., y_{k_2}) = \delta_{\mathrm{td}}(y_1, ..., y_{k_2})$ is d' regular. Since ϕ is linear we have $q(y_1, ..., y_{k_2}) = \sum_{\tau \in \mathrm{tbld}_\mu} \gamma_\tau c_{\tau,\mathrm{td}(y_1,...,y_{k_2})} =$
$\sum\{g(x_1, ..., g_{x_k})h(x_1, ..., x_{k_1} y_1, ..., y_{k_2}) | \langle x_1, ..., x_{k_1} \rangle \in A^{k_1}\}$.

Therefore by Lemma 16 and Lemma 19 q is d'-regular.

Corollary 21 . *Lemma 20 remains true if either the domain resp. the range of ϕ (or both) is $M^{\mu^*,\mu}$ resp. $M^{\lambda^*,\lambda}$ for some μ^*, λ^* and we consider the regularity of the elements a, $a\phi$ with respect to the corresponding standard basis.*

Proof. The proof is exactly the same as that of Lemma 20.

Lemma 22. *For all positive integers d, k and prime p there is a d' so that if $n > k$, μ^*, μ is a pair of partitions for n, and $\mu_1 = \mu_1^* = n - k$ then the following holds.*

*(**23**) If $a \in S^{\mu^*,\mu}$ is d-regular with respect to the tabloid basis of M^μ, then a is d' regular with respect to the standard basis of $S^{\mu^*,\mu}$.*

*(**24**) If $a \in S^{\mu^*,\mu}$ is d-regular with respect to the standard basis of $S^{\mu^*,\mu}$ then a is d' regular with respect to the tabloid basis of M^μ.*

Proof of (24). We want to apply Corollary 21. Let ϕ be the natural injection of $S^{\mu^*,\mu}$ into M^μ and let $e_t^{\mu^*,\mu}$ be an element of the standard basis of $M^{\mu^*,\mu}$ and let τ be a μ-tabloid. According to Corollary 21 it is sufficient to prove that if $f(t,\tau)$ is the coefficient of τ in $e_t^{\mu^*,\mu}$ then the function f (more precisely the function $f(\mathrm{tab}(x_1,...,x_k), \mathrm{td}(y_1,...,y_k)))$ is d-regular, if d is sufficiently large with respect to k and p. This is however an immediate consequence of the definition of $e_t^{\mu^*,\mu}$.

Proof of (23). We define a binary relation Φ on $T^{\mu^*,\mu}$ in the following way. If $t, t' \in T^{\mu^*,\mu}$ then $t\Phi t'$ holds iff $t \neq t'$ and there is a $\pi \in C_t^*$ so that $\{t\pi\} = \{t'\}$. In other words $t\Phi t'$ iff $t \neq t'$ and the tabloid $\{t'\}$ has a non-zero coefficient in $e_t^{\mu^*,\mu}$.

Since for each $t \in T^{\mu^*,\mu}$ the elements not outside μ^* are increasing down the coloumns we have that $t, t' \in T^{\mu^*,\mu}$, $t\Phi t'$, $t \neq t'$ implies that $\{t\} \lhd \{t'\}$. Since $\lhd$ is a partial ordering we may extend Φ, based on the transitivity, into a partial ordering that we will denote by $\preceq$. In other words $t \preceq t'$ iff there is a finite sequence t_i, $i = 1,...,s$ so that $t = t_1$, $t' = t_s$ and for all $i = 1,...,s$ $t_i \preceq t_{i+1}$.

We define a partial order $\sqsubseteq$ on the set of μ tabloids in the following way. Let $\tilde{T} = \{\tau \in \mathrm{tbld}_\mu | \exists t \in T^{\mu^*,\mu} \quad \tau = \{t\}\}$. The elements of $\mathrm{tbld}_\mu - \tilde{T}$ will be pairwise incomparable under the partial ordering $\sqsubseteq$, and any element of $\mathrm{tbld}_\mu - \tilde{T}$ will be greater than any element of $\tilde{T}$. If $\tau, \tau' \in \tilde{T}$, then $\tau \sqsubseteq \tau'$ iff $\tau = \{t\}$, $\tau' = \{t'\}$ and $t \preceq t'$ for some $t, t' \in T^{\mu^*,\mu}$.

*(**25**) There is a c depending only on k, so that for any sequence $t_1, \ldots, t_s$ of the elements of $T^{\mu^*,\mu}$, if $t_i \Phi t_{i+1}$ for all $i = 1, \ldots, s-1$, then $s \leq c$.*

Proof of (25). If t is a μ-tableau then we will denote by $\mathrm{set}(t)$ the set of all elements of the tableau which is outside the first row. ($\mathrm{set}(t)$ is a subset of I_n with

k elements.) We claim that if $t\Phi t'$ then $\mathrm{set}(t') \subseteq \mathrm{set}(t) \cup I_{2k}$. This is a consequence of the fact that the elements in the first row of t are inrcreasing from the to right and therefore at the first k positions (on the left) we have the smallest k elements of the set $I_n - \mathrm{set}(t)$. Since $|\mathrm{set}(t)| = k$, they are among the elements of I_{2k}. When we apply an element of C_t^* to t only those elements may leave the first row which are in the first k coloumn, therefore every element leaving the first row is included in I_{2k} and so we have $\mathrm{set}(t') \subseteq \mathrm{set}(t) \cup I_{2k}$. This implies that for all t_i, $i = 1, ..., s$ we have $\mathrm{set}(t_i) \subseteq \mathrm{set}(t_1) \cup I_{2k}$. Since the elements of each $t \in T^{\mu^*,\mu}$ are increasing in the first row the number of $t \in T^{\mu^*,\mu}$ with $\mathrm{set}(t) \subseteq \mathrm{set}(t_1) \cup I_{2k}$ is less than c, where c depends only on k, which completes the proof of 25

Definitions. 1. If τ is a μ-tabloid then $\mathrm{depth}(\tau)$ will denote the largest positive integer i so that there is a sequence $t_1, \ldots, t_s$ $t_i \in T^{\mu^*,\mu}$ $i = 1, ..., s$, so that $\tau = \{t\}$ and for all $i = 1, \ldots, s-1$, $t_i \Phi t_{i+1}$. If there is no such sequence then $\mathrm{depth}(\tau) = 0$. ((25) implies that there is a bound, depending on only on k, on the numbers $\mathrm{depth}(\tau)$, $\tau \in \mathrm{tbld}_\mu$.)

2. If f is a function on tbld_μ then let $f_{\min}$ be the set of all minimal elements $\{\tau \in \mathrm{tbld}_\mu | f(\tau) \neq 0\}$ under the $\sqsubseteq$ partial ordering. If g is a function defined on $T^{\mu^*,\mu}$ then we define the set $g_{\min}$ in a similar way using the $\preceq$ partial ordering.

(**26**) *Suppose that f is a Z_p-valued function on* tbld_μ *and g is a Z_p-valued function on $T^{\mu^*,\mu}$ so that $\sum_{\tau \in \mathrm{tbld}_\mu} f(\tau)\tau = \sum_{t \in T^{\mu^*,\mu}} g(t) e_t^{\mu^*,\mu}$, then $\{\{t\} | t \in g_{\min}\} = f_{\min}$.*

Proof of (26). For all $t \in T^{\mu^*,\mu}$ and for all of the tabloids τ occurring with non-zero coefficient in $e_t^{\mu^*,\mu}$ we have $\{t\} \sqsubseteq \tau$. Therefore if $t \in g_{\min}$ then $\{t\}$ does not occur with a non-zero coefficient in any $e_{t'}^{\mu^*,\mu}$, $t' \in g_{\min}$, $t' \neq t$ and so $f(\{t\}) \neq 0$, that is, $\{t\} \in f_{\min}$.

Assume that $\tau_0 \in f_{\min}$. $\sum_{\tau \in \mathrm{tbld}_\mu} f(\tau)\tau = \sum_{t \in T^{\mu^*,\mu}} g(t) e_t^{\mu^*,\mu}$ implies that there is a $t \in T^{\mu^*,\mu}$ so that $g(t) \neq 0$ and τ_0 has a non-zero coefficient in $e_t^{\mu^*,\mu}$ and therefore $\{t\} \sqsubseteq \tau_0$. Let $t_0 \in g_{\min}$ so that $t_0 \preceq t$. According to the already proven part of (26) we have that $\{t_0\} \in f_{\min}$ and so $\tau_0 \in f_{\min}$, $\{t_0\} \sqsubseteq \tau_0$ implies $\tau = \{t_0\}$. Since $t_0 \in g_{\min}$ this completes the proof of (26).

If f is a Z_p-valued function on tbld_μ and $a = \sum_{\tau \in \mathrm{tbld}_\mu} f(\tau)\tau \in S^{\mu^*,\mu}$, then there is a g' so that $a = \sum_{t \in T^{\mu^*,\mu}} g'(t) e_t^{\mu^*,\mu}$. Let g be a function defined on $T^{\mu^*,\mu}$ by

$g(t) = g'(t)$ for all $t \in g'_{\min}$ and $g(t) = 0$ otherwise. Clearly $g_{\min} = g'_{\min}$ and so by (26) $\{\{t\}|t \in g_{\min}\} = f_{\min}$,

(**27**) $g(t) = f(\{t\})$ for all $t \in g_{\min}$ and $g(t) = 0$ for all $t \notin g_{\min}$.

We will denote the function g by bottom(f).

If g is an arbitrary Z_p valued function on $T_{\mu^*,\mu}$ then, trivially, there is a function f on tbld_μ so that $\sum_{\tau \in \mathrm{tbld}_\mu} f(\tau)\tau = \sum_{t \in T^{\mu^*,\mu}} g(t) e_t^{\mu^*,\mu}$. We will denote this function f by tbasis(g).

(**28**) *For all positive integers d, k and prime p there is a d' so that the following holds: If μ^*, μ is a pair of partitions of n and $\mu_1 = k$ and f, g are Z_p-valued functions defined on* tbld_μ *resp.* $T^{\mu^*,\mu}$ *then we have:*

(**29**) *if f is d-regular, then* bottom(f) *is d'-regular,*

(**30**) *if g is d-regular, then* tbasis(g) *is d'-regular.*

Proof. (29) is an immediate consequence of (27) and the fact that the ordering $\preceq$ is c-definable, where c depends only on k. (30) is a consequence of (24).

Definition. If f is an arbitrary Z_p-valued function defined on tbld_μ, then let $\mathrm{depth}(f) = \max\{\mathrm{depth}(\tau)|f(\tau) \neq 0\}$.

If $\mathrm{depth}(f) = \mathrm{depth}(\tau)$ and $f(\tau) \neq 0$ then $\tau \in f_{\min}$. Indeed if $\tau \notin f_{\min}$ then there is a $\tau_0 \neq \tau$ so that $f(\tau_0) \neq 0$ and $\tau_0 \sqsubseteq \tau$. This implies $\mathrm{depth}(\tau_0) > \mathrm{depth}(\tau)$ which contradicts to the defintion of depth(f).

(**31**) $\mathrm{depth}(f - \mathrm{tbasis}(\mathrm{bottom}(f)) < \mathrm{depth}(f)$.

Proof. Let $h = f - \mathrm{tbasis}(\mathrm{bottom}(f))$. By (27) for each $\tau \in f_{\min}$, $h(\tau) = 0$, so $h(\tau) \neq 0$ and $f(\tau) \neq 0$ implies $\mathrm{depth}(\tau) < \mathrm{depth}(f)$. Assume that $h(\tau) \neq 0$ and $f(\tau) = 0$. In this case τ appears with non-zero coefficint in $e_t^{\mu^*,\mu}$ for some t, with $\{t\} \in f_{\min}$, and $\tau \neq \{t\}$, and therefore we have again $\mathrm{depth}(\tau) < \mathrm{depth}(f)$. *Q.E.D.*(31)

Finally we note that (28) and Lemma 16 implies that

(**32**) *if f is d-regular then $f -$* tbasis(bottom(f)) *is d' regular, where d' depends only on d, p and k.*

Now we may prove (23). Assume that $\sum_{\tau \in \mathrm{tbld}_\mu} f(\tau)\tau = \sum_{t \in T^{\mu^*,\mu}} g(t) e_t^{\mu^*,\mu}$ and f is d-regular. We have to prove that g is d'-regular. We prove this statement

by induction on depth(f). If depth(f) $= 0$ then $f = 0$, $g = 0$ and therefore g is trivially d'-regular. (25) gaurantees that that depth(f) $\leq c$ where c depends only on k, therefore it is enough to show that if the statement of the lemma holds for every i, ($i \leq c$) with $d' \to d_i$ then it also holds for $i+1$ with $d' \to d_{i+1}$ where d_{i+1} depends only on p, k and d_i.

Assume that depth(f) $= i+1$. By (31) we have depth($f - \text{tbasis}(\text{bottom}(f))) \leq i$. Therefore by applying the inductive assumption to $f - \text{tbasis}(\text{bottom}(f))$ we get that $g - \text{bottom}(f)$ is $d_i - regular$. By (29), bottom(f) is $\bar{d}$ regular where $\bar{d}$ depends on only d_i, k and p so, according to Lemma 16, g is d_{i+1}-regular. *Q.E.D.*(Lemma 22).

We define the homorphisms $\psi_{i,v}$ as in [J] Definition 17.10 p. 67.

Lemma 33. *For all positive integers d, k and prime p there is a d' so that if $n > k$, μ^*, μ is a pair of partitions for n, and $\mu_1 = \mu_1^* = n - k$ then the following holds.*

Suppose that ψ, and c are defined as in [J], *Theorem 17.13, p. 69. If $a \in S^{\mu^*, \mu R_c}$ is d-regular with respect to the tabloid basis of $M^{\mu R_c}$ then there is a $b \in S^{\mu^*, \mu}$ so that $b\psi_{c-1,\mu_c^*} = a$ and b is d'-regular with respect to both the standard basis of $S^{\mu^*, \mu}$ and the tabloid basis of M^{μ}.*

Proof. First we show that the statement of the lemma is true if a is an element of the standard basis of $S^{\mu^*, \mu R_c}$. In this case using the identity $e_t^{\mu^*, \mu}\psi_{c-1,\mu_c^*} = e_{tR_c}^{\mu^*, \mu R_c}$ we may find a b of the form of $e_t^{\mu^*, \mu}\psi_{c-1,\mu_c^*}$ which is clearly d'-regular. For each $t \in T^{\mu^*, \mu R_c}$, let $\bar{t}$ be the smallest tableau so that $e_{\bar{t}}^{\mu^*, \mu}\psi_{c-1,\mu_c^*} = e_t^{\mu^*, \mu R_c}$. Clearly the function $t \to \bar{t}$ is d'-definable.

An arbitrary a is a linear combination of the elements of the standard basis of $S^{\mu^*, \mu R_c}$ so that the coefficients form a d-regular function on $T^{\mu^*, \mu R_c}$. We have to show that if we form with these coefficients the linear combination of the elements $e_{\bar{t}}^{\mu^*, \mu}$ then we get an d'-regular element of $S^{\mu^*, \mu}$.

Definiton. Assume that $\mu = \langle \mu_1, \ldots, \mu_r \rangle$ is a proper partition of n with r non-zero parts. Then according to Corollary 17.18 of [J], p. 72, we have

$$S^\mu = \bigcap_{i=2}^{r} \bigcap_{j=0}^{\mu_i - 1} \ker \psi_{i-1,j}.$$

Let $\Psi = \{\psi_{i-1,j} \mid 2 \leq i \leq r, 0 \leq j \leq \mu_i - 1\}$. This definition implies that $|\Psi| = n - \mu_1$. We will use this fact later.

The image of each $\psi \in \Psi$ is in some M^{ν_ψ} where $\nu_\psi \rhd \mu$. Let $Y^\mu = \bigoplus_{\psi \in \Psi} M^{\nu_\psi}$. There is a natural homomorphism η of M^μ into Y^μ. The mentioned Corollary implies that the kernel of η is S^μ.

Lemma 34. *For all positive integers d, k and prime p there is a positive integer d' so that if $\mu = \langle \mu_1, \ldots, \mu_r \rangle$ is a proper partition of n and $\mu_1 = n - k$ then the following holds.*

If $a \in M^\mu$ is d-regular in the tabloid basis, then for all $i = 2, \ldots, r$, $j = 0, \ldots, \mu_{i-1}$, $a\psi_{i,j}$ is d'-regular in the tabloid basis.

Proof. Let i, j be fixed. $\psi_{i,j}$ is linear map of M^μ, into M^ν, $\nu = \nu_{\psi_{i,j}}$. Therefore according to Corollary 21 it is sufficient to show that $f(\tau, \tau')$ is $\bar{d}$ regular, where $\tau \in \mathrm{tbld}_\mu$, $\tau' \in \mathrm{tbld}_\nu$ and $\tau\psi_{i,j} = \sum_{\tau' \in \mathrm{tbld}_{\nu'}} f(\tau, \tau')\tau$. More precisely we have to prove that the function $f'(x_1, ..., x_k, y_1, ..., y_k) = f(\mathrm{td}(x_1, ..., x_k), \mathrm{td}(y_1, ..., y_l))$ is $\bar{d}$-regular, $\nu_\psi = \langle n - l, ... \rangle$. ($\nu_{psi} \rhd \mu$ implies $l \leq k$.) This is however an immediate consequence of the definition of $\psi_{i,j}$.

Lemma 35. *For all positive integers d, k and prime p there is a d' so that if $n > k$, and $\mu = \langle \mu_1, \ldots, \mu_r \rangle$ is a partition of n, $\mu_1 = n - k$ then the following holds. If $a \in Y^\mu$ is d-regular with respect to the tabloid basis and $a = x\eta$ for some $x \in M^\mu$ then there is a $b \in M^\mu$ so that $a = b\eta$ and b is d'-regular with respect to the tabloid basis.*

Proof. There is a sequence $\mu^{(1)},\dots,\mu^{(i)}$, $i \le k$ of proper partitions of n and a sequence $c_1,\dots,c_{i-1}$ of positive integers I_n so that for each $1 \le j \le i$, $\mu^{(j)},\mu$ is a pair of partitions for n and the following requirements are met.

(**36**) $\mu^{(1)} = 0$, $\mu^{(i)} = \mu$

(**37**) for all $j = 1,\dots,i-1$ $S^{\mu^{(j)},\mu}\psi_{c_j-1,\mu^{(j)}_{c_j}} = S^{\mu^{(j)},\mu R_c}$ and

(**38**) $S^{\mu^{(j)},\mu} \cap \ker \psi_{c_j-1,\mu^{(j)}_{c_j}} = S^{\mu^{(j)}A_{c_j},\mu} = S^{\mu^{(j+1)},\mu}$.

(**39**) For every $h = 2,\dots,r$ and $g = 0,\dots,\mu_h - 1$ there is a j, $1 \le j \le i$, so that $\psi_{h,g} = \psi_{c_j-1,\mu^{(j)}_{c_j}}$. (Actually this holds with $h = c_j$ and $g = \mu^{(j)}_{c_j}$.)

Let $d = d_1 < \ldots < d_i$ be a sequence of integers which grows sufficiently fast with respect to d, k and p. (The sequence does not depend on n).

We will show by induction on j that

(**40**) *there is a $b_j \in M^\mu$ so that b_j is d_j regular with respect to the tabloid basis and for all $s = 1,\dots,j$ we have $x\psi_{c_s-1,\mu^{(s)}_{c_s}} = b_j\psi_{c_s-1,\mu^{(s)}_{c_s}}$.*

First we prove (40) for $j = 1$. Since $a = x\eta$ is d-regular with respect to the tabloid basis of Y^μ clearly $x\psi_{c_1-1,\mu^{(1)}_{c_1}}$ is also d-regular with respect to the tabloid basis of $M^{\mu R_{c_1}}$. Therefore Lemma 33 implies that there is a $b_1 \in S^{\mu^{(1)},\mu} \subseteq M^\mu$ so that b_1 is d'-regular in the tabloid basis of M^μ and $x\psi_{c_1-1,\mu^{(1)}_{c_1}} = b_1\psi_{c_1-1,\mu^{(1)}_{c_1}}$

Assume now that (40) holds for j and we will to prove it for $j+1$. Let $x_j = x - b_j$. Clearly for all $s = 1,\dots,j$ we have $x_j\psi_{c_s-1,\mu^{(s)}_{c_s}} = 0$ that is $x_j \in \ker \psi_{c_s-1,\mu^{(s)}_{c_s}}$. Using this fact and (38) we can prove by induction on s that $x_j \in S^{\mu^{s+1},\mu}$ and therefore $x_j \in S^{\mu^{s+1},\mu}$. Since both x and b_j are d_j-regular with respect to the tabloid basis of M^μ, x_j is d'_j-regular with respect to the tabloid basis. Let $u = x_j\psi_{c_{j+1}-1,\mu^{(s)}_{c_{j+1}}}$. According to Lemma 34, u is d''_j regular with repsect to the tabloid basis of $M^{\mu R_{c_{j+1}}}$ and so, by Lemma 22 it is d'''_j regular with respect to the standard basis of $S^{\mu^{j+1},\mu R_c}$. Therefore Lemma 33 implies that there is a $v \in S^{\mu^{(j+1)},\mu} \subseteq M_\mu$ which is d''''_j-regular with respect to the tabloid basis of M_μ so that $u = v\psi_{c_{j+1}-1,\mu^{(j+1)}_{c_{j+1}}}$. (Moreover $v \in S^{\mu^{j+1},\mu}$ implies, that $v\psi_{c_s-1,\mu^s_{c_s}} = 0$ for all $s = 1,\dots,j$). Therefore $b_{j+1} = v + b_j$ is a d_{j+1}-regular element of M^μ with the property: $x\psi_{c_{j+1}-1,\mu^{(j+1)}_{c_{j+1}}} = b_j\psi_{c_{j+1}-1,\mu^{(j+1)}_{c_{j+1}}}$, which completes the proof of (40).

By (39) $b = b_i$ satisfies the requirements of the Lemma.

Definition. We define a homomorphism $\rho = \rho^\mu$ of Y^μ onto $(S^\mu)^\perp$ in the following way. Each element $(x \in S^\mu)^\perp$ induces a linear functional ξ_x on M^μ which is defined by $a\xi_x = a \cdot x$ for all $a \in M^\mu$. Clearly all of the linear functionals that we get this way are distinct, they are 0 on S^μ, moreover we get this way every linear functional which vanishes on S^μ. (We get the identity of the two spaces of functionals from the equality of their dimensions.)

Each element y of Y^μ also induces a linear functional ζ_y on M^μ defined by $a\zeta_y = (a\eta) \cdot y$ for all $a \in M^\mu$. (We define the inner product on $Y^\mu = \bigoplus_{\psi \in \Psi} M^{\nu_\psi}$ with respect to the tabloid basis of the direct sum, that is the basis that we get by taking the union of the tabloid basis of each direct summand M^{ν_ψ}.) Since the kernel of η is S^μ, ζ_y vanishes on S^μ. According to our previous remarks, for each $y \in Y^\mu$ there is exactly one $x \in (S^\mu)^\perp$ so that $\zeta_y = \xi_x$. If x, y satisfy this identity then let $y\rho = x$. Clearly ρ is a homomorphism of Y^μ into $(S^\mu)^\perp$. To show that ρ is "onto" it is enough to show that every linear functional vanishing on S^μ is of the form ζ_y for a suitable $y \in Y^\mu$.

Since the kernel of η is S^μ, the image X of M^μ with respect to η is isomorphic to M^μ/S^μ. Therefore, for every linear functional f vanishing on S^μ there is a linear functional g on X so that $f = \eta g$. g can be extended into a linear functional defined on the whole Y^μ, therefore it can be written in the form ζ_y, that is $f = \zeta_y$.

Lemma 41. *For all positive integers d, k and prime p there is a d' so that for all n the following holds. Assume that $\mu = \langle \mu_1, \ldots \rangle$ is a proper partition of n, $\mu_1 \geq n - k$ and $y \in Y^\mu$. If y is d-regular with respect to the tabloid basis of Y^μ then $y\rho^\mu$ is d' regular with respect to the tabloid basis of M^μ.*

Proof. Let B be the tabloid basis of Y^μ. ρ^μ is a linear map of Y^μ into M_μ, therefore according to Corollary 21 it is sufficient to show that the function $f(b, \tau)$, $b \in B$, $\tau \in \mathrm{tbld}_\mu$ is d'-regular where $b\rho^\mu = \sum_{\tau \in \mathrm{tbld}_\mu} f(b, \tau)\tau$.

$f(b, \tau) = b\rho^\mu \cdot \tau = \tau\xi_{b\rho^\mu} = \tau\eta\zeta_b = (\tau\eta) \cdot b$. The proof of Lemma 34 implies that this is d'-regular as a function of τ and b.

Theorem 7' . *For all positive integers k, l and prime p, there is a positive integer d so that for all positive integer n the following holds. Suppose that λ^r, $r = 1, \ldots, l$ is a sequence of proper partitions of n, and for each fixed r, $\lambda^r = \langle \lambda^r_1, \ldots \rangle$. If $\lambda^r_1 \geq n - k$ for $r = 1, \ldots, l$ and N is a submodule of the direct sum $\bigoplus_{r=1}^{l} M^{\lambda^r}$ then there is a subset G of N containing at most d elements so that G generates N (as a submodule) and each $g \in G$, is d-regular with respect to the tabloid basis.*

Proof. There is a total order $\leq_P$ on the set of all partitions of n which is an extension of the $\lhd$ ordering. Let μ be the minimum of the partitions λ^r under this ordering. We prove the theorem by induction on μ with respect to the ordering $\leq_P$. (The induction will go downwards on the ordered set of partitions.) If μ has only one class (this is the greatest partition), then the assertion of the theorem is trivial, since M^μ is of dimension 1 and so the dimension of the direct product $\bigoplus_{r=1}^{l} M^{\lambda^r}$ is l. Therefore every element is d-regular (if d is sufficiently large with respect to l) and the direct product has a system of generators consisting of $l \leq d$ elements.

Assume that $\min_{r=1}^{l} \lambda^r = \mu$. First we prove the theorem in the $l = 1$ case, that is we assume that N is a submodule of M^μ. (We give this proof only to make it easier to understand the general case.) According to the submodule theorem [J], Theorem 4.8, p. 15, either $N \supseteq S^\mu$ or N is orthogonal to S^μ (where we define an inner product on M^μ with respect to the tabloid basis).

Case 1. $N \supseteq S^\mu$. Let η be the homomorphism of M^μ into Y^μ as defined before Lemma 35 and let $N' = N\eta$. $Y^\mu = \bigoplus_{\psi \in \Psi} M_{\nu_\psi}$ where $\nu_\psi >_P \mu$ and $|\Psi| = n - \mu_1 \leq k$ therefore according to the inductive assumption there is a $G' \subseteq Y^\mu$, $|G|' \leq \bar{d}$ so that each $g \in G$ is $\bar{d}$-regular with respect to the tabloid basis of Y^μ. Lemma 35 implies that for each $g \in G$ there is a $b_g \in M_\mu$ so that $b_g\eta = g$ and b_g is d-regular with respect to the tabloid basis of M^μ. Since S^μ is the kernel of η we have that $\{b_g\}_{g \in G'} \cup S^\mu$ generates N. S_μ can be generated by a single e_t which is, $c_{k,p}$-generic over the tabloid basis, where $c_{k,p}$ depends only on k and p (this is an immediate consequence of the definiton of e_t). Therefore $G = \{b_g\}_{g \in G'} \cup \{e_t\}$ generates N, $|G| \leq \bar{d} + 1 \leq d$ and each element of G is d regular with respect to the tabloid basis, which completes the proof of Case 1.

Case 2. $N \subseteq (S^\mu)^\perp$. Let $N' = N\rho^{-1}$. N' is a submodule of Y^μ. As in Case 1. we may apply the inductive assumption to $N' \subseteq Y^\mu$. Let G' be a set of generators for N' so that $|G'| \leq \bar{d}$ and each $g \in G'$ is $\bar{d}$-regular with respect to the tabloid basis of Y^μ. Since ρ is a homomorphism of Y^μ onto $(S^\mu)^\perp$, we have that $G = \{g\rho \mid g \in G'\}$ is a system of generators for N. Clearly $|G| \leq |G'| \leq \bar{d} \leq d$, and Lemma 41 implies that each $g \in G$ is d-regular with respect to the tabloid basis. Which completes the proof of Case 2.

Now we start the proof for the general case, that is, we will have no restrictions on l.

Lemma 42. *$(S^\mu)^\perp = \{a \in M^\mu \mid \forall t,\ a\kappa_t = 0\}$. Moreover if U is a submodule of M^μ wich is not contained in $(S^\mu)^\perp$, then for any μ-tableau t there is a $u \in U$ with $u\kappa_t \neq 0$.*

Proof. Let $X = \{a \in M^\mu | \forall t, a\kappa_t = 0\}$. If $(a \in S^\mu)^\perp$ then for any tabloid t we have $0 = a \cdot e_t = a \cdot \{t\}\kappa_t = (a\kappa_t) \cdot \{t\} = ce_t \cdot \{t\}$ where c is an integer. (The last inequality follows from Lemma 4.7 of [J], p. 14.) Since $e_t \cdot \{t\} = 1$ we have that $c = 0$ and therefore $a\kappa_t = 0$ that is $a \in X$.

If $a \in X$ and t is a tableau, then $a \cdot e_t = a \cdot \{t\kappa_t\} = a\kappa_t \cdot \{t\} = 0$ and therefore $a \in S^\mu$

Lemma 43. *Assume that U is a submodule of M^μ which is not orthogonal to S^μ, V is a homomorphic image of $(S_\mu)^\perp$, and ϕ is a homomorphism of U into V. Then $S^\mu \subseteq \ker \phi$.*

Proof. Since U is not orthogonal to S^μ, Lemma 42 implies that there is an $a \in A$ and a tabloid $\{t\}$ so that $a\kappa_t \neq 0$. According to Lemma 4.7 of [J] we have that $a\kappa_t = ce_t$ where $c \not\equiv 0 \bmod p$. Therefore $e_t\phi = c'a\kappa_t\phi = (c'a\phi)\kappa_t$. $c'a\phi = b\psi$ for some $b \in (S^\mu)^\perp$ and homomorphism ψ therefore by Lemma 42 $e_t\phi = (b\psi)\kappa_t = (b\kappa_t)\psi = 0$ and so $S^\mu \subseteq \ker \phi$.

Definition. 1. Assume that Γ is a finite set, n is a positive integer, and μ is a proper partition of n. $W_{\Gamma,\mu}$ will denote the direct sum $\bigoplus_{\gamma\in\Gamma} M^\mu$ that is the

direct sum of $|\Gamma|$ copies of M^μ. A Γ by Γ matrix will be a function defined on the direct product $\Gamma \times \Gamma$ with values in Z_p. If A is a Γ by Γ matrix, then we may define the action of a matrix $A = \{a_{\lambda,\mu}\}_{\lambda\in\Gamma,\mu\in\Gamma}$ on $W_{\Gamma,\mu}$. If $v \in W_{\Gamma,\mu}$ and $v = \langle v_\gamma | \gamma \in \Gamma\rangle$, then $vA = \langle v_\gamma|\gamma \in \Gamma\rangle A = \langle \sum_{\lambda\in\Gamma} a_{\lambda,\gamma} v_\lambda | \gamma \in \Gamma\rangle$. The map obviously is a $Z_p\mathbf{S}_n$homomorphism of $W_{\gamma,\mu}$ into itself.

2. $S^\perp_{\Gamma,\mu}$ will denote the set $\{\langle v_\gamma|\gamma \in \Gamma\rangle \in W_{\Gamma,\mu} \mid \forall\gamma \in \Gamma,\ v_\gamma \in (S^\mu)^\perp\}$. Clearly $S^\perp_{\Gamma,\mu}$ is a submodule of $W_{\Gamma,\mu}$.

3. pr_{γ_0} will denote the natural projection of a direct sum $\bigoplus_{\gamma\in\Gamma} V_\gamma$ onto V_{γ_0} defined by $\langle a_\gamma\rangle \mathrm{pr}_{\gamma_0} = a_{\gamma_0}$. If $\Gamma' \subseteq \Gamma$ then $\mathrm{pr}_{\Gamma'}$ will be the natural projection of the direct sum onto $\bigoplus_{\gamma\in\Gamma'} V_\gamma$. ι_γ and $\iota_{\Gamma'}$ will denote the corresponding natural injections.

Lemma 44. *If $U \subseteq W_{\Gamma,\mu}$, is a submodule not contained in $S^\perp_{\Gamma,\mu}$, and t is a μ-tableau, then there is an invertible Γ by Γ matrix A, and a $u \in U$ so that if $\langle v_\gamma|\gamma \in \Gamma\rangle = uA\kappa_t$ then there is a $\gamma_0 \in \Gamma$ so that $v_{\gamma_0} = e_t$ and $v_\gamma = 0$ for all $\gamma \neq \gamma_0$,$\gamma \in \Gamma$.*

Proof. Since U is not contained in $S^\perp_{\Gamma,\mu}$ there is a $\gamma_0 \in \Gamma$ so that U_{γ_0} is not contained in $(S^\mu)^\perp$, where $U_{\gamma_0} = U\mathrm{pr}_{\gamma_0}$. Lemma 42 implies that there is a $u' \in U_{\gamma_0}$ so that $u'\kappa_t \neq 0$. There is an $u = \langle u_\gamma\rangle_{\gamma\in\Gamma} \in U$ so that $u' = u_{\gamma_0}$. Let $u_\gamma\kappa_t = c_\gamma e_t$ (see. [J], Lemma 4.7, p. 14.). We know that $c_{\gamma_0} \not\equiv 0 \pmod p$. Let $A = \{a_{\lambda,\nu}\}$, where $a_{\lambda,\lambda} = c^{-1}_{\gamma_0}$ for all $\lambda \in \Gamma$ and $a_{\lambda,\gamma_0} = -c_\lambda c^{-1}_{\gamma_0}$. It is easy to check that A statisfies the conditions of the Lemma.

Lemma 45. *If U is a submodule of $W_{\Gamma,\mu}$, and t is a μ-tableau, then there is an invertible Γ by Γ matrix A, and a $\Gamma' \subseteq \Gamma$ so that the folllowing requirements are met:*

*(**46**) for all $\gamma \in \Gamma'$ there is a $u_\gamma \in U$ so that the γ component of $u_\gamma A\kappa_t$ is e_t, and all of the other components of $u_\gamma A\kappa_t$ are 0,*

*(**47**) for all $\gamma \in \Gamma - \Gamma'$ and for all $u \in U$ the γ-component of uA is in $(S^\mu)^\perp$.*

Proof. Let Γ' be a maximal subset of Γ so that the requirements of 46 are met with a suitably chosen invertible Γ by Γ matrix A. We claim that (47) holds for this Γ' and A. Assume that (47) is not true. Let $UA = \{uA|u \in U\}$. Clearly UA

is a submodule of $W_{\Gamma,\mu}$. Let $U' = U\mathrm{pr}_{\Gamma-\Gamma'}$ U' is a submodule of $W_{\Gamma-\Gamma',\mu}$. Since (47) is not true, U' is not contained in $S^{\perp}_{\Gamma-\Gamma',\mu}$. Therefore, by Lemma 44, there exist a $\gamma_0 \in \Gamma - \Gamma'$, $u' \in U'$ and an invertible $\Gamma - \Gamma'$ by $\Gamma - \Gamma'$ matrix A' so that the γ_0 component of $u'A'\kappa_t$ is e_t and all of the other components are 0. Let $u \in U$ so $u\mathrm{pr}_{\Gamma-\Gamma'} = u'$ and suppose that $uA\kappa_t = \langle h_\gamma e_t \rangle_{\gamma\in\Gamma}$ and $v = u - \sum_{\gamma_{\in\Gamma'}} h_\gamma u_\gamma$. If $\gamma \in \Gamma'$ then $vA\kappa_t\mathrm{pr}_\gamma = uA\kappa_t\mathrm{pr}_\gamma - \sum_{\gamma'\in\Gamma'} h_{\gamma'}u_{\gamma'}A\kappa_t\mathrm{pr}_\gamma$. Since (46) holds for the sequence $\langle u_{\gamma'}\rangle_{\gamma'\in\Gamma}$ we get that $vA\kappa_t\mathrm{pr}_\gamma = 0$ if $\gamma \in \Gamma'$. If $\gamma \in \Gamma - \Gamma'$ then $u_{\gamma'}\mathrm{pr}_{\Gamma-\Gamma'} = 0$ for all $\gamma' \in \Gamma'$ implies that $vA\kappa_t\mathrm{pr}_{\Gamma-\Gamma'} = u'\kappa_t$.

We extend the matrix A' into a Γ by Γ matrix $\bar{A}$. Let $\bar{A}$ be the Γ by Γ matrix that we get from A' by adding 1's to its new diagonal elements and 0 everywhere else and let $\tilde{A} = A\bar{A}$.

The set $\Gamma \cup \{\gamma_0\}$ with the matrix $\tilde{A}$ and the elements u_γ, $\gamma \in \Gamma$ and $u_{\gamma_0} = v$ satisfies the conditions of (46) in contradiction to the minimality of Γ'.

Now we return to the proof of Theorem 7'.

Lemma 48. *It is sufficient to prove Theorem 7' with the following additional reqiurements on the submodule N:*

There is an l', $0 \le l' \le l$ so that for all positive integers r, $1 \le r \le l$, we have

(49) *if $1 \le r \le l'$ then $\lambda^r = \mu$, if $r > l'$ then either $\lambda^r \neq \mu$ or $N\mathrm{pr}_r \subseteq (S^\mu)^\perp$*

(50) *if $1 \le r \le l'$ then $\{a\iota_r | a \in S_\mu\} \subseteq N$.*

Proof. We may assume without the loss of generality that $\lambda^1 = \ldots = \lambda^{r_0} = \mu$ and for all $r > r_0$, $\lambda^r \neq \mu$. Let $\Gamma = \{1, \ldots, r_0\}$, and $N\mathrm{pr}_\Gamma = U$. Applying Lemma 45 we get a $\Gamma' \subseteq \Gamma$ and an invertible matrix A with properties (46) and (47). Let $U' = UA$ and $N' = U \oplus N\mathrm{pr}_{\Gamma-\Gamma'}$. the conditions (49) and (50) are satisfied with $N \to N'$. Since (46) implies that U contains $S^\mu\iota_\gamma$ for all $\gamma \in \Gamma'$ it is easy to show that conditions (49) and (50) are satisfied with $N \to N'$.

If Theorem 7' is true with the additional requirements then there is a set of generators G for N', consisting of elements which are d-regular with respect to the tabloid basis and containing no more than d elements. We may define the action of A^{-1} on any element of $x \in N$ so that we apply A only to the Γ component of x and

leave the other components unchanged. It is easy to see that $G' = \{gA^{-1} | g \in G\}$ is a system of generators for U, each gA^{-1} is d'-regular and $|G'| \leq |G| \leq d'$.

Lemma 51. *It is sufficient to prove Theorem 7' with the following additional requirements on the submodule N:*

There is an l', $0 \leq l' \leq l$ so that for all positive integers r, $1 \leq r \leq l$, we have

(**52**) *if $1 \leq r \leq l'$ then $\lambda^r = \mu$ and $N\mathrm{pr}_r \subseteq (S^\mu)^\perp$,*

(**53**) *if $l' < r \leq l'$ then $\lambda^r \neq \mu$.*

Proof. We want to prove the theroem with the additional requirements (49) and (50). Suppose that the submodule N meets these requirements. We define a homomorphism ϕ of $\Lambda = \bigoplus_{r=1}^{l} M^{\lambda^r}$ into $\Lambda' = \bigoplus_{r=1}^{l'} Y^\mu \oplus \bigoplus_{r=l'+1}^{l} M^{\lambda^r}$. If $v = \langle v_1, \ldots, v_l \rangle \in \Lambda$ then let $v\phi = \langle v_1\eta, \ldots, v_{l'}\eta, v_{l'+1}, \ldots, v_l \rangle$, where η is the natural homomorphism of M^μ into Y^μ. Since $Y^\mu = \bigoplus_{\psi \in \Psi} M^{\nu_\psi}$, where $\nu_\psi \triangleright \mu$ we have that Λ' can be written in the form $\Lambda' = (\bigoplus_{r=1}^{l'} \bigoplus_{\psi \in \Psi} M^{\nu_\psi}) \oplus \bigoplus_{r=l'+1}^{l} M^{\lambda^r}$. This satisfies already the conditions (52) and (53) (if we rearrange the direct summands) with $N \to N\phi$. The conditions $N\phi\mathrm{pr}_r \subseteq (S^\mu)^\perp$ hold since the corresponding components were not changed by ϕ and by (49) the analogue statement was true for N.

If Theorem 7' holds with the additional requirements (52) and (53), then $N\phi$ has set of generators G' so that $|G'| \leq d$ and each $g \in G'$ is d-regular with respect to the tabloid basis. According to Lemma 35 for each $g \in G'$ there is an $a_g \in \Lambda$ so that $a_g\phi = g$ and each a_g is d'-regular. (We get a_g by applying Lemma 35 separately for each gorup of coordinates where ϕ acts as η and leaving the other coordinates unchanged.) Let $\bar{G} = \{a_g | g \in G'\}$. Clearly $\bar{G} \subseteq N$. We get a set of generators for N if we add to $\bar{G}$ for each r, $1 \leq r \leq l'$ an element b_r whose r-th component is e_t and all of the other componnents are 0 (for an arbitrary μ-tableau t). $G = \bar{G} \cup \{b_1, \ldots, b_{l'}\}$ is a set of generators for N so that each $g \in G$ is d' regular and $|G| \leq |G'| + l' \leq d'$.

Now we show that Lemma 51 implies Theorem 7'. Assume that N satisfies the conditions (52) and (53). Let $B = (\bigoplus_{r=1}^{l'} Y^\mu) \oplus \bigoplus_{r=l'+1}^{l} M^{\lambda^r}$. Let σ be the homorophism of B into $\bigoplus_{r=1}^{l} M^{\lambda^r}$ defined by

$\langle a_1, \ldots, a_{l'} a_{l'+1}, \ldots, a_l \rangle\sigma = \langle a_1\rho^\mu, \ldots, a_{l'}\rho^\mu a_{l'+1}, \ldots, a_l \rangle$

and let $N' = N\sigma^{-1}$. N' is a submodule of B which is of the form $B = \bigoplus_{j=1}^{\bar{l}} M^{\nu^r}$, where $\nu_r <_P \mu$ and $\bar{l} \leq lk$. Therefore by the inductive assumption there is a subset G' of N' with at most $\bar{d}$ elements so that each $g \in G'$ is $\bar{d}$-regular with respect to the tabloid basis. Let $G = \{g\sigma |\ g \in G'\}$. Clearly $|G| \leq \bar{d}$ and Lemma 41 implies that each $g \in G$ is d-regular with respect to the tabloid basis, which completes the proof of Theorem 7'.

4. Proof of Theorem 2. As we have mentioned already in the introduction, the theorem that we have proved about the representations of the symmetric groups (Theorem 7) implies a theorem about symmetric systems of linear equations where the variables correspond to μ tabloids, where $\mu = \langle \mu_1, ..., \mu_i \rangle$ is a fixed partition of n with $\mu_1 = n - k$. We reformulate now Theorem 2 with these types of variables then we prove the new theorem using Theorem 7. Theorem 2 will be an easy consequence of the reformulated theorem.

Definitions. 1. Suppose that k, i, n are positive integers $\mu = \langle \mu_1, ..., \mu_i \rangle$ is a partition of n and $\mu_1 = n - k$. Let $T = T_\mu$ be the set of all μ tabloids and let Γ be a finite set. Suppose that for each $a \in T$, x_a is a variable and for each $a \in T$, $i = 1, ..., l$, $u_a^{(i)} \in Z_p$, $b_{i \in Z_p}$.

We say that the system of linear equations $\sum_{a \in T} u_a^{(i)} x_a = b_i$, $i = 1, ..., l$ is symmetric if for each permutation π of the set $A = \{1, ..., n\}$ and $i = 1, ..., l$ there is an $i' = 1, ..., l$ so that for all $a \in T$ we have $u_{a\pi}^{(i)} = u_a^{(i')}$.

Theorem 54. *For all prime number p and natural number k there are natural numbers c, j so that for all natural number n the following holds:*

Suppose that $A = \{1, ..., n\}$ and $\mathcal{A} = \langle A, \leq, ... \rangle$ is an interpretation of the theory T_j^p. Assume further that Γ is a finite set with at most c elements, l is a natural number, $\mu = \langle \mu_1, ..., \mu_j \rangle$ is a partition of n and for all $i = 1, ..., l$, $a \in T_\mu$, $\gamma \in \Gamma$ we have $u_{a,\gamma}^{(i)} \in Z_p$ and $b_i \in Z_p$. If the linear system $\sum_{a \in T_\mu, \gamma \in \Gamma} u_{a,\gamma}^{(i)} x_{a,\gamma} = b_i$, $i = 1, ..., l$ is symmetric and it has a solution in Z_p then it also has a solution $x_{a,\gamma} = t_{a,\gamma}$ in Z_p so that for each fixed $d \in Z_p$ and $\gamma \in \Gamma$ there is a first-order formula $\phi_{d,\gamma}(y_1, ..., y_k)$ of the language L_j^p so that the length of $\phi_{d,\gamma}$ is at most c and for each $a = \langle a_1, ..., a_k \rangle$ we have:

$t_{a,\gamma} = d$ *iff* $\mathcal{A}_{A,\leq,j,p} \models \phi_{d,\gamma}(a_1, ..., a_k)$.

Proof. If the system is homogeneous then the trivial solution is first-order definable in the sense of the theorem. Therefore we may assume that the system is not homogeneous. In this case may assume that our symmetric system of linear equations is the symmetric hull of a system E which contains only homogeneous equations with a single exception and the exceptional equation has a 1 on its righthand-side. Indeed we may form classes from the equations so that two equations, equations number i and i', $1 \leq i, i' \leq l$, are in the same class if there is a permutation π of A with $u^{(i)}_{a\pi,\gamma} = u^{(i')}_{a,\gamma}$ for all $\gamma \in \Gamma$ and $a \in T_\mu$. We pick one equation from each class. Let $e_1, ..., e_{l'}$ be the eqautions that we get this way. Assume that $e_1, ..., e_{l''}$, $l'' \leq l'$ are the non-homogeneous ones among them. If necessary we may multiply these equations by a non-zero element of Z_p, so we may assume that the righthand-side of each of the equations $e_1, ..., e_{l''}$ is 1. The system of equations E consisting of the equations $e_1, e_2 - e_1, ..., e_{l''} - e_1, e_{l''+1}, ..., e_{l'}$ clearly satisfies all of our requirements and the set of solutions of its symmetric hull is the same as the set of solutions of the original system. Each evaluation of the variables $x_{a,\gamma}$, $a \in T_\mu$, $\gamma \in \Gamma$, can be associated with an element of $M_\Gamma = \bigoplus_{\gamma\in\Gamma} M^\mu$ (this is the direct sum of $|\Gamma|$ copies of M^μ), namely if $x_{a,\gamma} \to \alpha_{a,\gamma}$ is an evaluation it will be associated with the element $\sum \alpha_{a,\gamma} a^{(\gamma)}$ where $a^{(\gamma)}$ is the copy of a ocurring in the direct summand corresponding to γ. Let $\bar{e}_1$ be the equation that we get from e_1 by replacing the 1 on its righthand-side by a 0, and let E_1 be the system that we get from E by replacing e_1 with $\bar{e}_1$.

If e is the equation $\sum_{a\in T_\mu, \gamma\in\Gamma} u_{a,\gamma} x_{a,\gamma} = b$ then let $e\pi$ be the equation $\sum_{a\in T_\mu, \gamma\in\Gamma} u_{a\pi,\gamma} x_{a,\gamma} = b$. We will denote by E_2 the system that we get from E by discarding the equation e_1 and adding the following set of equations to the system: $\{e_1 - e_1\pi \mid \pi \text{ is a permutation of } A\}$.

Both systems E_1 and E_2 are homogeneous. Let $\tilde{E}_1$, $\tilde{E}_2$ be the symmetric hulls of E_1, E_2. $\tilde{E}_1$ is a homogeneous system therefore the the set of elements of M_Γ associated with its solutions form a submodule N_1 of M_Γ. We will denote by N_2 the sobmodule that we get in a similar way from $\tilde{E}_2$. Clearly every solution of $\tilde{E}_1$ is also a solution of $\tilde{E}_2$, therefore $N_1 \subseteq N_2$. The fact that the original inhomogeneous symmetric system has a solution implies that $N_1 \neq N_2$. Now we apply Theorem 7 with $N \to N_2$. Since G is a system of generators for N_2 there is a $g \in G$ so that $g \notin N_1$. Therefore the coefficients of g are first-order definable in the sense of Theorem 7 moreover $g \in N_2$,

$g \notin N_1$. Let $\bar{g}$ be the evaluation of the variables associated with the element g. Clearly $\bar{g}$ is a solution of $\tilde{E}_2$ but it is not a solution of $\tilde{E}_1$. Since it is not a solution of $\tilde{E}_1$ there is a permutaion π of A, so that if we evaluate the lefthand-side of $e_1\pi$ according to $\bar{g}$ then we get some $w \in Z_p$, $w \neq 0$. According to the definiton of E_2 the same must be true for e_1 itself. Hence the evaluation corresponding to the element $w^{-1}g$ is a solution of our original system and clearly it is first-order definable in the sense required by the theorem. *Q.E.D.*(Theorem 54).

Proof of Theorem 2. First we note that if the variables are associated not with arbitrary sequences but with sequences with distinct elements then the theorem is an immediate consequnce of Theorem 54. Indeed in this case let μ be the partition which has a single class of size $n-k$ and k classes of size 1. Since there is a natural one-to-one correspondence between this tabloids and the set of sequences of length k with distinct elements, the statements of the two theorems are the same.

The case of arbitrary sequences can be easily reduced to the case of sequences with distinct elements. Assume that $x_{a,\gamma}$ is a variable for all $a \in A, \gamma \in \Gamma$. Let $\bar{A}$ be the set of those elements of A^k which have k distinct elements.

For each sequence $a = \langle a_1, ..., a_k \rangle$ let P_a be the partition of $\{1, ..., k\}$ defined by iPj iff $a_i = a_j$. Let Γ' be the set of all partitions of $\{1, ..., k\}$ and let $\Gamma_1 = \Gamma \times \Gamma'$. If $a \in A^k$ and P_a has j classes then let $s(a)$ be a sequence of length j that we get from a by going along the sequence from left to right and deleting those elements which has already occured earlier.

Let $y_{a,\gamma}$ be a new variable for each $a \in \bar{A}$, $\gamma \in \Gamma_1$. For each of the original variables $x_{a,\gamma}$, $a \in A$, $\gamma \in \Gamma$ we define a set $S(a,\gamma)$ of the new variables in the following way: $y_{a',\gamma'} \in S(a,\gamma)$ if $\gamma' = \langle \gamma, P_a \rangle$ and the first $|P_a|$ elements of the sequence a' forms the sequence s_a. (Therefore if $|P_a| = j$ then $S(a,\gamma)$ has n^{k-j} elements).

Now we define a new linear system E_1 in terms of the variables $y_{a',\gamma'}$ which will be equivalent to the original system E in the following sense. Suppose that τ is an evaluation the variables $x_{a,\gamma}$ we define an evaluation τ_1 of the variables $y_{a',\gamma'}$ by $\tau_1(y_{a',\gamma'}) = \tau(a,\gamma)$ if $y_{a',\gamma'} \in S(a,\gamma)$. We will define the new system E_1 so that τ is a solution of E iff τ_1 is a solution of E_1.

For each equation e of E we define new equations by simultaneoulsy replacing each variable $x_{a,\gamma}$ in e, by a variable $y_{a',\gamma'} \in S_{a,\gamma}$. All of the equations that we get this way will be in E_1. Apart form these, E_1 will also contain all of the equations $y_{a',\gamma'} - y_{a'',\gamma''} = 0$ if there is a pair a, γ so that $y_{a',\gamma'}, y_{a'',\gamma''} \in S_{\gamma,a}$. It is easy to see that E_1 is indeed equivalent to E in the described sense and each first-order definable solution of E_1 leads to a firstorder definable solution of E. *Q.E.D.*(Theorem 2).

For the applications concerning the modulo p couniting principles we need variables associated with even more complicated structures. Namely there we need variables associated with a sequence $D_1, ..., D_j$ so that each element of the sequence is either a subset of A or a subset of $A \times A$, $j \leq k$, $|D_i| \leq k$ for $i = 1, ..., j$. Since such a sequence can be coded by an element of $A^{k'}$ where k' depends only on k this theorem follows easily from Theorem 2.

Finally we prove Corollary 6 using theorem 2.

Let E_1 be the system based on the quadruplet u', A_0, A', b. That an evaluation ν of the variables can be defined by first-order formulae which are in L^p_j and has a length not greater then c_1, where both j and c_1 depend only on k and p. If $a_1, ..., a_r$ are the elements of A', so that $a_1, ..., a_{r'}$ are all of the elements of A_0 then there is a first-order formula $\psi(x_1, ..., x_r)$ of L^p_j of length not greater than $c_2(k,p)$ so that ν is a solution of E_1 iff $\psi(a_1, ..., a_r)$ holds.

Let now E be the symmetric hull of E_1 that is the system induced by the quadruplet u', A_0, A', b. Clearly ν is a solution of E iff

$\forall x_1, ..., x_r \ (\bigwedge_{i \neq j} x_i \neq x_j) \rightarrow \psi(x_1, ..., x_r)$,

that is there is a firstorder ψ' in L^p_j os length at most $c_3(k,p)$ so that ν is a solution iff ψ' holds.

According to Theorem 2 if the system has a solution it has also a first-order definable solution where, the length of the defining formula χ is in L^p_j and its length is at most $c_4(k)$. Beacause of the existence of the formula ψ', for every possible choice of χ the fact whether χ defines defines a solution will be a firstorder sentence in some $L^p_{j'}$. Since the number of choices for χ depends only on k and p there is a single first-order formula ψ'' of some $L^p_{j''}$ of length at most c_4 so that ψ'' holds iff E has a solution moreover j'' and c_4 depend only on k and p. According to Corollary 11 this implies the assertion of Corollary 6.

REFERENCES

[Ajt1] M. Ajtai, The complexity of the Pigeonhole Principle 29-th, Annual Symposium on Foundations of Computer Science, 1988, 346-358. (Accepted to Combinatorica)

[Ajt2] M. Ajtai, "Parity and the Pigeonhole Principle definability on finite structures," in Feasible Mathematics, Progress in Computer Science and Applied Logic, Vol. 9. Birkhauser, 1990.

[Ajt3] M. Ajtai, "On the Existence of mod p valued Cardinality Functions" in Feasible Mathematics II, accepted for publication.

[Ajt4] M. Ajtai, "The Independece of the modulo p Counting Principles", in Feasible Mathematics II., (to appear) in preparation.

[AW] M. Ajtai and A. Wigderson, Deterministic simulation of probabilistic constant depth circuits, Advances in Computing Research, Volume 5, pages 199-222.

[J] G. D. James "Representation Theory of the Symmetric Group". Springer Lecture Notes, 1972.